VIOLATIONS OF HUMAN RIGHTS IN DIGITAL ENVIRONMENTS

Hedwig BICSKEI [*]

Abstract

I would like to present aspects related to violations of privacy and also accomplishments to protect privacy in online environments. Some important topics covered, are as they follow: violation of privacy by searching and seizing digital property belonging to individuals; profiling of marginalized groups, targets of specific ethnic, gender or age groups; biometric data saving according to which large groups of populations are monitored and penalized; censorship in countries like Turkey and China, where internet and free speech are censored; business surveillance and big data businesses where companies are accused of violating users' privacy and reducing freedom of expression.

In my paper I would also like to bring some light on the efforts to protect privacy, by the government and also through a multinational collaboration where entire nations are bonding to establish privacy-by-design controls like the GDP Regulation adopted by the European Union.

Key Words: *digital environment, human rights, violations, privacy, GDPR, European Union.*

JEL Classification: [K24, K38]

1. Introduction

Generally, privacy rights refer to a person's right to be free from intrusion into their personal life by another individual, business or government. Whether a person's privacy rights have been violated will depend greatly on the surrounding circumstances and the relationship between the parties.

Privacy is a fundamental human right recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights and in many other international and regional treaties. Privacy underpins human dignity and other key values such as freedom of association and freedom of speech. It has become one of the most important human rights issues of the modern age. Nearly every country in the world recognizes a right of privacy explicitly in their Constitution. At a minimum, these provisions include rights of inviolability of the home and secrecy of communications.

In the early 1970s, countries began adopting broad laws intended to protect individual privacy. Throughout the world, there is a general movement towards the adoption of comprehensive privacy laws that set a framework for protection. Most of these laws are based on the models introduced by the Organization for Economic Cooperation and Development and the Council of Europe.

[*] Assistant Professor, "Bogdan Vodă" University, Faculty of Law Cluj-Napoca.

In 1995, conscious both of the shortcomings of law, and the many differences in the level of protection in each of its States, the European Union passed a Europe-wide directive which will provide citizens with a wider range of protections over abuses of their data.[1] The directive on the "Protection of Individuals with regard to the processing of personal data and on the free movement of such data" sets a benchmark for national law. Each EU State was obliged to pass complementary legislation by October 1998.

The Directive also imposed an obligation on member States to ensure that the personal information relating to European citizens is covered by law when it is exported to, and processed in, countries outside Europe. This requirement has resulted in growing pressure outside Europe for the passage of privacy laws. More than forty countries now have data protection or information privacy laws.

2. The legal framework of privacy

Of all the human rights in the international catalogue, privacy is perhaps the most difficult to define and circumscribe (Michael, 1994, p.1). Privacy has roots deep in history. The Bible has numerous references to privacy (Hixson, 1987). There was also substantive protection of privacy in early Hebrew culture, Classical Greece and ancient China. These protections mostly focused on the right to solitude. Definitions of privacy vary widely according to context and environment. In many countries, the concept has been fused with Data Protection, which interprets privacy in terms of management of personal information. Outside this rather strict context, privacy protection is frequently seen as a way of drawing the line at how far society can intrude into a person's affairs (Davies, 1996, p.23). It can be divided into the following:

1) Information Privacy, which involves the establishment of rules governing the collection and handling of personal data such as credit information and medical records;
2) Bodily privacy, which concerns the protection of people's physical selves against invasive procedures such as drug testing and cavity searches;
3) Privacy of communications, which covers the security and privacy of mail, telephones, email and other forms of communication; and
4) Territorial privacy, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space.

The 1950 Convention for the Protection of Human Rights and Fundamental Freedoms[2], Article 8 states:

(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

*Lect. Univ., Universitatea Bogdan Vodă, Cluj-Napoca, Facultatea de Drept

[1] Directive 95/ /EC of the European Parliament and the Council On the Protection of Individuals with regard to the processing of personal data and on the free movement of such data.

[2] Convention for the Protection of Human Rights and Fundamental Freedoms Rome, 4.XI.1950, https://rm.coe.int/1680063765 accessed on 12/04/2020.

with the exercise of this right except as 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 of morals, or for the protection of the rights and freedoms of others.

Interest in the right of privacy increased in the 1960s and 1970s with the advent of information technology (IT). The surveillance potential of powerful computer systems prompted demands for specific rules governing the collection and handling of personal information. In many countries, new constitutions reflect this right. The genesis of modern legislation in this area can be traced to the first data protection law in the world enacted in the Land of Hesse in Germany in 1970 This was followed by national laws in Sweden (1973), the United States (1974), Germany (1977) and France (1978) (Flaherty, 1989).

Two crucial international instruments evolved from these laws. The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data[3] and the Organization for Economic Cooperation and Development's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data[4] articulate specific rules covering the handling of electronic data. The rules within these two documents form the core of the Data Protection laws of dozens of countries. These rules describe personal information as data which are afforded protection at every step from collection through to storage and dissemination. The right of people to access and amend their data is a primary component of these rules.

The expression of data protection in various declarations and laws varies only by degrees. All require that personal information must be:

1) obtained fairly and lawfully;
2) used only for the original specified purpose;
3) adequate, relevant and not excessive to purpose;
4) accurate and up to date; and
5) destroyed after its purpose is completed.

These two agreements have had a profound effect on the adoption of laws around the world. The OECD guidelines have also been widely used in national legislation, even outside the OECD countries.

3. Violations of human rights regarding privacy

3.1. Search and Seizure of Digital Property

[3] Convention on the Protection of Individuals with regard to the Automatic Processing of Personal Data - Convention, ETS No. 108, Strasbourg, 1981. https://rm.coe.int/1680078b37 accessed on 12/04/2020.

[4] OECD, Guidelines governing the Protection of Privacy and Transborder Data Flows of Personal Data, Paris, 1981, https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf accessed on 11/04/2020.

The right to conduct a search and seizure of persons or places is an essential part of investigation and the criminal justice system. The societal interest in maintaining security is an overwhelming consideration which gives the state a restricted mandate to do all things necessary to keep law and order, which includes acquiring all possible information for investigation of criminal activities, a restriction which is based on recognizing the perils of state-endorsed coercion and its implication on individual liberty. Digitally stored information, which is increasingly becoming a major site of investigative information, is thus essential in modern day investigation techniques. Further, specific crimes which have emerged out of the changing scenario, namely, crimes related to the internet, require investigation almost exclusively at the level of digital evidence. The role of courts and policy makers, then, is to balance the state's mandate to procure information with the citizens' right to protect it.

In the Romanian Criminal Procedure Code we may find the definition of the digital search in art. 168, para.1, which states: "any IT system or any data saving device search is done by research, finding, identifying and gathering evidence through adequate technical means and procedures, which ensure the integrity of the information withheld by these"[5]. The digital search and seizure must take place exclusively based on a search warrant issued by a judge, and it is done in the presence of the suspect or the indicted on one hand, the prosecutor and criminal investigation body on the other hand. The person who is subjected to the search is allowed to be assisted or represented by a trustworthy person. When the person whose IT system or data saving device is arrested or detained, he/she will be taken to witness the search; when this is impossible, the search will be done in the presence of a representative. The criminal investigation bodies must ensure that private life circumstance are not affected and do not become unjustifiably public during the search, a principle which is highly important, stated in the Budapest Convention (Crisan, 2017, pp. 249-258).

In the Constitution of the United States, it is the Fourth Amendment that expressly grants protection against unreasonable searches and seizure[6], however, without a clear definition of what is unreasonable, it has been left to the courts to interpret situations in which the right to non-interference would trump the interests of obtaining information in every case, leading to vast and varied jurisprudence on the issue. The jurisprudence stems from the wide fourth amendment protection against unreasonable government interference, where the rule is generally that any warrantless search is unreasonable, unless covered by certain exceptions. The standard for the protection under the Fourth Amendment is a subjective standard,

[5] Art. 168, para.1 Romanian Criminal Procedure Code.

[6] The Fourth Amendment to the Constitution of the United States of America: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

which is determined as per the state of the bind of the individual, rather than any objective qualifiers such as physical location; and extends to all situations where individuals have a reasonable expectation of privacy, i.e., situations where individuals can legitimately expect privacy, which is a subjective test, not purely dependent upon the physical space being searched.[7]

Therefore, the requirement of reasonableness is generally only fulfilled when a search is conducted subsequent to obtaining a warrant from a neutral magistrate, by demonstrating probable cause to believe that evidence of any unlawful activity would be found upon such search. A warrant is, therefore, an important limitation on the search powers of the police.

3.2. Profiling of marginalized groups, targets of specific ethnic, gender or age groups

Police in the modern age can target specific ethnic, gender and age groups. Many police departments have implemented a system which predicts potential perpetrators and victims of gun violence. Individuals may be intimidated or arrested based on their features or of those who they are associated with. This is the danger of big data mining which may be used to repress minorities.

China is extremely abusive when using the "police cloud" system, which was designed to track and to predict the activities of activists, dissidents, ethnic minorities. One important thing to remember in this matter is that China has no enforceable protections for privacy rights against state surveillance. The authorities are collecting and centralizing more and more information about hundreds of millions of ordinary people, identifying people who deviate from what they determine to be "normal thought" and then surveilling them. Authorities aspire to connect disparate databases to better enable data sharing and analysis across government departments, national and local levels, and from private sources.

Chinese police are using various applications to analyse large volumes and varieties of data, including text, video, and pictures. These applications can deliver useful analytics in real or near-real time, such as monitoring traffic patterns. Chinese police have said the use of big data will improve the police force's ability to search for suspects, predict crime, and respond efficiently. But some of these systems also enable the police to arbitrarily gain unprecedented information about the lives of ordinary people, including those who have no connection to wrongdoing.

China's most ambitious and privacy-violating big data project is the Police Cloud, this system scoops up information from people's medical history to their supermarket membership. This system allows the police to track where these individuals have been, who they are with, what they have been doing, as well as make predictions about their future activities. This is designed to uncover

[7] https://cis-india.org/internet-governance/blog/search-and-seizure-and-right-to-privacy-in-digital-age#fn5, The Centre for Internet & Society, accessed on 12/04/2020.

relationship between events and "hidden" people, i.e. who has been staying in a hotel, or travelling, etc. Some of the data collected refer to patient records, like names and illnesses, names and causes of petitioners, like individuals who complain to the government, but this police also gathers data including user names and their IP addresses from telecoms companies, usernames of social media accounts, internet forums, senders' and receivers' names, phone numbers, package content from delivery companies.

China does not have a unified privacy or data protection law to protect personally identifying information from misuse, especially by the government. The police do not have to obtain any sort of court order to conduct surveillance, or provide any evidence that the people whose data they are collecting are associated with or involved in criminal activity. Police bureaus are not required to report surveillance activities to any other government agency or to publicly disclose this information. In practice, there are no effective privacy protections against government surveillance. It is very difficult for citizens to know what personal information the government collects, and how the government uses, shares, or stores their data. There is no way for citizens to know if they are being classified as "focus personnel," much less to challenge their treatment if so classified, or if associated with people designated "focus personnel." Those who try to investigate government surveillance are vulnerable to being charged with crimes including "stealing state secrets."[8]

3.3. Biometric data saving according to which large groups of populations are monitored and penalized

Despite the very particular character of such information, there are virtually no legal provisions in the world that are specific to biometric data protection. Legal texts instead rely on provisions relating to personal data protection and privacy in the broad sense. But such legislation sometimes proves to be poorly adapted to biometric data.

The EU data privacy law defines biometric data as "special categories of personal data" and prohibits its "processing."

The definition recognizes two categories of information that could be considered biometric data. The first is information pertaining to bodily characteristics — i.e., a person's physical or physiological traits. This category is fairly straightforward and is consistent with what most people would think of as biometric data, such as facial information, fingerprints, iris scans, etc.

The second category of biometric data, behavioural information, is broader. Logically, any behavioural characteristics that could permit the unique identification of a person would be considered biometric data. However, it is unclear just how narrowly regulatory authorities will interpret this category or what

[8] https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissent, accessed on 14/04/2020.

limiting principles, if any, will guide their analyses. Plausibly, information pertaining to someone's habits, actions or personality could be considered behavioural information within the scope of the definition. This is a potentially broad category as it has no nexus to the sort of bodily information typically thought of as biometric data. Due to this inherent uncertainty, privacy professionals should closely monitor guidance delineating the types of behavioural information deemed biometric data. Further, privacy professionals should proactively identify any behavioural data their organizations are already be processing.[9]

As the GDPR considers biometric data to be a special category of sensitive personal data, processing and protecting it must proceed under the framework reserved for sensitive personal data generally. While the GDPR broadly prohibits the processing of sensitive personal data, it recognizes certain bases to justify its processing, chiefly, the explicit consent of the data subject, the performance of specific contracts or processing for certain specific purposes.

However, merely having a legal basis to process biometric data is not in itself sufficient, as the GDPR introduces a new requirement that data controllers must conduct a privacy impact assessment when processing is likely to result in a high risk to the rights and freedoms of Data Subjects. This is especially true when the processing involves the use of new technologies. Privacy impact assessments are mandatory in the case of automated processing, large-scale processing, or when data controllers systematically monitor a publicly accessible area on a large scale. Additionally, the GDPR requires data controllers to consult with supervisory authorities prior to processing when the privacy impact assessment indicates that processing is likely to result in a high risk to individuals and there is an absence of measures taken by the Data Controller to mitigate such risk. Practically speaking, this consultation requirement may likely be avoided by identifying the relevant risks and implementing measures tailored to mitigate them.[10]

The Regulation protects EU citizens and long-term residents from having their information shared with third parties without their consent. Their processing for "uniquely identifying a natural person" is prohibited. However, it does contain some exceptions:

- If consent has been given explicitly
- If biometric information is necessary for carrying out obligations of the controller or the data subject in the field of employment, social security and social protection law
- If it is essential to protect the vital interests of the individual and he/she is incapable of giving consent
- If it is critical for any legal claims
- If it is necessary for reasons of public interest in the area of public health.

[9] https://securelist.com/biometric-data-processing-and-storage-system-threats/95364/, accessed on 13/04/2020.

[10] https://iapp.org/news/a/processing-biometric-data-be-careful-under-the-gdpr/ accessed on 10/04/2020.

Moreover, the Regulation permits the Member States to introduce other limitations regarding the processing of biometric information.

3.4. Censorship

Having presented the case of China in a previous chapter, this part of the paper would like to present the phenomenon of censorship in Turkey. Censorship is regulated by domestic and international legislation, the country passed an internet censorship law in 2007 in order to regulate, and to 'clean' the internet from undesirable content, which resulted in the censorship of websites. The censored sites ranged from child and adult pornography websites to commonly used platforms such as YouTube, Blogger or Alibaba.com.

Disregarding crimes such as child pornography, which are unacceptable in all cultures, internet censorship is usually justified by protecting the so-called "existing social system" in any given country. In this context, the social system implies the social and economic relationships between social classes and individuals. There is also a second implication for the social system which has personal overtones in the context of censorship. Adult pornography is an example which is regarded as a threat to this perception of social system. Many countries either apply varying degrees of censorship or develop measures for enforcing self-censorship to protect their social systems. Albeit with much harsher measures, Turkey is no exception in this matter. Internet censorship in Turkey used to have mainly two pillars: preventing "undesired" political messages and fighting pornography. Indeed, the majority of blocked websites reported by are related to pornography. There are also websites of political nature which are regarded to be harmful. However, it must be stated that the phrase "existing social system" is getting increasingly vague in Turkey due to the fervent efforts of the ruling AKP party and President Erdoğan to transform the country into what he calls "new Turkey."[11]

Constitutional and international guarantees are undermined by restrictive provisions in the Criminal Code, Criminal Procedure Code, and anti-terrorism laws, effectively leaving prosecutors and judges with ample discretion to repress ordinary journalistic activities.[12] The 2017 Council of Europe Commissioner for Human Rights' report on freedom of expression and media freedom in Turkey reiterated that censorship problems stem mainly from the Turkish Criminal Code and the Turkish Anti- Terrorism Law No. 3713. Prosecutors continued to bring a number of cases for terrorism or membership of an armed organization mainly based on certain statements of the accused, as coinciding with the aims of such organization. According to the Council of Europe Commissioner and to the Venice Commission for Democracy through Law, the decrees issued under the state of emergency since July 2016, conferred an almost limitless discretionary power to the Turkish executive to apply sweeping misuse against NGOs, the media and the public sector.

[11] https://policyreview.info/articles/analysis/internet-censorship-turkey, accessed on 10/04/2020.

[12] https://freedomhouse.org/country/turkey, accessed on 13/04/2020.

Specifically, many NGOs were closed, the media organizations seized or shut down and public sector employees as well as journalists and media workers arrested or intimidated.[13]

3.5. Business surveillance

Facebook today has over two billion users. It enables people to share private data about themselves with others they know and trust. The company protects a large amount of user data. However, owing to unclear consent and sharing of data with third-party applications, many have discovered that detailed information about them, such as contacts, phone numbers, and likes, was being collected and shared without their consent or awareness[14]. Furthermore, Facebook provided administrative staff controls to erase messages, while users do not have the same controls over their own information[15].

Facebook is not alone in being accused of violating users' privacy. Agencies such as Equifax, which collected credit ratings for millions of people allowed its systems to be breached. Health insurance companies purchase big data from health care facilities to create predictive formulas for identifying risk pools and determining rates (Thielman, January 10, 2017)[16]. More and more businesses are utilizing big data for customer analytics.

The USA, once a leader of restricting invasions of privacy, adopted regulations in 2017 that will remove the tradition of net neutrality. The ramifications of this decision will reduce freedom of expression and increase the power of big data businesses to conduct mass surveillance and sell information about users' viewing content, purchases, and other personal information (Miles, 2017). Google and other large internet search sites already engage in such practices. They sell our information to advertisers, insurers, and lobbying groups, crafting the world that we are exposed to with almost no external ethical oversight.

And there is the situation with employee privacy all over the world as corporate surveillance technology monitors workers' every move. Overall, corporate interest in surveillance seems to be on the rise. A 2018 survey found that 22% of organizations worldwide in various industries are using employee-movement data, 17% are monitoring work-computer-usage data, and 16% are using Microsoft Outlook- or calendar-usage data.[17]

---

[13] *Ibidem.*

[14] https://www.npr.org/sections/thetwo-way/2018/03/26/597135373/ftcconfirms-its-investigating-facebook-for-possible-privacy-violations, accessed on 13/04/2020.

[15] https://techcrunch.com/2018/04/05/zuckerberg-deleted-messages/ accessed on 13/04/2020.

[16] Thielman, Sam. "Your private medical data is for sale – and it's driving a business worth billions". The Guardian. January 10, 2017, https://www.theguardian.com/technology/2017/jan/10/medical-data-multibillion-dollar-business-report-warns, accessed on 15/04/2020.

[17] https://www.cnbc.com/2019/04/15/employee-privacy-is-at-stake-as-surveillance-tech-monitors-workers.html, accessed on 15/04/2020.

From Amazon using a patent for an ultrasonic bracelet that can detect a warehouse worker's location and monitor their interactions, to Walmart, who listens in on workers and customers, to UPS using sensors in their delivery trucks to track the usage of seatbelts and maintenance, to Microsoft's Workplace Analytics, who monitors employers data, such as time spent on email, meeting time, and after hours work, all these present a huge risk to the individuals privacy. The emergence of sensor and other technologies that let businesses track, listen to and even watch employees while on company time is raising concern about corporate levels of surveillance. Privacy advocates fear that, if the new technology is not wielded carefully, workers could be at risk of losing any sense of privacy while on the job.[18]

4. Efforts to protect privacy

Despite negative trends in the digital age, the right to privacy is still championed as an ideal by most of us. Multinational collaboration to protect digital rights is on the rise. Nations are bonding together to establish privacy-by-design controls that will protect data according to commonly agreed fundamentals. Governments, businesses, and criminal organizations have profited by invading our privacy, and supranational bodies are a potential buffer- a last line of resistance. The European Union recently adopted the General Data Protection Regulation (GDPR), which entered into force on May 25, 2018.

The GDPR is a massive (99 articles over 88 pages and 55,000 words), complex, omnibus data protection law that provides a comprehensive legal framework for the protection of Europeans' personal data, as well as for the promotion of responsible data processing for a range of legitimate purposes. It overhauls the ways in which organizations collect, use, and share personal data. It does so largely by recognizing that rapid developments in digital technology have increased the scale, scope, and speed at which personal data are collected, used, and distributed, thereby necessitating a stronger legal framework that enhances the rights of "data subjects." It has direct impact on the conduct of biomedical research, given that much of this research relies on the use of individually-identifiable information. It is also, all things considered, a well-drafted piece of legislation that raises the standards of data protection globally.[19]

Conclusions

While governments are demonized as infiltrators of our privacy, they are also guarantors of our digital rights and can reprimand those who violate them. Legislation that safeguards sensitive data is important, and many countries are

[18] *Ibidem*.

[19] The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era Article (PDF Available) in The Journal of Law Medicine & Ethics 46(4):1013-1030 · December 2018, author Edward S. Dove.

struggling to keep pace with innovations in information technology that have expanded the realm of digital rights. Governments must both protect privacy and promote transparency, tasks that may seem at odds with one another but often function in tandem[20]. Governments can ensure that citizens are made aware of private information that is collected about them, as well as displaying information about what it does with that data and its own work. Medical data, for example, is private data that governments often enact legislation to protect. Otherwise, individuals could be discriminated against for employment and insurance. An important question that has been posed on the right to privacy is whether to provide people with access to medical records that show genetic dispositions to disease, as this information may not provide positive assistance when preventative precautions do not exist[21]. Governments must debate the levels of privacy and transparency that are in the best interests of its citizens. Voter rights to privacy are also important in democratic nations, as they guarantee the free choice underlying the spirit of elections. Cybersecurity is also a national responsibility as international conflicts between nation-states often spill over into digital environments.

Bibliography

1. Crisan, E. G., 2017, pp. 249-258. *Rolul perchezitiei informatice in probarea infractiunilor contra drepturilor de proprietate intelectuala,* Acta Univ. Sapientiae Legal Studies 6, 2.
2. Davies, S., 1996, p.23. *Big Brother: Britain's web of surveillance and the new technological order.* London: Pan.
3. Flaherty, D., 1989. *Protecting Privacy in Surveillance Societies,* University of North Carolina Press.
4. Hixson, R., 1987. *Privacy in a Public Society: Human Rights in Conflict 3.*
5. Michael, J., 1994, p.1. *Privacy and Human Rights,* UNESCO.
6. Miles, Tom. "U.N. freedom of speech expert concerned about net neutrality". Reuters. December 20, 2017: https://www.reuters.com/article/us-usa-internet-un/u-n-freedom-of-speechexpert-concerned-about-net-neutrality-idUSKBN1EE2DA, accessed on 15/04/2020
7. Thielman, S., January 10, 2017. *Your private medical data is for sale - and it's driving a business worth billions,* The Guardian, available at https://www.theguardian.com/technology/2017/jan/10/medical-data-multibillion-dollar-business-report-warns accessed on 15/04/2020
8. Convention for the Protection of Human Rights and Fundamental Freedoms Rome, 4.XI.1950, https://rm.coe.int/1680063765 accessed on 12/04/2020.
9. Convention on the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention, ETS No. 108, Strasbourg, 1981. https://rm.coe.int/1680078b37 accessed on 12/04/2020.

[20] https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyDigitalAge/PiratePartiesInternational.pdf.
[21] *Ibidem.*

10. OECD, Guidelines governing the Protection of Privacy and Transborder Data Flows of Personal Data, Paris, 1981, https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf accessed on 11/04/2020.
11. https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyDigitalAge/PiratePartiesInternational. pdf, accessed on 12/04/2020
12. The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era Article (PDF Available) in The Journal of Law Medicine & Ethics 46(4):1013-1030 · December 2018, author Edward S. Dove, https://www.researchgate.net/publication/330316678_The_EU_General_Data_Protection_Regulation_Implications_for_International_Scientific_Research_in_the_Digital_Era, accessed on 12/04/2020
13. https://www.npr.org/sections/thetwo-way/2018/03/26/597135373/ftcconfirms-its-investigating-facebook-for-possible-privacy-violations, accessed on 13/04/2020
14. https://techcrunch.com/2018/04/05/zuckerberg-deleted-messages/ accessed on 13/04/2020
15. https://www.cnbc.com/2019/04/15/employee-privacy-is-at-stake-as-surveillance-tech-monitors-workers.html, accessed on 15/04/2020.
16. https://policyreview.info/articles/analysis/internet-censorship-turkey, accessed on 10/04/2020.
17. https://freedomhouse.org/country/turkey, accessed on 13/04/2020
18. Directive 95/ /EC of the European Parliament and the Council On the Protection of Individuals with regard to the processing of personal data and on the free movement of such data.
19. https://cis-india.org/internet-governance/blog/search-and-seizure-and-right-to-privacy-in-digital-age#fn5, The Centre for Internet & Society, accessed on 12/04/2020.
20. https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissent, accessed on 14/04/2020.
21. https://securelist.com/biometric-data-processing-and-storage-system-threats /95 364/, accessed on 13/04/2020
22. https://iapp.org/news/a/processing-biometric-data-be-careful-under-the-gdpr/ accessed on 10/04/2020.