Media Diversity Institute
Armenia

Understanding digital rights in Armenia and their importance in the information society

by David Sandukhchyan

Yerevan
2021

Understanding digital rights and their importance in the information society

1. Introduction

This article aims to introduce the concept of digital rights as they are perceived by legal professionals, scholars, and human rights activities. The rapid development of digital technologies and communications resulted in many new legal and public policy areas such as, for example, personal data protection, cyber policing, cybersecurity and many others. This article covers only one of those areas, often referred to as digital rights. It might be interesting and useful for civil society activities, politicians, public authorities, and those involved in policy decision-making or public discussion of such policies.

The article is written primarily for the Armenian audience, and its first part contains the analysis of Armenian policies, legal and regulatory frameworks. Section two is devoted to the concept of digital rights in general. Section three describes the general concept of digital rights and covers specific areas of their implication and relevant international documents. The last two sections describe the analysis of the Armenian legislation in the context of the implementation of digital rights and proposes some steps for strengthening their protection.

2. What do we understand under digital rights?

Any theory starts from the definition of concepts and notions that make discussion possible. It is especially important when discussants are people with different professional, cultural and educational backgrounds. This approach is especially important for interdisciplinary discussions covering technology and legal topics.

The Foundation

One of the questions that legal professionals often discuss is how digital rights are different from traditional fundamental human rights. Fundamental human rights are a well-known legal concept of individuals' natural rights protected under the international human rights treaties, such as the Universal Human Rights Declaration and the European Human Rights Convention. Digital rights are a new concept that is not directly defined per se in international treaties and or declaration but often referred to the human rights in the digital environment.

To answer how digital rights are related to traditional human rights concepts and the differences (if any), we would need to consider the international and European treaties' relevant implementation guidelines. The Council of Europe has adopted a whole library of documents related to digital rights and Internet-related freedoms. One of the first documents was the Council of Europe was the Declaration on Freedom of Communication on the Internet adopted on 28 May 2003.

The Declaration on Freedom of Communication on the Internet[1] has not been written from scratch: it is based on the European Court of Human Rights case-law, European Union legislation governing specific areas of Internet application, such as EU directives on e-commerce and personal data protection. The Declaration outlines seven principles of the freedom of communication on the Internet that might be considered a basis for digital rights

[1] Council of European Committee of Ministers Declaration on Freedom of Communication on the Internet. Adopted 28 May 2003
https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805dfbd5

as they are known or perceived today by legal professionals and civil society activists. Other Internet freedom related documents adopted by the Council of Europe institutions, such as declarations, recommendations of the Committee of Ministers and Guidelines, reflect and link with these basic principles.

The principles set by the Declaration on Freedom of Communication on the Internet are closely linked with the freedom of expression protected under Article 10 of the European Convention on Human Rights. Nevertheless, the principles go beyond the freedom of expression and include other rights protected under the ECHR. That is a crucial fact that we will discuss later in this document.

The First Principle is related to the rules on content regulation. The principle of **Content Rules for the Internet** declares the member states shall not adopt restrictions for Internet-based content other than exist for other types of content delivery, i.e. communication and media. It looks like an obvious requirement for compliance with Article 10 of the European Human Rights Convention. However, it was not so undisputable in the early 2000s and is still questioned in some member states of the Council of Europe.

The Second Principle, defined as **Self-Regulation and Co-Regulation**, is quite broad and not well-articulated. It declares that "member states should encourage self-regulation or co-regulation regarding content disseminated on the Internet." However, even very declarative principles could be useful when the government or legislative decide on a particular mechanism for addressing a public policy issue. For instance, if a state wants to address the problem of hate speech on the Internet, it should invite industry representatives or associations to propose a non-legislative, i.e. self-regulatory solution or a model that will include both: involvement of government with the active input of the industry.

One of the most critical principles defined under the Declaration, which is directly linked with Article 10 of the European Human Rights Convention, is the third principle of **Absence of Prior State Control.** The principles could and should be interpreted as a ban on filtering and blocking information that might contain illegal or controversial content. The principle could be referred to as Internet censorship. This does not mean that non-state actors such as, for example, schools, universities or Internet public access providers, may not use filters against content that could be inappropriate for minors. Apparently, the principle does not apply to those who voluntarily limit his/her access to some category of resources.

The principle of Absence of Prior State Control is not absolute: Internet content blocking might be a legitimate measure for preventing crime when it contains a public danger or infringement of someone's rights. In such a case, public authorities must seek a judicial review or decision of a competent authority entitled to make such a decision under the law.

The fourth principle is defined under the declaration as follows: Removal of Barriers to **Individuals' Participation in the Information Society**. This principle is a positive obligation of the member states to ensure citizens' access to information services and eliminate restriction for exercising their rights guaranteed under Article 10 of the European Human Rights Convention. When adopting the Declaration, most European countries have already adopted the concept, and relevant regulatory instruments are usually referred to as 'universal services.'

The fourth principle assumes that member states shall have both: passive and active obligations to removing barriers for the use of the Internet by individuals. First of all, the

member states must not restrict individuals' rights to freely access the Internet, i.e. without permission, special registration, or any other administrative procedure. It looks like a normal practice, but it is not: in some non-member-states jurisdictions, access is granted individually upon registration, permission if the mandatory check of users identity.

However, access to and free use of Internet services is not the only possible restriction that the Fourth Principle of the Declaration aims to address. Removal of Internet use barriers can and should be interpreted as a right to own domain name (country code, generic or foreign) and freely publish information that is not subject to industry sector-specific regulation (see First Principle).

The next fifth principle, is also linked with the freedoms of using the Internet, but rather in the economic context than the freedom of information and communication. The principle is defined as **Freedom to Provide Service via the Internet**. It states that the Internet's services shall not be subject to specific permission or authorization on the sole ground they are offered via electronic communication means. This principle is very different from traditional, i.e. EHRC protected rights and freedoms since de facto declares guarantees for economic activities without barriers and administrative obstacles. This principle de facto declares that the right to carry out economic activities via the Internet is vital for all individuals and should not be restricted without a legitimate reason.

The sixth principle is also closer to Internet-related businesses' economic framework. It looks unusual that the Council of Europe document touches upon economic rights, not civil rights and fundamental freedoms. It is well-known from the early EU regulation on electronic commerce and is defined as Limited Liability of Service Providers for Internet content. The principle is based on the idea that Internet service providers must not be liable for the content they do not generate and shall not be obliged to monitor Internet content.

However, this principle's description explains that service providers could be co-liable for cases when they knowledgeably refused to remove or block illegal content upon its discovery or on legitimate demand. In such a case, service providers must receive explicit instructions from law enforcement authorities. Member states shall define such procedures that will balance the public internist of the freedom of expression and protection of the society from illegal or harmful content.

Finally, the seventh principle is one of the digital rights frequently discussed today, worldwide. This principle's definition is just one word, but it the most frequently attacked principle in the current Internet-related policies of both old and emerging democracies. This principle is the **Anonymity**, a right that is a purely digital age and has not been something to struggle for merely one generation ago.

Internet users' anonymity became important with increasing footprints that individuals leave on the Internet, the rapid development of data processing capacity, and artificial intelligence for user profiling. However, the Declaration states that respect for users' anonymity shall not be an obstacle for "member states from taking measures and co-operating to trace those responsible for criminal acts, in accordance with the national law."

The Declaration clearly states that measures shall be taken for tracing those who are responsible for criminal acts. This clause is important because it calls member states to abstain from mandatory authentication of Internet users. The principles of the respect and

protection of anonymity in Internet communication have strong justifications. The main reason is that individuals shall be confident about their security in cyberspace. Identified persons are more vulnerable to adversaries from both sides: cybercriminals and officials abusing their power.

The principle described as "Anonymity" is not limited to states' obligation to abstain from mandatory authentication of users by service providers with the further obligation to disclose the data to law enforcement and security authorities. This principle is much broader and covers several other obligations of states and private actors. In particular, it means that the member states shall not practice restrictions on the use of cryptographic means by individuals and businesses. It also means there shall not be restrictions on secure communication protocols, such as for example, virtual private networks, secure sell layer or use of specific types of security certificates.

The restrictions mentioned above may look preposterous, but they do exist in some countries, including one member of the Council of Europe. In 2020 Russian government circulated a draft law[2] restricting the use of the most recent versions of secure shell layer and transport layer security protocols and some other restrictions preventing users from browsing without a risk to be profiled using the resources they visited. In June 2019, Kazakhstan's government tried to force users to install government-issued security certificates to allow security authorities to intercept users' traffic[3]. Though these measures had been mostly failed due to the adequate response of tech giants (Apple, Mozilla and Google) and some technological restrictions, the fact by itself is notable and quite worrying.

Which rights did we get?

It would be correct to say that the Declaration of the Committee of Ministers on the Freedom of Communication on the Internet is a fundamental document defining the main principles that should govern future development of the Internet regulatory framework actress the wider Europe. The Declaration was adopted in 2003 and based on realities and understandings of that time. The technologies have been growing so fast that by 2020, Internet-related human rights issues have almost doubled. Moreover, the implementation of principles declared under the constitution became complicated, and the threats to digital rights became so complicated that required efforts of multi-sector professional groups.

The important fact is that the Declaration defines seven critical principles and provides a ground for further development of the digital rights concept. It does not cover all the rights that we may classify as digital, but those the member states agreed to be fundamental at that time. Furthermore, if summarised, the principles could be combined to define a specific digital right as we know them today. The rights as a compilation of the principles could be formulated as follows:

---

[2] Several Russian and international technology magazines reported on draft law restricting use of secure protocols circulated by Russian government in mid-September. According to draft law the use of security protocols hiding the identification of an Internet web page. https://regulation.gov.ru/projects#npa=108513

[3] In 2019 the government of Kazakhstan requested ISP's to suspend service of users that do not use government issued certificate. Later, when tech giants (Google and Mozilla) blocked those certificates the government of Kazakhstan changed the policy to mandatory use of certificates for certain country based resourced. https://en.wikipedia.org/wiki/Kazakhstan_man-in-the-middle_attack

- Right to access and use the Internet for searching, receiving and disseminating information through it without prior control and media-specific restriction of content. This definition is a compilation of first, third and fourth principles;
- Right to provide services on the Internet without subject-specific authorization with the sole ground of transmission used and without the service providers' obligation to monitor the content transmitted using their services;
- Right on anonymous use of the Internet, including anonymous search, receipt, and communicate without mandatory prior permission, authorization of authentication. This critical digital right is new even in the context of the Council of Europe's fundamental document: European Human Rights Convention.

One more principle that is not well-presented in the declaration is the privacy of Internet users. However, it is not because privacy is undermined by the Council of Europe. On the contrary, individuals' privacy is one of the areas that the Council of Europe has constantly been addressing. The privacy in digital time is specifically covered by the Council of Europe documents that are discussed in the next section.

What about privacy?

Indeed, the Declaration became an essential foundation for shaping a new concept in jurisprudence and human rights theory, which we now refer to as digital rights. As mentioned above, it does not cover the entire circle of digital rights and is missing such essential rights as privacy. However, it would be unfair to say that the Committee of Ministers ignored privacy or forget about it. The Council of Europe always played a leading role in promoting privacy-related standards and principles, and in 1981 opened a personal data protection convention for the member states' signature. The European Union's first document aimed at harmonizing the member states legislation with the Council of Europe standards was adopted only fourteen years later in 1995.

The Council of Europe Convention on Protection of Individuals with regard to Automatic Processing of Personal Data (Personal Data Protection Convention) was developed when both public and private organizations were making first steps towards the use of computers to increase operational efficiency. It was driven by the increasing volume of personal data collected and processed by businesses and governments. It is described on the Council of Europe site as *"the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data and which seeks to regulate at the same time the trans-frontier flow of personal data."*

At the time when the Personal Data Protection Convention has developed, possible abuse of personal data collection and processing has been limited to misuse of data that could link persons to each other, find their relations, property and additional private information and if leaked to be an instrument of blackmailing or fraud. Misuse of personal data in political processes has been one of the concerns of the Council of Europe experts and civil society. The focus on technological threats in personal data protection has been growing since the opening of the Personal Data Protection Convention for signatures by the member and non-member states.

One of the valuable contributions of the Council of Europe Personal Data Protection Convention is the definition of key concepts and notions that later have been used in almost all European data and privacy policies. The notion of personal data was defined as any information relating to an identified or identifiable individual. Next-generation documents, such as European Union Directive 95/46/EC[4] and then the General Data Protection

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of

Regulation, used more extended definition with examples and assumptions. However, this notion's evolution is very important because it reflects how technologies expand the scope of personal data.

The Council of Europe Convention	EU Data Protection Directive	EU General Data Protection Regulation
Any information relating to an identified or identifiable individual (data subject).	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.	Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Evolution of the definition of personal data protection.

As we see from this table, personal data has been initially defined as information related to the data subject. The definition under the EU Data Protection Directive is similar by its essence but includes some specific data, such as, for example, mental, social or cultural identity, as well as multi-factor identification, which we now call profiling. The definition also includes physical identity, which is also known as biometric data.

Although biometric data was not widely used in the 90s for identifying people, it is mentioned as information that could be used for that purpose. This is a brilliant example of predicting the potential threat to individuals’ privacy before it has appeared. Twenty years after biometric data became a common method for identifying people, and there were already adequate remediations to address these challenges. The next technologies bring more individuals identification to the attention of policymakers and privacy experts that are reflected in the General Data Protection Regulation.

It would be worth to mention that one of the first Council of Europe’s documents related to privacy protection Internet was the Committee of Ministers Recommendation No R(99)5 on the Protection of Privacy on the Internet. However, the Recommendation is limited to guidelines for users and Internet Service Providers concerning the good practices, potential threats and cooperation between private and state actors.

New generation regulation (primarily GDPR) includes identity information linked with individuals' behavior on the Internet and communication technologies in general. Personal

such data. Has been replaced by Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR) adopted in May 2016 and entered into the force on May 2018.

information traditionally used to identify people, such as biometric data and profiling, has been amended by a new category of identification methods: location data and online identifiers. These two categories of personal data became critical due to the increasing role of Internet services and Internet users' location-based profiling.

When speaking about the potential threats that technologies may cause in terms of tracking individuals behavior and their profiling, we have to mention another Declaration of the Committee of Ministers on Risks for Fundamental Rights Stemming from Digital Tracking and other Surveillance Technologies (adopted on 11 June 2013 at the 1173rd meeting of the Ministers Deputies – Declaration on the Risks of Digital Tracking). The Declaration starts with the phrase: “the propensity to interfere with the right to private life has significantly increased as a result of rapid technological development and of legal frameworks which are slow to adapt.”

The Committee of Minister's declarations are not legally binding documents. The principles they usually outline are the agreed policy guides rather than an obligation each member state undersigned. Nevertheless, even this type of documents could be considered a source of rights, especially if a particular case is brought for judgment to the European Court of Human Rights. The Declaration on Risks of Digital Tracking refers to rights on respect of private and family life (Article 8 of the European Human Rights Convention) and the European Court of Human Rights' relevant case-law.

The Declaration on Risks of Digital Tracking emphasizes that according to Article 8 of the European Human Rights Convention and ECHR case-law, states have negative obligations, that is, to refrain from interference with fundamental rights and positive obligations, that is, to actively protect these rights. In other words, states have negative obligations to limit interference in individuals’ private lives to the cases defined by the law and necessary to protect the public interest in a democratic society. As in any case, when the state’s interference is required for the protection of public interest, the measures must be adequate and not excessive. The states also have positive obligations to protect individuals’ privacy from others' illegal interference, including, but not limited to, private companies and other public actors.

It is important to note that the Declaration on Risks of Digital Tracking does not call for a complete ban on tracking technologies. Without any doubt, tracking devices, applications, and their features may serve legitimate goals and benefit the public. Location tracking features and users’ profiles help companies improve the quality of services and make that services more secure. Public authorities may use digital tracking to provide better services, rescue people, or prevent and combat crime.

On the other hand, digital tracking functionalities integrated into portable devices and their applications may also be used for unlawful purposes. Abuse of such functionalities may lead to illegal access, data interception or interference, system surveillance, and misuse of devices or other forms of malpractice. For example, geo-location tracking could be used for defining the typical behavior of a person and make him/her more vulnerable to stalking. Profiling might be used for microtargeting social network users and spamming.

The following six paragraphs are the actual text of the final part of the Declaration on Risks of Digital tracking:

- Alerts member states to the risks of digital tracking and other surveillance technologies for human rights, democracy and the rule of law and recalls the need to guarantee their legitimate use which benefits individuals, the economy, society at large, and the needs of law enforcement;

- Encourages member states to bear these risks in mind in their bilateral discussions with third countries, and, where necessary, consider the introduction of suitable export controls to prevent the misuse of technology to undermine those standards;
- Welcomes steps taken by data protection authorities in some member states to raise awareness of the implications of tracking and surveillance technologies and to investigate these practices to ensure compliance with the provisions of Convention No. 108 and their national legislations;
- Draws attention to the criminal law implications of unlawful surveillance and tracking activities in cyberspace and the relevance of the Budapest Convention in combating cybercrime;
- Welcomes measures taken by both state and non-state actors to raise awareness among users, and, a fortiori, within the private sector and among technology developers about the potential impact of the use of such technologies on human rights and the steps which can be taken at the design stage to minimise the risks of interferences with these rights and freedoms (e.g. “privacy by design” and “privacy by default”);
- Recalls the Council of Europe Internet Governance Strategy 2012-2015, which includes a number of action lines relevant to the challenges identified in this Declaration and looks forward to the concrete results of the work of the competent Council of Europe bodies.

Unlike the Committee of Ministers Declaration on Freedom of Communication on the Internet, this Declaration does not define any specific principles that member states must follow when adopting or revising their legislation. From the perspective of usefulness, it is much weaker than other Committee of Ministers declarations related to Internet freedom, governance or any other Internet-related topic. However, some useful outputs might be found here too.

Privacy by design

The main positive output is accepting the principle “privacy by design” and “privacy by default” as a sort of standard that industry shall follow, and states must at least encourage the industry to obey these standards. These principles are not something new that the Committee of Ministers invented or formulated by itself. “Privacy by design” and “privacy by default” are principles that have been known in the IT industry for several years.

The principle “privacy by design” was formulated by *Ann Cavoukian*, Canadian legal professional and former Privacy Commissioner of Ontario and became a standard incorporated in many privacy documents, including EU General Data Protection Regulation. This principle is very important and should be explained in detail. The principle “privacy by design” includes seven basic rules:

- Proactive not reactive - preventive not remedial
- Privacy as the default setting
- Privacy embedded into design
- Full functionality – positive-sum, not zero-sum
- End-to-end security – full life-cycle protection
- Visibility and transparency – keep it open
- Respect for user privacy – keep it user-centric

The first rule means that privacy protection measures must be taken before users' privacy has been endangered. It is worth noting that this rule is not solely for the design of equipment or software but also privacy-related procedures and policies. As a general privacy-related rule, it also should be used for designing business processes.

Privacy, as the default rule, is also a universal standard and should be applicable to both processes and products. The idea behind this rule is that any process or product should be designed and delivered with maximal privacy protection settings that can be adjusted to less protected if users wish so. Protection of privacy shall not be a burden of a system or device user.

Privacy enabled into the design is another important rule, which means that protection of privacy must be part of the product development objectives. It must be planned and checked at every stage of the project development and testing. Privacy protection tools shall not be added when the system design is completed.

Full functionality or positive-sum, not zero-sum rule means that maximum degree privacy shall not be reached by worsening other functionalities, such as, for example, usability or reliability of a product. It is especially unacceptable if the proper level of privacy is achieved by trading-off system security. Though, in some cases, it could be a non-trivial task, the system designers must work on the achievement of a win-win result (positive sum).

End-to-end security – **full life circle protection** is a well-known rule that is widely used in the system security model. It could be considered as a logical extension of the “privacy enabled into design” rule to the entire life-circle of the product or system. This means that privacy protection shall be maintained thought the entire life-circle of the product or system, including customer support during the operation and even at the phase of utilization.

Visibility and transparency or keeping it open is a rule that might be considered as an application o open-source philosophy to the privacy protection model. The objective of keeping a system open is not merely for the trust, though the element of trusting the system is important too. Unlike close or proprietary models, the open model helps its designers and architects receive feedback from the professional community and be aware of flaws and errors that may endanger the security and users’ privacy.

And last but not least, the rule is **Respect for user privacy and keep it user-centric.** The user-centric approach is one of the important ones for designing any product and service. Usually it means that the product should be shaped to serve users’ needs better and be convenient. That can include, but not be limited to, easy management of privacy settings, intuitive understanding of privacy level and awareness about possible privacy risks. For instance, a user may want to enable location service. He must be notified by the system about the potential privacy risks and switch it on and off by intuitive, easy-setting instruments.

Of course, the above-described principles and rules are not an obligation that the Council of Europe member states must fulfill. Ideally, public authorities should consider the “privacy by design” principle while developing e-governance and e-document system. Public authorities can also work with private companies and professional associations to promote these principles. However, it is hard to imagine that the “privacy by default” principle will be adopted as a legally binding obligation or a standard for non-governmental institutions and individuals.

Other outputs of the Committee of Ministers Declaration on Risks of Digital Tracking that are worth to mention are encouraging the member-states to negotiate bilateral treaties with other (non-member states) countries to introduce expert controls that may help to prevent trade in technologies that may misuse or undermine the privacy standard of the Council of Europe.

Another not less important output of the Committee of Ministers Declaration on Risks of Digital Tracking and drawing the member-states attention to digital tracking potential danger, especially for criminal investigations. The Committee of Ministers reefers to the Council of Europe Cyber Crime Convention as a standard for users' privacy. The issue of privacy in investigations of crime, which is one of the most problematic points of cyber jurisprudence, will be discussed in this document again and in different contexts.

The Council of Europe has definitely played a triggering role in building the foundation for the new generation of human rights that we refer to as 'digital.' Apart from the Data Protection Convention, Declaration on the Freedom of Communication on the Internet and Declaration on Risks of Digital Tracking the Council of Europe has adopted several documents related to Internet governance, domain name management and many others that are not discussed in this document since that are not directly linked with the main subject: the digital rights.

Is self-protection allowed?

Based on the above analysis, a notion of *digital privacy* could be defined. It is certainly based on the concept of a privacy protected under Article 8 of the European Human Rights Convention and supported by several other Council of Europe documents. Digital privacy could be viewed as an implication of private and family life in the digital environment. As was mentioned, public authorities have negative obligations of abstaining from interference into the private domain of Internet users and positive obligations to protect them from unwanted interference and misuse of individuals' personal data by others. Meantime, it is worth mentioning the legitimacy of users' self-protection, which is also an actively debatable topic of present days.

As it was designed, the Internet is an open communication model that enables the end-users, corporate and public players to employ different instruments of identity, anonymity, protection of privacy, and confidentiality of communication. On the one hand, this helps Internet users protect their privacy and anonymity irrespective of the service offered by service providers. On the other hand, the Internet's open model makes them vulnerable to anonymous adversaries. In this context, public authorities also have a negative obligation not to restrict individuals' rights on self-defense and a positive obligation to protect users from adversaries, manipulators and fraudsters.

An important policy approach should be mentioned in the context of the negative obligations of public authorities in respect of the protection of individuals' digital privacy. Like the protection of traditional privacy, individuals shall have a right to self-protection of digital privacy. One of the widely used digital privacy protection instruments is the virtual private network (VPN) and its varieties. In this context, the negative obligation of states shall be abstaining from the restriction on the use of VPNs and other privacy protection instruments.

VPN is a privacy protection mechanism that, to some extent, protects Internet users from intermediary attacks (men in the middle attack) and interception of web surfing queries at the local level, i.e. service providers. Stronger protection of privacy and confidentiality of the communication services could be achieved by using cryptography. Cryptography hides the communication content, i.e. provides confidentiality of messages, does not fully hide users' identity. Finally, a combination of VPN and cryptography and overlay network architecture provides a substantial level of privacy and anonymity.

All the technologies could be used by users from almost any European country, both Americas and most Asia countries, with some exceptions such as China, Syria, Iran, Pakistan and partially in Russia and Turkey. Notably, Russia and Turkey are members of the Council of Europe, which specifically address the rights to use VPN for the protection of privacy in the Committee of Ministers Recommendation Rec(2012)3 on the Protection of Human Rights with regard to Search Engines (Recommendation on Search Engines). This is

another important document on both the positive and negative obligations of the states in regard to the protection of digital privacy.

Privacy in the transparent world

The Recommendation Rec(2012)3 is an attempt to respond to several human rights concerns related to the search engines. In particular, it addresses such potential threats as a selective non-transparent listing of searched results, risks of listing explicit and controversial content by default on the one hand and non-transparent filtering on the other. Respect for privacy rights is one of the focal points of the Recommendation on Search Engines and provides members states with remediation guidelines.

More specifically, the Recommendation on Search Engines calls upon the member-states to ensure compliance with data protection principles and undertake the following actions:

- ensure that the collection of personal data by search engine providers is minimized. No user's IP address should be stored when it is not necessary for the pursuit of a legitimate purpose and when the same results can be achieved by sampling or surveying or by anonymizing personal data. Innovative approaches promoting anonymous searches should also be encouraged;
- ensure that retention periods are not longer than strictly necessary for the legitimate and specified purposes of the processing. Search engine providers should be in a position to justify with demonstrable reasons the collection and the retention of personal data. Information in this connection should be made publicly available and easily accessible;
- ensure that search engine providers apply the most appropriate security measures to protect personal data against unlawful access by third parties and that appropriate data breach notification schemes are in place. Measures should include "end-to-end" encryption of the communication between the user and the search engine provider;
- ensure that individuals are informed with regard to the processing of their personal data and the exercise of their rights, in an intelligible form, using clear and plain language, adapted to the data subject. Search engines should clearly inform users upfront of all intended uses of their data (emphasizing that the initial purpose of such processing is to better respond to their search requests) and respect the user's right with regard to their personal data. They should inform individuals if their personal data has been compromised;
- ensure that the cross-correlation of data originating from different services/platforms belonging to the search engine provider is performed only if unambiguous consent has been granted by the user for that specific service. The same applies to user profile enrichment exercises as also stated in Recommendation CM(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

It might be strange to see all these measures that the Committee of Ministers recommends adopting by states that may not have a relevant legal instrument to enforce these measures on search engine providers. Nevertheless, in many cases, enforcement of such measures by bigger states brings benefits to smaller nations, and the unified approach is important for the legitimacy of the enforcement.

Despite the Recommendations Rec(2010)3 have been adopted in regard to search engines, many of principles might be considered as universal approaches towards computer applications and systems. Here again, we come to the question where coregulation may play an important role. In many cases, strict regulations may harm the development of technologies and soft regulation, including coregulation, and industry self-regulation could be much more effective. Governments, however, may play the role of promoters of a high

standard when developing their own products and services, outsourcing or purchasing information technologies products.

Stricter rules are outlined in another document of the Council of Europe, the Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the Protection of Human rights with regard to Social Networking Services (Recommendation on Human Rights in Social Networking Services).

- Provide an environment for users of social networks that allows them further to exercise their rights and freedoms.
- Raise users' awareness, by means of clear and understandable language, of the possible challenges to their human rights and the ways to avoid having a negative impact on other people's rights when using these services.
- Protect users from harm without limiting freedom of expression and access to information.
- Enhance transparency about data processing and refraining from illegitimate processing of personal data.
- Set up self- and co-regulatory mechanisms where appropriate in order to contribute to the respect of the objectives set out in the Appendix to this recommendation.
- Ensure accessibility to their services to people with disabilities, thereby enhancing their integration and full participation in society.

As we can see from the Recommendation on Human Rights in Social Networking Services, privacy is one of the potential risks that users may face while using social networks.

Both search engines and social network platforms are encouraged to collect a minimal volume of personal data, and even when users share such data voluntarily, the service provider/owner must apply adequate measures for the protection of personal data. Another requirement is the processing of personal data transparently. In general, the transparency of business processes and algorithms became of the key indicators of data protection compliance.

The standards listed in the Recommendations on Human Rights in Social Networking Services could be directly applied to all kinds of computer applications processing personal data. We will demonstrate later in this document how the transparency rules are applied in another growing IT segment: artificial intelligence. Both social networking and artificial intelligence are IT segments where personal data is processed for microtargeting marketing and, therefore, user profiling.

Profiling is a new type of identity

When speaking about profiling, we must mention another Recommendation of the Committee of Ministers CM/Rec(2010)13 on the Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling (Recommendation on Individuals Profiling). Being, in fact, explanatory documents related to the application of Data Protection Convention the Recommendation CM/Rec(2010)13 defines specific rules for profiling related processes that member states and processors have to respect.
There is no need to present Recommendation on Individuals Profiling, which is mostly an interpretation of the Data Protection Convention in this particular context. However, it is worth to outline key definitions and principles of lawful processing. The definition of profiling is important because it is a frequently used notion. The Recommendation CM/Rec(2010)13 defines it as "an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to make decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviors and attitudes."

Why did the Committee of Ministers and the Council of Europe experts address the risks of profiling and developed specific recommendations on this matter? The expiation is simple and complex at the same time. The main reason for considering profiling as a new specific category and privacy risk is the creation of new personal data (profile), which, depending on the profiling goal, can better target an individual in a particular environment.

When personal data is processed without profiling, the data is accurate and relate to identified or identifiable individuals. Data subjects are generally aware of or can guess the nature of the information the data controller holds concerning them. Since profiling generates new data for an individual based on data relating to other persons, the data subject a priori cannot suspect the existence of correlation processes that might result in certain characteristics of other individuals being attributed to him or her on the basis of a probability calculation.

By its nature, profiling is a very specific process that may or may not correspond to the objective that the personal data have been originally collected for. The use of big data science makes profiling even riskier than ordinary routine processing of personal data. Algorithms may find a correlation between different data and result not only in new identification pattern but in segmentation and even worse discriminatory grouping. The growing risks related to automatic profiling found relevant remediations under the General Data Protection Regulation.

GDPR (Article 22) stipulates restrictions related to the use of personal data for profiling, formulated as follows: “The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.” Article 22 defines exceptions for cases processed on the ground of contract, data subject’s consent or with the purpose of safeguarding data subject’s rights, freedoms and legitimate interests. In other cases, data controller must implement measures for the protection of data subject rights, including human intervention in decision making. An Important fact is that profiling is a technological and business reality and must be addressed properly.

Automated decision-making. Should humans be protected from artificial intelligence?

Similar to many technologies impacting human society at a large scale the artificial intelligence (also often referred to as “automated decision-making” or “algorithm decision-making”) naturally possess some risks for individuals’ civil rights and freedom. The technologies per se cannot be risky or dangerous: humans who make them dangerous for themselves.

In spite of the tremendous benefits of the use of AI in public administration and business, it also contains significant risks for human rights endangering individuals’ privacy and the use of hidden discriminatory practices. When using AI, both public and private authorities must be extremely careful and consider human rights violations risks. The principles of safeguarding individuals’ civil rights and freedom while using artificial intelligence are quite similar to those that are used in the case of personal data processing.

The remediation of threats to human rights and freedoms with regard to artificial intelligence could also be found in the Council of Europe. One of such documents with a holistic approach towards the mitigation of AI-related risks is Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (AS). Recommendation CM/Rec(2020)1 is a comprehensive document covering different aspects of the development and operation of algorithmic systems.

The recommendation is composed of two main parts: the preamble and guidelines. The preamble describes what kind of human rights threats might contain artificial intelligence, what could be consequences of the irresponsible use of algorithmic systems for processing of personal data and automatic decision making based on the processing of such data. The

preamble of this document calls upon the member-states to undertake proposed measures for the elimination of potential threats of AI for human rights and fundamental freedoms.

The second part of the Recommendation CM/Re(2020)1, the Appendix, provides detailed guidelines on addressing the human rights impacts of the algorithmic system. Due to the substantial volume of the guidelines, only the most essential parts are discussed here or presented in summary. First and most important is the necessity to adopt legislation that would govern the development and application of algorithmic systems. The Recommendations on Human Rights Impacts of Algorithmic Systems encourages member-states to review existing legislation and consider the adoption of new legal acts addressing the issues of human rights in regard to the algorithmic systems.

The Recommendations on Human Rights Impacts of Algorithmic Systems advises building an institutional framework that would be capable to carry out expert analysis of relevant products and deliver an impartial professional opinion. It also strongly encourages cooperation between the private sector, civil society, scholars and public authorities in studying the impact of AI on human rights. A separate section is devoted to the private sector and how self-regulation should address potential risks of human rights violations when using autonomous algorithm systems.

One of the main principles applicable to both the public and private sector is the mandatory analysis of AI/AS impact on human rights. Risk analysis must be done in a possible transparent way, and the results must be open for the public. The use of algorithmic systems in public administration shall be strongly justified.

Another important principle is that only anonymized personal data could be used for processing by algorithmic systems. When outputs of the processing or automated decision-making are planned, individuals (data subject or user) must be informed about that and have an opt-out opportunity at any stage of the processing. The opt-out request should be simple, understandable and fast.

The principles and rules on the development and operation of AI/AS are under rapid development. It is anticipated that in the next couple of years, many international institutions will address this new challenge. For now, the Recommendation CM/Rec(2020)1 is the most useful document that governments and civil society may use for risk mitigation.

3. From declaration to implementation.

As we found out from the Council of European documents' analysis, there are at least four digital rights that we can call either transformation or implication of traditional human rights protected under the European Human Rights Convention, UN Human Rights Declaration and International Covenant on Civil and Political Rights. These rights are the following:

- Right to access and use the Internet for searching, receiving and disseminating information through it without prior control and media-specific restriction of content.
- Right to provide services on the Internet without subject-specific authorization with the sole ground of transmission used and without the service providers' obligation to monitor the content transmitted using their services;
- Right on anonymous use of the Internet, including anonymous search, receipt, and communicate without mandatory prior permission, authorization of authentication.
- Right on digital privacy including, but not limited to, the protection of privacy and personal data from illegal interference of public authorities, unlawful use of personal data by third parties, as well as the right on the use of privacy self-protection tools.

Profiling and risks related to artificial intelligence (algorithmic systems) are not listed as a separate category of human rights since they fall under the border concept of digital privacy rights. Classification is not formal and is not strictly legal. Each of the listed digital rights could be expanded or narrowed depending on the context.

Now, when the scope of rights defined, it is worth presenting how these rights are implemented and enforced.

Universal service as a right to access the Internet

Removal of administrative barriers such as pre-authorization and pre-authentication requirements for getting access to the Internet is the negative obligation of a state based on the human rights defined under Article 10 of the European Human Rights Convention. Negative obligations of governments related to Internet access freedom also assume specific rules for Internet published content. Content filtering and blocking are not allowed unless it is the individual's decision or imposed as a measure for preventing a particular crime according to the due process defined by the law.

Negative obligations are usually simple in terms of implementation. The public authorities merely need to follow the principles and guidelines agreed upon by exert and adopted by representatives of the member states. However, the government often tries to restrict individuals' freedoms justifying such restrictions by public benefits—the actual reasons for such restrictions, yet, unwillingness to find a more complex compliance model. Implementation of positive obligations is much more difficult in terms of choosing an appropriate approach, funding and enforcement, and here we can see differences in approaches and models.

One such mechanism is the concept of universal services that have been developed in the '90s. The concept has been shaped by two international institutions: The World Bank and European Union, and widely implemented in many developed and especially developing countries. The idea of the universal service is based on the definition of the minimal scope of services at the defined price available on the entire territory of the county.

Originally the scope of universal services included only voice telephone and public telephone registry. However, by the mid-2000s in most of the countries where the universal service model implied Internet access was included in the universal service package. Some countries, such as EU member states, went further and made broadband access a part of the universal service package. Less prosperous countries where subsidizing universal service is not feasible universal access implemented through community access services.

As noted, the universal service model is based on the principle of subsidizing access services in places (usually rural communities) where commercial services are not economically profitable. There are three basic models of universal service subsidies. One called 'universal obligation,' another 'universal fund' and the third model is the 'direct public subsidies.' Direct public subsidies are a straightforward approach when government invests in the network, operates it or outsources the operation at regulated prices.

Universal service obligation, which is often referred to as the 'cross-subsidy' model, is the licensing burden (obligations) of services providers and network operators to provide universal services on the entire territory of the country at the regulated price. The cost of service is usually shared with a profitable part of the services. And the final model is universal service fund when commercial service providers are obliged to pay a universal service fee (usually a certain percent of income) that government or independent regulator use for subsidizing universal service providers directly. A combination of models, state and community funding, co-funding and public-private partnership is practiced for building a most efficient model on a particular market.

Network neutrality

The vast majority of the European countries have solved the issues related to content restrictions in traditional media many years ago. Of course, rapidly developing digital media is constantly bringing new challenges to the courtrooms of national judicial and for the judgment of the European Court of Human Rights. However, core principles that are the absence of prior control and unacceptance of media-specific restrictions are implemented almost in all member-states.

Nevertheless, in some countries, especially Eastern Europe, but not only, but digital censorship also turned into a fight with content generation platforms, including social networks. We already discussed attempts to restrict specific Internet protocols in Russia and Kazakhstan. Restrictions on specific technologies such as communication protocols, network architecture or routing schemes are a real threat to Internet freedom nowadays.

An important reality is those content-related restrictions do not always come from the public authorities. Serious battles over the abolishment of economic discrimination of Internet traffic priorities have been going on over the world since telecommunication operators realize that traditional business models are not that profitable as they use to be. The Council of Europe responded to the issue of discrimination of traffic with the Declaration of the Committee of Minister on network neutrality adopted by the Council of Ministers on 29 September 2010.

The Declaration states that free access to Internet-based content could be considered free only when applications and services are not discriminated against their nature, i.e. commercial or non-commercial. The principle of network neutrality is declared as a universal rule that should apply irrespective of the infrastructure or the network used for Internet connectivity.

Right to provide services on the Internet

Borne, as a means of critical communication very soon, the Internet became a place for business. Small and large businesses, local and global traders shift their attention to digital trading platforms. Public authorities realize that on the one hand, Internet commerce has enormous potential for economic growth and, on the other hand, contains several risks for both businesses and their customers. The Declaration on Freedom of Communication on the Internet of the Committee of Ministers declared the general principles of the freedom of business on Internet, including limited liability of service providers and the absence of specific regulation related to the business methods (Internet-based).

The most valuable legal document that played a substantial role in the development of Internet-based business and e-commerce worldwide is Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, also known as EU Directive on E-Commerce. The E-Commerce Directive defines fundamental rules that pre-defined the legal frameworks of electronic commerce for decades not only in the EU but in many other countries, including Eastern European states.

E-Commerce Directive states that member states must ensure that an information society service provider's activity may not be made subject to prior authorization or any other requirement having equivalent effect. Nevertheless, alongside the principle of general authorization E-Commerce Directive makes a reservation for countries to impose pre-authorization for some type of activities, such, for example, notaries, attorneys representing clients before the courts and medical practitioners. The Directive also made a reservation for gambling and lotteries.

Another necessary provision of the E-Commerce Directive defines that the EU member states shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:

- does not initiate the transmission;
- does not select the receiver of the transmission; and
- does not select or modify the information contained in the transmission.

The relevant provision of the E-Commerce Directive also required member states not to impose a general obligation on providers to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

The Directive contains several other positive obligations of states that are important for the normal operation of companies on digital markets. In particular, it also addresses such issues as unsolicited electronic commercial communications, court disputes resolution, the validity of the online contract and some other important aspects of e-commerce and electronic businesses. However, these regulatory standards are not fully relevant to the subject of this paper, which is primarily focused on digital rights rather than broad economic aspects of the digital economy.

Right on anonymous access and right on digital privacy

The right to anonymous access is clearly defined under several documents of the Council of Europe, including the Committee of Ministers Declaration on Freedom for Communication on the Internet. It looks to be a very easy implementing negative obligation of a state, but it faces large attacks from law enforcement institutions not only in new democracies but even in some traditional liberal democracies. In most cases, anonymity and digital privacy are challenged together, and in fact, these two rights are closely linked.

Anonymity helps to protect privacy, and protected privacy, by definition, helps to hide individuals' identities. In the age of big data, even anonymized personal data could be used for tracking individuals and finding their identity indirectly. This is one of the reasons for considering these two rights together. Another reason for the assessment of anonymity and privacy together is the overlapping legislation regulating these two interlinked digital rights.

The European Union is one of the pioneering institutions in the recognition and protection of digital rights. The EU Data Protection Directive 95/46/EC was one of the standards that many countries followed for decades. EU General Data Protection Regulation that replaced the Data Protection Directive in 2018 raise personal data protection to an even higher level. Due to its large market and purchase capacity, EU standards have been adopted by many other countries that want to supply goods and services in Europe.

In spite of high-level personal data protection standards on 15 March 2006, the European Parliament and the Council adopted the Data Retention Directive[5]. The Data Retention Directive required the providers of publicly available electronic communications services or public communications networks to retain traffic and location data belonging to individuals or legal entities. Such data included the calling telephone number and name and address of the subscriber or register user, user IDs (a unique identifier assigned to each person who signs with an electronic communications service), Internet protocol addresses, the numbers dialled, and call forwarding or call transfer records.

The retention period was to last for a minimum period of six months and up to two years, and the sole purpose of processing and storing the data was to prevent, investigate, detect, and prosecute serious crimes, such as organized crime and terrorism. The content of the

[5] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

communications of individuals was not retained. Based on the mentioned provision of the Data Retention Directive, many EU member states have adopted national legislation requiring Internet service providers (ISP) to retain personal data of users without the consent of data subjects.

Legislations adopted by national states have been challenged by a group of lawyers in Ireland and Austria. Irish legal firm Digital Rights Ireland has challenged the national legislation on the ground of non-proportional measures provided under the Directives without adequate safeguards of individuals' data. According to the European judicial framework, the national courts, in adjudicating cases, have the right to refer legal inquires to the European Court of Justice concerning the validity of national legislation adopted under the European legal framework.

The European Court of Justice has found that the stated that the retention of data in order to allow access by the competent national authorities constitutes processing of data and therefore affects two basic rights of the Charter of Fundamental Rights: the right to private life guaranteed by article 7, and the protection of personal data guaranteed by article 8. The European Court of Justice also found that the relevant provision of the Data Retention Directive violates the principle of proportionality. The Data Retention Directive becomes invalid from the time it became effective in 2006. The EU Members that have transposed the Directive into their national legal systems are required to take steps to ensure compliance with the judgment.

The European Court of Justice's ruling on the Data Retention Directive is a bright case of fundamental rights, including based on the digital rights of individuals, overriding European legislation that introduces non-proportional security measures. However, judicial review and enforcement are not the usual instruments for the protection of privacy and anonymity. The main instruments remain penalties and fines for the violation of data protection and privacy legislation and criminal liability for knowledgeable and wilful misuse of personal data. Penalties and fines prescribed under the GDPR vary from 10 to 20 million Euros or from 2% to 4% of the annual worldwide turnover of non-compliant companies.

4. Digital rights in Armenia

Armenia is a member of the Council of Europe and signatory of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Armenia also a signatory of the Budapest Convention on Cyber Crime, which also an important legal instrument in defining positive and negative obligations of Armenian authorities regarding due diligence procedures and other standards in the investigation of cybercrimes. Armenia has a relatively high internet freedom rank (75 according to the Freedom House Internet Freedom Research[6]) placed between Argentina and Japan, one score less than France and the USA.

Right to access the Internet (Armenia)

In spite of small territory Armenia still has limited opportunities for providing universal access to the entire territory of the country. Armenian authorities have originally[7] adopted the universal service fund model, which has never been established due to the disagreement of key policy and market players regarding the detailed legal framework, universal service fees, and subsidizing mechanism. Meantime, mobile Internet coverage is pretty good in Armenia, and generally, services are available everywhere at relatively affordable prices.

[6] Freedom House Assessment of Internet freedom 2019. Internet freedom 2019. https://freedomhouse.org/country/armenia/freedom-net/2020

[7] The Law of the Republic of Armenia on Electronic Communication of 2005. Art. 40.

Network neutrality (Armenia)

Network neutrality has never been introduced in Armenia. The Armenian National Regulatory Authority made several announcements about technological neutrality to be an important principle of regulation and policy enforcement. In spite of this fact, the network neutrality principle has never been adopted as a binding regulatory rule. The attempt of civil society to advocate the adoption of network neutrality standards under the Law on Electronic Communication faced strong resistance from network operators. The debates on the law amendments are still going on and will depend on the position of the government and members of the ruling parliamentary fraction.

Regulation of Internet-related businesses (Armenia)

Due to several European integration initiatives implemented during the past two decades, Armenian e-commerce legislation reflects the principles of the rights on Internet-based business activities. However, Armenian e-commerce legislation is not fully in line with the EU E-Commerce Directive. In particular, Armenia does not have well-defined rules on electronic unsolicited commercial communication (electronic spam) and does not have online arbitration requirements. However, part of the E-Commerce Directive related to service providers' limited liability is fully implemented under the amended Articles 416.1 and 416.2 of the Civil Code.

E-Commerce, however, is not the only type of Internet-based business, and the right on business on the Internet is not limited to e-commerce and e-trading. The basic element of all digital businesses is telecommunication services. The regulatory framework of telecommunications is much more complicated and include many directives and regulations. There is no need to discuss all the regulatory principles of telecommunication businesses, but only those of them that are very important in the context of freedom of Internet business and freedom of communication on the Internet.

Liberalization of telecommunications markers has been undertaken in the EU as a ground for the development of the industry. European policymakers believed that the industry could boost only the liberal regulatory environment. This policy approach has been implemented in EU Access Directive (to be replaced soon by European Electronic Communication Code), which states that electronic communication business should be subject to licensing, but general authorization unless it requires scarce resources or public funds. Armenian telecommunications legislation, which is too great extent based on the European regulatory principles, still requires network operators to obtain a license through the assessment procedure.

Right on anonymity and digital privacy

Implementation of the right to anonymity and digital privacy in Armenia is at the initial stage. Armenia has signed and ratified the Council of Europe Convention on Personal data protection; however, it largely aligned its legislation with European principles only in 2015. The anonymity of Internet access is respected but periodically challenged using the mobile identification model as in many post-soviet countries. Each such attempt faces the resistance of the Internet community, but after some period comes back again and again.

The most recent attempt of civil society to promote regulation prohibiting the bulk collection of personal data has been failed due to the resistance of law enforcement bodies and the ministry of high technology industry. Nevertheless, civil society activists continue advocating for changes, also promoting network neutrality regulation. Penalties for violation of personal data protection law are insignificant and, therefore, cannot guarantee a proper level of data protection.

Annex I – Subject relevant international documents

1. The Convention for the Human Rights and Fundamental Freedoms (European Human Right Convention). Drafted in 1950 by the Council of Europe, entered into the force on 3 September 1953.
2. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, 28 January 1981.
3. Declaration on freedom of communication on the Internet. (Adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers' Deputies).
4. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
5. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.
6. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
7. Recommendation CM/Rec(2015)6 of the Committee of Ministers to member States on the free, transboundary flow of information on the Internet
8. Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users (Adopted by the Committee of Ministers on 16 April 2014 at the 1197th meeting of the Ministers' Deputies).
9. Declaration of the committee of Ministers on risks to fundamental rights stemming from digital tracking and other surveillance technologies (Adopted by the Committee of Ministers on 11 June 2013 at the 1173rd meeting of the Ministers' Deputies).
10. Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines(Adopted by the Committee of Ministers on 4 April 2012 at the 1139th meeting of the Ministers' Deputies).
11. Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services (Adopted by the Committee of Ministers on 4 April 2012 at the 1139th meeting of the Ministers' Deputies).
12. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
13. Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. (Adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Ministers' Deputies).