AMERICAN UNIVERSITY OF ARMENIA

ՀԱՅԱՍՏԱՆԻ ԱՄԵՐԻԿՅԱՆ ՀԱՄԱԼՍԱՐԱՆ

LL.M. Program

ԻՐԱՎԱԳԻՏՈՒԹՅԱՆ ՄԱԳԻՍՏՐՈՍԻ ԾՐԱԳԻՐ

TITLE

DATA PROTECTION IN SOCIAL NETWORKS: COMPARISON BETWEEN ARMENIAN AND EUROPEAN UNION LAW

STUDENT'S NAME

Diana Sakanyan

SUPERVISOR'S NAME

Lilit Banduryan

NUMBER OF WORDS

11870

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

CoE	Council of Europe
CJEU	Court of Justice of the European Union
DPA	Data Protection Act
EC	European Commission
ECD	E-Commerce Directive
ECHR	European Convention of Human Rights
EDPS	European Data Protection Supervisor
EU	European Union
FBI	Federal Bureau of Investigation
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
RA	The Republic of Armenia
SNS	Social Networking Services
UK	The United Kingdom
WP29	Article 29 Working Party

INTRODUCTION

"Digital freedom stops where that of users begins..."

Stephane Nappo

An Austrian law student requested all the information that a social networking site kept about him on his profile. The social network sent him 1,224 pages of information. This included photos, messages, and postings on his page dating back several years, some of which he thought he had deleted. He realized that the site was collecting much more information about him than he thought and that information he had deleted – and for which the networking site had no need – was still being stored[1].

Have you ever thought how much data of yours is being kept daily for several years even for decades in social networking systems? Over recent years, social networks have gained an important role in enabling citizens to connect with each other, obtain information quickly, and participate in matters that affect them. This is a positive development as social networks allow people to become more active and informed citizens[2].

Social networks give us an opportunity to stay in touch with friends, family members, and colleagues, but they also present a risk that personal data, such as photos, videos, comments, marital status, or location details might be viewed more widely than we could imagine. In many cases, this can have financial, reputational, and even psychological consequences for the amateur "users". A large majority of Europeans (71%) think that the disclosure of personal data is an increasing part of modern life. At the same time, more than six out of ten users say that they do not trust landline or mobile phone companies and internet service providers (62%) or online businesses (63%). They feel they do not have complete control of their data[3]. A high level of data protection is essential to foster people's trust in online services and in the digital economy in general. Privacy concerns are among the top reasons for people not buying goods and services online. With the technology sector directly

[1] See Factsheet of the European Commission, "How Will the Data Protection Reform Affect Social Networks?", para. 1(2016).
[2] See "The EDRi papers an Introduction to Data Protection (ISSUE 06)", para. 14.
[3] See Factsheet of the European Commission, "How Will the Data Protection Reform Affect Social Networks?", para. 1 (2016).

contributing to 20% of overall productivity growth in Europe and 40% of overall investment aimed at the sector, individual trust in online services is vital for stimulating economic growth in the EU[4]. Let us remember the famous and most discussed data privacy issues on the Facebook back in 2018 concerning information leaking: "Mark Zuckerberg faces allegations that he developed a "malicious and fraudulent scheme" to exploit vast amounts of private data to earn Facebook billions and force rivals out of business[5]". Actually, this is the best example to see how even the most famous social network sites providers can sometimes have difficulties with data privacy issues.

Nowadays it is difficult to imagine a person who is not registered in any social network. Sharing information with online friends is common for SNS users but, actually, is the huge risk of losing individual data privacy. Users are more often unaware of the privacy regulations when joining a social network. Some of them even do not understand that their personal information can be publicly used or be available for everyone. This mostly appears as a result of quick registration only by one "click" without completely reading the privacy regulations or much more often used in SNS as "privacy policies" before joining the social network. The users should know their privacy rights and should understand what their status in the digital world is. Despite the negative fact of releasing personal data from the social network, however, sometimes it can be helpful, even a mandatory activity conducted by a state body. The FBI has dedicated undercover agents on Facebook, Twitter, MySpace, LinkedIn. One example of investigators using Facebook to nab a criminal is the case of Maxi Sopo. Charged with bank fraud, and having escaped to Mexico, he was nowhere to be found until he started posting on Facebook. Although his profile was private, his list of friends was not, and through this vector, where he met a former official of the Justice Department, he was eventually caught[6]. The subject matter of this thesis is the introduction and examination of data protection regulations and means of protection in social networks under EU and Armenian law. The significance of the subject matter is justified by the fact that the 21st century is being developed as a "digital age" where technology and particularly

[4] Ibid.
[5] See "Zuckerberg set up fraudulent scheme to 'weaponize' data, court case alleges" (2018), available at https://www.theguardian.com/technology/2018/may/24/mark-zuckerberg-set-up-fraudulent-scheme-weaponise-data-facebook-court-case-alleges (last visited on April 03, 2020).
[6] See "Privacy Concerns with Social Networking Services" (2015), available at https://en.wikipedia.org/wiki/Privacy_concerns_with_social_networking_services (last visited on March 9, 2020).

social networking systems play a huge role when collecting and processing enormous personal data. Hence, much more attention should be paid to the laws and regulations which protect the personal data especially online. The present paper aims to examine the acting laws both in Armenia and the EU, monitor court cases in the above-mentioned countries, and find means of protection in the event of data policy infringements. The judicial practice on data privacy issues in Armenia is quite small. The same can be spoken about the legislation which sometimes may not completely cover a practical data privacy case. In comparison, international practice has several major judicial cases concerning social media. On July 18, 2018, Sir Cliff Richard OBE was awarded £210,000 (about US$270,360) in general damages after the British Broadcasting Corporation (BBC) was held liable for infringing his privacy rights over the filming and broadcast of a search of his UK property by South Yorkshire Police (SYP) in relation to allegations of historical child sexual abuse[7]. This thesis paper literature is based on different conventions, laws and regulations, such as European Convention on Human Rights, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), General Data Protection Regulation (GDPR), Armenian Law "On Personal Data Protection" and so on. The paper also includes several citations of prominent scholars, from various books, articles, and newspapers. The following methods of analysis have been used for conducting the present paper: the comparative method, content analysis, case monitoring, etc. The paper consists of an introduction, three chapters, Conclusion, and the Bibliography. **The introduction** represents the background and justification of the problem. It briefly describes the subject matter of the paper, the justification of the subject matter, the literature and methods used while developing the present paper. **Chapter 1** gives an overview of the SNS, Data Controllers, and Data Subjects as the main actors of the SNS. **Chapter 2** represents the main rights and responsibilities of SNS providers as data controllers and its data subjects. **Chapter 3** introduces the remedies for the breach of data protection regulations under the EU and Armenia. The **Conclusion** sums up

[7] See "United Kingdom: Cliff Richard Wins Privacy Case Against BBC and South Yorkshire Police" (2018), available at https://www.loc.gov/law/foreign-news/article/united-kingdom-cliff-richard-wins-privacy-case-against-bbc-and-south-yorkshire-police/ (last visited on 11.03.2020).

discussed issues in all three chapters. It tries to give solutions and recommendations that can be helpful both in Armenia and other countries in the field of data privacy in social networks.

CHAPTER 1: DEFINITION OF SNS, DATA CONTROLLERS AND DATA SUBJECTS

1.1.What are Social Networking Sites?

Some users worry about the data privacy of social networking sites, as seen in the March 2018 revelations about how Cambridge Analytica, a political information firm, illegally gathered information from about 50 million pages of the U.S. users to target for highly politicized content[8]. In addition to potential leaks of personal information, including tax and personal identification information, SNS users who are not careful about their privacy settings find that strangers can track their movements or see questionable photos[9]. Moreover, criminals sometimes use social networking sites to find potential victims.

Overall, what is SNS? There are several definitions of SNS in the legal and software literature. The SNS is an abbreviation for Social Networking Services or Social Networking Sites. The first SNS, SixDegrees.com was started in 1997 and was soon followed by Friendster, MySpace, and Facebook. Today there are a wide range of SNS and approximately 80% of Americans have SNS profiles. SNS range from sites where users have general interests to those where users have very specific interests. Successful specialized SNS include Facebook, Instagram, Twitter, LinkedIn, Reddit, Snapchat, Tumblr, Pinterest, and TikTok. SNS profiles are very popular across the globe. Facebook alone boasts over 2.4 billion users worldwide[10].

To learn what is a social network or a social networking site, it is essential to discuss some definitions of it. According to the Cambridge, dictionary[11]: *"social network is a website or computer program that allows people to communicate and share information on the internet using a computer or mobile phone"*. One may notice that this a quite simple and literary definition that does not include any specific circle of people using SNS or the information which is mainly processed in it. This definition describes the social network in the form of a website or computer program. Whereas, in comparison with the following definition we may

[8] See "Social Networking Service—SNS" (2020), available at https://www.investopedia.com/terms/s/social-networking-service-sns.asp (last visited on 15.04.2020).
[9] Ibid.
[10] Ibid.
[11] See Online Cambridge Dictionary, available at https://dictionary.cambridge.org/dictionary/english/social-network (last visited on 24.03.2020).

notice some certain peculiarities which were not mentioned in the other one: *"A social networking service is an online platform which people use to build social networks or social relationships with other people who share similar personal or career interests, activities, backgrounds or real-life connections. Social networking sites allow users to share ideas, digital photos and videos, posts, and to inform others about online or real-world activities and events with people in their network."*[12] In this definition, the author concretely describes what an SNS is by providing clear information on the activities and content existing in the Social Networking Sites. But again, this definition lacks much information on any specific circle of people in SNS, in other words, it does not speak about the main "actors" in SNS. We may find almost a similar approach in the following definition*: "A social networking service (SNS) is an online vehicle for creating relationships with other people who share an interest, background, or real relationship."*[13] Social networking service users create a profile with personal information, photos, etc. and form connections with other profiles. These users then use their connection to grow relationships through sharing, emailing, instant messaging, and commenting. Social networking services may also be referred to as a "social networking site" or simply "social media"[14].

Anyway, the above-mentioned definitions do not include any legal references. Whereas, in practice, even a very professional lawyer can have difficulties to give a certain definition of SNS not to confuse it with any online application or search engine. Moreover, the most debatable issue is deciding whether a person is a data user or data controller in SNS, or whether an SNS is a data controller or not. To understand these issues, which may lead to lots of problems in practice, we need to refer to the definitions of SNS given in the most famous legal acts and discuss them in practice. The definitions of a Data User and Data Controller will be discussed in the 1.2. sub-point of this chapter.

According to WP29 in Opinion 5/2009 on Online Social Networking (adopted on 12 June 2009 and developed by the Article 29 Data Protection Working Party which is an independent

[12] See"Social Networking Service—SNS" (2020), available at https://en.wikipedia.org/wiki/Social_networking_service (last visited on 05.05.2020).
[13] See "Social Networking Service—SNS" (2020), available at https://www.investopedia.com/terms/s/social-networking-service-sns.asp (last visited on 15.04.2020).
[14] Ibid.

European advisory body on data protection and privacy), SNS can broadly be defined *as online communication platforms that enable individuals to join or create networks of like-minded user.*.[15] In the legal sense, social networks are information society services, as defined in Article 1 paragraph 2 of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 which lays down a procedure for the provision of information in the field of technical standards and regulations. The latter was amended by the Directive 98/48/EC of the European Parliament and of the Council of 20 July, 1998[16].

SNS share certain characteristics:

- User-generated content, such as photos, videos, marital status, political views, interests, religion;
- The ability to connect with others from all over the world;
- Registration is free. The income for an SNS is mostly raised through advertising;
- Connection of people with common interests, educational institutions, mutual friends, etc.;
- They may help to develop a professional network;
- They may be generally helpful for ordinary users to find necessary information, we aware of news all over the world, to do online shopping, etc.

Advertising which is demonstrated on social web sites and accessed by SNS users is the main revenue for the SNS. Users who share their interests on their profiles are offered relevant services or products by target advisers. Thus, it is essential that SNS process data in a way that respects the rights and freedoms of users who have a legitimate expectation that the personal data they disclose will be processed according to European and national data protection and privacy legislation[17]. Marketers use social networking for increasing brand recognition and encouraging brand loyalty. Since it makes a company more accessible to new customers and more recognizable for existing customers, social networking helps promote a brand's voice and content[18]. To sum up, we can conclude that:

[15] See Article 29 Data Protection Working Party, "Opinion 5/2009 on online social networking", para. 4 (2009).
[16] See "Publications Office of the EU", available at https://op.europa.eu/en/publication-detail/-/publication/695afd1d-539b-4475-a892-d1f5bbc9f489/language-en (last visited on 18.04.2020).
[17] Ibid.
[18] See "Social Networking" (2020), available at https://www.investopedia.com/terms/s/social-networking.asp (last visited on 14.03.2020)

- A social networking service (SNS) is an online platform to create relationships with other people;
- SNS generates enormous personal data on individuals, thus raising the risk of personal data leaking;
- Social networking services revenue is mostly based on online advertising;
- SNS can be used for both private and commercial aims and activities;
- Sometimes it can be difficult to determine the main real actors (data controller/data processor/or data user) of SNS.

1.2. Who are Data Controllers and Data Subjects?

There are at least two main actors who process personal data in social networking sites: a data controller and a data subject.

As mentioned in the previous sub-point of this chapter, sometimes it is quite difficult to determine who is the "real" data controller acting in SNS, and who is the data subject. One may wonder why it is so vital to discuss such a question? The answer is that there are lots of certain responsibilities that may arise in a certain situation considering the role of a person in the SNS. If there is a confusion between these two actors, the innocent victims in SNS can be harmed, illegal responsibilities (sanctions included) may be put on the individual or a legal person as well.

We are going to discuss the definition of a data controller, data subject, their characteristics, and also the more problematic questions raising in the legal practice in the scopes of social networking sites.

Under EU law, a controller is defined as someone *who "alone or jointly with others determines the purposes and means of the processing of personal data*[19]*"*. A controller's decision establishes the purposes and ways the data shall be processed. Under CoE law, Modernised Convention 108 defines a *"controller" as "the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has the decision-making power concerning data processing*[20]*"*. Such decision-making power concerns the purposes and means of the processing, as well as the data categories to be processed and access to the data.[21] Whether this power derives from a legal designation or factual circumstances must be decided on a case-by-case basis[22].

In the sense of the framework of Directive 95/46/EC*, a data subject is an individual to whom the information relates, provided that he or she is identified or sufficiently identifiable (art. 2, a).* Users are considered data subjects vis-à-vis the processing of their data by SNS[23].

According to GDPR, *the data subject is an identifiable natural person 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,*

[19] See General Data Protection Regulation of the European Union (2018), Art. 4 (7)
[20] See Modernised Convention 108 of the Council of Europe, Article 2 (d)
[21] See Explanatory Report of Modernised Convention 108 of the Council of Europe, para. 22.
[22] Ibid.
[23] See Article 29 Data Protection Working Party, "Opinion 5/2009 on online social networking", p.12 (2009).

physiological, genetic, mental, economic, cultural or social identity of that natural person[24]. As a result of adopting the new version of Directive 95/46/EC, that is GDPR, one may notice that the definition of a data subject is broadened by stipulating certain criteria for the identification of a natural person.

The controller is the entity who alone, or jointly with others, determines the purposes and means of the data processing. It is also possible that the controller chooses not to perform all the desired processing operations entirely by himself, but to have a whole or a part of the processing operations carried out by a different entity. A "processor" is then an entity that carries out such operations on behalf of the data controller[25].

Controllers are the ones who make decisions on data processing activities. They exercise the entire control of the personal data being processed and are, therefore, liable and responsible for the processing. Some controllers may be under a statutory obligation to process personal data. Section 6(2) of the Data Protection Act 2018 of the UK says that anyone who is under such an obligation and only processes data to comply with it will be a controller[26]. A controller can be a company or other legal entity or an individual. However, an individual processing personal data for a purely personal or household activity is not subject to the GDPR[27]. While the Article 29 Working Party has emphasized that to provide individuals with the more stable entity for the exercise of their rights, "preference should be given to consider as a controller the company or the body as such, rather than a specific person within the company or the body[28].

Thus, to be qualified as a controller, an entity must exercise at least some level of decision-making power with regards to both the purposes and means of a particular processing operation. The purposes for which a user processes personal data within an SNS typically vary according to the type of SNS and the audience it seeks to address.

Now let us discuss how an individual person can become a data controller.

[24] See General Data Protection Regulation (2018), Article 4(1).
[25] See Directive 95/46/EC of the European Parliament, Art. 2, e.
[26] ICO, "Guide to the General Data Protection Regulation" (2018).
[27] Ibid.
[28] See Article 29 Working Party (2010), Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, Brussels, 16 February 2010.

Data Subjects as Data Controllers

In the majority of cases, users process data for purposes of social interaction or self-expression. Other purposes may include career development, self-education. Every user can freely determine the purposes of his processing within a given SNS[29].

Generally, users are considered to be data subjects. If a user takes an informed decision to extend access beyond self-selected "friends" data controller responsibilities come into force.[30] Natural persons can be controllers under both EU and CoE law.

Contemporary developments in case law have confirmed that privacy may also be jeopardized by "ordinary: SNS users (natural persons). A case decided by the High Court of England involved defamatory statements that were made by using a Facebook profile[31]. The defendant had created a profile using the name of the plaintiff (MF) and created the group "Has MF lied to you?" which was linked to the profile by hyperlink. The false profile contained defamatory content relating to the plaintiff and his company; and also revealed information as to the defendant's sexual orientation, his relationship status, his birthday, and his political and religious views[32]. The High Court held that these activities led to a cause of action both for defamation and abuse of private information. However, no claims have been brought under the UK Data Protection Act. When processing data about others regarding a purely personal or household activity, private individuals do not fall under the rules of the GDPR and Modernized Convention 108 and are not deemed to be controllers[33]. Article 2(2) of the GDPR states, *"This Regulation does not apply to the processing of personal data (...) (c) by a natural persona in the course of a purely personal or household activity"*. Recital 18 continues, *"This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for*

[29] See "Social networks and web 2.0: are users also bound by data protection regulations?" (2009), available at https://link.springer.com/article/10.1007/s12394-009-0017-3 (last visited on 09.05.2020).
[30] See WP29 in Opinion 5/2009 on Online Social Networking, p.6 (2009).;
[31] See Applause Store Productions Ltd v. Raphael, Case No: EWHC 1781 (QB) (2008).
[32] See Applause Store Productions Ltd v. Raphael, Case No: EWHC 1781 (QB) (2008).
[33] See European Union Agency for Fundamental Rights and Council of Europe, "Handbook on European Data Protection Law", para. 102 (2018).

processing personal data for such personal or household activities[34]*"*. As we have seen, the EU law precisely states the feature of activity by which it can be described as an exemption from general liability, so the activity has to be "purely personal" or "household". It can be concluded that when a data user uses her social network sites for commercial purposes, such as online shopping, or professional development rather than for private life/family activities, she cannot be exempted from liability. In the legal sense, all the responsibilities that are mentioned in the EU law for a data controller slightly pass to the data usage which is already a data controller.

When personal data is processed by an individual for her personal, private/family, or household activities, the Data Protection Act of the UK considers it as an exemption. This exemption, which is enshrined in section 36 of the Act, is generally known as the "domestic purposes" exemption. The latter will be exercised in the event of usage online forum purely for domestic purposes by a natural person. The domestic purposes exemption does not refer to the organizational online forums' usage. Therefore, the companies that use social networking vehicles are subject to the Data Protection Act in a general way. Also, the exemption does not apply when ordinary persons process their data for non-domestic purposes. Individuals who use social media for purposes such as running a sole trader business are subject to the DPA in the usual way[35]. The same regulations are stipulated in the GDPR which will be discussed later. When a legal person, or amateur user acting for non-domestic purposes, posts personal data on an SNS, they will need to comply with the regulations of the Data Protection Act. The same scenario will be when the latter download personal information from an SNS and use it for non-domestic purposes. The section 36 exemption is based on the purposes for which the personal data is being processed, not on the nature or content of the data itself. It applies whenever someone uses an online forum purely in a personal capacity for their own domestic or recreational purposes. It does not apply when an organization or an individual uses an online forum for corporate, business, or non-domestic purposes[36].

The ICO, as well, does not consider complaints made against individuals who have posted personal data whilst acting in a personal capacity, no matter how unfair, derogatory, or distressing the posts may be. This is because where an individual is posting for their personal, family household

[34] See General Data Protection Regulation, Recital 18, and Explanatory Report of Modernised Convention 108.
[35] See Information Commissioner's Office, "Social networking and online forums – when does the DPA apply?" Version: 1.1 20140226, para. 2.
[36] Ibid.

or recreational purposes the section 36 exemption will apply. The ICO considers complaints about posts made by businesses, organizations, or individuals acting for nondomestic purposes in the normal way, using a proportionate approach[37].

Under Irish law where an individual uses Facebook for purely social and personal purposes to interact with friends etc. they are considered to be doing so in a private capacity with no consequent individual data controller responsibility. This so-called domestic exemption means for instance that there are no fair processing obligations that arise for an individual user when posting information about other individuals on their Facebook page[38]. Article 29 Working Party Opinion 5/2009 on online social networking also recognized this distinction (para. 24)".

We have already discussed some approaches related to "household exemption", but, overall, what activities are considered to be "personal" or "household". According to Convention 108, *personal or household activities are activities that are closely and objectively linked to the private life of an individual and which do not significantly impinge upon the personal sphere of others*[39]. These activities do not include professional or commercial features and refer exclusively to family/private life or household affairs such as sharing personal pictures or videos, or a friend list. The sharing of such kind of data mainly means sharing information in the scopes of family or friends, in other words, when the audience of the information is certain and limited and is based on trust. Whether activities are 'purely personal or household activities will depend on the circumstances[40]. Activities that have professional or commercial aspects cannot fall under the household exemption[41]. Thus, when the data is processed for professional or commercial full-time activity, a natural person/ SNS user could be considered as a data controller. In addition to the professional or commercial character of the processing activity, another factor that must be taken into account is whether personal data are made available to a large number of persons, obviously external to the private sphere of the individual.[42] As it was stated in WP29 in Opinion 5/2009 on

[37] See Information Commissioner's Office, "Social networking and online forums – when does the DPA apply?" Version: 1.1 20140226, para. 15.
[38] See "Data Protection Under GDPR", available at https://dataprotection.ie/viewdoc.asp?m=&fn=/documents/Facebook%20Report/final%20report/report.pdf (last visited on 24.04.2020).
[39] See Explanatory Report of Modernized Convention 108 of the Council of Europe, para. 28.
[40] Ibid, para. 27.
[41] See General Data Protection Regulation, Recital 18, and Explanatory Report of Modernised Convention 108, para. 27.
[42] See European Union Agency for Fundamental Rights and Council of Europe, "Handbook on European Data Protection Law", p. 103 (2018).

Online Social Networking, *"a high number of contacts could be an indication that the household exemption does not apply and therefore that the user would be considered a data controller"*. For example, when personal information is accessible to a large number of persons or persons outside of the family/private sphere, such as a public website on an online platform, the exemption will not apply. Similarly, the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his or her family home to protect the property, health and life of the homeowners, but which covers, even partially, public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, cannot be regarded as an activity which is a purely 'personal or household' activity.[43] The CJEU has not yet ruled on similar facts under the GDPR, which provides more guidance on the topics that could be considered outside the scope of the data protection legislation under the 'household exception', such as the use of social media for personal purposes[44].

Another famous and much-discussed case relating to the interpretation of the "household exemption" is the Lindqvist case[45]. The case concerned the reference to various individuals by name or by other ways, such as their telephone number or data on their hobbies, on social networking sites. The CJEU maintained that *"the act of referring, on an internet page, to various persons and identifying them by name or by other means [...] constitutes "the processing of personal data wholly or partly by automatic means"* within the meaning of Article 3 (1) of the Data Protection Directive.[46] Such personal data processing does not fall under purely personal or domestic activities, which are outside the scope of EU data protection rules, as this exception *"must [...] be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people[47]"*.

The Belgian Privacy Commission, in a recommendation regarding the sharing of pictures by individuals[48], also touched upon the question of personal use. It considered that where images are

[43] See František Ryneš v. Úřad, Case No: C-212/13 (2014).
[44] See European Union Agency for Fundamental Rights and Council of Europe, "Handbook on European Data Protection Law", p. 103 (2018)
[45] See USA v. Bodil Lindqvist, Case No: C-101/01 (2003).
[46] See Former Directive 95/46/EC, Article 3 (1), now General Data Protection Regulation, Article 2 (1).
[47] See the USA v. Bodil Lindqvist, Case No: C-101/01, para. 47 (2003).
[48], See the Belgian Privacy Commission, Recommendation 02/2007 (2007).

processed for the sole purpose of distribution among a select ("definable") group of friends, family members, or acquaintances, such processing could fall under the exception of personal use[49]. As examples it mentioned the transmission of pictures via email to the participants of a family event, or the posting of such pictures on a secured website, which is only accessible to the relevant family members; and which is protected against indexing by search engines.[50] The Dutch Data Protection Authority adopted an almost identical approach shortly thereafter in its Guidance Report relating to the publication of personal data on the internet[51].

In František Ryneš[52], Mr. Ryneš captured the picture of two persons who broke windows in his home through the domestic CCTV surveillance system he had installed to protect his property. The recording was then provided to the police and relied on within criminal proceedings. The CJEU stated that *"[t]o the extent that video surveillance [...] covers, even partially, public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely "personal or household [...]"."*Here, the CJEU narrowed the interpretation of "household exemption" stating, "(…)*the exception provided for ... must be narrowly construed*" (at 29), it then continued, "*the processing of personal data comes within the exception ... only where it is carried out in the purely personal or the household setting of the person processing the data"* (at 31). In its response to this case, ICO agreed with the interpretation of the court, stating, *"Clearly this is a significant judgment. We've previously considered the domestic exemption to be quite broad, but the judgment suggests a narrower interpretation, which could affect surveillance cameras[53]".*

In the following case, also the court could prove the absence of the "household exemption". So, in the "Law Society and Others v Rick Kordowski[54]", Mr. Kordowski founded and ran a website on which members of the public were invited, to 'name and shame' 'Solicitors from Hell'. He moderated posts and charged for a fee for adding or removing them. Mr. Justice Tugendhat had no hesitation in accepting that Mr. Kordowski was a data controller under the DPA, and this was not disputed by any party. It was clear in the circumstances that Mr.

[49] See "Social networks and web 2.0: are users also bound by data protection regulations?", available at https://link.springer.com/article/10.1007/s12394-009-0017-3 (last visited on 26.03.2020)
[50] See Belgian Privacy Commission, Recommendation 02/2007, p.21–22 (2007).
[51] See College Bescherming Persoonsgegevens, p. 12–13 (2007).
[52] See František Ryneš v. Úřad, Case No: C-212/13 para. 33 (2014).
[53] See ICO e-newsletter January 2015, available at http://ico.msgfocus.com/q/1AFB31cD3v/wv#story5 (last visited on 11.05.2020).
[54] See Law Society and Others v. Rick Kordowski (Solicitors from Hell), Case No: EWHC 3185 (QB) (2011).

Kordowski decided the purposes and manner in which the personal data was processed[55]. In Buivids[56], the court stressed again that exceptions must be "interpreted strictly" (at [41]) [S]ince Mr. Buivids published the video in question on a video website [YouTube] on which users can send, watch and share videos, without restricting access to that video, thereby permitting access to personal data to an indefinite number of people, the processing of personal data at issue (…) does not come within the context of purely personal or household activities (at [43]).

Moreover, ICO suggested that even if section 36 of the Data Protection Act does not apply another exemption might. This would refer to cases when a data controller processes personal data on an SNS for special purposes of journalism, art and literature; in the reasonable belief that publication would be in the public interest; and in the reasonable belief that compliance with the provision of the DPA in question would be incompatible with the special purposes[57]. Also, it worth to mention that even if the household exemption applies, a user might be liable according to general provisions of national civil or criminal laws (e.g. defamation, liability in tort for violation of personality, penal liability)[58].

Data Providers as Data Controllers

SNS providers are data controllers under the Data Protection Directive. They provide the means for the processing of user data and provide all the "basic" services related to user management (e.g. registration and deletion of accounts). SNS providers also determine the use that may be made of user data for advertising and marketing purposes - including advertising provided by third parties[59]. The same statement can be concluded as a result of interpretation of the Article 4(7) of GDPR, *" (...) natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;(...)"*. We have already discussed above all the characteristics which are necessary for the natural or legal person to be qualified as a data controller. Researching several social networking sites and its policies (such as Facebook, LinkedIn, Instagram, etc.), we found out they correspond to the

[55] See Information Commissioner's Office, "Social networking and online forums – when does the DPA apply?" Version: 1.1 20140226, para. 15.
[56] See Buivids v. Latvia, Case No: C-345/17 (2017).
[57] See Information Commissioner's Office, "Social networking and online forums – when does the DPA apply?" Version: 1.1 20140226, para. 15.
[58] See WP29 in Opinion 5/2009 on Online Social Networking, p.7 (2009).
[59] WP29 in Opinion 5/2009 on Online Social Networking, p.5 (2009).

definition of a data controller under EU law. For example, most of these sites use policies/cookies which include the purposes and means of the processing of the personal data. These sites mainly use the data for advertising purposes by transferring it to third parties. So, accordingly, they do determine the means and use of the personal data of the user, thus they are controllers. Moreover, if the site only allows posts subject to terms and conditions which cover acceptable content, and if it can remove posts which breach its policies on such matters, then it will still, to some extent, be determining the purposes and manner in personal data is processed. It will, therefore, be a data controller.[60]

Similar conclusions are made in case law. Besides the question of who the data controller in a certain case is, courts also discussed the amount of liability of an SNS as a data controller, its specific responsibilities (such as monitoring of the data), and so on. According to ECD (e-Commerce Directive), *"Member States are prevented from imposing a monitoring obligation on service providers only concerning obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities following national legislation.*"[61] According to the same Directive, Article 15, *"Member States shall not 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."* Here the directive explicitly defines no general obligation for data providers (in our case the SNS).

In AY v Facebook Ireland (2016)[62], there was a case with the repeated posting of naked photos of the plaintiff when aged 14 including on "shame page". The court held that Facebook was liable to filter via PhotoDNA. It reasoned that Facebook could block the "shame page" under general monitoring. *In CG v Facebook Ireland (2016)[63],* different postings referring to a convicted sex offender (CG) including data on his home address. The court held that Facebook was liable but only for failure to promptly take down material specifically flagged up to it. One of the reasoning of the court was that Facebook was a controller of this data.

ICO's approach is the same as GDPR regarding considering data providers as data controllers. According to ICO, the forum might be given free of charge, or the individual or company using the site might take much less of a role in moderating data. For instance, members of

[60] Ibid.
[61] See E-Commerce Directive 2000/31/EC, para 47
[62] See AY v Facebook (Ireland) Limited and Others, Case No: NIQB 76 (2016).
[63] See CG v Facebook Ireland Ltd., Case No: NICA 54 (2016).

a huge SNS can do posts directly to their pages without first having them revised by a site provider/moderator. However, even if the content is not moderated before the final posting this does not mean that the individual or company running the social networking site is not a data controller. If the SNS only allows posts subject to terms and conditions which cover acceptable content, and if it can remove posts which breach its policies on such matters, then it will still, to some extent, be determining the purposes and manner in which personal data is processed. It will, therefore, be a data controller[64].

To sum up, data subjects and data providers can be considered as data controllers. However, to make such a conclusion, there are necessary criteria to be relevant in a certain scenario. The natural persons (data subjects) can act in the role of a data controller but be exempted from general liability for a data protection breach under "household exemption". Also, the SNS is generally considered as data controllers under EU law. Whereas the question of its liability is not the same. It has to be determined under the “case-by-case” criterion.

[64] See Report of the International Commissioner’s Office “On Social Networking and Online Forums – When Does the DPA Apply”, available at https://ico.org.uk/media/for-organisations/documents/1600/social-networking-and-online-forums-dpa-guidance.pdf (last visited on 29.04.2020).

CHAPTER 2. THE RIGHTS AND RESPONSIBILITIES OF SNS AS DATA CONTROLLERS AND THEIR DATA SUBJECTS

After replacing the Data Protection Directive (1995), GDPR which came into force in 2018, has restricted the regulations concerning data protection by defining more responsibilities on data controllers and providing more data protection for data subjects. As the responsibilities and rights of both main actors mentioned above are quite wide, in this Chapter we are going to discuss the vital and most debatable ones.

In the first chapter, we have already discussed that SNS are mainly considered to be data controllers. At the same time, we concluded that in some cases SNS can be partially or wholly not liable for data protection thus escaping from some certain responsibilities. The same was concluded for the data subjects. Generally, we found out that from the moment a data subject turns into a data controller, it is subject to the responsibilities for a data controller under EU law. However, we realized that the latter can also be exempted from the liability under "household exemption". Thus, when speaking about certain responsibilities both for the data controller and a data subject, we have to use a “case-by-case” investigation method.

It is worth to mention that GDPR mentioned a list of rights for data subjects[65], and a bunch of responsibilities for data controllers[66]. We are going to discuss some of these rights and responsibilities follow.

In case a controller or processor is established outside of the EU, it is mandatory for the latter to appoint a representative for data protection issues in the EU. The GDPR underlines that the representative must be established “in one of the Member States where the data subjects, whose personal data are processed concerning the offering of goods and services to them, or whose behavior is monitored[67]”. If no representative is designated, legal action can still be initiated against the controller or the processor[68]. The latter means, that even the Republic of Armenia is not a member of the EU it still may be liable under GDPR when processing data of a Member State data subject.

---

[65] See General Data Protection Regulation of the European Union (2018), Chapter 3
[66] See General Data Protection Regulation of the European Union (2018), Chapter 2 and 4
[67] See European Union Agency for Fundamental Rights and Council of Europe, "Handbook on European Data Protection Law" (2018).
[68] See General Data Protection Regulation of the European Union (2018), Article 27 (5).

According to WP 29 Position in Opinion 5/2009, *SNS as data controllers "should establish visible complaints handling office for DP & privacy issues/complaints about members & non-members" (p. 11)*. Regarding the uploading of data, it suggests SNS provide proper warnings about privacy risks and fact may impinge on privacy and data protection rights. *"SNS users should be advised by SNS that if they wish to upload pictures or information about other individuals, this should be done with the individual's consent* (p. 7)". The latter then was enshrined in GDPR, Article 7 as the basic principle for "consent*": "Where the processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to the processing of his or her data. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner that is distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration that constitutes an infringement of this Regulation shall not be binding"*. GDPR also prescribes the data subject's right to withdraw his or her consent at any time. It can be concluded that when designating some rights for the data subjects, the corresponding obligations arise accordingly. For example, we have seen that a data controller must get the consent of a data subject in case of processing her/his data. Thus, it means that a data subject, consequently, will have a right (possibility) to demonstrate her/his consent in certain situations in SNS. The way of giving consent is also essential under GDPR. The following criteria should be maintained: 1) the request for the consent should be clear for an ordinary SNS user, 2) it should be presented in an easily accessible form, 3) it should be in reader-friendly (clear) language. One of the ways to get such consent that will be properly received is using "privacy policies" in SNS. "Privacy policies" are informative policies on SNS user's including its processing methods, purposes and transformation to third parties, and the rights of the data user in the SNS. Privacy policies should be composed in a way that an ordinary user easily understands her/his rights regarding data processing in the SNS. Here, consent is generally received by the user's "click" which enables the SNS provider to get the user's consent literally in seconds. However, many SNS still fail to keep these responsibilities. Particularly, when presenting some "privacy policies" or other forms (such as cookies) to get user's consent, SNS generally demonstrate it in very small letters and in places that are not accessible for the user. Consequently, there is still much work to do for the SNS to correspond to GDPR. At the

same time, there are cases when SNS are exempted from liability if there is a data protection breach in the reasoning that it has no responsibility for monitoring. The Belgian Data Protection Act, for example, states that the controller of the processing shall be exempted from liability *"if he can prove that the injurious fact cannot be attributed to him"*. The SNS provider can thus be exempted from liability under the Belgian Data Protection Act if he shows that she/he has continuously undertaken all reasonable measures to prevent the data protection breach from taking place and to limit their effects once they have been manifested.[69] Besides, as already discussed in the previous chapter, the e-Commerce Directive, for example, also prescribes no general liability for the SNS to monitor the personal data. According to WP 29 Position in Opinion 5/2009, controllers must take the appropriate technical and organizational measures, 'both at the time of the design of the processing system and at the time of the processing itself' to maintain security and prevent unauthorized processing, taking into account the risks represented by the processing and the nature of the data. As we have noticed, the Working Party mentioned data protection measures at the time of the design of the processing system as well. This approach is famous under the "data protection by design" concept which was developed by Anne Cavoukian, Ontario's Data Protection Commissioner in the '90s and presented at the 31st International Conference of Data Protection and Privacy Commissioners in 2009 with the title "Privacy by Design".[70] Privacy by design involves a focus geared towards risk management and accountability to establish strategies that incorporate privacy protection throughout the life cycle of an object (whether it is a system, a hardware or software product, a service, or a process). It involves taking into account not only the application of measures for privacy protection in the early stages of the project but also to consider all the business processes and practices that process associated data, thus achieving true governance of personal data management by organizations[71]. According to GDPR, Article 24: *"Taking into account the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that*

[69] See "Social Networks and Web 2.0: Are Users Also Bound by Data Protection Regulations" (2009), available at https://link.springer.com/article/10.1007/s12394-009-0017-3 (last visited on 09.05.2020).
[70] See "A Guide to privacy by Design" (2019), available at https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf (last visited on 11.05.2020).
[71] Ibid.

processing is performed by this Regulation. Those measures shall be reviewed and updated where necessary". SNS providers should inform data users of their identity and the various purposes for which they generate and process personal data according to the provisions laid out in Article 10 of the Data Protection Directive including, but not limited to: usage of the data for online marketing purposes; possible transfer of the data with specified categories of third parties, etc. The Working Party recommends that: SNS providers provide adequate warnings to users about the privacy risks to themselves and others when they upload information on the SNS, SNS users should also be reminded that uploading information about other individuals may impinge upon their privacy and data protection rights, SNS users should be advised by SNS that if they wish to upload pictures or information about other individuals, this should be done with the individual's consent[72]. There are also other responsibilities for social networking sites as data controllers, but because the scope of the present paper is not limited to only the rights and responsibilities of SNS and data subjects, we will not discuss them here.

The data subjects are provided with a bunch of rights under EU law. The GDPR, Chapter 3 mentioned the following rights for the data subjects: a right to be informed, right to rectification, right to erasure, right to restriction of processing, right to data portability, right to object, etc. One of the rights that interrelates most notably with the right to data protection is the right to freedom of expression. The relationship between the protection of personal data and freedom of expression is governed by Article 85 of the General Data Protection Regulation, entitled "Processing and freedom of expression and information". According to this article, Member States shall conform the right to personal data protection with the right to freedom of expression and information. Particularly, exemptions and derogations from the certain chapters of the GDPR shall be made for journalistic purposes or the purpose of academic, artistic, or literary expression, since they are essential to conform the right to data protection with the freedom of expression and information.

One of the most famous cases related both to the right of expression and the right to be forgotten is Google Spain. In Google Spain[73], the CJEU found out whether Google had an obligation to erase outdated data about the applicant's financial

[72] See Article 29 Data Protection Working Party, "Opinion 5/2009 on online social networking" (2009).
[73] See Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, App. No: C-131/12, paras. 81–83 (2014).

difficulties from its search engine list results. When examining if Google was obliged to delete the links related to the applicant, the CJEU held that the rights of erasure are not absolute. It needs to be balanced with other fundamental rights, particularly the interest and right of the public to have access to the data. The CJEU considered the factors to examine during the balancing research. The nature of the data in question is a vital factor, particularly. If the data is sensitive to the private life of the person, and where there is no public interest in the access of such data, information protection, and privacy would overrule the right of the general public to have access to the information. On the contrary, when the data subject is a public personality, or that the data is of such nature to justify granting the general public access to such information, then the interference with the fundamental rights to data protection and privacy is justified.

As stated in Lindqvist[74] , "Mrs. Lindqvist's freedom of expression in her work preparing people for Communion and her freedom to carry out activities contributing to religious life has to be weighed against the protection of the private life of the individuals about whom Mrs. Lindqvist has placed data her internet site" (at [86]). Besides, as we have already discussed this case also refers to the "household exemption" for the data subjects. While, here as Mrs. Lindqvist posted personal information of others on her internet site which was out of family or private sphere, she was liable as a data controller.

According to the RA Constitution (2015), Article 34(1*): "Everyone shall have the right to protection of data concerning him or her"*. The RA Law "On Protection of Personal Data" enshrines all the main rights and responsibilities for the data controllers and data subject. While the GDPR differentiates between a data controller and data processor, Armenian law gives only one definition under "processor of personal data", stating that it "shall mean a state administration or local self-government body, state or community institution or organization, legal or natural person, which organize and/or carries out the processing of personal data". The reason of this is probably the translation issue in Armenia, but for clarifying these two definitions the law could use the following definitions: data controller as "տվյալների համակարգող", data processor as "տվյալներ մշակող". The purpose of defining these two actors is to clarify and separate their responsibilities because the data controller is not always the data processor as it is stated under EU law. The logic of Armenian should also be based on the "purpose" of the processing of personal data to determine who is the

[74] See USA v. Bodil Lindqvist, Case No: C-101/01 (2003).

real data controller. What is more important, there is no clause in Armenian law referring to "household exemption". The latter means that there can be difficulties firstly to determine the real data controller especially in SNS, and later on to decide the size of liability.

Summing up, there are certain obligations under the EU law arising in the event of data processing for a data controller. However, the amount of liability can differ from case to case, considering the factor whether the data provider was obliged to monitor the data or not on the SNS. As we have seen, data subjects' rights have been broadly prescribed under GDPR having them an opportunity to protect their data completely.

CHAPTER 3: REMEDIES FOR THE BREACH OF DATA PROTECTION REGARDING ONLINE SOCIAL NETWORKING

SNS has become a wide part of life today, it used to be that individuals and organizations could only access the internet and social media from home, whereas now almost everyone can have the internet in their pocket and access it on the go. A vast number of individuals and businesses use social media, and there has been an increased number of criminal cases where people have been prosecuted for their actions on social media sites like Facebook, YouTube and Twitter[75]. Adopting legal regulations is not enough to ensure the protection of personal information within the EU. To make European data protection rules effective, it is necessary to establish enforcement mechanisms for Data subjects' rights that enable data subjects to counter breached their rights and to seek proper compensation for any damage suffered. It is also vital that supervisory authorities have the power to impose sanctions that are effective, justified, and proportionate to the data breach in question.

According to Modernised Convention 108, the national law of the Contracting Parties must establish proper remedies and sanctions against breaches of the right to data protection. In the European Union, the GDPR provides for remedies for data subjects in the event of infringements of their rights, as well as for sanctions against data controllers and processors who do not comply with the provisions of the data protection regulation. It also enshrines the data subject's right for compensation and liability.

Under both CoE and EU law, data subjects have the right to lodge requests and complaints to the respective supervisory authority if they find that the processing of their data is not being carried out in accordance with the law.

Modernized Convention 108 recognizes the right of data subjects to benefit from the assistance of a supervisory authority in exercising their rights under the convention, irrespective of their nationality or residence[76]. A request for assistance may only be rejected in exceptional circumstances, and data subjects should not cover the costs and fees related to the assistance[77].

---

[75] See "Rights and Responsibilities of Individuals Using Social Media" (2016), available at https://vidyareviewsblog.wordpress.com/2016/04/28/rights-and-responsibilities-of-individuals-using-social-media/ (last visited on 12.05.2020).

[76] See "Explanatory Report of Modernised Convention 108" of the Council of Europe, Article 18.

[77] Ibid., Articles 16–17.

Similar provisions can be found in the EU legal system. The GDPR requires supervisory authorities to adopt measures to facilitate the submission of complaints, such as the creation of an electronic complaint submission form[78].

The data subject can lodge the complaint with the supervisory authority in the Member State of his or her habitual residence, place of work, or place of the alleged infringement.[79] Complaints must be investigated, and the supervisory authority must inform the person concerned of the outcome of the proceedings dealing with the claim.[80] Potential data breaches by EU institutions or bodies can be brought to the attention of the European Data Protection Supervisor.[81] When there is an absence of a response from the EDPS within six months, the complaint shall be deemed to have been rejected. The CJEU can examine the appeals against the EDPS' decisions within the framework of Regulation (EC) No. 45/2001 stipulating an obligation to comply with data protection rules to EU institutions and bodies.

In addition to the right to complain to the supervisory authority, data subjects must have the right to an effective judicial remedy and to bring their complaint before a court. The right to a legal remedy is stipulated in the European legal regulations and is considered to be a fundamental right, both under Article 47 of the EU Charter of Fundamental Rights and Article 13 of the ECHR[82]. Data subjects, data controllers, or processors seeking to challenge a supervisory authority's legally binding decision may bring proceedings before a court.[83] The court action must be brought before the courts of the Member State where the relevant supervisory authority is established[84].

Moreover, data subjects, supervisory authorities, data controllers or processors may, in the course of national proceedings, ask the court to request clarification from the CJEU on the interpretation and validity of acts of the institutions and bodies of the. These clarifications are considered to be preliminary rulings. *Digital Rights Ireland and Kärntner Landesregierung and Others* was a joined case submitted by the Irish High

[78] See General Data Protection Regulation of the European Union (2018), Article 57 (2).
[79] Ibid., Article 77 (1).
[80] Ibid., Article 77 (2).
[81] See Regulation No: 45/2001 of the European Parliament and of the Council of 18 December 2000 "On the Protection of Individuals with Regard to the Processing of Personal Data by the Institutions and Bodies of the Community and on the Free Movement of Such Data (2001).
[82] See e.g. Karabeyoğlu v. Turkey, App No: 30083/10, (2016); Mustafa Sezgin Tanrıkulu v. Turkey, App. No: 27473/06 (2017).
[83] See General Data Protection Regulation of the European Union (2018), Article 78.
[84] See General Data Protection Regulation of the European Union (2018), Recital 143, Art. 78 (223).

Court and the Austrian Constitutional Court regarding the conformity of Directive 2006/24/EC (Data Retention Directive) with EU data protection law. The Austrian Constitutional Court proposed requests to the CJEU regarding the validity of Articles 3 to 9 of Directive 2006/24/EC under Articles 7, 9, and 11 of the EU Charter of Fundamental Rights. The request included if the specified provisions of the Austrian Federal Law on Telecommunications transposing the Data Retention Directive were incompatible with the respective provisions of the former Data Protection Directive and the EU Institutions Data Protection Regulation. Under CoE law, Contracting Parties must provide appropriate judicial and non-judicial remedies for infringements of the provisions of Modernized Convention 108[85]. Allegations data protection rights breaches contravening Article 8 of the ECHR against a Contracting Party to the ECHR, may be brought before the ECtHR when all possible national remedies have been exhausted. A plea of violation of Article 8 of the ECHR before the ECtHR must also meet other admissibility criteria (Articles 34–35 of the ECHR)[86].

Although applications to the ECtHR can be directed only against Contracting Parties, they can also indirectly deal with actions or omissions of private parties, since a Contracting Party has not fulfilled its positive obligations under the ECHR and has not ensured appropriate protection against breaches of data protection rights in its national law. *In K.U. v. Finland*[87], the applicant, a minor, complained that a publication of a sexual nature had been posted about him on an internet dating site. The SNS provider did not reveal the identity of the person who had posted the data because of confidentiality liabilities under Finnish law. The applicant claimed that Finnish law did not provide appropriate protection against such activities of an individual posting incriminating information about the applicant on the internet. The ECtHR held that states were not only compelled to abstain from arbitrary interference with individuals' private lives but may also be subject to positive liabilities that involve *"the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves"*. In the applicant's case, his practical and effective protection required that appropriate steps be taken to identify and prosecute the offender. However, the state failed to ensure such protection, and the Court held that there had been a breach of Article 8 of the ECHR.

[85] See "Explanatory Report of Modernised Convention 108" of the Council of Europe, Article 12.
[86] See European Convention on Human Rights, Articles 34–37.
[87] See K.U. v. Finland, App. No: 2872/02 (2008).

The right to an effective remedy must enable data subjects to claim compensation for any damage suffered as a result of processing their personal information in a manner that breaches the applicable law. The liability of data controllers and processors for illegal processing is enshrined explicitly in the GDPR[88]. The regulation provides the data subjects with the right to receive compensation from the data controller or processor for both material and non-material damages which, while its recitals stipulate that "the concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation"[89]. Controllers are liable and could be subject to compensation claims if they do not correspond with the obligations under the regulation. In the CoE legal framework, Article 12 of Modernized Convention 108 requires Contracting Parties to provide sufficient remedies for infringements of domestic law implementing the convention's requirements. Remedies must include the possibility to judicially challenge a decision or practice, while non-judicial remedies must also be made available under the Explanatory Report of Modernized Convention[90]. The modalities and different rules regarding the access of these remedies, together with the procedure to be followed, are left to the discretion of each Contracting Party. Contracting Parties and domestic courts should also take into account financial compensation provisions for material and non-material damages caused by the processing, as well as the possibility of enabling collective actions[91]. Under CoE law, Article 12 of Modernized Convention 108 provides that sufficient sanctions and remedies must be ensured by each Contracting Party for the breaches of national law provisions that give effect to the basic principles of data protection set out in Convention 108. The convention does not set up or impose a particular list of sanctions. On the contrary, it clearly states that each Contracting Party has the power to determine the nature of judicial or non-judicial sanctions, which may be criminal, administrative, or civil. The Explanatory Report of Modernized Convention 108 requires that sanctions must be effective, proportionate, and dissuasive[92]. Contracting Parties must respect this principle when determining the nature and severity of sanctions available in their national legal order. Under

[88] See General Data Protection Regulation of the European Union (2018), Article 82.
[89] Ibid., Recital 146.
[90] See "Explanatory Report of Modernised Convention 108" of the Council of Europe, para. 100.
[91] Ibid.
[92] Ibid.

EU law, Article 83 of the GDPR enables Member States' supervisory authorities to exercise administrative fines for violations of the regulation. The level of fines, and the circumstances that domestic authorities take into consideration when deciding whether to impose a fine, as well as the total maximum ceilings of that fine, are also provided for in Article 83. The sanctioning regime is, therefore, harmonized across the European Union.

The GDPR follows a tiered approach to fines. The supervisory authorities have the discretion to impose administrative fines for violations of the regulation of up to € 20,000,000[93] or, in the case of an undertaking, 4 % of its total worldwide annual turnover – whichever is higher. Breaches that can trigger this level of fine include infringements of the basic principles for processing and the conditions for consent, violations of data subjects' rights, and of the regulation's provisions regulating the transfer of personal information to recipients in third countries. For other breaches, supervisory authorities may impose fines of up to € 10,000,000 or, in the case of an undertaking, two percent of its total worldwide annual turnover – whichever is higher[94]. Although there are certain liabilities and sanctions under GDPR as discussed above, the case law lacks the court decisions where the court found the data controller/processor or data subject was liable for data protection under GDPR. In these cases, liabilities mostly arise for the breach of other rights and legal interests. For example, in *Applause Store Productions Ltd v Raphael*[95], a former friend and business associate (Raphael) created a fake Facebook profile of F linked to a Facebook group entitled "has F lied to you?". Both the profile and the group contained personal information of F including his sexual orientation, political and religious views as well as defamatory material related to F and F's company. The court held that Raphael was liable under defamation (£15K awarded as regards F and £5K for his company) as well as the tort of the misuse of private information. However, no action was pleaded here in data protection. The same scenario is in the Armenian judicial system. The latter lacks a court's pure reasoning for data protection breach under RA Law "On Personal Data Protection". Most cases refer to insult and/or defamation. Also, the sanctions are prescribed for data protection cases, not under RA Law "On Personal Data Protection", but under the RA Code on Administrative Offences". This is because of an absence of any clause in the RA Law

[93] See General Data Protection Regulation of the European Union (2018), Article 83 (5).
[94] See General Data Protection Regulation of the European Union (2018), Article 83 (4).
[95] See Applause Store Productions Ltd v. Raphael, Case No: EWHC 1781 (QB) (2008).

"On Personal Data Protection" about specific remedies, liabilities, or sanctions for data protection breaches as already discussed in the previous chapter. Moreover, there is no single data protection case on SNS in the annual report[96] of the RA Agency on the Protection of Personal Data which is the authorized body for data protection in Armenia.

So, the RA Code on Administrative Offenses, Article 189.17 states a penalty in the amount of 200,000-500,000 AMD for violation of the procedure established by the law on collection or recording or entry or coordination or organization or correction or maintenance or use or transformation or restoration or transfer of personal data, if the given act does not contain features of a crime. If it does, then the person is subject to criminal liability for a crime under the RA Criminal Code. Besides, the protection of personal data shall be carried out by the authorized body, which operates under the structure prescribed by the Decision of the Government of the Republic of Armenia[97]. Authorized body for the protection of personal data check, on its initiative or on the basis of an appropriate application, the compliance of the processing of personal data with the requirements of the Law, apply administrative sanctions prescribed by law in the case of violation of the requirements of the Law, require blocking, suspending or terminating the processing of personal data violating the requirements of the Law, require from the processor rectification, modification, blocking or destruction of personal data where grounds provided for by the Law exist, prohibit completely or partially the processing of personal data as a result of the examination of the notification of the processor on processing personal data, etc. Anyway, though Armenian law stipulates some authorities for the Authorized body to use preventing or prohibiting actions in case of data protection breaches, it still lacks the means of liability or sanctions in the mentioned cases both for data subjects (when they are not exempted from household activities) or data controllers. The omissions of Armenian data protection legislation and preferable changes or amendments have been already discussed in the previous chapter. Summing up, we can notice that the liabilities and fines for personal data infringements are clearly enshrined in EU law. The same cannot be said for the Armenian law. Armenian law "On Personal Data Protection" does not include any specific provisions on the data controller's liabilities and the fines for data breaches.

[96] See Report of Personal Data Protection Agency of the RA Ministry of Justice (2019), available at http://www.justice.am/storage/uploads/2019Annual-report-2019-ATPG.pdf (last visited on 15.05.2020).
[97] See the RA Law "On Personal Data Protection", Article 24.

It regulates the data breaching cases by providing certain authorities to a Personal Data Protection Agency. The fines are stipulated under other laws. So, there is an absence of a comprehensive data protection law that could include both the rights and liabilities for data controllers and subjects and also the liabilities, remedies, and fines for data infringement cases. Nevertheless, both the EU and Armenia lack judicial practice under data protection regulations. The reason for this scenario is the unawareness of data subjects on their rights and legal interests regarding data protection in social networking sites. When this problem is solved by informing people of their rights in SNS, they will be able to claim appropriate protection for their rights in front of a respective judicial body.

CONCLUSION

The social networks are the "online weapons" which sometimes can cause serious consequences in the field of data protection. The short oral survey among my relatives, friends, and colleagues that I used within my analytical work, shows that 80% of them is not aware of the privacy policies to which they have agreed on one when registering to any social network; this the main reason why there is a huge amount of data protection breach cases.

When having a glance at the daily feeds of the most used social network Facebook, you can see that lots of SNS users share their photos, status, so on. Some of them share the information which does not belong to them including the same identification details. As we have discussed above, these cases cannot be exempted from liability sometimes if its content is not a purely personal or household activity, which in turn means that in these cases they will bear the same liabilities as data controllers under the EU law.

The same data users sometimes play the role of a data controller or data processor without having imagination about that. What is most important, many people noticing their personal (intimate) data is being shared among others without their consent at the same time including content breaching their constitutional right to honor and dignity, basically do no act.

The reason for such a sad scenario is a) unawareness of rights and obligations in the social networks, b) fear to act because of threats (social factor), c) financial disability to protect data protection rights.

It is important for users to be able to feel confident that the information they share will be processed appropriately. They should know whether this information has a public or private character and be aware of the implications that follow from choosing to make the information public. In particular, children, especially teenagers, and other categories of vulnerable people, need guidance in order to be able to manage their profiles and understand the impact that the publication of information of a private nature could have, in order to prevent harm to themselves and others[98]. Although Armenian Law "On Personal Data Protection" is the only and main law regulation the data protection issues, it generally involves all the necessary requirements stipulated by the GDPR. The other question is the implementation and use of the law. Practically, the Law is not very widespread, and a small percent of the population is aware of its regulations.

[98] See "The EDRi papers an Introduction to Data Protection (ISSUE 06)".

Some practical steps can be offered for the data providers to comply with the data protection regulations, for example:

1) obtaining consent from the users before processing any of their personal data. They are free to choose the ways correspondent to the law;
2) protecting user's data privacy by keeping the data they share with them anonymously;
3) sending notifications to the users immediately in the event of a data flow or security breach;
4) notifying the users about the recent privacy policy changes (this step is almost not used practically);
5) providing a free electronic copy of all personal information collected from a given user upon request, and disclose the purpose for collecting such information;
6) erase data from the data system if there is sufficient ground provided by the user;
7) appointing a Data Protection Officer if the service provider requires regular monitoring of subjects on a large scale or deals with users who have been convicted of criminal offenses.

Finally, to sum up, above-mentioned chapters, our suggestion is to make the following changes or amendments in Armenian legislation to improve legal practice:

1. To include a separate chapter on SNS data protection in the RA Armenian Law "On Personal Data Protection" or;
2. To adopt a separate specific legal act on SNS data protection considering the vital role of SNS in people's life today, also the existing and possible threats to personal data protection issues;
3. To amend the relevant law with the definitions of "data controller", "data processor", "data subject", to add the definition of household exemption for data subjects, and to add a separate chapter for remedies and liabilities which do not exist.

BIBLIOGRAPHY

1.Books and articles

1.1. European Union Law: A Very Short Introduction, Anthony Arnull, Oxford University Press 2017

1.2. Data Privacy in Social Media: Who Takes Responsibility and Data Protection as a Priority Feature, Aigerim Berzinya, 2018

1.3. Privacy in Social Networks: A Survey, Elena Zheleva, Lise Getoor, University of Maryland, USA, MD 20742

1.4. European Union Agency for Fundamental Rights and Council of Europe, " Handbook on European Data Protection Law" (2018)

1.5. European Data Protection Supervisor (2017), Understanding the Internet of Things.

1.6. Factsheet of the European Commission, "How will the data protection reform affect social networks?" (2016)

1.7. The EDRi papers an Introduction to Data Protection (ISSUE 06)

1.8. Report of the International Commissioner's Office "On Social Networking and Online Forums – When Does the DPA Apply"

2. Websites and newspapers

2.1. https://www.theguardian.com/technology/2018/

2.2. https://edri.org/files/paper06_datap.pdf

2.3.https://www.theguardian.com/technology/2018/may/24/mark-zuckerberg-set-up-fraudulent-scheme-weaponise-data-facebook-court-case-alleges

2.4.https://www.loc.gov/law/foreign-news/article/united-kingdom-cliff-richard-wins-privacy-case-against-bbc-and-south-yorkshire-police/

2.5.https://ico.org.uk/media/for-organisations/documents/1600/social-networking-and-online-forums-dpa-guidance.pdf

2.6. http://ico.msgfocus.com/q/1AFB31cD3v/wv#story5

2.7. https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pd

2.8. https://link.springer.com/article/10.1007/s12394-009-0017-3

2.9.https://dataprotection.ie/viewdoc.asp?m=&fn=/documents/Facebook%20Report/final%20report/report.pdf

2.10. https://link.springer.com/article/10.1007/s12394-009-0017-3

2.11. https://link.springer.com/article/10.1007/s12394-009-0017-3

2.12. https://www.investopedia.com/terms/s/social-networking.asp

2.13.https://op.europa.eu/en/publication-detail/-/publication/695afd1d-539b-4475-a892-d1f5bbc9f489/language-en

2.14. https://www.investopedia.com/terms/s/social-networking-service-sns.asp

2.15. https://dictionary.cambridge.org/dictionary/english/social-network

2.16. https://www.investopedia.com/terms/s/social-networking-service-sns.asp

2.17. https://www.loc.gov/law/foreign-news/article/united-kingdom-cliff-richard-wins-privacy-case-against-bbc-and-south-yorkshire-police/

2.18. https://en.wikipedia.org/wiki/Privacy_concerns_with_social_networking_services

2.19.https://www.theguardian.com/technology/2018/may/24/mark-zuckerberg-set-up-fraudulent-scheme-weaponise-data-facebook-court-case-alleges

2.20.https://ico.org.uk/media/for-organisations/documents/1600/social-networking-and-online-forums-dpa-guidance.pdf

2.21.https://vidyareviewsblog.wordpress.com/2016/04/28/rights-and-responsibilities-of-individuals-using-social-media/

2.22. http://www.justice.am/storage/uploads/2019Annual-report-2019-ATPG.pdf

3.Conventions, laws, and regulations

3.1. The European Convention for the Protection of Human Rights and Fundamental Freedoms (1950)

3.2. General Data Protection Regulation (EU) 2016/679

3.2. Directive 95/46/EC of the European Parliament

3.3. E-Commerce Directive 2000/31/EC (2000)

3.4. WP29 in Opinion 5/2009 on Online Social Networking (2009)

3.5. RA Constitution (2015)

3.5. The RA Law On the Protection of Personal Data

3.6. The RA Code on Administrative Breaches

3.7.45/2001 of the European Parliament and of the Council of 18 December 2000 "On the Protection of Individuals with Regard to the Processing of Personal Data by the Institutions and Bodies of the Community and on the Free Movement of Such Data (2001)

3.8. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No.108ETS No.108

3.9. Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows (2001)

3.10. Protocol Amending the Convention for Protection of Individuals with Regard to Automatic Processing of Personal Data (2018)

3.11. Article 29 Working Party (2010), Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, Brussels, 16 February 2010

3.12. *Working Party (2011), Opinion 15/2011 on the definition of consent, WP 187, 13 July 2011*

3.13. Explanatory Report of Modernized Convention 108 of the Council of Europe

3.14. ICO, "Guide to the General Data Protection Regulation" (2018)

3.15. Modernised Convention 108 of the Council of Europe

3.16. Belgian Privacy Commission, Recommendation 02/2007

4. *Court Cases*

4.1. CG v Facebook Ireland Ltd., Case No: NICA 54 (2016).

4.2. K.U. v. Finland. K.U. v. Fin., App. No. 2872/02, 48 Eur. H.R. Rep. 52 (2009)

4.3. AY v Facebook (Ireland) Limited and Others, Case No: NIQB 76 (2016).4.5.

4.4. Applause Store Productions Ltd v. Raphael, Case No: EWHC 1781 (QB) (2008).

4.5. Irish DPA Facebook Ireland Ltd Audit [2011]

4.6. 218/CJEU, C-212/13, František Ryneš v. Úřad pro ochranu osobních údajů, 11 December 2014,

4.7. Law Society and Others v Rick Kordowski (Solicitors from Hell) [2011] EWHC 3185 (QB)

4.8. Google Spain, S.L. v. Agencia Española de Protección de Datos (Spanish Data Protection Agency) [2014]

4.9. Court of Justice of the EU, 11 December 2014, (František Ryneš v. Úřad) C-212/13

4.10. Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, App. No: C-131/12

4.11. USA v. Bodil Lindqvist, Case No: C-101/01 (2003)

4.12. Karabeyoğlu v. Turkey, App No: 30083/10, (2016); Mustafa Sezgin Tanrıkulu v. Turkey, App. No: 27473/06 (2017).

4.13. Kärntner. Landesregierung and Others [2013] O.J. C79/7.