UDC: 004.773.6/.7(4-672EU)
004.773.6/.7(497.11)

SOCIAL NETWORKS AND PROVING: NEW DILEMMAS FOR A NEW AGE[1]

Anđelija Tasić
Associate Professor, Faculty of Law, University of Niš
E-mail: andjelija@prafak.ni.ac.rs

Abstract

The development of social networks is one of the significant turning points in the short history of the Internet. The human need to "see" and "be seen", to project a good impression of themselves in the virtual world, is embodied in sharing information, photos and recordings about themselves, as well as about third parties. In the era of digital technologies, such behavior entails specific legal consequences but, above all, it has a significant impact on the transformation or (at least) adaptation of some conventional institutes, such as the burden of proof. This paper focuses on the issues of obtaining, adducing and evaluating evidence obtained from social networks in the course of civil procedure. The author analyzes the existing legal provisions on this matter, in an attempt to provide answers to the questions: whether the content found on social networks can be used as evidence in civil court proceedings, whether its usage depends on the fact that the content is publicly available or "locked"; and whether it implies the court-imposed duty to submit content from one's own and/or another's profile as evidence. The relationship between privacy on the Internet, protection of personal data, and the endeavor to accurately and comprehensively establish the factual grounds in a particular lawsuit have been reflected in the long-standing dilemma related to the use of evidence obtained in (il)legal ways.

Keywords: burden of proof, evidence, social network, digitization, illegally obtained evidence

1. Introduction

According to the results of the recent research 81% of households in 2021 has an internet connection (an increase of 0.9% compared to 2020). The internet is mostly used for telephoning over the internet/video calls (93.7%), sending online messages via Skype, Messanger, Whatsapp, Viber (84.7%), reading online information (76.8%) and participating in social networks (74.3%) (Statistical Office of the Republic of Serbia, 2021). The same source confirms that 74.3% of the Internet population has an account on social networks. The most used social networks are Facebook (60%), YouTube (44%) and Instagram (54%) (The Initiative for new media and digital

[1] The paper has been the result of the project "The legal and social context of responsibility" supported by the Faculty of Law, University of Nis (2021-2025).

literacy, 2020). The Facebook users usually look at the random content, posts from family and friends and notifications, e.g. They are mostly interested in photos (60%), posts (22%) and videos (10%). Finally, the results of the same research show that Internet users spend 104 minutes daily on social media in comparison to, e.g. 23 minutes reading a press. The typical Facebook user (the most popular social network in Serbia) is a woman younger than 32 years old, high-educated and employed. That is why is expected that her activities on the social network during working hours, as well as her post and activities in general, attract the attention of her employer.

Than, it is not hard to imagine the following example:

Example 1: Marko Marić took a sick leave. The report on temporary impairment for work stated that he could not perform the daily tasks of entering data into the database due to vision problems. By reviewing his Facebook profile, the employer noticed that Marko posted several songs during working hours, congratulated the two friends on their birthday and commented on the news on four internet portals. Irritated by Marić's behavior, his employer fired him for abusing his right to leave due to temporary impairment for work. Marko Marić has brought a lawsuit to annul the illegal dismissal. The employer wants to use data from Marko's account as evidence. Will the civil court accept this evidence? Will the decision depend on whether Marko's posts are public or available only to his friends? If posts are only available for friends, does it matter that Marko accepted the employer as a friend and does the situation change if the employer became his friend through a fake profile? Or if he saw Marko's social media activities through Marko's friend's profile?

The definition of a social network itself is "a network of individuals (such as friends, acquaintances, and coworkers) connected by interpersonal relationships" (Merriam-Webster online). To inform the friends, make a statement or simply an impression, social network users (hereinafter: user) share different information – posts, photos or videos. Even the friend list can tell a lot about someone's connections and relations or the absence of them. Even though users can select the audience for their post, such as a group, all of their friends, the public, or a customized list of people, not many of them do so. However, due to negligence, someone can make a follofing omission:

Example 2: Elena Petrović has brought a lawsuit for damage compensation due to the reduction of life activity because of injuries caused by a traffic accident. However, on her profile on the social network, the application shows that she runs up to 10 km a day in a preparation for the half marathon.

2. Right to privacy

The right to privacy is a fundamental human right, guaranteed by numerous international and national legal acts. Even though this right is prescribed by the Universal Declaration of Human Rights (Art. 12) [2] and the International Covenant on

[2] Universal Declaration of Human Rights, General Assembly resolution 217 A, proclaimed on 10 December 1948.

Civil and Political Rights[3] (Art. 17), the widest protection is given by Article 8 of the European Convention on Human Rights and Fundamental Freedoms - *Everyone has the right to respect for his private and family life, his home and his correspondence* - and the jurisprudence of the European Court of Human Rights[4]. It is worth mentioning the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[5], whose aim is to safeguard the right to respect privacy.

On the national level, the most significant act is the Constitution of the Republic of Serbia[6]. It protects the inviolability of home - *A person's home shall be inviolable* (Art. 40. l. 1), Confidentiality of letters and other means of communication - *Confidentiality of letters and other means of communication shall be inviolable* (Art. 41. l. 1) and Protection of personal data - *Protection of personal data shall be guaranteed. Collecting, keeping, processing and using of personal data shall be regulated by the law* (Art. 42, l. 1. and 2). Derogation of those rights shall be allowed only under special circumstances and following the law.

Protection of personal data is further regulated by law – Act on Personal Data Protection[7]. This Law shall set out the conditions for personal data collection and processing, the rights and protection of the rights of persons whose data are collected and processed, limitations to personal data protection, proceedings before an authority responsible for data protection, data security, data filing, data transfers outside the Republic of Serbia and enforcement of this Law. The right to privacy is also protected by the Act on Free Accession to Information of Public Importance[8] and the Act on Misdemeanors[9], e.g.

However, the change toward the protection of the right to privacy is obvious in the last two decades. From 9/11 until COVID-19 many turnovers led to the review of the right to privacy in favor of the right to security. Previous Serbian Criminal Procedure Code (2001), for example, prescribed covert surveillance only for cases when there is a suspicion that the act was committed, and the Criminal Procedure Code[10] from 2011 allows this surveillance even if there is a suspicion that there will be a crime committed in the future (Stepanović, 2020: 25).

[3] International Covenant on Civil and Political Rights, adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966.
[4] European Convention on Human Rights and Fundamental Freedoms, Rome 04/11/1950 - Treaty open for signature by the member states of the Council of Europe and for accession by the European Union.
[5] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg 28/01/1981 - Treaty open for signature by the member States and accession by non-member States.
[6] Constitution of Republic of Serbia, Official Gazette No. 98/2006 and 115/2021.
[7] Act on Personal Data Protection, Official Gazette No. 87/2018.
[8] Act on Free Accession to Information of Public Importance, Official Gazette No. 120/2004, 54/2007, 104/2009, 36/2010 and 105/2021.
[9] Act on Misdemeanors, Official Gazette No. 65/2013, 13/2016, 98/2016 - CC decision, 91/2019 and 91/2019 – other act.
[10] Criminal Procedure Code, Official Gazette No. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 – CC decision and 62/2021 – CC decision.

Even though the right to privacy, in general, is fairly protected, the employee's right to privacy is still in the "gray zone". One of the reasons is the absence of a strict border between private and professional life. This border is even thinner with the new forms of work, such as working from home and the fluid working hours. Regarding an employee's right to privacy it has more often been spoken about (allowed or not allowed) interference in an employee's right than their violation. Even Article 8 of ECHR stands that *there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.* The violation exists only when the interference is not allowed (Kovač-Orlandić, 2018: 63).

Having in mind that the regulation is incomplete and the jurisprudence is still insufficient, the US case law developed the standard of reasonable expectation of privacy[11] (Danilović, 2017: 172-176). This standard states that, having in mind that the employers are the owners of the means of work (economic power), they have a right to surveillance if it could have been reasonably expected. This expectation should fulfill two criteria: objective and subjective. Objective expectations exist if the society would expect privacy in a certain situation; subjective expectations exist if the employee could expect privacy in a concrete situation at a certain employer. Unlike the US jurisprudence, the European doctrine of the reasonable expectation of privacy put the right to dignity in the focus. However, the ECHR case law is closer to the US than to the European understanding of this doctrine.

There are several significant ECHR decisions that confirm communication from business premises are covered by the notions of "Private life" and "Correspondence" within the meaning of Article 8. The most important, probably, is *Barbulescu v. Romania*[12]. However, in this case the Court decided to leave open the question of whether the applicant had a reasonable expectation of privacy because, in any event, "an employer's instructions cannot reduce private social life in the workplace to zero. Respect for private life and the privacy of correspondence continues to exist, even if these may be restricted in so far as necessary". The State should provide the fulfillment of the proportionality criteria and procedural guarantees against arbitrariness. "In this context, the Court has set down a detailed list of factors by

[11] In the US the privacy is protected by the Fourth Amendment: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. The key question now is – what is covered by the Fourth Amendment in the modern era? (Silva, 2020: 607-627).

[12] Application No. 61496/08.

which compliance with this positive obligation should be assessed: (i) whether the employee has been notified clearly and in advance of the possibility that the employer might monitor correspondence and other communications, and of the implementation of such measures; (ii) the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy (traffic and content); (iii) whether the employer has provided legitimate reasons to justify monitoring the communications and accessing their actual content; (iv) whether there is a possibility of establishing a monitoring system based on less intrusive methods and measures; (v) the seriousness of the consequences of the monitoring for the employee subjected to it as well as the use made of the results of monitoring; and (vi) whether the employee has been provided with adequate safeguards including, in particular, prior notification of the possibility of accessing the content of communications. Lastly, an employee whose communications have been monitored should have access to a "remedy before a judicial body with jurisdiction to determine, at least in substance, how the criteria outlined above were observed and whether the impugned measures were lawful" (Council of Europe/European Court of Human Rights, 2021: 130-131).

However, ECHR has not developed the case law concerning monitoring the content of social media to provide legal evidence, so the answers to the abovementioned dilemmas have to be found somewhere else.

3. Social networks and collecting evidence

Social networks have their privacy settings. Everyone could decide on the publicity of his/her post, photos and videos. Except for the public information (name, profile picture, cover photo, gender, username, user ID (account number), and networks) the access to all other information could be restricted. For example, posts on Facebook could be public (available to all network users), private (available for profile friends only) or customized (available only for a certain group of people/ a single person, specified by the profile user).

Privacy on the Internet includes the right to personal information and its storage, use, security from the third parties and the displaying information, as well as the ID information about the visitors of the certain web page (Kostić, Vilić, 2013: 61).

In my opinion, a parallel could be drawn between the usage of the data from social media and the illegally obtained evidence. If the posts and photos were public – available to everyone, the social media owner could have expected they could be used in court. The same goes if the profile owner made the information public for his/her friends, knowing or having to be aware that interested parties could reach them. On the other hand, if the profile was locked, the evidence reached in that way should be considered illegally obtained evidence. The same should be considered for the information reached from the false friend's profile.

Where do the European, and where do the national regulations concerning illegally obtained evidence stand? More important, what falls under the scope of evidence?

The rules on Civil Procedure in European Union haven't been harmonized yet[13]. There has been certain progress in this area, made by forming a working group in 2014[14], with the support of the European Commission, with the aim of establishing civil procedure rules in several areas. However, these solutions are extremely significant because they provide guidelines for the future development of the European Civil Procedure Law. The Rules has been published in 2021[15].

According to these Rules, Parties may offer any relevant document as evidence. Document means anything in which information is recorded or maintained in any form, including but not limited to paper or electronic form[16]. Information may be recorded in writing, pictures, drawings, programmes, voice messages, or electronic data, including e-mail, social media, text or instant messages, metadata, or other technological means. It may be maintained electronically on, but not limited to, computer, portable electronic devices, cloud-based or other storage media (Rule 111). "The Rule, therefore, is open to the reality of electronic documents; although they may lack of tangible physical form of existence, they serve the same function by storing information permanently and displaying it authentically" (ELI/UNIDROIT Model European Rules of Civil Procedure - Explanatory report, 2021: 235). This attitude was highly unaccepted twenty years ago. At that time, US courts found evidence from the Internet "'voodoo information taken from the Internet," a source the judge regarded "as one large catalyst for rumor, innuendo, and misinformation," concluding that "any evidence procured off the Internet is adequate for almost nothing.'" (Browning, 2011: 470).

As for illegally obtained evidence – they must be excluded from the proceedings. Exceptionally, the court may admit illegally obtained evidence if it is the only way to establish the facts. In exercising its discretion to admit such evidence the court must take into account the behavior of the other party or non-parties and the gravity of the infringement (Rule 90). So, the intention is to reject illegally obtained evidence. However, the European Court of Human Rights accepted this exception in some decisions, which was the base for the approach accepted in the Rules[17].

[13] More on three groups of instruments for harmonization (coordination of national legislation, the establishment of minimum standards and the concept of individual procedure) Hess, 2016: 7-9.

[14] Within the project *'Transnational Civil Procedure - Formulation of Regional Rules'*, 2014, the ELI (European Law Institute) and the UNIDROIT formed a working group, divided into several areas, consisting of 30 prominent legal experts. First, they started with the work of groups that were involved in delivering, previous and temporary measures and access to evidence. Then, the work of the group expanded to the adjudicated matter *(res judicata)* and parallel proceedings and obligations of the parties, attorneys and judges; subsequently, their work included the issue of costs and decisions (Retrieved from https://www.europeanlawinstitute.eu, 31.5.2022).

[15] ELI/UNIDROIT Model European Rules of Civil Procedure (hereinafter Rules).

[16] The lack of electronic evidence lais in their vulnerability. They can be easily harmed, hard for processing and easy to manipulate (Čizmić, Boban, 2017).

[17] *L.L. v. France* (Application no. 7508/02) Second Section Judgment of 10 October 2006.

Serbian Civil Procedure Act[18] does not declare illegally obtained evidence. If it is taken that inadmissible evidence is the one that judicial decision cannot be based on, Civil Procedure Act only deals with the prohibition of testimony (Article 247 and 248)[19]. However, this situation does not apply to the above mention hypothetical cases. Unlike the Civil Procedure Act, Criminal Procedure Code prohibits the violation of the secrecy of letters and other mail (Article 142); unauthorized wiretapping and recording (Article 143); unauthorized photographing (Article 144); unauthorized publication and presentation of another's writings, portraits and recordings (Article 145); and unauthorized collection of personal data (Article 146).

So, it stays unclear what could be done with the information taken from the social media without the knowledge and approval of the profile's owner. The issue of evidence in Example 1 from the beginning of the article is important because the abuse of the right to a leave of absence due to temporary impairment to work is one of the reasons for the cancellation of the employment contract (Art. 179. l. 1. p. 3 of the Employment Act Serbia). The Serbian case law stands that "the abuse would exist, if the plaintiff's behavior during the temporary incapacity for work (…) prevented recovery or caused the deterioration of health, which is the reason for his inability to work"[20]. If the court allows the use of the data collected from the internet, it could be sufficient for the decision in favor of the employer.

The same goes for Example 2. According to Act on Contracts and Torts, for physical pains suffered, mental anguish suffered due to reduction of life activities, becoming disfigured, offended reputation, honor, freedom or rights of personality, death of a close person, as well as for fear suffered, the court shall, after finding that the circumstances of the case and particularly the intensity of pains and fear, and their duration, provide a corresponding ground thereof – award equitable damages, independently of redressing the property damage, even if the latter is not awarded (Article 200)[21]. So, if the application is to be considered valid evidence, the plaintiff's demand is most likely to be rejected.

To conclude, it seems that even the evidence collected without the knowledge of the social network profile owner could be used in the civil litigations. Whether or not the one who collected them could be punished in accordance with the rules of the Criminal Procedure Code is the question whose answer does not affect the civil litigation.

[18] Civil Procedure Act, Official Gazette No. 72/2011, 49/2013 - CC decision, 74/2013 – CC decision, 55/2014, 87/2018 and 18/2020.

[19] Unlike Serbian legislation, some other European Civil Procedure Acts deal with the use of illegally obtained evidence. More: Tasić, 2016.

[20] The Judgment of the Court of Appeal in Kragujevac Gž1 2973/2019 dated 4.2.2020.

[21] Act on Contracts and Torts, Official Gazette SFRJ No. 29/78, 39/85, 45/89 - CC decision 57/89, Official Gazette SRJ No. 31/93, Official Gazette SCG No. 1/2003 - Constitutional Charter and Official Gazette RS No. 18/2020.

4. Concluding Remarks

The concept of evidence has significantly changed in a digital era. The Internet has become a valuable source of information and it is recognized even in ELI/ UNIDROIT Model European Rules of Civil Procedure. Also, even though highly appreciated, the right to privacy is not safeguarded without restrictions. In certain situations, even interference in someone's privacy could be justified. European Court of Human Rights confirmed that in the situation when the disputed evidence it is the only way to establish the facts, it could be accepted. The Serbian legislator, unfortunately, goes far behind. Not only that evidence collected from the Internet are not mentioned in any way in Civil Procedure Act, but there is no definition or explanation of the usage of illegally obtained evidence.

References

1. Act on Contracts and Torts, Official Gazette SFRJ No. 29/78, 39/85, 45/89 - CC decision 57/89, Official Gazette SRJ No. 31/93, Official Gazette SCG No. 1/2003 - Constitutional Charter and Official Gazette RS No. 18/2020.
2. Act on Free Accession to Information of Public Importance, Official Gazette No. 120/2004, 54/2007, 104/2009, 36/2010 and 105/2021.
3. Act on Misdemeanors, Official Gazette No. 65/2013, 13/2016, 98/2016 - CC decision, 91/2019 and 91/2019 – other act.
4. Act on Personal Data Protection, Official Gazette No. 87/2018.
5. *Barbulescu v. Romania,* Application No. 61496/08.
6. Browning, J. (2011). Digging from the Digital Dirt: Discovery and Use of Evidence from Social Media Sites. SMU Science and Technology Law Review. Vol. XIV: 2011.
7. Civil Procedure Act, Official Gazette No. 72/2011, 49/2013 - CC decision, 74/2013 – CC decision, 55/2014, 87/2018 and 18/2020.
8. Constitution of Republic of Serbia, Official Gazette No. 98/2006 and 115/2021.
9. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg 28/01/1981 - Treaty open for signature by the member States and for accession by non-member States.
10. Council of Europe/European Court of Human Rights. (2021). Guide on Article 8 of the Convention – Right to respect for private and family life.
11. Criminal Procedure Code, Official Gazette No. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 – CC decision and 62/2021 – CC decision.
12. Čizmić, J. Boban, M. (2017). Elektronički dokazi u sudskom postupku i računalna fornzička analiza. Zbornik Pravnog fakulteta Sveučilišta u Rijeci. (1991) v. 38, br. 1.
13. Danilović, J. (2017). Pravo na privatnost zaposlenih. Anali Pravnog fakulteta u Beogradu. 2/2017.

14. ELI/UNIDROIT Model European Rules of Civil Procedure. (2021).
15. ELI/UNIDROIT Model European Rules of Civil Procedure - Explonatory report. (2021).
16. Employment Act Serbia, "Off. Herald of RS", Nos. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017-Decision of the CC, 113/2017 and 95/2018 - authentic interpretation.
17. European Convention on Human Rights and Fundamental Freedoms, Rome 04/11/1950 - Treaty open for signature by the member States of the Council of Europe and for accession by the European Union.
18. Hess, B. (2016). Harmonized Rules and Minimum Standards in the Europea Law of Civil Procedure. Brussels: Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament.
19. International Covenant on Civil and Political Rights, adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966.Universal Declaration of Human Rights, General Assembly resolution 217 A, proclaimed on 10 December 1948.
20. Kostić, M. Vilić, V. (2013). Privatnost korisnika društvenih mreža. Zbornik radova Pravnog fakulteta u Nišu. 64 (2013).
21. Kovač-Orlandić, M. (2018). Pravo zaposlenog na privatnost i njegova zaštita (doktorska disertacija). Beograd.
22. *L.L. v. France (Application no. 7508/02),* Second Section
23. Judgment of 10 October 2006.
24. Silva, J. (2020). Reasonable expectations and Privacy in the Digital Age. Seton Hall Legislative Journal. (44:3:2020).
25. Stepanović, I. (2020). Život na internetu: pravo na privatnost i online komunikacije. Beograd.
26. Tasić, A. (2016). The Use of Illegally Obtained Evidence in Civil Procedure. International Scientific Conference "Control in National, International and EU Law". Niš.
27. The Initiative for new media and digital literacy. Citizens and Media: consumption, habits and media literacy. Belgrade. 2020.
28. Usage of information and communication technologies in the Republic of Serbia, 2020. Statistical Office of the Republic of Serbia. Belgrade. 2021.
29. Merriam Webster retrieved from https://www.merriam-webster.com/dictionary/social%20network.