Privacy and Trust on Social Networks: Overview and Some New Solutions

Andreja Samčović[1,*]

[1]Faculty of Transport and Traffic Engineering, University of Belgrade, Vojvode Stepe 305, 11000 Belgrade, Serbia

Abstract

Because of the rapid development of technology, the number of users of social networks is growing significantly from year to year. The main reason is that they are very easy to be used and allow users to share information of different types, from text messages to photos and videos. However, sharing personal data in an online environment carries certain risks. There are different types of security threats that users face. The basic division categorizes them into three groups, conventional, modern and targeted threats. To minimize the threats, various methods have been developed and used. When users are assured that they can use a social network unhindered, without fear of malicious use of their personal information, the level of trust among users increases. Social networks have different privacy policies, which describe how collected data is used. It is necessary for privacy policies to be simple and transparent, so that users can understand them and thus develop trust. Given that the issues of security and trust are an inexhaustible topic, new methods must be constantly developed. Some of them are described in the last part of the paper.

Keywords

Security, trust, personal data, online threats, privacy policies

1. Introduction

With the rise in popularity of the internet in the mid-1990s, it became possible to share information in ways never seen before. However, sharing personal information was still not popular. At the beginning of the 2000s and with the appearance of the first social networks, the sharing of private data via the internet began, which society accepted [1]. The reasons for using it are numerous, the largest number of users use social networks to keep in touch with family and friends, fill their free time or get information.

Social networking involves expanding contacts with other people through networks such as Instagram, Facebook, X and many others. They bring people together to talk, share interests or make new friends, and also allow users to have group chats, play social games or communicate with other users and are very easy to use. Due to these benefits, more and more people are using mobile social networks.

At the end of 2023, it is estimated that there are about five billion users of social networks worldwide [2]. The largest number of users are in Asia, specifically in China, which is also the largest social network market in the world. The most popular network is still Facebook, followed by YouTube. Data on the other ten most popular networks are given in Figure 1. The graph shows the number of active users during one month, known as MAU (Monthly Active Users), and is expressed in millions.

There are various applications of social networks. Figure 2 shows the basic components of social networks and the areas in which they are significant. Since a large part of the population use social networks, they have become an increasingly important medium for business promotion and awareness campaigns. Depending on their use, they can be used for entertainment, business opportunities, building a career, improving social skills and creating relationships with other people [1]. Figure 3 shows the different types of social networking sites that can be broadly classified.

With the increasing number of users, services and platforms are trying to improve the user experience by providing personalized services, recommending content or friends, all with the aim of retaining old and attracting new users. Users have become increasingly dependent on sharing personal opinions,

BISEC'2024: 15th International Conference on Business Information Security, November 28-29, 2024, Niš, Serbia

*Corresponding author.

andrej@sf.bg.ac.rs (A. Samčović)

0000-0001-6432-2816 (A. Samčović)

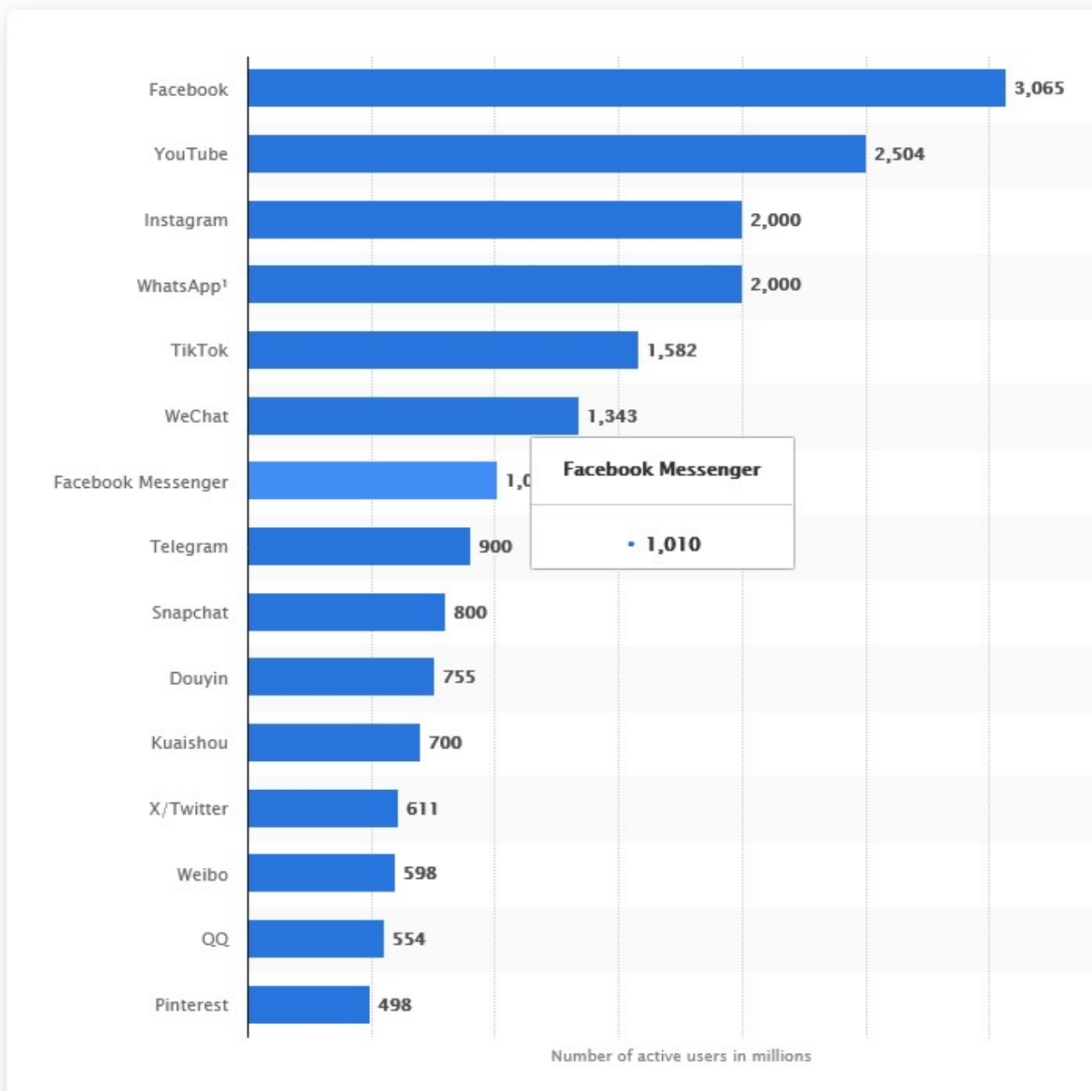

Figure 1: Number of users of social networks [2].

feelings and ideas with an ever-increasing group of "friends". As an increasing number of people consider social networks as a communication tool, it is necessary to protect the information stored on these sites, which is often neglected. Over time, more and more information is placed on social networks in various forms, which can easily lead to unauthorized access to personal and business data. The evolution of users in online communication enables the creation of a new world of content created by users.

2. Privacy and trust in social networks

Security and privacy in social networks are interrelated, and while privacy refers to control over personal information security involves protecting information from unauthorized access and malicious activity. In order to ensure adequate data protection that contributes to the preservation of user privacy, it is necessary to understand all spheres of privacy on social networks, which can be categorized as:

- Privacy when creating social graphs;

Figure 2: Basic components of social networks (https://cite.co.uk/thoughts/the-different-types-of-social-media/).

- Privacy of activities on social networks;
- Privacy when sharing multimedia content;
- Privacy in cyber-physical systems;
- Privacy in mobile social networks;
- Privacy in other applications.

Privacy when creating social graphs implies the use of data by a third party or for data mining. Social network graphs are commonly explored for marketing or data mining purposes, which can reveal sensitive information about individuals [3]. The layout of a social graph is shown in Figure 4. The numbers on the links represent the number of interactions between users.

A big problem with the algorithms used to create graphs are attacks on users due to poor anonymization. However, algorithms are constantly exposed to maintenance, privacy and usability challenges, and it is necessary to find a good compromise. Privacy must be sufficiently protected, but on the other hand utility must be guaranteed. This implies that the algorithms should reduce information loss and thus keep the graphs informative and meaningful for analysis.

Privacy of activities on networks means preventing the leakage of users information due to their activities, such as sharing or commenting on content. However, this is an unavoidable privacy risk that cannot be completely eliminated, but can only be mitigated. Some of the currently proposed solutions are calculating and then notifying users of possible risks, or proposing privacy configurations for each post.

Privacy when sharing is aimed primarily at the co-owner of the multimedia content. A co-owner of content is a person whose information is linked to another person, for example, posting pictures or videos that include another person. Commenting on networks can only endanger one person by sharing content that other people are on can give away information about them. In order to preserve the privacy of all owners of shared multimedia content, a system of credentials based on attributes with enhanced privacy protection was implemented [3].

The system works by allowing access only to those users who meet the access policy, instead of all users. The access policy is defined by all content co-owners and is based on viewer attributes, such as

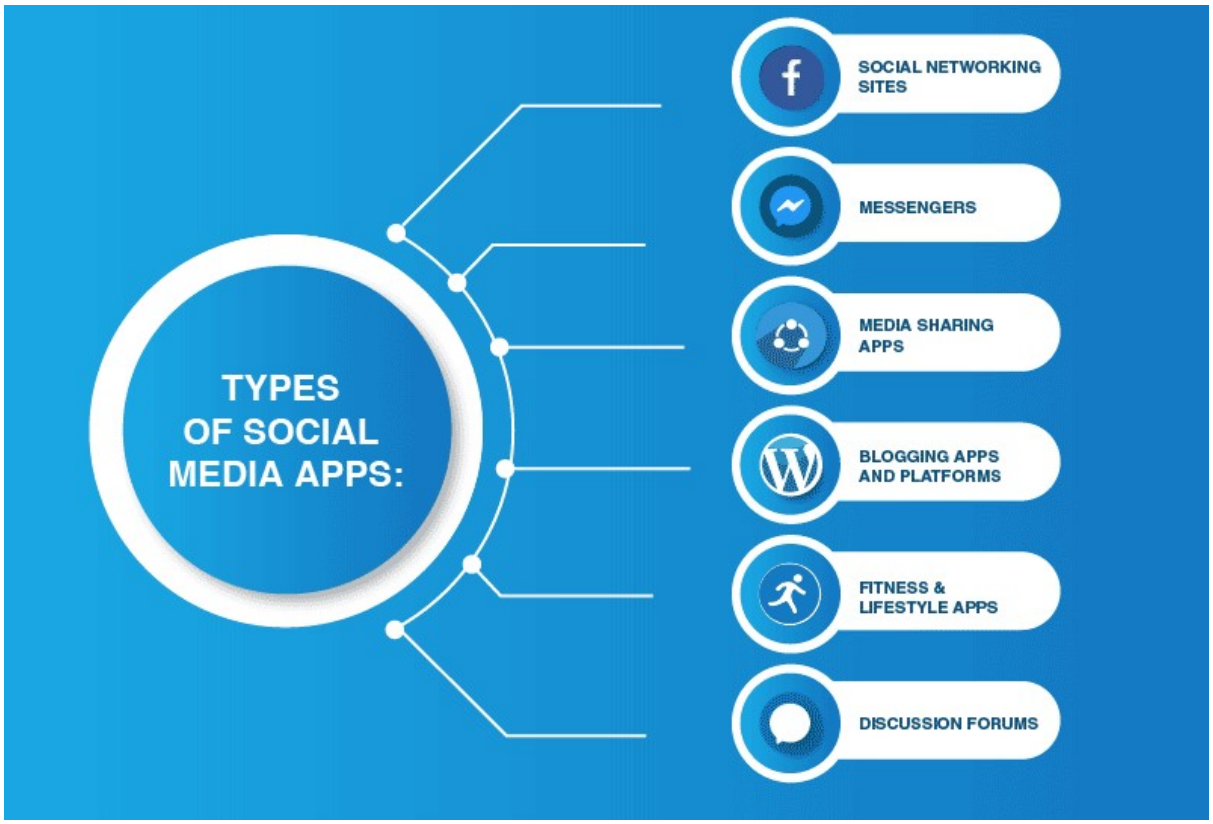

Figure 3: Various types of social networks.

gender or age. In this way, the privacy of co-owners is preserved, as well as viewers who can access without to reveal their identity.

Mobile social networks, such as Facebook or Instagram, allow users to share with others in real time what and where they are doing. The downside of this is that sensitive user information, such as their location, is exposed. Therefore, location privacy is particularly important in these systems. The privacy-preserving models used are different. Some include differential privacy when publishing data from social networks or using multiple location servers instead of just one server [3].

Other apps where privacy is compromised can be dating apps or spam filtering apps. When using dating apps, users upload their personal information, and several methods have been devised to prevent misuse of that information. For example, only users whose interests match can find each other. Also, decentralized infrastructure as a new way of protection has become the subject of various researches on the topic of privacy preservation.

In addition to mechanisms that protect user privacy, it is necessary for users to be informed about the threats lurking on the internet and social networks. They should be able to act conscientiously and use reliable security measures. Behavior depends a lot on their awareness and experience on social networks. For example, users who have been victims of identity theft or cyberbullying will have a very different perspective on security and trust than those who have not had such experiences. How much trust users will have also depends on how organizations protect the information that is shared. If there is a violation of some of the measures, the economic growth of the organization is reduced, but at the same time, the trust of the users is also violated. Because of this, business organizations are putting more and more effort into protecting user data.

The problem of security and trust are inextricably linked, namely the security of social networks can affect the analysis of user trust. The increase in trust provides a better awareness of the environment and a guarantee of security on networks. When it comes to large-scale mobile social networks, there is the possibility that users may belong to a number of communities or clusters. There is the problem

Figure 4: Social network graph.

of how to evaluate the user's trust. This assessment plays an important role in the social connection between users.

Users who are more aware of the issue of security and privacy on social networks, take more care of their data. If the platform offers easily accessible information about privacy and security, it can help to achieve better trust among users. It may happen that users are not aware of all the privacy options that a particular social network offers, and because of this, there is an unwitting oversharing of information. Therefore, it is necessary for social networks to provide users with easy access to privacy settings. Social networks with easy-to-understand interfaces and regularly updated privacy policies create users with a higher level of trust.

3. Social networks privacy policies

An understandable and easily accessible privacy policy can influence the increase of user trust. The privacy policy describes the ways in which the social network collects and manages the data of users. Its purpose is to best describe to users how to safely use social networks. Privacy policies should primarily provide users with information about what data is collected, how long it is stored, and who can see and use it. Users often do not attach enough importance to privacy policies, primarily because they do not understand why their data is being used. The understanding of the policy is most influenced by the way it is presented to the users. If it is written in a simple way, explicitly explaining the ways and reasons for data collection, users will understand it more easily and will be aware of how their data is used. Conversely, if it is vaguely written, users will ignore important information.

Using cookies and other technologies, social networks collect data about the user's device and location. Device information is: device type, identification information, access point from which the device receives WiFi signal, operating system details, storage space, battery level, etc. Important information is also which Internet service provider and operator are used, as well as the type of browser, operating

system and proxy server. When it comes to location, it is possible for social networks to receive GPS (Global Positioning System) location data. If the network is accessed via a mobile device, the location data depends on the settings of the device itself. Regardless of whether location settings are turned off, social networks obtain the IP address of the accessed device [4, 5, 6, 7].

3.1. Meta, X and LinkedIn privacy policies

Although in theory everything seems quite simple when it comes to privacy policies, practice says otherwise. The creators of social networks are aware of the need of users to stay in touch with each other. The biggest drawback of privacy policies is the way they are written. Most often, they are too extensive and not sufficiently understandable. Their authors deliberately use legal language, which discourages users from reading in its entirety [8]. This paper reviews the privacy policies of the following social networks: Meta (which includes Facebook and Instagram), X, LinkedIn and Telegram [9].

Account creation data includes username, password, e-mail or phone number. This is the data that all social networks collect. Other data depends on the social network. Meta provides users with the opportunity to provide information with special types of protection, such as information about sexual orientation, political views, health, racial or ethnic origin, and the like [10]. X collects user profile information, which, in addition to the above, also includes information about logging in using third parties. If the account is professional, the phone number on work and e-mail address are required, which will be publicly available to all users [11]. X also collects employment information, with the goal of suggesting business opportunities to users who provide such information.

LinkedIn is a professional social network used for establishing business contacts and job searching. Therefore, the collected data may differ from the other examples. The collected data has business nature, for example, information about the user's education, work experience, skills, photo of the user, location where he lives (e.g. city or country). It is possible for the user to attach, in addition to this, the verification of information or work establishment. This data is not necessary, but it helps to personalize the content and contacts that will be displayed to the user. Also, they are visible to all other users. If the user wants to make a purchase in one of the mentioned social networks, it is necessary to attach payment information, e.g. payment cards. This information is necessary on the social network LinkedIn, if the user wants to use the services of the premium service.

Meta, **X** and **LinkedIn** collect information about the content that the user creates or views. Ads and advertisements are included in this content, and the way users interact with them is monitored. Meta collects information about the metadata of content and messages in accordance with the law of the user's country, hashtags, time, duration and frequency of network use. Data about friendships and groups helps Meta to better suggest new friendships to users.

X tracks user communication with other users by collecting metadata. Metadata includes the content of the message, recipients, date and time of the message, in the case of direct messages. If encrypted messages are used, the content of such messages remains encrypted. When making a purchase, X may receive information about the transaction, such as when it was made or the amount of the payment.

The last group includes information obtained from third parties. Social networks receive data from partners when users use their services. The data obtained in this way can be device data, interactions with advertisements, websites visited by the user, information about purchases. Meta divided the other persons who access user data into partners, suppliers and third parties. Suppliers can be measurement service providers and marketing service providers, which include partners and third parties with whom social networks share user data.

Common to all mentioned social networks is that they collect data for the purpose of managing and personalizing services, conducting analytics, improving security and user experience based on reactions. Account data is stored as long as the account exists, other data is stored for eighteen months. If the rules of behavior of the social network are violated, the data can be stored for a longer period of time.

The privacy policies of the mentioned social networks are transparent, easy to understand and provide the necessary information to users. The data that is collected as well as the reasons why it occurs are clearly stated. Each privacy policy contains a section dedicated to user rights. These are the

rights to access and manage data, such as correction or deletion. When the user is aware of his rights, the fear of uncertainty is reduced and he can have more trust on the social network.

3.2. Telegram privacy policy

While other social networks are focused on mass data collection for the sake of advertising and better personalization of data, Telegram is a social network where the imperative is placed on protecting the privacy and trust of users. This is precisely why Telegram is becoming an increasingly popular social network and is gaining a lot of user trust. Telegram offers various options, primarily using end-to-end encryption of messages [12]. This approach implies a different privacy policy compared to most other social networks.

Unlike other social networks, **Telegram** points out that user data is not used for advertising and that only the information necessary for the functioning of the platform is stored. It is possible that Telegram stores data about the user's email address, when he opts for two-factor account verification. This address is not used for other purposes, such as sending advertisements. All messages and conversations in public groups are stored on the cloud, that is, no third-party services are used to store messages. All information on the cloud is encrypted and no one but the user can access the content. The only cookies that are collected are those for the functioning of the platform, no marketing cookies are used. Minimal data collection contributes to strengthening user trust. Users have more control over their data, which means that users can consider Telegram as a reliable platform.

A special feature that makes this network stand out is end-to-end encryption. This type of data protection means that all data is stored as encrypted data strings and is known only to users who have the decryption key, i.e. the recipient and the sender of the content. This means that neither the platform itself nor third parties have the possibility to access the content of the communication. Although encryption ensures that messages are accessible only to the recipient and the sender, problems with spam and phishing attacks are present. In order to protect against phishing attacks, Telegram checks messages reported by users.

4. Some new solutions to improve trust

With the increase in the number of users, maintaining security on social networks is a constant challenge. Various attacks, misinformation, fake news and misuse of data threaten users and their identity. The development and application of new technologies are necessary to ensure a safe environment for users. Some of the methods that can be used are blockchain, the Zero Trust model, and artificial intelligence which can be used to detect deepfakes. Blockchain technology offers opportunities to decentralize data and increase transparency. The Zero Trust model provides constant user verification and thus reduces the risks of unauthorized access. Finally, the use of artificial intelligence is becoming more and more prevalent.

One of the technologies that can lead to a big improvement in social network privacy and trust is blockchain. Blockchain is a distributed database that is shared among the nodes of a computer network. As a database, blockchain stores information in a digital format [10]. It is best known for its role in crypto-currencies, as it provides secure and decentralized records of transactions.

Blockchain is a chain consisting of blocks of information. This technology enables secure sharing of digital assets over a peer-to-peer network, where files are hosted within nodes present on the network, as shown in Figure 5. Due to the use of peer-to-peer technology, there is no need to use third parties for data transfer and storage [10].

Blockchain-based social networks often operate on the principle of rewarding content creators. For example, the social network Indorse is a decentralized version of the LinkedIn [10]. The apps use a reward system, using tokens to encourage users to actively post content on the app and approve other users' content. This creates an environment with personalized and more interesting content, which makes the platform more valuable and of better quality.

Figure 5: Blockchain in social network.

No globally popular network today uses blockchain. However, there are some less popular networks that are based on a blockchain. Some of them are Streemit, Minds, Diaspora [10]. Diaspora is a network based on the concept of groups ("pods"). This network gives users complete control over their data and allows them to anonymously join and participate in different groups. It is based on three basic principles, decentralization, anonymity and privacy. Minds is a social network characterized by the fact that there is no censorship and users have complete freedom of speech. The platform is completely open-source. Streemit is based on a user reward model. The network monetizes and rewards users who post content with crypto-currencies. Before being allowed to register on the network, each user goes through a verification process.

The next model is the *Zero Trust*. The traditional protection models cannot be adapted to the development of modern technologies. That's why a model called Zero Trust was designed, which is based on the concept of "never trust, always verify" [11]. The four principles on which architecture of Zero Trust is based are:

- User authentication: A security assessment is performed based on location and device to determine whether to allow the user access. Multi-factor user authentication is used.
- Device authentication: only trusted end devices are allowed to access resources.
- Access restriction: control models are used that grant access permissions to users.
- Adaptability: different sources are constantly producing information, so it is necessary to use machine learning to define different security policies

The challenges in the implementation of this model are numerous. First of all, there is the resistance of organizations to changes, and the transition from existing systems to new ones is technically complicated [11]. It is important to take care of the balance between security and efficiency, because frequent authentication can frustrate users and reduce the use of the social network.

Artificial intelligence has already found application in various aspects of social networks, predominantly for deepfake detection. Deepfake uses deep learning technology to manipulate images and videos to create new fake content [12]. GAN (Generative Adversarial Networks), sophisticated deep learning models, play a key role in creating deepfake. These models are trained on large data sets to create the most believable fake content. Some of the techniques used for deepfake detection are:

RNN (Recurrent Neural Network), CNN (Convolutional Neural Network) and LSTM (Long Short-Term memory) networks.

5. Conclusion

Social networks have been an essential part of everyday life for a long time. They have become one of the main ways of communication between people, but also a place where business opportunities develop. This is precisely why it is necessary to ensure the highest possible level of quality, so the trust of users continues to grow.

User trust is achieved by providing a secure social media environment and assuring users that their data is safe. It is necessary to create a sufficient level of trust between users and social networks, so that the number of users and the quality of the social network itself will continue to increase. Privacy policies have the greatest effect in achieving a high level of trust. They provide users with information about what data is collected, how long it is stored, and who can see and use it. Users often do not attach enough importance to privacy policies, primarily because they do not understand why their data is being used. Therefore, it is necessary for them to be clear, transparent and to explain to users in a simple way why their data is collected.

Finally, it is important to emphasize the continuous development of new technologies. Some of the most significant ones are described in the paper. Blockchain can provide enormous benefits if introduced into social network systems, primarily bringing greater transparency and decentralization of the system. The Zero Trust model is intended for user authentication and is based on the concept that no user should be trusted, and that all requests should be verified. Although artificial intelligence brings a number of advantages, it can also be used to create fake content, which represents a new threat to social networks. Therefore, special tools are being developed using machine learning models to detect such content.

Acknowledgment

This work is supported by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia.

Declaration on Generative AI

The author has not employed any Generative AI tools.

References

[1] A. K. Jain, S. R. Sahoo, J. Kaubiyal, Online social networks security and privacy: comprehensive review and analysis, Complex & Intelligent Systems 7 (2021) 2157–2177.

[2] S. J. Dixon, Most popular social networks worldwide as of april 2024, by number of monthly active users, 2024. URL: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.

[3] V. V. H. Pham, S. Yu, K. Sood, L. Cui, Privacy issues in social networks and analysis: a comprehensive survey, IET networks 7 (2018) 74–84.

[4] Facebook Business Help Center, About fact-checking on facebook, instagram, and threads, 2024. URL: https://www.facebook.com/business/help/2593586717571940.

[5] X, X privacy policy, 2024. URL: https://x.com/en/privacy.

[6] LinkedIN, Linedin privacy policy, 2024. URL: https://www.linkedin.com/legal/privacy-policy#data.

[7] D. Petrović, Sociologija e-komunikacija, 2022.

[8] LinkedIN, Telegrad privacy policy, 2024. URL: https://telegram.org/privacy?setln=fa.

[9] A. Samčović, Security related use of facebook as a communication channel, in: Proceedings of the 14th International Conference on Business Information Security (BISEC'2023), 2024, pp. 26–31.
[10] M. A. Hisseine, D. Chen, X. Yang, The application of blockchain in social media: a systematic literature review, Applied Sciences 12 (2022) 6567.
[11] Y. He, D. Huang, L. Chen, Y. Ni, X. Ma, A survey on zero trust architecture: Challenges and future trends, Wireless Communications and Mobile Computing 2022 (2022) 6476274.
[12] A. M. Almars, Deepfakes detection techniques using deep learning: a survey, Journal of Computer and Communications 9 (2021) 20–35.