Journal of Global Research in Computer Sciences e-ISSN: 2229-371X

Balancing Privacy and Security: Navigating the Complexities of Digital Privacy in the Modern World

Mohammed Al-Harthi[1]*, Ahmed Al-Raisi[1] , Ali Al-Humairi[1,2]

[1]Department of Computer Science, German University of Technology, Muscat, Oman

[2]Department of Computer Science, Duisburg-Essen University, Rhine-Westphalia, Germany

Research Article

Received: 04-Mar-2023, Manuscript No. GRCS-23-90922; **Editor assigned:** 08-Mar-2023, Pre QC No. GRCS-23-90922 (PQ); **Reviewed:** 22-Mar-2023, QC No. GRCS-23-90922; **Revised:** 29-Mar-2023, Manuscript No. GRCS-23-90922 (R); **Published:** 05-Apr-2023, DOI: 10.4172/ 2229-371X.14.2.0010

***For Correspondence:** Mohammed Al-Harthi, Department of Computer Science, German University of Technology, Muscat, Oman

E-mail: 22-0880@student.gutech.edu.om

Citation: Al-Harthi M, et al. Balancing Privacy and Security: Navigating the Complexities of Digital Privacy in the Modern World. J Glob Res Comput Sci. 2023;14:0010

ABSTRACT

Privacy as we know it has changed dramatically since the start of the internet and the rise of Social Media Networks (SMN), where the Oxford dictionary gave privacy the following definition “the state of being alone and not watched or interrupted by other people”, this statement could be reflected on privacy before the age of SMN since privacy was limited to physical privacy, but now we have a new type of privacy which is the information privacy and we can’t use the same statement to define it, where the data online can be accessed by people or even Artificial Intelligence (AI) programs. With the new type of privacy new challenges, legislations and even human behaviour need to be discussed, implemented or changed. This paper tries to shed some light on the current understanding of privacy, the challenges of privacy in SMN and the laws and regulation that aims to secure this privacy for the people.

Keywords: Artificial intelligence; Estonian personal data protection act; Social media networks; Consumer data protection act; General data protection regulation

INTRODUCTION

Social networks existed long before the creation of social media and will continue to exist after the end of it. Until the human race perishes there will always be the concept of social network. In a famous study an experiment involved sending packets of information to people in the United States with instructions to send them to a specific person, located in Massachusetts, The participants were given only the person's name, occupation, and general location, and they were told to send the packet to someone they knew who was more likely to know the target personally, the study found that on average it took six hops reach the person, this was known as the “six degree of separation”, a study done by Facebook to explore this famous concept in social media networks and found that the average number of hops to connect any two users was 3.57 hence the name “Three and a half degree of separation”, this showed that the world has become closer together [1,2].

Platforms for social media encompass a range of software, interfaces, and online sites that enable users to create, share, and engage with content produced by other users, encompassing written material, visuals, video, and sound. These interactive digital environments provide individuals the chance to connect with friends, family, and other people, get involved in various groups, subscribe to certain pages, and integrate into virtual communities. Notable examples of such platforms include Twitter, TikTok, Instagram, Facebook, YouTube, and LinkedIn.
The origin of social media can be traced back to the dawn of the internet era, from the inception of the first email or the first online service for sharing thoughts. However, it wasn't until the late 1990s that the inaugural social media site, "SixDegrees.com," came online, established by Andrew Weinreich. Since then, numerous other social media networks have emerged, such as Friendster, Myspace, Foursquare, and Vine [3].

Social media networks made life easier for a lot of people in reaching their loved ones sharing memorable moments, thoughts or even a place just to run away from oppressive social construct, but as this new place thrived, privacy concerns rose with it, who can see it, who can use it, is the data protected enough, many issues that needed to be addressed, laws and legislations needed to be implemented or updated, but as all new things not all aspects could be covered and handled from day zero, that's why we have laws that get updated periodically or based on a precedent .This paper tries to explore the literature review on the topic of privacy in social media networks trying to find a definition for privacy in them and exploring new challenges that come along with it, and take a closer look at the laws and legislation in different regions of the globe that protect the personal privacy of individuals, and the possible methods in increasing the level of privacy in such sites.

MATERIALS AND METHODS

What is privacy?

The privacy of one's home, this statement describes the definition of the Oxford dictionary on privacy where it states that privacy is "the state of being alone and not watched or interrupted by other people" [4]. With the digital age and the rise of Social Media Networks (SMN) the statement privacy of one's home should be changed to the privacy of one's information, where the ability to control who can view your information, your ability to delete/edit data on SMN and your ability to stay anonymous is what define the new type of privacy [5].Since we have two types of privacy we need to find a suitable definition for both, physical privacy and information privacy. The first type of privacy has been the center of many debates in different aspects of life such as social and legal and have been discussed and still in discussion from hundreds and thousands of years, and the changes to the private/public spheres of privacy, where does the authority of an individual ends and the society authority begins [6]. While the second type of privacy is relatively new, just a few decades old, since the creation of the internet a new type of interaction came to exist, a new way to communicate with people and things around us.

A study on privacy argued that previous studies have used one of two paradigms to define privacy; the first was "privacy as control", where the amount of control that a person can exert over different aspects of privacy such as physical privacy, Information privacy or even social privacy.

The second paradigm was "privacy and control", in this paradigm privacy is considered separate from control where privacy is defined by having one's information protected from others accessing it, while control is a way which could be employed to manage the privacy, and control can be enforced through consent, correction or choice. The study then proposed a new model to fit the privacy in SMN where the model states that "An individual's assessments of

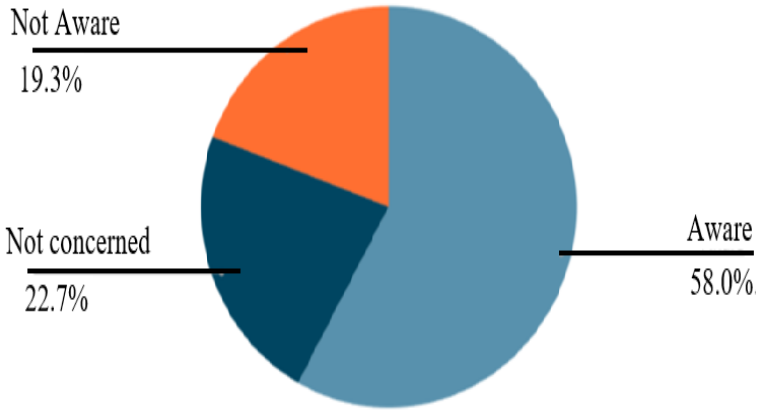
(a) The level of access to this person in an interaction or relationship with others (people, companies, institutions).
(b) The availability of the mechanisms of control, interpersonal communication, trust, and norms for shaping this level of access.
(c) Self-disclosure as (almost intuitive) behavioral privacy regulation.
(d) Control, interpersonal communication, and deliberation as means for ensuring (a somewhat more elaborated) regulation of privacy.

In social media, then, the availability of the mechanisms that can be applied to ensure privacy are crucially influenced by the content that is being shared and the social media affordances that determine how this content is further used". Privacy definition changes depending on the situation an individual is in as such there is no single statement to define it but multiple ones that can apply depending on the case.

With new privacy comes new challenges

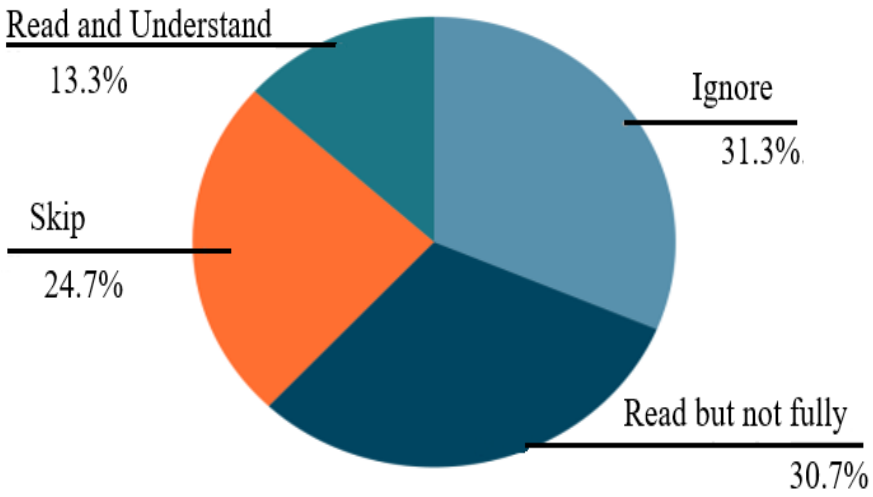
Humans and the new privacy: As a new type of privacy rises, adapting to it is a must, and each age group adapts to it differently; a study done on TikTok users showed that younger users are less concerned regarding privacy and risk than the older users [7]. A survey done in the UAE on 150 people recorded the observation in the tables below [8] (Figure 1).

Figure 1. level of shared data security. **Note:** Not aware-19.3%; Not concerned-22.7%; Aware-58.0%.



Social networks and privacy policies: Social media networks are a business and operate as such, and every business main goal is to increase revenue, but what happens when the main source of revenue is the amount of time people spend on the app or the amount of original content or post shares, does increasing the amount of privacy for individuals, help the business to flourish (Figure 2). In 30 popular SMN the average length of terms and conditions was 3850 words and the individual needed a level of reading comparable to a junior at the university, also the SMN tries to hide the privacy terms by using click-wraps, thus creating barriers for the users to understand their rights and that is because of legislation existing which require the SMN to have privacy policy but not require it to be easy to be understood by the users [9].

Figure 2. Privacy and ethical policy on social media sites. **Note:** Read and Understand-13.3%; Skip-24.7%;)Read but not fully-30.7%; Ignore-31.3%.



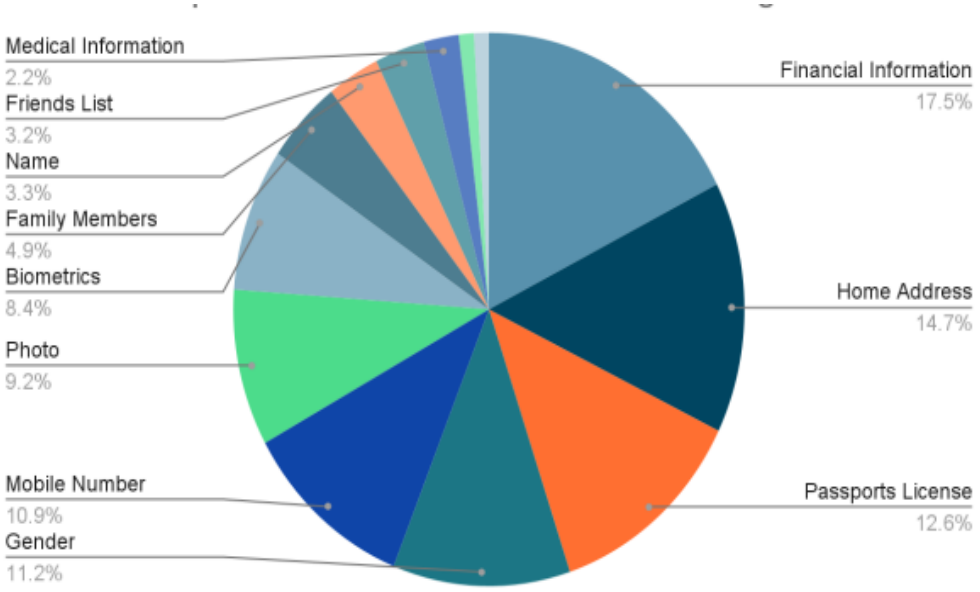
Oversharing

Defining oversharing: The act of disclosing too much personal information to others is called oversharing, and in SMN oversharing refers to the same act [10]. The only difference is that the act is done online, Oversharing can put the person at the risk of cyberbullying or stalking, which puts oneself safety at danger. performing this act might

have a negative effect on relationships development where a line needs to be drawn between self-disclosure and oversharing depending on the receiving party for the information was it a stranger or a partner [11].

Issues of oversharing: In a research utilizing three different evaluation methods - the brief symptom inventory scale, the brief histrionic personality scale, and the Bergen social media addiction scale - the relationship between anxiety, attention-seeking, and social media dependency was assessed. The study involved 352 participants, of which 270 were female and 82 were male. The goal was to explore the connection between excessive sharing of personal information, anxiety, and attention-seeking. The findings suggested that cultural stereotypes, which inhibit face-to-face sharing amongst boys in certain regions, often lead to an increased reliance on social media as an outlet for expression. Conversely, in other regions, it was more common for girls to excessively share information online. Furthermore, a notable correlation was discovered between attention-seeking behavior and oversharing. [12] (Figure 3). Parents usually tend to overshare all kind of pictures and content on SMN, forgetting the right or need of privacy of their children and that might cause direct or indirect harm to their offspring's such as psychological damages when parent post embarrassing photos to the child, or exposing the child to online predators [13].

Figure 3. Personal information is important according to users. **Note:** Financial information-17.5%; Home address-14.7%; Passports license-12.6%; Gender-11.2%; Mobile number-10.9%; Photo-9.2%; Biometrics-8.4%; Family members-4.9%; Name-3.3%; Friends list-3.2%; Medical information-2.2%.



Protective laws

Governments and organizations around the world started to recognize the new privacy and could see the damage that it can cause without proper regulation of it. A report in 2014 showed that the downtime that was caused by data loss, made businesses lose over 1.7 trillion US dollars, another report in 2016 showed that personal data breaches increased by 24%.

Many countries started to establish new regulations and laws to prevent or minimize such losses, but laws that tries to regulate new concepts need revision and considerations of different factors, the General Data Protection Regulation (GDPR) and Estonian Personal Data Protection Act (EPDPA) used to allow people to take pictures without consent of the people in the photograph and needs the consent in case of disclosure, as such in a case where a

man filmed a 14 years old girl nude, the Sweden court ruled that the man was not guilty because the law didn't forbid the act of not having consent to film at the time. EU and international laws try to set laws to protect the right to privacy including children, but no law forbids the parents from sharing their child data as they should have the best interest in mind for their child [13].

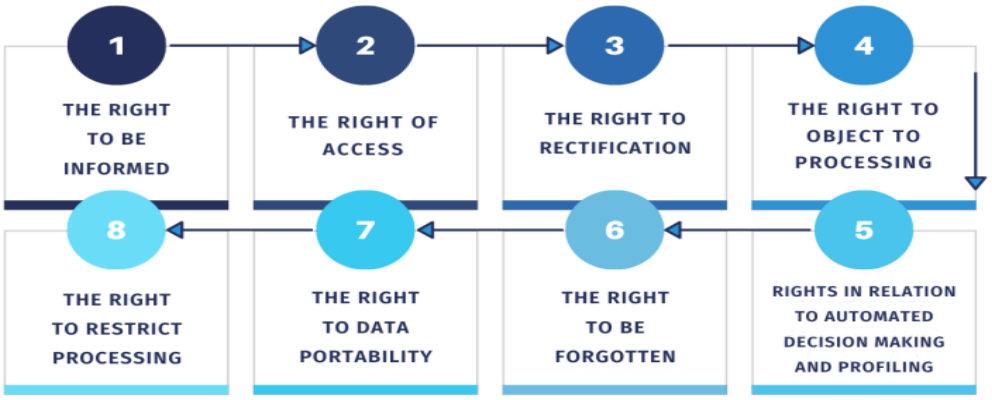
European law: General Data Protection Regulation (GDPR) privacy as a right was established and stated as "Everyone has the right to respect for his private and family life, his home and his correspondence" in the European Convention of human Rights which was a long time before the formation of the EU. As the internet started spreading, the EU saw the need for new privacy protection laws, and in 1995 the Data Protection Directive was passed, but the growth rate of the internet was fast and in 2011 the data protection authority announced the need for a more detailed law on data protection, and since then the work on a new law has taken place, where in 2016 the GDPR law passed the European parliament and in 2018 all entities were obligated to follow it. This law is applicable to all companies that process data of individuals located in the EU even if the company is in a different country. The data protection principles which the GDPR stands on are listed in the diagram below (Figure 4).

Figure 4. Principles of the GDPR. **Note:** ( )Lawfulness, fairness and transparency;( )Purpose Limitation;( )Data minimization;( )Accuracy;( )Storage limitation;( )Integrity and confidentiality; ( )Accountability.

The law made rules on taking consent from users to be more strict, one of the main points on it was to be distinguishable clearly from the other matters and also the content must be in understandable form and uses clear language, the user also can revoke a consent he gave previously and this must be respected also an important rule was that an evidence of consent must be kept [14]. European law provides its citizens with a set of rights that the companies handling their data need to understand and respect these rights (Figure 5).

GDPR is a type of law that can operate outside the country of origin (extraterritorial) where if a company is trying to process data of EU citizens this law will still be applied on it, and consciousness will be severe if they failed to comply with it, the max fine in the GDPR is 20 million euros or 4% of the company yearly revenue whichever is higher.

Figure 5. The General Data Protection Regulation (GDPR) user rights.



USA data protection laws: At the time of writing this article there was no one comprehensive law that protect personal data in the United States of America, but a collection of laws on different levels that protect personal data such as the federal level laws:

- The Electronic Communications Privacy Act (ECPA)
- The Health Insurance Portability and Accountability Act (HIPAA)
- The Fair Credit Reporting Act (FCRA)
- The Children's Online Privacy Protection Act (COPPA)
- The Gramm-Leach-Bliley Act (GLBA)

Numerous states have enacted their specific protective legislation, such as the Consumer Data Protection Act (CDPA) in Virginia or the California Consumer Privacy Act (CCPA). These laws share similarities with the GDPR, and when combined, they collectively provide the necessary protection for personal data.

Chinese law: Prior to 2020, China adopted a model similar to the United States where multiple specific laws existed for the safeguarding of personal data. However, in 2021, China enacted the Personal Information Protection Law (PIPL) [15] aligning its approach more closely with that of Europe's GDPR, with which it shares many parallels as well as some distinct disparities [16]:

1. The legal basis of data processing.
2. The scope of operation (where does the company operate).
3. The definition of sensitive personal information has a wider range than the GDPR.
4. The punishment in PIPL can reach suspension from accessing some IT systems.
5. The liability of the person in charge of personal data protection.

Privacy regulations in the Middle East (Gulf region): The evolution of data protection legislation in Gulf nations bears notable similarity to the trajectory witnessed in Chinese law. What began as a compilation of various laws aimed at safeguarding personal data eventually transformed into a more comprehensive legal framework. Interestingly, the existing data protection law in these regions closely mirrors the European model. This is due to the GDPR being perceived as the gold standard in personal data protection, inspiring Gulf legislators to reach similar objectives

while concurrently acknowledging their countries' unique cultural and geographical contexts. Table 1 below presents a comparative analysis of personal data protection legislation in Gulf countries:

Table 1. Comparison of the Gulf countries' data protection laws.

Country	Scope	Penalties	Data subject rights	Basis of data processing	Cross-border data transfer
Bahrain	Covers processing of individuals data by natural and legal persons in Bahrain.	Fines of up to BHD 20,000 ($53,000) and imprisonment for serious offenses.	Access, correct, and delete individual data, as well as the data portability and object to processing.	Consent, performance of a contract, compliance with a lawful commitments, or protection of critical interests.	Permitted with appropriate safeguards.
Kuwait	Applies to processing of individuals data in Kuwait by data controllers and processors.	Fines of up to KWD 20,000 ($66,000) and imprisonment for serious offenses.	Access and correct individuals data, as well as the right to object to processing.	Consent, performance of a contract, or compliance with a lawful commitments.	Permitted with consent or if the recipient is subject to similar data protection standards.
Oman-2022	Applies to processing of individuals data by controllers and processors in Oman, including those operating outside Oman if the processing relates to goods or services offered to individuals in Oman.	Fines of up to OMR 500,000 ($1.3 million) and imprisonment for serious offenses.	Access, correct, and delete individual data, as well as the data portability and object to processing.	Consent, performance of a contract, compliance with a lawful commitments, or protection of critical interests.	Permitted with consent or if the recipient is subject to similar data protection standards.
Qatar	Applies to processing of individuals data in Qatar by data controllers and processors.	Fines and imprisonment for non-compliance.	Access, correct, and delete individual data, as well as the data portability and object to processing.	Consent, performance of a contract, Compliance with a lawful commitments, or protection of critical interests.	Permitted with consent or if the recipient is subject to similar data protection standards.
Saudi Arabia	Applies to processing of individuals data in Saudi Arabia by data controllers and processors.	Fines of up to SAR 5 million ($1.3 million) and imprisonment for serious offenses.	Access, correct, and delete individual data, as well as the data portability and object to processing.	Consent, performance of a contract, Compliance with a lawful commitments, or protection of critical interests.	Permitted with consent or if the recipient is subject to similar data protection standards.
UAE	Applies to processing of individuals data in the UAE by data controllers and processors.	Fines of up to AED 50 million ($13.6 million) and imprisonment for serious offenses.	Access, correct, and delete individual data, as well as the data portability and object to processing.	Consent, performance of a contract, Compliance with a lawful commitments, or protection of critical interests.	Permitted with consent or if the recipient is subject to similar data protection standards.

RESULTS AND DISCUSSION

User education on privacy

Research suggests that by providing privacy education, we can heighten user understanding of privacy concerns, thereby encouraging more informed and privacy-conscious actions. Thus, it's imperative that governments, communities, and organizations invest in initiatives that aim to enlighten individuals about the importance of information privacy and the potential risks associated with technology usage.

Homomorphic encryption

Social media networks rely heavily on data analysis for efficient user segmentation and categorization. A revolutionary concept known as Homomorphic encryption, as outlined in an academic paper, allows the scrutiny of encrypted information without the necessity for prior decryption. This makes it possible to conduct predictive analysis and user categorization without revealing the real data. For example, given the encrypted values 20, 16, 12 transformed into 7h3732j, 236hy77e, 27636h663, the inspection is performed only on the obfuscated data, and the yielded result remains shielded until a decryption key is applied [17].

Decentralized analysis

The heart of the financial and content tactics of social media platforms lies in the extraction and scrutiny of data. A modern methodology that upholds user privacy involves keeping the raw data on the users' gadgets and conducting on-site analysis. The refined data, which cannot be deciphered easily, is subsequently transmitted to the server, guaranteeing limited vulnerability. Extra security measures might include the implementation of K-anonymity and differential privacy. These measures sever the link between the data and the user, and introduce irregularity to the data, respectively [19-25].

CONCLUSION

The research attempts to find a proper definition for privacy in social media and finds the difference between the concept of privacy in human life and the concept of privacy in social media. Exploring the literature on privacy in social media networks showed that companies try to exploit users for their own gains, proper laws and legislation are needed for limiting these companies' exploitation of personal data and enforcing them to handle data with more care and transparency. The research endeavors to find methodologies to have better privacy for individuals.

REFERENCES

1. Milgram S. The small world problem. Psychology Today. 1967; 1:60-67.
2. Backstrom L. Three and a half degrees of separation. Facebook Research. 2016.
3. Susanne Barth, et al. The privacy paradox – investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. Telemat Inform. 2017;34: 1038-1058.
4. Privacy noun -Definition, pictures, pronunciation and usage notes. Oxford Advanced Learner's Dictionary at Oxford Learners Dictionaries.com.
5. Trepte. The social media privacy model: privacy and communication in the light of social media affordances. Communication Theory. 2020; 31: 549–570.
6. Dowding, et al. Privacy: defending an illusion. 2011.
7. Zhu X, et al. Mechanism of platform interaction on social media users' intention to disclose privacy: a case study of tiktok app. Information. 2022; 13:461.

8. Abdul R, et al. Social media and privacy in the united arab emirates: field research. J Humanit Soc Sci. 2022;19: 569–604.
9. Johnathan Y. Deliberately confusing language in terms of service and privacy policy agreements. Inf Syst. 2022; 23: 138-149.
10. Oversharing noun -Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com.
11. Berman JW, et al. Oversharing and relationship development: how much sharing is too much? Communication monographs. 2011; 78:202-217.
12. Shabahang R, et al. Oversharing on social media: anxiety, attention-seeking, and social media addiction predict the breadth and depth of sharing. Psychol Rep. 2022;22;332941221122861.
13. Iskül A, et al. Child right to privacy and social media – personal information oversharing parents. Balt J Law Politics. 2021; 14: 101–122.
14. Briefing C. PIPL vs GDPR -key differences and implications for compliance in china. China Briefing News. 2022.
15. Personal information protection law of the people's republic of china.
16. Authority PDP. The law | | kingdom of bahrain.
17. Mshangi M, et al. Enhancing privacy in social networks systems using homomorphic cryptographic techniques in ubiquitous computing environment. IEEE. 2018; 9-11.
18. Datta, et al. Decentralized online social networks. Handbook of Social Network Technologies and Applications. 2010;349–378.
19. Royal decree 6/2022 promulgating the personal data protection laW .2022. Official Gazette 1429.
20. Wolford B. What is GDPR, the EU's new data protection law? GDPR.eu. 2022.
21. Data protection laws -The official portal of the UAE government.
22. Privacy and data protection in the kingdom of Saudi Arabia.
23. MOTC releases guidelines on personal data privacy protection law.
24. Communication & information technology regulatory authority home.
25. What are 8 data subject rights according to the gdpr.data privacy manager.