Migration Letters

Volume: 21, No: 4, pp. 726-737

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)
www.migrationletters.com

Compliance of Saudi Arabian Personal Data Protection Law 2021 to Islamic Principles of Privacy

Jawahitha Sarabdeen[1], Mohamed Mazahir Ishak[2]

Abstract

Right to privacy is considered as an important principle for human dignity under Islamic law and other legal system. Various Quranic verses and Hadiths emphasize the importance of right to privacy. From the general principles of the Quranic verses and Hadiths, it is possible to extend to cover various types of privacy that have been discussed under the modern privacy law. Saudi Arabia in 2021 passed a comprehensive legislation on Personal Data Protection to complement the existing privacy legal framework. The main objective of this article is to analyses the Islamic privacy law and the Saudi Personal Data Protection Law 2021 to see the compliance of the Personal Data Protection Law 2021 to Islamic privacy principles. The finding suggests that the Saudi legislature by applying the public interest principle has enacted Personal Data Protection Law 2021 that provides a comprehensive data protection regime, and it follows Islamic Law.

Keywords: *Privacy; Human Right; Data Protection Law; Compliance; Islamic Law; Saudi Arabia.*

1. Introduction

Privacy is considered as one of the fundamental rights under the Universal Declaration of Human Rights (Article 12) and the European Convention on Human Rights 1950, (Article 8). The Convention states that the right to private and family life should be protected along with his residence and correspondence. Any breach of right to privacy will be considered as a violation to the Universal Declaration and European Convention. The countries which are not signatories to the Declaration and/or Convention are expected to protect the right to privacy as a best practice in the era of interconnected trades and businesses. Ensuring protection of privacy along with other rights will help the countries to achieve the United Nation's Sustainable Development Goal (SDG)16 which spells out the necessity of peace, access to justice and strong institutions. The literature in defining right to privacy has followed different theoretical dimensions. Those who followed the social theory defined privacy as something private matter and should be kept so for better protection (Dutta & McCrohan, 2002; Allen, 1988; Bok, 1983). Those who considered privacy as individual right, defined privacy as information that the owner has the right to control and manage it as he wishes (Westin, 2003; Decrew, 1989). Others defined privacy as right and interest, it stated that privacy grands an interest to restrict the access and observation of oneself irrespective of the purpose and consequences of those access and observation (Reiman, 1976). From the literature it could be derived that

[1] Prince Sultan University, Saudi Arabia
[2] Prince Sultan University, Saudi Arabia

privacy should be treated as integral part of human life and self esteem and it should be respected to create value to the individual and society (Eloff & Von Solms, 2000).

Islamic law is also unequivocal on the recognition of privacy as part of self-esteem and important aspect of human dignity. Though there are no special terminologies of "privacy" exist under the Islamic law, the terms like Hifz as-Sir, Hijab, 'Awrah, Mahjurah, and Hima (Mohamed Mazahir, 2008) can be used to infer various types of privacy. In protecting privacy, the Quran clearly mentions the requirement of getting consent before entering a dwelling (Al Quran, An-Nur 27). The consent to enter is a requirement that is applicable to adults and children who attained the age of puberty (Al Quran, An-Nur: 59). This Quranic verse could cover not only private home but also business premises. In term of data privacy, there is a clear warning against collection of information about others, spying and speaking ill about others. It is also advised to avoid being suspicious about others (Al Quran, Al-Hujurat: 12). The content of the above Quranic verse shows that protection of physical space and data related to person and business is necessary and there should not be any misuse of the data. Abuse of data could cause dissatisfaction and misunderstanding among members of family and society. Hence, the Islamic law made it very clear on the need to uphold privacy that could include physical, information and other privacy.

The Prophetic (P.B.U.H.) saying and action are also a manifestation on the protection of privacy and data protection. The Prophet (P.B.U.H.) in emphasizing data privacy mentioned that the "the most wicked among the people in the eye of Allah on the Day of judgment is the men who goes to his wife, and she comes to him, and then he divulges her secret" (Muslim, Hadith No.1437a, ND). This Prophetic saying clearly indicates that protecting personal information of his family and others will be measured to decide an individual Muslim's status in the Hereafter. In protecting the privacy, the Prophet Muhammad (P.B.U.H.) was even reluctant to take a man's confession of adultery citing the Quranic verse "it is not for us to speak of it" (Surah An-Nur: 11-17). Though this Quranic verse was revealed mainly to protect the dignity of women from slander, and it could also be used to protect privacy (Kamali, 1997).

The Quranic verses and the Sunnah of the Prophet (P.B.U.H) could be taken as an authority to respect different types of privacy. Additionally, the emphasis on sanctity and security of life could mean that privacy of the individuals should be respected to achieve sanctity and security of life. Respecting privacy is also in line with achieving dignity of human life. In this context, the Quran in Surah al-Isra, states that "dignity is bestowed on the progeny of Adam… and conferred on them special favours above a great part of our creation" (Al Quran, al-Isra: 70). Accordingly, dignity for all human beings is highly regarded without any limitation. In explaining human dignity, Kamali (2006) mentions that humanity in general irrespective of race, religion and level of piety are given nobility and dignity. While addressing dignity, Prophet Mohammed (P.B.U.H.) turning his face to the Ka'bah, said the sanctity and honour of a believer, his life and his property, is far greater than honor given to Ka'bah in the eyes of God (Ibn Majah, Hadith No. 3932, ND). These are the express indications that recognition of rights to privacy is fundamental of human dignity which is highly valued in Islam. According to A'l Maududi (1981) Islamic fundamental rights are universal, and it recognizes different types of right that could be applied to Muslims and non-Muslims. Similarly, Galwash (1940) reiterates the fact that equality in the application of human rights is a distinct part of Islamic principles of law. Islamic principles of privacy could be applied to all types of privacy in all types of situations. It could also be extended to cover the privacy issues caused by the application of information technology.

Currently, among the types of privacy, the data privacy attracted attention of many legislators in the world. The European Union amended and adopted the General Data Protection Regulation (GDPR) in 2018 to ensure data privacy and it required all the member countries to adopt the GDPR 2018. One of the important provisions that has

implication to the rest of the world is Article 44 which only allows the data transfer from European Union member countries to a third country if the third country has similar protection like EU member countries (Meskic, Z, et al., 2021). This provision and the urge to protect local community and businesses, many non-European countries passed data protection laws like GDPR 2018. Following the need and the trend, Saudi Arabia passed the Personal Data Protection Law 2021 to provide comprehensive framework for data protection in the technology driven era. The Personal Data Protection Law 2021was implemented by Royal Decree M/19 of 9/2/1443H (16 September 2021)

Hence the objective of this article is two folds. Firstly, the article will analyze the new Saudi Arabian Personal Data Protection Law 2021. Secondly, it will compare the Saudi Personal Data Protection Law 2021 with the Islamic principles of privacy to see if the Principles in Personal Data Protection Law 2021 follow the Islamic principles of privacy. Since modern legal system and Islamic law consider privacy as one of the important rights to human dignity and accomplishment of life, this article will be able to shed light on the comparability and compatibility of Islamic principles to protect data privacy. It will also show if the Saudi Personal Data Protection Law 2021 follows Islamic principles of privacy. A comparative study with religious principles and the modern legislative principles on data protection is new and there is a dearth of literature in this context. Therefore, this article will fill the gap by showing that Islamic privacy principles could be used to protect modern privacy concerns including concerns related to data privacy and the Personal Data Protection Law 2021 follows Islamic privacy principles.

The contents of the article are arranged as follows: Section 1 provides an introduction with objectives of the study. Section 2 elaborates on the methodology while section 3 looks at literature on privacy in Islamic law. Section 4 discusses the Saudi Arabian Personal Data Protection Law 2021. A discussion on compliance of the Personal Data Protection Law 2021 with Islamic privacy principles is included in section 5 followed by a conclusion, challenges, and limitation of study in section 6.

2. Methodology

The research used a systematic literature review (SLR) to identify, collect and analyse laws, regulations and literature in the subject matter and used a comparative method to analyse the privacy principle in Islam in comparison with Saudi Personal Data Protection Law 2021.The SLR method is used in this research as researchers would like to assess the existing literature and laws in data privacy under the Islamic and Saudi Law. In the use of SLR, the researchers followed the planning stage that involved understanding the motive of the research and devised an appropriate research plan to review literature to achieve the research objective. In the next stage, relevant literature was collected following the research plan. In the final stage of reporting, the researchers mapped and analysed the literature and reported the finding (Teixeira et al, 2019; Kitchenham, 2004; Webster & Watson 2002).

In collecting the literature, the researchers used popular data bases like Google Scholar, ScienceDirect, IEEEXplore, and Scopus using keywords like “privacy” “Privacy and Islamic Law”, “Data Protection” “Saudi Data Protection law 2021”, “Compliance and data privacy”. Moreover, data were collected from classical documents, websites, and news reports. Once the literature was collected, the abstract was screened to see the relevancy. If they were found to be relevant, they were short listed and were set for analysing. The authors looked at all the relevant concepts, principles, and themes before analysing so that proper mapping of literature with the principles and concepts could be conducted. The comparative analysis method was also used to compare the Islamic law on privacy and the Saudi Arabian Personal Data Protection Law 2021. The main purpose of the comparison was to see if the Personal Data Protection Law 2021 complies with the Islamic law. The comparative analysis could also show the level of compliance, and this

could help to recommend actions to be implemented if there are any non-compliance issues.

3. Privacy under Islamic Law

Islamic law insists on consent requirement and imposes a mandatory requirement of seeking consent before entering others' dwelling (Al Quran, An-Nur: 27). This instruction helps to maintain a certain self-respect and privacy of the occupant and the owner. There is also prohibition in reading others' letters. This prohibition could be extended to access others' data without consent or authorization. From the forgoing, any kind of surveillance or interception should only be installed with consent or proper notice. Any violation of privacy is considered serious even though the violator is a government entity. Prophet Mohammed (P.B.U.H) once stated that "When a ruler seeks to make imputations against the people, he corrupts them" (Abi Dawud, Hadith No. 4889, ND). If a ruler searches for causes of dissatisfaction, he will spoil them. This shows that unnecessary searches should be avoided as it is a violation of fundamental human rights and could instill tension and unrest within the public at large. Moreover, Islam states that one's duty to God includes the duty to members of the society and society itself. As such the Islamic states are obliged to protect the rights of individual (Hussain, 1997). Protection of privacy is the obligation of individuals and the state. The state should take all measures to ensure that privacy is protected, and any unnecessary violations are avoided. The prominence of individual rights under Islam could be seen when it is stated that violation of human rights could only be mitigated if the victim can forgive the violation. It shows that Allah who bestowed the right, gives up His authority to forgive and left the right to forgiveness to the victim to decide. Accordingly, the state cannot be a violator but should be a protector of the rights and it should penalize the violation according to the law (Hussain, 1997).

The Prophet (P.B.U.H) stated that one should control his gaze while waiting for permission to enter a premise, he mentioned that if your eyes have entered means, the person already entered without permission. Regarding private group meeting, it was reported that Prophet (P.B.U.H) stated to the effect that the confidentiality of the meeting should be maintained by all the attendees and any disclosure should lead to mistrust (Abi Dawud, Hadith No. 4869, ND). Thus, any kind of eavesdropping should be avoided. It is also good to note that protecting privacy is more important than penalizing certain sinful activities. It could be derived from the Prophetic saying that Muslims should not dishonor another by revealing the secret of one's disgraceful act (Sahih Muslim, 1988). This implies that some sort of crime investigation could be dropped if it violates personal privacy. From the verses of Quran and the Sunnah of the Prophet, it could be deducted that every one's privacy should be respected, the extent of privacy recognition could be dependent on the nature of the information, time of observation and the amount of information collected. There could be possibility of joint liability of keeping information confidential. When information is disclosed for certain purposes, that information should be kept confidential too. It could be seen that it is discouraged to investigate the secret of others and any violation of privacy should be punishable (Mohamed Mazahir, 2018).

The high regard for privacy in Islam could be seen in evidential requirement too. For instance, in proving adultery, there is a need to four witnesses who have seen the commission of the crime. This requirement is very difficult to meet while there is a clear deterrence from violating the privacy of others. Consequently, the case could be dropped and those who falsely accused someone of a crime could be prosecuted for slander. Additionally, there is a tendency of not accepting the evidence of witnesses who are in fiduciary relationship with the accused. This is mainly done to protect unnecessary revelation of private matters to which the witness is acquainted with. When an accused confessed of his crime in private to someone of his crime and the accused requested to

keep it confidential, the matter should be kept confidential. Some of the Hanafi school of law scholars supported maintaining confidentiality and not accepting confession in breach of confidentiality or privacy principles (Ahamed, 2009). Though the Prophet (P.B.U.H) discouraged from confessing or reporting wrongdoing in violation of privacy (Al Bukhari, ND), it should not be construed to say that one can commit as many crimes as possible without being caught by law. The main take from this narration is to advise to stay away from unnecessary interference of baseless violation of one's privacy, however, once the crime is reported the Prophet (P.B.U.H) insisted on prosecuting the criminal. Since the recognition and protection of right to privacy is a precursor for the perfection of life and honor, Islam considered that mandatory protection of privacy rights is warranted. The protection necessitates passing of appropriate laws that should prescribe sanctions for violations. Any legislative initiatives on this respect shall be respected by Muslims and even in the absence of legislative framework, respecting privacy of others becomes compulsory on each Muslim.

The concept of Maqasid al-Shari'ah (Objectives of Shariah) could be considered in passing appropriate law to regulate privacy. There are clear indications in Quran and Sunnah that Allah does not inflict hardship on you (Al Quran, Al-Maidah: 6) and the Prophet (P.B.U.H) has been sent but a mercy to the universe (Al Quran, Al-Anbiya: 107). It can be said that the underlying theme of the above-mentioned Qur'anic verses is to create ease and benefit (maslahah). By considering the objectives of Shariah, during Prophet Muhammad (P.B.U.H) and Caliph 'Umar bin al Khattab many rules were issued based on the concept of Maslahah. Following the footprint, it is possible to have comprehensive legislation on current issue related to privacy or data protection.

Maqasid al-Shari'ah is classified into three categories: essential (maslahah daruriyyah), the complementary benefits (maslahah hajiyyah), and the embellishment (maslahah tahsiniyyah). The essential maslahah covers essentials of human being like faith life, property etc. Protections of essentials are important for orderly life and faith, any disturbance to it is prohibited (Kamali, 2002). Right to privacy is one of the essentials for decent and dignified human life, protecting it also falls with the ambit of essential. Complementary maslahah is not an independent category, and it is used to remove severity and hardship of life so that life could be normalized. To apply this, it should be shown that the use of this principle will help to prevent evil, as Islam emphasizes prevention of harm or evil. Ensuring privacy protection or passing laws for this purpose could also falls within this category, as they could prevent harm that could cause due to violation of privacy or personal data (Mohamed Mazahir, 2008). The Maslahah under tahsiniyyah is used to obtain desirability to achieve perfection in conduct or life. For achieving this, Islamic law, for instance, encourages cleanness, good manners etc. Similarly, the judiciary and the executives are encouraged not to be too eager in enforcing penalties if there are other alternatives available (Kamali, 2002). Applying this to the protection of data or privacy, it is desirable on everyone to respect privacy and any undue intrusion should be avoided so that perfection in life could be achieved. As privacy is considered as one of the essentials for human life in Islam, passing laws and educating people in protecting and promoting privacy is part of Islamic law. In fact, the government in Islam is entrusted to pass appropriate law for the protection under any of the Maslahah principles.

4. The Saudi Arabian Personal Data Protection Law 2021 (Decree M/19)

The passing of Personal Data Protection Law 2021 is an important milestone in personal data protection of living and identifiable individuals in Saudi Arabia. The law protects personal data and whoever, collects, processes, stores, or transferring personal data, shall follow the data principles set in the Personal Data Protection Law 2021. The law requires that the data subject must be informed of the purpose of data collections, the type of data

to be collected and their data collector's detail along with the information about the limitation of its use. If the data are to be transferred to a third party for the similar purpose for which the data initially collected, it should also be disclosed so that the data subject could make an informed decision concerning his data. The law provides various rights to data subjects besides right to consent. They have the right of access to the data and understand the data processing procedures and protocols. They can also ask for the actual data and the purpose for which the data is being used. If they decided to withdraw their consent, it is also possible, and they can request for the erasure of data, and exercise right to be forgotten. If these rights are exercised, the data controller must stop using the data and completely erase the data from the system. Right to restrict processing is another right granted to the data subject. The data subject as a person has a say in the processing of their data, they can restrict the use of their data for certain processes, or they also can request stop further processing of data. Right to be informed is incorporated under the law along with right to rectification. The right to rectification is an important right to ensure that the data are accurate, and any decision based on the data does not affect the interest of the data subject. The data subject is granted right to object to process their data if the processing is going to cause injury to the interest of the data subject. For instance, if the data are going to be used for mass marketing or monitor consumer behaviour, then the customer will have an absolute right to object processing of data. Right to data portability allows the data subject to move data from one system to another system if the condition for the portability is met. Various rights given to a data subjects show that in the data protection framework, the data subject has the control over his data and will exercise many rights to ensure control of his data (Albakjaji, et, al, 2020; Al-Abdullah, et, al, 2020; Sullivan & Burger, 2017).

Besides various rights, the Personal Data Protection Law 2021 encompasses widely acceptable data principles that includes accountability, transparency, consent, data quality, data access, use and other related data protection principles. The Accountability principle requires that data controller is to be responsible in soliciting consent for the data collection and management of the data. This principle will also require appropriate measure to be in place for internal and external use of the data that are collected following data collection principles. In the event of any violation, the measures to rectify should also be elaborated. There should be periodical review of the privacy management system. The review should assess the suitability of measures taken in protecting data by considering the nature of the data, context, purposes of data collection, the risk involved and the rights of various parties. Review should also investigate the disaster management steps to evaluate feasibility of these measures so that action could be taken and implemented in case of any violation of data (Lichtenthaler, 2021, Sarabdeen, 2022; Sarabdeen et al, 2022).

Data principle relating to transparency will require disclosure of sufficient information about the purpose of data collection, detail of the data collector, storage measures and subsequent use of the data. Additionally, contact details of the users and third party who may access to data should also be disclosed under this principle. Data collected for one purpose should not be utilized for other non-disclosed purpose unless authorized to do so. If a third party is involved in handing data, there is a need to ink a detailed agreement about the responsibilities, accountability, and transparency issues along with other issues on security protocols, encryption and security measures (Georgiopoulou, et al. 2020; Guerbouj, et al, 2019; Feltus, 2019).

Choice and Consent principle gives the choice to opt out from data collection and if the data subjects' data are to be included, it is necessary to get informed consent. In order to satisfy the requirement of informed consent, the data controller has to disclose the purpose of data collection. If consent is given for a particular purpose, sticking to the purpose is required. However, if the data collected is for national safety, security and public health or related justifiable purposes, the consent requirement could become

irrelevant. If the consent is withdrawn, the record should reflect the withdrawal even though the withdrawal shall not affect the prior decisions based on consent. To have robust system about consent, it may be advisable to have consent management system so that consent information, request for alteration and revocation of consent could be kept up-to date. The consent management system should include the requirement for parental or guardian consent if the children information is processed (Georgiopoulou, et al, 2020).

Limiting data collection is encouraged under the Personal Data Protection Law 2021. This principle which is known as minimalization principle requires the data controller to collect data for specific purpose and no excessive data should be collected for future purpose. It ensures that unnecessary data for anticipated future use are not to be collected in advance and the data controller is accountable for the data collected, the ways they are collected, and the safeguards taken to protect the data. The data minimalization principle also will require that the data is adequate, relevant, and limited the purpose for which the data was collected (European Commission, 2016). The minimalization principle is linked to use, retention, and destruction principle. This principle will place an obligation on the data controller to use the data to the agreed purposes only and any other unrelated use will trigger a new consent requirement. Additionally, the collected data are to be retained for period that is reasonable to achieve the collected purpose. Though there is no specific mention of length of retention of data, the retention of data should be directly linked to the purpose. In processing data, the data controller must conduct Data Protection Impact Assessment (DPIA) if the processing will create a high risk to the rights of data subject. In case of high risk, it is required to consult relevant authority before processing the data (European Commission, 2016). Appointment of a data protection officer will help in conducting DPA and coordinating action with various stakeholders. Besides these obligations, organizations should also designate a qualified Data Protection Officer (DPO), who should monitor compliance with law and act as a point of contact between the organization and supervisory authorities. Once the data is used, it should be destroyed without impacting the data subject. This will require appropriate organizational measures to ensure that the data destroyed are not accessible to anyone. Different types of data might require different type of measures, for example sensitive data related to financial, banking, health, religious and related matters should be destroyed carefully so that no one will be able to reverse the process to get access to original data. A special eraser software could be deployed that should make retrieval of erased document to be impossible (Barber, 2018). The problem with some technologies like blockchain is that once a transaction is recorded, it cannot be deleted (Halamka & Ekblaw, 2017). In these circumstances, the possible solution to meet the requirement of law is to store the user data off-chain or modify them without affecting the public ledger (Finck, 2018). The other possibility is to provide a supplementary statement to correct or delete any existing data (Al-Abdullah, et al, 2020).

Access to data requires limiting access to data to authorized personals only and any third-party access should be handled according to the law. However, the data subject should be given access to data as well as a decision made based on the data. Moreover, when a decision is taken based on automated processes and there is no human involvement, the data subject should be informed about it, should be given access to original data, output and the decision. They should also be given an opportunity to review and seek modification to the decision. Any review should be done by someone who has the authority to revise the automated decision.

The security principle under the Personal Data Protection Law 2021 requires the data controller and processor to deploy an internationally acceptable standard of security system and measures to protect the user data in addition to a detailed data security plan. The plan should have an appropriate policy to show the responsibility towards data subjects and should include security feature like pseudonymization, encryption authentication and authorization mechanisms to control unauthorised access internally

and externally (Tankard, 2016; Romanou, 2018). Perhaps different types of security features need to be introduced in combination to provide better protection. For instance, blockchain documents can either be encrypted or hashed for security. However, encrypted data can be decrypted and hashed data with additional information could be used to identify data subjects. Since neither encryption nor pseudonymization gives complete security to the data, other technical measures should be implemented to disconnect the link between the data subject and intelligible data (Mourby et al., 2018; Smith et al., 2016; Al-Abdullah, et al, 2020). However, any kind of security measures will not provide total security, the data security plan should include the steps and actions are to be taken in any security breaches to mitigate the damages and to stop future security breaches (O'Brien, 2016).

The Data Quality principle imposes an obligation of the data controller to collect current and accurate data. Any outdated data should be deleted from the system and use of any defective or outdated data could create liability. Monitoring and compliance are another important principle introduced by the Personal Data Protection Law 2021. Successful compliance will require maintaining the record of all data collected and processed. The data controller should adopt Privacy by Design and by Default principles so that all the necessary privacy principles that applied to the organisations' data processing has been captured accurately from beginning to the end of data processing. The organisational technical measures alone will not meet the compliance requirement, it is also necessary to educate the employees to change their mindset of data protection culture (Freitas & Mira da Silva, 2018). There should also be a systemic routine review of monitoring and compliance (Tikkinen-Piri et al., 2018). This should be carried out by categorizing the types of data that the organisation possesses and the application of the law to the data. Once this initial assessment is completed, data management policies and guidelines should be implemented to ensure compliance with the law (Boban, 2018; Gabriela et al., 2018). This will help to identify the flaws, risks, and rectification strategy to achieve compliance (Lopes & Oliveira, 2018). Based on the data management policies, it is possible to implement an audit-alert to check if a particular data falls with the personal data protection regime.

5. Discussion on Compliance of Personal Data Protection Law 2021 to Islamic Concepts of Privacy

The Islamic law recognises privacy as a fundamental principle of human dignity. Special reference could be seen in relation to data privacy when the Quran (Surah Al Hujuraat, verse: 12; Surah An Nour: Verse 27 - 28) and Sunnah prohibit actions like entering without permission, breaching trust or confidentiality, eavesdropping, or accessing others communication. This seems to suggest that the main reason for the prohibition is to protect the secrets held within a house or business entity. Under Islamic law any kind of intrusion be it a mere entry to the home or spying on the occupants is prohibited unless justified. However, it is expected from an occupant that he must take reasonable measures to protect privacy (Almebrad, 2018). On the issue of listening to conversation inside a premise, it is also considered prohibited. The Prophet (P.B.U.H) reported to have said that …whoever eavesdrops then molten lead will be poured into his ears on the Day of Resurrection … (Al-Bukhari, Hadith No, 7042, N.D). The Islamic view of data privacy could be easily applied to any kind of invasive technologies and no technology could be placed in one's home or business without the knowledge of the occupant. Beside the forgoing the prohibition on reading peoples' correspondence will be relevant today as it could be expended to cover personal data, notes, and confidential documents. Those documents containing personal data could not be accessed without explicit permission.

About invasion of privacy in public places, it may be assumed that there is a reasonable expectation of privacy, and the data subject would like to control the data about

themselves. Islamic law of data protection is broader and seeks to encompasses the entire range of protection of personal data or confidential information irrespective of the space where it has taken place. Therefore, collection of data from emerging technologies like Facial Recognition Technology (FRT), GPS, AI must satisfy the requirement of obtaining consent well before the data collection otherwise penal section could be imposed (Neogi,, 2021; Almarzoqi & Albakjaji, 2021). Islamic state has a broader interest in protecting individual and societal well being, it is authorised to pass laws according to five norms: prohibited, obligatory, recommended, disapproved, and neutral. As the law in Muslim countries should provide same level of protection like in any other countries, the Personal Data Protection Law 2021 of Saudi Arabia was passed to elaborate more on protecting the data of identifiable individual in the information era. This law not only follows the Islamic law but also complements the existing Islamic principles on data privacy. Table 1 shows a simple comparison of important data privacy issues available under Islamic law and Data Protection Law 2021.

6. Conclusion, Challenges and Limitation of the Study

Islam considers right to privacy and data protection is crucial to achieve full satisfaction of life, and that respecting privacy in general is considered as a fundamental duty of every individual and the State. The right is broader, and it covers data that are available in public and private spare. The restriction on the right to data privacy is limited in scope and only justifiable if it is necessary to protect greater interest of public or just cause. Any use of technology to snoop is prohibited and the state is obliged to pass law to ensure protection. The Saudi Government following this mandate passed a comprehensive data protection law in 2021 which includes various aspects of data protection rights, responsibility, exceptions to protection, and penalties.

Personal Data Protection Law 2021 is one of the first that has been passed in the region and has the effect of giving an upper hand to data subject in management of his data. Any request of the data subject should be accepted by the data controller unless it is unjustifiable to comply with request or the request will infringe someone else's data privacy. The data controllers are expected to comply with the law by implementing appropriate organization and technical measures. They are expected to invest in internationally accepted technical standards in terms of security, data management, training, and risk assessment. The compliance to the Personal Data Protection Law 2021 is expected to be higher as it is religiously obligatory on every Muslim and their State to respect the privacy of others.

The major challenge in this research, is the availability of latest literature on data privacy on Islamic law. The authors need to find out the traditional literature and extract the general principles related to privacy and data protection. There is also limited research on privacy and data protection in Saudi Arabia. The authors reviewed the literature on privacy and data protection from different parts of the world and try to find the common concepts before analysing the Personal Data Protection Law 2021 of Saudi Arabia.

The limitation of this research is that only the Islamic privacy concepts were analysed and compared with the Personal Data Protection Law 2021 of Saudi Arabia, it did not look at other applicable laws. It also has limitation in term of methodology where this research used the systematic literature review (SLR) to identify, collect and analyse laws, regulations and literature in the subject matter and used a comparative method to analyse the privacy principle in Islam in comparison with Saudi Personal Data Protection Law 2021. The research did not utilise quantitative methods since the research objectives could be achieved by using systemic literature and comparative research method. The future research might look at compliance of other laws to Islamic principles and could also use a survey method to find out the perception of people on compliance.

Conflicts of Interest: The authors declare no conflict of interest.

Acknowledgments: The authors would like to acknowledge the support of Prince Sultan University (PSU) for the research and for paying the Article Processing Charges (APC) of this publication. They would like to record the support provided by the Governance and Policy Research Lab.

References

Abi Dawud, (ND). Sunan Abi Dawud. Retrieved from Retrieved from https://sunnah.com/abudawud.

Ahmad, A.A. (2009). The Right to Privacy. In Islam, Modernity, Violence, and Everyday Life. New York, USA: Palgrave Macmillan.

Albakjaji, M., & Adams, J., Almahmoud, H., & Sharafaldean Al Shishany, A. (2020). The Legal Dilemma in Governing the Privacy Right of E-Commerce Users: Evidence from the USA Context. International Journal of Service Science, Management, Engineering, and Technology, 11(4), 166-187. Retrieved from https://www.igi-global.com/.

Al-Abdullah, M., Alsmadi,I., AlAbdullah, R & Farkas,B. (2020). Designing privacy-friendly data repositories: a framework for a blockchain that follows the GDPR. Digital Policy, Regulation and Governance, 22 (5/6): 389-411.

Al Bukhari, (N.D). Sahih Al-Bukhari. Book 18, Hadith 34. Retrieved from https://www.sahih-bukhari.com/

Allen, A. (1988). Uneasy Access: Privacy for Women in a Free Society. London, UK:Rowman and Littlefield.

Almarzoqi, R. & Albakjaji, M. (2021). The Patentability of AI Invention: The Case of the Kingdom of Saudi Arabia Law, International Journal of Service Science, Management, Engineering, and Technology, 13(1), DOI: 10.4018/IJSSMET.307111

Almebrad, A., (2018). The Sufficiency of Information Privacy Protection in Saudi Arabia. Theses and Dissertations. Retrieved from https://www.repository.law.indiana.edu/etd/56

Barber, N. (2017). The GDPR and its implications on cloud services. Retrieved from https://documents.pub/document/the-gdpr-and-its-implications-on-cloud-may-include-elements-of-saas-iaas-and-paas.html?page=1.

Boban, M. (2018). Protection of personal data and public and private sector provisions in the implementation of the general EU directive on personal data (GDPR). In 27th International Scientific Conference on Economic and Social Development (pp. 161-169). Rome, Italy: ESD Proceeding.

Bok, S. (1983). Secrets: On the Ethics of Concealment and Revelation. New York, USA: Panthcon Books.

Decrew, J. (1989). The scope of privacy in law and ethics. Law and Philosophy, 5(2):145-173.

Dutta, A. & McCowan, K. (2002). Management's role in information security in a cyber economy. California Management Review, 45(1): 67-87.

European Commission (2016). Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (general data protection regulation). Official Journal of the European Union, 59:1-88.

Feltus, C. (2019). Deriving Information System Security and Privacy From Value Cocreation Theory: Case Study in the Financial Sector. International Journal of Service Science, Management, Engineering, and Technology, 10(4), 1–25. doi:10.4018/IJSSMET.2019100101

Finck, M. (2018). Blockchains and data protection in the European Union. European Data Protection Law Review, 4(1):17.

Freitas, M.C. & Mira da Silva, M. (2018). GDPR compliance in SMEs: there is much to be done. Journal of Information Systems Engineering & Management, 34 (4):30.

Gabriela, G., Cerasela, S.E. & Alina, C.A. (2018). The EU general data protection regulation implications for Romanian small and medium-sized enterprises. Ovidius University Annals (EconomicSciences Series), 18(1): 88-91.

Galwash, A.A., (1940). The Religion of Islam. Cairo, Egypt: Al-azhar Magazine

Georgiopoulou,Z., Makri, E & Lambrinoudakis, C. (2020). GDPR compliance: proposed technical and organizational measures for cloud provider. Information & Computer Security, 28(5): 665-680

Guerbouj, S., Gharsellaoui, H., & Bouamama, S. (2019). A Comprehensive Survey on Privacy and Security Issues in Cloud Computing, Internet of Things and Cloud of Things. International Journal of Service Science, Management, Engineering, and Technology, 10(3), 32–44. doi:10.4018/IJSSMET.2019070103

Halamka, J.D. & Ekblaw, A. (2017). The potential for blockchain to transform electronic health records. Harvard Business Review, 3(3): 2-5.

Hussain, S.S. (1997). Human Rights in Islam. New Delhi, India: Kitab Bhavan.

Ibn Majah, (N.D). Sunan Ibn Majah. Retrieved from https://sunnah.com/ibnmajah.

Kamali, M.H. (1997). Freedom of Expression in Islam. Retrieved from http://www.karamah.org/articles_quraishi.htm.

Kamali, M.H. (2002). The Dignity of Man: An Islamic Perspective. Oxford, UK: Islamic Texts Society.

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. Keele University, Keele: Department of Computer Science.

Kumar, K. & Pradhan, P. (2020). Trust Management: Social vs. Digital Identity. International Journal of Service Science, Management, Engineering, and Technology. 11(4). Retrieved from https://orcid.org/0000-0002-6753-1557.

Lichtenthaler, U. (2021). Profiting From Digital Transformation?: Combining Data Management and Artificial Intelligence. International Journal of Service Science, Management, Engineering, and Technology, 12(5), 68–79. doi:10.4018/IJSSMET.2021090105

Lopes, I.M. & Oliveira, P. (2018). Implementation of the general data protection regulation: a survey in health clinics. (pp. 1-6). In 13th Iberian Conference on Information Systems and Technologies. Caceres, Spain: IEEE.

Maududi, S.A.A (1981). Basic Human Rights. in Said Khan, A and Ahmad, K (Trans.). Markfield, UK: Islamic Foundation.

Meskic, Z., Albakjaji, M., Omerovic, E., & Alhussein, H. (2021). Transnational Consumer Protection in E-Commerce: Lessons Learned from the European Union and the United States. International Journal of Service Science, Management, Engineering, and Technology, 13(1). Retrieved from https://www.igi-global.com/

Mohamed Mazahir, M.M. (2008). E-health Personal Data Privacy: A comparative Study of Malaysian Australian Laws. Retrieved from https://studentrepo.iium.edu.my/bitstream/123456789/1493/1/t00011026591MOHAMEDISHAKKPG942.7C65M697E2008_SEC_24.pdf

Mourby, M., Mackey, E., Elliot, M., Gowans, H., Wallace, S.E., Bell, J., Smith, H., Aidinlis, S. & Kaye, J. (2018). Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. Computer Law & Security Review, 34(2): 222-233.

Muslim. (1990). Sahih Muslim, 9. Beirut, Lebanon: Darul-Kutub Al-'Ilmiyah.

Neogi, D. (2021). Combating Cyber Crime: How Can Technology Intervention Supplement Legal Provisioning? International Journal of Service Science, Management, Engineering, and Technology, 12(6), 1–15. doi:10.4018/ IJSSMET.2021110101

O'Brien, R. (2016). Privacy and security: the new European data protection regulation and it's data breach notification requirements. Business Information Review, 33(2): 81-84.

Reiman, J. (1976). Privacy, intimacy, and personhood. Philosophy and Public Affairs, 6(1): 26-44.

Romanou, A. (2018). The necessity of the implementation of privacy by design in sectors where data protection concerns arise. Computer Law & Security Review, 34: 99-110.

Sarabdeen, J. (2022). Protection of the rights of the individual when using facial recognition technology. Heliyon, 8(3):1-11.

Sarabdeen J, Chikhaoui, E, & Mohamed Ishak, M.M. (2022). Creating standards for Canadian health data protection during health emergency – An analysis of privacy regulations and laws. Heliyon, 8:1-9.

Smith, J., Tennison, J., Wells, P., Fawcett, J., & Harrison, S., (2016). Applying blockchain technology in global data infrastructure. Retrieved from https://theodi.org/article/applying-blockchain-technology-in-global-data-infrastructure/. Open Data Institute

Sullivan, C. & Burger, E. (2017). E-residency and blockchain, Computer Law & Security Review, 33(4): 470-481.

Tankard, C. (2016). What the GDPR means for businesses. Network Security, 2016(6):5-8.

Teixeira, A.G., da Silva, M.M. & Pereira, R, (2019). The critical success factors of GDPR implementation: a systematic literature review. Digital Policy, Regulation and Governance, 21(4): 402-418.

Tikkinen-Piri, C., Rohunen, A. & Markkula, J. (2018). EU general data protection regulation: changes and implications for personal data collecting companies. Computer Law & Security Review, 34: 134-153.

Webster, J. & Watson, R.T. (2002). Writing a literature review. MIS Quarterly, 26 (2):13-23.

Westin, A. (2003). Social and political dimension of privacy. Journal of Social Issues, 9(2): 431-453.