The Digital Transformation in the Kingdom of Saudi Arabia

Naif A. Alghamdi

Jeddah, Saudi Arabia

Abstract
The research deals with the concept of digital transformation, digital rights, Saudi Personal Data Protection Regulation (SPDPR), the Egypt' Personal Data Protection Law (EPDPL) No. 151 of 2020, and the European Union (EU) General Data Protection Regulation (GDPR) No. 679/2016. It also draws comparison among them. It shows basic definitions and concepts, the established rights for data subjects, the obligations that fall on controllers and processors, and the penalties for violating the provisions of those regulations.

Keywords:
Digital, transformation, digital rights, Saudi, Data Protection, regulations.

1. Introduction

The law, in turn, always addresses the modern phenomena in society to establish rights and impose obligations through abstract general binding rules to protect rights against violation and abuse, whether by natural or legal persons. There is a phenomenon that resulted from technological and scientific progress in the field of the Internet and the virtual world, which facilitates various aspects of life through the use of platforms, websites and search engines. It motivated governments to transform the services that were carried out within its headquarters to those online platforms, which led to save time, effort and expenses. This is the digital transformation that we are witnessing today.

However, there are risks and damages that natural persons may suffer when using this feature, due to violation of people's privacy and access to their personal data through digital transformation, which exposes them to a lot of harm if anyone can access these data.
Therefore, it was necessary to enact laws and regulations that protect personal data from being violated or misused. Indeed, many countries, which were not interested in this matter before, began to develop systems to protect these data that users place on the Internet to obtain services, against violation or illegal use from the part of the recipient of that data.

Research importance:
The importance of the research lies in protecting personal data as being one of the digital rights resulting from digital transformation. It also shows the role of the law in protecting such data and rights.

Research problem:
It raises the problematic issue of to what extent can legal systems achieve the necessary protection for personal data of natural persons.

Research goals:
The research aims to clarify the rules and provisions set by the Saudi regulator for the protection of personal data provided by public or private, natural or legal persons to the entities they deal with via the Internet. They also intend to point out the effectiveness of these rules in achieving their goals.

Methodology:
The researcher adopted the descriptive and the analytical approach for analyzing laws, and the comparative approach for comparing Saudi regulation and Egyptian law of protecting personal data.

Research plan:
First topic: digital transformation and rights
Second topic: legal framework for protecting users' digital rights in KSA.

First topic: Digital transformations and rights
Essence of digital transformation

Digital transformation means the process of applying digital technologies to accelerate the achievement of business or to use technology to bring about fundamental changes in business and services by using artificial intelligence techniques, items of the virtual world and other advanced technologies. Digital transformation represents a new method of carrying out tasks and services while saving time and effort. This can be achieved by defining the path and using electronic and technological techniques in

Manuscript received September 5, 2022
Manuscript revised September 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.9.63

carrying out various tasks.[1] It is also defined as the use of modern digital technologies, social media, mobile devices, or embedded devices to improve business and customer services, streamline operations, or create new business models.[2] Digital transformation is also defined as making changes in how individuals perceive, think and act at work and seeking to improve work environment by focusing on the use of information and communication technology.[3]
The digital transformation mechanism initially defines the strategic objectives of transformation in order to achieve them. It begins with perceiving labor needs and the drivers of change and ends with digital transformation through the development of an effective strategy to advance human activity through modern technologies.

Thus, digital transformation is based on developing a digital strategy that begins with diagnosing the current situation to determine the current digital capabilities and what they should be in the future. Then, this strategy should be implementing by allocating the necessary resources, following up the implementation process, and continual assessment to update data and develop human resources in line with digital transformation. If this process is carried out correctly, it will help overcoming daily work problems faced by various institutions, such as actual attendance, crowding, and daily routine that affects businesses. Doing so saves effort and time and creates new opportunities for innovation and entrepreneurship. This can be achieved through providing the necessary legal environment to protect the values related to modern technology.[4]
In the field of digital transformation, KSA has done many achievements through a number of highly reliable digital programs and initiatives such as Meras, Etimad, and Absher programs, which linked more than 130 governmental services used by citizens. In the field of digital health, digital transformation is used in transferring to hospitals, smart clinics and telemedicine by using Sehhaty application, which was able to reduce the number of visits and medical consultations through attendance by 50%.
KSA has organized the 2nd edition of the "Hajj Hackathon", which is the largest technical gathering for programmers. This hackathon broke the record and was registered in the Guinness Book of Records as the largest hackathon in the world. It aimed at attracting leading minds in the field of programming to innovate technical solutions that can enrich and improve the experience of pilgrims. Some of these smart applications will be developed and transformed into pioneering projects.[5]

Essence of digital rights

Digital rights are those rights that allow a person to access, use, create and publish digital media, or access and use computers and other electronic devices or communication networks.[6] DW Akademie defines digital rights as human rights applied in the digital sphere that allow him to use the Internet and digital technology freely and in a safe manner. This means that digital rights are an extension to human rights based on the Universal Declaration of Human Rights in 1948, and agree with the contents of the International Covenant on Civil and Tourism Rights issued in 1966. Thus, digital rights are recognized and protected by some international laws and treaties. Moreover, the United Nations and Human Rights Council approved a number of resolutions stating that the same rights that people enjoy in the real world should also be protected in the virtual world.
Others also define it as the rights that enable the person to circulate and use information and data in his environment, and communicate with whomever he desires through various communication networks.[7] Digital rights appeared as a result of the virtual world. The whole world heeded towards modern technologies and digital transformation in communication and various aspects of life to save time and effort and improve the quality of services provided. This resulted in a set of rights for users; the most important of which is the right to digital privacy. It is the protection of personal data published and circulated through digital media including e-mails, bank accounts, personal photos, work information, and all information and data used on the Internet when using a computer, mobile phone or any digital means of communication on the web.
Accordingly, the privacy of telephone, postal and e-mail correspondence and information are persons' rights whether they are installed on computers, or the Internet through private sites or institutions linked to the state or the state

[1] This definition is published on the Federation of Egyptian Banks Portal: febgat.com
[2] Liere – netheler, k., packmohr, svogelsang, k. 2018, Drivers of Digital Transformation in Manufacturing. In: Hawaii international conference on system science, Waikoloa beach, HI PP 3926-3935. It is referred to by Rizq Sa`d Ali, Reflections of Digital Transformation on Contemporary Criminal Policy, Legal and Economic Studies Journal, Faculty of Law, Sadat City University, 2021, p. 11.
[3] Abdul-Rahman Hasan, Reality of Digital Transformation in KSA, Administrative and Financial Sciences Journal, Echahid Hamma Lakhdar University - El Oued, College of Economy and Commerce, 2020, p. 15.
[4] Shahata, Muahmmad Musa. In`ikasat Taf`il Aliyat Al-Tahul Al-Raqamy fi Daw' Mubadarat Al-Shumul Al-Mali `Ala Tatbiqat Al-Hukumah Al-Iliktruniyyah Bigumhuriyat Misr Al-Arabiyyah, Journal of Contemporary Commercial Studies, Issue no. 9, January 2020, p. 204.
[5] Hasan, Abdul-Rahman Hasan. Waqy` Al-Tahuwwl Al-Raqamy Lilmamlakah Al-Arabiyyah Al-Saudiyah, p. 21.
[6] https:// ar.m.wikipedia.org.
[7] Ghitas, Jamal Muhammad. Al-Dimuqratiyyah Al-Raqamiyyah, Nahdat Misr, 2006, p. 40.

institutions themselves. Thus, digital privacy is the right of the individual/user/citizen, the institution, or the group to determine a certain time for this privacy as when, how and to what extent their information can reach others. Moreover, they have the right to control the process of collecting their personal data and how these data are automatically treated, saved and distributed.

In brief, privacy is a person's control of his personal data. Due to importance of digital privacy and the increasing interaction of individuals with the digital world, digital privacy and personal data has become a material that is used commercially in marketing propaganda, monitored by companies, or exposed to theft and exploitation for purposes that may harm data subjects. Dealing with these abuses whether they are practiced by companies or other parties require many directions on how to protect them by updating the relevant legal frames.

Second topic: Legal Framework for Protecting User's Digital Rights within the KSA

The current situation of digital transformation in all countries has prompted comprehensive changes in social relations and cultures, represented in changing the culture of the society in communication, which affected the prevailing social values that necessarily requires treatment through social studies. This also forced a change to the legal framework resulting from the change in cultural and societal relations. If using technology by the society, its institutions and individuals is commendable, there are other types of social and criminal behaviors that appear accordingly. This is because these technological tools help to expand privacy violations and criminal activities based on information technology.[8] Modern information crimes are illegal activities that can be committed through modern technological methods. Thus, the development in the circulation of digital information and the ease of obtaining it without restrictions has imposed a change in the legal framework and environment through which information and daily actions of both governmental or private institutions are circulated.[9] KSA has already begun developing its legislative environment to keep pace with the developments in technology, information and digital transformation. This action began with joining Arab Convention on Cyber Crimes in 21/12/2010, out of belief in the necessity of confronting the crimes resulting from the use of information technology. The Saudi regulator also issued a package of regulations in order to keep pace with these developments. We will tackle the most important legislative developments enacted to achieve digital transformation and protect its users and their digital rights, especially the privacy right; users' personal data. It explicitly stipulates the criminalization of acts that are regarded as information crimes. In 9/16/2021 A.D., 9/2/1443 A.H., the Saudi regulator issued Personal Data Protection Regulation (PDPR), which includes a set of definitions related to the regulation, scope of its application, rights of data subject, defined periods for accessing and collecting data and their content. The purpose of providing these definitions is reducing the possibility of interpretation for other than the purpose for which the regulation was introduced as is the case of other regulations in other countries.

First: essence of personal data:

The European Union issued Regulation No. 2016/679 for the protection of natural persons with regard to the processing of personal data and the freedom to move such data, which entered into force on May 14, 2018. The regulation aims to strike a balance between a person's right to protect his personal data, and the goal of smooth and secure movement of such data. It defines personal data in article 4 as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

The Egyptian legislator defines it in Law No. 151/2020 concerning data protection as: "Any data related to identifiable natural person, or that can be identified directly or indirectly by linking these data with any other data such as name, voice, photo, identification number, online identifier, or any data that identifies psychological, health, economic, cultural, or social identity."

Article 1 of the Saudi regulation defines personal data as any data, whatever their source or form, that identify a person or make it possible to identified directly or indirectly, such as the name, identity number, bank account numbers, credit cards, fixed or animated photos, and other data of a personal nature.

It is noted that the data mentioned in this definition are not stated exclusively, which means if any other data appear,

[8] Hany Abu Siriy`, *Rua Al-Shabab Nahwa Al-Jara'im Al-Ma`lumatiyyah fi Al-Mujtama Al-Misry*, National Criminal Journal, Issue no. 2, July 2011, p. 87.

[9] Qashqush, Huda Hamid. *Al-Asalib Al-Ijramiyyah Al-Ma`lumatiyyah wa Akhlaqiyat Al-Ma`lumat*, Symposium on the Ethical, Legal, Social Aspects of Information, Cairo 1999, p. 20; See also: Muhammad Samy Al-Shawwa, *Thawrat Al-Ma`lumat wa In`ikasuha Ala Qanun Al-U`ubat*, Dar Al-Nahdah Al-Arabiyyah, 1995, p. 45.

they will be dealt with according to this regulation. This is understood from the phrase, "such as".
The European Regulation stated special categories of personal data (sensitive data), which may only be processed in special cases: “Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of identifying a natural person, health-related data or data related to natural persons' sexual life or inclinations shall be prohibited.”

The Egyptian legislator defined them as: “The Data revealing psychological, mental, physical or genetic health, biometric and financial data, religious beliefs, political opinions, or security situation. In all cases, children’s data are considered sensitive data.”
The European legislator refers to data revealing racial, ethnic, or union membership, or data related to nature or sex. These data are not stated by the Egyptian legislator. On the other hand, the latter refers to the data on the security situation, which is not mentioned by the former.
Then, the Saudi regulator defines other types of data, which are sensitive, genetic, health and credit data.
Article 1 defines sensitive data as every personal data indicating tribal, religious, intellectual, or political affiliations, or indicating membership in civil institutions, criminal and security status, biometric, genetic data, credit, health, or location data. It also includes data indicating persons of unknown lineage.

Article 1 also defined genetic data as every personal data related to the genetic characteristics of natural persons that clearly identify the physiological or health characteristics of that person, which is acquired from analyzing person’s biological sample, such as nucleic acids analysis or any other sample defining genetic data.

As for health data, they include all physical, mental, or psychological data, or those related to his health services.
Article 1 defines credit data as every personal data related to financing requesting or obtaining, whether for a personal or familial purposes from a financing entity. It also includes any data indicating his ability to receive or pay credit, or his credit history.

The aforementioned definitions indicate that they are personal data, not a general one. All of them should be legally protected in the same terms because the regulator defines them as "every personal data”. He intended to protect all personal data in all fields of life that violating them may cause harm to data subject.

Second: Scope of Application of Personal Data Protection

In the European Union regulation, data protection is limited to natural persons alone, not legal ones. The regulation and other legislations do not distinguish between citizens and foreigners. The regulation is applicable to every resident in the European Union with regard to processing their personal data. It stipulates respecting the principles and rules of protecting natural persons' personal data, regardless of their nationalities or place of residence.[10]
Egyptian law, article 2 stipulates putting the provisions into force regarding the protection of personal data that are partially or completely processed by any holder, controller or processor without indicating the nationality of the controller or processor. However, article 5 pertaining to processor's obligations, item 12 implies that the processor outside Egypt should have a representative inside Egypt as the law is applicable only on those processors recorded inside the state.[11]

As for the Saudi regulator, it stipulates the application of Personal Data Protection regulation to any processing of citizens or residents' personal data that takes place in the KSA by any means from any party outside the Kingdom.
Processing of personal data includes any manual or automatic process such as collection, recording, archiving, indexing, arranging, coordinating, storing, modifying, updating, merging, retrieval, use, disclosure, transmission, publication, data sharing, interconnection, blocking, erasing or destruction.
However, if processing of personal data takes place inside the Kingdom, the Personal Data Protection Regulation will be applied. This is also applied to citizens or residents' personal data, which is processed by entities outside the KSA.

Third: Rights of Data Subject

These rights are stated in article 4 of the SPDPR, article 15 of the EU GDPR, and article 2 of EPDPL.
The Saudi regulator provided for the following rights:

1- The right to be informed: it means to inform him of the legal or scientific justification and purpose for collecting his personal data. Otherwise, these data will not be processed in a way that opposes the purpose of its collection or in cases other than those stipulated in article 10 of the regulation.
2- The right to access his personal data possessed by the controller, which means any entity or person with natural or legal capacity that defines the purpose and method of processing personal data.

[10] European Union Regulation, whereas: 2.

[11] See: Egyptian personal data protection law, article 2.

The processor is a public entity or any person with a natural or legal capacity, which processes data on behalf of the controller. Thus, he has the right to access, view, or have a clear and free copy to his personal data that conform with the records.

3- The right to correct, complete, or update his personal data possessed by the controller.

4- The right to request destruction of his personal data that are no longer needed. Destruction means removal of personal data and inability to view or retrieve them again.

As for the Egyptian legislator, it approves these rights and adds that data subject has the right to request abolishing his prior consent to keep or process his personal data, or to confine processing of data to a specific scope. He can also object to the processing of his personal data or their results when they conflict with his basic rights and freedoms.[12]

As for the EU GDPR, article 15 stipulates that data subject has the right to obtain confirmation from the controller whether his personal data is processed or not. In this case, he has the right to access his data. Article 16 states that data subject has the right to correct his inaccurate personal data without unjustified delay, while taking into account the works of processing. Article 18 also stipulates that individuals can request a limit on how their personal data is used in one of the following cases:

1- To contest the accuracy of his personal data for a period that allows the controller to verify their accuracy.
2- To object and request erasing or restricting personal data if they are illegally processed.
3- If the controller is no longer using such data for processing purposes, but it needs them to establish, exercise or defend a legal claim.

Fourth: Controller's obligations:

The European legislator describes these obligations as principles, since they are closely related to various aspects of personal data processing. The regulation stipulates it in Chapter Two and outlined it in article 5 under the title: Principles Relating to Processing of Personal Data. It stipulates that personal data must be processed legally, fairly, transparently, rationally and accurately for the purposes they were collected for.

As for the Saudi regulator, it has stated those obligations in articles from five to twenty-nine. We will highlight the most important of them as follows:

1- The controller may not process personal data or change the purpose of processing them without a prior consent of data subject. The regulation shows consent conditions and the circumstances where approval should be in a written form.
2- The Saudi regulator obligates the controller, when choosing the processor, to choose the body that abides by the law and regulations, and it should constantly verify their compliance with the instructions related to protection of personal data in a manner that does not conflict with the provisions of the law and regulations.
3- The Saudi regulator holds the controller responsible if the processor breaches its obligations.
4- The controller is not permitted to collect personal data except from their owners directly, or process such data except to achieve the purpose for which they are collected except in the following cases:
   a- If data subject agrees according to the regulations.
   b- If personal data are publicly available or collected from publicly available sources.
   c- If the controller is a public entity and collects personal data from other than their direct owners, or its processing was for a purpose other than that for which they were collected such as security or judicial purposes in accordance with the provisions specified by the regulations.
   d- If compliance with this restriction may cause harm or affect the vital interests of data subject.
   e- If collecting or processing personal data is required to protect public health and safety, or the life or health of the individual.
   f- If personal data will not be recorded or stored in a form that makes it possible to identify the owner directly or indirectly.

Moreover, the aforementioned exceptions are restricted with specific controls and procedures in the executive regulation. This aims at protecting the confidentiality of personal data and so that those exceptions would not be used as a pretext to access or disclose these data without a requirement.

The Saudi regulator stipulates that the purpose of collecting personal data should be directly related to the purposes of the controller and that the methods and means of collecting these data should not conflict any legally established provision. These methods should also be clear, direct, secure, appropriate to owner's circumstances, and free of deception, misleading or extortion. Moreover, the content of the data must be appropriate and limited to what is required to achieve the purpose of its collection. It should

[12] Ibid.

not also identify data subject. If it becomes clear that the collected data is no longer required, the controller must stop collecting them and immediately erase what it has previously collected.

Article 4 and 5 of the Egyptian law hold the controller and processor responsible. It obligates the controller to get or receive personal data from the bodies concerned with providing them after the approval of data subject, or in the cases authorized by law. They should make sure that these data are accurate, consistent, and sufficient to the purpose of collecting them.

The method, means, and criteria of processing should agree with the defined purpose unless the processor is authorized to do this by virtue of a written contract. The purpose of collecting data should agree with the purpose of processing them.

The legislator also obligates the controller not to do any act that makes personal data available except in the cases authorized by law. The controller should also take all technical and organizational measures and apply the necessary standards to protect and secure personal data against disclosure, hacking, erasing, or changing before any illegal action.

The controller should erase personal data directly after fulfilling their defined purpose. However, if it keeps them for any legitimate reasons, they must not remain in a form that identifies their owner. it should correct any error in these data as soon as he is informed or become aware of.

As for processor's most important obligations in the Egyptian law, it is obligated in article 5 to process personal data according to the rules stated in this law and its executive regulations. This should be based on written instructions sent by the center, controller, or concerned persons according to the circumstances, especially in matters related to the scope, subject and nature of this process, and the type of data and their agreement and adequacy with the identified purpose.

The purposes and practice of processing must be lawful and agrees with public order or morals. The purpose and duration of the processing shall not be exceeded. The controller or the person concerned with the data should be notified of the required period for processing.

The processor guarantees erasing personal data when the processing period ends or delivers these data to the controller. The processor should not do any act that may reveal personal data or the results of the processing except in the cases authorized by law. It should not also process data in a way that contradicts the purpose or activity of the controller, unless it is for a statistical or educational purposes without violating privacy.

Fifth: Punishments Stated in Personal Data Protection Regulation

To carry out the provisions stated in the articles of both SPDPR, and EPDPL, and to ensure the commitment the controllers and processors of those texts, the Saudi and Egyptian regulations have criminalized a set of actions to deter violating these data and protect privacy and public freedoms.

Article 35 of Saudi regulation states: Without cancelling other severer penalties stipulated in other laws, the penalty for committing the following violations shall be in accordance with what is stated before them:

a- Any person who discloses or publishes sensitive data in violation of the provisions of the regulation shall be punished with imprisonment for a period not exceeding two years and a fine not exceeding three million Riyals, or with one of these two penalties if this violation is intended to harm the data subject or to achieve a personal benefit.

b- Whoever violates the provisions of article 29 of the regulation[13] will be imprisoned for a period not exceeding one year and a fine not exceeding one million Riyals, or one of these two penalties. Article 36, paragraph 1 stipulates that any violations that are not stated in article 35, without abrogation of severer punishments stated in another regulation, will be warned and then punished with a fine not exceeding five million Riyals. This punishment will be applied to any natural or legal person who violates any of the provisions of the regulation. The fine may be doubled if the violation is repeated even if the fine exceeds the maximum limit, provided that it does not exceed twice of that limit.

It is noted that the Saudi regulator has limited the penalty mentioned in article 35 to violating sensitive data only whether this violation is done by public or private person. However, this was restricted by existent of a special element, which is the intent to harm data subject or achieve personal benefits from this disclosure. Then, article 36 stipulates that the penalty of warning or fining will only be applied if the provisions of this regulation are violated. This means that violation of sensitive data will be punishable according to the text of article 35. As for violating other personal data, the provisions of article 36 will be applied if the violator is

[13] Article 29 of the regulation states that except in cases of extreme necessity to preserve the life of data subject outside the Kingdom or his vital interests, or to prevent, examine or treat a disease or an infection, the controller may not transfer personal data or disclose them to a party outside the Kingdom unless by virtue of an agreement to which the Kingdom is a party or for other purposes determined by the regulations.

a private natural or legal person, which means that public natural or legal persons are excluded from this text. The researcher believes that there is no need to differentiate between public and private person with regard to the stated offenses.

As for the Egyptian legislator, it stipulates in articles 35 and 49 the acts that, if committed, would constitute a crime related to protected personal data. Thus, it stipulates punishing every possessor, controller or processor who collects, discloses, or circulates electronically processed personal data by any means in other than the cases authorized by the law or without the consent of data subject. The Egyptian legislator also stipulates the punishment of any holder, controller or processor who refrains, without a legal requirement, from permitting data subject to exercise his rights stipulated in Personal Data Protection Law.

It also stipulates the punishment of the controller or processor who breaches his obligations stipulated in the aforementioned law, and punishes any holder, controller or processor who collects, circulates, treats, discloses, stores, transmits or saves sensitive personal data without the consent of data subject or in other than the cases authorized by law.

In article 49, the Egyptian legislator regarded these crimes to be reconcilable. It also stipulates that the accused may, at any state of the criminal case and before the judgment becomes final, prove reconciliation with the victim, his special agent, or his general successor.

It is noted that enacting criminal penalties in the Saudi regulation and Egyptian law is the effective guarantee for the protection of personal data. The privacy right and private life is one of the rights that should be protected. Those penalties made personal data a sanctity that may not be violated, just as the sanctity of homes, the violation of which constitutes a crime, except in accordance with the law.

Conclusion

Outcomes:

- Digital transformation has a significant importance for all countries. They should deal with its positive and negative consequences as a societal phenomenon through enacting legislations that protect people against the resulting harms and protect digital rights emanating from the process of digital transformation, which affects persons' personal data directly or indirectly.
- Some Arab countries are encountering a big problem, which is the absence of a regulation protecting persons' personal data. Violating these rights harms individuals' interests and privacy, which motivates countries to enact laws to regulate receiving, preserving, storing and erasing such data in a legitimate way and prevent violating or hacking them.
- EU GDPR, the SRPPD, and the EPPDL developed a set of technical definitions about the processes in which such data is used and the parties dealing with these data. Moreover, they identified the rights of data subjects and the obligations of those receiving such data.
- Personal data mentioned in the European regulation, Egyptian law, and Saudi regulation were stated for example, but not limited to the aforementioned examples to include any data, by which the person can be identified.
- The Saudi regulator did not impose any obligations on the processor, except for protecting confidentiality stated in article 41. The Egyptian legislator organized the obligations of the controller and the processor separately and stipulated penalties for each of them for violating their commitments.
- The Saudi regulation imposes freedom-restricting penalties in only two cases; disclosing sensitive data in violation of the regulation, and violating article 29 related to the transfer of data outside the Kingdom of Saudi Arabia. As for the rest of the penalties, they are financial ones. The Egyptian legislator imposes severe deterrence than that of the Saudi regulation. In addition to financial penalties, it stipulates freedom-restricting penalties for many violations.

Recommendations

- We recommend the Saudi regulator to specify the exact obligations of the processor in order to bear the responsibility of its mistakes, which may not relate to the controllers.
- We recommend the Saudi regulator to impose freedom-restricting penalties in addition to financial fines as stated in article 36 for violating the provisions of the Personal Data Protection Regulations in order to make the regulation more effective in protect personal data.
- We recommend Saudi social institutions to conduct awareness sessions for users who may voluntarily contribute in violating their privacy and their personal data due to lack of awareness. Thus, users should be aware of the implications of sharing their data.

We recommend the Saudi regulator to promote international cooperation among countries via the United Nations to facilitate the process of detecting hackers and penetration of personal data, as these are cross-border crimes

References

[1] Ghitas, Muhammad Jamal. *Al-Dimuqratiyyah Al-Raqamiyyah*, Nahdat Misr, 2006.

[2] Ali, Rizq Saad. *In`ikasat Al-Tahawwul Al-Raqamy Ala Al-Siyasah Al-Jinaiyyah Al-Muaasirah*, Journal of Legal and Economic Studies, Faculty of Law, Sadat University, 2021.

[3] Hasanin, Saad Atif. *Al-Himayah Al-Jinaiyah Lilmusanafat Al-Raqamiyyah*, Comparative Study, Dar Al-Mufakir Al-Araby, Alex.

[4] Hasan, Abdulrahman Hasan. *Waqi Al-Tahawul Al-Raqami Lilmamlakah Al-Arabiyyah Al-Saudiyyah*, Administrative and Financial Sciences Journal, College of Economy and Commerce, University of Eloued, 2020.

[5] Shihatah, Muhammad Musa. *Inikasat Tafeel Aliyat Al-Tahuwwul Al-Raqamy fi Dawa Mubadarat Al-Shumul Al-Mali Ala Tatbiqat Al-Hukumah Al-Iliktruniyyah in Egypt*, Journal of Contemporary Commercial Studies, issue no. 9, January 2020, p. 204.

[6] Al-Shawa, Muhammad Samy. *Thawrat Al-Maalumat wa Inikasatiha Ala Qanun Al-Uqubat*, Dar Al-Nahdat Al-Arabiyyah, 1995.

[7] Mashal, Muhammad Ahmad Salamah. *Al-Haqq fi Mahw Al-Bayanat Al-Shakhsiyyah*, an analytical study in light of EU (GDPR), published in www.google.com.

[8] Ali, Muhammad Hasan Abdullah. *Al-Nizam Al-Qanuni Lihimayat Al-Bayanat Al-Shakhsiyyah Al-Mualajah Iliktruniyan*, Journal of Legal Sciences, College of Law, Ajman University, 2021.

[9] Hani Abu Siri. *Ruaa Al-Shabab Nahwa Al-Jaraaim Al-Maalumatiyyah fi Al-Mujtama Al-Misry*, National Criminal Journal, issue no. 2, July 2011.

[10] Qasqus, Huda Hamid. *Al-Asalib Al-Ijramiyyah Al-Maalumatiyyah wa Akhlaqiyyat Al-Maalumat*, Symposium on the Moral, Legal and Social Aspects of Information, Cairo, 1999.

Laws and Regulations

1- EU General Data Protection Regulations, European Parliament.
2- Royal Decree no. (M/19) in 3/2/1443 A.H., on Saudi Protection of Personal Data.
3- Law no. 151 in 2020 on Protecting Personal Data in Egypt.

Websites:

https:// ar.m.wikipedia.org

www.google.com

Naif A. Alghamdi
joined Saudi Aramco in 2013. He is currently serving as Computer Operation System Specialist in AITD. He received a B.S. degree in Information technology from King Abdul Aziz University.