

حملة - المركز العربي
لتطوير الإعلام الاجتماعي
7amleh - The Arab Center for
the Advancement of Social Media



An Exploratory Study:

The Reality of Privacy

& Digital Data Protection

in Palestine

August 2021

7amleh –The Arab Center for Social Media Advancement

An Exploratory Study: The Reality of Privacy and Digital Data Protection in Palestine

Researcher :Dr .Omar Abu Arqoub

Study editing :Mona Shtaya and Inas Khatib

Translation into English :Ritaj Managerial Solutions

English Proofreading :Ritaj Managerial Solutions

Designed by :Amal Shoufany

This research was issued by funding from the Norwegian Representative Office .The research reflects the researcher’s and7 amleh’s position and does not necessarily reflect the position of the donor.



The Representative Office of Norway
to the Palestinian Authority

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

To view a copy of this license, visit: <http://creativecommons.org/licenses/by-nc-nd/4.0/>

Contact Us:

info@7amleh.org | www.7amleh.org

Tel: +972 (0)774020670

Find us on Social Media: **7amleh**

Table of Contents

Executive Summary	5
Chapter One: Introduction	8
Chapter Two: Literature Review	10
The Concept of Privacy and Personal Data	10
Personal Data	11
Technologies for Collecting and Using Personal Data	12
Global Privacy and Data Protection Laws	14
The Reality of Privacy and Data Protection in Palestine	16
The Privacy of the Palestinians and the Control of the Israeli Occupation	18
Chapter Three: Study Methodology	18
The Study Sample	18
Chapter Four: Presenting the Results	19
Focus Groups	19
The Concept of Privacy and Digital Personal Data	20
Violation of the Privacy of Palestinian Users	21
The Role of the Occupation in Controlling the Privacy of the Palestinians	22
Towards a Palestinian Privacy and Data Protection Law	22
The role of local authorities in enacting a privacy and data protection law	23
Personal Interview Analysis	24
The Concept of Privacy and Digital Personal Data	24
Data Collection Stage	25
Data Processing Stage	26
Data Use Phase	26
Violation and Exploitation of Personal Data	26
Compliance with Privacy Policies and Protection of Personal Data	28

The Relationship between Privacy Law, Democracy and Human Rights	29
What should be Protected and what should be Made Accessible	30
Privacy and Data Protection in Palestine from an International Perspective	31
The Israeli Control over the Privacy of the Palestinians	31
Model 1: The Online Payment Company MaalChat	33
Model 2: Call U Internet Service Provider	35
Towards a Palestinian Privacy and Data Protection Law	36
Features of the Desired Palestinian Privacy and Data Protection Law	38
Recommendations	40

Executive Summary

This study seeks to identify the reality of privacy and protection of digital personal data in Palestine¹ in terms of the collection, processing and use of Palestinian users' data. It addresses some of the human rights violations faced by Palestinian users as well as the key parties that violate their data privacy. It also identifies the main features and principles of the desired Palestinian privacy and data protection law. Qualitative research methodology was used in preparing this research, through the use of two tools for data collection and analysis. The first tool, focus groups, utilised three geographically distributed groups who participated from the West Bank, the Gaza Strip, and East Jerusalem. The number of participants ranged from 14-16 participants. The second tool is the in-depth, personal interviews with a sample of 12 individual stakeholders with the experience and knowledge of the case under study.

The focus groups showed that the concept of privacy and personal data is relatively new and not fully known, especially in Jerusalem, and that efforts are needed to publicize it and its importance. This is considered a main reason for the low percentage of those who read and are familiar with the privacy policies of sites, applications and services before using them. The majority of participants agree on the necessity and importance of enacting a comprehensive Palestinian law on privacy and data protection to be applied in all Palestinian areas whose main objective is to protect Palestinians' data and prevent the violation of their privacy.

On the other hand, and due to the specificity of the political, security and human rights situation related to the Palestinian cause and its dimensions, the parties that seek to violate and breach the privacy of Palestinians and their private data vary, according to what the participants in the focus groups and personal interviews indicated. These parties can be classified as follows: the Israeli occupation, the Palestinian Authority, private sector companies and external parties, including global social media platforms such as Facebook. The reasoning for these violations varied, the most prominent including security goals, political goals, commercial and advertising goals.

The majority of participants in focus groups and in-depth interviews expressed, as per their classifications and geographic areas, great interest in the importance of enacting a Palestinian law and legislation to protect the privacy and data of Palestinians. All civil society organizations and sectors participate, and work with governmental and legal authorities, to support the enactment and adoption of this law in all Palestinian areas. The focus was on the proactive role of Palestinian civil

1. Palestine -in this report- refers to the West Bank, Gaza Strip and East Jerusalem.

society, in the process of raising societal awareness of the law and the importance of privacy and protection of personal data at the popular and official levels. This is the first fundamental step towards enacting the law, where citizens must be made aware of privacy and data protection in the digital era before the law is enacted, and in light of the low percentage of those who are well informed about the concept of privacy and personal data.

This can be compared with the perceptions of European citizens about privacy and data protection through opinion polls on the trend of European public opinion with regard to privacy and data protection during 2012. The results showed that European citizens are aware of the basic principles of the concept of privacy and data protection ;however their awareness of the specific aspects of privacy as an individual right and a social principle was rare .The majority of Europeans believe that they have lost control of their personal data ,in addition to their data not protected ,which requires regulating laws.²

In-depth interviews revealed that several private or public parties may be working on collecting Palestinians 'personal data ,and although they do not have sufficient technical and logistical ability to process this data and analyze it using artificial intelligence algorithms and techniques ,yet ,in the coming years ,the process may become more accessible by all parties who collect personal data .It is only a matter of time until these companies and agencies have the ability to process this data, due to the analysis and processing of this level being used in major international companies such as Facebook and others ..Therefore ,in order not to create chaos regarding the analysis of user data and behavior ,it is necessary to develop a regulating law that manages and protects the privacy of Palestinian users and serves as the main step towards building permitted and prohibited actions and within the framework of data collection ,processing and use.

In the same context ,the privacy policies of companies and various entities that should be approved by users and subscribers ,must be clear and consistent with the law itself .The law must also detail them so as to put an end to the indiscriminate privacy policies ,or those policies that violate the privacy of individuals indirectly. The standard should be that the data of users who agree to privacy policies ,are preserved and not violated by these policies.

One of the biggest problems and gaps that emerge from the absence of such a law is that the door to jurisprudence regarding privacy and data protection remains open .It is not understood what data is allowed or prohibited and how it should be

2. Hallinan, Dara, Friedewald, Michael, & McCarthy, Paul. (2012). Citizens' perceptions of data protection and privacy in Europe. *Computer Law and Security Review*, 28(3). Pp. 263–272. <https://doi.org/10.1016/j.clsr.2012.03.005>

analyzed ,used and utilized ,which forces the Palestinian user to deal with different privacy policies for each company and/or a party according to what it deems appropriate and meets its needs .This in result may hold these bodies accountable and responsible if they make a mistake or do not abide by privacy standards that are not stipulated locally ;this is why we are facing a real issue regarding privacy.

The report showed that there is a lot of information being collected, while companies are not transparent about their data collection, the nature of its use, processing and exchange with internal or external third parties, carrying out these operations under cover. The issue is, that in the absence of a party responsible for monitoring and following up on this issue, we cannot know the extent to which our data is hacked on a daily basis.

The contradiction in statements given by the owners of private sector companies, human rights organizations and participants in the focus groups was clear. The respondents indicated, for example, that the Palestinian security forces, whether in the Gaza Strip or the West Bank, have the ability to access any information held by private sector companies, whether by legal means or through cooperation with these parties and the use of concealed methods, nepotism and wasta (tr: who you know), for public or personal purposes. The laws enacted and applied in the West Bank and Gaza facilitated this breach of privacy, which demands a thorough review of previous laws and regulations in a serious manner in order to change these laws and harmonize them with international standards, especially the Cybercrime Law.

Ministries and agencies responsible for following up on privacy issues with private sector companies create computerized systems that try to protect and preserve privacy, and limit access to data; however, the controls of these computerized systems remain incomplete and inaccurate or are not linked to a law that clarifies what information these systems must provide, what they must withhold, and who has the authority to view, program and maintain these systems. Government agencies and ministries are still working on diligence in this matter. The absence of the law on which these systems are based, is the biggest loophole through which any violation of privacy can be committed. One cannot speak about the issue of privacy in the absence of a supervisory body based on laws and legislation, and judicially approved standards and provisions for monitoring Palestinian users' data.

Eventually, the report suggested a set of recommendations, such as the formation of a Palestinian commission to protect and regulate privacy and personal data, and the need to pass a comprehensive Palestinian privacy and data protection law. The report presented the most important features of the desired Palestinian law in this context, in addition to stressing the importance of public and official awareness of the issue of privacy and data protection in Palestine.

Chapter One: Introduction

The tremendous technological development of digital means of communication on the internet has led to the generation of Big Data for users. This huge archive of public and personal data about users and their interactions on the Internet has created a new wealth that has come to be known as digital oil (digital data is the new oil). For-profit, non-profit, private and governmental institutions and organizations use this data in various ways, and their decision-making process depends on the data generated. The use of personal data does not necessarily benefit individuals, and its use is not necessarily tangible and visible, and herein resides the risks of owning and controlling this data.

Most of the data is collected without the owner's notice or consent, and in most cases includes their identity and personal information, which is then saved, archived and analyzed to be used according to the need of who holds this data. This makes individuals vulnerable to inevitable risks, in the absence of a law that protects them and their privacy from data collectors, especially in the absence of the right to be forgotten (to have private information removed). Consequently, it has become imperative for the official and competent authorities to take action to protect human rights and the privacy of users, and to organize the collection and use of individuals' personal data in a manner that preserves their privacy and prevents its misuse or exploitation.

We can't separate privacy and the protection of users' personal data from the concepts of human rights and democracy, as the privacy of individuals and their private data is guaranteed in international human rights charters and conventions. It is stipulated in Article 12 of the Universal Declaration of Human Rights that, "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation; Everyone has the right to the protection of the law against such interference or attacks."³ Moreover, autonomy and personal freedom are a basic principle according to the democratic system, and accordingly is one of the most important conditions and foundations of efficiency for democratic countries, where privacy and data protection are basic conditions for independent, free thinking and action. Therefore, it is the duty of democratic constitutions to protect privacy and to enact laws and regulations that protect personal and digital user data and that push towards the protection of human rights within its general goals.⁴ In 2016, the European Union passed a privacy

3. الأمم المتحدة. (1948، 10 كانون الأول). الإعلان العالمي لحقوق الإنسان. منظمة الأمم المتحدة. ص2. تاريخ الاسترداد 2021.

4. Boehme-Neßler, Volker. (2016). Privacy: A matter of democracy. Why democracy needs privacy and data protection. *International Data Privacy Law*, 6(3). Pp. 222–229. <https://doi.org/10.1093/idpl/ipw007>

and data protection law after vigorous deliberations and amendments, which came into force in 2018. The law focuses on the processing of personal data and the limits of the movement of that data inside and outside the European Union, and the rest of the countries are still uneven in the path of passing similar laws to them⁵.

As for Palestine, the issue is more complicated in light of the Israeli occupation, internal political turmoil and the Palestinian internal division. These factors led to the absence of a central authority responsible for regulating and protecting individuals' lives and privacy. With the absence of an effective legislative authority, there was a lack of structure causing a publicity of private data, and the ability of any party, whether official, private or security, to exploit the data of citizens present in the Palestinian territories. Palestinian laws, regulations and policies are still inadequate in terms of privacy, data protection and related electronic crimes, and the right to access information. This is what caused real problems worthy of evaluating the reality and proceeding with procedures and laws regulating all these developments, which this study seeks to discuss and research.

This study aims to identify the reality of privacy and protection of personal digital data in Palestine, by surveying the mechanisms of data collection, how it is processed and its uses. Then, it presents the human rights violations that Palestinian users are exposed to with regard to their personal data, in order to shed light on the basic features and principles on which the Privacy and Data Protection Law should be based.

5. European Union. (2018). [General Data Protection Regulation \(GDPR\)](#). Retrieved May, 2021.

Chapter Two: Literature Review

The Concept of Privacy and Personal Data

Privacy is the right of an individual to preserve their personal information and private life voluntarily and freely, and to prevent unauthorised access to it. Privacy refers to private life including personal data, for example medical data, private data (photos and conversations), bank data, contact information and others. It is an integrated and harmonious system of physical and spiritual characteristics and features, lifestyle and ethics, and a vision of the self and the other⁶. Privacy draws the boundaries that regulate the ability of society to interfere in the lives of individuals, and it has four basic boundaries. The first is the privacy of personal information, its collection and processing; the second, is the privacy of the body from physical interference; the third, is the privacy of communication and the security of all forms of correspondence; and the fourth is the specificity of the spatial space in which the individual resides. Privacy has two main aspects, the first being right to freedom of a private life; and the second, the right to the secrecy of this life⁷.

The development of information technology and the subsequent developments that affected big data, its form and areas of exploitation, and the the principles of big data, came in conflict with the principles of privacy and protection of personal data, such as those established by the European General Data Protection Law⁸. The digital era has accelerated the erosion of the information privacy of users on the Internet, with an immense amount of information available in the digital space, forcing data to shift from the private to the public domain. The danger of this information, as collected by social media platforms, lies in its use for criminal purposes to harm others or for security and sometimes military purposes. Privacy is a human right, and part of the digital rights that constitute an extension of human rights in the digital space, thus, whoever violates them is subject to legal accountability; according to the American Judicial Institute, “every person who seriously and unlawfully violates the right of another person not to have his or her affairs and conditions reach others, and his image not being exposed to the public’s attention, shall be considered responsible before the victim⁹.” The reality shows that the violation of privacy is a prevalent matter, even in democratic countries that operate in accordance with legislation to protect privacy due to the absence of law enforcement tools. In many countries, the police and security forces are given powers that take precedence

6. قوتال، ياسين. (2013). حق الخصوصية الإلكترونية بين التقييد والإطلاق. جامعة عباس لغرور. ص 56.

7. المصدر السابق.

8. Wolford, Ben. (2018). [What is GDPR, the EU's new data protection law?](#) Retrieved May, 2021.

9. قوتال، ياسين. مصدر سابق. ص 57-58.

over privacy laws, which make committing violations easy. In the Arab countries, legislation is unable to confront violations of the right to privacy, and there is a need to spread cultural awareness of the right to privacy and its meanings, and to clarify its dimensions and harmful impacts¹⁰.

The concept of information crime is linked to what is included in the means of communication and media of data and information that are collected, circulated, stored and processed automatically, digitally or electronically. This in turn facilitated, accelerated and expanded its access, hacking and penetration, and this data may be linked to countries and entities or to specific individuals and people. This prompted states and societies to reconsider their legal and legislative system and criminalize such acts. Thus, information crime has become a threat to modern and digital societies that rely on internet use and electronic devices¹¹. We can point out that the risks of information crime are not necessarily related to computers and digital technologies themselves, which are by nature neutral; however the way they are used or exploited is the real threat in the absence of modern regulations and laws that control the use of these technologies¹².

Personal Data

Personal data is defined by the General Data Protection Regulation (EU GDPR), as any information relating to individuals, by which we can identify them directly or indirectly, for example, name, email, address, geographic location, race, gender, photo, religion beliefs, browsing information about websites, political opinions, nicknames, and all data that can be considered personal that may be a threat in identifying the identity of a particular person¹³.

Personal and digital data available on the internet or at companies/institutions/governments reveals a lot about individuals, their thoughts, lifestyle and movements, and it became easy to exploit this data to harm and entrap them and influence their choices. For example, some repressive governments have used the digital personal data of journalists and activists to track down and harm them. Data exploitation is not limited to governments and institutions. Even individuals can exploit the

10. الضناوي، زينب. (2019). الحماية القانونية للخصوصية على الإنترنت في ظل الجهود الدولية والداخلية. لدى سرور، طالبي. (مشرّف). [كتاب أعمال المؤتمر الدولي المحكم حول الخصوصية في مجتمع المعلوماتية](#) (ص 22-37). لبنان: طرابلس. مركز جيل البحث العلمي.

11. خلايفة، هدى. (2019)، الإطار القانوني الدولي والداخلي لحماية الخصوصية على الإنترنت، التشريع الجزائري نموذجًا. لدى سرور، طالبي. (مشرّف). [كتاب أعمال المؤتمر الدولي المحكم حول الخصوصية في مجتمع المعلوماتية](#) (ص 39-58). لبنان: طرابلس. مركز جيل البحث العلمي.

12. نسمة، بطيحي. (2019). الجرائم المتعلقة بانتهاك الأحكام الإجرائية المقررة لحماية الحق في الخصوصية الرقمية في التشريع الجزائري. لدى سرور، طالبي. (مشرّف). [كتاب أعمال المؤتمر الدولي المحكم حول الخصوصية في مجتمع المعلوماتية](#) (ص 59-86). لبنان: طرابلس. مركز جيل البحث العلمي.

13. Wolford. Ibid.

personal data of other individuals to blackmail and harm them. Therefore, it has become necessary to ensure the protection of personal and digital data for each individual, and to provide them with the right to choose who they want to share their information with, and who has access to it, as well as the length of time that they can be kept in databases, with the individual's ability to modify this data whenever they want¹⁴.

Technologies for Collecting and Using Personal Data

Modern communication technology and the internet have produced a set of techniques, methods and ways of collecting, analyzing and using personal data of users. Perhaps the most widespread technology is cookies, which follow the consumer across the internet. It enables websites to collect information about users' for example, the type of device and processor, the user's IP number, the method of Internet connection, the sites visited, the number of hours spent on the Internet, the nature of interests, what one is looking for, and one's electronic purchases. They also collect all personal information that the user puts in any registration form on the internet, such as credit card numbers, phones, and addresses, while visitors to websites often are not aware. Advertisers also exploit this information for the benefit of their advertisements, which are also usually used by third parties, which requires a comprehensive regulation by the competent authorities of aspects of collecting and using this data¹⁵.

In the same context, the use of mobile phones, with its technologies such as identifying the geographical location and sharing it on social media platforms, has benefited marketers in directing advertisements mainly according to the data collected by this technology, in order to send its appropriate advertising messages and select its target audience accordingly¹⁶.

In addition, and based on the huge amount of information that has become available through modern technologies and communication development, the ease of hacking websites, databases and personal data through organized hacker attacks that target individuals or specific institutions, which constitutes an open war by taking advantage of available electronic loopholes. This is usually done through complex programs, fraudulent methods, and hacking of devices and anything that

14. الصيادي، أمانة. (2019، 25 كانون الثاني). البيانات الشخصية: ما مدى أهميتها حمايتها وهل من تشريع؟ منظمة أكسس ناو. تاريخ الاسترداد: أيار/ مايو، 2021.

15. عزي، عبير. (2015). تأثير استخدام المعلنين لملفات تعريف الارتباط (الكوكيز Cookies) لتتبع المستهلك عبر شبكة الانترنت على حماية الحق في الخصوصية. المجلة المصرية لبحوث الإعلام. جامعة القاهرة. ص 301-346.

16. عزي، عبير. (2018). تأثيرات استخدام المعلنين لتقنيات التتبع الجغرافي للمستهلكين عبر الهواتف الذكية. المجلة العلمية لبحوث العلاقات العامة والإعلان. ص 509 - 549.

is connected to the internet. According to Al-Mousawi and Fadel Allah, the breach of privacy on the internet can be carried out by three main parties, *the internet service provider, who can monitor everything you do on the internet (the place and time of accessing the network, the sites visited by the browser, the times, and the words searched, conversations, emails, etc.), *the websites visited by the browser are in turn able to determine users actions through cookies, *and Hackers, by focusing on the loopholes of electronic forums and social media platforms¹⁷.

After users' data is collected by institutions and companies, it is used to target them more accurately, and there are institutions and companies that sell this data to third parties, which is at the heart of the privacy breach¹⁸. Privacy is also breached on social media platforms by making their users' personal information available to developers and digital service companies, enabling them to access users' interactions without any control by social media platforms. In the early years of social media platforms, users did not control their personal data, and these platforms did not see the need to inform users of which of their data was published and that others could get them. All this exposed these platforms to legal accountability, which forced them to make changes to protect data permanently, which are still not enough to tackle this issue¹⁹. The digital future poses a challenge to privacy, especially on social media platforms, which have become dominant over sites and applications by allowing the use of their accounts to register and fill out instant personal data for different sites and applications²⁰, in addition to making data available or voluntarily selling it, or obtaining it by hacking methods. There are also employees who process personal data of customers and users who are entrusted with the task of searching, processing and storing digital data, and that makes them capable of violating privacy²¹.

On the other hand, governments collect the data of their citizens under various administrative laws, including car registrations, residence and taxes in addition to information about financial, marital status, use of electricity, water, etc. This information enables government agencies to carry out their tasks efficiently, but the danger arises from the disclosure of citizens' data and its access for illegal and illegitimate purposes, by the governments themselves and by third parties²².

17. الموسوي، منى؛ وفضل الله، جان. (2013). الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها. *مجلة كلية بغداد للعلوم الاقتصادية الجامعة العدد الخاص بمؤتمر الكلية*.

18. جابر، أشرف. (2015). استهداف مستخدمي الإنترنت بالإعلانات التجارية وحماية الحق في الخصوصية. *مجلة العلوم الإنسانية*.

19. فضيلة، تومي. (2017). إيديولوجيا الشبكات الاجتماعية وخصوصية المستخدم بين الانتهاك والاختراق. *مجلة الباحث في العلوم الإنسانية والاجتماعية*، العدد 30، ص 41-50.

20. Weber, Rolf. H. (2015). The digital future - A challenge for privacy? *Computer Law and Security Review*, 31(2). Pp. 234–242. <https://doi.org/10.1016/j.clsr.2015.01.003>

21. Ibid.

22. Ibid.

It is important to talk about the protection of privacy and personal data because the ways, means and methods that can be used on the internet are vast and varied, and some are still not discovered or documented, and is a technology that is developing in parallel with the development of technology and communication technologies and the internet. Thus, it is important to have awareness of the basic rules that may help reduce the amount of information and personal data that others can know about the user.

Global Privacy and Data Protection Laws

According to data from the United Nations Conference on Trade and Development, 128 out of 194 countries have passed laws or are in the process of adopting laws to protect privacy and digital data²³. The European Union's General Law on General Data Protection Regulation (EU GDPR), enacted in 2018, provides a positive framework to protect users and individuals to regain control of their personal and digital information. This is the most comprehensive law and has become a source of inspiration for many governments, legislative and legal bodies. This act stresses that one of the main components of privacy and data protection after data collection restriction is the data processing stage. GDPR defined it as any processing or process carried out on personal information, whether automated through programs, algorithms or manual, which includes the processes of collecting, analyzing, recording, organizing, dividing, classifying, using, and scanning of digital users/individuals data who may be clients or users or visitors to the Website. It also states the need to know who has the right to view and process the data and define their powers in a clear and known manner, even if they are an employee or owner of user data, or a third party that manages this data legally and securely²⁴.

Privacy and data protection policies and the laws related to them, obligate all parties that own or collect and process personal data to abide by them. For example, each website must have a privacy policy that explains to its users what information is collected, how it is used, how it is shared, and how to secure it. These policies can be inspired by privacy and data protection laws and legislation, which are mostly American and European laws, and it is essential for business owners and institutions to abide by the provisions of privacy and data protection laws. This way it will be easier and less expensive to comply with these standards rather than applying different rules that cause legal and rights violations, or negatively affect

23. UNCTAD. (2021). [Data protection and privacy legislation worldwide](#). United Nations Conference on Trade and Development. Retrieved June, 2021.

24. Wolford. Ibid.

the decisions of users and customers whose data protection issue has become a fundamental and key issue that negatively affects the reputation of the institution/ company²⁵.

Access Now, based on the GDPR, stressed that all legal frameworks in all countries that seek to adopt privacy and data protection laws must take into account the imposition of adequate penalties for all those involved in personal and privacy data, including the criminalization of; unauthorized access to systems identity or other databases containing personal data, unauthorized monitoring of identity systems or databases, unauthorized alteration of data collected or stored, unauthorized interference with identity systems or databases holding personal data²⁶.

In the United States, there is no comprehensive federal law governing data privacy, as there is a complex mixture of laws for the public and private sectors, including those laws and regulations dealing with communications, health information, credit information, financial institutions, and marketing, most of which were issued in specific states²⁷.

The following are seven principles to protect personal data and enable accountability provided for by the GDPR due to the comprehensiveness and modernity of this act²⁸:

1. Dealing with personal data in a lawful ,legitimate ,transparent and fair manner towards the data owner.
2. Determining the direct and exact purpose of data processing and informing the data owner when collecting it.
3. Reducing the amount of data collected and limiting it to information necessary for the specific purpose.
4. Maintaining the accuracy of personal data and updating it so that it is not false or misleading.
5. Establishing clear and strict restrictions on the storage of personal data that are strictly necessary for a purpose.
6. Commitment to integrity and complete secrecy in data processing to ensure safety and security ,such as data encryption.
7. Ensuring the accountability of the data controller responsible for collecting, preserving and processing data before the law.

25. Carson, Angelique. (2021). Data privacy laws: What you need to know in 2021.[Osano](#). Retrieved June, 2021.

26. The World Bank. (2019). [Data protection and privacy laws](#). Retrieved June, 2021.

27. Carson, Angelique.Ibid.

28. Welford .Ibid.

The Reality of Privacy and Data Protection in Palestine

Palestinian internet users face challenges on several levels with regard to privacy and data protection. In addition to the violations by international companies that all users are exposed to, Palestinians face Israeli violations and local Palestinian violations. The Israeli occupation controls the Palestinian ICT infrastructure as well as electronic monitoring tools that collect data and violate the privacy of every Palestinian under the pretext of security. At the local level, the absence of a legislative authority capable of enacting laws and legislation that keeps pace with developments in the world of technology, opens the door to violations of privacy and protection of personal data in the public and private sectors. Until now, there is no clear and comprehensive Palestinian personal and digital data protection and privacy law.

The Palestinian Basic Law, which serves as the constitutional framework for the Palestinian legal system, criminalizes attacking the sanctity of private life. According to the law, “every attack on any of the personal freedoms or the sanctity of the private life of the human being and other rights and public freedoms guaranteed by the Basic Law or the law, is a crime in which neither criminal nor civil lawsuits are subject to statute of limitations, and the National Authority guarantees a fair compensation for those who have been harmed.” Efforts on the ground to protect the privacy of Palestinian individuals and preserve their personal information appear to be limited, as the Palestinian Authority has given priority to adopting the cybercrime law despite the deep controversy surrounding it.²⁹

Law 16 on Cybercrime in 2017 was approved by presidential decree in July, but the Palestinian authorities subsequently indicted several journalists based on this law. Although the law was amended in 2018, it still faces strong opposition from Palestinian activists, journalists, and civil society due to its vaguely worded provisions that threaten freedom of expression and the right to privacy on the Internet, and enables the Palestinian authorities to misuse it with the aim of suppressing political opposition and media^{30 31}.

The Cybercrime Law deals with privacy and protection of personal data ,as Article (22) stipulates that:

1. Arbitrary or unlawful interference with the privacy, family, home or correspondence of any person is prohibited.

29. هيومن رايتس ووتش. (2017، 20 كانون الأول). [على فلسطين إصلاح قانون الجرائم الإلكترونية التقيدي](#). تاريخ الاسترداد: أيار/ مايو 2021.

30. المصدر السابق. .

31. عابدين، عصام. (2020). [الحقوق الرقمية في فلسطين بين الطوارئ وجائحة كورونا](#). حيفا: حملة - المركز العربي لتطوير الإعلام الاجتماعي. تاريخ الاسترداد: أيار/ مايو 2021.

2. "Anyone who creates a website, application, or electronic account, or publishes information on the electronic network or an information technology means with the intention of publishing news, photos, audio or video recordings, whether live or recorded, related to illegal interference in the private or family life of individuals even if they are correct, shall be punished by imprisonment for a period of no less than one year, or by a fine of no less than one thousand Jordanian dinars, and not more than three thousand Jordanian dinars, or its equivalent in the legal currency of circulation, or by both penalties³².

In 2019, the Palestinian Council of Ministers in Ramallah issued Resolution No. (3) of 2019 regarding the protection of personal data of Palestinian citizens, provided that it is valid in the West Bank and Gaza Strip. The law consists of two articles that state:

Article 1: It is prohibited to use the personal data (directly/indirectly) of the citizens receiving the service from the companies and institutions that provide it for commercial purposes, without obtaining their prior permission, under pain of prosecution.

Article 2: All competent authorities, each within its jurisdiction, shall implement the provisions of this law by decree, and it shall be enforced from the date of its issuance, and shall be published in the Official Gazette³³.

Perhaps the Palestinian medical data leakage crisis, which was revealed last year (2020), reflects the extent of the chaos that pervades the field of protecting the privacy and personal data of Palestinians. During an online symposium organized by 7amleh on March 29, 2021, within the activities of the Palestine Digital Activism Forum, Dr. Wissam Sbeihat, responsible for the coronavirus medical files in the north of the occupied West Bank, stated that these leaks are controlled by the Ministry of Health's individual behavior, which is one of the challenges that the Ministry of Health is working on. On the other hand, the digital platform on which the results of the corona tests are published on the Ministry of Health website is one of the tools through which the medical privacy of Palestinians can be hacked, as anyone can enter another person's ID number and know the result of their test results directly³⁴.

32. قرار بقانون رقم (01) لسنة 8102م بشأن الجرائم الإلكترونية. المقتفي. تاريخ الاسترداد: أيار/مايو 2021.

33. قرار مجلس الوزراء رقم (3) لسنة 2019م بالبيانات الشخصية الخاصة بالمواطنين. موسوعة القوانين وأحكام المحاكم الفلسطينية. تاريخ الاسترداد: حزيران / يونيو 2021.

34. حملة. (2021). هاشتاغ فلسطين 2020. حيفا: حملة- المركز العربي لتطوير الإعلام الاجتماعي. تاريخ الاسترداد: حزيران / يونيو 2021.

The Privacy of the Palestinians and the Control of the Israeli Occupation

In its report on privacy and protection of personal data in Palestine, Access Now believes that the adoption of a data protection law by the Palestinian Authority will provide only a limited level of protection due to the fact that the Palestinian information and communication technology infrastructure is under full Israeli control since its occupation of the Palestinian territories in 1967. Despite signing the Oslo agreement for peace in 1993, the Israeli authorities still control information, communications and electromagnetic waves, in addition to controlling the import and installation of any equipment by Palestinian telecommunications companies and Internet service providers, for undisclosed “security reasons.” This legal structure and infrastructure has played an essential role in allowing the mass surveillance of Palestinian society and the exploitation of their personal data for decades without any accountability³⁵.

It is worth emphasizing that Israel uses surveillance and espionage techniques, designed specifically to spy on and track individuals, such as journalists, dissidents, and activists, such as “AnyVision” technology, in addition to the cooperation of major international companies that run social media platforms with the Israeli security units on everything related to the Palestinian user, as documented by 7amleh³⁶.

Chapter Three: Study Methodology

The current study adopted a qualitative approach to understand the size and reality of the problem of privacy violations and digital personal data in Palestine that we are dealing with, through in-depth personal interviews with officials directly involved in information technology, and through focus groups that included activists, academics and specialists in this regard.

The Study Sample

The first sample, in-depth personal interviews, where twelve interviews were conducted with experts directly related to the subject of the research, as shown in Table (2) in Annex (1).

35. فطافطة، مروة. وسمارو، ديماء. (2021، 22 آذار). *عُرْضة للكشف والاستغلال: حماية البيانات في منطقة الشرق الأوسط وشمال أفريقيا*. أكسس ناو.

36. حملة. (2021). مصدر سابق.

The second sample, focus groups, where three focus groups participated in the study, from the West Bank, Gaza Strip and East Jerusalem³⁷. Each group included 14 to 16 individuals, male and female digital activists on various social networks, journalists, followers of the issue of privacy and data protection, master's students in the fields of communication, representatives of civil society organizations, human rights institutions, technicians, and experts in programming, big data and e-marketing. Ages of the group members ranged between 22-50 years old. Table (3) in Annex (2) shows the demographic details of the focus groups participants.

Chapter Four: Presenting the Results

Focus Groups

At the beginning of the focus groups, participants were asked a set of questions to determine their knowledge of the concepts of privacy and digital personal data and their protection (Table 1) in general, and then the groups followed the discussion, each according to its geographical and political characteristics.

Table 3: Who answered yes to the closed questions, distributed by groups.

No	Question	West Bank (16)	Gaza Strip (15)	East Jerusalem (14)	Total (45)	The Percentage (100)
1	Do you clearly know what digital privacy means?	10	10	2	22	49%
	Do you clearly know what digital personal data means?	62%	55%	14%		
2	Is there a need to protect personal data and digital privacy?	11	12	8	31	69%
	Does Palestine have a privacy and data protection law?	68%	80%	57%		
3	Do you usually read the privacy policies of websites and applications before using them?	15	13	13	41	91%
		93%	86%	92%		
4	Do you clearly know what digital privacy means?	12	12	3	27	60%
	Do you clearly know what digital personal data means?	75%	80%	21%		
5	Is there a need to protect personal data and digital privacy?	5	6	5	16	36%
	Does Palestine have a privacy and data protection law?	31%	40%	35%		
6	Do you usually read the privacy policies of websites and applications before using them?	16	10	14	40	89%
		100%	66%	100%		

The above table summarizes the responses of the participants in the three focus groups. كل واحدة من هذه المناطق الجغرافية لها خصائصها السياسية التي تتميز فيها ولهذا ستنين لنا صورة أشمل بكل ما يتعلق بالخصوصية والبيانات الشخصية الرقمية.

distributed in the West Bank, Jerusalem and Gaza. The most prominent indicators that we can see in the table include:

- The concepts of privacy and personal data are not clearly understood by the majority of group members.
- A small percentage of group members read the privacy policies of sites and applications before using them, only about a third of individuals read the privacy policies before using sites or applications.
- The majority of participants agree on the necessity and importance of enacting a comprehensive Palestinian law to protect privacy and personal digital data from infringement.
- The East Jerusalem group stood out for its lack of knowledge of the concepts of privacy and personal data and what is legally related to them, in addition to the fact that the majority of the group's members were not aware of the privacy policies of websites and applications before using them.
- As for the Gaza group, while about 90% of individuals agreed that there is a need to enact a law to protect privacy and personal data, around 60% of them encourage the enactment of the law.

The Concepts of Privacy and Personal Data and their Context

The two groups of the West Bank and Gaza did not differ in the definition they gave for the concepts of privacy and personal data, although the definition was insufficient. In addition, the two groups agreed on the importance of data protection and the ease of breaching it, as well as the necessity of citizen consent to use their data. As for the East Jerusalem group, it did not address the concepts of privacy and personal data and their meaning. The groups differed when talked about the contexts of privacy and personal data; when the members of the Gaza and East Jerusalem groups talked about these concepts within the context of the Israeli occupation and its repeated violations, the West Bank group discussed the government agencies' use of their data to improve the quality of services, which they do not see as a violation, unlike the use of this data by private companies with the aim of advertising and marketing.

Violation of the Privacy of Palestinian Users

The groups were asked about the parties that violate the users' privacy according to their opinion and goals. In the West Bank Group, it became clear that government agencies are the most entities violating users' privacy. It allows Palestinian security authorities to access users' personal data. In addition to exchanging data with Israeli security agencies, government agencies do not violate citizens' privacy for security reasons only; they also exchange personal data with private sector companies. The group members summarized that the majority of violations are a result of commercial reasons, then Palestinian political and security reasons, and then Israeli security reasons. The group members expressed their concern about the collection and use of their data and its preservation by telecommunications companies, the financial sector, institutions and ministries. The participants inquired about the official bodies responsible for the information, its collection, its use and its protection.

As for the Gaza Strip group, the most prominent and key parties that breach and violate the personal data of the Palestinians are the Israeli occupation, by following up and monitoring all information related to individuals and the occupation's control over technology. The Palestinian Authority agencies in the Gaza Strip is considered the second most important party violating the privacy of Palestinian users, especially violating the rights of journalists and activists who participate in demonstrations or hostile publications to Hamas authority, as it is the ruling authority, in addition to violating the digital privacy of detainees against whom complaints were filed for opposition to the ruling authority. The private sector companies including the Internet and telecom service providers came in third place. These companies allow the government to access the personal data of users; In addition to using this data for commercial and advertising purposes. Furthermore, group members stated that private external parties are violating the digital privacy and personal data of Gazans for their own personal political interests and ambitions.

The East Jerusalem group did not differ from the other two groups in considering the occupation authorities as a primary party targeting and infiltrating the privacy of Palestinian Jerusalemites, whether for security, civil or commercial advertising reasons. Israel not only violates the digital rights of Palestinians by tracking their movements on official and unofficial websites, but also monitors them with digital and non-digital monitoring and listening devices. East Jerusalem group members indicated that there is coordination between the Israeli authorities and the Palestinian Authority to exchange data for Jerusalem users, which consecutively means targeting them by the Palestinian Authority.

The Role of the Occupation in Controlling the Privacy of the Palestinians

The three groups unanimously agreed on the full control of the Israeli authorities of the Palestinians' data and their continuous and persistent violation of their privacy in order to pursue them politically, civilly and healthily (since the start of the Corona pandemic last year). *The West Bank group* highlighted the tools used by the Israeli authorities to track them, and their obligation to use these tools, for example, the coordinator's application where they had to enter their personal data collected by the Israeli authorities in order to track and prosecute them.

The Gaza group stressed the methods, tools and algorithms used by the Israeli authorities to collect data and use them to assess Gazans socially and psychologically to predict potential resistance members and those who pose a threat to Israel, as they claim. In addition, the Gaza group mentioned Israel's role in blocking and restricting Palestinian content on social media platforms.

East Jerusalem group members unanimously agreed that the level of privacy and protection of personal data for Jerusalemites is zero percent. They stated that one of the main reasons for privacy violations and data exploitation is political and security pursuits. The Israeli authorities' violations of Jerusalemites' data are not limited to political and security goals, as they are persecuting them for health (since the Corona pandemic) and demographics reasons by tracking their phones and personal IDs with the aim of displacing them from their homes in Jerusalem into the Palestinian Authority areas.

Towards a Palestinian Privacy and Data Protection Law

The members of the three groups unanimously agreed on the importance of creating a law that harmonizes the technological development that the world is witnessing to protect and regulate the issue of privacy, including defining privacy policies for each site and service. They agreed that it should be comprehensive and addresses all issues with clear provisions, and defines crimes and their punishment in a way that preserves human rights. It also should not include any exceptions except with a judicial justification, and that it should regulate data collection, processing, sharing or use, and the terms of each process since data collection must have an authorized purpose. There is also a need to provide a mechanism to follow up on the application of privacy policies, and the importance of providing an oversight body for law enforcement. They stressed that the law would contribute to stopping the prosecution of journalists and activists, especially in the Gaza Strip. East Jerusalem group members stressed the importance of users' consent to the use of their data.

The speakers proposed a set of recommendations, the most prominent of which are as follows; The greatest danger is that the problem of privacy violation has been legally legislated with the adoption of the cybercrime law, the need to adhere to achieving transparency at various levels and fields as one of the basic foundations for the protection of digital and human rights, and the existence of a privacy law that leads to achieving transparency and integrity, and that its lack would lead to the contrary. It is also necessary to establish an independent body to manage the telecommunications sector and user data, and to include the telecommunications law with the possibility of imposing fines and penalties on telecommunications companies, and the need to disclose the agreements signed between the Palestinian Authority and the occupation regarding privacy and data protection.

The role of local authorities in enacting a privacy and data protection law

The group members agreed on the urgent need to launch awareness campaigns on privacy and personal data in order to pressure the authorities to enact a law protecting the privacy and personal data of Palestinian users. *The West Bank group* referred to the role of Palestinian civil society organizations in spreading awareness about privacy as well as awareness campaigns for the public about the importance of privacy. Furthermore, the group noted the possibility of establishing a Palestinian authority to protect the privacy and data of Palestinians.

Regarding the formation of an independent body to protect privacy and digital rights, the speakers in the *Gaza Strip group* recommended that a body to regulate dealing with privacy should be found and followed up to work on enforcing the law, and involving the relevant parties to set the law, including: an official, judicial, communications, unions, academic departments, civil society, and all involved actors.

Privacy issues in Jerusalem are unique and there is no Israeli privacy law that includes Palestinians, specifically Jerusalemites, as they are not considered as Israeli citizens, and there is no reliable body that can be resorted to for accountability in the event that an individual is subjected to a violation of their privacy. This is why it is the responsibility of civil society in East Jerusalem to work on educating Jerusalemites about ways to confront privacy breaches and how they should work to protect their personal data. Palestinian journalists in Jerusalem also play a role of educating people about data breaches through the media materials they produce, whether audio, written, visual, or even through their Facebook posts.

Personal Interview Analysis

The Concept of Privacy and Digital Personal Data

Abdeen³⁸ and Jamous³⁹ agreed that the concepts of privacy and personal data are mentioned in the Palestinian Basic Laws in their traditional form without clarification, detail and comprehensiveness of digital privacy. However, it is possible to build on the traditional concept of privacy in that it is a fundamental and inalienable right in Palestinian constitutional rights, and its violation results in a constitutional crime, accountability and compensation for those who have suffered harm, according to Articles 32 and 17 of the Palestinian Basic Law. The two concepts of privacy and digital personal data include preserving the personal freedoms of the individual and the inviolability of the private life affairs of the person, such as one's family, home, office, telephone, and any digital data that may directly or indirectly indicate this.

In light of the digital development of the means of communication, it has become possible to divide the use or abuse of privacy and digital personal data - by in companies, governments, websites, social media, etc. - into three basic stages: the stage of collecting personal data, the stage of processing it, and the stage of its use.

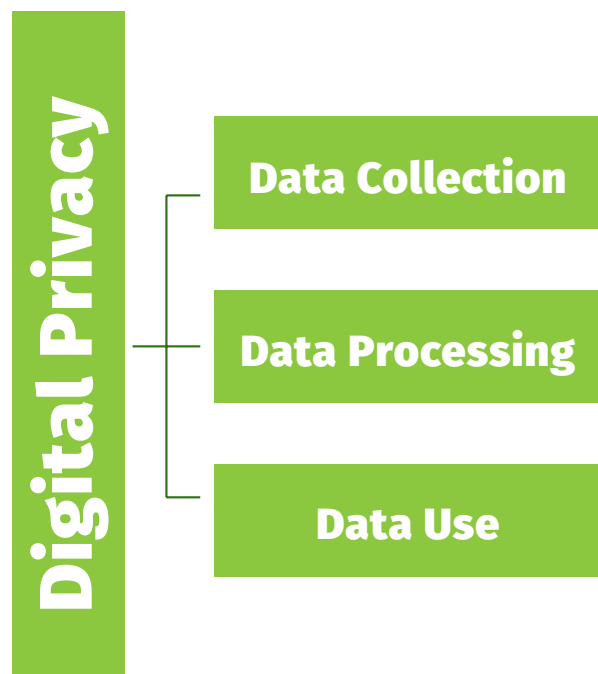


Illustration 1: Stages of the process of assaulting privacy and personal digital data

38. عابدين، عصام. مقابلة شخصية. نيسان، 2021.

39. جاموس، عمّار. مقابلة شخصية. أيار، 2021.

Data Collection Stage

There are many different ways in which personal data is collected, most notably: registration for services and subscriptions (for example, telecommunications companies and banks); Cookie technologies implanted within the Websites⁴⁰; geolocation technologies; mobile; mobile applications; Smart applications such as electronic payment applications, credit cards, and others. The application usually requests access to photos, microphone, studio, and contacts, and this is data that the application collects directly if you agree to the privacy policies, and sometimes information may be collected unintentionally from some parties, because the use of the World Wide Web and applications generates and collects personal data automatically^{41 42}.

The sources of personal data can be divided into two main sources, first: the data that the user declares or records with his consent, such as his personal information and any information that indicates his identity, name, home...etc, second: data that describes user behavior, interests and practices such as browsing, purchasing, search and interests, is usually collected indirectly and without the user's awareness⁴³.

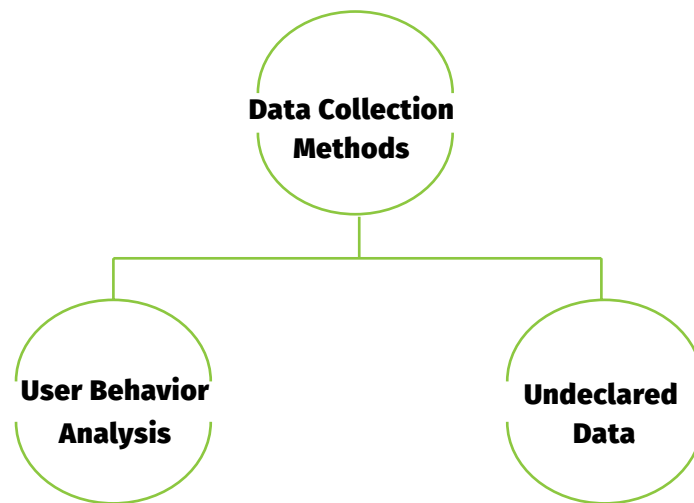


Illustration 2: Sources of personal digital data collected about users

40. يعد الكوكيز الآلية الأساسية في جمع البيانات فهو الطريق لأي عملية تجميع بيانات تحدث على الجهاز، تخبرك بالمواقع، التي زرتها والبيانات التي تخزنها على جهازك ويقوم برصدها، وبالتالي يمكن تخزين خارطة البيانات الخاصة بالشخص بناء على السلوك أو التصرف، فهو عبارة عن هوية تشمل بيانات وسلوك المستخدم.

41. فطافطة، عبد المنعم. مقابلة شخصية. نيسان، 2021.

42. أبو بكر، إبراهيم. مقابلة شخصية. نيسان، 2021.

43. فطافطة، عبد المنعم. مصدر سابق.

Data Processing Stage

Processing the data available to the majority of Palestinian authorities is mostly done to reach general and statistical data and primarily marketing goals, for example, knowing the age group involved in a particular service, the best-selling products, the geographical division of customers or users...etc. However, data processing requires advanced techniques such as artificial intelligence programs and algorithms, which are still not available to the Palestinian public and private sectors, and although some of them work to collect information, they are unable to delve deeper into their analysis and benefit from them remains limited.⁴⁴

Data Use Phase

The stage of data use is a broad and complex stage related to the objectives of each party and its need for available information, and is often used to determine audience specifications to target a specific group for a specific purpose.⁴⁵ The data is used either in the normal and legal framework, or in the context of the illegal violation and exploitation of users' data. It can be asserted that there is no such thing as absolute data protection, but rather there is relative protection that varies and ranges between programs and equipment and between certain parties⁴⁶.

Violation and Exploitation of Personal Data

The violation of privacy and the exploitation of personal data are very important and dangerous issues, due to the availability of huge digital data about each individual, to the extent that helps to impersonate one's personality and know their psychological, economic, social and even political condition⁴⁷. Violation of data privacy can be understood as obtaining customer or user information and data and attacking what is related to the individual's private boundaries, including accessing bank accounts and balances, in order to cause damage and theft, or in a manner that tracks an individual's contacts, exploiting their behavior to set him/her up or spying on him/her^{48 49}. In addition, the risk lies in the confidentiality of sales and

44. أبو بكر، إبراهيم، مصدر سابق.

45. فطافطة، عبد المنعم، مصدر سابق.

46. جبارين، شعوان. مقابلة شخصية. آذار، 2021.

47. فطافطة، عبد المنعم، مصدر سابق.

48. الزيتاوي، إياد. مقابلة شخصية. نيسان، 2021.

49. عابدين، عصام، مصدر سابق.

exchange of personal data that no one knows or has evidence of its violation and exploitation except those who executed and participated in these acts⁵⁰.

On the local level, telecommunications and electronic payment companies and banks violate the privacy of their users when they allow the Palestinian security forces to access the data of customers and users, their behavior and interests without a court order or an official request, as stated by Jabareen⁵¹ during the personal interview we conducted for the purposes of this study. He added that these violations sometimes are for personal purposes related to those responsible for protecting this data. In addition, there is a perversion of citizens' data, which makes it vulnerable to theft and exploitation for personal and political gains. This happened in 2021 when the voter register was breached in some areas of the West Bank in order to manipulate their polling places⁵². The same applies to the leakage of lists of people infected with the coronavirus, which are mainly owned by the Ministry of Health⁵³.

The political events that escalated recently after the killing of the political activist Nizar Banat at the hands of the Palestinian security forces, after which the Palestinians organized huge demonstrations in the Palestinian street to protest against what happened to Nizar Banat and to demand justice for him. These demonstrations were suppressed by members of the Palestinian security forces (in uniform and civilian clothes) and some supporters of Fatah movement in the West Bank confiscated and stole the demonstrators' mobile phones during the oppression of these demonstrations. This consequently led to a breach of the demonstrators' right to privacy, especially after photos and videos for the demonstrators with the aim of inciting and defaming them were published, especially female activists, and limiting their ability and/or preventing them from participating in peaceful demonstrations in the future.

It seems that the most violating entity to users' privacy is the Palestinian Authority and its official institutions. It operates primarily under the cover of the Cybercrime Law, which allows law enforcement agencies to monitor phone lines, eavesdrop on conversations, monitor the Internet, hack and intercept communications, and search and get inside electronic devices and phones⁵⁴. On the other hand, the Cybercrime Law deals with the issue of privacy in some of its articles succinctly and in broad terms. Although this law is considered a good basis to build on regarding protecting privacy and digital personal data, yet some of its texts violate the right

50. جاموس، عمّار. مصدر سابق.

51. جبارين، شعوان. مصدر سابق.

52. عابدين، عصام. مصدر سابق.

53. سمارة، ديمة. مقابلة شخصية. أيار، 2021.

54. جاموس، عمّار. مصدر سابق.

to privacy⁵⁵. Legally, the law is broad and inconsistent with Palestine's obligations to international covenants, human rights treaties, and the International Covenant on Civil and Political Rights. The law contravenes the right to freedom of opinion and expression and the right to obtain information.

The law does not apply in the Gaza Strip where there are special laws that have been amended and approved by the Hamas Legislative Bloc. For example, the Hamas Bloc amended an article in the Penal Code (Penalty Law No. 74 of 36, Article 262 bis) called "the misuse of technology." Thus, everything related to cybercrime and privacy falls under the "misuse of technology". The criticism mentioned about the cybercrime law in force in the West Bank applies to this amendment to, and it leaves the prosecution to interpret the legal texts as it sees fit⁵⁶. The extent of the breach of privacy and the exploitation of personal data in the Gaza Strip is not different from that in the West Bank, and the breach of privacy is not limited to government institutions that allow security agencies to access citizens' personal data, but also individuals with personal relationships and influencers can access citizens' personal data too⁵⁷.

Compliance with Privacy Policies and Protection of Personal Data

Providing privacy policies has become an essential matter for every service, site or application to contribute to protecting the privacy of individuals⁵⁸. However, the problem lies in setting privacy policies that violate privacy rather than maintaining it, and users often agree to them without awareness of their content. According to the current Palestinian law, and since we lack a comprehensive privacy law, once users' consent to privacy policies, the law does not protect them if they consent to the exploitation of their data without their knowledge⁵⁹.

The government agencies regulating the work of the private sector, for example, the Palestinian Monetary Authority, which regulates the work of electronic payment companies, and the Ministry of Communications that regulates the work of telecommunications companies, see that these companies are committed to the basic privacy policies found in their licenses and approved by each ministry. In addition, these parties work to protect the rights of users and their data, determine the technical outsourcing of companies, and prevent the retention of Palestinian

55. عابدين، عصام. مصدر سابق.

56. حماد، حسين. مقابلة شخصية. نيسان، 2021.

57. المصدر السابق.

58. جبارين، شعوان. مصدر سابق.

59. عابدين، عصام. مصدر سابق.

data outside the country. The licenses for such companies are conditional on several procedures that guarantee privacy and data protection. Such procedures is based on the legislation adopted by the Monetary Authority, the conditions of licenses and the Payments Law, where all of this is constantly being developed in order for the services to be in conformity with international standards such as (ISO-International Organization for Standardization) as well as in conformity with the economic agreements with international agencies for providing money transfer services^{60 61}.

The Palestinian Monetary Authority also refuses to have free access to user data in banks and electronic payment companies, or to keep data in an insecure place, because it operates under strict laws and regulations that govern all of this. There is no doubt that the data of users in the banking sectors and electronic payment companies is subject to a computerized system, and in the event of any change or violation, the system detects it easily. Computer systems used and known globally (as Temenos, RTGS, Credit Registry) prevents the sharing of user data with third parties even if the customer agrees to this, and prevent unauthorized access, does not give detailed information about users, and does not allow user data analysis or monitoring their behavior and personal interests. In the event that users' privacy is violated, the Monetary Authority has a system of criminal penalties and financial penalties, such as withdrawing licenses and going to court⁶².

The Relationship between Privacy Law ,Democracy and Human Rights

Jabareen (2021) stressed that the existence of a privacy and data protection law is a strong indicator of a country's democracy, transparency and integrity. The relationship is direct, if there is respect for privacy; it provides a democratic atmosphere that respects human rights and freedoms⁶³. The concept of freedom is closely related to privacy and data protection, since respecting personal freedom and private life and not attacking the freedom of others and their personal data is a fundamental principle in the concept of freedom and human rights⁶⁴. It can be considered that one of the best laws capable of protecting human rights and freedom and preventing their violation is GDPR⁶⁵.

60. أبو بكر، إبراهيم. مصدر سابق.

61. الزيتاوي، إباد. مصدر سابق.

62. المصدر السابق.

63. جاموس، عمّار. مصدر سابق.

64. عابدين، عصام. مصدر سابق.

65. حماد، حسين. مقابلة شخصية. نيسان، 2021.

The concept of privacy in its general form is related to the transparency of the system and good governance, it is actually linked to the system of all human rights, because all rights are linked to data and rights are indivisible. Practically speaking, the privacy and data protection law is supposed to dominate the human rights system, and a national integrity system cannot be built without respect for privacy, and without that, the military and security forces will invade civilian life to end it and turn it into a totalitarian regime⁶⁶. Unfortunately, the Palestinian reality in dealing with privacy and data protection issues depends largely on the concepts of *wasta* and nepotism, and the mistakes committed in this aspect will continue unless a comprehensive and regulating privacy and data protection law is available⁶⁷.

What should be Protected and what should be Made Accessible

It should be noted that the Palestinian Access to Information Law (2021) has not yet been approved, given that it has been proposed as a draft since 2005. It is necessary to understand the essential difference between what information and data must be protected through the Privacy and Data Protection Law and what must be made accessible. The law on access to information stipulates the public data of official bodies and information, statistics, services they must provide, the way they are managed, public money management and everything related to the public and the public interest. Information that can be classified as to national security should be taken into consideration, and global standards for that and what information must be withheld and disclosed^{68 69}. The privacy and data protection law involves the data of individuals, and in the event that the individual does not agree to the transfer of this data from the private to the public sphere, the following question must be asked: Can what happened be considered as a process of arbitrary and unlawful exposure to life and private information or not? An example is the case of health service records provided by the Ministry of Health, which is a public space for everyone, such as knowing the number of people infected with the COVID-19 virus. However, the health record of the individual must be subject to medical confidentiality, and therefore, if medical confidentiality is breached, privacy is breached⁷⁰. The principle is the protection of all data, but the level of privacy is lower for public figures, so dealing with the health status of the president, the prime minister, or a public official is different from a citizen who can file a lawsuit if his privacy is violated and his illness condition is declared without their permission⁷¹.

66. المصدر السابق.

67. جبارين، شعوان. مصدر سابق.

68. عابدين، عصام. مصدر سابق.

69. أبو بكر، إبراهيم. مصدر سابق.

70. المصدر السابق.

71. جاموس، عمّار. مصدر سابق.

Privacy and Data Protection in Palestine from an International Perspective

Samaro (2021) considers that privacy and data protection in Palestine is unique if compared to the international context, due to several reasons, most notably the challenges facing Palestinian society and its use of the Internet. It is actually not possible to talk about privacy and data protection in light of the existence of military laws affiliated with the Israeli occupation authorities that controls the digital space, and the information and communication technology infrastructure, for example, the third generation of the internet (3G) took years to reach the Palestinians at the beginning of 2018 due to the prohibition of the occupation authorities. The Palestinians actually do not have sufficient sovereignty and control over the infrastructure of telecommunications and Internet companies⁷².

In addition, monitoring levels of Palestinian data carried out by the occupation authorities is huge and extensive. According to Haaretz newspaper, the Israeli surveillance operations in the West Bank are one of the largest surveillance operations, so how can the respect of privacy and the protection of personal data be imposed on an occupying country! On the internal level, the internal Palestinian division between the West Bank and the Gaza Strip, the disruption of the Legislative Council, and the inconsistency in the application of the new laws in both parts of the country, hinders the acceleration of the legislation of the privacy and data protection law, and the inability of international organizations and supporting countries to assist in that⁷³.

The Israeli Control over the Privacy of the Palestinians

The mindset of governments is designed to collect as much data on users as possible because they derive all their influence from information, and governments are good at using data⁷⁴. The Israeli authorities have technological superiority, which highlights that major companies working in the field of the Internet and web design are Israeli companies or use Israeli technologies. From a technical point of view, Israel has the technical ability to penetrate the privacy of the Palestinians, and also has the will and desire to do so⁷⁵. It is not possible to underestimate the number of Palestinians who use Israeli telecommunications companies, whether they are forced, such as those living in Jerusalem and the Palestinian interior, or choose to do so such as Palestinians living in the West Bank and Gaza, due to their

72. سمارة، ديما. مصدر سابق.

73. المصدر السابق.

74. عابدين، عصام. مصدر سابق.

75. فطافطة، عيد المنعم. مصدر سابق.

competitiveness compared to Palestinian companies, and as such these companies are somehow able to collect their data and breach their privacy⁷⁶.

The Israeli security monitoring of Palestinian individuals and institutions should be added to these factors, where it monitors and targets the pages of Palestinian human rights organizations on social media and try to distort their image by communicating with their international supporters, as what happened with the Al-Haq and Al-Mizan institutions.

On May 11, Israeli intelligence sent text messages (SMS) to the phones of worshipers in Al-Aqsa Mosque informing them that they had been “classified as participants in acts of violence in Al-Aqsa Mosque, and accordingly the Israeli intelligence will hold them to account later⁷⁷.” This message came mostly as a result of the Israeli intelligence’s use of the GPS tracking system, according to which it determined the geographical location of these worshipers, which is a violation of their right to privacy.

It can be said that Israeli control includes the digital data of the Palestinians through social media, controlling the Palestinian communications infrastructure, knowing all techniques and devices that enter or exit from the borders, the existing surveillance cameras between cities and settlements, whether in the West Bank or inside the green line, and facial recognition technologies in Occupied Jerusalem in particular and at the checkpoints. This gives them the ability to monitor the Palestinians at all times . In Israel, there is a privacy law called the “Personal Data Protection and Privacy Law” that has been in place since 1981, and they also have guidelines for the Israeli Privacy Authority that was established in 2006. However, this law does not apply to Palestinians in Jerusalem, the West Bank, or the Gaza Strip, as they are not Israeli citizens, and it does not apply to the Palestinians inside the green line, in a process of clear discrimination against them⁷⁸.

Of course, there is a possibility to sue the Israeli occupation state for violating the privacy of the Palestinians, but there are basic obstacles, namely, where will it be prosecuted and according to what law? and how will it be proven that it violated the Palestinian data? No one knows anything about its cyber units, especially the cyber unit of the Israeli military intelligence⁷⁹. It can be noted that the Palestinians should focus on attracting international attention to what they suffer from including the

76. حماد، حسين. مصدر سابق.

77. El-Kurd, Mohammed {@m7mdkurd}. (2021). Many Palestinians are receiving this message to their phones. “Hello! You have been identified to have taken part in violent acts at Al-Aqsa Mosque. We will hold you accountable.- Israeli intelligence”. Israel is likely using a GPS system, like the one for corona outbreaks.[Twitter](#). Retrieved June, 2021.

78. سمارو، ديما. مصدر سابق.

79. عابدين، عصام. مصدر سابق.

intrusion and violation of their privacy and personal data at the hands of the Israeli occupation. They should also cooperate with as many international institutions and organizations to pressure towards preserving the rights of the Palestinians. They also should work on training journalists, activists, and human rights experts to focus on privacy issues and the violation of Palestinian personal data. The existence of a Palestinian privacy and data protection law that is in line with international laws and protects individuals and provides justice to them will be a qualitative leap in the discussion of such issues and will draw the attention of the international community to them⁸⁰.

Examples from the Palestinian Private Sector

Due to the importance of the Palestinian private sector in privacy issues and the collection and processing of personal data and their role, this study reviews three models of Private Palestinian companies that provide their services to Palestinians and have a large amount of personal data associated with them. These models give a close look at the reality of privacy and personal data protection in Palestinian companies and the private sector. The models cover three important areas related to the privacy and personal data of users, which are communications, electronic payment, and the provision of Internet services.

Model 1:: The Online Payment Company MaalChat

MaalChat is a Palestinian e-wallet company that provides electronic payment services that enables users to manage payments, facilitate spending habits, facilitate shopping, negotiate and make deals, in addition to transfer and request services. It is a financial technology company that seeks to meet the needs of community members in order to achieve financial inclusion⁸¹.

MaalChat collects the basic and necessary data for subscribing to its services, such as name, ID number, date of birth, etc., as any other organization does, and it is authorized by the user directly and with their permission, and is subject to the customer's approval based on the privacy policy announced on the site or application. Through this data and according to the company's policy and agreements signed with the Monetary Authority it is verified if the subscriber is on the terrorist lists or not. At the present time, it can be asserted that the company does not have customer behavior analysis, due to the lack of a huge amount of data, as well as the need for artificial intelligence techniques such as algorithms, but in the future

80. سمارة، ديماء. مصدر سابق.

81. مالتشات. مالتشات-المحفظة الذكية. تاريخ الاسترداد: أيار، 2021.

it may be possible to identify customers' purchasing trends. It is worth noting that user data can only be accessed by one person who is a controller and custodian of users' data⁸².

Abu Shamleh⁸³ stressed that it is forbidden for an employee within the company to ask about a customer's data, as it is against the internal system on the one hand, and there is no technical ability to access a particular user's data except through the employee responsible for data protection. The system that operates on the company's devices does not give powers to any employee, not even the company manager, who needs a permit to do so; in addition, the system records every process of accessing users' data and can return to it if it is done. No information about subscribers is released unless a court ruling is available, and so far no government agency has requested data without judicial permission.

The data available through the company's application is collectively analyzed to record general and not personal data, and is used in the field of advertisements such as sending messages to the customer if he/she wishes to subscribe to a particular service according to their interest, thus the company sends these messages and does not give the customer's number to any third party. However, at the same time, companies have the right to benefit from customer data in legitimate ways, such as knowing users' behavioral and purchasing trends in accordance with the privacy policy in return for the service they provide to them without forcing them and in a way that legally protects both parties⁸⁴.

Privacy policies are built on the basis of the circulars and laws of the Monetary Authority mainly confidentiality of data and preservation and retention of data records for a long time with regard to users or merchants, and the law provides for the retention of this data for a period of 10 years of the last transaction and there are some details that are related to the company's policy itself and consumer protection agreements. The Monetary Authority plays the role of supervising and controlling data protection and company systems and making sure that it applies their policies and conditions. Sometimes it requests a random sample of the company's subscribers from dealers and agents with numbers without personal information in order to make sure that everything is going legal. However, the Monetary Authority does not always issue instructions about saving and handling the data, the number of people who can see the data, and other details.⁸⁵

82. أبو شملة، محمود. مقابلة شخصية. نيسان، 2021.

83. المصدر السابق.

84. المصدر السابق.

85. المصدر السابق.

Model 2: Call U Internet Service Provider

Call U was established in 2009 to carry out its service activity in the field of providing Internet services in Palestine. The company works with its subscribers through subscription terms that are notified to the subscriber and are available on the company's website. According to Elian⁸⁶ the company's manager, it can be said that there are no privacy conditions within an agreement signed between two parties. The company also has two types of data, first: the subscriber's data, such as the phone number, name, residence, etc., and second: data related to the subscriber's use of the service, which is the hours of use of the Internet.

One of the company's principles is to maintain the confidentiality of users' personal data. The only party that may request information from the company and can be disclosed to is the Public Prosecution by a judicial decision. Usually, an "IP" of a person at a certain hour and who was using it, is requested, since the law compels the company to keep usage data for a period of 3 years; other than that, there is no party with whom privacy data can be exchanged. Note that there are no algorithms to analyze people's behavior, and the company does not know the nature of the use, but only the amount of use. For example, it can be known that one of the subscribers consumed 15 gigabytes of data, but what is inside this data is not known by the company⁸⁷.

Users' data is only available to one employee inside the company, and no one can view it, and this employee has strict instructions and procedures regarding data protection. It is also impossible to see a company screen where complete information about the subscribers is available, as it is encoded so that the employee does not know the name of the subscriber, but parts of their phone numbers to distinguish it, even when a holiday congratulatory message is sent to subscribers, the system creates it and sends it automatically by SMS without looking at the numbers and names. The company also denies benefiting from the data by selling or exchanging it with third parties at all, and the use of user data is limited to quality control and customer service only, such as knowing the service availability for some subscribers. The company pointed to the ministry's limited role in following up on the issue of privacy, which sometimes is limited to a request to view subscribers' data⁸⁸.

86. عليان، رائد، مقابلة شخصية، نيسان، 2021.

87. المصدر السابق.

88. المصدر السابق.

Towards a Palestinian Privacy and Data Protection Law

The importance of having a comprehensive and regulating Palestinian law on privacy and data protection lies in imposing a complete regulation of dealing with privacy and personal data in detail, providing full oversight and protection, and distributing clear tasks and responsibilities, which is consistent with Palestine's commitment to international conventions such as the International Covenant on Civil Rights. On the other hand, it has become impossible to address a basic right of the individual on this scale through general texts and loose legislation, thus the existence of a privacy law that is fully in line with international standards is an essential building block in the institutionalization of a national integrity system⁸⁹.

There is no doubt that the modern situation, the tremendous technological developments, and the shortcomings of previous laws and legislation call for the necessity of enacting such a law, which in turn works to protect citizens from crime, reduce its level in society, and close a legal loophole that used to allow success to personal data of the individual and encourage its violation and penetration without fear of punishment⁹⁰. On the other hand, the existence of a privacy and data protection law constitutes a protection for the parties that own the information (private sector, civil, government) and not only for individuals, so that they know their limits and what is allowed and what is prohibited to work accordingly, but in its absence the company may breach the privacy of individuals without knowing which leads to judicial and other problems⁹¹.

The Council of Ministers Resolution No (3) of 2019, relating to the protection of the personal data of citizens cannot be considered a "law". In terms of the strength of laws and legislation, the constitution comes first, then the law, then the system, and finally, resolutions. Thus, this resolution cannot cancel what is stipulated at the previous higher levels, since the cybercrime law is stronger and higher than this resolution. It is not possible to set penalties and to punish individuals based on a cabinet resolution. The penalty is imposed only by law according to Article (15) of the Palestinian Constitution, except that the penalty is not clear and undefined. Most importantly, a fundamental right cannot be dealt with through a resolution since the right must be institutionalized, through issuing a data protection law for example. Such a law should define the competent authority to follow up on privacy, if it has financial and administrative independence, if it is part of the official structure of the government, the tasks and powers entrusted to it in its dealings with the public and private sectors, the oversight mechanisms that ensure the enforcement of this right,

89. عابدين، عصام. مصدر سابق.

90. جبارين، شعوان. مصدر سابق.

91. أبو شملة، محمود. مصدر سابق.

the complaints system, who monitors the complaints system, the effectiveness of the complaints system and its compliance with international standards.^{92,93}

In the event of striving to harmonize and reproduce the European GDPR in Palestine, there are two important steps that can also be considered as two main obstacles. First, the need to amend local Palestinian laws such as the Cybercrime Law and amend articles that may affect the right to privacy which are fundamentally inconsistent with international agreements signed by the Palestinian Authority. Second: attempting to completely lift the occupation's control over the infrastructure and impose effective sovereignty for the Palestinian Authority, which is a complex matter agreed upon in agreements such as Oslo, specially that the occupation forces the Palestinians to use certain applications that violate their privacy, such as imposing the "coordinator" application on more than 50,000 Palestinian workers who work in the occupied interior⁹⁴.

It is clear from the aforementioned that there is no supervisory body specialized in imposing legal control on private sector companies and/or public sector institutions through a comprehensive regulatory law that details the stages that are supposed to be implemented and followed. Thus, assuming that a punitive provision is enough for judicial authorities to act only if there is a complaint is considered a failure in the application of the concept of privacy and data protection⁹⁵. Jabareen⁹⁶ and Hammad⁹⁷ consider that the level of control over users' personal data is rare and does not receive sufficient attention, and this applies to the reality of the West Bank and Gaza Strip and to governmental and private institutions, and that control should not be only governmental, but must provide civilian oversight to protect citizens' data.

It has also become necessary to enact a comprehensive law that contributes to changing the prevailing societal culture around the habit of violating privacy in Palestinian society. Therefore, the process of enacting the law must be preceded by a process of community awareness of privacy and the protection of personal data, its importance, necessity and ethics. Then the law comes to set a framework for this, to regulate it and deepen the public knowledge of it. Thus, it is not possible to enact a law about that the society knows nothing about, and where practices on the ground are the exact opposite⁹⁸. Therefore, the law must also be issued through the

92. جاموس، عمار. مصدر سابق.

93. عابدين، عصام. مصدر سابق.

94. سمارو، ديما. مصدر سابق.

95. عابدين، عصام. مصدر سابق.

96. جبارين، شعوان. مصدر سابق.

97. حماد، حسين. مصدر سابق.

98. عليان، رائد. مصدر سابق.

legal procedures and channels approved in the enactment of laws and legislation and through a legislative council without the singularity of a governmental or political body over its formulation and determining its content, and after conducting extensive consultations with civil society and relevant private sector companies, since such a law needs to involve all parts of Palestinian society⁹⁹.

Palestinian civil society must put pressure towards the independence of the judiciary, and work to build capacities and skills, mobilize and train activists and actors so that they are able to lead civil society and pressure government agencies to contribute to overcoming the obstacles that prevent the enactment of a comprehensive privacy law and its realistic implementation. It should also work on raising awareness of the issue of privacy and data protection in the community, and implementing media campaigns, lobbying and advocacy campaigns at the local and international levels. This could include forming a coalition of Palestinian civil society organizations to create and increase the public and institutions awareness of the importance of privacy for Palestinians in particular and in the context of the occupation reality which tries to control all Palestinian data in general¹⁰⁰.

Features of the Desired Palestinian Privacy and Data Protection Law

It is possible to summarize some of the main points that the study sample referred to directly or indirectly to depend on ,in addition to basic guidelines to contribute to defining the parameters of a comprehensive Palestinian privacy and data protection law ,taking into account that these points do not negate the role of the judicial and competent authorities and their responsibilities ,but rather sheds light on the most prominent components of the law:

- Having a full commitment to everything stated in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, and the harmonization of all Palestinian legislation, public policies and judicial applications with this commitment and with the European GDPR.
- Understanding and demanding the realization of the principle of the right to digital oblivion and providing the option to delete personal data after finishing or in the event that there is no necessity for its existence. There must be controls to prevent the misuse of data that cannot be erased from the digital archives of institutions, companies and sites, and to impose a penalty on those who may

99. جاموس، عمار. مصدر سابق.

100. سمارو، ديما. مصدر سابق.

violate this and use personal data even after a hundred years. for example, the data of the users of the Palestinian telecom companies is not deleted and we cannot force them to do so without a law, since the current law forces them to keep the users' data after the end of the service

- Giving clear definitions about the independent competent authority concerned with following up the privacy file and personal data in the state, does it have financial and administrative independence, is it part of the official structure of the government, what are its tasks and responsibilities towards the public and private sectors, what are the followed effective oversight mechanisms to ensure respect for this right, and how it would work on developing an effective complaints and penalties system?
- Not using broad and vague terms, the law must be clear and specific, specifying the nature of the law for crimes that may be committed in the context of privacy and personal data and to determine how to deal with them.
- One of the most important elements on which the law must be based is a clear penal system for all crimes that may be committed and ensuring the diversity and severity of penalties so that they are not only financial, as well as providing a system of criminal accountability for the violation of the right to privacy by state employees or private sector companies.
- Establishing strict standards defined by law for those who have permission to save and process data for users.
- Respecting human rights in general, the right to freedom of opinion and expression, the right to access information, and respecting private freedoms and cultures.
- Determining the responsibilities, tasks and conditions of the persons who are supposed to have access to the data of users and subscribers and the specifications of the persons who are able to access this data, and how employees should deal with this personal data.
- Determining the responsibility for supervising the commitment to data privacy, how personal data is dealt with within government agencies and the private sector, how it is used, and persistent follow-up of any cases of privacy violations, and it is usually better not to give broad powers to deal with private data.
- The process of releasing data to any third party must be regulated in accordance with the law and a clear and explicit permission from the data owner himself/herself. It also needs to control what the data owner can be asked to declare

and for what purpose, specially that there are purposes that the owner of the data should not be asked to declare because they are not aware of its damage to their privacy.

The desired Palestinian law, like its European counterpart, should guarantee a set of rights such as: the right to access data, which guarantees the right of users to obtain confirmation if their data is collected or used, to know for what purpose it was used, and to know the identity of the entity that used it. It should also guarantee the right to object, which means the right of users to object to the collection and processing of their data. It should ensure the right to erase and forget data, which means guaranteeing the users' right to request deletion of their personal data when they exit the service or application. It also includes the right to rectification and amendment, which guarantees the right of users to request the amendment and updating of their personal data and to ensure its accuracy. It should also include the right to information that guarantees users' right to receive clear and understandable information about any activity and nature of the use of their data by the entities that own it. It ensures the right to inquiry, which guarantees the users' right to inquire about the objectives of data collection and processing, and their right to know the results reached by those who analyzed the data through algorithms and other means, as well as knowing the decisions that resulted from such analysis.

Recommendations

After delving into the issue of privacy and protection of personal data in Palestine, its reality and what parts are safe in it, this study presents some important recommendations inspired by the discussions of the relevant stakeholders and the analysis of the study sample, and they can be summarized as follows:

- *Forming a Palestinian Commission to protect privacy and personal data and regulate them.*

The need to find an entity that is closer to the status of the general observer of privacy and data protection in Palestine, which enjoys a high level of credibility, whose reference is the Palestinian Legislative Council, and seeks to implement and enforce the law that is supposed to regulate and protect the privacy of Palestinians, and to collect and process their data. For example, the Ministry of Communications should impose strict privacy and oversight policies in consultation with this commission, whereas the General Observer should supervise and monitor compliance with privacy policies within the performance of companies and websites in the public and

private sectors, and in the local and international context. In order to institutionalize this issue, the functions that the authority responsible for monitoring privacy and personal data must perform, its powers, need a control system in place, and a complaints system that allows citizens to claim their rights and report violations of privacy to which they may be subjected, must all be determined beforehand.

What are its powers, what is the monitoring system followed, and the complaints system that allows citizens to claim their rights and report privacy violations that they may be exposed to.

- *7amleh recommends the necessity of enacting a privacy and data protection law, to protect citizens from violations committed against them by various parties, in consultation with civil society and the relevant competent authorities. This should take place after expediting the process for holding legislative elections, because the Legislative Council has the inherent jurisdiction over legislation. Until then, 7amleh demands the application of the constitutional rule stipulated in Article No. 32 regarding all violations of electronic privacy and personal data, which considers any attack on the sanctity of a person's private life a crime for which neither criminal nor civil lawsuits are subject to statute of limitations.*
- *Raising awareness of the issue of privacy and data protection in Palestine, publically and officially*

All concerned parties, including civil society organizations, relevant government agencies and international institutions operating in Palestine, should work to educate the Palestinian public about the issue of privacy and data protection, its importance, dangers, impact and dimensions, and hold seminars, courses and trainings, and call upon experts and technicians to discuss the issue from more technical angles. These efforts should be Institutionalized through studies, research and scientific production, as well as introducing some topics and courses to university students, especially to faculties of media, communication, law and computer science. There should be also calls for research and studies in this aspect and delving into it to study all its aspects, developments and techniques and to compare the Palestinian reality with the global context in the issue of privacy.

On the other hand, this study's recommendations in particular agree recommendations of previous studies in terms of the need for international organizations to carry out their duty towards this issue and to educate the public and users about its dimensions and how to protect their digital privacy and ways to do so, by urging countries to work on joint projects, putting pressure on them to enact such laws. The recommendations also demanded international organizations to impose international sanctions to be implemented on all violators of the privacy law in any country, and to consider this as one of the basics for the establishment of democracies around the world.

Annex:1

Table 2: in-depth interviews sample and their relationships to the topic of the research

No.	Name	Position/Title
1	Iyad Al-Zitawi	Executive Director of the Financial Stability Group and Director of the Risk Management Office at the Palestinian Monetary Authority
2	Abdel Moneim Fatafta	Social media and digital marketing expert
3	Shawan Jabarin	Director of Al-Haq Foundation for Human Rights
4	Ibrahim Abu Bakxer	Head of the Computer Emergency Response Center at the Palestinian Ministry of Communications
5	Hussein Hammad	A representative of Al Mezan Center for Human Rights – Gaza
6	Dima Samaro	Lawyer and digital rights expert in the Middle East and North Africa region ,was previously a Policy Analyst – for the Middle East and North Africa at Access Now
7	Dr .Issam Abedin	Academic and legal expert
8	Raed Elyan	Director of Call You Internet Services Company
9	Mahmoud Abu Shamaleh	CEO of online payment company Maalchat
10	Ammar Jamous	A representative of the Independent Commission for Human Rights and responsible for the privacy and data protection file in Palestine

Annex:2

Table 3: Distribution of the focus group sample

Geographical Area	Number of individuals	Session duration	Male	Female
West Bank	16	2:00	6	10
Gaza strip	15	2:00	8	7
East Jerusalem	14	2:00	6	8
Total	45	6 hours	20	25

Contact 7amleh:

info@7amleh.org | www.7amleh.org

Find us on social media : **7amleh**

