المعهد القومى للملكية الفكرية
The National Institute of Intellectual Property
Helwan University, Egypt

المجلة العلمية للملكية الفكرية وإدارة الابتكار

دورية نصف سنوية محكمة يصدرها

المعهد القومي للملكية الفكرية

جامعة حلوان

العدد الثالث
يوليو٢٠٢٠

الهدف من المجلة:

تهدف المجلة العلمية للملكية الفكرية وإدارة الابتكار إلى نشر البحوث والدراسات النظرية والتطبيقية فى مجال الملكية الفكرية بشقيها الصناعي والأدبي والفني وعلاقتها بإدارة الابتكار والتنمية المستدامة من كافة النواحي القانونية والاقتصادية والادارية والعلمية والأدبية والفنية.

ضوابط عامة:

- تعبر كافة الدراسات والبحوث والمقالات عن رأى مؤلفيها ويأتي ترتيبها بالمجلة وفقا لإعتبارات فنية لا علاقة لها بالقيمة العلمية لأى منها.
- تنشر المقالات غير المحكمة (أوراق العمل) فى زاوية خاصة في المجلة.
- تنشر المجلة مراجعات وعروض الكتب الجديدة والدوريات.
- تنشر المجلة التقارير والبحوث والدراسات الملقاه في مؤتمرات ومنتديات علمية والنشاطات الأكاديمية في مجال تخصصها دونما تحكيم في أعداد خاصة من المجلة.
- يمكن الاقتباس من بعض مواد المجلة بشرط الاشارة إلى المصدر.
- تنشر المجلة الأوراق البحثية للطلاب المسجلين لدرجتى الماجستير والدكتوراه.
- تصدر المجلة محكمة ودورية نصف سنوية.

ألية النشر فى المجلة:

- تقبل المجلة كافة البحوث والدراسات التطبيقية والأكاديمية في مجال حقوق الملكية الفكرية بكافة جوانبها القانونية والتقنية والاقتصادية والادارية والاجتماعية والثقافية والفنية.
- تقبل البحوث باللغات (العربية والانجليزية والفرنسية).
- تنشر المجلة ملخصات الرسائل العلمية الجديدة، وتعامل معاملة أوراق العمل.
- يجب أن يلتزم الباحث بعدم إرسال بحثه إلى جهة أخرى حتى يأتيه رد المجلة.
- يجب أن يلتزم الباحث بإتباع الأسس العلمية السليمة في بحثه.
- يجب أن يرسل الباحث بحثه إلى المجلة من ثلاثة نسخ مطبوعة، وملخص باللغة العربية أو الانجليزية أو الفرنسية، فى حدود ٨ ـ ١٢ سطر، ويجب أن تكون الرسوم البيانية والإيضاحية مطبوعة وواضحة، بالإضافة إلى نسخة إلكترونية Soft Copy، ونوع الخط Romanes Times New ١٤ للعربى، و١٢ للانجليزي على B5 (ورق نصف ثمانيات) على البريد الالكتروني: ymgad@niip.edi.eg
- ترسل البحوث إلى محكمين متخصصين وتحكم بسرية تامة.
- في حالة قبول البحث للنشر، يلتزم الباحث بتعديله ليتناسب مع مقترحات المحكمين، وأسلوب النشر بالمجلة.

مجلس إدارة تحرير المجلة	
أ.د. ياسر محمد جاد الله محمود	أستاذ الاقتصاد والملكية الفكرية وعميد المعهد القومي للملكية الفكرية (بالتكليف) - رئيس تحرير المجلة
أ.د. أحمد عبد الكريم سلامة	أستاذ القانون الدولي الخاص بكلية الحقوق بجامعة حلوان والمستشار العلمي للمعهد - عضو مجلس إدارة تحرير المجلة
أ.د. وكيل المعهد للدراسات العليا والبحوث	سكرتير تحرير المجلة
أ.د. جلال عبد الحميد عبد اللاه	أستاذ الهندسة الانشائية بكلية الهندسة بالمطرية بجامعة حلوان - عضو مجلس إدارة تحرير المجلة
أ.د. هناء محمد الحسيني	أستاذ علوم الأطعمة بكلية الاقتصاد المنزلي بجامعة حلوان - عضو مجلس إدارة تحرير المجلة
أ.د. وزير مفوض/ مها بخيت محمد زكي	مدير إدارة الملكية الفكرية والتنافسية بجامعة الدول العربية - عضو مجلس إدارة تحرير المجلة
اللواء أ.د. عبد القدوس عبد الرزاق العبيدلي	رئيس مجلس إدارة جمعية الامارات للملكية الفكرية - عضو مجلس إدارة تحرير المجلة
Prof Dr. Alexander Peukert	أستاذ القانون المدنى بجامعة جوته فرانكفورت أم ماين – ألمانيا - عضو مجلس إدارة تحرير المجلة
Prof Dr. Andrew Griffiths	أستاذ القانون التجارى بجامعة نيو كاسل - بريطانيا - عضو مجلس إدارة تحرير المجلة

المراسلات

ترسل البحوث إلى رئيس تحرير المجلة العلمية للملكية الفكرية وإدارة الابتكار بجامعة حلوان
جامعة حلوان - ٤ شارع كمال الدين صلاح - أمام السفارة الأمريكية بالقاهرة -جاردن سيتى
ص.ب: ١١٤٦١ جاردن سيتي
ت: ٠٢ ٢٥٤٨١٠٥٠ + ٢٠ محمول: ٢٠١٠٠٠٣٠٠٥٤٨ + ف: ٠٢ ٢٧٩٤٩٢٣٠ +
http://www.helwan.edu.eg/niip/
ymgad@niip.edu.eg

Is the legal protection of digital privacy enough in Egypt ? " Protection of Digital Data Privacy "

Ossama Ahmed Attalla

Is the legal protection of digital privacy enough in Egypt ? " Protection of Digital Data Privacy "

Ossama Ahmed Attalla

Introduction

The digital era upends many traditional privacy safeguards. People now have little protection against spying by foreign countries. Privacy advocates recognize the need to plug this loophole. Privacy on personal data issue has recently emerged and becoming an increasing concern due to the way the government and private companies collect and process privacy on personal data.

Digital economy is huge and rapidly increasing and it is predicted that digital economy would contribute to the national economy.

Since the advent of a digital society with online accounts, organizations that harvest user data which have amassed tremendous powers, The conversion of information to digital form has subverted legal safeguards, because data now moves over arbitrary paths; its location in transit and in storage is often unpredictable or unknown[1].

Our identities are the most valuable thing we own. They are a form of wealth: identity capital. We should expect our identities to be protected from embezzlement and exploitation. Unfortunately,

[1] Stephen J. Schulhofer, An international right to privacy? Be careful what you wish for, Oxford University Press and New York University School of Law, 2016, p 239.

both staggering breaches of privacy take place and personal data is used for corrupt purposes.[1]

Privacy is a very broad topic, which expands to include many relative aspects of human life. This paper focuses on the importance of sufficient legal protection regarding online data privacy in Egypt with the focus of personal data. It is also confined with the effectiveness and strength of this protection. Also, we show the current state of the privacy-preserving techniques in Egypt in 3 parts: first section speaks about general meaning of the right to privacy, second one deals with types of infringement on this right in online data protection and third one discovers the data privacy protection serviced in Egypt.

Section One
Definition of the Right to Privacy

Privacy can be understood as the right of every individual to separate aspects of their private life from the public domain. When we talk about digital privacy we refer to this privacy protection in the field of cyberspace.

Currently, this right to privacy is being put to the test, since both governments and the private sector are taking advantage of technology to access the most intimate sphere of citizens, not always with justifiable objectives. For this reason, it is mandatory to be vigilant and safeguard ourselves from any abuses.

[1] Goldstein, Keith, Shem Tov, Ohad and Prazeres, Dan The Right to Privacy in the Digital Age, April 9, 2018, p5 .

Privacy is traditionally seen as the possibility for an individual to retain some form of anonymity in his or her activities and to have the ability to isolate oneself in order to best protect his or her interests. It is intimately linked to the notion of freedom . But the fact shows that this notion tends to disappear in favor of the control of information[1].

Some scholars argue that there are seven different types of privacy, including privacy of the person, privacy of behaviour and action, privacy of personal communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space and privacy of association (including group privacy)[2]. As such, all of these types need to be considered when formulating privacy protections.

Digital Privacy is a collective definition that encompasses three sub-related categories; information privacy, communication privacy, and individual privacy[3]

Privacy protection does not only include contemplated provisions, but also encompasses technical, technological and administrative measures enshrined to stop violation. Also, the major concern here is to find the legal mechanism for seeking redress.

---

1 Privacy in digital world: beyond compliance, towards trust, Wavestone ed, 2016, p10.
https://www.wavestone.com/app/uploads/2017/01/privacy-digital-world-compliance-trust.pdf.pdf

2 These seven types of privacy were first elaborated in an annex prepared for the PRESCIENT D1 report, available at http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1---final.pdf

3 Hung, Humphry; Wong, Y.H. (2009-05-22). "Information transparency and digital privacy protection: are they mutually exclusive in the provision of e-services?". Journal of Services Marketing. 23 (3): 154–164.

Tech company like Facebook or Twitter is accused of data breach, it used to aggregate, and monetize information about us when we voluntarily share it with them[1].

Our identities are abused by companies who track customers to sell products, interest groups who manipulate social media to shape elections, and governments that seek omnipotent powers. Online businesses are often multinational and can hide between borders. Neither small organizations nor large governments can be trusted to restrict themselves. The right to privacy in the digital age demands a united, multinational alliance that will ensure all individuals in the world share an inalienable right to protect their identities

There is no opportunity for the users of social networks to express their desire **to accept certain parts of the privacy policy while rejecting others**. Even were users able to do so, however, privacy policies can be changed at any time, making even the most informed user vulnerable to sudden, unexpected and unilateral changes in privacy by the social networking providers[2]. It has been suggested that this complete volatility in dealing with private data is as "if tenants had no rights to privacy in their homes because they happen to be renting the walls and doors. This week, you are

6.https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html.

2 Electronic Privacy Information Center. (2011). Social Networking Privacy. Retrieved December 13, 2011, from https://epic.org/privacy/socialnet/.

allowed to close the door but, oops, we changed the terms-of-service[1]

It has been documented that both Google Android and Apple iPhone smartphones regularly, transferring information about their location, their user and other potentially personal information such as Wi-Fi networks in range across the Internet[2]

The mobile Internet service provider, device manufacturer, operating system provider and app providers all have a certain level of control over user personal data.[3]

It has been noted by a US Government Privacy Working Group: "These benefits, however, do not come without a cost: the loss of privacy. Privacy in this context means 'information privacy,' an individual's claim to control the terms under which personal information – information identifiable to an individual – is acquired, disclosed and used."[4]

From initial registration of Internet users through Internet service providers or at Internet cafes, to numbering and

1 Tufekci, Zeynep. (2010), Facebook: The Privatization of our Privates and Life in the Company Town. Technosociology: Our Tools, Ourselves. Retrieved December 13, 2011, from http://technosociology.org/?p=131.

2 Angwin, Julia, & Valentino-Devries, Jennifer. (2011). Apple's iPhones and Google's Androids Send Cellphone, Wall Street Journal. Retrieved December 13, 2011. http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html.

3 Mendel, Toby. Puddephatt, Andrew. Wagner, Ben Hawtin, Dixie. Torres, Natalia. Global survey on internet privacy and freedom of expression, UNISCO series on internet freedom, 2012, P36.

4 Gates, J., & Privacy Working Group. (1995). Privacy and the National Information Infrastructure: Principles for Providing and using Personal Information. Information Policy Committee, Information Infrastructure Task Force. Retrieved from http://aspe.hhs.gov/datacncl/niiprivp.htm.

identification of Internet devices which are themselves often linked to Internet accounts, to individual IDs which are provided by browsers or stored as cookies, as well as the IP-Addresses which are assigned to Internet users through Internet protocols. All of these identification procedures may serve to make an Internet user less anonymous, but in some cases these identities may also be necessary for provision of services on the Internet. It is difficult to use the Internet without an IP-Address – although of course an IP Address can be assigned dynamically or anonymised – and many other Internet services rely on some form of identification.

Cookies are stored on the computer of an Internet user when they visit a website, and the user's Internet browser. Depending on how this website is constructed and the settings of the Internet user's browsers, anything from one to a dozen cookies can be stored or updated when visiting a website. By storing cookies on users' computers, each user can be tracked across the Internet. Particularly in the case of cookies which are set outside of the domain which the user is visiting – so-called third party cookies – these cookies can 'follow' users across most parts of the Internet. Cookies also form a component of user analytics, a common practise for user tracking across the Internet[1].

Credible estimates suggest that between 40 and 60% of the largest Internet websites use Google Analytics, a traffic tracking tool that allows website administrators to gauge their traffic. Of all Internet websites, similar estimates suggest that close to 70% use

[1].Cookies: What you need to know and how they work, https://www.kaspersky.com/resource-center/definitions/cookies

some kind of user tracking based on various different Internet analytics packages.[1]

Adware also fits into the category of privacy-invasive and consent-ignoring software, which is inadvertently stored on computers. This software is very difficult for users to recognise, as the software tends to masquerade as an anti-virus program, a search tool or a similar 'useful' technology that the user would want to use. It is often also bundled with software that seems to be free. However it is instead used to show unwanted advertisements to the user and track their computing behavior.

Limits of digital privacy:

It is noted that people has become more aware of their privacy on personal data since their personal data is being collected, distributed and disseminated without their prior consent by businesses.

Mistrust towards such companies can be attributed to the amount of data they collect and use on individuals, as well as recent high-profile prosecution cases related to such use. However, this result reveals a paradox. Despite this evident lack of trust, individuals continue to frequently use the services provided by these actors, due in part to a lack of alternative, as well as the information entrusted seeming to be, often wrongly, harmless and insignificant in the eyes of the individual.[2]

[1] Mendel, Toby and et, op.cit., P40.
Google Analytics Usage Statistics - Websites using Google Analytics. BuiltWith.com, Retrieved December 13, 2011, from http://trends.builtwith.com/analytics/Google-Analytics.
[2] Privacy in digital world: beyond compliance, op.cit., p21.

The limits of privacy can be disputed, understanding that it is not an absolute right. It is the discussion that arises when the authorities request access to certain personal information, to the companies, for a criminal investigation.

With the increased terrorist threat in recent years, governments have invaded, to some extent, the private space of their citizens, with the excuse of national security. It is important that we, as a society, have to be careful and have to define the limits of this invasion in order to avoid violation of this fundamental right.

There are also cases where we decide to give up certain aspects of our privacy, to get something in return. For example: when we buy online, we use a public Wi-Fi, etc … But in some cases we are not aware of what we are giving or to whom. To avoid these abuses is for what is legislated in this regard.

"General Data Protection Regulation" (GDPR), is defining "the right to be forgotten" or the right to oblivion, which gives citizens the possibility of requiring companies to delete their personal data in certain circumstances.

In conclusion, the concept of privacy is evolving and adapting to the new technological reality. All the actors involved are regulatory bodies, companies and users.

Is digital privacy a right or privilege for individuals? The answer depends on various factors, including regional regulations, geography, culture, and financial agreements between users and

services. These are just a few of the considerations that may influence one's viewpoint on the desirable, expected and demanded level of digital privacy.

Definition of Personal Data

According to the GDPR, personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;[1]

Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data and falls within the scope of the GDPR. Personal data that has been rendered anonymous in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymised, the anonymisation must be irreversible.

Section 2
Infringement Forms of Digital Data Privacy

[1] Art. 4 GDPR
The GDPR protects personal data regardless of the technology used for processing that data – it's technology neutral and applies to both automated and manual processing, provided the data is organised in accordance with pre-defined criteria (for example alphabetical order). It also doesn't matter how the data is stored – in an IT system, through video surveillance, or on paper; in all cases, personal data is subject to the protection requirements set out in the GDPR....This regulation states that'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed; [Article 4 (12)]

Privacy incursions occur frequently, affecting our search and digital behaviour patterns. These incursions are not only about a person or in this case a user – they can also affect a group, a family, a community. [1]

As one of the many examples of privacy infringement, Businesses commit activities based on data automation and collection and so encroach on our privacy.[2]

Our digital privacy is at risk in unprecedented ways[3]. Personal data can affect our reputations, it can be used to exercise control over us and in the wrong hands, it can cause great harm. People need a partner to safeguard their identity and defend them

[1] The Pegasus software allowed the Mexican Government to spy on human rights defenders, journalists and anti-corruption activists. In this specific case of government sponsored cyberattacks, the WhatsApp feed of the son of a prominent lawyer and civil right journalist was the target of intrusion and privacy infringement (New York Times 2017).

[2] The latest scandal involves Facebook users and Cambridge Analytica researchers mishandling the data of over 40 million users. The dubious data gathering tactic included the use of Facebook Graphs API (application program interface) "that makes possible all the interconnectivity and the data delivery Facebook boasts when claiming that the platform was building a web where the default option is sharing" What is worrisome is that FB claims that its interface is based on the pretence that users are in control of what it is shared. In actuality, Facebook users have next to no control what is covertly shared about them – meaning the information and metadata others can extract....Governments and militant organizations utilize internet censorship to shape the public's beliefs and curb dissent. From the most developed countries to the least, examples are prevalent of bloggers, activists, and political opponents being harassed and silenced.

see Albright, J. (2018). The Graph API: Key Points in the Facebook and Cambridge Analytica Debacle Accessed on line at: https://medium.com/tow-center/the-graph-api-key-points-in-the-facebook-and-cambridge-analytica-debacle-b69fe692d747

[3] Sydell, Laura. "FTC Confirms It's Investigating Facebook For Possible Privacy Violations" NPR. March 26, 2018: https://www.npr.org/sections/thetwoway/2018/03/26/597135373/ftc-confirms-its-investigating-facebook-for-possible-privacy-violations

from nefarious actors. They need help identifying the important elements of their digital life that need to be kept private and secure[1].

Online piracy is one of the most common type of assaults on Data privacy which necessarily include copyrighted works .[2]

Data privacy is a crosscutting matter applicable to all sectors, including IP. IP practitioners deal constantly with the collection and handling of personal data – and many of them are not sure how to handle them properly.

Technologies as artificial intelligence advanced computing power and sophisticated data analysis tools to gather and store data in cost-effective ways and then mine these data for economic, social, and commercial intelligence, Big Data has become the new oil fuelling the evolution and growth of the new digital economy.[3]

The most popular types of Data Breach are cyber attacks [4], Theft or loss of devices[1], Employee data theft or data leak, Human errors[2], Phishing[3], Insider threat.

---

[1] Digital Privacy and the Right to be Protected, https://www.nortonlifelock.com/blogs/research-group/digital-privacy-and-right-be-protected

[2] Rantou, Maria, 'The growing tension between copyright and personal data protection on an online environment: The position of Internet Service Providers according to the European Court of Justice', European Journal for Law and Technology, Vol. 3, No. 2, 2012

[3] . Shaw, Jonathan, 'Why "Big Data" Is a Big Deal': [Harvard Magazine March-April 2014] http://harvardmagazine.com/2014/03/why-big-data-is-a-big-deal. Accessed 10 May 2019.

Munir, Abu Bakar and Mohd Yasin, Siti Hajar and Muhammad-Sukki, Firdaus, Big Data: 'Big Challenges to Privacy and Data Protection' (May 21, 2015). [International Scholarly and Scientific Research & Innovation 9(1) 2015] https://ssrn.com/abstract=2609229 Accessed 11 May 2019.

4 Cyber attacks is one of the most prevalent forms of data breach since the attacker needn't be physically present on your business premises to steal your data. The ways in which cyber criminals try to gain access to your systems are becoming more sophisticated. Often it isn't always obvious that an attack has taken place until significant damage has been done. Cyber attacks can come in

While most organizations focus on external threat factors, insiders pose a more significant threat than any one can imagine. According to an Insider Threat study by CA(cyber attack) Technologies and Cybersecurity Insiders, 53% of organizations faced insider attacks[4].

Beside these traditional forms of breaches, I believe that processing Data and Controlling it[5]may become, in some extent, a type of privacy invasions nowadays[1].

---

various forms, including denial of service, malware and password attacks. All a cyber attacker needs is a computer with internet access and a couple of hacking tools to grab your data without your knowledge. Hackers use malware, phishing, social engineering, skimming and related techniques to gain access to protected information. Data breach by cyber-attacks can go on for months or even years without anyone noticing, especially if the hacker did his/her job well. Often, the intrusion is discovered when the damage has already been done, i.e., after the data breach has taken place.

This is called also Unlawful interception of email or telephone communications or online form submissions

[1] This includes Loss or theft of a physical file or electronic device containing personal data and Loss of a decryption key relating to securely encrypted personal data

[2] Human error, for example (1) an email attachment containing personal data being sent to the incorrect recipient or records being deleted accidentally (2) Sharing of passwords or other credentials with third parties(3) Controlled documents being left unattended to be copied, read or photographed by an unauthorised person

[3] 'Blagging' whereby an individual obtains personal data by deception.

[4] Know Your Enemy: The 5 Different Types of Data Breach, https://readwrite.com/2019/08/12/know-your-enemy-the-5-different-types-of-data-breach/

[5] The data controller is any natural or legal person which has the function of obtaining personal data and determining the way, means and standards of preservation, or processing and controlling according to the specified purpose or activity. In GDPR and other privacy laws, the data controller has the most responsibility when it comes to protecting the privacy and rights of the data's subject, such as the user of a website. Simply put, the data controller controls the procedures and purpose of data usage. Data controllers must be responsible for and able to demonstrate compliance with the GDPR's principles GDPR, art. 5.https://www.i-scoop.eu/gdpr/data-controller-data-controller-duties/

Because the same concern, GDPR lays out seven guiding principles for the processing of personal data. While these principles are not "hard and fast rules" themselves, they inform the interpretation of the GDPR and its more concrete requirements.

1 - Lawfulness, fairness, and transparency
2 - Purpose limitation
3 - Data minimization
4 - Accuracy
5 - Storage limitation
6 - Integrity and confidentiality (i.e., data security)
7 - Accountability

Egypt does not have at this moment a definite law which regulates protection of personal data or sensitive data. Also, There is no national authority responsible for data protection in Egypt, or

[1] In the GDPR, Data Processing is a range of processes based on personal data for the interest of the processor or on the interest of controller by agreement with him and under his instructions the processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
The data processor is the third-party company that the data controller chose to use and process the data. The third-party data processor does not own the data that they process nor do they control it. This means that the data processor will not be able to change the purpose and the means in which the data is used. For instance, Sterling Company has a website that collects data on the pages their visitors visit. This includes the page they enter the site with, the pages that they visited next, and how long they stayed in each page. Sterling Company is the data controller, as they decide how all of this information is going to be used and processed, and for what purpose. Furthermore, data processors are bound by the instructions given by the data controller. Sterling Company uses Google Analytics to find out which of their pages are most popular and which ones are making Web site visitors leave. This helps them plan their content better by knowing exactly how much time each visitor spends on a particular page. Not only does Sterling Company know which topics to write on, but also discover new topics that might be of interest to their customers. Plus, it helps them improve on the content that is already there. Sterling Company needs to share the data that they get to Google in order to get the insights they want from Google Analytics. In this case, Google Analytics is the data processor.

even requirement in Egypt for organizations to appoint a data protection officer.

Section 3
Legislative Confrontation of Data Protection

The Egyptian Constitution issued in 2014 Article (57) provides that internet security is considered an essential part of the economic institution and national security and that the state is responsible for taking any required measures to maintain said security as regulated by the law. However, Egyptian law does not have any specific provisions which regulate online privacy.

There are some Scattered provisions in connection with data protection in different laws and regulations in Egypt as follows[1] :

1 - The Banking Law, which stipulates that all bank customer accounts, deposits, trusts, safes, and their related dealings must remain confidential, except with the written permission of:

- the owner of the account, deposit, trust, or safe;

- the account owner's successors, anyone to whom all or some of such funds have been bequeathed; or

- a legal representative or authorised attorney or pursuant to a judicial ruling or an arbitral award. (Article 97.)

2 - The Egyptian Civil Status Law (Law No. 143/1994), which provides for the confidentiality of citizens' civil status data (Article 13).

3 - The Competition Protection Law, which imposes confidentiality obligations on its officials and employees, relating to all information related to individuals and corporations (Article 16).

[1] Abdel-gawad, Mohammed AND Elewa, Yomna, Data protection in Egypt overview, practical law, 2019 , p2.

4 - The executive regulations of the Mortgage Finance Law, which provide for the confidentiality of client data of mortgage finance companies related to the relationship (Article 35bis(6)).

5 - The Egyptian Telecommunication Regulation Law, which provides for the privacy of telecommunications and imposes penalties for infringement of its regulations.

6 - Article no. 50 of the Civil Law no. 131\ 1948 sets forth the right to halt any infringement to privacy and asking for remedy[1].

7 - Articles (309 bis) and (309 bis A) from the Egyptian penal code criminalize the violation of an individual's private live without their permission.

8 - The Egyptian law of combating cyber crimes no. 175 in the year 2018.

9 - Regarding Privacy on personal data according to Labour Law. The Labour Law protects employee personal data (such as name, job, professional skills, workplace, domicile, marital status, salary, employment starting date, holiday leave, workplace sanctions, and employee reports) and states that: employers must keep employee personal data for at least one year from the end-date

[1] Every person who was subject to an unlawful infringement to one of the rights inherent to his personality is entitled to demand the cessation of such infringement and the compensation of the prejudice suffered by him.

of the employment relationship; and only authorised individuals should have access to personal employee data[1].

10 - Also, the Penal Code provides sanctions for disclosing, facilitating the disclosure of, or using a recording or document obtained by any of the following methods: recording or transmitting via private conversations or telephone by any method; or shooting, taking, or transmitting a picture of anyone in a private place by any means, without the consent of the photographed party[2].

The dictated crimes and sanctions are not sufficient to counter the current breaches of privacy which bypass the traditional types of violations until the data protection law draft passes. The draft will be examined practically through operational application to test whether or not has covered all conceivable criminal activities on line regarding violating privacy.

11 - The Egyptian Civil Code grants general protection against the infringement of private data on the basis of Tort liability, if the data subject suffers damages.

However, the Egyptian Parliament has discussed(the "Data Protection Draft Law"), which has been under discussion since 2017 and is expected to be promulgated soon.

The Data Protection Draft Law aims to capitalize on Article (57) of the Egyptian Constitution and shall be in conformity to its

[1] (Article 77)
[2] (Article 309)

provisions to safeguard personal data and information of users/consumers.

The draft is totally inspired by the GDPR, The EU's General Data Protection Regulation, as it is stated in the preamble of the Joint Committee report upon the draft presented by the Egyptian Government[1].

Data Protection Draft Law provides, principally two types of data: (i) Personal data, which includes any data relating to an identified natural person or one who can be identified directly or indirectly by way of linking personal data to another such as: a name, a voice, a picture, an identification number, an online identifier, or any data which determines the psychological, physical, economical or cultural identity of that person; (ii) sensitive data, which includes data relating to mental, physical or psychological health, genetic data, biometric data, financial data, religious beliefs, political views, criminal records, and children's data.

Data Protection Draft Law excludes the following data from its scope of application and law enforcement: Personal data processed for the national census or legal compliance; Personal data that natural persons hold and process for personal purposes; Personal data that national security authorities and Central Bank of Egypt hold; and Personal data relating to law enforcement reports and public prosecution investigations, including terrorism and other criminal cases.

[1] See the Report of the Joint Committee composed of communication and information technology committee and legislative and constitutional, planning, budget , defence and national security committees, p8.

The Egyptian data protection law draft defines the processing of Data and the **Definition of a Data Controller in article no.1.**

The data controller will be the one to dictate how and why data is going to be used by the organization. A data controller can process collected data using its own processes. In some instances, however, a data controller needs to work with a third-party or an external service in order to work with the data that has been gathered. Even in this situation, the data controller will not relinquish control of the data to the third-party service. The data controller will remain in control by specifying how the data is going to be used and processed by that external service.

Obligations of Data Controllers and Processors[1]

Accountability and enforcement are key to the success of the protection of personal data. Every law should clearly define data controllers and processors, the parties responsible for complying with the law, and provide clear responsibilities, obligations, and liability for both. The law should also address the relationship between controllers and processors and specify clear requirements as to what is expected of each of them. Controllers and processors should also be subject to record-keeping obligations, security obligations, and data breach notification requirements.

[1] The Keys to Data Protection, a Guide for Policy Engagement on Data Protection, August 2018, p 72 .
https://privacyinternational.org/sites/default/files/2018 09/Data%20Protection%20COMPLETE.pdf

The principle of accountability puts the burden on data processors to prove that they fulfill their obligations under data protection, including the requirements to keep a record of all processing undertaken under their authority, and to keep that record up-to-date.

Data controllers and processors are responsible for ensuring that they take all necessary measures to ensure that they comply with the law. It is not enough that they comply with the law, but they must clearly illustrate how they are compliant to demonstrate, that processing is performed in accordance with the law.

Data controllers and data processors should implement appropriate technical and organizational measures to ensure, and to be able to demonstrate, that processing is performed in accordance with the law[1].

Controller Obligations

In addition to the Core data protection principles, the Draft Law imposes a number of explicit obligations on controllers of personal data, according to article no. 4.

There are also some obligations for **processor stipulated in article no 5, for example :**

- ensuring that the objectives of any personal data processing are legitimate and do not offend against public order or morality;

[1] chapter3, article 4 of the law draft, and Art. 32 GDPR

- delete or return personal data to the controller once the purposes of the processing have been achieved;

- not carrying out any processing outside the controller's specific instructions unless for statistical or not-for-profit educational purposes;

- compile and maintain a "Personal Data Log", detailing the categories of personal data, the identity of those who have access to the data, relevant retention periods, any restrictions imposed on processing data, procedures for deleting and/or updating data, technical and organisational measures used to secure the data and any cross-border transfers of data;

- obtain any necessary licence(s) or permit(s) from the PDPC to process personal data.

- keep records of processing activities.

The law should provide security safeguards not only to protect the data itself, but the obligation of protection should be expanded to include the devices and the infrastructure itself used at every stage of processing including generation, collection, retention and sharing (i.e. data at rest and data in transit)[1].

The GDPR also requires controllers and processors to implement technical and organizational measures to ensure a level of data security that is "appropriate to the risk" presented by the

1 • the pseudonymisation of personal data • the encryption of personal data • a guarantee of ongoing confidentiality, integrity, availability and resilience of processing systems and services • the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident • a process for regularly monitoring and evaluation as well as audit of the effectiveness of technical and organisational measures for ensuring the security of the processing, including privacy by design and effectiveness of Data Protection Impact Assessments (DPIAs).

data processing. In implementing data security measures, organizations must consider the "state of the art, the costs of implementation," the nature, scope, and context, and purposes of processing, and the likelihood and potential severity of an infringement on individual rights if data security were to be violated. The GDPR does not impose a "one-size-fits-all" requirement for data security, and security measures that are "appropriate" (and therefore mandatory) will depend on the specific circumstances and risks. For example, a company with an extensive network system that holds a large amount of sensitive or confidential information presents greater risk, and therefore must install more rigorous data security protections than an entity that holds less data.

The Cyber security law, the Anti-Cyber and Information Technology Crimes[1], No. 175/2018 includes some general provisions governing the confidentiality of personal data. Until the new Data Protection Law is enacted, the use and disclosure of personal data is governed by the anti cyber crimes law which is published in the *Official Gazette* on August 19, 2018, consists of 45 provisions. Among them, The Cyber security Law provided that service providers are under a duty to maintain the privacy of the

[1] The law aims at fighting extremist and terrorist organizations that use the internet to promote their ideas among youth. The Law also bans the online dissemination of information on army and police movement and criminalizes hacking into information systems. For this sake, article 2 requires telecommunications companies to retain and store users' data for 180 days in order to assist the authorities in identifying users, metadata, and computer IP addresses. Article 4 of the Law obliges the Ministries of Foreign Affairs and International Cooperation to reach bilateral agreements covering Internet Technology (IT) and cybercrime with as many foreign governments as possible to block some websites in foreign countries. Article 7 grants the investigative authorities the power to block any website whenever they deem that the website's content promotes extremist ideas that violate national security or damages the Egyptian economy.

data stored and not disclose it without a reasoned order from a relevant judicial authority[1]. This duty includes personal data belonging to one of the consumers or any data or information on the websites and personal accounts used by the consumers or the persons or bodies with whom they communicate.

This law has penalized many activities which include Data breach in articles no. 14 : 26.

Under the current draft, sanctions include imprisonments, financial sanctions, or both. regulated in articles from no. 35 to 49.

But, there is something remaining regardless of the issuing or enacting the data protection law, which is the non-existence of the awareness of the complete theory of the right to privacy and the implications resulted in violations upon it which cause basically and supposedly, filing tort liability proceedings pertaining digital privacy breaches. Actually, there is no recorded case against service provider, data controller or regulator at courts which is based on tortuous liability grounds.

That means one of both explanations: the first is the lack of digital awareness in the field of digital privacy. The second potential reason is losing of the legal basis to file this kind of cases but, we are not convinced with the latter reason as the civil liability based on tort theory is profound and broad to cover all aspects of violations.

For now, I strictly believe that the reason of lack or missing data breach civil cases is the technical issues which burden, obstruct and block any online user from filing these kinds of cases.

[1] (Article 2).

When seeing the repeated events of massive data breach in the developed world, and consequent class actions thereof, it is meaning that the third developing world is lagging behind and do not have the privilege to seek relief from the substantial damages of overwhelming rapidly evolving technology.

Notification of Data Breach Requirement

The primary purpose of data breach notification laws is to ensure that if personal information belonging to platform users and service consumers is compromised, then the **target of the breach** is under obligation to duly notify any person whose data has been leaked.

A good analogy is to say that in the case of Facebook, these laws only take into account the cybersecurity "walls" surrounding Facebook's databases, because they only recognize the **security perimeter** above the surface. What these laws fail to understand, is that there are tunnels underneath the surface accessing Facebook's databases, where personal information is being extracted from almost unrestrictedly. If our current laws are unable to characterize similar incidents as data breaches, then they are missing their purpose [1].

Data breach notification regime under the current draft is regulated for the first time in the draft data protection law that would not require notification or registration before processing

[1] See, e.g., Aaron Smith, Americans and Cybersecurity, PEW RESEARCH CTR. (Jan. 26, 2017), http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/ ("This survey finds that a majority of Americans have directly Experienced some form of data theft or fraud, that a sizeable share of the public thinks that their personal data have become less secure in recent years, and that many lack confidence in various institutions to keep their personal data safe from misuse

personal data. Now also , notification or registration is not required before processing data[1].

Under the draft data protection law, data collection or processing is only legal if the data subject's consent is obtained or as otherwise authorised by law. For the collection or processing of sensitive data, the draft law specifies that this consent must be express. For sensitive data of children, the consent of the child's guardian must be obtained. In all cases, an authorisation must be obtained from the regulator for the processing of sensitive data.

It is noted that the notification is required when the regulator or the controller aware of any data breach. What if the violator is the regulator or controller himself ? what is the situation if the infringement is coming from inside the company or organization where the regulator or the controller belongs to. So it is notably important to discuss the distinction between active and passive cyber attacks.

In Active cyber attacks, victims immediately become aware of when they occur. Active attacks are highly malicious in nature, often locking out users, destroying memory or files, or forcefully gaining access to a targeted system or network. Viruses, worms, malware, Denial of Service attacks, and password crackers are all examples of active cyber attacks.

[1] The notification requirement under the current draft obliges the controller or processor, upon becoming aware of any personal data breach, to notify the centre of personal data protection within 24 hours from the date of the accident, which in turn, notifies immediately the national security entities, and is obliged to inform the centre within 72 hours from the date of notification. Such notification must also. (Article 7)

While Passive cyber attacks often employ non-disruptive and covert methods so that the hacker does not draw attention to the attack. The purpose of the passive attack is to gain access to the computer system or network and to collect data without detection. Many data security breaches involving the exposure of credit card and debit card payment information are the result of passive attacks, as are data breaches where the targeted data collected during the attack is user name, passwords and other personal identifying information. Information that is gathered in a passive cyber attack is usually sold on the blackmarket and dark web for the financial gain of whoever perpetrated the passive attack[1].

Conclusion:

With the amount of data growing exponentially, there is little doubt that it will change the world in the coming years in ways that we can scarcely imagine today. Processing reliable data can help discover certain trends, which can contribute to reducing the waste of resources and improve policy-making. However, data can also be used to put people under complete surveillance, in breach of their fundamental rights In an interconnected electronic world.

This is why the protection of personal data is so crucial. Safeguards are necessary to give citizens and consumers trust in administration, business and other private entities. If data are the new currency, we need to learn the painful lessons of the banking industry – weak regulation and excessive faith in the market will

[1] DiGiacomo, John, Active vs Passive Cyber Attacks Explained, February 14, 2017, https://revisionlegal.com/internet-law/cyber-security/active-passive-cyber-attacks-explained/

lead to catastrophic loss of trust, with consequences for every single citizen.

It is well established that a good law needs good enforcement. Effective and predictable levels of enforcement will serve to enhance and preserve the area of privacy protection. It will also serve to transform consumer expectation of privacy from a hope to a demand.

due to the huge opportunities offered by developments such as social networks, “Big Data” and cloud computing, it is crucial to get the full benefit from these developments , also citizens need to trust them. For this trust to be realised, privacy needs to be built into every stage of the design process – privacy by design – as well as every stage of the implementation process – purpose limitation and privacy by default.

We need to expose the ability of using class actions as a way to cover online privacy breach, and therefore trying to find the legal basis dedicated to get relief.

The paper concludes that the current Egyptian legal system is covering many aspects of data breach when taking in account the Cyber Crime Law, but not sufficient to impose comprehensive protection on internet privacy until the data protection law draft passes. After that, the given protection will substantively be embedded in a wide extent to the awareness of digital privacy and its horrible risks along with integrated procedural protection with regard to the enforcement.

The need for issuing the draft expressly appears in some critical points which are fatal in providing comprehensive

protection like Data breach notification, framing sensitive personal data, and the strict multiple obligations upon controllers and processors

However, the current status of the draft is not totally satisfying as there are some shortcomings regarding the range of exceptions for the scope of application and law enforcement.

The hotly debated Data Breach Class Actions are overarching demonstration evidence showing the quantitative and qualitative online data breach regardless who committed the violation a service provider, data controller or processor . To sum up, these kinds of litigations force the violated companies to rectify and reorganize their measures and policies which lead to the question of why we do not have these kind of cases in Egypt?

References

Books and Articles

- ✓ Aaron S. , (2017) Americans and Cyber security, PEW RESEARCH CTR.
- ✓ Albright, J. (2018). The Graph API: Key Points in the Facebook and Cambridge Analytica Debacle Accessed on line .
- ✓ Angwin, J., & Valentino-Devries, J. (2011). Apple's iPhones and Google's Androids Send Cellphone
- ✓ BuiltWith. (2011). Google Analytics Usage Statistics - Websites using Google Analytics. Retrieved
- ✓ Electronic Privacy Information Center. (2011). Social Networking Privacy.
- ✓ Ramirez, E. (2017), Fed. Trade Comm'n, Opening Remarks at Privacy
- ✓ Gates, J., & Privacy Working Group. (1995). Privacy and the National Information Infrastructure:
- ✓ Hung, Humphry; Wong, Y.H. (2009). "Information transparency and digital privacy protection: are they mutually exclusive in the provision of e-services?". Journal of Services Marketing..
- ✓ Goldstein K. Dr. Shem O. , and Mr. Prazeres, D. (2018) The Right to Privacy in the Digital Age.
- ✓ AbdelGawad, M. AND Elewa, Y. (2019) Data protection in Egypt overview, practical law.

✓ Munir, Abu Bakar and MohdYasin, Siti Hajar and Muhammad-Sukki, Firdaus, (2015), Big Data: 'Big Challenges to Privacy and Data Protection'.

✓ Sydell, Laura. (2018) "FTC Confirms It's Investigating Facebook For Possible Privacy Violations" NPR.

✓ Tufekci, Z. (2010), Facebook: The Privatization of our Privates and Life in the Company Town.

✓ Mendel, T. Puddephatt, A. Wagner, B. Hawtin, D. Torres, N. (2012) Global survey on internet privacy and freedom of expression, UNISCO series on internet freedom.

✓ The Keys to Data Protection, a Guide for Policy Engagement on Data Protection, August (2018).

✓ Techno sociology: Our Tools, Ourselves. (2011).

✓ PRIVACY IN THE DIGITAL WORLD: BEYOND COMPLIANCE, TOWARDS TRUST, (2016).

Journals:-

✓ Rantou, M. I, 'The growing tension between copyright and personal data protection on an online environment: The position of Internet Service Providers according to the European Court of Justice', European Journal for Law and Technology, Vol. 3, No. 2, 2012

✓ Shaw, Jonathan, 'Why "Big Data" Is a Big Deal': [Harvard Magazine March-April 2014.

✓ Stephen J. Schulhofer, An international right to privacy? Be careful what you wish for, Oxford University Press and New York University School of Law, 2016.