Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 5, (page 203 - 212), 2021
DOI: https://doi.org/10.47405/mjssh.v6i5.780

Malaysian Journal of Social Sciences and Humanities (MJSSH)

Volume 6, Issue 5, May 2021

e-ISSN : 2504-8562

Journal home page:
www.msocialsciences.com

Privacy in the Era of Big Data: Unlocking the Blue Oceans of Data Paradigm in Malaysia

Atiqah Binti Azman[1], Nur Shaura Azrin Binti Azman, Nurul Sahira Binti Kamal Azwan, Sherie Aneesa Binti Johary Al Bakry, Wan Nur Afiqah Binti Wan Daud, Hartini Saripan, Nurus Sakinatul Fikriah B.T. Mohd Shith Putera
[1]Faculty of Law, Universiti Teknologi MARA, 40450, Shah Alam, Malaysia

Correspondence: Atiqah Binti Azman (atiqahazman37@gmail.com)

Abstract

Big Data has revolutionized the process of online activities such as marketing and advertisement based on individual preferences in the eCommerce industry. In Malaysia, the integration of Big Data in the commercial and business environment is keenly felt by establishing the National Big Data Analytics Framework catalyzing further economic growth in all sectors. However, the distinct features of Big Data spawn issues relating to privacy, such as data profiling, lack of transparency regarding privacy policies, accidental disclosures of data, false data or false analytics results. Hence, this research provides an insight into the intersection between Big Data and an individual's fundamental rights. The trade-off between privacy breaching and preserving is becoming more intense due to the rapid advancement of Big Data. Suggesting comparative analysis method as the data analysis approach, the adequacy of the Malaysian Personal Data Protection Act 2010 (PDPA 2010) in governing the risks of Big Data is evaluated against the European Union General Data Protection Regulation (GDPR) in managing the risk arising from the integration of Big Data. This research is hoped to initiate the improvement to the legislative framework, provides fundamentals to the formulation of national policy, and creation of specific law on Big Data in Malaysia, which will subsequently benefit industrial players and stakeholders.

Keywords: big data and law, big data and data protection laws, Personal Data Protection Act 2020

Introduction

The International Trade Administration (2020) reported that in 2020, around 80% of the Malaysian population were active internet users. Its research identified as well, that 62% of mobile users usually use their device to shop online and more than 50% of Malaysian use their device to shop online. Big Data is becoming prominent in the e-Commerce industry and contributes to storing, processing, and interpreting massive volumes of data. More mundanely, Big Data is used to analyse and collect information of its users from various online platforms for the benefits of business online industries. Generally, Big Data is defined as "a large volume of high velocity, complex and variable data that requires techniques and technologies to enable the capture, storage, distribution, management and analysis of information" (Abu Bakar Munir & Siti Hajar Mohd Yasin, 2012). However, a comprehensive definition of Big Data is absent as each organisation assign different interpretation of this technology (Andrea et al., 2016). For instance, the Organization for Economic Cooperation and Development (OECD), defines Big Data as data that transcends the processing capacity of

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 5, (page 203 - 212), 2021
DOI: https://doi.org/10.47405/mjssh.v6i5.780

conventional database systems where the data is too large to be reasonably operated by the current traditional technologies (OECD Secretariat, 2016). Big Data is also comprehended as a gigantic digital dataset created inside a company or corporations for business operations, which are then extensively analysed using computer algorithms (Auffray et al. 2016). Regardless of the unavailability of a uniformed definition, its usage in eCommerce amplifies companies' performance, increasing the company's value chain rates a 5–6% higher efficiency in the industry (Barocas and Selbst, 2016) (McFee & Brynjolfsson, 2012).

Literature Review

Tambe (2014) states that companies investing in Big Data, yields higher labour productivity levels and customer responsiveness as Big Data facilitates the returns of management practices (Avinash and Akarsha, 2017). Merchants are also able to trace individual user's behaviour and maintain the number of regular customers in the online business with advertisements through Big Data. Big Data heightens company growth and productivity in various functional areas of the eCommerce industry such as marketing, human resources management, production and finance (Akter & Wamba, 2016). It is especially crucial in the online business industries as the activity of retailing and wholesaling products requires a significant volume of data to be processed for better growth of the company. Thus, it supports human development and rights, as it creates entirely new industries, infrastructure and markets depending on their labour costs. Big Data also assisted developing and developed countries to thrive in the eCommerce industry due to its need for more significant decision-making when dealing with large amounts of customer-related information. For example, in China, because of its highly concentrated market, eCommerce emerges as the leading domain application of Big Data. Taobao 's marketing practise is a good example of using Big Data for marketing purposes. According to Beyond Summits (2019), the peak time of online users is usually before 12 noon, therefore, a great number of Taobao sellers exploit its consumptive features to carry out promotional activities at midnight, which could improve sales. In the United States, Big Data is becoming the interlink that merges physical retail and e-Commerce stores. In 2016, the e-Commerce industry in the United States alone, achieved sales revenue of 322.17 billion US dollars (Singh, 2018). Meanwhile in Indonesia, Big Data plays a very important role in the e-commerce world, starting from consumer analysis to product innovation. This analysis is useful in providing an overall framework, such as consumer profiles, and what potential can be derived from these consumers. Capitalising on Big Data's disparate features, the implementation of consumer data is collected, and their interactions are carried out on eCommerce websites and analysed in order to maximise sales (Anugerah and Indriani 2018). In Singapore, companies are making big waves in eCommerce through the help of Big Data, for instance, Y Ventures foresees trends for retail brands across 28 online markets, such as Amazon, Lazada and Qoo10 using data analytics (Weizen, 2017). In Malaysia, the adoption of Big Data is at its infant state.

This is seen through the missions held by Malaysia Digital Economy Corporation (MDEC) is equipped with another task that is to build a national Big Data Analytics (BDA) to promote economic growth in all industries and to expand local market access in the eCommerce industry to the global stage, (National e-Commerce Roadmap, 2019). MDEC has an objective to create a robust BDA industry, to make BDA a demand in all industries, including the public sector. MDEC has the vision to produce an outcome of stimulating advancement in the IT industry, increase workplace efficiency and to enable the people to garner benefits of having a robust BDA. Big Data technologies are significant for Malaysia's digital economy as it is critical for the delivery of efficient citizen services, innovation growth and added value in industries (Sharon, 2019). This is in line with Malaysia's vision as an eCommerce hub to attract digital and technological investments. For instance, the collaboration between Fusionex International Plc and Alibaba Group to provide e-Services, a digital trade facilitation platform powered by Big Data as opportunities for SMEs to access global consumers via e-commerce in Malaysia (Samantha, 2018). Nevertheless, the ground-breaking impact of Big Data to the commercial industry comes at a cost. The distinctive character of Big Data could easily be susceptible to privacy and security issues. Sheer volume of large scale data which contains valuable and sensitive information belonging to a company makes it a more appealing target to hackers and will subsequently lead to a potential opportunity for cybercriminals (Thi Mai Le and Shu-Yi Liaw, 2017). The most

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 5, (page 203 - 212), 2021
DOI: https://doi.org/10.47405/mjssh.v6i5.780

targeted data usually in the form of personal information, credentials consists of logins and passwords as well as card payment information. These data seized by cybercriminals will be then sold to another company resulting in widespread data loss of people. In 2018, Marriot International Inc the owner of Starwood Hotels and Resorts reported an authorized access to the database of Starwood guest reservation, where there were a number of personal information of their customers has been encrypted and copied. Such information consists of the names, phone numbers, email addresses, passport numbers and also Starwood Preferred Guest's account information. The Marriot International Inc then was fined amounted to £99,200,396 (a maximum fine in General Data Protection Regulation [GDPR] limits) for breaching the privacy of their customers and the data protection law (Gromenko, 2017).
The British Airways faced a similar issue when the airline company was fined nearly $230 million as result of their poor security, allowing hackers to transfer approximately 500,000 customers visiting its website to a deceitful website where their personal information such as names, addresses, payment details were disclosed (Satariano (2019). Meanwhile in Malaysia, the risk of Big Data is reflected in the case of Basheer Ahmad Maula Sahul Hameed v PP [2016], where the two accused who were the husband and wife (in which the wife worked in a bank) were found guilty for using a debit card owned by a victim from an airplane accident to withdraw some cash as well as they were guilty for an unauthorized transfer of money from other victims' online banking account. Furthermore in 2019, Malindo Air discovered a data breach of its passenger, committed by their former employees of its eCommerce contractor. The news was made public after a Moscow-based cybersecurity firm, Kaspersky Lab, reported that the data of almost 30 million of the passengers of Malindo and Thai Lion Air were posted in online forums for sale on the Dark Web (Bernama, 2019). The nature of Big Data that frequently contains huge amounts of personal data identifies information of the users itself has triggered the privacy issues of the users.

This is due to the fact that the use of Big Data enables the data users to identify patterns and trends which may predict people's dispositions, for example, matters related to health, interests, political viewpoints or sexual orientation. The creation of Big Data therefore permits organizations to create information about data that were never apparent or originally intended in the source information. Big Data involves the reuse of data which leads to the repurposing of data. This technology has the ability to discover valuable knowledge through various personal data where bigger data sets are placing the principle of purpose limitation on edge. According to this principle, organizations which use collected personal data as a basis for predictive analysis must ensure that the analysis is compatible with the original purpose for collecting the data (Norjihan Abdul Ghani et al., 2016).

This is where most data users are on the grey line whether the data they discovered are fully for the original purpose or they have already violated the retention principle. It is still debatable as to what extent the data will be a use for the original purpose. In addition, they mentioned that Big Data also repurposes data that is obtained for a different purpose and in some cases by another organization too. This means considering how the new purpose affects the privacy of the individuals concerned and whether it is within their reasonable expectations that their data could be used in this way. Big Data has prompted issues relating to privacy such as data profiling, lack of transparency regarding privacy policies, unplanned disclosures of data, false data or false analytics result. In eCommerce, it is inevitable that there is a need to collect and use the consumer's personal data (Rubeinstein, 2013). There is no doubt that the personal data may be used by business owners for their own interests as a way to control the market. In most online transactions, consumers will need to leave their personal data and these traces of consumers' personal data will be left on the web in various ways. This indirectly causes leakage of consumers' personal information online (Tchao et al., 2017). Moreover, this also concerns the right of the users when using the World Wide Web for their transaction. There is an ever growing threat to the rights and freedoms of individuals, particularly in respect of their data considering the potential repercussions of processing a huge amount of data (Ajibade, 2018). It is also foreseeable that the owner which controls the large amount of data is likely to be exposed to risk of cyber threats and data leakage (Zarsky, 2017). Massive amount of data resources and powerful data analytic techniques make traditional ways of protecting individual's privacy no longer effective (Qing Tan & Frederique Pivot, 2015). With such personal information made available for the benefit of the society, abuse of data is inevitable. Hence, the present research charts the intricacies of the adoption of

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 5, (page 203 - 212), 2021
DOI: https://doi.org/10.47405/mjssh.v6i5.780

Big Data to the existing data protection law in Malaysia, challenging the adequacy of the current legal framework in addressing the risk posed by Big Data.

Methodology

This research is a doctrinal research centralising on data collection, that deliberates on the development of legal doctrines, construes and organises laws relevant to Big Data. The library-based search and document review of secondary sources were conducted by categorising the literatures into several themes: 1) The Intersection of Big Data and Law 2) Data Protection Laws 3) Big Data and the Concept of Privacy. Suggesting comparative analysis method, the adequacy of the Personal Data Protection Act 2010 (PDPA 2010) in governing the risks of Big Data was then evaluated against the European Union General Data Protection Regulation (GDPR). The EU's GDPR was chosen given its status as one of the leading countries at the forefront of regulating Big Data, setting a global standard for other countries. The comparative analysis has shed lights in understanding Malaysian data protection and privacy law as a whole and its inadequacy that affects data subjects personal information. This understanding can be achieved through comprehensive research on privacy laws, cases and scholars that has emphasised on the risk of Big Data without proper governance, given the absence of technology-specific law governing Big Data in Malaysia.

Result

This research identified that Big Data negates the working principle of data protection embedded in PDPA. The right to privacy is a multi-dimensional concept, and striking the right balance in terms of protection is essential. Finn et al. (2013) states that privacy is best defined when an individual can sustain his personal information free from others' invasion. Therefore, it can be seen that privacy is something that can be evaded by others which cause annoyance and invasion of personal space and information. These metaphors illustrate different concepts of privacy that can be found in numerous standards in theories of privacy, according to (Pardo & Siemens, 2014). Scholars consider privacy to be related to confidentiality which can be breached upon, such as contracts or trust. However, based on Hummerick (2018), privacy in Big data is a difficult concept that scholars are in disagreement in terms of a specific and unified concept of privacy as what they have on the law of torts. Regardless, people are voluntarily willing to disclose their private and personal information, photographs on social media websites and personal info in the eCommerce platform, an act which is facilitated by the advancement of accessibility provided by technologies. In Malaysia, there is no express recognition of a right to privacy within the Constitution or in any legislations. However, privacy protection becomes one of the most affected area with the progress of Big Data as human privacy is usually challenged by the development of technology. The Personal Data Protection Act 2010 (PDPA 2010), which came into force on 15 November 2013, sets out a comprehensive cross-sectoral framework for the protection of personal data concerning commercial transactions. The PDPA 2010 is a key enabler to strengthen consumer confidence in electronic commerce, and business transactions gave rise to the rising number of cases of credit card fraud, identity theft and selling of personal data without customer consent (Kandiah, 2019). Before the PDPA 2010, data protection obligations were spread out among certain sectoral secrecy and confidentiality obligations, while personal information was primarily protected as confidential information through contractual obligations or civil actions for breach of confidence.

The European Union General Data Protection Regulation (GDPR) sets a number of data protection principles that drive compliance. These principles outline the obligations that organisations must adhere to when they collect, process and store an individual's personal data. The seven principles of GDPR provide organisations with a guide on how they can best manage their personal data and achieve compliance with the GDPR. The first principle is lawfulness, fairness and transparency, possibly the most important and emphasises total transparency for all European Union data subjects. The second principle is purpose limitation where the data can only be used for the designated purpose and must not be processed for any other use, unless the data subject has provided their explicit consent. Next is data minimisation where the organisations should only store the minimum amount of data

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 5, (page 203 - 212), 2021
DOI: https://doi.org/10.47405/mjssh.v6i5.780

required for their purpose. The fourth principle is accuracy whereas personal data must be accurate, fit for purpose and up to date. Fifth principle is storage limitation which once the data processor no longer needs personal data for the purpose for which it was collected, it should be deleted or destroyed unless there are other grounds for retaining it. Sixth principle is integrity and confidentiality, which data processor must ensure that all the appropriate measures are in place to secure the personal data they hold. The final principle is accountability and this a new principle under the GDPR, which states that data processors must take responsibility for the data they hold, and they must demonstrate compliance with the other principles. Under the PDPA 2010, there are 7 principles that the data user needs to comply with to protect the right of the data subject. The principles are General Principle, Notice and Choice Principle, Disclosure Principle, Security Principle, Retention Principle, Data Integrity Principle and Access Principle (Protection 2010). Big Data has caused considerable frictions to these principles specifically with the General Principle, Notice and Choice Principle and the Security Principle which are the translation of the Principle of Lawfulness, Fairness and Transparency Principles, Purpose Limitation Principle and Security Principle embedded under the GDPR (Quinn and Quinn 2018).

Under the GDPR, the Lawfulness, Fairness and Transparency Principles, have provided how the controller and processor are required to process personal data to secure the integrity and transparency of personal data. The goal is to administer data processing to ensure that it is fair and lawful (Information Commissioner's Office 2018). In order to ensure the administration of data is fair and lawful, there must be communication with the data subject regarding the object and purpose of data collection. This subsequently elevates the data subjects' awareness regarding the usage of their data by the data processor's. The principle of lawfulness on the other hand propel to gather the data subjects' consent regarding one or several purposes of data usage. In realising the purpose of these two principles, the government ought to introduce stricter transparency obligations and a tighter definition of consent (Rubinstein, 2013). Other than that, the Lawfulness, Fairness and Transparency Principles are relatively connected to the Purpose Limitation Principle. If the controller uses the data for unfair, unlawful or 'invisible' reasons, the controller has breached these principles. Article 6(1)(b) of the GDPR provides that the collection and processing of personal data are restricted for a "specific, explicit and legitimate" purpose (Zarsky 2017). In other words, the data subject's consent is only said to be freely given if such data is used for the right purposes. This indirectly helps the data users to know the link between the specific purpose for which the collection of data and the real purposes for processing the data. However, Big Data applies the principle of "letting the data speak for itself" where the system will first collect all kinds of data and then find the purpose for those data (Wastermann, 2018). This is contrary to the Purpose Limitation Principle as the controller should first have a specific purpose and consent for the collection before it occurs. Notwithstanding this, the situation is possible under Recital 33 of GDPR where data subjects' consent to extensive processing of data is permitted only for scientific research purposes and no other purposes. Hence, eCommerce companies with the intention of researching for future marketing are only allowed to collect information from consumers within a limited scope. This is because an unnecessarily broad purpose might even be considered as "illegitimate" and thus lead to unacceptable processing (Zarsky, 2017). However, the position under Malaysian law differs in terms of the method to govern Big Data. The general principle under Section 6(1) PDPA 2010 provides that a data user shall not process any personal data about a data subject unless the data subject has given his consent to the processing of personal data. The processing of personal data must be necessary and directly related to that specific purpose, and personal data is sufficient but not excessive. The most vital prohibitions in the General Principle are the act of processing personal data without the consent of the data subject.

In this context, the PDPA 2010, fails to define consent. Broadly, consent is defined as a freely given informed sign that the data subject indicates his approval of his data being processed (Abu Bakar Munir & Siti Hajar Mohd Yasin, 2012). In getting consent, the data user has to notify in advance regarding the data processing and its purpose to the data subject, which falls under the Notice And Choice Principles. Section 7(1) of the PDPA 2010 requires the data user to inform the data subject through a written notice. The data user must bear in mind that consent, once granted, will not last forever (Abu Bakar Munir & Siti Hajar Mohd Yasin, 2012). Section 38 of the PDPA 2010 states that a data subject may withdraw his consent by notice, in writing data. The data user shall receive the notice and stop the processing of the personal data. The processing of personal data must only be for a lawful

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 5, (page 203 - 212), 2021
DOI: https://doi.org/10.47405/mjssh.v6i5.780

purpose. Notice, on the other hand, may suggest disclosure to an accessible data repository and possibly more efficient than individual notice. Although the changes in the new approaches to data protection are burdensome, the Notice and Choice Principles require improvement to ensure effectiveness. In cases of data withdrawal, there is little guidance on the effect of such withdrawal of consent from data subjects, but the data user may have to delete the personal data of the data user in question if the withdrawal of consent is made under the right to be forgotten and right to erasure (Berman, 2013). However, it should be noted that such rights are not governed under PDPA 2010. Still, the value of personal information is ambiguous at the time of receiving the notice and consent. This restricts the future use of the said data, and it would require second consent from every individual. It is not only impractical to do, but it is too costly to undertake such actions. These realities challenge the most primary privacy mechanism of notice and consent. This method may expose individuals' privacy for the other users to access, as it will force individuals to make drastic manipulative decisions according to the information in a short time that may cause a long-term implication (Cate & Schönberger, 2013). As data is vital in the eCommerce industry, the conception of information security, which includes integrity, availability, confidentiality and system resilience under the GDPR ensures the customer's trust when using the e- Commerce platform.

The European Commissioner has revised the GDPR to include several protective measures for the security of the data to counter the security concerns introduced by Big Data (Storr & Storr, 2017). The GDPR has mandated that processors and controllers to enforce technical safeguards geared towards scope, nature, purposes and context of data processing in accordance with the effects it has on the freedom and rights of individuals under Article 32 of GDPR. Under Article 33 and Article 34 of the GDPR, notifications on data breaches are mandatory. According to Hoofnagle et al. (2019), if there is a data breaches, the controllers must document all the breaches, even those that do not require the notifications to the users. As for notification, the controller must inform the user through a public communication or similar nature. However, if the cost of individual notification is disproportionate, the controller must notify data subjects through a public communication or similar measure (Hoofnagle et al., 2019). This directly shows that the right to be informed of any data breaches exists under GDPR. Although, it may be inefficient as the data subjects may not receive the information via public communication. Nevertheless, it is commendable that the data users are compelled to take those steps to inform the data subject of the breaches. Conversely, the Security Principle under the PDPA 2010 requires the data controller to take practical steps to protect personal data from any loss, modification, misuse, unauthorised or accidental access and to protect it from alteration, disclosure or destruction. However, this provision highlights the words "practical steps". This shows that not every data user is obliged to follow the procedures as it is merely optional. Based on Abu Bakar Munir & Siti Hajar Mohd Yasin (2012), the data user only has an obligation to take measures proportionate with the risks presented to the cost of enforcement. Thus, the provision provides leeway to the data user to balance the cost of implementing the system measures and the level of risk presented in the event of security failure. Most significantly, the issues that PDPA 2010 failed to highlight are the right to be forgotten, the right to be informed and right to erasure after the data is used for its purpose or in cases of data breaches. This differs from the GDPR as it touches upon the right to be forgotten as the data has to undergo anonymisation or pseudonymisation, which allows the connection between data and consumers to be severed. In practice, the right to be forgotten is ineffective as data can only be concealed by the data users and the data processor, and it could not be fully forgotten as expressed by the learned AG Szpunar in the case *Eva Glawishing v Facebook Ireland Limited* (2019). Regardless, the security measures taken by the data users in dealing with data subjects' personal data under GDPR is evidently higher than those in PDPA 2010.

Discussion

Due to the complexity of Big Data, the current law is insufficient to truly governs the privacy of the users in e-Commerce. The implementation of the specific law towards Big Data is hard to achieve as the legislators are having difficulty in deciding the right definition of Big Data in PDPA 2010. Thus, the next step is to examine whether the technology specific law is necessary to regulate Big Data in e-Commerce. To achieve that, there is a need to analyse the governance criteria for Big Data as a central

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 5, (page 203 - 212), 2021
DOI: https://doi.org/10.47405/mjssh.v6i5.780

concept to strengthen the area of law that fails to govern Big Data in e-Commerce. Thus, suggestions and recommendations to improve the current legislative framework regarding privacy law is crucial to govern Big Data in e-Commerce. The PDPA 2010 was enacted to regulate the processing and collection of personal data for commercial purposes and all other matters that connect to, whether intentionally or on purpose, consumers' personal data. The Act requires companies and organisations that handle consumers' personal data in commercial transactions to notify and obtain the data subject's consent for any collection and processing of their personal information. Besides the applicability of the PDPA 2010, there is a lack of awareness on the PDPA 2010, specifically on the concept of personal data protection as a whole. Many business owners are clueless as to their status as data users. Data users are uncertain which issues fall under the purview of the PDPA 2010 and the steps that data users need to take. Business owners are still unsure of what constitutes personal data. Therefore, having a compulsory awareness campaign for every company or even to the public will give them some exposure. There is an effort to increase knowledge on the PDPA 2010 through seminars and public awareness campaigns using the media. Nevertheless, there is still room for improvement to educate the public and business entities. Under the enforcement of the PDPA 2010, there is a requirement for business entities and service providers to register, or they will face penalties under Section 16(4) of the PDPA 2010. Since it has been years since the enactment of the PDPA 2010, relevant parties and the authorities have to take measures to identify the gaps to fill in the legal requirements and industry standards and to develop a strategic guideline to address the gaps in the law. The data users need to know of their rights for data infringement under this Act, which leads to user-friendly guidelines. User friendly guidelines can be made available to the data user for easy access to increase knowledge regarding the necessary steps to take if there is a breach of data privacy. The usage of Big Data in processing personal data of the data subject has caused many negative effects. One of them is regarding the breach of privacy of the data subjects. As this impact is a well aware impact in most countries, the enactment of regulations to cater to this issue has come into existence. For example, in the European Union through the GDPR has set up several principles for the data processor as guidance for them in processing personal data of the data subjects. Transparency relates with the rights of the data subjects to request information about the processing of their data, how and by whom. The data controllers have an obligation to give the data subjects with such information. The rise of Big Data has indirectly caused deprivation towards the rights of the data subjects. Through transparency criteria in e-Commerce, data subjects can monitor the usage of their personal data, and it will directly give an obligation towards data controllers to disclose details regarding the processing (it will indirectly prevent the data controller from selling such data to the data broker). The transparency here does not refer to transparency of the rights of the data subject only, but also includes transparency obligations for data controllers. However, there is a prohibition on processing certain personal data of the data subjects if it exceeds its initial purposes. Limitation of purpose under Article 6 of the GDPR provides for personal data processing to be fairly and lawfully, and there must be a specification during the collection which is explicit and for legitimate purposes. Hence, the application of this criteria seems difficult to be applied. This is due to the fact that in processing Big Data, there is a massive amount of data collection to be processed and the purpose of the collection may only be clear afterwards. Nevertheless, this criterion is essential to prevent any misapplication of data. In e-Commerce, misapplication of personal data belonging to data subjects is not something new. For example, when data given by data subjects for registration have been used to advertise their products or even advertising products from different companies.

Conclusion

Big Data is revolutionising the business and commercial landscape, most profoundly at the expanse of users' data protection and privacy preservation. in a changing global order, there is a greater need than ever before, to reflect on the principles underpinning that right to our society, and to strengthen the realisation of the right to data protection as a fundamental human right owed to all individuals. Law in this frame of discussion, is seen as facing the known 'lagging' connotation in coping with this transformative technology and therefore, perturbing. In a changing global order, there is a greater need than ever before, to reflect on the principles underpinning that right to our society, and to strengthen the realisation of the right to data protection as a fundamental human right owed to all individuals

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 5, (page 203 - 212), 2021
DOI: https://doi.org/10.47405/mjssh.v6i5.780

(Mcdermott, 2016). The EU's initiative in keeping the GDPR relevant to the governing of Big Data is commendable, precisely on its initiative in incorporating the Privacy-by Design (PbD) model. This model of governance preserves one's privacy by developing measures that integrate the fundamentals of data protection in the technological system of information processing (Monreale et al., 2019). The underlying concept of (PbD) model involves the enjoyment of individuals in securing their fundamental protection to data privacy "automatically" when using the IT system. For PbD, the developer has to take into account the privacy of its users at the beginning and throughout the development process of any new products, processes or services that involve the processing of personal data, in accordance to the legislative framework (Van et al., 2014). This differs from the usual formulation of a system, where the developer will tackle the issue of privacy after the completion of a system. Incorporating privacy into the design of a system minimises the risk of privacy breaches by reducing trust in processors and data collectors when handling sensitive data and leaving the duty to secure data in the system itself, an initiative that should drive the drafting of governance framework for Big Data in Malaysia.

References

Abu Bakar Munir & Siti Hajar Mohd Yasin. (2012). Personal Data Protection Act: Doing Well by Doing Good. *Malayan Law Journal xxxiii*, *1*(1), lxxxiii - xcv.

Abu Bakar Munir et al. (2015). Big Challenges to Privacy and Data Protection. *International Journal of Computer and Information Engineering*, *9*(1), 355-363. Retrieved May 10, 2019, from https://waset.org/publications/10000669/big-data-big-challenges-to-privacyand-data-protection

Akter, S., Wamba, S.F. (2016). Big data analytics in E-commerce: a systematic review and agenda for future research. *Electron Markets 26*, 173–194. https://doi.org/10.1007/s12525-016-0219-0

Anugerah, Dian Purnama, and Masitoh Indriani. 2018. "Data Protection in Financial Technology Services: Indonesian Legal Perspective." in IOP Conference Series: Earth and Environmental Science.

Auffray, Charles, Rudi Balling, Inês Barroso, László Bencze, Mikael Benson, Jay Bergeron, Enrique Bernal-Delgado, Niklas Blomberg, Christoph Bock, Ana Conesa, Susanna Del Signore, Christophe Delogne, Peter Devilee, Alberto Di Meglio, Marinus Eijkemans, Paul Flicek, Norbert Graf, Vera Grimm, Henk Jan Guchelaar, Yi Ke Guo, Ivo Glynne Gut, Allan Hanbury, Shahid Hanif, Ralf Dieter Hilgers, Ángel Honrado, D. Rod Hose, Jeanine Houwing-Duistermaat, Tim Hubbard, Sophie Helen Janacek, Haralampos Karanikas, Tim Kievits, Manfred Kohler, Andreas Kremer, Jerry Lanfear, Thomas Lengauer, Edith Maes, Theo Meert, Werner Müller, Dörthe Nickel, Peter Oledzki, Bertrand Pedersen, Milan Petkovic, Konstantinos Pliakos, Magnus Rattray, Josep Redón i Màs, Reinhard Schneider, Thierry Sengstag, Xavier Serra-Picamal, Wouter Spek, Lea A. I. Vaas, Okker van Batenburg, Marc Vandelaer, Peter Varnai, Pablo Villoslada, Juan Antonio Vizcaíno, John Peter Mary Wubbe, and Gianluigi Zanetti. 2016. "Making Sense of Big Data in Health Research: Towards an EU Action Plan." Genome Medicine.

Avinash & Akarsha. (2017). Big Data Analytics for E-Commerce - Its Impact on Value Creation. *International Journal of Advanced Research in Computer and Communication Engineering*, 6(1), 181-188.

Barocas, Solon, and Andrew Selbst. 2016. "Big Data's Disparate Impact." California Law Review.

Basheer Ahmad Maula Sahul Hameed v PP 2016 6 CLJ 422.

Benefits of Big Data Indonesia for E-commerce Business in the Pandemic Period. (n.d.). *Soltius*. Retrieved September 5, 2019, from https://www.soltius.co.id/blog/benefits-of-big-data-indonesia-for-e-commerce-business-in-the-pandemic-period

Berman, J. (2013) *Principles of Big Data: Preparing, Sharing, and Analyzing Complex Information*. Morgan Kaufmann (Elsevier): Waltham.

Bernama. (2019, September 27). Customer Data Breach Contained, Says Malindo Air. *New Straits Times*. Retrieved from https://www.nst.com.my /news/nation/2019/09/525208/customer-data-breach-contained-says-malindo-air

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 5, (page 203 - 212), 2021
DOI: https://doi.org/10.47405/mjssh.v6i5.780

Cate, F. and Schönberger, V. (2013). Notice and Consent in a World of Big Data. *International Data Privacy Law, (3)*2, 67-73.

Datastax. (2012). Big Data: Beyond the Hype Why Big Data Matters to You. 1-19. Retrieved May 7, 2019 from http://docplayer.net/822486-Big-data-beyond-the hype.html

European Commission. (2013). *Article 29 Data Protection Working Party.* Opinion 03 / 2013 on Purpose Limitation. (Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC). (pp. 1-70)

Eva Glawishing v Facebook Ireland Limited, unreported Court of Justice of the European Union (No 128/19, 3 October 2019).

Finn, R., Wright, D., Friedewald L.M., Fraunhofer & Karlsruhe. (2013). *Seven Types of Privacy*. 7. Retrieved October 1, 2020, from https://www.researchgate.net/publication/258892458_Seven_Types_of_Privacy#citations

Girard, M. (2019). Big Data Analytics Need Standards to Thrive: What Standards Are and Why They Matter. *Centre for International Governance Innovation*. Retrieved on September 25, 2019, from https://www.cigionline.org/sites/default/files/documents/Paper%20no.209.pdf

Gromenko, B. D. (2019). Corporate Security in the EU and GDPR: Data breaches in British Airways and The Marriott International [Unpublished master dissertation]. University of Economics, Prague.

Gürses, S., Troncoso, C., & Diaz, C. (2015). Engineering privacy by design reloaded. In *Amsterdam Privacy Conference* (pp. 2).

Ho, S. (2018, June 25). Powering Alibaba's eWTP with big Data Analytics, AI and Machine Learning. *The Edge Markets*. Retrieved October 5, 2019, from https://www.theedgemarkets.com/article/powering-alibabas-ewtp-big-data-analytics-ai-and-machine-learning

Hoofnagle, H. J., Van der Sloot, B. & Borgesius, F.Z. (2019). The European Union General Data Protection Regulation: What it is and What it Means. *Information & Communications Technology Law, 28*(1), 65-98. https://doi.org/10.1080/13600834.2019.157350

Hummerick, M. (2018). The Tortoise and the Hare of International Data Privacy Privacy Law: Can the United States Catch Up to Rising Global Standards? *Catholic University Journal of Law and Technology.* 27. p.89.

Information Commissioner's Office. 2018. Guide to the General Data Protection Regulation (GDPR).

Kandiah, S. (2019). Malaysia. In A.C. Raul (6th Eds.), *The Privacy, Data Protection and Cybersecurity Law Review*. (pp. 251-265). 2019 Law Business Research Ltd. Retrieved on September 28, 2019, from https://www.sidley.com/-/media/publications/theprivacydataprotectionandcybersecuritylawreviewedition6.pdf

Mcdermott, Y. (2017). Conceptualising the Right to Data Protection in an Era of Big Data. *Big Data & Society*, 2-5, https://journals.sagepub.com/doi/pdf/10.1177/2053951716686994

McFee, A., & Brynjolfsson, E. (2012). Big Data: The Management Revolution. *Harvard Law Review, 90*(10), 60-66. https://hbr.org/2012/10/big-data-the-management-revolution

Monreale, A., Rinzivillo, S., Pratesi, F. *et al.* (2014). Privacy by Design in Big Data Analytics and Social Mining. *EPJ Data Science.* 3(10), 3, https://doi.org/10.1140/epjds/s13688-014-0010-4

National e-Commerce Roadmap. (2019). Malaysia Digital Economy Corporation Sdn Bhd, Malaysia. Retrieved December 8, 2019, from https://mdec.my/aboutmalaysia/government-policies/national-ecommerce-roadmap/

Norjihan Abdul Ghani, Suraya Hamid & Nur Izura Udzir. (2016). Big Data and Data Protection: Issues with Purpose Limitation Principle. *International Journal Advancement Soft Computer Application, 38*(8), 117-120.

OECD Secretariat. 2016. Big Data: Bringing Competition Policy To The Digital Era.

Oluwayomi A. Ajibade. (2018). *A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape* [Master Thesis, Tilburg University]. ResearchGate. http://dx.doi.org/10.13140/RG.2.2.18365.31207

Pardo, A., & Siemens, G. (2014). Ethical and Privacy Principles for Learning Analytics. *British Journal of Educational Technology,* 43(3), 438-450.

Protection, Personal Data. 2010. "Laws of Malaysia Act 709 Personal Data Protection Act 2010." 10 June 2010.

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 5, (page 203 - 212), 2021
DOI: https://doi.org/10.47405/mjssh.v6i5.780

Qing Tan & Frederique Pivot. (2015). 'Big Data Privacy: Changing Perception of Privacy' IEEE. *International Conference*. Retrieved September 12, 2019, fromhttps://ieeexplore.ieee.org/document/7463831

Quinn, Paul, and Liam Quinn. 2018. "Big Genetic Data and Its Big Data Protection Challenges." Computer Law and Security Review.

Rubinstein, I,. S,. (2013). Big Data: The End of Privacy or a New Beginning?. *International Data Privacy Law, (3)2*, 74-87.

Satariano, A. (2019, July 8). After a Data Breach, British Airways Faces a Record Fine. *The New York Times*. Retrieved September 20, 2019, from https://nyti.ms/2NE2qGB

Sharon, A. (2019, October 10). Big Data Key for Achieving Malaysia's Digital Economy Aspirations. *Open Gov*. Retrieved December 10, 2019, from https://opengovasia.com/big-datakey-for-achieving-malaysias-digital-economy-aspirations/

Singh, H. (2018, November 5). How Big Data is Helping E-commerce and Physical Businesses? Retrieved September 5, 2019, from https://customerthink.com/how-big-data-is-helping-e-commerce-and-physical-businesses/

Storr, C. & Storr, P. (2017). Internet of Things: Right to Data from a European Perspective. In Corrales, M., In Fenwick, M., & In Forgó, N. (Eds.), *New technology, big data and the law* (2017). (pp.66-94). http://doi.org/ 10.1007/978-981-10-5038-1_4

Tambe, P. (2014). Big Data Investments, Skills, and Firm Value. *Management Science, 60*(6), 1452-1469. https://dx.doi.org/10.2139/ssrn.2294077

Tchao, E.T., Diawuo, K., Kotey, S.D. & Aggor, C. (2017). Ghanaian Consumers Online Privacy Concerns: Causes and its Effects on E-Commerce Adoption. I*nternational Journal of Advanced Computer Science and Applications, 8*(11), 157-163. https://arxiv.org/pdf/1801.01086

The International Trade Administration. (2020, August 19). *Malaysia e-Commerce. United States Department of Commerce*. https://www.export.gov/article?id=Malaysia-E-Commerce

The Power of Big Data in the China Market. *Beyond Summits*. Retrieved September 5, 2019, from https://www.beyondsummits.com/blog/power-big-data-china-market

Thi Mai Le & Shu-Yi Liaw. (2017). Effects of Pros and Cons of Applying Big Data Analytics to Consumers' Responses in an E-Commerce Context. *Sustainability Journal 9*(798), 1-19. www.mdpi.com/2071-1050/9/5/798/pdf-vor

Van Rest J., Boonstra D., Everts M., Van Rijn M., Van Paassen R. (2014). Designing Privacy-by-Design. In B. Preneel and D. Ikonomou (Eds.), *Privacy Technologies and Policy. APF 2012. Lecture Notes in Computer Science, 83*(19), 55–72. doi:10.1007/978-3-642-54069-1_4

Wastermann, H. (2018). *Change of Purpose The effects of the Purpose Limitation Principle in the General Data Protection Regulation on Big Data Profiling* [Master Thesis, Lund University]. Lund Universities Libraries. http://lup.lub.lu.se/student-papers/record/8941820.

Weizen, T. (2017, February 24). In The Business of Big Data, Singapore Has Built A Cutting Edge. *Today*. Retrieved September 5, 2019, from https://www.todayonline.com/singapore/business-big-data-singapore-has-built-cutting-edge

Zarsky, T. Z. (2017). Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review, 47*(995), 995-1020. https://scholarship.shu.edu/shlr/vol47/iss4/2