PERSONAL DATA PROTECTION OF PREDICTIVE ANALYTICS IN ONLINE SHOPPING: FROM MALAYSIAN LEGAL PERSPECTIVE

Muhammad Afdal bin Noor Azman
Dr Muhammad Nizam bin Awang

ABSTRACT

Lack of legal coverage over personal data protection in predictive analytics of online shopping is a huge concern. This would expose their personal data to misuse whether for legal or illegal purposes especially in online shopping, hence cause privacy intrusion. It was argued that the information used during the processes of predictive analysis will not infer any particular person, thus deprive their privacy of life. Study shows that, the latest Personal Data Protection Act (PDPA) 2010 does not cover the usage of personal information under predictive analytics processes. This shows the lacuna or the gap of the gazetted law. Besides, a statistic in September 2019 reported that more than 26 million of Malaysians are using internet, and the data from *GlobalWebIndex* also shows that 80 percent users between the ages of 16 and 64 are using online shopping platforms. The main aim of this paper is to propose a number of preliminary suggestions to ensure that the personal data gathered from online shopping which were used in predictive analytics are covered under the PDPA 2010 with reference and comparison from the leading jurisdictions such as United Kingdom and United States of America, and also from Asian Pacific countries such as Hong Kong, New Zealand and Australia. This paper focuses on the online shopping platforms because the personal data can be easily collected and exposed to many users compared to the collected data in other type of businesses. The most testing question here is whether the data used in the predictive analytics of the online shopping is within the ambit of personal data protection under PDPA 2010 in particular, and under the General Data Protection Regulation (GDPR) in general. In this context, the PDPA 2010 only covers the personal information from the commercial transaction with exception to, Federal and State Governments, as well as the personal data processed outside Malaysia. Furthermore, predictive analytics is commonly defined as an area of statistics that deals with extracting information from data and using it to predict trends, behaviour patterns, and etc. To achieve the objective of this paper, the study will be conducted through literature review which is qualitative in nature. A recent study shows that some countries such as Australia does consider a set of individual information used in predictive analytics deemed as personal data and should be protected under the law. Thus, it is recommended that the personal data involved in the predictive analytics collected from the online shopping to be covered under the ambit of PDPA 2010.

Keywords: *Predictive analytics, online shopping, online retail, data protection law, Malaysian Personal Data Protection Act 2010.*

Introduction

Understanding the customer's needs and maximize their satisfaction is one of the main focuses for every online retailer to succeed in the long run (Cirqueira et. Al, 2019). In the recent era of the twenty first century, technology has become the main pushing factor which helps human to achieve a better result in any fields and industries. The discussion of the personal data protection has emerged since 1960's and 1970's which associated with the development of technology (Saad, 2005). In the context of business data analysis, studies shows that these analysis helped traders to predict theirs customer's behavior as to help them produce more product and advertisement which could gain them more profit in the future (Satish & Yusof, 2017). The predictive mechanism and tools through the advancement of the technology coupled with the big data, internet of thing (EUR, 2016) and artificial intelligent, also could help to predict other field such as the outbreak of disease, weather forecasting, market trend, etc (San, 2020). These prediction tools were coming

from the creation of a complex algorithm through an analysis process which helps human to analyze a huge amount of recorded data that might has been stored for many years (Matsumi, 2017).

These expansion of data analysis tools also has reach the online shopping as people nowadays especially Malaysian are tend to purchase items through the online platforms. A study shows that, 91% of Malaysian population ranged from 16 to 64 years old was searched online for a product or service to make a purchase, 90% whom visited an online retail store on the any website, and 82% purchased an online product (44% through laptop or computer, 64% through mobile device) (Digital, 2020).

An analysis over billions of personal data from the online shopping platform to predict the behavior and pattern amongst the e-consumer's preferences is one thing; however, these analyses over the personal data could cause privacy intrusive. For example, if a data subject had a sensitive information regarding himself such as health condition, political view and etc stored in the online shopping platforms, this can cause a discomfort or insecure. This might not be the case in other sector such as the health report in the medical which the purposes were clear and usually approved by the data subject (San, 2020). It was argued that the information used during the processes of predictive analysis will not infer any particular person, thus deprive their privacy of life.

This paper will be discussing on the legal status of predictive analytics over personal data in the online shopping or in the other words, online retail under the preview of Malaysian personal data protection law. The Malaysian personal data protection falls under Personal Data Protection Act 2010 (PDPA 2010) which was enforced and gazetted in 2013 as the purpose of this law is to control how the personal data is collected, recorded, stored, processed, until it seized to be used by the data user (Yusoff, 2011).

Besides, the paper is aimed to observe and examine on the applicability of the personal data protection law (PDPA 2010) of predictive analytics in the online shopping and whether the Malaysian parliament should extend the coverage of this law towards the predictive analytics activities in the future. Thus, the paper will be outlined as follows. The Second part will be discussing on the predictive analytics in Malaysian online shopping, as to explain on how these analysis works in online retail. The third part is on the status of general predictive analytics in Malaysian Personal Data Protection law. How the law protects and safeguard the information of the data subject, and how the law ensure the data subject have the rights to check, review, and change their own data as well as to allow or seize its usage.

An analysis will also be made to some samples of privacy policy from different online shopping website such as Lazada, Shoppee, and etc. These online shopping websites were chosen due to its recent popularity in Malaysia. The fourth part is the analysis through comparison of the legal status from United State of America (USA), European Union (EU), and also from Asian Pacific countries such as Hong Kong, New Zealand and Australia. As a well developed nation, these countries were chosen based on their strong foundation of personal data protection law. For example, EU had developed a very high standard law law through General Data Protection Regulation (GDPR) that was enforced on 25 May 2018, while USA as a nation that strongly protects the right to privacy although there is no comprehensive laws were enacted, as they depends on the sectoral law to protect personal data (San, 2020). The paper will be concluded in fifth part.

Predictive Analytics in Online Shopping

It cannot be argued that online shopping has become a trend nowadays especially amongst Malaysian. The variety of products offered in the online shopping platforms has increased the number of online buyers from all different ages (Pal). A study shows that the online purchasers around the globe purchased $2.86 trillion on the web in 2018, which is 18% higher than the previous year (Cirqueira et. Al, 2019). It is a matter practice in the e-Commerce that predictive analytics is applied as a method to predict a collective behaviour amongst data subjects who are also considered as the customers, e-consumer, online buyers, and etc (Das, 2017).

Their behaviour are highly relied on the online activities such as number of clicks, previous session, session duration, purchase session, clicks rate per session and etc (Pal). The usage of predictive tools is wide and differs from one company to another. It can be used to predict a customer's tendency or behavior to buy a certain product, such as offering an 'A' product which would invite the customer to buy 'B' product. Another benefit to this is that the tools which made from a very complex algorithm can help an online retailer to optimize their product's prices, in another word, they can offer different amount of prices or

dynamic prices that can create the interest amongst the online buyers (Gupta, 2014). Hence, this would maximize the customer's satisfaction (Avinash & Akarsha, 2007). It can't be denied that these processes would provide great value to the society, enhancing productivity, improving public and private sectors, as well as social participation, but its drawback should not be set aside (Christos et. al, 2018).

A study shows that, there are three factors that influenced a customer's decision making in order to purchase an item through online platform, which is the customer's needs, the product's popularity, and the customer's preferences (Qiu, 2014). It that sense, the online retailer will use the prediction tools to based on these factors in order to make a better plan for their business such as marketing, inventory, human resources, administration, and etc. If it succeeded, this would increase the success rate of acquiring customers, increase sales, as well as to compete at the national market or even worldwide.

Another study also suggested that a purchase from the customers were divided into two types of purchase in online shopping, one is the firm-initiated purchase which is a consequence of the firm making recommendations. The second type is divided into self-initiated purchase which is a purchase that is not related with the past purchase, while an association-initiated purchase is a purchase that related with the past experience (Anand, 2008). Thus, the study of this paper is focusing more on the association-initiated purchase which can be analyzed more conveniently compared to other type of purchase.

These analysis comes from a large amount of data as per collected from an online shopping website. As in practice, an online customer needs to register a personal account in order to login into a shopping website. The most frequent data that includes are name, email address, a unique password, date of birth, address, and etc. Some website also requires a bank account number for the purpose of auto debit process. These data are relatively important and significant for the data subject, as it will cause privacy intrusive to the owner of these data if it were being misused which is in accordance with the Personal Data Protection Act (PDPA) 2010. Although an online website had stated the purpose of the collected data and its usage within the website, such as for the research and analysis purposes, the questions that arise here is how these research and analysis being done, which data involved, who are the person processing it, and which parties involved. Most of the online shopping privacy policy (Most frequently term used) does stated the data might be share to the third party for the purpose of providing the customer with a better service. In fact, this is stay unclear for so long without any clear guidance as to how these processes should be done. It also worth to note that the competent human resources is compulsory to handle these data and tools together with a consideration to data privacy and security (Avinash & Akarsha, 2007).

One of the examples of analyzing the customer's behavior through collected data can be seen as follows:

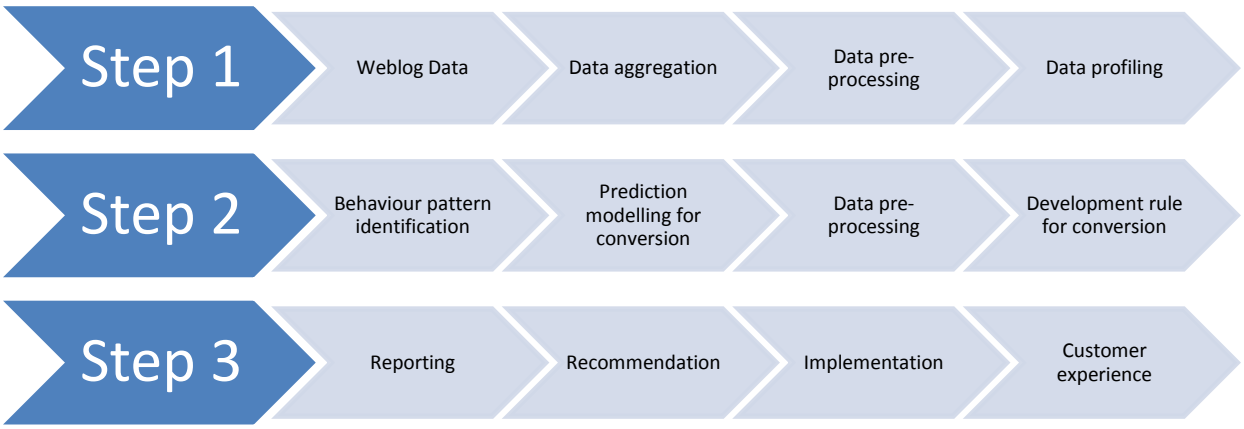

Figure 1: Online Buyer's Behavior Analysis.

Status of General Predictive Analytics in Malaysian Personal Data Protection Law

The enactment of Personal Data Protection Act (PDPA) 2010 is a legal development of e-commerce in Malaysia with a massive and increasingly valuable amount of personal information are being stored,

processed and exploited (Zulhuda, 2014). Besides, the formulation of the personal data protection legislation started in 1998, and the first draft of the PDPA was prepared and release for public consultation in 1999/2000 (Hassan, 2012). PDPA was passed to Parliament in 2010, it was enforced and gazette in 2013 (Yusoff, 2011). The PDPA applies to a data user who, in the Act, is defined as the person who processes or has control over or authorizes the processing of data (Munir, 2012). According to a report by Malaysian Data Protection Authority (MDPA) in 2015, approximately 140 complaints have been lodged since its implementation in 2013 (Seah, 2017).

Besides, there are seven principles of the Act 2010 that should be adhered by all parties in the commercial transaction especially the data users, failure to comply will commits an offence which carries a fine not exceeding RM200,000 or imprisonment not exceeding two years or both (San, 2020). The significant guiding principles are as follows:

a) **General principle**: No process of personal data which is excessive and/or without the consent of data subject (Setion 6 of the PDPA 2010).
b) **Notice and choice**: Proper notification on the purpose of that data collection / processing (Section 7 of the PDPA 2010).
c) **Disclosure**: prohibits unauthorized disclosure or sharing of personal data (Section 8 of the PDPA 2010).
d) **Security**: Imposes security measures by data users that commensurate the risk of security breach.
e) **Retention**: Personal data shall not be kept unnecessarily (Section 10 PDPA 2010).
f) **Data integrity**: Right of data subject to correct and update their personal data (Section 11 of the PDPA 2010).
g) **Data access**: Right of data subject to have access to his own personal data at the user's database (Section 12 of the PDPA 2010).

According to a recent paper by Tay Peck San titled as, predictions from data analytics: Does Malaysian Data Protection Law Applied? This paper concluded that the predictive analytics over the personal data in the commercial does not cover under the well known Malaysian Personal Data Protection Act 2010 (PDPA 2010). It was argued that the data used during the process of analysis will not determine any specific individuals as define under the PDPA 2010, otherwise the analyzed data shall be governed under the law.

The personal data is defined under the ambit of Section 4 of PDPA 2010 as any information in respect of commercial transactions, which:

(a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose. (b) is recorded with the intention that it should wholly or partly be processed by any means of such equipment; or (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user including any expression of opinion about the data subject.

The issue here is whether the data collected and grouped for analysis and prediction would identify any data subject or individuals or causing them to be identifiable. Most of the current data analyses are only mentioning a specific figure such as, number of clicks per session, browses frequency, number of purchases, session duration, customer's tendency and etc. However, these data will not exist without their primary source from the registered account and its past data of the online buyers. In Addition, the General Data Protection Regulation (GDPR), under Recital 26 provides that there will be no concern to the processes of anonymous information, statistical or research purposes, as it would not cause a person being indentified (Christos et. al, 2018).

It was further submitted by the author that the classification of all analyzed data into an identifiable personal data (according to section 4 of PDPA 2010) is not relevant and would defeat the balance between the privacy of data subject and commercial realities. Firstly, because the analyzed data might not infer any person's profile, as prediction is a mere guess. For example, an online shopping company might predict that a group of customer X is likely to purchase Books if a set of pen was displayed. Secondly, classifying all predictions from data analytics as falling within the remit of data protection law may lead to bad implication

to the commercial world. The ultimate aim of the law itself is to prevent from any distress and damage over the data subject, thus a proper law need to be suggested to strike a balance between the data subject and the commercial world, especially in online shopping. Finally, predicting an individual behaviour in a similar group of people as shown in the above example cannot be said as causing any privacy intrusive or harm to a person's privacy. If the law imposed the unlimited right to the data subject over predictive analytics activities, this would open a floodgates to claims of privacy invasion, regardless of how the case might be (San, 2020).

However, it is worth to suggest that the predictive analytics fall within the exception in section 45 of PDPA 2010, as long as the analyzed group of personal data does not cause any identification of a particular individual.

Legal Status from other Developed countries

European Union

The leading General Data Protection law was first introduced to all the European Union (EU) members in 1995 by the Data Protection Directive (Fuster, 2013). Under the EU law, data protection has been acknowledged and affirmed under Article 16 of the Treaty of the functioning of the EU, as well as in Article 8 of the EU Charter of Fundamental Rights. Its purposes is to protect the fundamental rights and freedoms of natural persons and in particular their rights to privacy with respect to the processing of personal data, and as a prevention of barriers to the free flow of personal data across the community by virtue of reasons connected with the above protection (Munir & Yasin, 2010).

In conjunction with rapid development of technologies in the modern days, EU has adopted a new legislation in 2016 to protect the data more efficiently. Then, the first General Data Protection Regulation (GDPR) was introduced and applicable to all members of EU in May 2018, replacing the Data Protection Directive (Christos et. al, 2018).

It was defined by Article 4(1) of the regulation that 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 identifiable or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. It can be understood from the provision that, it is not only refer to the identifiable person, but also referring to person who is related or capable of being identified by it (San, 2020).

The regulation was further explains that in order to determine whether a person is identifiable. Firstly, an account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. Secondly, to ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments (GDPR).

Article 21(1) and 21(2) of the regulation gives the data subject a right to disallow or object any processing of their information for the purpose of profiling by the data users. Profiling has been defined under Article 4(4) of the regulation as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Although the prediction aspect was stated in the provision, the regulation is silent on whether the prediction through profiling is considered as personal data (San, 2020).

Many cases were decided by the Court of Justice of the European Union (CJEU), however, the term of predictive analytics is yet to be applied by the court. In the case of Lindqvist, it was held that by publishing personal data of a number of people working with her on a voluntary basis into her internet site would constitute as breach of Swedish legislation on the protection of personal data (Lindqvist, 2003). In another case of Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V (Fashion ID, 2019), by embedding a plug-in in its website: Facebook's 'Like' button, it has caused an automatic transfer of its user's IP and browser string to Facebook when they land on the Fashion ID's website. The court held that, this constituted

as personal data. In the case of Costeja Gonzalez v Google Spain and Google (Kulk & Borgesius, 2014), the CJEU had decided that the indexed data which stored by the search engines was considered as personal data.

In a working document on summary of the request for a preliminary ruling pursuant to Article 98(1) of the Rules of Procedure of the Court of Justice (Humains, 2019), the constitutional court of Belgium had mentioned regarding the usage of predictive algorithms for the purpose of prevention, detection, investigation of terrorist offences and serious crime through passenger database in Belgium. However, it does not explain further on the prediction analysis in particular, but it was clear that the passenger databases are considered as personal data.

In general, CJEU strongly agrees that whenever the data could identify a person or a group of people or causing an individual being identifiable, it would constitute personal data.

United States of America

Historically, the emergence of personal data protection in the United State of America (USA) has begun in 1965 due to the large amount of personal information which progressively used the electronic database since the first commercially available computer in 1951 (Saad, 2005). A Social Science Research Council recommended the establishment of a Federal Data Centre as a single repository of government statistical information but it was rejected by the Congressional Hearing (Havard). However, after several years, automated data systems caused a huge concern amongst consumers in USA. Thus, a code of practice on personal information has been developed by an Advisory Committee on Automated Personal Data System in 1972 which later embodied a Privacy Act 1974 (Nehf, 2003).

In the United State of America (USA), there is no plenary law that regulates the personal data protection especially for the online businesses, as it relies significantly on industry self-regulation as well as safe harbor principles (Munir & Yasin, 2010). This is due to different laws were enacted for different sector from each states such as health, communication, banking and human services (San, 2020). Although there is a law enacted at the Federal level which is the Federal Trade Commission (FTC) under Section 5 of the Federal Trade Commission Act (Amendment 2006), the law is too general and has limited jurisdiction over banks, insurance companies, non-profit entities, and even some internet service providers (O'Connor, 2018). Besides, the law only protects the consumers against any deceptive and unfair practices as well as to enforce federal privacy and data protection regulation. The law also protects the consumer from the company's failure to comply with its privacy policies, failure to provide adequate security of personal data, and the deceptive marketing or advertising (Chabinsky & Pittman, 2020).

An example can be seen on consumer's data privacy which is the California Consumer Privacy Act (CCPA) that protects the consumer's information including the online retail, there is no absolute provision in the law that mentioning the protection of predictive analysis over personal data. In fact, the law allows the data brokers to collect (from many sources including websites, other businesses, and public records), analyzes, and packages the data for sale to other businesses.

It was clearly showed that the USA's personal data protection law is the industry's dependant law which differ from one state to another, thus it is vague whether it covers the predictive analytics regulation over the personal data especially in online retail.

Hong Kong

Hong Kong's first personal data protection law was first enacted in 1995 trough Personal Data (Privacy) Ordinance 1995. The ordinance applied the six data protection in accordance with the Organization for Economic Co-operation and Development (OECD) privacy guidelines. However, this ordinance does not provide any provision to establish a commissioner to execute the law and an appeal board to provide any compensation and other remedies to the complainant as well as to penalize any company that breaches the law (Munir & Yasin, 2010). Personal data according to Section 2 of the ordinance is defined as any data relating directly or indirectly to a living individual, from which it is practicable for the identity of the individual to be directly or indirectly ascertained, and in a form in which access to or processing of the data is practicable.

In one of the articles written by Privacy Commissioner for Personal Data of Hong Kong (Woo, 2010), there is concerns on e-shopping has been raised when it comes to personal information which being used for processing, commercial transaction as well as to protects the data from computer hackers or unintended users, but no further discussion has been made with regards to the predictive analytics. This lacuna and lack of discussion on this area can cause major concern if failed to be prevented at the early stage.

New Zealand

In New Zealand, the very first comprehensive law which was enacted is the New Zealand's Privacy Act 1993 which covers a wide broad of personal data protection towards private and public sectors as well as establishing an office of Privacy Commissioner (Woo, 2010). The 12 information privacy principles adopted by the Act was based on the OECD guidelines with some influence from Australia data protection law, and it was said to be the most successful enforced law in the region (Greenleaf, 2011). Every year the commissioner received approximate 650 numbers of complaints which resulted in most of the agreed settlement (Greenleaf, 2011). It was later a Privacy Amendment Bill was introduced to New Zealand's parliament in 2018 to strengthen the power of Privacy Commissioner, to ensure the privacy breaches being mandatorily reported, introducing the offshore data transfer's regime, new offences, and increased fines (Valentine, 2020).

Personal data is defined under the Act as information about an identifiable individual; and includes information relating to a death that is maintained by the Registrar-General pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995, or any former Act (as defined by the Births, Deaths, Marriages, and Relationships Registration Act 1995).

However, particular provision pertaining to the protection of personal data for the process of predictive analytics is nowhere to be found in the Act. Similar to Malaysian's PDPA 2010, the law provides general protection of personal information of the data subject.

Australia

In 1988, Australia had enacted its very first Privacy Act 1988 in the region that follows the Information Privacy Principles which in accordance to OECD's guidelines. The law also established an office of the Privacy Commissioner. After three years, the law was expanded to cover credit reporting in 1999, and then it includes the private sector in 2001. This law has its own exception to employment records, small business operators, political and media activities (Munir & Yasin, 2010).

The law was amended in 2019 . According to the Act, individual is given a right to know on reason of their personal information being collected, the purpose of the information being used, disclosure of the information, and right to make correction in their own information. Besides, businesses are responsible to protect the personal information from any misuses, interference, loss, and etc. According to the general definition of personal information under the Act, predictions from data analytics considered as personal information as long as they are about an identified or a reasonably identified individuals (San, 2020).

Should Predictive Analytics in Online Shopping be Subject to the PDPA 2010?

The predictive analytics in online shopping will fall under the PDPA 2020 when there is personal data involved, as 'Personal data' is defined in the PDPA as any information in respect of commercial transactions that relates to a data subject who is identified or identifiable from that information or from that and other information in the possession of a data user (San, 2020). On the other hand, when the analyzed data were anonymous towards certain targeted group of people, the process will not fall within the ambit of PDPA 2020.

It should be understand that the processing of personal data in PDPA 2020 is comprises of 4 types of processes. The first type of process is when the personal data were organized adapted and altered. The second type of process is when the personal data is being retrieved, consulted and used by the data user. The third type is the disclosure of personal data by transmission, transfer, dissemination and making the data available. And the last type of process is the alignment, combination, correction, and destruction of the

personal data. In the predictive analytics over personal data in the online shopping, the first step as shown in the figure 1 is consider to be similar with the first and second steps under PDPA where the data are being organized and retrieved by the data user. Besides, the second step as shown in the figure also related with third and fourth types of processes under PDPA 2020, where the data were made available, transmitted, analyzed, combined and applied.

It is opined that through the analysis made in this paper, the predictive analytic over personal data in the online shopping should be mentioned in the PDPA 2020 as one of the subsection under section 45. It is suggested that the provision stated as one of the exceptions to the collection, storing, use, etc of personal data from online shopping platforms during the process of predictive analytics as long as it does not infer any particular individuals directly or indirectly as prescribed by section 4 of the Act.

Conclusion

The main purpose of the PDPA 2020 is to provide protection over personal data in commercial transaction as prescribed under the Act. Besides, the process of analyzing over tons of collected data from online shopping platforms is necessary in today's modern world as to strengthen an online business data management as well as to predicting future marketing planning and etc in the future. However, the law cannot shy away from this issue because the predictive analytics does involve the usage of personal data, and it does not covered under the provided Act. This lacuna might cause jeopardy to the data subject in the long run if it does not addressed by the parliament, as technology is developing and improving in a very high pace.

References

Advancing the Internet of Things in Europe. European Commission. (2016). Retrieved from: https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-internet-things-europe.

Anand, V. B. (2008). Recommendation Systems with Purchase Data. Journal of Marketing Research. Vol. XLV. 77-93. American Marketing Association.

Avinash, B. M., & Akarsha, B. M. (2007). Big data analytics for e-commerce–its impact on value creation. *International Journal of Advanced Research in Computer and Communication Engineering ISO*, *3297*.

California Consumer Privacy Act. Xavier Becerra, Attorney General. Retrieved from: https://oag.ca.gov/privacy/ccpa.

Chabinsky, S., Pittman, F.P. (2020). USA: Data Protection 2019' in D Gabel and T Hickman (eds), The International Comparative Legal Guides to Data Protection Laws and Regulations 2019 (Global Legal Group, 2019). Retrieved from: https://iclg.com/practiceareas/dataprotection-laws-and-regulations/usa.

Christos, G., Giovanni, B., Michael, O., (2018). Handbook on European Data Protection Law 2018 Edition. Luxembourg: Publications Office of the European Union.

Cirqueira, D., Hofer, M., Nedbal, D., Helfert, M., & Bezbradica, M. (2019). Customer Purchase Behavior Prediction in E-commerce: Current Tasks, Applications and Methodologies. In *International Workshop New Frontiers in Mining Complex Patterns*. Dublin City University, Dublin, Ireland.

Das, S., Singh, P., & Puri, G. (2017). A Predictive Analytics Model for Maximising Profit in e-commerce Companies. *E-Commerce for Future & Trends*, *4*(2), 10-23.

Digital Data : Malaysia (2020). Data Reportal. Retrieved from: https://datareportal.com/reports/digital-2020-malaysia.

Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV. (2019). In Case C-40/17.Retrieved from: http://curia.europa.eu/juris/liste.jsf?num=C-40/17.

Fuster, G. G. (2013). Security and the future of personal data protection in the European Union. *Security and Human Rights*, *23*(4), 331-342.

General Data Protection Regulation (GDPR), Recital 26. Retrieved from: https://www.privacy-regulation.eu/en/recital-26-GDPR.htm.

Greenleaf, G. (2011). Asia-Pacific data privacy: 2011, year of revolution?.*Kyung Hee Law Journal, Forthcoming*.

Gupta, R., & Pathak, C. (2014). A machine learning framework for predicting purchase by online customers based on dynamic pricing. *Procedia Computer Science*, *36*, 599-605.

Harvard Law Review Association. Privacy and Efficient Government: Proposals for a National Data Center. *Harvard Law Review*, *82*, 400-417.

Hassan, K. H. (2012). Personal data protection in employment: New legal challenges for Malaysia. *Computer Law & Security Review*, *28*(6), 696-703.

Kulk, S., & Borgesius, F. Z. (2014). Google Spain v. González: Did the court forget about freedom of expression. *Eur. J. Risk Reg.*, *5*, 389.

Ligue des droits humains v Conseil des ministres (2019). Request for a preliminary ruling from the Cour constitutionnelle (Belgium) lodged on 31 October 2019. In Case C-817/19.

Lindqvist, B. (2003). In Case C-101/01. Retrieved from: http://curia.europa.eu/juris/showPdf.jsf;jsessionid=F794862E6D911887DD1B988235CA9B1C?docid=48382&pageIndex=0&doclang=EN&dir=&occ=first&part=1&cid=6877229.

Matsumi, H. (2017). Predictions and Privacy: Should There Be Rules about Using Personal Data to Forecast the Future. *Cumb. L. Rev.*, *48*, 149.

Munir, A. B., & Yassin, S. H. M. (2012). Personal data protection act: Doing well by doing good. *Malayan Law Journal*, *1*.

Munir, A. B., Yasin, S. H. M. (2010). Personal Data Protection in Malaysia: Law and Practice. Malaysia. Sweet & Maxwell Asia.

Nehf, J. P. (2003). Recognizing the societal value in information privacy. *Wash. L. Rev.*, *78*, 1.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' (1980). Retrieved from: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

O'connor, N. (2018). Reforming the US approach to data protection and privacy. *Council on Foreign Relations*, *30*.

Pal, S. Know your buyer: a predictive approach to understand online buyer's behavior', white paper. *Happiest Minds*.

Personal Data (Privacy) Ordinance, Chapter 486.

Qiu, J. (2014). A predictive Model for Customer Purchase Behavior in E-Commerce Context. In *PACIS* (p. 369).

Saad, A. R. (2005). *Personal Data & Privacy Protection*. Malayan Law Journal Sdn. Bhd.

Satish, L., & Yusof, N. (2017). A review: big data analytics for enhanced customer experiences with crowd sourcing. *Procedia computer science*, *116*, 274-283.

San, T. P. (2020). Predictions from data analytics: Does Malaysian data protection law apply?. *Information & Communications Technology Law*, 1-17.

San, T. P. (2020). The Impact of The Personal Data Protection Act 2020 on Data Analytics in The Retail Industry. Malayan Law Journal Articles.

Seah, L. (2017). Brief Comparison Between The Malaysian Personal Data Protection Act 2010 and Other Jurisdiction. 1 LNS(A) xlvi. Current Law Journal.

Valentine, N. (2020). Data Protection Laws of the World: New Zealand. DLA PIPER. Retrieved from: www.dlapiper.com.

Woo, R.B. (2010). 'Data Protection Principles in the Personal Data (Privacy) Ordinance: from the Privacy Commissioner's perspective (2nd Edition)'. Pg. 68. Retrieved from: https://www.pcpd.org.hk/english/resources_centre/publications/books/files/Perspective_2nd.pdf.

Yusoff, Z. M. (2011). The Malaysian personal data protection act 2010: A legislation note. *NZJPIL*, *9*, 119.

Zulhuda, S. (2014). Legal Framwork on The Enforceability, Fairness and Data Protection Surrounding the Election Transaction: A Case of Malaysia. Lex Mercatoria: Journal of International Trade and Business Law. Volume 2, Number 1. Graduate Study Atma Jaya School of Law.