Available Online at www.e-iph.co.uk
Indexed in Clarivate Analytics WoS, and ScienceOPEN

E-B Environment - Behaviour Proceedings Journal

International Virtual Colloquium on Multi-disciplinary Research Impact (2nd Series)
Organised by Research Nexus UiTM (ReNeU)
Office of Deputy Vice Chancellor (Research and Innovation)
Universiti Teknologi MARA 40450 Shah Alam, Malaysia, 15 June 2022

e-IPH e-International Publishing House Ltd., United Kingdom

Artificial Intelligence in the Tourism Industry: A privacy Impasse

Nurus Sakinatul Fikriah Mohd Shith Putera, Hartini Saripan, Mimi Sintia Mohd Bajury, Syazni Nadzirah Ya'cob

Faculty of Law,
Universiti Teknologi MARA, Shah Alam, Malaysia

nurussakinatul@uitm.edu.my, hartinisaripan@uitm.edu.my, mimisintia@uitm.edu.my, syazni@uitm.edu.my
Tel: +60195778006

Abstract
Artificial Intelligence (AI) adoption in the tourism industry has resulted with privacy concerns as companies feed a vast amount of consumer data into AI, creating sensitive customer information. Therefore, this research aims at investigating the adequacy of the Personal Data Protection Act 2010 in addressing the privacy challenges raised by AI. Combining the doctrinal methodology and a case study, this research produced systematic means of legal reasoning pertinent to AI applications in the tourism industry. Ensuring privacy and security through every phase of the data lifecycle is pivotal to avoid legal liability for the tourism players while preserving customer confidence.

Keywords: Artificial Intelligence and Law, Privacy and Artificial Intelligence, Privacy Engineering Model, Data Protection and Artificial Intelligence

DOI: https://doi.org/10.21834/ebpj.v7iSI7.3812

1.0 Introduction

In a world full of disruptive technologies, Artificial Intelligence (AI) technology is one of the most innovative inventions that have transformed various industries all around the globe. The tourism industry is not an exception (Go et al., 2020). The tourism industry is regarded as one of the key industries to drive economic growth. Thanks to the advancement of technologies, the performance and quality of service delivery within the tourism ecosystem have levelled up incrementally. AI in this context has permeated the tourism and hospitality industries after making its footprint in other prominent industries (Pagallo et al., 2018). Automating business operations and restructuring business activities have constantly been the main concepts enabled by AI in the business context to thrive in the competitive industrial setting (Loureiro et al., 2020). AI is widely utilized in the tourism sector for a variety of objectives, including, but not limited to, personalizing travel experiences, customizing consumer suggestions, and assuring speedier response, which boosts service interactions (Pillai & Sivathanu, 2020). The integration of AI has become prevalent in the industrial setting that it is being used to assist and communicate with the customers and thus strengthen the quality of engagement (revfine.com, 2019). All these will not be possible without AI's twin sister – Big Data. It is a known fact that AI performs the best when it is in possession of vast volumes of rich, big data. The more facets the data covers, the speedier the algorithms can learn and enhance their predictive assessments. These data flows have been incorporated into a global networked data-processing infrastructure in recent years, centred on, but not limited to, the Internet. This infrastructure serves as a universal platform for communication, data access, and the delivery of both private and public services. It allows citizens to buy, use banking and other services, pay taxes, receive government benefits and entitlements, gain access to information and knowledge, and

DOI: https://doi.org/10.21834/ebpj.v7iSI7.3812

develop the social connection. Algorithms, which are frequently powered by AI, mediate citizens' access to content and services, picking information and possibilities for them while also tracking any action. Today, it appears that this global networked data-processing infrastructure includes around 30 billion devices – computers, smartphones, industrial equipment, cameras, and so on – that generate vast amounts of electronic data. Figure 1 provides an idea of the growth of data creation.

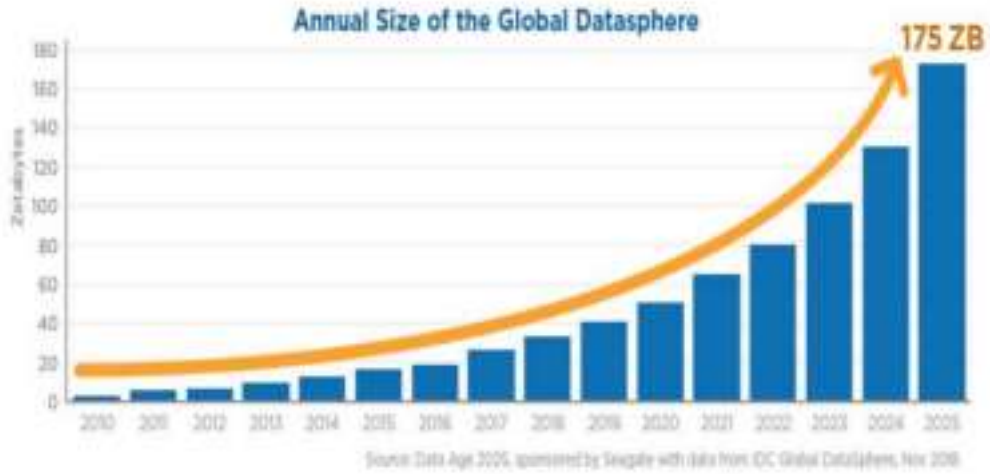

Figure 1: Growth of Global Data
Source: (Bieresborn, 2019)

Successful machine learning phases depends significantly on large and broad data sets – especially personal data. With that said, the literature is replete with discussion on the domain applications of AI within the tourism ecosystem. However, relatively little attention is given to the legality of processing personal data by AI systems resulting in privacy breaches, precisely in the Malaysian landscape. More light should be thrown on the interaction between the AI applications in the tourism industry and privacy principles embedded in the data privacy governance model in Malaysia of which this research seeks to achieve. In doing so, this research attempts to address the knowledge gap by investigating the legislative ability available in tackling AI-related data privacy breaches in the tourism industry.

2.0 Literature Review

2.1 The Friction between AI and Data Privacy Principles

Privacy concerns ought to be the emphasis of the entire development and deployment of Black-Box Artificial Intelligence (AI) (Adadi & Berrada, 2018). Privacy in this sense is pivotal in at least two areas: gathering a massive amount of data for the machine learning phase and processing the data to identify and infer the intended patterns (London, 2019). Algorithm developers need to assemble data from multiple sources to train machine learning algorithms. Hose data—as well as data about how the algorithms perform in practice— may then be shared with other entities in the system for behaviour prediction. In each case, AI-related data privacy risks are a concern, most notably as mandated under the Personal Data Protection (PDPA) 2010. Sensitive information leakage, creating discriminatory treatment and systemic disparities in society (Article 29 Data Protection Working Party, 2018) as well as impenetrable black-boxed internal operation of AI (Sullivan & Schweikart, 2019) causing the inability to evaluate the reliability and fairness of the system are instances of privacy risks evident in today's AI-driven world. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted in 1980, articulate eight basic principles of data privacy protection: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability (Stead, 2018). Most data privacy governance models in the world introduce requirements based on these principles, including the PDPA 2010. AI, however, is in tension with most of these data privacy principles (European Data Protection Supervisor, 2016). The core of these principles is ensuring that personal information ought to be utilised coherently with the privacy protection of the data subject and that individuals are entitled to decide how their personal data is used.

2.2 AI an Accountability Gap

Notably, the concept of accountability mandates the preservation of records of the purpose of processing activities in several circumstances, all while organisations handle personal data at the risk of undermining individuals' rights and freedoms. Section 6 of the 2 PDPA provides that in processing a person's personal data, that person's consent (as the data subject) must be obtained (Personal Data Protection Act 2010 (Act 709), 2010). The data user must also ensure transparency between the data user and data subject before any processing data activities are conducted. It is to make sure the consent given by the data owner is informed consent and to avoid conflicts. This is evidently a challenging criteria for businesses that utilize AI-driven technologies to meet, given the fact that the end goal of data analysis is not always clear at the beginning and may vary in tandem with discovery of new correlations in the data (Kaplan & Haenlein, 2019). This problem is even more apparent in the tourism industry as the sector is highly vulnerable to privacy breaches primarily due to its enormous fragmentation, the complexity of the travel booking and payment networks involving numerous agents and third-party service

providers, the poor privacy policy embedded within the IT and point-of-sale (POS) systems, the millions of travellers interacting with travel organizations in the cyberspace and many more factors (Paraskevas, 2020). Likewise, organizations are obligated to adopt privacy and security measures that are "appropriate to the risk" involved in the processing of that data. For organizations that utilize AI applications, where the level of risk often evolves in parallel with the AI's use, given its adaptive and self-learning nature, this may be a difficult requirement to adequately comply with (Wischmeyer & Rademacher, 2019). Additionally, organizations habitually confide in individuals' consent to legitimize the processing of personal data, AI techniques nevertheless, render the attainment of meaningful consent to be difficult for relevant individuals (Torre et al., 2020). This has led to the introduction of the Explainable AI by the legal and technical scholars to provide sufficient clarification as to how AI derives its outcome, however, the discussion has not given any directions as to its implementation. Organizations that utilize AI applications may therefore seek out for more unique approach to obtain consent when necessary, such as by requesting consent from individuals at various times throughout the program's use or through exploration of agent-based consent made by software agents on behalf of individuals.

2.3 AI, Automated Decision, and the Issue of Profiling

A further challenge relates to the right to be given an explanation by a natural person of decisions based on automated processing affecting an individual's access to enormous social services such as credit scoring, housing and employment loans and many more (Araujo et al., 2020). The outcome of machine learning algorithms results from enormous compilations of data suggesting the non explainable state of its operation; black box AI (Holzinger, Langs, Denk, Zatloukal, & Müller, 2019). In these circumstances, it may not be possible to give a more meaningful explanation than a description of the processes used and the categories of data that have been input into it (Zerilli et al., 2019), to a certain extent, causing discriminatory treatment to the data subjects. The Black-Box AI and automated decision making of AI are not specific to the Tourism industry, however, given the colossal personal data accumulated at the pre-stage, during and post travelling phases, these concerns are further augmented and alarming. A real-life example of such algorithmic discrimination occurred in the United States where an algorithm that was used to allocate healthcare to patients was systematically discriminating against people of colour by allocating lower risk scores to them even when they suffered the same ailments as their white counterparts. As a result, such people of colour were less likely to be referred to programmes that provided more personalized care (Silberg & Manyika, 2019). Such discriminatory occurrences have the potential to deprive data subjects of core rights such as the respect for human dignity, freedom, equality, the rule of law and respect for human rights to mention just a few. If this discrimination that could be occasioned by AI goes unchecked, it has the potential to wipe out the benefits of AI in one breath as the courts are usually unhesitant in nullifying any form of discrimination. Imagine if AI chatbots categorize travellers based on data it collects from the traveller's online shopping and credit expenses, denying their rights to premium services and luxury destinations packages or worse, prohibition of traveller's access to certain countries based on their skin colour, race or gender due to the misinterpretation of AI facial recognition. Whilst Section 3(2) of the PDPA specifically exempts the act of data processing outside Malaysia unless it is intended to be processed further in Malaysia, the activity of surveillance and profiling of Malaysian citizens performed outside Malaysia has become increasingly inevitable due to the rapid expansion of digital economy which is not addressed by the PDPA (Personal Data Protection Act 2010 (Act 709), 2010). To close the gap between personal data laws in Malaysia and the GDPR which provides data subjects with the right not to be subject to a decision based solely on automated processing, including profiling that produces legal effects concerning them or significantly affects them, the Commissioner is considering expanding the application of the PDPA to data users outside Malaysia who monitor and actively profile Malaysians (InsiderTAPS, 2020).

2.4 AI and Security Concerns

Due to the large volume of big data being processed by AI systems coupled with the sensitivity of such personal data, its security is a very important topic. The security of personal data used by AI applications in medical tourism especially could be at more risk given that personal data is needed for testing and experimenting environments. This is because to carry out the machine learning process through which AI systems are trained to perform their tasks, large volumes of big (personal) data are uploaded into AI systems and except there are proper security measures in place, this may impact negatively on the confidentiality, integrity, availability and resilience of processing systems and services (Bae et al., 2018). There is also the tendency that personal data could be accessible to more people than would ordinarily have access to it in the traditional practice of medicine. For instance, in Telerobotic/telemedicine surgeries and robot-assisted surgeries, engineers and information security experts will be some of the experts needed as part of the team for such surgery due to the fundamental nature of computer systems and technology to that process. Sensitive personal data will also be uploaded on different computer systems and transmitted both online and offline. This could raise serious concerns like the hacking of such systems, unauthorized access amongst other non-medical personnel experts on (or even outside) the team who should not have access thereby granting data access to unauthorized persons in infraction of the extant data protection laws.

3.0 Methodology

This study compares its activities to those of a legal interdisciplinary interest, a method for developing legal arguments involving input from other fields of knowledge, in this case, Artificial Intelligence, information security and data protection law (Naudé Fourie, 2015). In the context of this research, the doctrinal analysis is employed to synthesize rules, principal, norms, interpretive guidelines, and framework (Hutchinson & Duncan, 2014), in which it explains or makes coherent of intersection of the data protection law and the AI-powered privacy-sensitive data analysis. The principal purpose of the doctrinal legal research, includes, among others, the development and construction of new legal principles, upholding legal scholarship, and the maintenance of certainty and consistency in the legal realm. It is argued that the primary objective of doctrinal legal study is to enhance the significant portion of the law (Kharel, 2018), which can most likely impact

the bigger picture where the law is not simply just a mechanism to regulate conduct. This research explores sources for the doctrinal analysis approach depicted in written sources such as statutory legislation, case law, regulation guideline documents, journal articles and reports retrieved from a library-based search. The library-based search was aided by the UiTM Online Public Access Catalog (OPAC) system to identify primary data such as the Personal Data Protection Act 2010, the General Data Protection Regulation and law cases (Ghapheryc & White, 2012). Whereas the secondary data consisted of journal articles and reports were obtained by browsing law databases such as the Malayan Law Journal, the Current Law Journal, HeinOnline and other databases, namely Springer, ScienceDirect, SAGE, Emerald and others.

Data analysis approaches adopted by this research include the comparative method and interpretive method. For comparative analysis, this research leverages this method in producing suggestions to improve the current legal position on AI in the tourism industry (Nelken, 2016). In general, comparative analysis observes a systematic perusal of rules, procedures, institutions, implementations within a single or multiple legal systems based on objective comparative assessments of similarities, differences and their repercussions (Van Hoecke, 2016). A jurisdiction is selected as the country comparison for it provides more legal certainty and a better response to a particular event (Von Mehren et al., 1988). For comparative analysis, this research leverages this method in producing suggestions to improve the current legal position on AI in the tourism industry (Nelken, 2016). In general, comparative analysis observes a systematic perusal of rules, procedures, institutions, implementations within a single or multiple legal systems based on objective comparative assessments of similarities, differences and their repercussions (Van Hoecke, 2016). A jurisdiction is selected as the country comparison for it provides more legal certainty and a better response to a particular event (von Mehren et al., 1988). For this research, the European Union is selected as the jurisdiction comparison given the formulation of the research question that emphasizes the adequacy of the Malaysian data privacy governance in regulating AI-related privacy breaches. In this setting, the researchers' prior knowledge of the EU as the leading jurisdiction with a comprehensive global framework on privacy is used as the taxonomy of comparison (Pieters, 2009).

4.0 Findings

Artificial Intelligence has been tremendously fuelling a succession of advancements and applications in the tourism industry, which includes changing or revolutionising destination management organisations (Zsarnoczky, 2017), tourism enterprises everyday operations (Go et al., 2020) and ultimately personalising tourists' travel experiences (Buhalis et al., 2019). At its foundation, AI is built on training and inference, which necessitate a vast amount of (training) data being supplied to the algorithm in order for it to continuously adapt, develop and learn how to make judgments (inferences) on its own (Scality, 2019). With the information intensive nature of the tourism industry, AI may promote more and more invasive use of consumer data despite higher risks for privacy breaches. Likewise, cost-efficiency and better business performance offered by AI could tempt enterprises to abandon their pledge in privacy or data security. The current data privacy governance model enshrined in the Personal Data Protection Act 2010 in this context, is obsolete in addressing the privacy risks of AI applications in the tourism industry. It revolves around the following issues:

4.1 The Inability of the Personal Data Protection Act 2010 in Governing the Illegitimate Use and Processing of Consumer Data

The requirements set forth under Section 6 of the PDPA requiring that personal data should be processed lawfully and transparently are the fundamental principles of data protection law (Personal Data Protection Act 2010 (Act 709), 2010). These principles require that personal data should be processed based on a justifiable legal basis and that the nature and purpose of the processing activity should be clearly communicated to the data subjects. AI, however, processes large volumes of big data with a high tendency to discover more purposes for data processing (known as the repurposing of data) which were not identified at the beginning of the processing activity. In the repurposing of data, the processing of personal data on a justifiable legal basis as well as informing data subjects about the new purposes for the processing operation are gradually impossible for the data controllers (Duan et al., 2019). This is because the initial legal basis that was used for the processing activity may not be applicable for the further use that is uncovered. In data repurposing, adequate information about the nature and purpose of the processing activity must also be provided in a manner that the data subject must know when to expect privacy and when he or she may part with his/her privacy (Coeckelbergh, 2020). For example, AI has allowed tourists to rely on automated systems such as intelligent personal assistants or chatbots, a system that is capable of replicating its human counterparts of imprecise or defined characteristics leading to a possibility of creating interactions or conversations (Ukpabi et al., 2019). These personalised customer service systems are originally used to provide speedy responses to a customer's needs, eventually increasing services encounters. Unfortunately, the accumulation of data by these systems is manipulated to exploit customers' preferences and consumer behaviour in the quest of the tourism providers to increase profit-making (Um et al., 2020).

4.2 The Absence of Provision of Control under the PDPA 2010 on Endpoint Security to Reduce the Risk of Breaches of Sensitive Data by AI Systems

Due to the large volume of data being processed by AI systems coupled with the sensitivity of such personal data, its security is crucial. For example, AI-based facial recognition technologies streamline the otherwise tedious airports and other forms of station check ins, without the need for any in-person document verifications by the relevant authorities. The technology is a form of biometric artificial intelligence which possesses the ability to recognise or authenticate a person's identification based only on their face and typically works by comparing a digital image or video frame to the faces in a database, matching up facial features and/or skin textures. Despite its enormous contribution, the technology has been considered as rather invasive due to its collection of biometric data which are at risks of being exploited or misused if it reaches the wrong hands. The PDPA 2010 in this sense is vague in providing safeguards to control the way biometric are handled, especially as databases of biometric data that are often targeted by identity thieves (Pascu, 2020). Having

biometric data compromised can be catastrophic as the damage caused by its loss can be deadly. Additionally, there is also the issue of technological inaccuracy which plagues facial recognition software owing to its relatively early phase of development and the trial-and-error approach associated with it. The lack of accuracy may seem as a minor setbacks in comparison to the benefits derived from such technology but it could also potentially lead to misidentifications, erroneous diagnoses, wrongful convictions, and false arrests (Intellectyx, 2020).

4.3 The Failure of The PDPA 2010 in Addressing the Unauthorised Data Profiling and Discrimination Generated by AI Models

As mentioned earlier, AI relies extensively on data, notably personal data, to realise its full potential. AI supports and operates on the data-driven models maximizing the amount of information on individuals for identification and tracking, to extrapolate their identity and ultimately, predict their behaviours (Obschonka & Audretsch, 2020). This model has drawn the interest of the tourism industry players to optimise its abilities in generating strategic planning endeavours in tourism destinations, hospitality management, customer relation management and destinations advertising (Miah et al., 2017). The data analytics capabilities of AI are promising for the tourism industry but at a cost. It is now observed that AI applications are gradually playing a role in determining access to credit scoring, housing loans and other social services. Mostly without the knowledge or consent from consumers, AI is utilised to automatically categorise, assess and rank people, eventually denying the avenues to challenge the outcomes, reliability or effectiveness of those processes (Sartor, 2020). AI generates profiles and decisions that are gleaned from both the data that we have willingly submitted and those obtained unknowingly – a data profiling process. Although Regulation 3(1) of the PDPA 2010 stipulates that the consent from the data subject is required to process personal data, however, the provision is unclear as to what amounts to 'sufficient' or 'explicit' consent as the basis for processing personal data and sensitive personal data under Section 6 of the PDPA 2010 (Lexology, 2020). This data profiling issue is coupled with AI's aptness in finding correlations in datasets, leading to discrimination that data subjects could suffer based on the biases that have been trained into the algorithms of the AI system during the machine learning phase. The fact is that any AI system that has been designed to classify, rate or produce any useful result to justify any decision is bound to discriminate in the sense of making distinctions between people based on certain features. There are yet to be standardized and generally accepted thresholds regulating the development of algorithms in this sense under the PDPA 2010. The implication of this is that these algorithms could therefore be subject to the biases of the engineers, system, processes, non-divergent data categories and even non-divergence in the data subjects that are used at the development and trial stage with varying consequences of grave proportions for unrepresented or underrepresented data subjects (Manyika et al., 2019).

5.0 Discussion

The abovementioned problems have become indispensable and call for a revisit on the existing data privacy governance model enshrining the PDPDA 2010 in Malaysia. Conversely, the possibility of adopting the privacy engineering model mandated by law as a better data privacy governance model ought to be emphasised in following the global trend for data privacy and data protection laws. Over the previous few decades, various data protection efforts in Europe have evolved, including work on privacy standards, privacy engineering, and awareness-raising events. The privacy engineering model, in particular presupposes safeguarding privacy by developing measures that incorporate the fundamentals of data protection in the technological system of information processing structure. Table 1 and Table 2 below provide the overview in terms of how and where different privacy-by-design strategies can be applied.

Table 1: Data-related Tasks

Data-related tasks	
Minimise	Limit as much as possible the processing of personal data.
Separate	Separate the processing of personal data as much as possible from the data itself.
Abstract	Limit as much as possible the detail in which personal data is processed.
Hide	Protect personal data or make it un-linkable or unobservable. Make sure it does not become public or known.

Source: (Hoepman, 2018)

Table 2: Process-related Tasks

Process-related tasks	
Inform	Inform data subjects about the processing of their personal data in a timely and adequate manner.
Control	Provide data subjects adequate control over the processing of their personal data.

Enforce	Commit to processing personal data in a privacy-friendly way and enforce this adequately.
Demonstrate	Demonstrate that you are processing personal data in a privacy-friendly way.

Source: (Hoepman, 2018)

5.1 The Privacy Engineering Model in Governing AI-related Privacy Risks

In essence, privacy engineering is the theory of understanding the integration of privacy as a non-functional requirement in systems engineering (Spiekermann & Cranor, 2009). Generally, privacy is supplementary to the system's primary purpose given its appearance as a functional requirement. It may be required for compliance purposes, customer trust, risk management, or ethical concerns, but, in theory, the base system usually functions without consideration given to privacy (Duncan, 2007). Integrating principles into the systems engineering life cycle help to foster business operations and core objectives. For some organizations, privacy engineering's primary motive will be for regulatory compliance purposes or reducing organizational risk (Del Alamo, 2016). Beyond that, organizations may need to protect their reputation or brand in the market or leverage privacy as a differentiator or competitive advantage. Given the breadth of this model, this research proposes the incorporation of 3 variants to develop a more efficient privacy governance model for AI in Malaysia.

5.1.1 Automated Compliance and Tools for Transparency

Scholars argue that automating forms of regulation in a digital world are imminent. While the area is receiving tremendous attention and debates, the implementation of such an approach is already evident. Based on the limitations of the existing data privacy governance model, the PbD model is considered to be the prime solution in governing the privacy risks modelled by modern technologies (Barati et al., 2020). The PbD model is originally entrenched in systems engineering. Yet, it is the global data privacy governance that resuscitates this concept as applied to AI and Big Data. Increasingly, the long arm of the law is extending into AI fuelled by Big Data, but certainly not via regulatory enforcement that PbD is being thrust into the spotlight once more (Everson, 2019). The European Union General Data Protection Regulation (GDPR) spearheaded the incorporation of Privacy by Design and Privacy by Default in its effort to develop best practices for privacy, accountability and trust (Layton, 2017). The provision compels the controller to devise appropriate technical and organizational measures in complying with the requirements of the GDPR and protect the rights of data subjects to ensure that, by default, only personal data that are required for each definite purpose of the processing are processed. The method is based on the incorporation of privacy into the design requirements of technologies, business processes, and physical infrastructures (Romanou, 2018). PbD, as a pedagogical framework, encourages managers and creators to consider the data and privacy interests that will be consumed from the outset of the design process, rather than as an afterthought in the development lifecycle (Everson, 2019). In review, the fundamental principles of PbD include: 1) proactive, not reactive, preventative not remedial; 2) privacy as the default setting; 3) privacy embedded into design; 4) full functionality-positive-sum, not zero-sum; 5) end-to-end security full lifecycle protection; 6) visibility and transparency-keep it open, and 7) respect for user privacy-keep it user-centric. The approach has been given a wide recognition by the international community, evident by the adoption of a resolution on Pbd at the 32nd International Conference of Data Protection and Privacy Commissioners (Resolution on Privacy by Design, 2010), incorporation of PbD as a statutory requirement in the GDPR, acknowledged as one of the best practices of data privacy governance model by the US Federal Trade Commission (Federal Trade Commission, 2015) and treated as a referral point in the Japanese Diet Resolution during the amendment course of the Japanese Personal Information Protection Act (Japanese Cabinet, 2016). The risk of neglecting the PbD model precedes the development of privacy-related solutions or a data management culture embedded with highly confidential data attributes but with a significantly limited controls framework. Notwithstanding the extensive chorus of discussion on the potential of the PbD model as the emerging data privacy governance that is robust, the investigation of each of its core tenants underlying the 7 foundational principles is absent. It is therefore presumed that through in-depth comprehension of all the 7 fundamental principles that the applicability of PbD within the tourism industry is best considered, which this research attempts to accomplish.

5.1.2 User-centered Data Protection

The principle of user-centricity has always been an ideal foundation within the aspect of data protection. Nevertheless, the increasing scenario of abusive utilisation of personal data has resulted in calls to return the exercise of control of such data to the users. The users' consent must be obtained as to the specific purpose their personal data is collected (Sobolewski et al., 2017). On top of this, at all times, users should be entitled to freedom of choice in retaining rights to be forgotten, to object to processing, to the portability of data on request and to object to profiling to ensure users' empowerment in protecting their own personal data.

5.1.3 Shared Computation Space for Data Analytics

The primary goal of shared computation space is to enable the exchange of analytics or analytics outcomes rather than share data. This can be accomplished by creating a shared computational environment that functions as a trustworthy third party using trust mechanisms based on encryption or data transformation (Curry et al., 2021). Previously, such a third party needed to be a legal entity, now this third party can be a computational, transformed space. The benefit of such a space is that only aggregated data or locally calculated analyses are given, allowing one to collaborate with both trustworthy and less trusted partners without disclosing one's data. At the moment, there are several drawbacks: multi-party computing does not function effectively for all data manipulations and this can be detrimental towards its performance.

6.0 Conclusion and Recommendations

AI is transforming the way we live, work, and socialize. Already on the market are virtual personal assistants, recommendation engines, self-driving cars, surveillance systems, crop prediction, smart grids and others. More recently, as AI is significantly improving, businesses in the tourism sector, in particular, are using AI to automate some administrative and customer service tasks. Nonetheless, the tourist's information privacy issues generated by the big data available to the destination and service providers are key challenges, which are detrimental to the tourism industry's sustainability and economic value. This research investigates the privacy concerns that AI brings to the table and eventually the adequacy of the existing Malaysian data protection law in addressing the privacy risks posed by AI. While this research contributes to highlighting the AI-related privacy risks in the tourism industry, future investigations are necessary to validate the kinds of conclusions that can be drawn from this study. It is a question of future research to devise a more preventative and evidence-based approach to assuring privacy in the tourism industry via the privacy engineering model, eventually fostering trustworthiness in the governance of AI. This can be done by verifying the 3 variants proposed by this research empirically, as the framework of the privacy engineering model for a better privacy governance model in Malaysia. The findings of this research are significant to advocate the integration of the privacy and principles of personal data processing into AI systems, eventually fostering the sustainability of the tourism industry post-pandemic. The outcome of this research is also expected to be in tandem with the Strategic Thrust 2 of the Shared Prosperity Vision 2030, aiming at developing cluster-based ecotourism destinations through transformative technologies outlined in the Key Economic Growth Activities (KEGA) 14 (Advanced & Modern Services) and also the National Ecotourism Plan 2016-2025.

Acknowledgement

The authors would like to express their gratitude for the financial support from Universiti Teknologi MARA under the Lex Praesta Research Grant (600-TNCPI 5/3/DDF (FUU) (001/2020) granted for this research.

References

Adadi, A., & Berrada, M. (2018). Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI). *IEEE Access*, *6*,52138-52160.

Araujo, T., Helberger, N., Kruikemeier, S., & de Vreese, C. H. (2020). In AI We Trust? Perceptions About Automated Decision-Making by Artificial Intelligence. *AI and Society*, *35*, 611-623.

Article 29 Data Protection Working Party. (2018). Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679. *October*. Bae, H., Jang, J., Jung, D., Jang, H., Ha, H., & Yoon, S. (2018). Security and Privacy Issues in Deep Learning. In *arXiv*, 1-20. Barati, M., Rana, O., Petri, I., & Theodorakopoulos, G. (2020). GDPR Compliance Verification in Internet of Things. *IEEE Access*, *8*, 119697- 119709.

Bieresborn, D. (2019). The Impact of the General Data Protection Regulation on Social Security. In *ERA Forum*, *20*, 285-306. Buhalis, D., Harwood, T., Bogicevic, V., Viglia, G., Beldona, S., & Hofacker, C. (2019). Technological Disruptions in Services: Lessons from Tourism and Hospitality. *Journal of Service Management*, *30(4)*, 484-506.

Coeckelbergh, M. (2020). AI Ethics. In *AI Ethics*.

Curry, E., Metzger, A., & Pazzaglia, S. Z. J. (2021). The Elements of Big Data Value. In *Springer*.

Del Alamo, J. M. (2016). Privacy Engineering: Shaping an Emerging Field of Research and Practice. *IEEE Symposium on Security and Privacy*, *14*(2), 40-46.

Duan, Y., Edwards, J. S., & Dwivedi, Y. K. (2019). Artificial Intelligence for Decision Making in the Era of Big Data – Evolution, Challenges and Research Agenda. *International Journal of Information Management, 48*, 63-71.

Duncan, G. (2007). Engineering: Privacy by Design. *PubMed*, *317*(5842), 1178–1179.
European Data Protection Supervisor. (2016). Artificial intelligence, Robotics, Privacy and Data Protectuion. *38th International Privacy Conference*.

Everson, E. (2019). Privacy by Design: Taking Ctrl of Big Data. *Cleveland State Law Review*, *65*(1), 27–43. Ghapheryc, J., & White, E. (2012). Library use of Web-based Research Guides. In *Information Technology and Libraries*, *31*(1), 21-31. Go, H., Kang, M., & Suh, S. B. C. (2020). Machine Learning of Robots in Tourism and Hospitality: Interactive Technology Acceptance Model (iTAM) – Cutting Edge. *Tourism Review*, *75*(4), 625-636.

Hoepman, J.-H. (2018). Privacy Design Strategies (The Little Blue Book). *Transactions of the Canadian Society for Mechanical Engineering*, 30.

Hutchinson, T., & Duncan, N. (2014). *Defining and Describing What We Do: Doctrinal Legal Research*. *Deakin Law Review, 17*(1), 83- 119.

InsiderTAPS. (2020). *PDPA Alert: Proposed Amendments to the Personal Data Protection Act 2010 MARCH*. Intellectyx. (2020). *Facial Recognition in Retail and Hospitality: Cases, Law & Benefits*. 2020. Retrieved fromhttps://www.intellectyx.com/blog/facial-recognition-in-retail-and-hospitality-cases-law-benefits/

Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in My Hand: Who's the Fairest in the Land? On the Interpretations, Illustrations, and Implications of Artificial Intelligence. In *Business Horizons*, *62*(1), 15-25.

Kharel, A. (2018). Doctrinal Legal Research. *SSRN Electronic Journal*, *23*(2), 1-16.

Layton, R. (2017). How the GDPR Stacks Up to Best Practices for Privacy, Accountability and Trust. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2944358

Lexology. (2020). *PDPA Alert: Proposed Amendments to the Personal Data Protection Act 2010* - 2020. Retrieved from https://www.lexology.com/library/detail.aspx?g=f0386bab-cc6c-432c-a680-978df77b366e

London, A. J. (2019). Artificial Intelligence and Black-Box Medical Decisions: Accuracy Versus Explainability. *Hastings Center Report*, *49*(1), 15–21.

Loureiro, S. M. C., Guerreiro, J., & Tussyadiah, I. (2020). Artificial Intelligence in Business: State of the Art and Future Research Agenda. *Journal of Business Research*, *129*, 911-926.

Manyika, J., Silberg, J., & Presten, B. (2019). What Do We Do About the Biases in AI? In *Harvard Business Review*. Retrieved from https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai

Miah, S. J., Vu, H. Q., Gammack, J., & McGrath, M. (2017). A Big Data Analytics Method for Tourist Behaviour Analysis. *Information and Management*, *54*(6), 771–785.

Personal Data Protection Act 2010 (Act 709), Gazette 1 (2010).

Naudé Fourie, A. (2015). Expounding the Place of Legal Doctrinal Methods in Legal-Interdisciplinary Research. *Erasmus Law Review*, *3*, 95-110.

Nelken, D. (2016). Comparative Legal Research and Legal Culture: Facts, Approaches, and Values. In *Annual Review of Law and Social Science*, *12*, 45-62.

Obschonka, M., & Audretsch, D. B. (2020). Artificial Intelligence and Big Data in Entrepreneurship: A New Era has Begun. *Small Business Economics*, *55*, 529-539.

Pagallo, U., Corrales, M., Fenwick, M., & Forgó, N. (2018). The Rise of Robotics & AI: Technological Advances & Normative Dilemmas. In *Perspectives in Law, Business and Innovation*. Springer Singapore, 1-13.

Paraskevas, A. (2020). Cybersecurity in Travel and Tourism: A Risk-Based Approach. *Handbook of E-Tourism*, *June*, 1–24. Pascu, L. (2020). *Malaysia Commissioner Wants Facial Biometrics Security in Personal Data Protection Act*. 2020. Retrieved from https://www.biometricupdate.com/202003/malaysia-commissioner-wants-facial-biometrics-security-in-personal-data-protection act

Pieters, D. (2009). Functions of Comparative Law and Practical Methodology of Comparing. *Research Master in Law.*, 1–35. Pillai, R., & Sivathanu, B. (2020). Adoption of AI-based Chatbots for Hospitality and Tourism. *International Journal of Contemporary Hospitality Management*, *32*(1), 3199-3226.

Romanou, A. (2018). The Necessity of the Implementation of Privacy by Design in Sectors Where Data Protection Concerns Arise. *Computer Law and Security Review*, *34*(1), 99-110.

Sartor, G. (European U. I. of F. (2020). The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence. *Panel for the Future of Science and Technology (STOA)*.

Scality. (2019). *How AI Needs Data Like a Rocket Needs Fuel - Scality*. Retrieved from https://www.scality.com/how-ai-needs-data-like a-rocket-needs-fuel/

Silberg, J., & Manyika, J. (2019). Notes From the AI Frontier : Tackling Bias in AI (and in Humans) Article. In *McKinsey Global Institute*, 1-6. Spiekermann, S., & Cranor, L. F. (2009). Engineering Privacy. *IEEE Transactions on Software Engineering*, *35*(1), 67-82. Stead, A. (2018). Data Protection Principles. In *Information Rights in Practice*, 191.

Sullivan, H. R., & Schweikart, S. J. (2019). Are Current Tort Liability Doctrines Adequate for Addressing Injury Caused by AI? *AMA Journal of Ethics*, *21*(2), 160-166.

Torre, D., Abualhaija, S., Sabetzadeh, M., Briand, L., Baetens, K., Goes, P., & Forastier, S. (2020). An AI-Assisted Approach for Checking the

Completeness of Privacy Policies Against GDPR. *Proceedings of the IEEE International Conference on Requirements Engineering*, 136-146.

Ukpabi, D. C., Aslam, B., & Karjaluoto, H. (2019). Chatbot Adoption in Tourism Services: A Conceptual Exploration. *Robots, Artificial Intelligence and Service Automation in Travel, Tourism and Hospitality*, *January 2020*, 105–121.

Um, T., Kim, T., & Chung, N. (2020). How Does an Intelligence Chatbot Affect Customers Compared with Self-Service Technology for Sustainable Services? *Sustainability (Switzerland)*, *12*(12), 5119.

Van Hoecke, M. (2016). Methodology of Comparative Legal Research. *Law and Method*, 1-35.

Von Mehren, A. T., Weir, T., Zweigert, K., & Kotz, H. (1988). An Introduction to Comparative Law. *The American Journal of Comparative Law*, *36*(4), 782-783.

Wischmeyer, T., & Rademacher, T. (2019). Regulating Artificial Intelligence. In *Regulating Artificial Intelligence*. Zerilli, J., Knott, A., Maclaurin, J., & Gavaghan, C. (2019). Transparency in Algorithmic and Human Decision-Making: Is There a Double Standard? *Philosophy and Technology*, *32*, 661-683.

Zsarnoczky, M. (2017). How Does Artificial Intelligence Affect the Tourism Industry? *Journal of Management Social Sciences Vadyba Journal of Management*, *31*(2), 85-