UUM JOURNAL OF LEGAL STUDIES
https://e-journal.uum.edu.my/index.php/jls

How to cite this article:
Hesam Nourooz Pour. (2025). Data protection challenges in smart cities: An examination of the Malaysian legal framework. *UUM Journal of Legal Studies*, *16*(1), 115-129. https://doi.org/10.32890/uumjls2025.16.1.7

DATA PROTECTION CHALLENGES IN SMART CITIES: AN EXAMINATION OF THE MALAYSIAN LEGAL FRAMEWORK

Hesam Nourooz Pour
Faculty of Law, University of Malaya, Malaysia

Corresponding author: s2106772@siswa.um.edu.my

Received: 6/6/2023 Revised: 14/5/2024 Accepted: 22/10/2024 Published: 31/1/2025

ABSTRACT

Smart cities are the future of urban development as they incorporate state of the art technology to enhance the living standards of the citizens. However, these advances have real challenges in terms of data protection, more so in countries like Malaysia, where the legal aspects are still developing. This paper will critically analyze Malaysia's legal framework for data protection in the context of the Malaysian Smart City Framework and its data collection and processing practices. In this paper, the three fundamental principles of data protection, namely necessity, consent and safeguards will be examined. Using a comparative law approach, this research compares Malaysian laws with international standards, in particular the General Data Protection Regulation of the EU. This comparison shows some serious gaps and hurdles in Malaysia's approach, particularly with regard to protection from automated decision-making and surveillance technology. This research will also show that Malaysia must improve its legislation to ensure privacy will not be invaded when the smart city technologies are have already become so widespread. The findings advocate the need for Malaysian laws and policies to be positively realigned with technology to create a privacy-aware model and fit for purpose for the shifting requirements of smart urban arenas.

Keywords: Smart cities, data protection, artificial intelligence, comparative legal analysis, personal data protection act.

INTRODUCTION

The concept of 'smart cities' is fast becoming a touchstone for urban development across the world in a rapidly changing digital landscape. Such high-tech urban spaces utilize advanced technologies such as

the Internet of Things (IoT) and artificial intelligence (AI) to realize the vision of a better quality of life, efficient operations, better economic development, and increased sustainability. Basically, due to this recent global trend, Malaysia was bound to implement the Malaysian Smart City Framework (MSCF) in 2018, stating categorically a broad-based vision for urban digital transformation.

The MSCF is implemented within a larger legal landscape that includes laws and regulations such as the Personal Data Protection Act 2010 (PDPA). Issues related to data protection, specifically regarding data collection and processing that are integral to smart city operations, remarkably when AI technologies are at play, are not squarely addressed by the MSCF (Bunders & Varró, 2019). Recognizing this, the capability of the legal environment in Malaysia for the creation of 'privacy-aware' smart cities will be critically examined in the present study, with an emphasis on data protection, in respect of its core elements: necessity, consent, and safeguards. These elements constitute the base for any lawful and ethical collection and processing of data and are quite important in ensuring trust and security in any smart city's operation.

This research will focus on this main question: How well does the current legal framework in Malaysia address the challenges that will come up with data protection, especially within the smart city context? In answering this question, the study has adopted a qualitative research methodology, drawing on legal analytics and comparative case studies as the main investigative tools. A careful perusal of relevant legal documents has allowed for the dissection of Malaysia's legal environment in relation to data protection in smart cities. Equally important was the examination of case studies from other jurisdictions, which would provide insights into international standards and best practices related to AI-driven data protection.

In the literature review, detailed discussions were carried out on the concept of smart cities and the MSCF, especially from the perspective of legal principles related to data protection and within the framework of new technologies such as AI. In the following section, the legal challenges of the infusion of data protection laws in the design and implementation of smart cities will be explored. The third part of the study is devoted to a detailed analysis of the following three major principles of data protection: necessity, consent, and safeguards. In so doing, the present systematic inquiry makes it possible for one to take a structured walk across the legal landscape of data protection in a smart city.

LITERATURE REVIEW

The Notion of a Smart City

The term 'smart city' embodies numerous ideas that have developed significantly since its début in the 1990s (Vasseur & Dunkels, 2010). The earliest discussions were about the contribution of ICT to the development of urban infrastructures (Alawadhi et al., 2012). Over time, this rhetoric has grown to encompass social capital and urban development, reframing 'smartness' as an agent of sustainable growth and improved quality of life. Two dominant views have been put forward in the literature so far, both critical but complementary. The first is anchored in smart governance, where technologies deployed in the infrastructures of cities are meant to facilitate city management and better cater to the needs of citizens (Nam & Pardo, 2014).

The second view focuses on how intelligent technologies have contributed to economic growth and the management of urban development (Saxena & Al-Tamimi, 2018). Spanning across these two views, it

is the consensus that a smart city ushers in ICT in order to make government services more effective and the citizens' life better (Cardullo & Kitchin, 2019). It refers to the intelligent, not just the implementational, use of technology. Furthermore, Giffinger et al. (2007) have identified six dimensions of a smart city, which include the following: smart economy, smart environment, smart mobility, smart people, smart living, and smart governance—all of these emphasize those aspects of urban life that can be significantly enhanced by the intelligent use of ICT.

Legal and Regulatory Challenges in Smart Cities

It is widely agreed in the literature that a smart city is the combination of technology and creativity looking for solutions to urban problems in an innovative way (Gassmann et al., 2019). Therefore, the very concept of a smart city does not rest only with the technology, which is available, but how well this technology meets the needs of the people and their surroundings. Even though, the concept of smart cities is attractive, this advancement in technology is accompanied by a number of legal and privacy issues. These issues in turn entail data privacy and security, informed consent, and accountability in the provision of algorithmic decisions.

There is the omnipresence of data collection and surveillance technologies within smart cities that will threaten the fundamental human right to privacy recognized in the Universal Declaration of Human Rights and in the International Covenant on Civil and Political Rights (ICCPR) (Bunders & Varró, 2019). Among the top privacy concerns are fears of using an individual's personal data, which could be collected through city-wide sensors and smart devices for unauthorized surveillance or unwarranted profiling of individuals (Finch & Tene, 2013). Those risks are thus, amplified by the lack of transparency in the collection practices and consent mechanisms, further eroding control over personal data by the said individuals (Bridges, 2021). In view of these challenges, many jurisdictions have ordained legal frameworks to protect privacy rights. The most notable is the General Data Protection Regulation (GDPR) by the European Union (EU), which provides strong protection for personal data, requires affirmative consent in collecting and using data, and imposes heavy penalties for breach of these provisions.

The massive data generated by various activities and services in a smart city makes, in many cases, data practices obscure, hence overwhelmingly difficult for citizens to understand how and where their personal information is being used (Finch & Tene, 2013). This concern needs strong legal frameworks that not only protect data, but also guarantee transparency and control for the data subjects. For instance, GDPR (2016) not only sets the strictest and most robust data protection regime, but also empowers data subjects with rights that put them in the driver's seat with regard the use of their data. One of those rights is expressed in Article 20 of the GDPR, hence allowing a data subject to obtain his or her data in a structured, commonly used, and machine-readable format, which enables easy transfer to another controller without undue delay.

Another regulatory model where different legal frameworks can help inform and enhance local policies is the California Consumer Privacy Act (CCPA). The CCPA stands as an exemplary model for such dynamic and evolving laws concerning data protection responses to the complexities of modern urban development. The CCPA, like the GDPR, provides a structured set of safeguards but is contextual in the unique cultural and legal context of California. This act provides strong rights to individuals over their personal data, including the right of access to personal information (Section 1798.100), the right to request deletion of personal information (Section 1798.105), and the right to opt-out of the sale of personal information (Section 1798.120). Much like the GDPR principles, though these provisions

parallel them, they introduce specific measures addressing new aspects of consumer privacy that are emerging concerns in smart city ecosystems.

The selection of these frameworks was done with due consideration to offering a broad perspective on how jurisdictions try to address the challenges of data protection faced in smart cities. The GDPR serves as a landmark for global standards on data protection and provides a robust framework, which many countries, including Malaysia, refer to when shaping their laws. Following the GDPR discussion, the inclusion of the CCPA will be used to present a different model, one that is no less rigorous and challenging from the United States, which like the EU has been pioneering and responding to concerns at the interface of technology advancement and privacy in urban environments.

The CCPA was picked specifically because it is relatively new and has pioneering provisions that address new aspects of consumer privacy, which are not as explicitly covered under the GDPR. These examples, therefore, are illustrative of the range of legislative responses to data protection in smart cities and provide comparative bases from which Malaysia might draw lessons or inspiration. While the cultural and legal context is different, exploring these frameworks allows us to show potential adaptations and come up with tailored solutions that could work in addressing the unique challenges that Malaysia is facing in the management of privacy within a smart city.

The use of AI systems in smart cities raises several concerns, in particular, regarding transparency, accountability, and non-discrimination. Some characteristics of AI—opacity, complexity, dependence on data, and autonomous behaviour—could lead to impacts on fundamental rights (Walz & Firth-Butterfield, 2019). The Artificial Intelligence Act (AI Act) by the EU seeks to address these and more concerns by developing a robust, risk-based framework for safeguarding and promoting the said fundamental rights. The Act puts in place a framework for trustworthy AI and respective obligations for all actors involved in the AI value chain, including rights such as human dignity, respect for private life, and protection of personal data; it also includes the requirement for non-discrimination and equality (AI Act, 2024).

The AI Act (2024) also considers potential prejudices and harmful impacts in high-risk AI services such as named and unnamed remote biometric identification systems in real-time and post-use, and introduces some provisions related to logging and human supervision. Furthermore, it identifies the potential dangers of law enforcement, more specifically spying and profiling based on race, as threats of AI and deems those AI systems as high-risk. These considerations underscore the importance of clarity and responsibility in the use of AI and the need for the use of appropriate data in order to train the AI so that it is free from bias and therefore more useful in that context, especially in relation to smart cities.

The Smart City Concept in Malaysia

Malaysia has been actively working towards smart cities project as part of its digitization moves. The journey in this regard is laid out in various policies and strategic development plans such as the 11th Malaysian Plan, the National Physical Plan (NPP3), the National Urbanization Policy (NUP2), Malaysia Smart City Framework (MSCF), and Malaysia Smart City Outlook (MSCO). The actions that have been set forth through the Green Technology Master Plan 2017-2030 and the Low Carbon Cities Framework (LCCF) on very environmentally friendly features also make sure that Malaysia sticks to sustainability. Malaysia is going to use technology for urban living but will also change its course of

resource distribution for building projects and will make the quality of management better (Lim et al., (2021).

The MSCF stands out as a ray of hope in this fast-pace yet difficult digital arena. The smart city development plan of the country incorporating AI, IoT and the dynamic 5G technology is embedded in the MSCF. The core of these technological advancements includes facial recognition, predictive policing, and active monitoring to ensure security. Thus, despite the charming vision of a smart city utopia, major pitfalls lurked in the shadows. While clothed with good intentions, the MSCF opens the gates for undue and grave violations of fundamental citizen rights and civil liberties if, and only if, a strong and adequate legal framework does not forestall such acts.

Nevertheless, as one threads through the discussion of smart city technologies and legal issues, the rhetoric of data protection becomes more imperative. It evokes and accentuates the urgency of implementing a holistic legal architecture which will put Malaysia in a better position to embrace the smart city direction it has long aspired.

THE LAWFULNESS PRINCIPLE IN THE SMART CITY CONTEXT

Understanding the Lawfulness Principle

The principle of lawfulness or commonly known as the legality principle, is one of the basic tenets in law (Lynn, Jr, 2009). This principle revolves around the aspect of the assumption that all acts done by private persons, corporations, or public authorities must conform to the law. In simple terms, it does not suffice for an action which is said to be lawful to exist only in books, rules or regulations; it must also be properly and reasonably exercised and not applied in a whimsical fashion (Lawson, 1995).

This principle upholds the integrity of the law, prevents abuse of power, and ensures fairness in decision-making processes. However, understanding the lawfulness principle is not solely about comprehending its definition. It also entails appreciating its far-reaching implications. Lawfulness forms the foundation of trust between citizens and government entities, corporations, and other individuals. It fosters a social contract wherein everyone agrees to abide by the rules for the collective good (Fung, 2015).

Operationalizing the Lawfulness Principle in Smart City Frameworks

As one navigates the uncharted terrain of smart city developments, the role of the lawfulness principle becomes increasingly paramount. Its application, however, brings forth a myriad of legal complexities. In the EU, for example, the GDPR enshrines the lawfulness principle in Article 5(1), dictating that personal data must be “processed lawfully, fairly and in a transparent manner in relation to the data subject”. Article 6 of the GDPR provides six legal bases that could justify data processing. These encompass a range of justifications such as obtaining the data subject's consent, meeting contractual obligations, adhering to legal requirements, safeguarding the vital interests of the data subject, executing tasks in the public interest, and fulfilling the legitimate interests of the data controller or a third party (Islam et al., 2022).

Every legal environment has its own considerations on what constitutes legitimacy. For instance, when considering consent, the assumption here is that the individual has the freedom of choice to agree to the

processing of his/ her personal data. Conversely, when talking about complying with a legal obligation or entering into a contract, the legitimacy is based on the justification and positive compliance with the laws and agreements (Taylor, 2017). This layered understanding of the principle of lawfulness provides a strong support structure for data protection legislation.

The smart city framework has imposed additional difficulties in the implementation of the lawfulness principle. This is so because it reduces free choice which is a critical aspect under the umbrella of the concept of consent in the smart city setting. This necessitates a shift from an individualistic consent-based paradigm to a framework which places the burden of responsibility on the data controllers (Chritofi et al., 2021). The new framework covers several areas such as carrying out activities for public purposes, having legitimate aims, legal measures when handling particular categories of data, and concerns regarding the processing for crime control purposes (Edwards, 2016). One of the cases in point is the growing trend that is focused on biometrics in smart city projects, which include among others facial recognition systems (Vitunskaite et al., 2019).

The concept of legality in Malaysia is very rooted in the country's legal system. Article 5(1) of the Federal Constitution of Malaysia contains a significant provision. It upholds the right of personal liberty, providing that no one can be deprived of this right without a lawful basis. The PDPA, as a key legal instrument, further represents this principle. The Act serves as a safeguard against unlawful data processing in the course of commercial transactions. The General Principle of the Act protects personal data, allowing its processing only with the clear consent of the individual.

The protection of rights in the digital sphere has also emphasized on other legal frameworks such as the Communications and Multimedia Act 1998 (CMA). This legal instrument sets out the rules on the use of networks and their components. It clearly prohibits any interference with one’s privacy that in turn brings the principle of legality into the digital sphere. The principle of legality is also embedded in the laws, for example, the Financial Services Act 2013 and the Islamic Financial Services Act 2013. Such legislation requires all financial institutions to always keep the details of their clients private and as a result, the principle has a wide reach in all those areas.

As Malaysia makes a foray into creating its own smart city, the lawfulness principle is at the forefront of its smart city vision. The MSCF guides the developers to ensure that the approach to data processing is structured, transparent, and accountable throughout the country. Despite these efforts, it is apparent that the journey of the lawfulness principle within the current legal framework is far from complete (Nor et al., 2021). While this has an impact that stretches from the constitutional foundations to the flowering of digital innovation, the legal landscape remains ongoing and should provide further development in order to accommodate the thorny issues involved in developing a smart city. This sets up the next discussion on the challenges and solutions for navigating these issues.

KEY SUBJECTS OF DATA PROTECTION IN SMART CITY FRAMEWORKS

Conventional principles of data protection are further complicated when refracted through the prisms of a smart city. In this section, the key topics of concern in data protection — necessity, consent, and safeguards — and their relevance in the automated decision-making and public surveillance indispensable to smart city operations will be analysed. Under each of those topics, the present paper looks at the adequacy and consequences of those provisions in the PDPA which address these issues and further learn from international law and literature.

Necessity

The concept of 'necessity' in the context of processing personal data, especially in smart cities, poses a number of subtle implications. In essence, necessity means a balancing act, a specific kind of delicate balancing act, between the processing of personal data and the preservation of individual privacy; this balance is all exceptionally contextual and varies according to each case-use scenario (Drachsler & Greller, 2016). Automated decision-making and profiling, at the core of smart city operations, add to the challenges of assessing necessity. As far as Malaysia is concerned, there is no definition of the ambit of necessity provided in the PDPA. It does however, contain guiding principles including the General Principle which states that "personal data shall not be processed unless the data subject has given his consent to the processing" (Section 6).

Furthermore, the Notice and Choice Principle (Section 7) requires data users to inform data subjects of the purpose for data processing, a requirement that aligns with the broader concept of necessity as it informs data subjects as to why their data is being processed. Yet, the lack of an explicit definition and guidelines on how to measure necessity, particularly in the context of automated decision-making and profiling, presents a challenge in assessing the legitimacy and ethical basis of data processing in smart cities (Christofi et al., 2021). These challenges become even more apparent when one considers initiatives like those presented in the MSCO.

The MSCO (2021) covers a digital transformative plan, which entails large volume data to be harvested. For example, smart healthcare issues enumerated in the MSCO will invoke data-driven solutions for personalized health services, prediction analytics, outbreak analysis, and telemedicine. In these cases, necessity dictates that the processing of other data will be performed only when it is absolutely necessary for the operation of smart systems and encroaches upon the rights of the individuals concerned.

Despite these nuances, the PDPA's present formulation calls into question how necessity is to be measured, especially when sensitive personal data is concerned. This regulatory gap raises concerns about justifying the extensive data processing required for these activities and ensuring sufficient measures are in place to mitigate privacy risks. The CCPA, for example, imposes certain requirements to uphold the necessity of collection and processing of personal data. Section 1798.140 of the CCPA on the minimization of data collection prohibits carrying out any processing apart from what is required for the primary focused activities. Such provisions act to enhance the direct correlation between data use and the reasons for which the data was collected in the first place, thus curbing unnecessary data processing practices.

The GDPR also requires that personal data processing must meet the requirement of "necessity" for all legal bases outlined in Article 6(1), except for cases based on consent. While the GDPR does not involve a direct definition for 'necessary,' various judgements passed by the CJEU signify the interpretation of this concept. In the *Huber* case, the Court interpreted the "public task" legal basis, concluding that necessity requires a clear and essential link between the purpose of data processing and the processing activities themselves (*Huber v. Bundesrepublik Deutschland, 2008*). The court believes that one cannot properly conduct the task without this specific data processing. Accordingly, processing of data is justified only if it is necessary for the performance of public interest objectives, or if such processing improves the performance of public interest objectives.

However, such extensive interpretation of necessity with respect to the 'public task' legal basis may have unwanted consequences, allowing the use of personal data and processing technologies to optimize almost anything that public administration can offer. This view leads to central inquiries about how far the goal of efficiency and optimization can support the pervasive spread and application of data processing technologies in the urban setting (Christofi et al., 2021).

The EU data protection authorities have gradually adopted a stricter interpretation of 'necessity,' requiring more than a simple causal link between data processing activities and their goals. This rigorous approach involves a testing method similar to that used for the 'necessity' standard in Article 52(1) of the Charter. The European Data Protection Supervisor (EDPS) clarifies that "least intrusive" means should be selected only after all alternatives are proposed and evaluated (EDPS, 2017). In its strict view of necessity, legitimate purposes must be evoked, alternatives exhaustively considered, and substantiation provided to underwrite data processing, hence making it most relevant regarding automated decision-making and profiling in smart cities. This demands an assessment of processes with a view to achieve responsible and necessary data processing.

The Singapore Personal Data Protection Act (PDPA) (2012) offers valuable guidance on interpreting "necessity." It specifies that organizations may collect, use, or disclose personal data only for purposes a reasonable person would find appropriate in the circumstances, provided individuals are informed (Section 18). This provision introduces the following two fundamental elements of necessity: "appropriate purpose" and "duty to inform."

The "appropriate purpose" provision allows indirect assessment of necessity, as a reasonable person expects data processing to be justifiable only if it is necessary in achieving the purpose stated and if no less intrusive alternatives are available (Parts 3 and 4). The approach seeks to harmonize the relationship between necessity and transparency, but this approach also establishes the basis whereby responsible data handling is supported, especially in some settings that involve heightened data processing, such as in smart cities. Similarly, the "duty to inform" supports the necessity principle by helping individuals understand why their data is needed, giving them an opportunity to assess and, if necessary, challenge the processing's necessity (Part 4). However, like Malaysia, Singapore's Act lacks a clear definition or criteria for assessing "necessity," instead relying on the subjective judgment of a "reasonable person." This reliance can lead to varied interpretations and introduces ambiguity, especially in complex areas such as automated decision-making and profiling within smart cities.

Consent

Securing data processing consent in smart cities presents a complex challenge, given the vast amount and diversity of personal data collected and processed by smart technologies. Such technology, including sensors, cameras, and AI-driven systems, are deeply embedded in public spaces and infrastructure. They continuously gather data to streamline services, track resources, and boost safety. However, their passive and omnipresent nature makes obtaining explicit, informed consent from each individual impractical, despite the fundamental role of consent in ensuring transparency, personal privacy, and citizen control over their data (Alam, 2021).

The PDPA places a high level of importance on the principle of consent, which is explicitly stipulated under Section 6 of the Act, known as the Consent Principle. The Consent Principle delineates consent as an explicit, informed agreement to the processing of an individual's personal data that is freely given by the person themselves. This implies a conscious and voluntary action on the part of the data subject

to permit their data to be processed. In other words, the individual must be adequately informed about the nature of the data processing and must voluntarily agree to it. The form of this agreement under the PDPA can be either verbal or written.

Nonetheless, the Act states that this consent cannot be considered as infinite and immutable. It allows for the possibility of the retraction of consent at any time, thus empowering the individuals over their personal data. Yet, it also recognizes practical needs by stating that withdrawing the consent does not affect the legality of data processing that occurred before the consent was withdrawn (Section 38). Moreover, the PDPA highlights the need to obtain the explicit consent of the individual before undertaking any activities involving the processing of sensitive data (Section 40). Such data includes any detail which relates to a person's health or mental condition, any political affiliations or relations, or any prior convictions. This heightened threshold of consent required from an individual prior to such sensitive data being processed underlines the Act's concern over the protection of the rights and privacy of the individuals.

While the PDPA provides a robust mechanism for protection, there are shortcomings as regards the specific details of the process of obtaining consent. The Act is silent about the extent of control, such as granularity or ability to revoke such consent. This vagueness and lack of directions poses a significant problem particularly when dealing with smart cities, where a range of data processing activities is ubiquitous, ongoing and often passive. The several modes of data processing designed for and utilized in a smart city pose serious challenges to compliance with the data protection laws on consent. It raises the issue of how to obtain consent from the individuals who are surrounded by such an all-encompassing systematic solicitation and processing of their personal information (Caron et al., 2016).

In contrast, the GDPR emphasises that 'consent' be the primary condition for the processing of personal data. Under Article 4(11), consent must be obtained prior to data processing and should be given freely, and specific, informed, and unambiguous. Underscoring the inherent meaning of consent, the processors must notice unambiguity in the assent of data processing by individuals. Furthermore, Article 7(1) highlights the role of the data controller in ensuring that the data subject has effectively consented to the processing of the subject's personal data. This provision on the obligations of the data controllers highlights the need to put in place mechanisms for the collection, storage and retrieval of the records of consent given when data is collected.

Beyond the initial granting of consent, the GDPR also empowers individuals with control over their personal data post-consent. Under Article 7(3), it is declared that the data subject shall have the right to withdraw their consent at any time. The withdrawal of consent should not be subject to any detriment and must be as straightforward as when the consent was initially given. This provision maintains a level of personal autonomy and control for individuals over their data, even after it has been processed. Further elaboration on consent is found within the GDPR's guidelines, which discusses the concept of 'granularity' in consent mechanisms. According to the Guidelines on Consent under Regulation 2016/679 (2020), consent should not be bundled together for different processing operations. Instead, consent must be obtained for each processing operation separately, thus allowing the data subject to have control over exactly which data processing operations they consent to and which they do not.

The CCPA takes a very different stance on consent, especially when it comes to selling personal information. Section 1798.120 states that businesses must disclose information about selling data and must allow consumers to opt out, this is a form of implied consent, meaning the data is sold unless the consumer opts out. That is a different approach from the GDPR's insistence on express consent and the

PDPA's emphasis on obtaining clear and intelligent consent for all data processing activities. In an attempt to increase transparency, the CCPA requires a "Do Not Sell My Personal Information" on the homepage of businesses so that it is easily accessible to the opt-out button. In addition, 1798.135 mandates that businesses allow consumers to opt-out without having to create accounts, which makes it much easier to rescind permission.

The Challenge of Public Space

According to the Malaysian Communications and Multimedia Commission (MCMC 2008) public spaces are any areas that can be accessed and utilized by the public at large. MCMC further clarifies the concept of public spaces, defining them as 'spaces that any person is entitled to access and use freely, in contrast to private spaces, where entry and use may be restricted. This encompasses spaces like public parks, public baths or swimming pools, highways, bridges, road ferries, and even public vehicles and their parking spaces as opposed to private spaces which may carry a range of limitations. The intricate dynamics of these public spaces, especially in smart cities, involve constant, pervasive, and often non-intrusive data collection, rendering informed consent a complex proposition (Kirwan & Zhiyong, 2020). Surveillance technologies, such as CCTV cameras and sensors, pervade these spaces, serving a range of purposes from ensuring safety and detecting crime, to managing traffic and safeguarding both public and private properties (Finch & Tene, 2013).

However, surveillance is inherently an infringement on personal privacy, making obtaining consent for processing personal data a nuanced challenge. Striking a balance between the legitimate interest of public safety and potential invasions of privacy necessitates careful calibration of how, when, and what sensitive data can be processed (Kirwan, & Zhiyong, 2020). The prevalence of public surveillance in smart cities further complicates this issue. While beneficial for security purposes, it raises significant questions about the necessity and legality of processing personal data without explicit consent.

Within the PDPA, the data generated from public surveillance such as facial recognition technology arguably falls within the definition of "personal data" under section 4 of the PDPA as it enables the identification of the data subject. However, as was previously discussed, the PDPA primarily applies to personal data concerning commercial transactions, with section 3(1) explicitly excluding its application to the Federal and State Governments. Furthermore, the Act excludes any personal data processed outside Malaysia, unless further processed in the country, and does not include data processed for credit reporting businesses. Therefore, since public surveillance in Malaysia is mainly utilized for security purposes, the PDPA seems to fall short in offering adequate legal safeguards for individuals whose privacy may be compromised through its use by private companies or governmental bodies. Moreover, it is important to note that the PDPA does not provide the right to take private action, thus an aggrieved person could only lodge a written complaint to the Personal Data Protection Commissioner as a potential course of action (Chong, S & Kuek, 2022).

Individuals possess legitimacy to claim infringement of their constitutional rights when the discretional powers of public entities are exercised improperly in a manner that invades the privacy of individuals. This has been endorsed in the case of *Koperal Zainal Mohd Ali & Ors. v. Selvi Narayan & Anor* (2021), where three interacting factors tend to support such claims: It is necessary to assert in appeal that the plaintiff's constitutional right was breached. The person who committed the violation was acting in the course of authority of a state body, and third, the plaintiff must illustrate what loss or violation of his right was caused by the acts or omission of the said individual. However, it would be reasonable to mention that these cases are rather narrow – they are predominantly concerned with the issues of

monitoring and privacy of personal information under the PDPA. Hence, these cases leave many issues regarding public monitoring practices unresolved.

The EUAI Act (2024) adopts a more rigorous stance to regulate the applications of AI technologies that are considered high risk, including those deployed for monitoring public spaces. Article 5 of the Act places extreme compliance obligations on operational remote biometric recognition systems in publicly accessible spaces. These encompass reasonable risk mitigation, enhanced oversight, and strong data management to counter abuse of surveillance apparatus that may contravene fundamental rights. Moreover, AI systems that are to be used for the surveillance of the public must be subjected to appropriate testing and evaluation against the parameters given in Article 15. The Article posits that rights of citizens need to be protected from the arbitrary use of AI systems in public spaces through transparency about how and why such systems are used. It includes clear information on the system's capabilities, the type of data it collects and the end purpose for which the processing of data is targeted, to ensure that surveillance technologies are executed responsibly and ethically.

Safeguards

The success of as a smart city heavily depends on AI's ability to process, manage, and interpret data which according to the MSCO (2021), is a "vital part of any smart city implementation." Data collection within smart cities occurs through the 'interconnectivity' of IoT devices and AI systems such as sensors, cameras and even advertisement billboards. The main objectives are to improve public services and the quality of life for residents; however, these goals sometimes touch on fundamental rights, making robust safeguards essential. For example, the Crime Prevention through Environmental Design (CPTED) system, mentioned in the MSCO, requests processing a vast amount of personal data. In this case, preventive measures are essential in protecting personal data against abuse and infringement of rights.

Preventive measures serve as fences that defend the threats to privacy and help strike a balance between the competing interests. Safeguards do not come as mere options but rather basics in promoting the appropriate and moral use of information (Bu, 2021). The GDPR emphasizes the significance of additional measures, creating a firm architecture for the legal protection of data. An important element of the set of rules that the GDPR seeks to enforce concerns the principle of 'privacy by design and default' laid down in Article 25. This principle necessitates the creation of privacy-protecting features in the design and operation of data processing systems from the earliest possible stage. The Regulation also establishes the basis of transparency and responsibility in the possible abuse of personal data. Article 5(1)(a) of the GPDR outlined a core requirement relating to the legal, fair, and transparent processing of personal data.

On the other hand, the current version of the PDPA lacks any express provisions regarding protecting individual rights during the automated decision-making or monitoring process. This ambiguity that does not delineate explicit safeguards is a major concern in the protection of personal information. The PDPA does require the permission to use the data and provides guidelines on how long such private information may be kept, as well as how to protect it. However, it does not have any specific provisions on 'privacy by design and default', transparency and accountability which are major safeguarding mechanisms. Additionally, Section 3 of the PDPA categorically states that the Act does not apply to the federal and state governments, which creates a potential loophole in the data protection regime.

The Personal Information Protection Act (PIPA) of South Korea (2020), constitutes a good example of a legislatively bottled notion of an enhanced level of data protection. Article 23 of the PIPA decrees

that personal data processing systems must obtain necessary technical, administrative and physical safeguards to ensure security and confidentiality of personal data. In addition, Articles 28 and 29 of the Act requires that the controllers must ensure transparency of processing and upholding data subject's right to notification. This model endorses a normative stance towards privacy, which is similar to the GDRP.

Furthermore, the Malaysian legal system does not provide guidance on data breaches, civil remedies, and the right to erasure. While the Malaysian Communication and Multimedia Commission's guidelines for 'Video Surveillance in Public Spaces' (2008) require the relevant authorities to take measures such as avoiding the monitoring and recording of private dwellings and obtaining consent where such action is unavoidable, these guidelines do not generalise a prohibition for the capture and use of images without the subject's permission. In contrast, the GDPR pays more attention to these issues. For example, Article 33 of the GDPR stipulates that the appropriate oversight authority shall be notified of a data breach no later than 72 hours after the management body has knowledge of it. Articles 17 and 18 of the Regulation recognises the right to erasure ('right to be forgotten') and right to restriction of processing.

CONCLUSION

In the age of burgeoning digital transformation, the drive towards creating 'smart cities' is fundamentally redefining urban landscapes. With this rapid metamorphosis comes the indispensable need to ensure robust data protection, particularly in the domains of data collection and processing, which stand at the heart of smart city functionalities. As the foregoing discussions have clearly shown, this need is both profound and pressing in the Malaysian context, given the ambitious vision of the MSCF.

The crux of the present inquiry has revolved around the readiness of Malaysia's existing legal structures, chiefly the PDPA (2010), to safeguard citizen data in an AI-powered smart city environment. It has dissected the key facets of data protection — necessity, consent, and safeguards, which together form the core of privacy protection in data-centric operations, ensuring lawful and ethical data collection and processing. However, it is evident that the current PDPA framework lacks specific guidance on how these principles are to be applied within the smart city context.

The argument was made that data processing in smart cities urgently needs stronger safeguards. Although the PDPA outlines general principles, comparing it to the GDPR reveals opportunities for more specific and thorough protections. Concepts in the GDPR, like "privacy by design and default" and strict standards for when data processing is necessary, could be useful for enhancing the PDPA. This comparative study also illuminates the delicate balance between the grand vision of smart cities and the imperative necessity of strong data security. This implies that a well-crafted legal scheme for smart cities should incorporate a subtle balance of need, consent, and protections, delicately calibrated to the local environment and the distinct problems offered by smart city technologies.

Lastly, it is important to note that the present research is by no means a comprehensive study of all possible data privacy issues in smart cities. There are so many other issues — data ownership, data localization, transparency — that deserve more exploration. However, it is hoped that the present research will help act as a stepping stone for future research on this topic and contribute to the overall conversation of building 'privacy-conscious' smart cities. In the era of AI and digitization, data security in smart cities is not just a legal requirement, but a social and moral imperative. While Malaysia marches

onward towards its smart city future, it must not forget that its legal structure must be ready to support a data protection society that is as intelligent as its cities.

ACKNOWLEDGMENT

This research received no specific grant from any funding agency in the public, commercial, or not-for profit sectors.

REFERENCES

Ahmad, R. A., & Yeo, P. (2021). Malaysia Smart City Outlook 2021–2022 (pp. 1–130). Malaysian Industry-Government Group for High Technology. https://icsc-my.org/programmes/malaysia-smart-city-outlook-2021-2022-msco/

Alawadhi, S., Aldama-Nalda, A., Chourabi, H., Gil-Garcia, J. R., Leung, S., Mellouli, S., & Walker, S. (2012). Building understanding of smart city initiatives. *Electronic Government: 11th IFIP WG 8.5 International Conference, EGOV 2012, Kristiansand, Norway, September 3–6, 2012. Proceedings* (Vol. 11, pp. 40–53). Springer Berlin Heidelberg.

Alam, T. (2021). Cloud-based IoT applications and their roles in smart cities. *Smart Cities*, *4*(3), 1196-1219.

Baron, M. (2012). Do we need smart cities for resilience? *Journal of Economics & Management, 10*, 32–46. https://www.ue.katowice.pl/fileadmin/_migrated/content_uploads/3_Baron_Do_We_Need_Smart_Cities_for_Resilience.pdf

Bridges, L. (2021). Infrastructural obfuscation: Unpacking the carceral logics of the Ring surveillant assemblage. *Information, Communication & Society*, *24*(6), 830-849.

Bu, Q. (2021). The global governance on automated facial recognition (AFR): Ethical and legal opportunities and privacy challenges. *International Cybersecurity Law Review*, *2*(2), 113–145.

Bunders, D. J., & Varró, K. (2019). Problematizing data-driven urban practices: Insights from five Dutch 'smart cities'. *Cities*, *93*, 145-152.

California Consumer Privacy Act, 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375). https://oag.ca.gov/privacy/ccpa

Cardullo, P., & Kitchin, R. (2019). Smart urbanism and smart citizenship: The neoliberal logic of 'citizen-focused' smart cities in Europe. *Environment and Planning C Politics and Space*, *37*(5), 813–830. https://doi.org/10.1177/0263774X18806508#_i13

Caron, X., Bosua, R., Maynard, S. B., & Ahmad, A. (2016). The internet of things (IoT) and its impact on individual privacy: An Australian perspective. *Computer Law & Security Review*, *32(*1), 4–15. https://doi.org/10.1016/j.clsr.2015.12.001

Chong, S. Z., & Kuek, C. Y. (2022, December). Facial recognition technology in Malaysia: Concerns and legal issues. *International Conference on Law and Digitalization*, (pp. 101–109). Atlantis Press. https://doi.org/10.2991/978-2-494069-59-6_10

Christofi, A., Wauters, E., & Valcke, P. (2021). Smart cities, data protection and the public interest conundrum: What legal basis for smart city processing? *European Journal of Law and Technology*, *12*(1), 1–36. https://ejlt.org/index.php/ejlt/article/view/822

Communications and Multimedia Act 1998 (Incorporating latest amendment - Act A1220/2004) https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Act588bi_3.pdf

Drachsler, H., & Greller, W. (2016). Privacy and analytics: It is a delicate issue—a checklist for trusted learning analytics. Proceedings of the Sixth International Conference on Learning Analytics & Knowledge (pp. 89–98). https://doi.org/10.1145/2883851.2883893

Edwards, L. (2016). Privacy, security, and data protection in smart cities: A critical EU law perspective. European Data Protection Law Review, 2(1), 28–38. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2711290

European Data Protection Board. (2020). Guidelines 05/2020 on consent under Regulation 2016/679 (Version 1.1). https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

European Data Protection Supervisor (2017), 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit'. https://edps.europa.eu/sites/edp/ files/publication/17-04-11_necessity_toolkit_en_0.pdf

European Parliament and Council. (2024, June 13). Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Official Journal of the European Union.

Finch, K., & Tene, O. (2013). Welcome to the metropticon: Protecting privacy in a hyperconnected town. *Fordham Urban Law Journal, 41*, 1581–1604. https://ir.lawnet.fordham.edu/ulj/vol41/iss5/4/

Fung, A. (2015). Putting the public back into governance: The challenges of citizen participation and its future. *Public Administration Review, 75*(4), 513–522. https://doi.org/10.1111/puar.12361

Gassmann, O., Böhm, J., & Palmié, M. (2019). *Smart cities: Introducing digital innovation to cities*. Emerald Group Publishing. https://www.researchgate.net/publication/333459285_Smart_Cities_Introducing_Digital_Innovation_to_Cities

Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., Pichler-Milanovic, N., & Meijers, E. J. (2007). *Smart cities*: *Ranking of European medium-sized cities*. Final report. Vienna University of Technology. https://www.researchgate.net/publication/261367640_Smart_cities_-_Ranking_of_European_medium-sized_cities

Heinz Huber v Bundesrepublik Deutschland, C-524/06, ECLI:EU:C:2008:724.

Islam, M. T., Sahula, M., & Karim, M. E. (2022). Understanding GDPR: Its legal implications and relevance to South Asian privacy regimes. *UUM Journal of Legal Studies, 13*(1), 45–76. https://doi.org/10.32890/uumjls2022.13.1.3

Kirwan, C. G., & Zhiyong, F. (2020). *Smart cities and artificial intelligence: Convergent systems for planning, design, and operations* (1st ed). Elsevier.

Koperal Zainal Mohd Ali & Ors v. Selvi Narayan & Anor 2021 6 CLJ 157. https://www.elaw.my/JE/01/JE_2021_19.pdf

Lawson, G. (1995). Outcome, procedure, and process: Agency duties of explanation for legal conclusions. *Rutgers Law Review, 48*, 313–357.

Lim, S. B., Abdul Malek, J., Hussain, M. Y., & Tahir, Z. (2021). Malaysia smart city framework: A trusted framework for shaping smart Malaysian citizenship? *Handbook of Smart Cities* (pp. 515–538). Springer International Publishing.

Lynn Jr, L. E. (2009). Restoring the rule of law to public administration: What frank goodnow got right and leonard white did not. *Public Administration Review, 69*(5), 803–813. https://doi.org/10.1111/j.1540-6210.2009.02030.x

Ministry of Housing and Local Government. (2018). *Malaysia Smart City Framework.* https://www.kpkt.gov.my/kpkt/resources/user_1/GALERI/PDF_PENERBITAN/FRAMEWORK/FRAMEWORK_SMART_CITY_EXECUTIVE_SUMMARY.pdf

Nam, T., & Pardo, T. A. (2014). The changing face of a city government: A case study of Philly311. *Government Information Quarterly, 31*(Suppl. 1), S1–S9. https://doi.org/10.1016/j.giq.2014.01.002

Nor, M. A. B. M., Tasrib, M. A. B. M., Francis, B., Hesham, N. I. B., & Othman, M. B. B. (2021). A study on the laws governing facial recognition technology and data privacy in Malaysia. *Malaysian Journal of Social Sciences and Humanities, 6*(10), 480–487.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

Samsudin, N. A., Rosley, M. S. F., Lai, L. Y., Omar, S. R., Rashid, M. F., Hanifi, N. S. N. M., & Bakhtiar, I. S. (2022). A comparative study of smart city initiatives in Malaysia: Putrajaya and Iskandar Puteri. *Planning Malaysia Journal, 20*(5), 1–20. https://doi.org/10.21837/pm.v20i24.1180

Sarker, I. H. (2022). Smart City Data Science: Towards data-driven smart cities with open research issues. *Internet of Things, 19*, 100528. https://doi.org/10.1016/j.iot.2022.100528

Saxena, S., & Al-Tamimi, T. A. S. M. (2018). Visioning "smart city" across the Gulf Cooperation Council (GCC) countries. *Foresight, 20*(3), 237–251. https://doi.org/10.1108/FS-11-2017-0068

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society, 4*(2). https://doi.org/10.1177/2053951717736335

The Malaysian Communication and Multimedia Commission. (2008). *Video surveillance in public space.* https://www.scribd.com/document/707530753/CCTV-report-MCMC

The Singapore Personal Data Protection Act (2012). https://sso.agc.gov.sg/Act/PDPA2012

Vasseur, J. P., & Dunkels, A. (2010). *Interconnecting smart objects with IP: The next internet.* Morgan Kaufmann. https://www.researchgate.net/publication/234817468_Interconnecting_Smart_Objects_with_IP_The_Next_Internet

Vitunskaite, M., He, Y., Brandstetter, T., & Janicke, H. (2019). Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. *Computers & Security, 83*(6), 313-331. https://doi.org/10.1016/j.cose.2019.02.009

Walz, A., & Firth-Butterfield, K. (2019). Implementing ethics into artificial intelligence: A contribution, from a legal perspective, to the development of an AI governance regime. *Duke Law & Technology Review, 18*, 176–200.