

Personalised by Data, Exposed by Design: Legal Implications of AI-Driven Cosmetic Marketing and Data Privacy in Malaysia

Muhammad Azril Roslan^{1*}, Muhammad Aqib Aiman Puasa²

¹Department of Law, Universiti Teknologi MARA, Negeri Sembilan campus, Malaysia

²Faculty of Accountancy, University Technology MARA, Menara Sultan Abdul Aziz Shah (SAAS), 40450 Shah Alam, Selangor

DOI: <https://doi.org/10.47772/IJRISS.2026.100600017>

Received: 21 May 2026; Accepted: 26 May 2026; Published: 16 June 2026

ABSTRACT

The cosmetic industry is increasingly shaped by artificial intelligence, biometric analysis and data driven marketing. In Malaysia, AI powered cosmetic platforms are now capable of analysing facial images, skin texture, pigmentation, pores, behavioural preferences and purchase patterns to generate personalised product recommendations. Although such technology enhances consumer engagement and commercial efficiency, it also introduces significant legal concerns relating to biometric data, informed consent, algorithmic profiling, consumer manipulation and liability for harm. This article examines the legal implications of AI driven cosmetic marketing in Malaysia, with reference to the Personal Data Protection Act 2010, the Personal Data Protection Amendment Act 2024 and the Consumer Protection Act 1999. It argues that the 2024 amendment represents an important development because it introduces biometric data into the definition of sensitive personal data, but this reform does not fully resolve the broader challenges created by AI cosmetic systems. These systems remain difficult to regulate because they operate through opaque algorithms, fragmented data processing arrangements and complex relationships between cosmetic companies, platform providers and technology vendors. Through doctrinal and comparative legal analysis, this article draws selected insights from Australia and South Korea, both of which provide useful models on biometric data protection, consent and privacy governance. The article concludes that Malaysia requires a more integrated regulatory framework for AI cosmetic marketing, combining stronger data protection enforcement, clearer consent standards, algorithmic accountability, shared liability and sector specific guidance for cosmetic businesses using AI technologies.

Keywords: AI cosmetic marketing, biometric data, data privacy, PDPA 2010, cosmetic liability, algorithmic profiling

INTRODUCTION

The cosmetic industry has moved beyond traditional advertising, product sampling and beauty consultation. In the contemporary digital marketplace, cosmetic brands increasingly rely on artificial intelligence to analyse consumer appearance, predict beauty preferences and recommend personalised products. Perret and Schwientek (2025) explain that beauty technology now uses artificial intelligence and augmented reality to improve customer experience and product personalisation. Hash et al. (2025) similarly observe that artificial intelligence is increasingly used in customised skincare to support product recommendations based on skin related analysis. AI powered cosmetic platforms may include mobile skincare applications, virtual try on tools, smart mirrors, online beauty diagnostic systems, chatbot based product advisers and in store facial scanning devices. These systems process facial images and skin related information to identify features such as skin tone, pigmentation, wrinkles, acne, pores, dryness, oiliness and facial shape. The result is a personalised marketing environment in which cosmetic products are targeted to individual consumers based on biometric and behavioural data rather than broad consumer categories.

This development presents both commercial promise and legal risk. AI cosmetic personalisation may increase consumer engagement, reduce uncertainty in product selection and strengthen brand loyalty. However, Barocas

and Nissenbaum (2014) caution that big data practices can weaken meaningful consent because individuals may not fully understand how data is collected, inferred or reused. This concern is particularly relevant to cosmetic platforms because consumers may not know what data is collected, how long it is retained, whether facial images are converted into biometric templates, whether the data is shared with third party providers, and whether the recommendation is based on reliable analysis or commercial profiling. Tene and Polonetsky (2012) similarly argue that data analytics may reduce user control when information is combined and used for purposes beyond the consumer's reasonable expectation.

The legal issue is therefore not merely whether AI improves cosmetic marketing. The more important question is whether Malaysian law can protect consumers when beauty personalisation depends on biometric processing, automated profiling and algorithmic decision making. Malaysia's cosmetic sector already operates within a regulatory environment involving product notification and post market control under the Guidelines for Control of Cosmetic Products in Malaysia (National Pharmaceutical Regulatory Agency, 2022). At the same time, the Consumer Protection Act 1999 provides broader consumer protection mechanisms, including protection against misleading conduct and defective products (Malaysia, 1999). When AI is added to this landscape, harm may arise not only from the cosmetic product itself, but also from the data processing system that recommends the product, the algorithm that classifies the consumer's skin condition, the platform that stores facial data or the marketing design that encourages consumers to rely on automated advice.

Malaysia's data protection framework has recently undergone significant reform. The Personal Data Protection Act 2010 remains the principal statute governing personal data processing in commercial transactions (Malaysia, 2010). The Personal Data Protection Amendment Act 2024 strengthened the framework by inserting a statutory definition of biometric data and expanding sensitive personal data to include biometric data (Malaysia, 2024). This reform is important because facial scanning, skin analysis and other biometric tools used in cosmetic platforms can now be assessed through a more protective legal lens. Nevertheless, Sarabdeen (2022) argues that facial recognition and facial analysis technologies create serious risks to individual rights when used without adequate legal control. Recognition of biometric data is therefore only the first step. Malaysian law must still address AI profiling, automated cosmetic recommendations, algorithmic opacity, platform accountability and consumer redress.

The current Malaysian framework remains fragmented. The Personal Data Protection Act 2010 focuses mainly on personal data processing in commercial transactions, while the Consumer Protection Act 1999 addresses consumer rights, misleading conduct, defective products and guarantees relating to goods and services (Malaysia, 1999, 2010). The National Guidelines on AI Governance and Ethics provide a useful policy direction for responsible AI development in Malaysia (Ministry of Science, Technology and Innovation, 2024). However, those guidelines remain general in nature and do not create a specific legal regime for AI cosmetic marketing. Consumers may therefore still face difficulty when challenging inaccurate AI recommendations, withdrawing consent, understanding how facial data is used or identifying the party responsible for harm.

This article contributes to Malaysian cosmetic liability scholarship by shifting the discussion from defective cosmetic products to defective digital recommendation environments. Roslan et al. (2023) have examined producer liability for harmful cosmetic products under Malaysian product liability law. This article extends that discussion by arguing that AI cosmetic marketing creates a separate layer of legal risk because harm may arise from biometric data processing, automated profiling, algorithmic recommendations and fragmented platform responsibility. Its originality lies in connecting data protection law, consumer protection law and cosmetic liability within a single AI cosmetic marketing framework.

This article examines the legal implications of AI cosmetic marketing by focusing on the nature of consumer data collected by AI cosmetic platforms, the regulation of biometric data under Malaysian data protection law after the 2024 amendment, the limits of consent and transparency in AI based cosmetic personalisation, the allocation of liability where AI generated recommendations cause harm, and the comparative lessons that may be drawn from Australia and South Korea. It argues that Malaysia should move beyond a narrow consent-based approach and develop a sector sensitive governance model for AI cosmetic marketing. Such a model should combine stronger protection for biometric data, layered consent, privacy and algorithmic impact assessments,

consumer rights against automated profiling, shared accountability between cosmetic companies and technology providers, and more active enforcement by data protection and consumer protection authorities.

METHODOLOGY

This study adopts a qualitative doctrinal legal research methodology. Doctrinal legal research is appropriate where a study seeks to analyse legal rules, statutory provisions, principles and regulatory instruments to determine their meaning, scope and limitations (Hutchinson & Duncan, 2012). In this article, the doctrinal method is used to examine Malaysia's legal response to AI driven cosmetic marketing, biometric data processing and automated product recommendations. The analysis focuses on primary legal sources, including the Personal Data Protection Act 2010, the Personal Data Protection Amendment Act 2024, the Consumer Protection Act 1999 and relevant Malaysian policy instruments on artificial intelligence governance. Chynoweth (2008) explains that legal research often involves the systematic reading and interpretation of legal texts. This approach is therefore suitable for assessing whether existing Malaysian legal rules are adequate to address the risks created by AI cosmetic platforms.

The doctrinal analysis is conducted through four analytical steps. First, the article identifies the relevant legal rules governing personal data, biometric data, consumer protection and product liability. Second, it interprets the scope of those rules in the context of AI cosmetic marketing. Third, it evaluates the gaps that arise when existing laws are applied to biometric processing, algorithmic recommendation, automated profiling and platform-based responsibility. Fourth, it proposes legal reforms that can improve consumer protection, data governance and accountability. This analytical structure allows the article to move beyond description and provide a normative assessment of whether Malaysian law is sufficiently responsive to AI driven cosmetic marketing.

The study also adopts a comparative legal approach. Comparative legal research is useful where legal systems are examined to identify similarities, differences and possible lessons for reform. Zweigert and Kötz (1998) explain that comparative law should not merely describe foreign legal rules but should assist in understanding legal problems through functional comparison. In this article, Australia and South Korea are selected as reference jurisdictions because both provide relevant insights for the Malaysian context. Australia is selected because its privacy framework treats certain biometric information as sensitive information and because its privacy regulator has issued guidance on facial recognition risk assessment. South Korea is selected because its Personal Information Protection Act provides a stricter privacy regime, supported by biometric information guidance and developing rights in relation to automated decision making. These jurisdictions are therefore useful for benchmarking Malaysia's approach to biometric data, consent, explainability and AI accountability.

Secondary sources are used to support the legal analysis. These include journal articles, regulatory guidance, policy reports, legal commentaries and comparative legal materials. Such sources assist in explaining the relationship between data privacy, algorithmic profiling, cosmetic product liability, consumer protection and AI governance. The article does not treat these secondary sources as empirical evidence of consumer behaviour. Rather, they are used to support doctrinal interpretation, identify regulatory gaps and justify proposed reforms.

This study does not conduct empirical fieldwork, interviews or surveys with cosmetic users, regulators, technology providers or cosmetic businesses. This limitation is justified because the objective of the article is to evaluate the adequacy of the existing legal framework, not to measure actual consumer understanding or industry compliance. Future empirical research may examine how Malaysian consumers understand consent, facial scanning, biometric data collection and AI generated cosmetic recommendations in practice. Paris (2016) cautions that comparative legal research should avoid uncritical legal transplantation. Accordingly, the comparative discussion in this article does not seek to transplant Australian or South Korean law wholesale into Malaysia. Instead, it identifies selected principles that may assist Malaysia in developing a more coherent framework for biometric data, automated profiling and cosmetic platform accountability.

Methodological Limitations and the Need for Empirical and Technical Validation

This article is limited by its reliance on doctrinal and comparative legal analysis, as it does not incorporate empirical data from Malaysian consumers, cosmetic companies, technology providers, legal practitioners or

regulatory authorities. This limitation means that the article evaluates the legal adequacy of Malaysia's framework but does not directly measure how AI cosmetic marketing operates in practice, how consumers understand biometric consent, or how industry actors manage algorithmic recommendation systems. The absence of empirical evidence is significant because AI driven cosmetic marketing involves not only legal rules, but also consumer behaviour, platform design, data processing practices and commercial decision making. As Barocas and Nissenbaum (2014) argue, data intensive systems may weaken meaningful consent where individuals do not fully understand how their data is collected, inferred or reused. Similarly, Tene and Polonetsky (2012) explain that data analytics may reduce user control when information is combined and applied beyond the consumer's reasonable expectation. The study is also limited by its restricted technical analysis of AI system design, particularly in relation to algorithmic bias, machine learning accuracy, facial recognition reliability and cybersecurity risk. This limitation is important because black box algorithms may make automated outcomes difficult to explain or challenge (Gryz & Rojszczak, 2021), while algorithmic bias may produce unequal or inaccurate results where training data does not adequately represent diverse users (Belenguer, 2022). Therefore, while the doctrinal method is suitable for identifying legal gaps, the findings should be read as a legal and normative analysis that requires further empirical and technical validation in real world Malaysian AI cosmetic marketing contexts.

AI Powered Cosmetic Personalisation and the Nature of Consumer Data

AI powered cosmetic personalisation refers to the use of algorithmic systems to analyse consumer data and generate customised cosmetic recommendations. Unlike ordinary online advertising, which often relies on broad demographic categories, AI cosmetic platforms process more specific personal information. Perret and Schwientek (2025) explain that beauty technology increasingly uses artificial intelligence and augmented reality to support personalised product experiences. In practice, a consumer may upload a facial image, answer questions about skin sensitivity, provide age and lifestyle information, allow access to purchase history or use a camera-based tool that scans visible skin conditions. The system may then recommend moisturisers, cleansers, sunscreens, foundations, serums or beauty routines based on the perceived condition of the consumer's skin.

The data collected through AI cosmetic systems is legally significant because it may reveal more than ordinary consumer preference. Hash et al. (2025) observe that artificial intelligence is increasingly used in customised skincare to analyse skin characteristics and support personalised skincare recommendations. Such systems may process facial geometry, melanin levels, pore structure, skin elasticity and behavioural preferences. Facial images and skin-based data may also relate to identity, health condition, ethnicity, age, gender presentation and other sensitive aspects of a person. Even where the platform claims that the data is used only for product recommendation, Tene and Polonetsky (2012) caution that data analytics may reduce user control when information is combined, reused or applied beyond the consumer's reasonable expectation.

The first legal concern is biometric processing. Facial scanning tools may not merely store a photograph. They may extract measurable facial features and convert those features into biometric templates. This distinction matters because a facial image used for display carries a different risk from facial data processed for automated recognition, classification or comparison. Sarabdeen (2022) argues that facial recognition technologies may affect privacy, autonomy and individual rights when deployed without adequate legal control. The 2024 amendment to Malaysia's data protection law is therefore important because it recognises biometric data as personal data resulting from technical processing relating to physical, physiological or behavioural characteristics (Malaysia, 2024). AI cosmetic platforms that technically process facial or skin related features may now fall more clearly within this enhanced category.

The second concern is behavioural profiling. Cosmetic personalisation does not depend only on facial data. Platforms may also collect browsing history, purchase records, product reviews, geolocation, search terms, social media engagement and interaction with advertisements. These data points allow companies to build detailed profiles of consumer insecurity, preference and purchasing likelihood. For example, a consumer who repeatedly searches for acne products, whitening products or anti-ageing products may be categorised into a marketing segment that receives targeted messages designed to increase urgency and purchase intention. This raises questions about manipulation, fairness and autonomy, especially where consumers do not understand how their data is being used.

The third concern is the black box problem. Many AI systems operate in ways that are not easily explainable to ordinary users. Even the cosmetic company deploying the system may not fully understand the internal logic of a proprietary algorithm supplied by a third-party technology vendor. Gryn and Rojszczak (2021) explain that black box algorithms create accountability problems because affected individuals may struggle to understand or challenge automated outcomes. In the cosmetic context, this becomes problematic when a consumer asks why a particular product was recommended, whether the recommendation considered allergies or sensitivity, and whether commercial incentives influenced the result. A recommendation may appear scientific because it is generated by AI, but it may still be shaped by incomplete data, biased training sets or commercial priorities.

The fourth concern is consumer reliance. AI cosmetic platforms often present recommendations in confident and personalised language. Consumers may trust the system because it appears objective, technical and data based. However, if the recommendation is inaccurate, unsuitable or misleading, the consumer may suffer physical, financial or dignity-based harm. Physical harm may occur where the consumer uses a product unsuitable for sensitive skin, while financial harm may occur where the consumer purchases products based on exaggerated claims. Barocas and Nissenbaum (2014) show that data intensive systems may weaken meaningful consent and autonomy, and this concern is particularly relevant when cosmetic platforms classify appearance related features in ways that reinforce insecurity or harmful beauty standards.

These concerns show that AI cosmetic marketing should not be treated as ordinary advertising. It involves data protection, consumer protection, product liability, service accountability and ethical governance. In Malaysia, cosmetic products are already regulated through notification and post market control mechanisms under the Guidelines for Control of Cosmetic Products in Malaysia (National Pharmaceutical Regulatory Agency, 2022). However, AI based recommendation systems introduce a separate layer of risk involving biometric processing, behavioural profiling and algorithmic influence. The legal framework must therefore address not only the safety of cosmetic products, but also the safety and fairness of the digital systems that shape consumer decisions.

Malaysian Legal Framework on Data Privacy and AI Cosmetic Marketing

Malaysia's primary legislation on personal data processing in commercial transactions is the Personal Data Protection Act 2010. The Act is directly relevant to AI cosmetic marketing because section 4 defines "commercial transactions" broadly to include transactions relating to the supply or exchange of goods or services. AI cosmetic platforms that collect facial images, skin related information and behavioural data for product recommendation therefore fall within a commercial data processing environment. The same section also defines "processing" broadly to include collecting, recording, holding, storing, using, disclosing, aligning, combining, correcting, erasing and destroying personal data. This definition is important because AI cosmetic systems do not merely collect consumer information. They may also combine facial images, skin condition data, purchase history and behavioural patterns to generate personalised recommendations. Section 5 further requires data controllers to comply with the seven Personal Data Protection Principles, namely the General Principle, Notice and Choice Principle, Disclosure Principle, Security Principle, Retention Principle, Data Integrity Principle and Access Principle, which are set out in sections 6 to 12 of the Act.

The Personal Data Protection Amendment Act 2024 further modernised the Malaysian framework. Section 2 of the Amendment Act replaces the terms "data user" and "data users" with "data controller" and "data controllers" throughout the principal Act, except in specified contexts. This change is conceptually important because it aligns Malaysian terminology more closely with contemporary data governance language. More importantly, section 3 of the Amendment Act amends section 4 of the PDPA by inserting a definition of "biometric data" as personal data resulting from technical processing relating to the physical, physiological or behavioural characteristics of a person. The same amendment also expands the definition of "sensitive personal data" by inserting biometric data into that category. This reform is directly relevant to facial scanning, skin analysis, virtual try on tools and other cosmetic technologies that technically process facial or appearance related features.

Consent remains a central legal requirement under the PDPA. Section 6 contains the General Principle. Under section 6(1)(a), personal data other than sensitive personal data must not be processed unless the data subject has given consent. Where sensitive personal data is involved, section 6(1)(b) refers the matter to section 40. This is significant after the 2024 amendment because biometric data is now included within sensitive personal data.

Section 40 provides that sensitive personal data shall not be processed except in accordance with specified conditions, including explicit consent. In AI cosmetic marketing, this means that ordinary consent hidden in general privacy terms may be insufficient where the platform technically processes facial or skin related biometric data. Tene and Polonetsky (2012) are useful here because they explain how data analytics can weaken user control where data is combined and reused beyond the consumer's reasonable expectation.

The PDPA also contains provisions relevant to transparency. Section 7 establishes the Notice and Choice Principle. It requires the data controller to inform the data subject by written notice that personal data is being processed, to describe the personal data, to state the purposes of collection and further processing, to identify the source of the data, to explain the right of access and correction, to state the class of third parties to whom the data may be disclosed, and to explain whether the supply of data is obligatory or voluntary. This section is highly relevant to AI cosmetic marketing because consumers should know whether their facial images are merely used for temporary display, converted into biometric templates, stored for future analysis, shared with third party technology vendors or used for marketing segmentation. Section 7 is therefore not merely a procedural notice provision. In AI cosmetic platforms, it becomes a foundation for meaningful consumer awareness and choice.

The Disclosure Principle under section 8 is also relevant. It prohibits disclosure of personal data without the consent of the data subject for purposes other than the purpose for which the data was disclosed at the time of collection, or a directly related purpose, and to parties outside the class of third parties specified in the notice. This provision is important because AI cosmetic platforms may involve several actors, including cosmetic brands, application developers, cloud service providers, AI vendors and advertising partners. If facial or skin related data is shared beyond the original purpose of product recommendation, section 8 may become relevant. The legal issue is therefore not only whether the consumer consented to use a beauty tool, but whether the subsequent disclosure or reuse of personal data remains within the purpose and third-party categories disclosed to the consumer.

The PDPA further imposes obligations relating to security, retention, accuracy and access. Section 9 requires practical steps to protect personal data from loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction. This is particularly important for biometric data because facial templates and skin related identifiers may create long term privacy risks if leaked or misused. Section 10 requires personal data not to be kept longer than necessary and requires reasonable steps to destroy or permanently delete data that is no longer required. This matters where cosmetic platforms retain facial scans after the virtual try on or skin diagnosis function has ended. Section 11 requires reasonable steps to ensure that personal data is accurate, complete, not misleading and kept up to date, while section 12 gives the data subject access to personal data and the ability to correct inaccurate, incomplete, misleading or outdated data. These provisions are relevant because inaccurate skin classification or outdated consumer profiles may produce unsuitable or misleading product recommendations.

However, these PDPA provisions were not designed specifically for AI recommendation systems. Sections 6 to 12 regulate consent, notice, disclosure, security, retention, data integrity and access, but they do not expressly create a right to explanation for automated decisions, a right to challenge AI generated recommendations, or a duty to conduct algorithmic impact assessments. This is where the Malaysian framework remains incomplete. Gryz and Rojszczak (2021) argue that black box algorithms create accountability problems because affected individuals may struggle to understand or contest automated outcomes. In AI cosmetic marketing, this gap is significant because a recommendation may appear scientific and personalised even where it is shaped by incomplete data, biased training material, commercial prioritisation or an opaque ranking system.

Before examining the specific consumer protection provisions, it is important to establish the scope of the Consumer Protection Act 1999. Section 2 provides that the Act applies to goods and services offered or supplied to consumers in trade, including transactions conducted through electronic means. This is important because AI cosmetic platforms normally operate through online applications, websites, digital beauty tools or electronic retail systems. Section 3 further defines key terms such as "advertisement", "consumer", "goods", "services", "supplier" and "trade". These definitions support the argument that AI cosmetic recommendations may operate not only as product promotion, but also as personalised advertising, digital advisory services or part of the process of supplying cosmetic goods to consumers.

The Consumer Protection Act 1999 is also relevant because AI cosmetic marketing affects consumer decision making. Section 9 prohibits misleading conduct, while section 10 prohibits false or misleading representations. These provisions may apply where an AI cosmetic platform creates the impression that a product recommendation is scientifically accurate, dermatologist verified or individually suitable when the claim is not properly supported. Section 18 is also relevant because it creates a presumption of liability for advertisements in the context of Part II. This matters where AI generated product recommendations function as personalised advertising. In addition, sections 19 and 20 on safety standards may become relevant where cosmetic products are subject to prescribed safety standards.

The CPA also provides implied guarantees that may be relevant where AI cosmetic marketing leads to the supply of goods or services. Section 32 provides an implied guarantee that goods supplied to a consumer are of acceptable quality, while section 33 provides an implied guarantee that goods are reasonably fit for a particular purpose made known to the supplier or represented by the supplier. These provisions may become relevant where a consumer relies on an AI recommendation that presents a cosmetic product as suitable for a particular skin concern. Where the AI tool is treated as a service, section 53 provides an implied guarantee that services will be carried out with reasonable care and skill, and section 54 provides an implied guarantee that services and any product resulting from the services will be reasonably fit for the consumer's particular purpose or expected result. These service-based guarantees are important because AI cosmetic recommendation may operate not merely as sale of goods, but also as a digital advisory service.

For product liability, Part X of the CPA is central. Section 66 defines key terms such as "damage", "producer" and "product". Section 67 provides the meaning of "defect", stating that there is a defect in a product if the safety of the product is not such as persons generally are entitled to expect. Importantly, section 67 requires all relevant circumstances to be considered, including the manner and purposes for which the product has been marketed, the get up of the product, the use of any mark, and instructions or warnings. This is significant for AI cosmetic marketing because an algorithmic recommendation may shape consumer expectations about product suitability. Section 68 imposes liability for defective products on the producer, own brander and importer where damage is caused wholly or partly by a defect in the product. Sections 69 to 72 further address the extent of liability, application of other written law, prohibition on exclusion from liability and available defences. These provisions provide a useful product liability route, but they do not fully resolve harm caused by inaccurate algorithmic advice or biometric profiling where the product itself may not be defective.

The current Malaysian framework therefore remains fragmented. The PDPA provides section-based protection through sections 4, 5, 6, 7, 8, 9, 10, 11, 12 and 40, while the 2024 Amendment Act strengthens section 4 by recognising biometric data as sensitive personal data. The CPA provides relevant protection through sections 9, 10, 18, 19, 20, 32, 33, 53, 54 and Part X sections 66 to 72. However, neither statute provides a complete AI cosmetic marketing framework. The PDPA regulates data processing but does not specifically address algorithmic explainability or automated recommendation rights. The CPA regulates misleading conduct, guarantees and defective products but does not clearly allocate responsibility between cosmetic companies, AI vendors, platform operators and data processors. Malaysia has therefore made important progress, but a more effective model should combine data protection law, consumer protection law, cosmetic regulatory guidance and responsible AI governance.

Liability for Harm Arising from AI Cosmetic Recommendations

AI cosmetic marketing creates difficult liability questions because harm may arise from several interconnected sources. A consumer may suffer harm because the cosmetic product itself is defective, because the AI system recommends an unsuitable product, because the platform makes misleading representations, or because biometric data is misused. The Consumer Protection Act 1999 is relevant because Part X establishes a statutory product liability regime. Section 66 defines important terms such as "damage", "producer" and "product", while section 67 provides the statutory meaning of "defect". Section 68 then imposes liability where damage is caused wholly or partly by a defect in a product. These provisions are important for AI cosmetic marketing because the consumer may argue that the product was defective, or that the way the product was marketed through an AI recommendation affected the consumer's expectation of safety.

The first category of harm is product-based harm. Under section 67 of the Consumer Protection Act 1999, a product is defective if its safety is not such as persons generally are entitled to expect. The section requires all relevant circumstances to be considered, including the manner and purposes for which the product has been marketed, its get up, the use of any mark, instructions or warnings, and what might reasonably be expected to be done with the product. This is particularly important for AI cosmetic recommendations because the recommendation may shape the consumer's expectation that the product is suitable for a particular skin condition. If an AI platform presents a product as personalised, scientifically selected or suitable for sensitive skin, that representation may become part of the wider circumstances for assessing defect under section 67. Section 68 then identifies the parties who may be liable for damage caused by a defective product, including the producer, own brander and importer. Amin (1999) and Roslan et al. (2023) are useful secondary authorities because they explain the Malaysian product liability framework and its relevance to harmful cosmetic products.

Common law negligence principles may also support the analysis, especially where statutory product liability does not fully capture the harm caused by an AI recommendation. In *Donoghue v Stevenson*, the House of Lords recognised that a manufacturer may owe a duty of care to the ultimate consumer even without a direct contract. The case is relevant because it established the broader principle that a party who places a product into the stream of consumption may owe a duty to those foreseeably affected by it. In *Grant v Australian Knitting Mills Ltd*, the Privy Council applied similar reasoning where defective woollen underwear caused dermatitis to the consumer. That case is useful by analogy because it shows that liability may arise where a consumer suffers harm from a product that appears ordinary but contains a latent risk not discoverable by the consumer. In AI cosmetic marketing, the latent risk may arise not only from the product formulation but also from an inaccurate digital recommendation that exposes the consumer to a product unsuitable for their skin condition.

The second category is recommendation-based harm. This arises where the cosmetic product itself may not be defective, but the AI system recommends it to the wrong consumer, misclassifies the consumer's skin condition or omits relevant warnings. The Consumer Protection Act 1999 contains implied guarantees that may assist consumers in such circumstances. Section 32 provides an implied guarantee that goods supplied to a consumer are of acceptable quality, while section 33 provides an implied guarantee that goods are reasonably fit for a particular purpose where that purpose is made known, either expressly or by implication. If a consumer uses an AI cosmetic tool and is told that a product is suitable for oily skin, sensitive skin, acne prone skin or pigmentation concerns, section 33 may become relevant because the recommendation may amount to a representation of fitness for a particular purpose. Where the AI tool is treated as part of a digital advisory service, section 53 is also relevant because it provides an implied guarantee that services will be carried out with reasonable care and skill. Section 54 further provides an implied guarantee that services and any product resulting from the services will be reasonably fit for a particular purpose or expected result.

Negligence may also be relevant to recommendation-based harm. A cosmetic company that deploys an AI recommendation system arguably owes a duty to take reasonable care in designing, testing and monitoring that system. Reasonable safeguards may include using reliable data, avoiding exaggerated claims, disclosing limitations, testing the system across diverse skin profiles and ensuring that recommendations do not exceed the system's technical competence. Buiten (2024) explains that AI liability is difficult because AI systems may be unpredictable, partly autonomous and difficult to monitor, especially when fault and causation are hard to prove. This difficulty is directly relevant to AI cosmetic platforms because a consumer may not know whether the harmful recommendation was caused by poor training data, defective algorithm design, inadequate warnings, inaccurate user input, or commercial ranking priorities.

The third category is misleading representation. Sections 9 and 10 of the Consumer Protection Act 1999 are central here. Section 9 prohibits misleading or deceptive conduct in relation to goods or services, including conduct that is likely to mislead or deceive the public as to the nature, characteristics, suitability for a purpose, availability or quantity of goods or services. Section 10 prohibits false or misleading representations, including representations that goods or services are of a particular kind, standard, quality, grade, quantity, composition, style, model or suitability. These provisions may apply where an AI cosmetic platform gives the impression that a product recommendation is scientifically accurate, dermatologist verified, individually suitable or based on reliable skin analysis when that impression is not properly supported. Section 18 is also relevant because it creates a presumption of liability for advertisements in proceedings involving misleading or false

representations. AI generated cosmetic recommendations may therefore be analysed not only as advice but also as personalised advertising.

The fourth category is data-based harm. Harm does not arise only when the consumer suffers physical injury. Biometric data misuse, unauthorised sharing, discriminatory profiling, reputational harm and loss of control over personal identity may also be serious concerns. The Personal Data Protection Act 2010 becomes relevant here. Section 4 defines “processing” broadly to include collecting, recording, holding, storing, using, disclosing, combining, erasing and destroying personal data. Section 5 requires compliance with the seven Personal Data Protection Principles, while sections 6 to 12 set out the General Principle, Notice and Choice Principle, Disclosure Principle, Security Principle, Retention Principle, Data Integrity Principle and Access Principle. Section 40 governs sensitive personal data and becomes especially important after the Personal Data Protection Amendment Act 2024 inserted biometric data into the category of sensitive personal data. Where an AI cosmetic platform processes facial scans or biometric templates, the liability issue may therefore involve not only defective products but also breach of data protection obligations.

Causation remains a major difficulty. A consumer may argue that the AI tool produced an inaccurate recommendation, but the cosmetic company may respond that the product was safe, that the consumer voluntarily purchased it, that the reaction arose from individual sensitivity or that the consumer provided inaccurate information to the platform. The technology provider may argue that it merely supplied the system and did not control the cosmetic product, marketing content or final consumer decision. This difficulty is not unique to AI. In product liability, courts have long examined whether the defect caused the damage. In *A v National Blood Authority*, the English court considered defect in the context of infected blood products and applied a consumer expectation approach to product safety. Although the case arose under the UK Consumer Protection Act 1987, it is useful by analogy because Malaysia’s section 67 also adopts an expectation-based approach to defect. The case supports the argument that safety must be assessed from the standpoint of what persons are generally entitled to expect, not merely from the producer’s internal knowledge or intention.

The central legal problem is that AI cosmetic recommendations may fall between product liability, service liability, negligence, misleading representation and data protection law. Chagal Feferkorn (2019) argues that algorithms do not always fit neatly within traditional product categories. This is important because an AI recommendation may operate as software, a service, advertising, consumer advice and a product selection mechanism at the same time. If the cosmetic product is defective, Part X of the Consumer Protection Act 1999 may apply through sections 66 to 72. If the product is not defective but the recommendation is misleading, sections 9, 10 and 18 may be more relevant. If the consumer relied on the system as a digital service, sections 53 and 54 may be relevant. If biometric data is misused, the PDPA principles and section 40 become relevant. The difficulty is that none of these provisions was drafted specifically for AI generated cosmetic recommendations.

Shared accountability is therefore necessary. In AI cosmetic marketing, the cosmetic brand, platform operator, technology developer, data processor, product manufacturer and importer may each contribute to the risk. Section 68 of the Consumer Protection Act 1999 already recognises that more than one party may be exposed to product liability, including the producer, own brander and importer. However, AI cosmetic marketing adds further actors who may not fit neatly within those categories. A company that commercially deploys biometric AI to sell cosmetic products should not avoid responsibility merely because the algorithm was supplied by a third party. Similarly, technology providers should not avoid accountability where harm results from defective system design, poor data governance or inadequate safeguards. Liability should therefore be structured around responsibility for risk creation, consumer reliance and control over the relevant part of the AI cosmetic ecosystem.

Comparative Insights from Australia and South Korea

A comparative review of Australia and South Korea provides useful lessons for Malaysia because both jurisdictions have developed stronger approaches to privacy governance, biometric data protection and accountability for digital technologies. The comparison is not intended to suggest that Malaysia should copy foreign law directly. Rather, it highlights selected principles that may assist Malaysia in strengthening its own

legal framework for AI cosmetic marketing. Australia is useful for understanding how biometric information may be treated as sensitive information in commercial settings, while South Korea is useful because of its stricter personal information protection regime and developing rules on automated decision making.

Australia provides a useful comparative model because the Privacy Act 1988 expressly treats certain biometric information as sensitive information. Under section 6(1) of the Privacy Act 1988, the definition of “sensitive information” includes biometric information that is to be used for the purpose of automated biometric verification or biometric identification, as well as biometric templates. This is directly relevant to AI cosmetic marketing because facial scanning, virtual try on systems and skin analysis tools may involve biometric information where the system technically processes facial features or creates biometric templates. For Malaysia, the Australian approach reinforces the view that biometric data should not be treated as ordinary marketing data. It requires a higher level of consent, transparency and privacy protection.

Australian privacy guidance also specifically addresses facial recognition technology in commercial and retail environments. The Office of the Australian Information Commissioner issued guidance in 2024 on assessing privacy risks before deploying facial recognition technology, including risks relating to necessity, proportionality, consent, notice, accuracy, bias and security (Office of the Australian Information Commissioner, 2024a). This guidance is relevant to cosmetic businesses because beauty stores, mobile applications and online platforms may use facial analysis in similarly consumer facing settings. The Australian approach suggests that businesses should not deploy facial analysis merely because it is commercially attractive. They must first consider whether biometric processing is necessary, whether less intrusive alternatives exist and whether consumers are given clear and meaningful choices.

Recent Australian enforcement also shows that biometric technologies are not treated lightly. In 2024, the Australian privacy regulator found that Bunnings Group Limited breached privacy law by collecting personal and sensitive information through a facial recognition technology system. The system captured the faces of customers entering 63 stores in Victoria and New South Wales between November 2018 and November 2021 (Office of the Australian Information Commissioner, 2024b). Although the Bunnings case was not about cosmetic marketing, it is relevant because it involved facial recognition in a consumer facing retail environment. The lesson for Malaysia is that businesses should not assume that retail convenience, commercial efficiency or security justification automatically legitimises biometric data collection. AI cosmetic platforms should therefore be required to justify why facial scanning is necessary, how consent is obtained, how long biometric data is retained and how consumers may avoid or withdraw from such processing.

South Korea provides another important point of comparison. Its Personal Information Protection Act regulates personal information processing and provides a comprehensive legal framework for privacy protection (Republic of Korea, 2011). South Korea has also issued a specific Biometric Information Protection Guideline, which is listed by the Personal Information Protection Commission as a 2022 regulatory guideline (Personal Information Protection Commission, 2022). This is relevant to AI cosmetic marketing because facial images, skin scans and appearance-based data may involve biometric or sensitive data related processing. Malaysia may therefore benefit from developing a similar technology specific or sector specific guideline for biometric processing in cosmetic and beauty technology platforms.

South Korea is also useful because it has moved towards recognising rights in relation to automated decision making. Kim and Park (2024) explain that the revised South Korean Personal Information Protection Act introduced Article 37-2, which deals with data subjects’ rights in relation to automated decisions. This development is important for AI cosmetic marketing because product recommendations may increasingly be generated through automated systems. If an AI tool classifies a consumer’s skin condition or recommends a product based on facial analysis, the consumer should have some ability to understand, question or challenge the automated outcome. Malaysia’s current legal framework does not yet provide a specific right to explanation or objection for AI cosmetic recommendations.

Taken together, Australia and South Korea offer three lessons for Malaysia. First, biometric data should be treated as a high-risk category requiring clear consent, transparency and stronger protection. Second, businesses using facial or biometric systems should conduct privacy risk assessments before deployment, especially where

consumers cannot meaningfully avoid the technology. Third, consumers should have rights in relation to automated recommendations, including the right to know when AI is used, the right to withdraw consent, the right to request explanation and the right to challenge harmful outcomes. Malaysia has already taken an important step through the 2024 PDPA amendment, but recognition of biometric data should now be supported by sector guidance, automated decision rights and stronger institutional oversight.

Ethical and Human Rights Concerns in AI Cosmetic Marketing

AI cosmetic marketing raises ethical and human rights concerns because it does not merely recommend products. It also evaluates, classifies and commercialises human appearance. When a cosmetic platform scans a person's face, analyses skin features and recommends products based on perceived imperfections, the system may affect how consumers understand their own identity, dignity and bodily autonomy. UNESCO (2022) places the protection of human rights and dignity at the centre of AI ethics and emphasises transparency, fairness and human oversight. These principles are highly relevant to AI cosmetic marketing because the technology deals directly with the human face, skin, appearance and personal self-perception.

One major ethical concern is autonomy. Consumers may appear to make free choices when purchasing AI recommended cosmetic products, but their choices may be shaped by algorithmic profiling, targeted advertising and personalised persuasion. In data driven environments, companies may collect and combine information in ways that consumers do not reasonably expect, thereby weakening individual control over personal data (Tene & Polonetsky, 2012). This problem becomes more sensitive in cosmetic marketing because the data used may relate to acne, wrinkles, pigmentation, skin tone, ageing, facial shape or other appearance related concerns. A consumer may therefore be influenced not only as a buyer, but also as a person whose insecurities can be commercially identified and targeted.

A second concern is algorithmic bias. AI systems are trained on data, and if the training data does not represent diverse skin tones, facial features, ethnic backgrounds, ages or gender presentations, the system may produce inaccurate or unfair outcomes. Belenguer (2022) explains that AI bias may arise when algorithmic systems reproduce discriminatory patterns or produce unequal results for different groups. In the cosmetic context, this may occur where a facial analysis tool performs better on some skin tones than others, misclassifies certain facial features or recommends products based on narrow assumptions about beauty. Such outcomes may reinforce exclusion and undermine equality.

A third concern is non-discrimination and inclusivity. The OECD AI Principles promote trustworthy AI that respects human rights and democratic values, and the OECD explains that these principles were adopted in May 2019 (OECD, 2019). Applying this principle to cosmetic marketing means that AI systems should not promote discriminatory beauty standards or treat certain appearances as less desirable. Cosmetic AI may silently encode assumptions about what counts as normal, attractive, youthful or desirable. Where such assumptions are embedded into product recommendations, the technology may contribute to social pressure, appearance-based exclusion and unequal treatment.

The Malaysian context adds another layer of concern. Cosmetic choices may intersect with culture, religion, gender norms, ethnicity, age and social identity. AI systems used in Malaysia should therefore be sensitive to local diversity and should avoid imposing narrow or imported beauty standards. Malaysia's National Guidelines on AI Governance and Ethics provide a policy foundation for safe, ethical and responsible AI development (Ministry of Science, Technology and Innovation, 2024). However, voluntary ethical guidelines should be supported by clearer legal duties when AI systems process biometric data, profile consumers and influence purchasing decisions in the cosmetic sector.

Ethical governance should therefore move beyond general corporate responsibility. Cosmetic companies using AI should be required to design systems that respect privacy, dignity, autonomy, fairness and non-discrimination. This includes testing AI systems for bias, giving consumers meaningful control over biometric data, avoiding manipulative design, disclosing commercial influence and ensuring human oversight where recommendations may affect wellbeing or self-perception. Without such safeguards, AI cosmetic marketing may transform personal appearance into a data asset and expose consumers to profiling, manipulation and dignity-based harm.

RECOMMENDATIONS FOR REFORM

Malaysia should develop a clearer and more integrated regulatory framework for AI cosmetic marketing. The 2024 amendment to the Personal Data Protection Act 2010 is an important starting point because it recognises biometric data within the Malaysian data protection framework (Malaysia, 2024). However, statutory recognition alone is not enough. AI cosmetic platforms involve facial scanning, skin analysis, behavioural profiling, automated recommendations and commercial persuasion. These activities require more specific rules than ordinary data processing. Malaysia should therefore move from a general data protection model towards a sector sensitive governance model that addresses the risks of biometric cosmetic personalisation.

First, Malaysia should issue sector specific guidance for AI cosmetic platforms. The amended PDPA should be implemented through practical guidance on how cosmetic companies should collect, store, analyse and delete facial images, skin related information and biometric templates. This guidance should explain when biometric data is being processed, what level of consent is required, what security safeguards must be applied and when data should no longer be retained. The National Pharmaceutical Regulatory Agency already provides cosmetic product control through notification and post market mechanisms (National Pharmaceutical Regulatory Agency, 2022). However, AI cosmetic marketing requires additional guidance that connects cosmetic regulation with data protection and AI governance.

Second, Malaysia should require explicit and layered consent for biometric processing in cosmetic platforms. Consent should not be obtained merely through general privacy notices or bundled terms and conditions. The ASEAN Guide on AI Governance and Ethics emphasises practical governance measures for organisations that design, develop and deploy AI technologies in commercial applications (ASEAN, 2024). Applying this approach to cosmetic AI, consumers should be asked separately whether they agree to facial scanning, biometric template creation, personalised product recommendation, marketing use, third party sharing and AI model training. This layered model would make consumer choice more meaningful and reduce the risk that consumers unknowingly surrender control over sensitive appearance-based data.

Third, businesses using AI cosmetic systems should be required to conduct privacy and algorithmic impact assessments before deployment. Malaysia's National Guidelines on AI Governance and Ethics provide a policy foundation for responsible and ethical AI development (Ministry of Science, Technology and Innovation, 2024). However, these guidelines should be translated into enforceable or sector specific duties for high-risk consumer applications. Cosmetic AI should be treated as higher risk where it processes facial data, makes automated skin classifications or influences product choices affecting wellbeing. An impact assessment should examine the necessity of biometric processing, data minimisation, accuracy, bias, cyber security, commercial influence, consumer vulnerability and available redress mechanisms.

Fourth, Malaysia should create consumer rights against automated cosmetic profiling. These rights should include the right to know when AI is used, the right to withdraw consent, the right to request deletion of biometric data, the right to obtain a basic explanation and the right to challenge harmful or misleading automated recommendations. South Korea provides a useful reference because its revised Personal Information Protection Act introduced Article 37 2 on data subjects' rights in relation to automated decisions (Kim & Park, 2024). Malaysia does not need to copy the South Korean model entirely, but it should recognise that consumers affected by AI recommendations require more than ordinary privacy notices. They need practical rights that allow them to question and contest automated outcomes.

Fifth, liability rules should be clarified to reflect shared responsibility between cosmetic companies and technology providers. AI cosmetic marketing often involves multiple actors, including the cosmetic brand, application developer, AI vendor, data processor, platform operator and product manufacturer. If harm occurs, each party may attempt to deny responsibility by pointing to another actor. Malaysia's Consumer Protection Act 1999 remains relevant where harm arises from defective products, misleading representations or service-related consumer protection issues (Malaysia, 1999). However, AI cosmetic recommendations require a broader responsibility model. A cosmetic company that commercially deploys an AI recommendation system should not avoid liability merely because the algorithm was supplied by a third party. Similarly, technology providers should be accountable where harm results from defective system design, poor data governance or inadequate safeguards.

These reforms should be supported by stronger enforcement capacity and public education. The Department of Personal Data Protection should be equipped with technical expertise to audit AI systems, investigate biometric data misuse and review data protection compliance in consumer facing digital platforms. Coordination should also be improved between data protection authorities, consumer protection regulators and cosmetic regulatory bodies so that complaints involving AI cosmetic platforms do not fall between separate regulatory systems. The aim of reform is not to reject AI in the cosmetic industry, but to ensure that AI is used responsibly while protecting privacy, dignity, autonomy, consumer safety and access to legal remedies.

CONCLUSION

AI driven cosmetic marketing has transformed the way cosmetic products are promoted, personalised and consumed. Through facial scanning, skin analysis, virtual try on tools and automated product recommendations, cosmetic companies are now able to target consumers based on biometric and behavioural data. This development offers commercial benefits, but it also creates serious legal concerns involving consent, transparency, biometric data protection, algorithmic accountability and liability for harm. The issue is therefore not merely whether AI improves cosmetic marketing, but whether Malaysian law can adequately protect consumers when personal appearance becomes a source of commercial data and automated decision making.

Malaysia has made an important legal development through the Personal Data Protection Amendment Act 2024, particularly by recognising biometric data within the sensitive personal data framework (Malaysia, 2024). This reform strengthens the legal protection of facial and body related data used in AI cosmetic platforms. Nevertheless, the amendment does not fully resolve the wider regulatory challenges created by AI cosmetic marketing. The existing framework remains fragmented because the Personal Data Protection Act 2010 focuses mainly on data processing, while the Consumer Protection Act 1999 addresses consumer rights, misleading conduct and defective products (Malaysia, 1999, 2010). Neither statute provides a complete framework for algorithmic profiling, automated cosmetic recommendations, explainability, shared platform responsibility or consumer redress.

The comparative analysis of Australia and South Korea shows that Malaysia can strengthen its framework by adopting clearer rules on biometric data, privacy risk assessment, automated decision rights and regulatory accountability. Australia's privacy framework treats certain biometric information as sensitive information, while its 2024 facial recognition guidance emphasises necessity, proportionality, consent, notice, accuracy, bias and security (Commonwealth of Australia, 1988; Office of the Australian Information Commissioner, 2024a). South Korea provides another useful reference through its biometric information guidance and developing legal treatment of automated decision making (Kim & Park, 2024; Personal Information Protection Commission, 2022). These comparative insights show that Malaysia should not rely only on general consent provisions but should develop more specific protections for AI based consumer profiling.

This article therefore argues that Malaysia requires a more integrated governance model for AI cosmetic marketing. Such a model should combine stronger implementation of the amended PDPA, explicit and layered consent, privacy and algorithmic impact assessments, clearer transparency duties, consumer rights against automated profiling, shared liability between cosmetic companies and technology providers, and stronger enforcement coordination. Malaysia's National Guidelines on AI Governance and Ethics provide a useful policy foundation, but ethical guidance should be supported by clearer legal duties where biometric data and consumer vulnerability are involved (Ministry of Science, Technology and Innovation, 2024).

Ultimately, the future of AI cosmetic marketing in Malaysia should not be framed as a choice between innovation and regulation. The real challenge is to ensure that innovation proceeds within a legal framework that respects privacy, dignity, autonomy, fairness and consumer safety. As cosmetic personalisation becomes increasingly dependent on facial data and automated profiling, Malaysian law must recognise that harm may arise not only from unsafe products but also from unsafe digital recommendation systems. A coherent framework combining data protection, consumer protection and AI accountability is therefore essential to ensure that consumers remain protected in an increasingly personalised beauty market.

REFERENCES

1. A v National Blood Authority [2001] 3 All ER 289
2. Amin, N. (1999). Product liability under the Consumer Protection Act 1999. *IIUM Law Journal*, 7(2), 175–198.
3. ASEAN. (2024). ASEAN guide on AI governance and ethics. Association of Southeast Asian Nations. https://asean.org/wp-content/uploads/2024/02/ASEAN-Guide-on-AI-Governance-and-Ethics_beautified_201223_v2.pdf
4. Barocas, S., & Nissenbaum, H. (2014). Big data's end run around anonymity and consent. *Privacy, big data, and the public good: Frameworks for engagement*, 1, 44-75.
5. Belenguer, L. (2022). AI bias: exploring discriminatory algorithmic decision-making models and the application of possible machine-centric solutions adapted from the pharmaceutical industry. *AI and Ethics*, 2(4), 771-787.
6. Buiten, M. C. (2024). Product liability for defective AI. *European Journal of Law and Economics*, 57(1), 239-273.
7. Chagal-Feferkorn, K. A. (2019). Am I an algorithm or a product: when products liability should apply to algorithmic decision-makers. *Stan. L. & Pol'y Rev.*, 30, 61.
8. Chynoweth, P. (2008). Legal research. In A. Knight & L. Ruddock (Eds.), *Advanced research methods in the built environment* (pp. 28–38). Wiley Blackwell.
9. Commonwealth of Australia. (1988). Privacy Act 1988. Federal Register of Legislation. <https://www.legislation.gov.au/C2004A03712/latest/text>
10. *Donoghue v Stevenson* [1932] AC 562.
11. *Grant v Australian Knitting Mills Ltd* [1936] AC 85
12. Gryz, J., & Rojszczak, M. (2021). Black box algorithms and the rights of individuals: No easy solution to the "explainability" problem. *Internet Policy Review*, 10(2), 1-24.
13. Hash, M. G., Forsyth, A., Bret-Ashleigh, C., Li, V., Julia, V. B., & Frasier, K. M. (2025). Artificial intelligence in the evolution of customized skincare regimens. *Cureus*, 17(4).
14. Hussain, B., Aslam, S., & Imran, A. (2025). Manufacturing beauty: How AI and Social media are redefining aesthetic norms in emerging digital cultures. *Acta Psychologica*, 260, 105734.
15. Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: doctrinal legal research. *Deakin law review*, 17(1), 83-119.
16. Kim, D. H., & Park, D. H. (2024). Automated decision-making in South Korea: a critical review of the revised Personal Information Protection Act. *Humanities and Social Sciences Communications*, 11(1), 1-11.
17. Malaysia. (1999). Consumer Protection Act 1999 (Act 599). Percetakan Nasional Malaysia Berhad.
18. Malaysia. (2010). Personal Data Protection Act 2010 (Act 709). Percetakan Nasional Malaysia Berhad.
19. Malaysia. (2024). Personal Data Protection (Amendment) Act 2024 (Act A1727). Government of Malaysia.
20. Ministry of Science, Technology and Innovation. (2024). The national guidelines on AI governance and ethics. Malaysian Science and Technology Information Centre.
21. National AI Office. (2024). Governance. Malaysia National AI Office. <https://ai.gov.my/governance/>
22. National Pharmaceutical Regulatory Agency. (2022). Guidelines for control of cosmetic products in Malaysia (2nd ed.). Ministry of Health Malaysia.
23. OECD. (2019). OECD principles on artificial intelligence. Organisation for Economic Co-operation and Development. <https://www.oecd.org/en/topics/ai-principles.html>
24. Office of the Australian Information Commissioner. (2024a). Facial recognition technology: A guide to assessing the privacy risks. Australian Government. <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/facial-recognition-technology-a-guide-to-assessing-the-privacy-risks>
25. Office of the Australian Information Commissioner. (2024b, November 19). Bunnings breached Australians' privacy with facial recognition tool. Australian Government. <https://www.oaic.gov.au/news/media-centre/bunnings-breached-australians-privacy-with-facial-recognition-tool>

26. Paris, M. L. (2016). The comparative method in legal research: the art of justifying choices. *Legal Research Methods: Principles and Practicalities* (Clarus Press 2016), UCD Working Papers in Law, Criminology & Socio-Legal Studies Research Paper, (09/16).
27. Perret, J. K., & Schwientek, J. (2025). Beauty Tech—Customer Experience and Loyalty of Augmented Reality-and Artificial Intelligence-Driven Cosmetics. *Digital*, 5(2), 21.
28. Personal Information Protection Commission. (2022). Biometric information protection guideline. Republic of Korea. <https://www.pipc.go.kr/eng/user/lgp/law/ordinancesList.do>
29. Republic of Korea. (2011). Personal Information Protection Act. Korean Law Translation Center. https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG
30. Roslan, M. A., Aziz, N. A., Abd Rani, A. R., Roslan, R., & Che Mohamad, C. A. (2023). Product liability law: Producer's liability for harmful cosmetic products. *Malaysian Journal of Social Sciences and Humanities*, 8(5), Article e002323.
31. Sarabdeen, J. (2022). Protection of the rights of the individual when using facial recognition technology. *Heliyon*, 8(3).
32. Tene, O., & Polonetsky, J. (2012). Big data for all: Privacy and user control in the age of analytics. *Nw. J. Tech. & Intell. Prop.*, 11, 239.
33. UNESCO. (2022). Recommendation on the ethics of artificial intelligence. United Nations Educational, Scientific and Cultural Organization. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>
34. Zakuan, Z. Z. M., & Ismail, R. (2019). Health supplement and product liability in Malaysia: A call for reform. *Malaysian Journal of Consumer and Family Economics*, 23(1), 33-55.
35. Zweigert, K., & Kötz, H. (1998). *An introduction to comparative law* (T. Weir, Trans.; 3rd ed.). Oxford University Press.