行政院 113 年度委託研究計畫

強化人工智慧(AI)商品或服務之消費者保護法制研究報告

受委託單位：南臺學校財團法人南臺科技大學

計畫主持人：郭戎晉

協同主持人：林昕璇

專家顧問：邱映曦

研究期程：113年5月7日至113年12月5日

報告完成日期：113年11月30日

目錄

摘要

人工智慧作為當前最受矚目的資通訊技術，已快速滲透商業活動各個層面，幾近所有行業均可窺見人工智慧的應用實例。由於人工智慧系統可能不具可解釋性或透明度不足，而人工智慧決策亦可能存在偏頗與歧視情形，加諸大量使用消費者個人資料，從而易於產生包括消費者保護在內的各項爭議。為解決人工智慧衍生爭端，國際上針對人工智慧展開的治理討論，已由早期以自律為主的情形，開始轉為以他律為主，而歐盟更在 2024 年 6 月通過全球首部人工智慧全面性監管專法：人工智慧法，於同年 8 月生效，同時刻正推動人工智慧責任指令，以期有效因應人工智慧系統實務應用帶來的民事責任處理問題。除歐盟外，包括美國、日本及英國在內的國家，則未推動人工智慧專法，透過包括行政指導在內的軟法機制，以期因應人工智慧帶來的消費者保護挑戰。

回歸我國而論，國科會於 2024 年 7 月預告「人工智慧基本法」（草案），惟草案在定位為基本法下，針對人工智慧實務應用可能引發的消費者保護爭議，仍有必要評估應否就我國消費者保護法制進行必要調適。本研究梳理人工智慧商品或服務於我國消費者保護法（以下簡稱消保法）之適用議題並提出法規調適建議，其一，人工智慧商品/服務於消保法上之定性，本研究認為人工智慧可能本身即為商品或服務，或作為商品或服務之重要部分，從而應有我國消保法之適用，而現行消保法及施行細則有關商品或服務之定義，並無須對應人工智慧商品或服務之判斷需求而進行修正，於個案判斷上遇有爭議時可透過函釋方式進行說明。

其二，人工智慧商品/服務所涉及之可合理期待安全性，考量消保法第 7 條所要求之「安全性」，係針對「所有」受消保法規範的商品或服務之通案規範，本研究認為針對人工智慧商品或服務消保法第 7 條規定應可直接適用而無立即進行調適之必要。有關個案處理上可能遇有安全性究應如何認定等問題，現階段已有司法實務提出「技術標準」之適用可能，可關注「人工智慧基本法」（草案）中有關風險分級與評測機制之後續推動情形。

其三，人工智慧商品/服務所涉及之消費資訊揭露，包括消保法第 4 條與第 5 條在內、現行消保法中有關商品或服務所涉及之消費資訊揭露要求，性質上屬於原則性規範。對應特定商品或服務的消費資訊揭露要求，歷來多見於目的事業主管機關針對其主管商品或服務所制定的「定型化契約應記載及不得記載事項」之中，爰本研究認為針對人工智慧商品/服務所涉及之消費資訊揭露要求，並無須於消保法本身進行調適，而應思考如何透過既有的商品或服務之定型化契約應記載及不得記載事項之增修，從而使其可得充分因應人工智慧所帶來之挑戰。

其四，針對人工智慧商品或服務產生侵權時之法律責任，由於人工智慧本身所具備的特徵，對於使用人工智慧商品或接受人工智慧服務的消費者而言，恐產生難以預見的損害及訴訟上舉證之困難。考量人工智慧民事侵權問題的處理需求，歐盟也在既有的民事法與產品責任規範體系之外，針對人工智慧另行推動人工智慧責任指令（草案）。歐盟推動人工智慧責任指令的主要目的便在於解決人工智慧侵權問題之舉證難題，就我國法而言，消保法原即採取「舉證責任倒置」設計，此外，民法第 191 條之 1 規定亦採納「過失推定」設計，在我國民法已有關聯設計之下，或無參考歐盟立法制定人工智慧相應責任規範之急迫需求。另一方面，考量人工智慧技術暨其關聯實務應用仍屬於人們認識有限之事物，當人工智慧商品或服務肇致消費者損害，現階段實務操作上或仍有不易判斷其因果關係之可能，本研究亦試擬建議條文供委託機關參考。

我國消費者保護法制如何因應人工智慧帶來之衝擊，除消保法本身之調適評估外，另一應併同思考與推動之處，係各目的事業主管機關按消保法授權所制定的「定型化契約應記載及不得記載事項」之調適。本研究認為並非全數的定型化契約應記載及不得記載事項，均受到人工智慧影響或有因應人工智慧衝擊而進行調適之必要，務實方向應優先擇定現階段與人工智慧應用關係較為直接並已實制定定型化契約規範之領域。按 Statista 研究成果，現時人工智慧實務應用占比最高的前五大行業別，分別為：1、醫療健康照護；2、金融；

3、製造；4、商業暨法律服務；以及5、交通，可基此進行評估，並檢視其他可能應用人工智慧技術且數位連結較深連結較深之特定商品或服務型態，其定型化契約應記載及不得記載事項亦有無進行調適之必要。針對有調適必要者，現階段建議可針對消費者知悉與風險告知等事項，著眼消費資訊揭露制定相應之定型化契約應記載事項，同時可針對國際關注之人工智慧/演算法可能存在的偏見與歧視問題，制定相應之定型化契約不應記載事項，本研究並試擬關聯建議。

當前國際因應包括消費者保護在內、人工智慧實務應用衍生的各項爭議，除立法論層面（硬法）的討論與推動，亦不乏側重軟法機制之應用。本研究辦理的「人工智慧商品或服務之消費者保護焦點座談會」與「實務深度訪談」，相關專家多數亦認為人工智慧尚處於發展階段，現時課予過重規範或恐阻礙產業發展，且亦有規範不易之可能，我國初期或宜採取低度管理策略，先軟法（例如制定指引）而後評估必要法制之介入。對此，參考日本消費者廳推動經驗，立於消費者保護主管機關角度研訂諸如日本消費者廳人工智慧活用手冊之行政指導文件，不失為可行方向。

關鍵詞：人工智慧、人工智慧法、人工智慧責任指令、消費者保護法、定型化契約應記載不得記載事項

Abstract

Artificial intelligence (AI), as the most prominent information and communication technology today, has rapidly permeated all aspects of business activities, with examples of AI applications observable in nearly every industry. However, AI systems may lack explainability or transparency, and AI-driven decisions can involve biases and discrimination. Combined with the extensive use of consumer personal data, these factors are prone to giving rise to disputes, including those related to consumer protection.

To address disputes stemming from AI, international governance discussions on AI have shifted from an initial focus on self-regulation to a more externally regulated approach. Notably, in June 2024, the European Union passed the world's first comprehensive AI-specific regulatory law, the Artificial Intelligence Act, which took effect in August of the same year. Concurrently, the EU is advancing the AI Liability Directive to effectively tackle civil liability issues arising from the practical application of AI systems. In contrast, countries such as the United States, Japan, and the United Kingdom have not implemented AI-specific laws. Instead, they rely on soft-law mechanisms, including administrative guidance, to address the consumer protection challenges posed by AI.

Turning to the situation in Taiwan, the National Science and Technology Council announced a draft of the Fundamental Artificial Intelligence Act in July 2024. However, as the draft is positioned as a foundational law, it remains necessary to evaluate whether adjustments to Taiwan’s consumer protection legal framework are required to address disputes arising from the practical application of AI.

This study examines issues related to the application of AI products or services under Taiwan's Consumer Protection Act (hereinafter referred to as the CPA) and proposes regulatory adjustment recommendations.

First, regarding the classification of AI products/services under the CPA, this study suggests that AI may itself constitute a product or service or serve as an essential component of a product or service. As such, it should fall within the scope of the CPA. The current definitions of "product" and "service" under the CPA and its enforcement rules do not necessitate amendments to specifically address AI-related determinations. Any disputes in individual cases can be clarified through interpretative guidelines issued by relevant authorities.

Second, regarding the reasonably expected safety of AI products/services, the "safety" requirement under Article 7 of the CPA applies as a general standard to all products and services regulated by the Act. This study posits that Article 7 of the CPA can be directly applied to AI products or services without the immediate need for adjustments. As for challenges in determining safety in individual cases, current judicial practices have already proposed the potential application of "technical standards." Future developments in the risk classification and assessment mechanisms outlined in the draft Fundamental Artificial Intelligence Act can also be closely monitored to inform case-by-case evaluations.

Third, regarding the disclosure of consumer information related to AI products/services, the requirements for consumer information disclosure under Articles 4 and 5 of the CPA are fundamentally principle-based regulations. Specific consumer information disclosure requirements for particular products or services have traditionally been addressed through the Mandatory and Prohibitory Provisions of Standard Contracts established by the competent authorities for the respective products or services. Therefore, this study suggests that there is no need to amend

the CPA itself to address the consumer information disclosure requirements for AI products/services. Instead, efforts should focus on revising and updating the Mandatory and Prohibitory Provisions of Standard Contracts for relevant products or services to adequately respond to the challenges posed by AI.

Fourth, regarding legal liability arising from torts involving AI products or services, the unique characteristics of AI may result in unforeseen damages and evidentiary difficulties for consumers using AI products or receiving AI services. Recognizing the need to address civil liability issues related to AI, the European Union, beyond its existing civil law and product liability framework, has introduced a draft AI Liability Directive to tackle such challenges. The primary goal of this directive is to resolve evidentiary difficulties in AI-related tort cases. In the context of Taiwan’s legal framework, the CPA already adopts a "reversal of the burden of proof" approach, while Article 191-1 of the Civil Code incorporates a "presumption of negligence" design. Given these existing provisions, there may not be an urgent need to emulate the EU's legislative efforts by introducing specific liability rules for AI. However, considering that AI technology and its practical applications remain relatively novel and not fully understood, it may still be challenging in practice to establish causal relationships when AI products or services cause harm to consumers. In light of this, this study has drafted proposed provisions for consideration by the commissioning authority to address potential gaps in the current legal framework.

How Taiwan’s CPA should respond to the challenges posed by artificial intelligence (AI) requires not only an evaluation of adjustments to the Act itself but also consideration of necessary updates to the Mandatory and Prohibitory Provisions of Standard Contracts established by sectoral regulators under the CPA's authority. This study suggests that not all standard form contract provisions are impacted by AI or require adjustment to address AI-related challenges. A pragmatic approach

would prioritize sectors where AI applications are most directly relevant and where standard form contract regulations are already established. According to research by Statista, the top five industries with the highest adoption of AI applications are: Healthcare, Finance, Manufacturing, Business and legal services, and Transportation. These industries can serve as a starting point for evaluation. Additionally, other goods or services with significant AI integration and deep digital interconnectivity should be reviewed to determine whether their standard form contract provisions require adjustments. For areas where adjustments are deemed necessary, it is recommended to focus on enhancing consumer awareness and risk disclosure by specifying relevant information in the "mandatory provisions" of standard form contracts. Simultaneously, to address international concerns about potential biases and discrimination in AI and algorithms, corresponding "prohibited provisions" should be developed. This study has also drafted related recommendations for further reference.

The current international responses to disputes arising from the practical application of artificial intelligence (AI), including those related to consumer protection, involve not only discussions and advancements in legislative measures (hard law) but also emphasize the application of soft law mechanisms. In the focus group discussions and practical interviews conducted for this study, most experts agreed that AI is still in its developmental stage. Imposing excessively stringent regulations at this point could potentially hinder industrial growth and present difficulties in enforcement. As such, Taiwan may initially consider adopting a low-regulation strategy, beginning with soft law measures (e.g., issuing guidelines) and subsequently assessing the necessity for legal interventions. In this regard, drawing on the experience of Japan's Consumer Affairs Agency, it would be feasible for Taiwan's consumer protection authorities to develop administrative guidance

documents, such as Japan's AI Utilization Handbook, to address these issues flexibly and pragmatically.

Keywords: Artificial Intelligence, Artificial Intelligence Act, AI Liability Directive, Consumer Protection Act, Mandatory and Prohibitory Provisions of Standard Contracts.

壹、緒論

一、研究背景

數位經濟成為當前全球經濟發展重心的關鍵因素，其一是網路的高度普及，全球總人口在 2022 年 11 月正式突破 80 億人，而網路使用人口在 2023 年 1 月達到 51.6 億人，普及率為全球總人口的 64.4%。另一重要因素則是嶄新資通訊技術的持續發展，其中「人工智慧」（Artificial Intelligence, AI）更是對商業活動及人類生活各個層面，帶來難以想見的結構性變革。隨著人工智慧技術發展持續精進與應用領域的多元化，此一嶄新技術引發的問題也隨之增加，除演算法黑箱與歧視公平等問題，近期 AI 商品或服務對消費者保護可能帶來的危害，亦日益受到關注。

人工智慧技術正快速地滲透各個行業並催生眾多過往難以想見的創新應用，但在人們嘗試受惠於此一嶄新技術的同時，當人工智慧商品或服務肇致損害，如何確定並建立妥適的責任規範，也成為人工智慧技術與實務應用是否足資信賴的關鍵因素之一[1]。

面對人工智慧發展伴隨而生的各項問題之處理，「自律」與「他律」機制各有擁護者，儘管自律概念立意良善且有助於彌補人工智慧發展初期的監管真空（regulatory vacuum）情形，在人工智慧衍生爭端急遽增加且難以套用既有的監管經驗之下，國際上應對人工智慧的治理思維也開始出現變化。除由全然自律開始加入他律，近年更有進一步向他律靠攏、甚至轉以他律為主之趨勢。

本研究計畫以「人工智慧商品或服務之消費者保護法制」為研究對象，首先梳理國際上有關人工智慧/人工智慧之定義與實務應用現況，進而針

[1] Tambiama Madiega, Artificial Intelligence Liability Directive, European Parliamentary Research Service PE 739.342 (2023), at 2.

對所設定的目標國別（美國、歐盟、日本及英國），分析各國著眼人工智慧治理以及所涉消費者保護問題之法制適用討論與新興法制推動情形。其次，在國內外法制比較研析以及專家座談討論成果等基礎上，進一步檢視人工智慧商品或服務在我國所涉及的消費者保護問題以及現行消費者保護關聯法制之適用問題，以期針對我國消費者保護法制，包括消費者保護法（以下簡稱消保法）本身及關聯定型化契約規範如何因應人工智慧發展，提出具體法規調適建議。

二、研究方法

(一)、法制比較分析

本研究計畫以人工智慧商品或服務所涉及的消費者保護法制為研究對象，為利掌握我國消費者保護法制如何因應人工智慧帶來的挑戰，以及現行規範有無進行調適的必要與具體調適作為，了解主要國家作法即有其必要性。本研究計畫設定殊值研究的目標國別，計包括歐盟、美國、日本及英國。

藉由掌握相關目標國家針對人工智慧商品或服務所涉消費者保護議題與關聯法制之討論情形與法制推動現況，以利在國、內外法制比較之基礎上，針對人工智慧商品或服務在我國消費者保護法下之適用與法規調適提出具體建議。

本研究計畫針對國際法制分析之進行，涵蓋下列面向：

1、了解目標國家（歐盟、美國、日本、英國）著眼人工智慧所推動之具體立法或法制草案，以及是否存在關聯之軟體機制，諸如指引及產業標準等。

2、上述相關硬法及軟法機制中，與人工智慧商品或軟體有關之規範或討論情形；

3、藉由比較法之研究，了解我國消費者保護法等相關法規，有關人工智慧商品或服務所涉消保機制之利弊得失。

(二)、研究文獻分析

除上述目標國家暨我國法制之比較研究，本研究計畫亦針對人工智慧商品或服務衍生的消費者保護議題與法律適用，分析關聯文獻資料。研究文獻資料範疇包括：

1、四個目標國家（歐盟、美國、日本、英國）針對人工智慧暨人工智慧所涉及之消費者保護問題，所發布之法制政策分析文獻、研究報告暨其他關聯研究文獻資料；

2、重要國際組織如「聯合國貿易暨發展會議」（United Nations Conference on Trade and Development, UNCTAD）、「經濟合作暨發展組織」（Organisation for Economic Cooperation and Development, OECD）及消費者保護關聯國際組針對人工智慧/消費者保護所提出之政策文件或研析報告；

3、國內外學者專家撰寫發表之關聯研究論文。

(三)、焦點座談及專家訪談

人工智慧無疑是時下多數人知悉的名詞，但人們對於此一新興技術暨其衍生爭端的認識仍十分有限。為利完整掌握人工智慧商品或服務對

消費者保護暨關聯立法帶來的影響，並評估我國消費者保護法制有無進行適度調適之必要，藉由辦理「焦點座談會」，蒐集包括專家學者、優良消保團體、相關機關及地方政府消保官等各方先進之意見。此外，本研究計畫將賡續座談會結論與研究發現，辦理「實務訪談」，俾利使本計畫之研究發現與提出之法規調適建議，契合各界之意見與寶貴建議。

貳、人工智慧實務應用與消費者保護爭端

一、人工智慧（人工智慧系統）之定義

(一)、世界智慧財產權組織

人工智慧就字面意義而言泛指「非人類（機器）所表現的智慧」，惟此一簡要定義易於使人工智慧被誤解為單一或特定技術，但人工智慧其實是眾多技術的結合運用[2]。就技術層面而言，世界智慧財產權組織（World Intellectual Property Organization, WIPO）於 2019 年發布的人工智慧技術趨勢報告便明確表示人工智慧並非單一技術概念[3]。

根據 WIPO 的說明，人工智慧涵括多個細部技術概念，主要包括：1、機器學習（Machine Learning）；2、邏輯程式設計（Logic programming）；3、模糊邏輯（Fuzzy Logic）；4、概率推理（Probabilistic Reasoning）； 5、本體工程（Ontology Engineering）；以及 6、功能應用（Functional Application）關聯技術。而最後的功能應用關聯技術，又可再細分為：1、電腦視覺（Computer Vision）；2、自然語言處理；3、語音處理（Speech Processing）及 4、其他功能應用等子概念[4]。

[2] 郭戎晉，論人工智慧技術應用、法律問題定位及監管立法趨勢－以美國實務發展為核心，成大法學，第 39 期，頁 180，2020 年 6 月。

[3] World Intellectual Property Organization. WIPO Technology Trends 2019: Artificial Intelligence (2019), at 24.

[4] *Id.* at 24-26.

(二)、經濟合作暨發展組織

除了上述 WIPO 由技術面針對人工智慧所進行之定義，經濟合作暨發展組織（Organisation for Economic Cooperation and Development, OECD）在 2019 年發布的人工智慧建議書（The OECD's Recommendation of the Council on Artificial Intelligence），則是針對「人工智慧系統」（AI System）一詞進行定義並受到廣泛引用。依 OECD 人工智慧建議書之定義，人工智慧系統係指「一種基於機器的系統，其可以針對由人類所界定的目標，作成影響真實或虛擬環境之預測、建議或決策。人工智慧系統可被設計為具有不同程度之自主性」[5]。

OECD 在 2023 年 11 月修正上揭建議書中有關「人工智慧系統」之定義[6]，將之重新界定為「一種基於機器的系統，針對明確或隱含目標，根據所接獲的輸入推斷如何產製可能影響真實或虛擬環境之預測、內容、建議或決策等輸出。不同的人工智慧系統實際部署後之自主性與適應性程度各不相同」[7]。

除專業名詞定義，OECD 人工智慧建議書還揭櫫了「可信賴人工智慧之負責任管理原則」與「可信賴人工智慧之國家政策與國際合作」等重要內容。自發布以降，OECD 人工智慧建議書已受到諸多國家的採納；OECD 將採納國家稱為「跟隨者」（Adherents），除了歐盟，還包括了 38 個 OECD 成員國及 8 個非成員國[8]。

---

[5] Organisation for Economic Cooperation and Development (OECD), Recommendation of the Council on Artificial Intelligence, https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449 (last visited Nov. 1, 2024).

[6] *Id.*

[7] AI system: An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.

[8] 8 個非成員國為：阿根廷、巴西、埃及、馬爾他、秘魯、羅馬尼亞、新加坡與烏克蘭。

(三)、歐盟

OECD 提出的「人工智慧系統」概念與定義受到廣泛引用，歐盟於研訂人工智慧法（Artificial Intelligence Act；以下簡稱 AIA）時，也直接採納了「人工智慧系統」一詞。自歐盟執委會提出 AIA 草案，截至 2023 年 6 月歐洲議會通過其談判立場版本，歐盟將人工智慧系統定義為「指基於機器之系統，其被設計為以不同程度自主運行，可得針對明確或隱含之目標，產製影響真實或虛擬環境之預測、建議或決策」[9]，此一定義直接反映了 OECD 在 2019 年人工智慧建議書中針對「人工智慧系統」所作定義。

隨著 OECD 在 2023 年 11 月修正「人工智慧系統」定義，歐盟在 2024 年最終通過 AIA[10]時，其人工智慧系統定義也隨之調整為「指基於機器的系統，以不同程度的自主性進行操作並得於部署後展現適應性，針對明確或隱含的目標，根據所接獲的輸入推斷如何產製可能影響真實或虛擬環境之內容、建議或決策等輸出」[11]。

---

[9] Art. 3(1) 'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;

[10] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 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)Text with EEA relevance, OJ L, 2024/1689, 12.7.2024.

[11] Art. 3(1) 'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;

(四)、我國

受到歐盟等國際立法推動之影響，國家科學及技術委員會（以下簡稱國科會）於 2024 年 7 月 15 日預告「人工智慧基本法草案」。在此之前，亦曾有立法委員及學者嘗試提出「人工智慧基本法」，而部分立法委員之提案，甚至早於歐盟正式著手研訂 AIA。

1、立法院「人工智慧發展基本法草案」之定義

2019 年 5 月 15 日立法委員許毓仁等 21 位委員率先提出「人工智慧發展基本法草案」[12]以降，立法院即持續針對人工智慧立法進行提案。歷來可見版本尚包括 2020 年 9 月 16 日立法委員鄭麗文等 20 位委員提出之「人工智慧發展基本法草案」[13]、2022 年 9 月 28 日台灣民眾黨黨團提出之「人工智慧發展基本法草案」[14]、2023 年 12 月 6 日台灣民眾黨黨團提出之「人工智慧發展及管理條例草案」[15]、2024 年 4 月 12 日立法委員吳宗憲等 17 位委員提出之「人工智慧基本法草案」[16]、2024 年 4 月 26 日立

[12] 立法院第 9 屆第 7 會期第 14 次會議議案關係文書，院總第 1021 號委員提案第 23371 號，2019 年 5 月 15 日。

[13] 立法院第 10 屆第 2 會期第 1 次會議議案關係文書，院總第 1021 號委員提案第 24935 號，2020 年 9 月 16 日。

[14] 立法院第 10 屆第 6 會期第 2 次會議議案關係文書，院總第 1021 號委員提案第 28966 號，2022 年 9 月 28 日。

[15] 立法院第 10 屆第 8 會期第 11 次會議議案關係文書，院總第 20 號委員提案第 10043021 號，2023 年 12 月 6 日。

[16] 立法院第 11 屆第 1 會期第 9 次會議議案關係文書，院總第 20 號委員提案第 11002784 號，2024 年 4 月 10 日。

法委員賴士葆等 28 位委員提出之「人工智慧基本法草案」[17]及 2024 年 10 月 25 日立法委員林宜瑾等 21 人提出之「人工智慧基本法草案」[18]。

以 2019 年 5 月 15 日最先提出之「人工智慧發展基本法草案」為例，依草案第 2 條第 1 項規定，其所界定的「人工智慧」如下：

「所謂人工智慧係指符合下列任一款情形者：

一、在沒有顯著的人為監督，及不同與不可預測的情況下，得執行任務的人為謀劃系統或得從人類的經驗中學習，並提高效能的系統。

二、任何運行模式與人類思考相似的系統，如人的認知架構和神經網絡。

三、表現像人類的系統，例如通過圖靈測試或經由自然語言處理、知識呈現、自動推理、及學習等其他相當的測試。

四、尋求逼近特定認知任務的技術，如機器學習。

五、行為理性的系統，如智慧軟體代理人與通過感知、規劃、推理、學習、溝通，決策、及行動來實現目標的實體化機器人」。

就上述定義而言，與現今國際組織及可見人工智慧立法所界定的人工智慧或人工智慧系統，有著相當之差異。

2、人工智慧法律國際研究基金會「人工智慧基本法草案」之定義

受到歐盟於 2021 年開始推動 AIA 影響，包括我國在內，各國紛紛始討論有無推動人工智慧專法之必要。就國內發展而言，除上述立法院之倡議外，由學者及產業專家組成的人工智慧法律國際研究基金會，也在 2023 年 3 月提出學者版之「人工智慧基本法草案」。

[17] 立法院第 11 屆第 1 會期第 9 次會議議案關係文書，院總第 20 號委員提案第 11003774 號，2024 年 4 月 24 日。

[18] 立法院第 11 屆第 2 會期第 6 次會議議案關係文書，院總第 20 號委員提案第 11007216 號，2024 年 10 月 23 日。

依草案第 3 條規定，其所界定的「人工智慧」為：「本法所稱人工智慧，指接收人類或機器資料輸入，以下列各款全部或部分方式，實現預測、建議、決策或其他特定目的之軟體、硬體及其他相關之系統：

一、使用監督式學習、非監督式學習、強化學習或其他利用資料建立模型之機器學習方式。

二、使用各種知識表示方式建立之知識庫系統，以推理引擎進行歸納、演繹、反證或其他模仿人類邏輯推理能力之方式。

三、使用統計、搜尋、剖析、優化或其他方法，建立決策或推理模型之方式。

四、使用前三款以外之模仿人類思考及反應模式，進行感知、規劃、推理、學習、溝通、修正或其他之方式。」

3、國家科學委員會「人工智慧發展基本法草案」之定義

國科會在 2024 年 7 月 15 日預告制定「人工智慧基本法」草案，草案總說明指出「為確立我國推動人工智慧技術與應用發展之方向及作法，建構人工智慧技術與應用之良善運作環境，為政府刻不容緩之責任。故此，制定人工智慧發展之基本法律，從基本原則、政府推動重點等構面提出基本價值、治理原則及施政方針，期使我國人工智慧發展促進創新兼顧人權與風險，進而提升我國競爭力，爰擬具『人工智慧基本法』草案」。

草案第 2 條規定「本法所稱人工智慧，係指以機器為基礎之系統，該系統具自主運行能力，透過輸入或感測，經由機器學習與演算法，可為明確或隱含之目標實現預測、內容、建議或決策等影響實體或虛擬環境之產出」。立法說明指出此一定義係參考美國國家人工智慧創新法案（National AI Initiative Act of 2020）、國際標準化組織（ISO）及國際電工委員會（IEC）聯合制定技術規範（ISO/IEC）42001：2023 人工智慧管理系統、美國國

家標準暨技術研究院（National Institute of Standards and Technology，NIST）AI 風險管理框架，以及歐盟人工智慧法（AIA）對於人工智慧系統之定義，說明人工智慧必須被設計為具備一定程度之自主運行能力，透過輸入或感測，可為明確或隱含之特定目的， 經過機器學習與演算法實現諸如預測、內容、建議或決策等影響實體或虛擬環境之產出，與其他軟體系統有別[19]。

二、人工智慧之實務應用現況

(一)、逐步深入各個行業並催生龐大商機

人工智慧技術持續發展並快速滲透商業活動及人類生活各個層面下，公、私部門已有不勝枚舉的人工智慧應用案例出現。就私部門應用而言，普華永道（PricewaterhouseCoopers, PwC）在 2017 年所作研究指出人工智慧發展潛力最為顯著的業態，前三位分別為醫療照護、交通運輸及金融服務，此一情形也反映了人工智慧的早期應用大抵以「管制性行業」為主[20]。

伴隨人工智慧應用領域的擴大，當前幾近「所有行業」均可窺見人工智慧之使用，市場研究機構 Statista 在 2024 年指出當前全球人工智慧使用情形，若按行業別占比進行排序，前十大分別為：

1、醫療健康照護（15.7%）；

2、金融（13.65%）；

3、製造（13.65%）；

---

[19] 國科會所預告之「人工智慧基本法」草案全文，可參見國科會，預告制定「人工智慧基本法」草案，網址：https://join.gov.tw/policies/detail/4c714d85-ab9f-4b17-8335-f13b31148dc4（最後瀏覽日：2024 年 10 月 25 日）。

[20] PricewaterhouseCoopers, Sizing the Prize What's the Real Value of AI for Your Business and How Can You Capitalise? (2017), at 11-14.

4、商業暨法律服務（13.6%）；

5、交通（10.75%）；

6、保全（9.9%）；

7、其他（5.81%）；

8、能源（5.29%）；

9、媒體娛樂（4.92%）；

10、零售（4.35%）[21]。

在深入並受到幾近所有行業採用之下， Statista 同時指出全球人工智慧市場規模預計於 2024 年達到 1,840 億美元，並可望以 28.46%年複合成長率在 2030 年進一步擴大為 8,267 億美元，其規模著實驚人[22]。

(二)、近期另有生成式人工智慧快速崛起

早期人們對人工智慧的討論以鑑別式人工智慧為主，近期生成式人工智慧（Generative Artificial Intelligence, Generative AI）則快速擷取人們目光。特別是 2022 年 ChatGPT 上市後，旋即於兩個月後其月活躍用戶便達到 1 億規模，成為史上成長速度最快的消費者應用程式。ChatGPT 屬於「文本生成」領域的生成式人工智慧應用，而當前在「圖像生成」、「語音生成」、「音樂生成」、「影像生成」及「軟體生成」等領域，亦可窺見相關的生成式人工智慧產品面世[23]。

在各行業事業爭先導入及運用生成式人工智慧下，生成式人工智慧也被認為可能大幅改變消費市場的面貌，特別是在行銷層面，企業經營者

[21] Statista, Artificial Intelligence - Worldwide, https://www.statista.com/outlook/tmo/artificial-intelligence/worldwide (last visited Oct. 25, 2024).
[22] *Id.*
[23] McAfee, Daniel Rock & Erik Brynjolfsson, *How to Capitalize on Generative AI*, 101(6) HARVARD BUSINESS REVIEW 42, 42-43 (2023).

可望以生成式人工智慧創造消費者導向（客製化）的廣告內容與消費者進行對話24。根據 Bloomberg Intelligence 的研究，以消費者為導向的生成式人工智慧，市場規模估將由 2022 年的 400 億美元，在 2032 年時成長為 1.3 兆美元[25]。

三、人工智慧衍生風險與治理課題

(一)、技術發展與實務應用衍生爭議概覽

1、人工智慧系統不具可解釋性/透明度

無論是早期的自律機制如人工智慧倫理指引，抑或近期漸受重視的人工智慧監管立法，可解釋性與透明度是持續受到關注的主題。特別是「深度學習」（deep learning）等子技術的採用，人工智慧系統具備串接大量數據藉以輸出決策建議的能力，但相關決策的作成卻始終難以除去「黑箱」（black box）作業之爭議。包括消費者保護面向在內，如何解決人工智慧應用上的不透明（opacity）現象，成為各國無可迴避的棘手問題。

2、人工智慧決策可能存在偏頗/歧視情形

與演算法黑箱經常併同討論的問題則是人工智慧系統可能存在著偏頗與歧視情形。研究指出自動化決策依資料處理的階段性進程，可能衍生

[24] *Id.* at 44-48.
[25] Bloomberg Intelligence, Generative AI to Become a $1.3 Trillion Market by 2032, Bloomberg Intelligence (June 1, 2023), https://www.bloomberg.com/company/press/generative-ai-to-become-a-1-3-trillion-market-by-2032-research-finds/ (last visited Nov. 5, 2024).

多重構面的資訊偏頗，包括了：1、原始系統設計者或使用者的既存偏見、2、軟硬體及周邊設備所存在的技術偏見，以及 3、AI 模型設計完成後甫出現的的突發性偏見等。諸如消費者的信用評等以及針對風險用戶的分類判斷等，歷來均曾衍生人工智慧系統所造成的偏頗或不當歧視問題。

3、大量蒐集及利用個人資料產生之隱私爭議

運用人工智慧的商品或服務在研發產製過程中，必須蒐集及利用大量個人資料，藉以系統地匯總並預測用戶的行為與個人偏好，以利後續針對個人進行客製化的廣告精準投放，從而促使消費者做成購買與其他有利於企業經營者之決策。但可能被運用於人工智慧的個人資料，可能出現：1、企業經營者蒐集資料時並未取得當事人的同意；及 2、將用戶個人資料供人工智慧之用，超過所設定「特定目的」等問題。

4、近期受矚目之生成式人工智慧亦衍生智慧財產權侵害等爭議

無論是最為人熟知的文本生成，或圖像、語音、音樂、影像甚或軟體生成等其他領域，在「從無到有」的生成過程中，直接面臨生成內容權利屬性與歸屬等爭議。而運用生成式人工智慧工具進行創作，可能分成全部由人工智慧根據資料庫自動生成呈現結果，或生成後由人類進行部分修改再呈現結果，抑或為根據人類鍵入特定指令所呈現之結果等不同情形，連帶使用生成式人工智慧衍生的智慧財產權問題，有著複雜難解之勢。此外，生成式人工智慧有時亦會產生扭曲或完全捏造的輸出（不實生成內容），也易於造成爭議。

(二)、人工智慧爭端處理與治理難題

1、難題一：難以避免規範上出現「空白現象」

隨著應用領域的多元化，人工智慧所引發的問題也隨之增加，但人工智慧法律爭議早期討論經常出現眾說紛紜或莫衷一是的情形，並有所謂的「空白現象」。人工智慧治理上難以避免「空白現象」，其可能成因包括了：1、人工智慧發展與創新速度之快，使得對應此一技術的監管路徑存在著高度不確定性；2、民選政府可能為了避免背負破壞技術前瞻發展，而選擇漠視人工智慧之監管；3、在影響層面過大之下，協調不同的法律與主管機關，長期存在困難；以及 4、私部門往往對政府監管採取抵制立場[26]。特別是人工智慧技術與應用領域的快速發展與更迭，更讓各國在面對人工智慧所肇致的風險時，不免有著捉襟見肘之感[27]。

2、難題二：難以正確框列及評估衍生風險

人工智慧發展同時帶來正反效益，促使主要國家積極思考人工智慧合宜的監管作法，然而人工智慧監管架構建構上最重要、但也是最為困難的首要步驟，便是確定人工智慧衍生的風險型態與風險級別[28]。為避免著眼人工智慧治理的規範設計，動輒出現規範過度（over regulation）抑或規範不足（under regulation）之制度設計偏頗，人工智慧監管上實有必要先將可能的潛在風險加以定序[29]。

---

[26] David Bollier, Artificial Intelligence, The Great Disruptor: Coming to Terms with AI-Driven Markets, Governance and Life, y The Aspen Institute 23-24 (2018).

[27] 郭戎晉，人工智慧風險治理與監管機制建構之研究－以歐盟監管專法（AIA）與美國風險管理標準為核心，世新法學，第 17 卷第 1 期，頁 119-120，2023 年 12 月。

[28] Thomas Giacobbe, *Adapting to Challenges Posed by The Fourth Industrial Revolution: A Regulatory Call to Action Concerning Cybernetic Technology*, 15 WASH. U. JURISPRUDENCE REV. 141, 164 (2022).

[29] 林昕璇，初探 AI 自動化決策下之差別待遇－以美國法為鑑，開南法學，第 14 期，頁 81，2023 年 2 月。

歷來包括人工智慧在內，著眼於技術發展提出的監管立法，往往面臨著：1、如何跟上技術進步；2、如何在促進技創新與保護基本權利和價值之間取得平衡；3、監管方向係應順從社會多數共識抑或應反其道而行；以及 4、如何平衡手段的有效性與合法性等爭議[30]。但若出於對人工智慧衍生爭端的焦慮，便主張應該以「預先立法」的立場，提早處理與人工智慧發展所帶來的假設性問題，恐有值得商榷之處[31]。

3、難題三：難以援引既有的監管經驗

面對資通訊科技應用衍生的治理課題，若國家在所涉領域的監理發展時間較早，多有著顯著的「路徑依循」（path dependence）特質，亦即面對科技應用帶來的監管難題，執政者往往傾向依循過往的監管經驗，同時援引既有可用之立法進行處理。惟人工智慧所涉技術與應用領域的複雜性，使得人工智慧難以直接援引既有的監管經驗，不乏研究指出當前針對特定議題所採行的監管作法，在欠缺合適性之下，實不應輕易地套用於人工智慧等嶄新技術的監管推動[32]。

4、難題四：治理推動易於落入科林格里奇困境

David Collingridge 在 1980 年提出「科林格里奇困境理論」（Collingridge Dilemma），其是指前瞻技術可能出現的負面影響，在技術發展前期往往難以預測，在無法獲得所生影響的必要資訊下，我們可以控

[30] Ronald Leenes et al., *Regulatory Challenges of Robotics: Some Guidelines for Addressing Legal and Ethical Issues*. 9 L. INNOVATION & TECH. 1, 1-2 (2017).
[31] 劉靜怡，人工智慧潛在倫理與法律議題鳥瞰與初步分析，收錄於劉靜怡編，人工智慧相關法律議題芻議，元照出版，頁 7，2018 年 11 月。
[32] Braden R. Allenby, *Governance and Technology Systems: The Challenge of Emerging Technologies*, in THE GROWING GAP BETWEEN EMERGING TECHNOLOGIES AND LEGAL-ETHICAL OVERSIGHT 3, 3-18 (Gary E. Marchant *et al*. ed., 2011).

制卻不知該控制什麼；當創新技術已在市場上佔有穩固地位，即使其所生影響隨著技術的發展而逐漸明朗，我們知道該控制什麼卻已陷入難以控制之困境[33]。

當執政者的監管創新動能落後於人工智慧技術之創新發展，人工智慧治理討論便可能落入所謂的「科林格里奇困境」。特別是人工智慧細部技術概念包羅萬象，由於不同的技術對應產生的風險或危害往往不盡相同，在人們尚無法完全掌握人工智慧發展走向及所生風險之下，過早或失當的監管可能會適得其反；但若囿於不確定性而躊躇不前，最終亦可能出現技術應用已在社會中根深蒂固而愈發不易監管[34]。

(三)、根源人工智慧之消費者保護爭端態樣

OECD 指出人工智慧與演算法可得影響消費者的脆弱性，由於數位平臺已愈頻繁地使用人工智慧、演算法與大數據，自動化與其產品有關的決策與流程，諸如運用量身訂製的服務使消費者受益。然而，相關做法也可能帶來全新的風險，形成為對特定消費者的偏見與歧視。趨勢顯示特定消費者可能因其脆弱性而成為事業鎖定的目標，並可能易於遭受攻擊[35]。

日本消費者保護主管機關：消費者廳（消費者庁）為因應人工智慧帶來的衝擊，於 2020 年 1 月成立「消費者因應數位化檢討會之人工智慧小組」（消費者のデジタル化への対応に関する検討会 AI ワーキンググループ；以下簡稱人工智慧小組），並於同年 7 月發布「消費者因應數位化

[33] Leenes et al., *supra* note 30, at 35; Matthew Gaske, *Regulation Priorities for Artificial Intelligence Foundation Models*, 6 VAND. J. ENT. & TECH. L. 1, 32 (2023).
[34] 郭戎晉，前揭文，註 2，頁 229。
[35] Organisation for Economic Cooperation and Development, Consumer Policy and Digital Technologies, https://www.oecd.org/en/topics/sub-issues/consumer-policy-and-digital-technologies.html (last visited Sept. 25, 2024).

檢討會之人工智慧小組報告書」(消費者のデジタル化への対応に関する検討会 AI ワーキンググループ報告書),報告書提出了當前人工智慧技術發展與實務應用衍生的三大消費者保護議題:

1、人工智慧與消費者安全相關議題

消費者廳指出當人工智慧商品或服務對消費者造成損害,諸如自駕車等如搭載人工智慧的商品導致消費者財物毀損,此時消費者可得依據日本「產品責任法」或日本「民法」向商品銷售商或製造商等提出損害賠償請求[36]。

若消費者選擇基於日本「產品責任法」提出請求,爭議焦點將在於該等商品是否具備「通常應有之安全性」;而在根據日本「民法」提出請求之情況下,討論重心將在於系爭商品銷售商或製造商是否確實存在違反契約或侵權行為[37]。

儘管上述法律制度主要涉及消費者安全受有損害時之「事後救濟」。然而為防止損害發生,並使消費者安全地使用商品,實有必要使消費者可得於使用產品時,知悉其應採取何等措施,以及透過詳細閱讀商品使用說明書等方式,確認與認知商品實際運作可能產生之風險[38]。

2、人工智慧與消費者自主決策相關議題

人工智慧可影響消費者的自主決策,諸如人工智慧向消費者推薦不符合其需求的商品並因而簽訂契約,以及在未確實了解商品風險之前提

[36] 消費者のデジタル化への対応に関する検討会 AI ワーキンググループ,消費者のデジタル化への対応に関する検討会 AI ワーキンググループ報告書,頁 9,2021 年 7 月。
[37] 同前註。
[38] 同前註。

下，根據聊天機器人的提案而簽訂契約，前述情形均表明人工智慧所為推薦在一定程度介入了消費者的決策過程。若消費者簽訂與其意圖不符的買賣契約，消費者可得考慮依據日本「消費者契約法」第 4 條或日本「民法」第 95 條規定，基於意思表示錯誤取消契約。惟消費者主張是否成立，仍視其是否滿足相關法律規定之要件[39]。

為了防止上述風險，消費者實有必要認識到人類存在對於電腦等自動化判斷過於信任之認知傾向，亦即存在所謂的「自動化偏見」，並應意識人工智慧所推薦的商品，並無法提供與如同真人面對面銷售之詳細資訊與解釋說明，從而消費者實有必要更加主動地進行資訊蒐集[40]。

3、人工智慧與消費者隱私保護相關議題

人工智慧亦存在不當蒐集及利用消費者隱私資料之風險，諸如智慧音箱可能蒐集過多的消費者個人資料，並可能超出特定目的利用所蒐集之個人資料，向第三方事業發送消費者對話內容等，此時可能產生違反日本「個人資料保護法」之疑慮。從而在實務運作上，實有必要加強消費者對於人工智慧產品所涉及的資料蒐集與利用上之安全措施的理解[41]。

除上述三大議題外，消費者廳人工智慧小組於研訂報告書過程中，亦曾指出梳理人工智慧所涉「法律責任」的重要性，並指出三項觀察重點：1、現階段人工智慧已展現高度的自主性，並開始融入成為商品與服務之一部分，惟責任主體並不會因為人工智慧而有所改變；析言之，當前人工

[39] 消費者のデジタル化への対応に関する検討会 AI ワーキンググループ，消費者のデジタル化への対応に関する検討会 AI ワーキンググループ報告書，頁 9，2021 年 7 月。
[40] 同前註。
[41] 同前註，頁 10。

智慧並不被視為「人」，亦不具「法人格」。2、由於資通訊技術發展與商業模式日益複雜，導致事故原因的查明變得愈發困難；析言之，包括人工智慧在內、根據於資通訊技術所提供的服務易於出現舉證困難問題。3、人工智慧所具備的特徵，對於可預見性、違約、缺陷等法律概念之適用與邊界，產生劇烈衝擊，從而產生有無必要擴大嚴格責任之討論[42]。

[42] 落合孝文，AI に関連する消費者被害の対応について，消費者のデジタル化への対応に関する検討会 AI ワーキンググループ（第 4 回）会議資料，頁 2，2020 年 5 月。

參、目標國家關聯法制規範分析

一、國際人工智慧監管思維變化

(一)、以自律機制為主的早期討論情形

人工智慧的早期治理討論，主要聚焦於「自律機制」。具代表的討論如 2014 年日本人工智慧學會（人工知能学会）設置了「人工智慧倫理委員會」並發表「人工智慧倫理指引」（人工知能学会倫理指針）[43]，國際電機電子工程師學會（Institute of Electrical and Electronics Engineers, IEEE）也於 2016 年提出了「人工智慧倫理設計準則」（Ethically Aligned Design）[44]，相關組織均強調希望透過具彈性的自律方式，使得人工智慧的技術發展及實務應用獲得適當之約束。

(二)、由自律轉向他律之近期發展趨勢

2018 年輪值七大工業國組織（Group of Seven, G7）主席的加拿大[45]，有鑑於人工智慧適度規範的重要性，開始倡議人工智慧之全球監管合作。2019 年 5 月加拿大「創新、科學與經濟發展部」（Innovation, Science and Economic Development Canada, ISED）建議仿照「政府間氣候變化專門委員會」（Intergovernmental Panel on Climate Change, IPCC），成立「人工智

[43] 人工知能学会倫理委員会，「人工知能学会倫理指針」について，https://www8.cao.go.jp/cstp/tyousakai/humanai/1kai/siryo3-4.pdf（最後瀏覽日：2024 年 8 月 15 日）。

[44] Institute of Electrical and Electronics Engineers, Ethically Aligned Design First Edition, https://standards.ieee.org/wp-content/uploads/import/ documents/other/ead_v1.pdf (last visited Aug. 15, 2024).

[45] 除加拿大，G7 成員還包括美國、德國、英國、法國、日本與義大利。

慧專門委員會」（Intergovernmental Panel on Climate Change, IPCC），並同時發布「國際人工智慧小組宣言」（Declaration of the IPAI），揭櫫參與國家所應承諾及遵循的十款共同價值[46]。

ISED 提出的十款共同價值，包括了：1. 以人權為基礎，促進以人為本與道德方法應對人工智慧；2. 支持以多方利害關係人方法應對人工智慧；3. 藉由人工智慧刺激創新、成長與福祉；4. 使人工智慧得與永續發展目標相互結合；5. 藉由人工智慧強化多樣性與包容性；6. 促進人工智慧系統的透明度與開放性；7. 促進對人工智慧的信賴與問責機制；8. 促進與保護民主價值觀念、程序與制度；9. 消弭數位落差；10. 促進人工智慧領域之國際科學合作[47]。

在 ISED 進行上述倡議的同時，經濟合作與發展組織（OECD）亦著眼人工智慧監管問題，於 2019 年 5 月發布「人工智慧建議書」（Recommendation of the Council on Artificial Intelligence）[48]。OECD 並於建議書中提出了五款「可信賴人工智慧之負責任管理原則」（Principles for responsible stewardship of trustworthy AI），包括：1、包容性成長、永續發展與福祉；2、以人為本的價值觀和公平；3、透明度及可解釋性；4、穩健與安全；以及 5、問責機制[49]。

隨著主要國家幾無例外地共通重視人工智慧帶來的挑戰，ISED 倡議成立的人工智慧專門委員會於 2020 年 6 月更名為「人工智慧全球夥伴聯盟」（Global Partnership on Artificial Intelligence, GPAI），並與 OECD 所作

[46] Innovation, Science and Economic Development Canada, Declaration of the International Panel on Artificial Intelligence, at https://www.canada.ca/ en/innovation-science-economic-development/news/2019/05/declaration-of-the -international-panel-on-artificial-intelligence.html (last visited Aug. 15, 2024).
[47] *Id.*
[48] Organisation for Economic Cooperation and Development (OECD), Recommendation of the Council on Artificial Intelligence, at https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449 (last visited Aug. 15, 2024).
[49] *Id.*

討論整合，正式架構於 OECD 之下[50]。截至 2024 年 8 月，全球共有 28 個國家及歐盟加入 GPAI[51]。

觀察此一發展與討論過程，可以發現無論是人工智慧專門委員會闡述的共同價值抑或 OECD 所提出之負責任管理原則，國際上針對人工智慧的治理討論，已由早期初相對寬泛且上位的倫理與道德層面，逐步聚焦於愈發明確之議題，進而帶動了國際組織與主要國家思考應否透過立法方式，更富效率地規範人工智慧的技術發展與實務應用。

二、制定人工智慧專法模式：歐盟

(一)、人工智慧法制推動現況

1、歐盟人工智慧監管專法：人工智慧法推動經緯

歐盟執委會在 2018 年發布「歐洲人工智慧政策報告」（Artificial Intelligence for Europe）[52]，並於報告中揭示歐洲人工智慧的三大發展願景，包括：1、增加針對人工智慧的公私部門投資；2、著眼社會發展預先作好準備；以及 3、確保適當的道德與法律架構（Ensure an appropriate ethical and legal framework）[53]，強調了「適當法律架構」的重要性暨執委會擬著手推動之事項[54]。

---

[50] Government of India, GPAI members come to a consensus about the future vision of GPAI; To pave way for renewed integrated partnership for harnessing the potential of AI for Good and for All, https://pib.gov.in/PressReleasePage.aspx?PRID=2030534 (last visited Aug. 15, 2024).

[51] 完整名單可參見：Global Partnership on Artificial Intelligence, Members, https://gpai.ai/community/（最後瀏覽日：2024 年 8 月 15 日）。

[52] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, COM (2018) 237 final.

[53] *Id.* at 3.

[54] *Id.* at 13-16.

為有效落實上述願景，歐盟執委會成立了「人工智慧高級專家小組」（The High-Level Expert Group on Artificial Intelligence, AI HLEG）並在 2019 年 6 月發布「可信賴人工智慧政策及投資建議書」（Policy and Investment Recommendations for Trustworthy Artificial Intelligence），針對人工智慧法律規範的建構，建議書提出了「風險管制基準」（risk-based approach）概念，認為歐盟針對人工智慧監管的推動，包括監管介入的時機與監管力道等，應取決於人工智慧系統所產生的風險類型；歐盟並應根據基於比例與預防原則等方法，具體區分風險級別[55]。

可信賴人工智慧政策及投資建議書發布以降，風險管制基準也成為歐盟在人工智慧監管法律規範設計上之核心原則。在充分考量上述人工智慧高級專家小組建言並整合各界回饋意見之下，歐盟執委會於 2020 年 2 月發布「人工智慧白皮書」（White Paper On Artificial Intelligence: A European Approach to Excellence and Trust）[56]，並正式表明歐盟將採取風險管制基準，作為人工智慧監管之核心精神，並基此制定人工智慧監管專法[57]。

經過廣泛討論，歐盟執委會在 2021 年 4 月公布「AIA 草案」[58]，期藉由制定全球首部人工智慧全面性監管專法，使歐洲成為其所揭示的「值得信賴的人工智慧之全球樞紐」（The Global Hub for Trustworthy Artificial Intelligence）此一重要目標[59]。惟 AIA 草案提出後旋即落入漫長的討論過程，繼 2023 年 6 月 14 日歐洲議會（European Parliament）通過其談判立

[55] High-Level Expert Group on AI, Policy and Investment Recommendations for Trustworthy Artificial Intelligence (2019), at 37-38.
[56] White Paper on Artificial Intelligence: A European Approach to Excellence and Trust, COM (2020) 65 final.
[57] *Id.* at 17.
[58] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM (2021) 206 final.
[59] European Commission, Europe Fit for the Digital Age: Commission Proposes New Rules and Actions for Excellence and Trust in Artificial Intelligence, European Commission (Apr. 21, 2021), https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682 (last visited Aug. 15, 2024).

場版本，歐洲議會與歐盟理事會（Council of the European Union）並於 2023 年 12 月 9 日針對 AIA 草案內容達成臨時協議（provisional agreement）[60]。

歐盟執委會根據臨時協議要求，持續修正 AIA 草案細節並由輪值主席國將其最終版本提交予所有成員國代表批准。歐洲議會與歐盟理事會於 2024 年 3 月 13 日及 5 月 21 日正式投票通過 AIA，全文並於同年 7 月 12 日於歐盟公報發布[61]，於公布後 20 日（同年 8 月 1 日）正式生效。

(二)、重要人工智慧立法分析：歐盟人工智慧法

1、設定四個風險等級並基此提出相應之監管要求

歐盟甚早便確立基於「風險管制基準」立場研訂 AIA 草案，並根據人工智慧實務應用可能衍生的風險，設計不同風險級別的人工智慧系統所應受到之規範。自 AIA 草案提出以降至最終正式獲得通過，歐盟將 AIA 所界定的人工智慧系統風險，持續界定為下述四個風險等級：

(1)、無法接受的風險（unacceptable risk）；

(2)、高度風險（high risk）；

(3)、有限風險（limited risk）；

(4)、最小風險（minimal risk）或無風險（no risk）。

[60] Council of the European Union, Artificial Intelligence Act: Council and Parliament Strike a Deal on the First Rules for AI in the World, Council of the European Union (Dec. 9, 2023), https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/ artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/ (last visited Aug. 15, 2024).

[61] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 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) Text with EEA relevance, OJ L, 2024/1689, 12.7.2024.

除設定與區分風險級別，AIA 同時根據風險級別的高低，設定其相應之規範密度。若人工智慧系統經判定屬於「無法接受風險」，除符合 AIA 所臚列的例外條件，將完全禁止此等人工智慧系統之實務應用。若被認定為「高度風險」，該等人工智慧系統於實際應用（進入市場）前，必須遵循嚴格的規範，包括執行風險評估與採取風險降低措施、提供人工智慧系統高品質之資料集以減少歧視性結果發生、留存活動紀錄以確保人工智慧系統設計過程得以追溯，並提供清楚且足夠之資訊予使用者等[62]。

若人工智慧系統被判定為「有限風險」，其應遵循並符合最低限度透明度之要求，以利使用者作出明智決策，同時在實際應用後，使用者亦可得決定是否繼續使用。若人工智慧系統屬於最後之「最小風險」等級，因不存在風險或僅對民眾造成極小之風險，歐盟將不會對此類系統進行干預[63]。

2、「無法接受之風險」級別之人工智慧系統所受規範

歐盟 AIA 明訂「無法接受之風險」之人工智慧系統應予禁止，而為確定哪些人工智慧系統落入此一級別從而受到禁止，歐盟 AIA 明訂了「無法接受之風險」之人工智慧系統具體態樣：

(1)、於市場展示、出於特定目的提供服務或使用之人工智慧系統，該系統採用超出個人意識之潛意識技術，或有目的之操縱或欺騙性技術，其目的或效果係嚴重扭曲個人或群體之行為，明顯損害該人做出明智決定之能力，從而導致該人做出其原先不會作成之決定，導致或極可能導致該人、其他人或群體受到重大傷害。

[62] 郭戎晉，前揭文，註 27，頁 132-133。
[63] 同前註，頁 133。

(2)、於市場展示、出於特定目的提供服務或使用之人工智慧系統，該系統利用特定自然人或群體肇因其年齡、殘疾或特定社會或經濟狀況所存在之任何弱點，其目的或效果係嚴重扭曲該人或隸屬該群體之人之行為，導致或極可能導致該人或其他人受到重大傷害。

(3)、於市場展示、出於特定目的提供服務或使用之人工智慧系統，根據自然人或其所屬群體之社會行為，或已知或預測之個人或人格特徵，在一定時期內對自然人或其群體進行社會分數評估或分類。基此所產生之社會分數導致下述其一或兩款情形：

(i)、在與最初產製或蒐集資料之目的無關的社會背景下，對特定自然人或整個群體造成不利或負面之對待；

(ii)、對特定自然人或整個群體之差別對待，導致其社會行為或社會地位受到不公平或不合比例之影響。

(4)、於市場展示、出於特定目的提供服務或使用之人工智慧系統，針對自然人進行風險分析，僅根據針對自然人所作分析或評量其人格特質與特徵，藉以評估該自然人從事刑事犯罪之風險。本款規定並不適用於支持針對特定人是否參與犯罪活動進行人類評估之人工智慧系統，而該等評估係基於與犯罪活動直接相關之客觀且可資驗證之事實。

(5)、於市場展示、出於特定目的提供服務或使用之人工智慧系統，透過網際網路或監視器錄影畫面，無針對性地獲取人臉畫面，藉以創建或擴展人臉識別資料庫。

(6)、於市場展示、出於特定目的提供服務或使用之人工智慧系統，係應用於工作場所與教育機構等領域，藉以推斷自然人之情緒反應。但出於醫療或安全事由從而擬於市場展示或已於市場實際使用之有關人工智慧系統，不在此限。

(7)、於市場展示、出於特定目的提供服務或使用之生物識別分類系統，根據生物識別資料針對自然人進行分類，藉以推斷或斷定其種族、政治觀點、工會成員身分、宗教或哲學信仰、性生活或性取向。本款規定不包括針對合法取得的生物識別資料集所進行之標記或過濾，諸如基於生物識別資料之影像或執法領域之生物識別資料分類

(8)、出於執法目的於公共場所使用「即時性」遠端生物特徵識別系統，但出於下述目的之一且絕對必要者，不在此限：

(i)、針對性地尋找綁架、人口販運或性剝削之特定受害者，以及尋找失蹤者；

(ii)、防止對自然人之生命或人身安全造成具體、重大與急迫之威脅，或防止真實存在或當前可預見之恐怖攻擊威脅。

(iii)、對應附件二所臚列之犯罪行為進行刑事調查、起訴或執行刑事處罰，且有關犯罪行為在相關成員國可被判處不少於四年之監禁或拘留令，針對犯罪嫌疑人進行定位或身分識別[64]。

3、「高風險」級別之人工智慧系統所受規範

除完全禁止的不可接受風險人工智慧系統，高風險人工智慧系統無疑地是歐盟 AIA 規範重心。歐盟 AIA 明訂於符合下述兩項要件時，人工智慧系統將被視為高度風險系統：

(1)、該人工智慧系統擬作為產品的安全元件（safety component）加以使用，或人工智慧系統本身即屬於受附件一所臚列之歐盟立法所規範之產品；

[64] 歐盟 AIA 第 5 條第 1 項。

(2)、根據第(1)款規定人工智慧系統係產品之安全元件，或人工智慧系統本身即作為一項產品，被要求接受第三方合格評估，以利根據附件一所臚列之歐盟立法，使產品進入市場或提供使用[65]。

基於上述規定，當人工智慧系統作為產品之安全元件或人工智慧系統本身即屬於產品，同時受到 AIA 附件所表列的歐盟產品相關立法之規範，該等產品在市場銷售或提供使用前，必須通過由第三方進行之合格評估，即屬於所謂的高度風險級別之人工智慧系統。

除根據上述基本原則從而界定的高度風險人工智慧系統，歐盟 AIA 另規定該法附件三所臚列之人工智慧系統，亦應當視為高度風險人工智慧系統[66]。若進一步觀察 AIA 附件三內容，其提出下述八項關鍵應用領域，從而相關領域下之特定人工智慧系統，將被視為高度風險人工智慧系統：

(1)、生物辨識，受歐盟或成員國立法允許使用；

(2)、關鍵基礎設施；

(3)、教育與職業培訓；

(4)、就業、員工管理與自僱職業；

(5)、獲得及享受基本的私人與公共服務及福祉；

(6)、執法部門，受歐盟或成員國立法允許使用；

(7)、移民、難民庇護與邊境管制，受歐盟或成員國立法允許使用；

(8)、司法執法與民主推動之用。

無論是基於歐盟 AIA 第 6 條第 1 項抑或同條第 2 項規定，當人工智慧系統被判定為高風險級別時，歐盟 AIA 要求此等高度風險人工智慧系統，應恪遵針對此一風險級別所制定的專門規範，並應慮及其預期目的以及人工智慧暨其關聯技術受到公認之技術水平。

[65] 歐盟 AIA 第 6 條第 1 項。
[66] 歐盟 AIA 第 6 條第 2 項。

高度風險人工智慧系統所受到的具體要求，主要包括：

(1)、應建立風險管理系統[67]；

(2)、應建立資料運用暨資料治理規範[68]；

(3)、編撰必要之「技術文件」並保持最新狀態[69]；

(4)、應落實記錄留存[70]；

(5)、確保透明度與資訊提供[71]；

(6)、進行人類監督[72]；

(7)、確保正確性、穩定性與網路安全[73]。

4、「有限風險」與「最小風險/無風險」級別之人工智慧系統所受規範

除了禁止使用的「不可接受風險」人工智慧系統，以及受到嚴格規範的「高風險」人工智慧系統，針對兩者以外的風險等級，包括「有限風險」與「最小風險/無風險」之人工智慧系統，考量其風險性相對輕微，歐盟 AIA 要求依該法所成立的「歐盟人工智慧辦公室」（AI Office）以及各該歐盟成員國家，應當鼓勵與促進制定「行為守則」（codes of conduct），使高度風險以外的其他風險等級之人工智慧系統，可得自願應用並遵循歐盟 AIA 第三篇第二章之有關規範[74]。

對此，歐盟 AIA 明訂人工智慧辦公室與歐盟成員國應當制定可對應所有人工智慧系統的具體要求之自願性行為準則，並以明確的目標與「關

[67] 歐盟 AIA 第 9 條。
[68] 歐盟 AIA 第 10 條。
[69] 歐盟 AIA 第 11 條。
[70] 歐盟 AIA 第 12 條。
[71] 歐盟 AIA 第 13 條。
[72] 歐盟 AIA 第 14 條。
[73] 歐盟 AIA 第 15 條。
[74] 歐盟 AIA 第 95 條。

鍵績效指標」（Key Performance Indicators, KPI）作為基礎，以利監管機關衡量有關目標之具體實現情形。

為助益行為守則之訂定，歐盟 AIA 同時例示了行為準則之可能內容，包括：

(1)、歐盟可信任人工智慧道德準則（Ethics Guidelines for Trustworthy AI）所規定之適用要件；

(2)、評估並盡量減少人工智慧系統對環境永續（environmental sustainability）之所生影響，包括節能編程（programming）與有效設計、訓練與使用人工智慧之技術；

(3)、提升人工智慧素養，特別是從事人工智慧開發、操作與使用人員的素養之提升；

(4)、促進人工智慧系統的包容性與多元化設計，包括透過建立包容性與多元化的開發團隊，並促進利害關係人參與此一過程；

(5)、評估並防止人工智慧系統對弱勢族群或弱勢族群所屬團體產生的負面影響，包括身心障礙者之無障礙環境以及性別平等。

5、歐盟 AIA 之後續實施時程

廣受全球注目的歐盟 AIA，其全文在 2024 年 7 月 12 日正式於歐盟公報發布，並依規定於同年 8 月 1 日生效。惟歐盟 AIA 並非於 2024 年 8 月 1 日即全面實施，而是採取分階段施行作法。

其重要施行時程如下：

(1)、生效後 6 個月（2025 年 2 月 2 日）：正式禁止「無法接受之風險」之人工智慧系統。

(2)、生效後 9 個月（2025 年 5 月 2 日）：確定通用人工智慧之實務操作行為準則。

(3)、生效後 12 個月（2025 年 8 月 2 日）：

A、實施通用人工智慧之治理規則；

B、成員國確定其主管機關；

C、執委會進行年度審查並評估是否修正禁止項目。

(4)、生效後 18 個月（2026 年 2 月 2 日）：委員會發布實施法，針對高風險人工智慧提供者提出上市後監控計畫範本。

(5)、生效後 24 個月（2026 年 8 月 2 日）：

A、實施附件三臚列之高風險人工智慧系統之所負義務；

B、成員國實施罰則；

C、成員國主管機關建立人工智慧監理沙盒；

D、執委會進行審查並評估應否修正高風險人工智慧系統清單。

(6)、生效後 36 個月（2027 年 8 月 2 日）：實施附件二臚列之高風險人工智慧系統之所負義務。

(三)、重要人工智慧立法分析：歐盟人工智慧責任指令草案

1、人工智慧責任指令草案之提出

歐盟執委會在前揭 2020 年提出的「人工智慧白皮書」中，除承諾促進人工智慧的實務應用，並表明實有必要基於「以人為中心」（human-centric）的策略方法，解決人工智慧應用衍生之相關風險[75]；而執委會同年度發布的「人工智慧責任報告」（Report on Artificial Intelligence Liability），

[75] White Paper on Artificial Intelligence: A European Approach to Excellence and Trust, COM (2020) 65 final, at 3.

則進一步強調了人工智慧對於歐盟現有責任規範體系所帶來之具體挑戰[76]。

歐洲議會於 2020 年 10 月根據 歐盟運作條約（Treaty on the Functioning of the European Union, TFEU）第 225 條規定，通過著眼人工智慧民事責任之立法倡議決議（legislative own-initiative resolution），要求歐盟執委會應針對人工智慧衍生的民事責任之處理，提出具體之立法建議[77]。

為實現前揭白皮書揭櫫目標並具體回應歐洲議會之立法要求，歐盟執委會於 2022 年 9 月 28 日正式提出「人工智慧責任指令草案」（Artificial Intelligence Liability Directive；以下簡稱 AILD 草案），針對人工智慧系統所生損害所涉及的「非契約民事責任」（non-contractual civil liability）建立統一規範，以期有效解決了人工智慧爭端救濟上所面臨的舉證困難問題，並確保合理的主張不致受到阻礙[78]。

2、草案係適用於「非契約」情況下之賠償請求

歐盟強調 AILD 草案的制定宗旨，在於解決「非契約民事責任」，其總體目標係促進足資信賴的人工智慧之推廣，確保人工智慧系統所生損害的受害者，可獲得與一般商品所生損害的受害者相同之保護。

依歐盟 AILD 草案第 1 條第 1 項規定「本指令明訂下述之一般規則：(a)、揭露高風險人工智慧系統之證據，俾利請求權人可得證明存在基於

[76] REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final.

[77] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)), OJ C 404, 6.10.2021

[78] European Commission, Liability Rules for Artificial Intelligence, https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en (last visited Aug. 15, 2024).

非契約過失之民事損害賠償請求權；(b)、針對人工智慧系統所造成的損害，向各國法院提起的非契約過失民事損害賠償請求案件中之舉證責任分配」。此外，AILD 草案第 1 條第 2 項另規定「本指令適用於非契約過失之民事損害賠償請求，亦即人工智慧系統所造成的損害，係發生於『轉換期間結束之後』（the end of the transposition period）[79]。同時本指令並不適用於刑事責任之追究」。

3、建立對應人工智慧特徵的「因果關係推定」機制

歐盟 AILD 草案宗旨之一在於確保遭受人工智慧系統侵害之人，可得享受與受到其他技術侵害之人相同的保護水平。考量人工智慧技術的複雜性與不透明等情形，歐盟 AILD 草案將創建一套可舉反證推翻的「因果關係推定」機制，藉以減輕受害者針對人工智慧系統所造成的損害之舉證責任[80]。

在 AILD 草案提出前，歐盟現行的責任規範架構包括了「產品責任指令」（Product Liability Directive, PLD）以及與之並行適用的歐盟成員國內國責任規定。前者係針對肇因產品缺陷所導致的損害賠償請求，實施「無過失責任（嚴格責任）」制度，PLD 廣泛適用於各類產品，要求製造商針對存有缺失的產品之所生損害承擔責任，而受害者則必須可得證明缺陷、損害與兩者之間的因果關係。在成員國內國責任規範部分，則包括了基於行為（亦即「過失責任」）或與過失無關（亦即「嚴格責任」）進行賠償請求兩者。針對過失責任，受害者必須證明損害、過失和兩者之間的因果關

[79] 依歐盟運作條約（Treaty on the Functioning of the European Union, TFEU）第 288 條第 3 項規定「指令具約束力，以使每一成員國達致所訂立目標，但成員國當局可選擇其形式和方法」（A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods.）。儘管指令依歐盟運作條約屬於具拘束力的強行法，惟基於該項後段規定，必須經過成員國的「立法轉換」，從而產生「轉換期間」之概念。

[80] Madiega, *supra* note 1, at 1.

係；而在嚴格責任之下，受害者只消證明應承擔責任之人所造成的風險即可，而無需積極證明過失[81]。

歐盟 AILD 草案係於現有的 PLD 規範之外，針對國家基於過失的責任制度進行目的性改革，使之可得適用於任何自然人或法人針對人工智慧系統所生損害的過失，對任何人所提出之賠償請求[82]。

考量人工智慧所具備的相關特性，使得人工智慧系統所涉及的民事賠償請求之因果關係判斷與舉證責任分配等，難以全然套用現有機制，而過高的舉證成本或將使得受害者斷然放棄賠償請求，基此，歐盟 AILD 草案提出了「因果關係推定」機制，為基於人工智慧系統所生損害進行賠償請求之人，提供更合理的舉證責任與成功請求賠償之機會。

(2)、推定存在因果關係之基本條件

歐盟 AILD 草案第 4 條規定可舉反證推翻（rebuttable）的因果關係推定機制，此一機制顧名思義，即在於滿足草案所規定的相關條件時，將推定人工智慧系統的應用行為與損害結果之間存在著因果關係：

依歐盟 AILD 草案第 4 條第 1 項規定，在滿足該項所列所有條件之下，法院應推定被告的過失與人工智慧系統的輸出或應輸出而未輸出之間，兩者存在著因果關係，並據此選擇損害賠償請求所應適用之責任原則：

(a)、請求權人業已證明或法院已根據本指令第 3 條第 5 項規定，推定被告或可歸責於被告的主體存在過失，包括違反歐盟法律或歐盟成員國法律所規定、其直接目的在於防止發生損害之注意義務規定；

[81] Madiega, *supra* note 1, at 2.
[82] Madiega, *supra* note 1, at 5.

(b)、根據案例事實，可得合理地認為其過失影響了人工智慧系統的輸出或導致人工智慧系統未能輸出；

(c)、請求權人業已證明，人工智慧系統的輸出或未能輸出，導致了損害之發生。

(3)、高風險人工智慧系統之適用

當損害賠償請求係針對歐盟 AIA 所規定的「高風險人工智慧系統」之提供者，或針對歐盟 AIA 所規定、應承擔前述提供者所負義務之主體提出時，僅請求權人可資證明提供者或承擔提供者所負義務之主體未能遵守下述要求之一，且併同考量歐盟 AIA 所規定的風險管理系統之步驟與結果後，甫推定存在因果關係：

(a)、系爭人工智慧系統利用資料模型進行訓練，但未基於符合歐盟 AIA 所規定品質標準的資料集進行訓練、驗證與測試後加以開發；

(b)、人工智慧系統的設計與開發方式並未符合歐盟 AIA 所規定的透明度要求；

(c)、人工智慧系統的設計與開發方式，並不允許自然人根據歐盟 AIA 規定在使用期間內針對人工智慧系統進行有效監督；

(d)、人工智慧系統並未實現其預定的設計與開發目的，並未符合歐盟 AIA 所規定的適當精準度、穩定性與網路安全水平；

(e)、未立即採取必要補救措施，使人工智慧系統符合歐盟 AIA 第三篇第 2 章規定之義務，或根據歐盟 AIA 相關規定審酌情況撤回或召回系爭人工智慧系統[83]。

[83] 歐盟 AILD 草案第 4 條第 2 項。

此外，針對高風險人工智慧系統所提出之損害賠償請求，歐盟 AILD 草案規定若請求權人可得證明用戶符合下述條件之一時，該當上述第 1 項第(a)款規定：

(a)、未履行其根據附隨之使用說明書約定使用或監控人工智慧系統，或於適當情況下根據歐盟 AIA 暫停或中斷其使用之義務；

(b)、將其控制下的人工智慧系統應用於輸入與該系統的預期用途無關之資料[84]。

(4)、成員國有利於消費者之保護規定仍有其適用

值得留意者，歐盟 AILD 草案依循歷來歐盟立法上普遍採納的「最低限度協調機制」（minimum harmonisation approach），允許索賠人在人工智慧系統造成損害的情況下，援引對其更為有利的內國法律規則[85]。基此，歐盟成員國內國立法可得保留根據國家過失責任制度之舉證責任倒置（reversals of the burden of proof）之規定，或保留適用於人工智慧系統造成損害之「無過失責任」（no-fault liability）制度規定[86]。

(四)、重要人工智慧立法分析：歐盟產品責任指令修正草案

1、PLD 適用於人工智慧之潛藏問題

[84] 歐盟 AILD 草案第 4 條第 3 項。

[85] AILD 的提案法律依據係 TFEU 第 114 條，該條規定採取措施藉以確保內部市場之建立與運作。選擇指令形式為歐盟成員國內部立法轉換提供了一定的彈性，蓋若採取直接適用的「規則」形式，針對侵權責任的範疇規範恐過於嚴格，且侵權責任的範疇設定，多係基於各個成員國特定且長期發展所建立的傳統狀態。

[86] Madiega, *supra* note 1, at 8.

歐盟執委會在 2018 年提出的「產品責任指令評估報告」[87]，具體 PLD 在應對新興數位技術，特別是人工智慧的不足之處。首先，執委會發現特定無形元素（intangible elements），包括數位內容、軟體與數據等，對眾多新興產品的有效運作至關重要，但這些無形元素可否被視為 PLD 所稱之產品，事實上未臻明確，導致肇因於軟體（包括其更新）所引起的損害如何進行賠償以及責任歸屬等，易於出現法律適用上的不確定性。其次，新興技術往往帶來全新的風險，諸如影響系統安全或網路安全風險等，然而 PLD 僅針對「物理或物質損害」（physical or material damage）進行賠償。第三、人工智慧本身的特性，如不透明/缺乏透明度、可解釋性、自主行為（autonomous behaviour）、持續適應（continuous adaptation）與有限的可預測性等，亦使得因果關係的存在判斷與舉證責任判斷等問題變得愈發困難，並可能導致成員國法院處理人工智慧造成的損害時，採取不同的做法，進而引發法律之碎片化（legal fragmentation）[88]。

歐盟執委會指出為因應數位時代帶來的挑戰，近期歐盟針對現行 PLD 規定進行審視並倡議必要修正，以期該法可得適用於數位環境，並在與時俱進的同時，確保其技術中立本質（technology-neutral nature）與適用範疇[89]。

2、PLD 之修正與人工智慧

[87] Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC), COM(2018) 246 final.

[88] Madiega, *supra* note 1, at 3-4.

[89] Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC), COM(2018) 246 final, at 34.

歐盟在 2022 年 9 月提出 PLD 修正提案[90]，其主要宗旨係著眼製造商針對缺陷產品的嚴格責任規則，進行必要修正，確保過往存在適用爭議的產品，包括數位商品與整新商品（refurbished products）等，受害者於此類商品對其造成損害時仍可獲得公平之賠償。此外，修正後的 PLD 亦可望助益人工智慧商品所生損害之受害者，向製造商提出更為有效之賠償請求。基此，PLD 將適度調整有關製造商針對缺陷商品之嚴格責任機制，允許在無需證明過失之情況下賠償消費者所受損害[91]。

歐盟理事會於 2024 年 10 月 10 日正式通過 PLD 之修正，新法命名為歐盟「缺陷產品責任指令」（Directive on Liability for Defective Products）[92]，成員國必須於「缺陷產品責任指令」在官方公報正式公布後兩年內將其轉化為內國法律。而在「缺陷產品責任指令」及各成員國轉化的內國法正式生效前，人工智慧商品（服務）仍將受到原有 PLD 之規範，之後將為新法所取代[93]。

在歐盟 AIA 正式底定後，歐盟除持續強化針對人工智慧系統的監管，亦日益強調人工智慧系統實務應用衍生民事損害爭端之處理，AILD 草案及「缺陷產品責任指令」或將成為歐盟在人工智慧法制建構上之下一波討論重點。

三、未制定人工智慧專法模式：美國、日本及英國

(一)、美國

[90] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on liability for defective products, COM/2022/495 final.
[91] Madiega, *supra* note 1, at 3-4.
[92] Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC (Text with EEA relevance), O.J. (L, 2024/2853).
[93] Covington, What Can You Expect From the New Product Liability Directive?, COVINGTON (Oct. 11, 2024), https://www.cov.com/en/news-and-insights/insights/2024/10/what-can-you-expect-from-the-new-product-liability-directive (last visited Nov. 25, 2024).

1、美國人工智慧規範推動現況

(1)、以「部門立法」為主，白宮並發布聯邦推動立法時之共通基本原則

作為科技大國，歷來美國面對新興科技與嶄新數位應用帶來的治理難題，其應對思維往往呈現出濃厚的務實色彩，嘗試賦予產業自律遵循空間，在引領產業發展之際維持應有的秩序，必要時甫立法進行管制，並盡量以部門導向為優先選項[94]。

史丹佛大學「以人為本 AI 研究院」（Stanford Institute for Human-Centered Artificial Intelligence, Stanford HAI）曾分析 25 個國家立法機關在 2016 年至 2021 年之間實際通過的人工智慧關聯法案，發現美國以 13 部立法居全球首位[95]。惟當前美國並無「全面性監管專法」，已通過的人工智慧相關立法亦不以監管面向為限，還包括以促成產業應用為主之立法。

考量部門立法漸增，為確保各機關所制定的人工智慧立法不致造成不當影響，並避免出現疊床架屋情形，白宮亦針對聯邦機構推動人工智慧立法制定監管指南與立法共通基本原則。2019 年 2 月時任美國總統川普（Donald Trump）簽署「維持美國人工智慧領域領導地位行政命令」（Executive Order to Maintain American Leadership in Artificial Intelligence），要求針對人工智慧制定必要的監管指南[96]。

---

[94] 郭戎晉，前揭文，註 27，頁 134。

[95] Stanford Institute for Human-Centered Artificial Intelligence, Artificial Intelligence Index Report 2022 (2022), at 177-78.

[96] Executive Order on Maintaining American Leadership in Artificial Intelligence, 84 Fed. Reg. 3967 (Feb. 14, 2019), at 3970.

基此，白宮在 2020 年 11 月正式發布「人工智慧應用監管指南」（Guidance for Regulation of Artificial Intelligence Applications），提出美國聯邦機構在制定人工智慧應用立法時，應當納為考量的十項基本原則，包括：1、公眾信任；2、公眾參與；3、科學誠信與資訊品質；4、風險評估與管理；5、效益與成本；6、靈活性；7、公平與非歧視；8、公開與透明；9、安全保障；以及 10、機關間之相互協調等重要要求[97]。

近期美國各州人工智慧立法亦受到矚目，由於現時在聯邦層級尚無全面性的人工智慧立法，也促使各州開始思考有無必要自行擬議及推動必要的人工智慧監管立法。根據 David Stauss 及 Owen Davis 的研究，已有超過四分之一的州著手推動監管私部門的人工智慧立法，而可見的州立法中，其規範重心則包括了演算法歧視、自動化就業決策（Automated employment decision-making）及個人權利保障等[98]。值得留意的是 2024 年 5 月科羅拉多州通過了「人工智慧消費者保護法」（Consumer Protections for Artificial Intelligence Act），成為美國州法層級第一部全面性人工智慧監管立法。

(2)、同時運用「軟法機制」（產業管理標準）應對人工智慧衍生風險

美國秉持歷來面對科技應用監管議題所採取的務實立場，在跨越全然以自律為主的階段，著眼人工智慧的立法倡議已與日俱增，除必要部門立法推動討論外，也積極思考透過以「產業管理標準」為主的軟法機制之推動，助益公、私部門識別人工智慧系統風險並建立相應之內部管理機制。2019 年發布的「維持美國人工智慧領域領導地位行政命令」，即要求商務

[97] The White House, Guidance for Regulation of Artificial Intelligence Applications (2020), at 3-7.
[98] David Stauss & Owen Davis, A Look at Proposed US State Private Sector AI Legislation, IAPP (Feb. 28, 2024), https://iapp.org/news/a/a-look-at-proposed-u-s-state-private-sector-ai-legislation (last visited Aug. 25, 2024).

部長應自該命令發布之日起 180 天內，協同國家標準暨技術研究院（National Institute of Standards and Technology, NIST）首長公布聯邦政府參與人工智慧技術標準與相關工具開發的計畫，以支持可靠、強大及值得信賴的人工智慧系統[99]。

在經過廣泛討論後，NIST 在 2023 年 1 月正式發布「人工智慧風險管理框架」(Artificial Intelligence Risk Management Framework 1.0；AI RMF）[100]。AI RMF 旨在促進人工智慧的可信賴性，包括如何因應並解決人工智慧在設計、發展及使用過程中所產生的正確性、可解釋性及避免歧視等課題。

NIST 於 AI RMF 中指出此一標準文件之宗旨為「實用性」，不同規模及能力的組織均可按 AI RMF 推動其風險管理機制，俾利整體社會可得自人工智慧獲益，同時也免受其潛在危害。考量如何識別、減輕及最小化涉及人工智慧技術的風險與潛在危害，無疑是各界開發可信賴人工智慧系統及其負責任使用上的重要步驟。對此，AI RMF 在風險識別的基礎上建構人工智慧風險應有的治理架構與管理標準，並提出以治理（Govern）、路徑（Map）、量測（Measure）及管理（Manage）為核心之風險管理架構設計[101]。

2、與人工智慧消費者保護有關之規範作法

相較於歐盟制定全面性人工智慧監管專法，美國則是以部門立法為主，同時可見部門立法並不以監管為限。此外，美國亦強調軟法機制的重要性，並已實際制定人工智慧風險管理產業標準，使公、私部門及各個產

[99] Executive Order on Maintaining American Leadership in Artificial Intelligence, 84 Fed. Reg. 3967 (Feb. 14, 2019).
[100] NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0),
[101] 郭戎晉，前揭文，註 27，頁 172。

業別均可運用官方發布的 AI RFM，建立可持續運作的人工智慧衍生風險管理機制。近期美國政府持續就消費者保護在內的議題，針對人工智慧發布相關指導性文件，本計畫認為殊值國內重視者，包括「人工智慧權利法案藍圖」（Blueprint for an AI Bill of Rights）與「安全可靠且可資信賴之人工智慧行政命令」（Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence）兩者。

(1)、人工智慧權利法案藍圖

拜登政府於 2022 年 10 月發布的「人工智慧權利法案藍圖」，提出在設計、使用與部署自動化系統上的五項基本原則，包括：

A、建立安全有效的系統；

B、保護民眾免於演算法歧視；

C、維護資料隱私；

D、自動化系統運作之透明化；

E、保障退出權利[102]。

儘管「人工智慧權利法案藍圖」全文中並未見「消費者」一詞，但其所揭櫫的系統安全、免受歧視及隱私保護等，均是實際受到討論、人工智慧商品或服務可能衍生的消費者保護議題，如前揭日本消費者廳「消費者因應數位化檢討會之人工智慧小組報告書」即提出的消費者保護議題，即與此完全相同，從而人工智慧權利法案藍圖所揭示的建議作法與要求，仍具高度參考性。

(2)、安全可靠且可資信賴之人工智慧行政命令

[102] The White House, Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People (2022), at 5-7.

繼「人工智慧權利法案藍圖」，拜登政府另於 2023 年 10 月發布「安全可靠且可資信賴之人工智慧行政命令」，進一步提出八項行動目標，包括：

A、著眼人工智慧安全制定新標準；

B、保護美國公民隱私；

C、促進公平性與公民權利；

D、保障消費者、病患與學生；

E、支持勞工；

F、促進創新與競爭；

G、提升美國針對人工智慧的全球領導地位；

H、確保聯邦政府係負責任且有效地運用人工智慧[103]。

相較於前述「人工智慧權利法案藍圖」未提及任何「消費者」用語，「安全可靠且可資信賴之人工智慧行政命令」則明確強調消費者保護之重要性，其指出「在日常生活中越來越多地使用、互動或購買人工智慧與人工智慧產品的美國民眾，其利益必須獲得保障。使用人工智慧等嶄新技術時，並不能免除事業之法律義務，在技術變革的時刻，來之不易的『消費者保護』較以往任何時刻均更加重要。聯邦政府將執行現有的『消費者保護』法律與原則，並制定適當之保障措施，防止人工智慧帶來的詐欺、偏見、歧視、隱私侵害與其他危害」。「此類保護在醫療保健、金融服務、教育、住房、法律與交通等關鍵領域尤為重要，在前述領域人工智慧的錯誤或濫用可能導致病患的傷害，使消費者或小型企業付出代價，或危及安全或權利。與此同時，聯邦政府將促進負責任地使用人工智慧，以保護消費者，提高商品與服務的品質，降低價格，或擴大選擇與可用性」[104]。

[103] Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (2023).
[104] *Id*. at (e).

除上述兩項文件，美國消費者保護主要執法機關：聯邦交易委員會（Federal Trade Commission, FTC）近期亦強調實有必要強化針對人工智慧技術暨其實務應用之監管，資以確保消費者權益不受侵害，並維護市場競爭之公平性。諸如 FTC 於 2024 年 8 月 14 日通過最終規則（Final Rule），禁止運用人工智慧產製及發布虛假評論與薦證內容[105]。

此外，有鑑於運用人工智慧欺瞞消費者之情形急遽增加，FTC 亦於 2024 年 9 月宣布將推動「AI Comply」行動，鎖定利用人工智慧進行炒作之行為，以及銷售可用於遂行欺騙的人工智慧技術之行為，採取必要執法行動，避免消費者遭受損害[106]。

(二)、日本

1、日本人工智慧規範推動現況

(1)、確認以「軟法機制」滿足人工智慧治理需求

日本於 2018 年 5 月由內閣府成立「以人為中心之人工智慧社會原則研商會議」（人間中心の AI 社会原則会議），由產官學民等多方利益關係人共同探討並制定「以人為中心之人工智慧社會原則」，以期妥善地將人工智慧應用於日本社會。以人為中心之人工智慧社會原則定位為軟法

[105] Federal Trade Commission, Federal Trade Commission Announces Final Rule Banning Fake Reviews and Testimonials, FTC (Aug. 14, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/08/federal-trade-commission-announces-final-rule-banning-fake-reviews-testimonials (last visited Nov. 25, 2024).

[106] Federal Trade Commission, FTC Announces Crackdown on Deceptive AI Claims and Schemes, FTC (Sept. 25, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes (last visited Nov. 25, 2024).

（自律規範），針對人工智慧應用提出總體架構與相應之社會指導原則，其中針對人工智慧商品的開發者與提供者，揭櫫一系列著眼人工智慧商品開發所量身訂作之共通標準[107]。

面對全球人工智慧發展熱潮，日本政府採取發展與治理並重立場，除上述的「以人為中心之人工智慧社會原則」，內閣府另成立「人工智慧戰略研商會議」（AI 戰略会議），提出國家級人工智慧戰略文件。有鑑人工智慧技術發展與商業服務型態日新月異，日本政府認為短期內實難以實現全面性公部門監管，從而在人工智慧治理上側重採取「軟法機制」，透過行政指導或制定遵循指引進行規範，其優點為相較於硬法（監管專法），軟法工具可得快速地制定與修改，並且更加廣泛地獲得採用。

(2)、由關聯部會制定發布指引或進行行政指導

在確認以軟法機制為主之下，針對人工智慧實務應用衍生的爭議，由關聯部會透過發布指引或進行行政指導方式，確保人工智慧獲得適當規範。以日本經濟產業省與總務省於 2024 年 1 月共同制定「人工智慧事業遵循指引草案」（AI 事業者ガイドライン案）為例，除一體適用的總則規定，亦分別針對「AI 開發者」、「AI 提供者」及「AI 利用者」制定相應之遵循指引[108]。就本指引而言，其與消費者保護直接關聯內容，包括了：

(1)、為利識別、評估與減輕 AI 生命周期中的風險，必須在 AI 系統整個開發過程採取適當措施（安全性、透明性）；

[107] 日本「以人為中心之人工智慧社會原則」全文，可參見：https://www8.cao.go.jp/cstp/aigensoku.pdf (最後瀏覽日：2024 年 10 月 5 日)。

[108] 日本「人工智慧事業遵循指引草案」全文，可參見：https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20240119_1.pdf (最後瀏覽日：2024 年 10 月 5 日)。

(2)、進入市場後，應識別可能存在的弱點及可能遭到濫用的事件型態（安全性、可課責性）；

(3)、針對 AI 系統開發者，制定與實施根基於風險的 AI 治理暨風險管理方針，其中應包括個人資料保護政策（可課責性）；

(4) 、在技術可行之前提下，開發並導入內容認證與記錄機制，俾利使用者可得識別人工智慧所生成的內容（透明性）。

2、與人工智慧消費者保護有關之規範作法

日本政府在人工智慧治理推動值得關注的面向，係其消費者保護主管機關（消費者廳）甚早即關注人工智慧對消費者保護產生之影響並思索合適的因應作法。

面對數位經濟的快速發展及嶄新技術如人工智慧帶來之劇烈衝擊，日本消費者廳在 2020 年 1 月成立「消費者因應數位化檢討會之人工智慧小組」（消費者のデジタル化への対応に関する検討会 AI ワーキンググループ）[109]。

歷經多次會議討論與廣泛研商，上揭人工智慧小組在 2020 年 7 月發布「消費者因應數位化檢討會之人工智慧小組報告書」（消費者のデジタル化への対応に関する検討会 AI ワーキンググループ報告書），並同時公布「人工智慧活用手冊：巧妙運用人工智慧（AI 利活用ハンドブック：AI をかしこく使いこなすために），闡述人工智慧對於消費者帶來的效益，並提出因應人工智慧衍生風險之建議。

109

https://www.caa.go.jp/policies/policy/consumer_policy/meeting_materials/assets/review_meeting_004_200206_0001.pdf (last visited Nov. 15, 2024).

日本消費者廳近期持續針對人工智慧進行討論，除了在 2024 年 2 月完成及發布「有關人工智慧之第一回消費者意識調查結果報告」（第 1 回消費者意識調查結果（AI に対するイメージについて））[110]，另考量生成式人工智慧快速普及運用並已有紛爭漸生之勢，日本消費者廳繼 2020 年 7 月發布的「人工智慧活用手冊」，於 2024 年 3 月另行發布「人工智慧活用手冊：生成式人工智慧篇」（AI 利活用ハンドブック～生成 AI 編），以期充分因應人工智慧系統暨生成式人工智慧對於消費者可能產生的影響。

本研究認為日本以軟法機制靈活規範人工智慧有其可資學習之處，而其消費者保護主管機關在不立即進行法規調適之前提下，透過發布行政指導文件之方式，提醒企業經營者與消費者留意人工智慧可能產生的風險與所應留意之處，亦為我國可評估參納之作法。

(三)、英國

1、英國人工智慧規範推動現況

(1)、正式脫歐後展現異於歐盟之監管思維

英國在全球人工智慧發展上長期居關鍵地位，除技術研發享譽全球的圖靈研究所（Alan Turing Institute），其人工智慧發展政策亦是重要助力。英國政府在 2021 年 9 月發布「國家人工智慧戰略」（National AI Strategy），揭櫫使英國成為全球人工智慧超級大國的十年計畫；而 2021 年 1 月正式

[110] 消費者廳針對 1200 名消費者進行人工智慧意識調查，其調查成果顯示近半的受訪者對人工智慧抱持負面印象；而人工智慧最令消費者感到不安的事項中，占比最高者為「資料之處理」。消費者庁，第 1 回消費者意識調查結果（AI に対するイメージについて），頁 16，2024 年 4 月。

脫歐後，英國在人工智慧發展及相應的監管層面，更逐步展現異於歐盟之思維[111]。

英國科學創新暨技術部（Department for Science, Innovation & Technology, DSIT）在 2023 年 3 月發布「科學技術基礎架構報告」（The UK Science and Technology Framework），DSIT 於報告法規標準專章中明言「英國應善用脫歐後的自由，在人工智慧所涉技術標準與國際規範制定上立於引領者角色。監管應當有利於創新、刺激對於科學技術的需求、吸引投資，並且可同時表徵英國所展現的價值觀並保護公民。英國應利用其科學技術優勢與國際關係，確保在人工智慧規範與技術標準領域之影響力」[112]。

(2)、確定根基部會固有權責處理人工智慧之衍生問題

針對人工智慧衍生爭端的處理，以英國「文化傳媒與體育部」（Department for Culture, Media and Sport, DCMS）為首的相關部會在 2022 年 7 月共同發布「人工智慧監管政策文件」（AI Regulation Policy Paper），倡議英國應建立一套可充分支持創新的人工智慧監管架構，同時人工智慧監管架構應當該充分對應人工智慧具體特徵，以「跨部門原則」（cross-sectoral principles）為基礎加以推動，並使相關監管機關可得在既有的職權範疇內，解釋與實施相關跨部門原則。

英國政府在 2023 年 3 月正式發布之「支持創新之人工智慧監管作法白皮書」（A Pro-innovation Approach to AI Regulation），白皮書確定英國人

[111] Office for Artificial Intelligence (UK), National AI Strategy (2021), at 4-5.
[112] Department for Science, Innovation & Technology (UK), The UK Science and Technology Framework (2023), at 15.

工智慧監管架構方向，表明英國現階段將不制定人工智慧全面性監管專法，亦不建立單一專責單位負責人工智慧監管工作[113]。

英國政府強調應避免可能扼殺創新的嚴峻立法，並在不新設「單一監管機關」之前提下，授權現有相關監管機關根據其所轄行業的人工智慧實際使用情形，量身打造合適的監管作法[114]。

2、與人工智慧消費者保護有關之規範作法

(1)、消費者保護主管機關發布「人工智慧戰略」揭示包括消費者保護在內之重要原則

「支持創新」是當前英國在人工智慧治理推動所秉持的核心原則，儘管英國政府亦體認最終或仍有必要採取立法行動，特別是針對生成式人工智慧/通用人工智慧系統所衍生的監管問題，惟英國政府堅信現時立法尚為時過早，最佳方法應係詳加理解與人工智慧有關的風險與挑戰、監管落差以及解決相關爭議之最佳方法[115]。

英國消費者保護主管機關「消費者暨競爭局」（Competition and Markets Authority, CMA）於 2024 年 4 月更新其「CMA 人工智慧戰略」（CMA AI strategic），CMA 指出人工智慧快速發展為企業與消費者帶來益處，但也帶來了挑戰。人工智慧可以為英國社會與經濟帶來真正變革，大幅提升生產力，改變諸多現有的產品與服務，並將跨部門的創新推向市

113 UK Government, A Pro-innovation Approach to AI Regulation (2023), at 3.
114 *Id.*
115 Valeria Gallo & Suchitra Nair, The UK's framework for AI regulation, DELOITTE (Feb. 21, 2024), https://www.deloitte.com/uk/en/Industries/financial-services/blogs/the-uks-framework-for-ai-regulation.html (last visited Oct. 25, 2024).

場。然而，若缺乏強有力的消費者保護機制，利用人工智慧進行創新的潛力將無法實現，其益處也無法在全社會廣泛分享[116]。

(2)、消費者保護主管機關之因應思維

A、充分掌握消費者面臨的風險

CMA 指出儘管根基人工智慧所驅動的服務，可透過提供更高品質、更低價格以及愈發客製化的產品與服務，從而使消費者受益，但此一新興技術也可能導致不公平的消費者行為，諸如：

(1)、消費者可能接觸大量的虛假與誤導性訊息：人工智慧技術使得創建虛假或誤導性訊息成為輕而易舉之事，事業可得以更低成本與更大的規模實施不公平的商業手法，諸如訂閱制陷阱（subscription traps）、隱藏式廣告（hidden advertising）或虛假評論（fake reviews）等，從而誤導消費者並使消費者遭受損害[117]。

(2)、不利於消費者的個人化定價：人工智慧也讓事業可得對應個別消費者提供客製化服務，諸如個人化定價（personalised pricing）或個人化優惠（personalised offers）等，但如果相關應用係不公平地鎖定弱勢消費者（ vulnerable consumers），或是產生不公平的分配效應（distributive effects），則仍可能對消費者有害[118]。

B、針對消費者在生成式人工智慧下所受保護提出六項原則

[116] Competition and Markets Authority, CMA AI Strategic Update, CMA (Apr. 29, 2024), https://www.gov.uk/government/publications/cma-ai-strategic-update/cma-ai-strategic-update (last visited Oct. 25, 2024).
[117] *Id.*
[118] *Id.*

為確保企業在發展生成式人工智慧的同時可得有效保障消費者，CMA 制定了六項原則，敦促企業經營者根據相關原則，確保其業務活動可得充分保障消費者。CMA 表明其所提出的六項原則，目的在於補充英國政府揭櫫之「支持創新」治理方法與規範原則，立於 CMA 的職權，自敦促競爭與消費者保護角度建構良好運作的經濟市場[119]。

對比歐盟使用的「通用人工智慧」，CMA 則是使用「基礎模式」（Foundation Models, FMs）一詞描述生成式人工智慧，而其針對基礎模型提出的六項原則分別為：

(1)、開放近用

確保人工智慧開發人員可得確保對於關鍵輸入（critical inputs）之近用。

(2)、充分的消費者選擇

消費者應擁有充分自由，選擇其所使用的人工智慧（基礎模型）系統以及如何使用。

(3)、選擇權利

確保企業經營者與消費者擁有充分的自由與知識，以利企業經營者與消費者可得決定如何運用基礎模型；

(4)、公平交易

避免藉由產業夥伴關係或其他形式的整合行為，影響企業之間的有效競爭。

(5)、透明度

應向消費者提供有關其所使用的基礎模型服務之充分資訊，以利消費者作出明智之選擇。

(6)、問責機制

[119] *Id.*

確保基礎模型開發人員與部署人員，針對其形塑的價值鏈之相關投入部分加以負責，同時採取必要行動，資以確保消費者獲得充分保障[120]。

C、與其他機關共同合作解決人工智慧衍生問題

考量人工智慧衍生問題的多元化與複雜情形，CMA 體認其必須與其他監管機關進行，並確保各機關所採取監管作法的一致性。CMA 指出其職責係競爭與消費者保護，然而人工智慧的實務應用尚涵蓋了其他重要的政策領域，諸如個人資料保護、資訊安全與智慧財產權保護等，從而使得監管機關之間的合作格外重要，CMA 也必須與其他監管機關在關聯政策制定層面保持密切聯繫，甫能有效處理人工智慧衍生之消費者保護爭議問題[121]。

[120] *Id.* Simon Bollans, AI update – CMA's approach to AI, STEPHENSON HARWOOD LLP (June 4, 2024), https://www.shlegal.com/insights/ai-update-cma's-approach-to-ai (last visited Oct. 25, 2024).
[121] Competition and Markets Authority, CMA AI Strategic Update, CMA (Apr. 29, 2024), https://www.gov.uk/government/publications/cma-ai-strategic-update/cma-ai-strategic-update (last visited Oct. 25, 2024).

肆、人工智慧商品/服務於我國消費者保護法之適用分析

一、人工智慧與商品/服務之界定

(一)、我國消保法上之商品與服務之概念

面對人工智慧發展浪潮，我國現行消費者保護法律體系，包括消保法本身及依據消保法所制定之定型化契約等規範，對應人工智慧商品或服務之消費者保護機制是否完備、如何與人工智慧的技術發展與產業應用獲致衡平，實有通盤檢視與評估調適與否之必要。

針對人工智慧商品或服務所涉消費者保護爭議，其先決問題當在人工智慧商品或服務是否有我國消保法之適用。對此，於依消保法第 2 條第 3 款規定「消費關係：指消費者與企業經營者間就商品或服務所發生之法律關係」，可知受消保法保障的前提，即在於消費者與企業經營者針對「商品」或「服務」產生的消費關係之實際存在。

1、消保法上之「商品」

消保法制定時，並未就商品進行定義，論者指出除第 7 條至第 10 條未有界定其概念與範圍之明文，第 2 條之名詞定義中亦未納入；有鑑於消保法未就商品之概念與範圍加以規定，法律適用上將導致困擾，爰於制定消保法施行細則時納入商品之定義[122]。

依消保法施行細則第 4 條規定「本法第 7 條所稱商品，指交易客體之不動產或動產，包括最終產品、半成品、原料或零組件」，由此可知消

[122] 朱柏松，消費者保護法論，翰蘆圖書出版，頁 79，1998 年 12 月；姜志俊，消費者保護法，國立空中大學出版，修訂再版，頁 47，2020 年 8 月。

保法所界定的商品概念，以民法所稱之「物」，包括動產與不動產為原則。基此，歷來學者論及消保法上的商品概念，亦係以動產與不動產為準[123]。

司法實務操作上亦以消保法施行細則第 4 條規定之定義為準，高等法院便曾指出「消費者保護法第七條所稱『商品』，指交易客體之不動產或動產，同法施行細則第四條規定甚明，而消費者保護法各條款均見商品之用語，有關『商品』之定義僅於上開施行細則第四條中明訂，又別無其他理由應將消費者保護法各章節之『商品』作不同定義，自應認為上開施行細則第四條有關商品之定義適用於消費者保護法中之所有使用『商品』之條款」[124]。

2、消保法上之「服務」

相較於商品在消保法上有著明確定義，現行消保法及其施行細則對於「服務」則未加以定義。行政院消費者保護處曾函釋指出消保法並未就服務加以定義，有關消保法服務責任之範圍，宜由法院參酌社會經濟發展，依實際情形以個案方式認定之[125]。

主要國家多未將服務如同商品納入商品責任客體，各國立法未將服務納入商品責任之範圍，其原因包括：1、概念不易清楚界定：可歸類為服務之活動不計可數，凡勞務之提供者皆可能屬服務的範圍，服務之概念本身不容易界定清楚，在適用範圍上必會發生困難；2、服務性質差異甚大：服務之種類各式各樣，且各種服務間之性質差異甚大，若欲以單一方式規範全部之服務，將造成許多不良後果[126]。

---

[123] 許政賢，臺灣消費者保護法的創新與挑戰－二十週年的反思，月旦民商法雜誌，第 45 期，頁 40，2014 年 9 月。

[124] 臺灣高等法院 89 年度上字第 1062 號民事判決。

[125] 行政院消費者保護處，院臺消保字第 1080101991 號函，2019 年 10 月 25 日。

[126] 洪誌宏，消費者保護法，五南出版，五版，頁 88，2021 年 6 月。

(二)、人工智慧實務應用有該當消保法上商品與服務之可能

本研究認為人工智慧/人工智慧系統有該當消保法上「商品」與「服務」之可能，包括了：1、人工智慧本身就是一種商品或服務；以及 2、人工智慧是受消保法規範的商品或服務之重要組成部分。

以歐盟 AIA 為例，該法第 6 條規定「於符合下述兩項要件時，人工智慧系統應被視為高度風險系統：(1)、該人工智慧系統作為產品的安全元件（safety component）加以使用，或人工智慧系統本身即屬於受附件一所臚列之歐盟立法所規範之產品。(2)、根據第(1)款規定人工智慧系統係產品之安全元件，或人工智慧系統本身即作為一項產品，被要求接受第三方合格評估，以利根據附件一所臚列之歐盟立法，使產品進入市場或提供使用」。從前揭條文即可發現歐盟 AIA 亦表明人工智慧系統本身可能即屬於一項產品，抑或可能為產品之重要組成部分（安全元件）。

二、人工智慧與可合理期待之安全性

(一)、AI 商品或服務應滿足消保法第 7 條規定之要求

消保法第 7 條第 1 項規定「從事設計、生產、製造商品或提供服務之企業經營者，於提供商品流通進入市場，或提供服務時，應確保該商品或服務，符合當時科技或專業水準可合理期待之安全性」。企業經營者若有違反此一規定時，依同條第 3 項規定，「企業經營者違反前二項規定，致生損害於消費者或第三人時，應負連帶賠償責任。但企業經營者能證明其無過失者，法院得減輕其賠償責任」。論者指出依據前開規定，我國商

品責任已不再強調「行為人的過失」之歸責基礎，已經從「人的過錯行為」轉向至「物的危險狀態」[127]。

此外，依消保法第 7 條之 1 規定，「企業經營者主張其商品於流通進入市場，或其服務於提供時，符合當時科技或專業水準可合理期待之安全性者，就其主張之事實負舉證責任」;「商品或服務不得僅因其後有較佳之商品或服務，而被視為不符合前條第一項之安全性」。

有關消保法第 7 條第 1 項之「符合當時科技或專業水準可合理期待之安全性」，消保法施行細則第 5 條進一步規定，「本法第 7 條第 1 項所定商品或服務符合當時科技或專業水準可合理期待之安全性，應就下列情事認定之：

一、商品或服務之標示說明。

二、商品或服務可期待之合理使用或接受。

三、商品或服務流通進入市場或提供之時期。」

儘管消保法施行細則第 5 條針對母法第 7 條之「符合當時科技或專業水準可合理期待之安全性」之判斷，提出三款判斷標準，論者指出消保法施行細則第 5 條規定內容僅為「例示性質」[128]。析言之，縱使消保法施行細則提出三款判斷標準，實務操作上仍有賴進一步具體化判斷因素。

(二)、「當時科技或專業水準可合理期待之安全性」之認定標準

行政院消費者保護處組改前之行政院消費者保護委員會，曾函釋指出「所稱『當時科技或專業水準可合理期待之安全性』，其主要之認定如下：（一）依照消費者保護法第 7 條之 1 第 2 項規定，商品或服務不得僅

[127] 王澤鑑，侵權行為法，作者自版，增訂新版，頁 728，2021 年 11 月。

[128] 同前註，頁 729。

因其後有較佳之商品或服務，而被視為不符合當時科技或專業水準可合理期待之安全性。理由在於：避免妨礙企業經營者從事商品或服務改良或創新之意願，從而兼顧企業之良性發展。（二）依照消費者保護法施行細則第 5 條規定，商品或服務是否符合當時科技或專業水準可合理期待之安全性，應就下列情事認定之：1、商品或服務之標示說明。2、商品或服務可期待之合理使用或接受。3、商品或服務流通進入市場或提供之時期」[129]。

(三)、「當時」（時間點）之具體判斷

消保法第 7 條第 1 項規定「從事設計、生產、製造商品或提供服務之企業經營者，於提供商品流通進入市場，或提供服務時，應確保該商品或服務，符合當時科技或專業水準可合理期待之安全性」。

就上開條件中的「當時」一詞而言，其具體時間點的判斷對於是否成立消保法上商品責任，影響至鉅。然而對於何謂「當時」，論者指出國內外法規均未有明確定義，論者指出學理討論上判斷該時間存在兩說：1、以損害發生時為基準，係由消費者之立法進行觀察，消費者會期待在利用商品之時點具有安全性；以及 2、以商品開始流通進入市場時為基準，係自製造人之立場觀察，以製造人使該商品脫離自己之手而流通進入市場時為基準[130]。當前多數學者係採「流通進入市場」時作為消保法第 7 條第 1 項規定之判斷時點[131]。

---

[129] 行政院消費者保護委員會，消保法字第 0990007740 號函，2010 年 8 月 12 日。

[130] 陳煥武，智慧醫材之當時科技水準探究與規範調適—從傳統醫療器材判決出發，高大法學論叢，第 19 卷第 2 期，頁 23，2024 年 3 月。

[131] 王澤鑑，註 127，頁 728；陳聰富，民法債編總論（一）：侵權行為法原理，元照出版，3 版，頁 713，2023 年 11 月。

觀察我國歷來司法實務，大抵亦認為我國消保法第 7 條「安全性有無欠缺」之判斷時間點，係商品「流通進入市場」之時，如瑕疵於商品進入市場之時並未存在，而係因消費者使用相當時期後始發生者，則非屬消保法第 7 條所規定之商品責任範疇[132]。

三、人工智慧與消費資訊揭露要求

(一)、消費資訊揭露向為國際規範及我國消保法強調事項

「聯合國消費者保護準則」（United Nations Guidelines for Consumer Protection）強調「透明度」的重要性，針對企業經營者應有之「良好商業行為原則」，在準則提出之六項原則中，即強調了「資訊揭露與透明度」的重要性。此外，在「保護消費者之國家政策」部分，針對國家所應制定鼓勵的企業經營者行為，亦納入「企業經營者所提供的商品或服務之明確與及時之資訊，以及有關交易的條款與條件」[133]。

就我國消費者保護法制進行觀察，消保法第 4 條首先規定，「企業經營者對於其提供之商品或服務，應重視消費者之健康與安全，並向消費者說明商品或服務之使用方法，維護交易之公平，提供消費者充分與正確之資訊，及實施其他必要之消費者保護措施」；另第 5 條亦規定「政府、企

[132] 以最高法院判決為例，採此一觀點者包括：最高法院 98 年度台上字第 1356 號民事判決、最高法院 101 年度台上字第 803 號民事判決、最高法院 102 年度台上字第 4451 號民事判決、最高法院 104 年度台上字第 172 號民事判決、最高法院 106 年度台上字第 1 號民事判決、最高法院 106 年度台上字第 28 號民事判決、最高法院 109 年度台上字第 2959 號民事判決、最高法院 111 年度台上字第 339 號民事判決、最高法院 111 年度台上字第 857 號民事判決、最高法院 112 年度台上字第 299 號民事判決等。

[133] United Nations Conference on Trade and Development, United Nations Guidelines for Consumer Protection (2015), at para. 11, 14.

業經營者及消費者均應致力充實消費資訊，提供消費者運用，俾能採取正確合理之消費行為，以維護其安全與權益」。

此外，消保法第二章消費者權益下亦訂有「消費資訊之規範」專節規定，其中，消保法第 22 條規定，「企業經營者應確保廣告內容之真實，其對消費者所負之義務不得低於廣告之內容」；「企業經營者之商品或服務廣告內容，於契約成立後，應確實履行」。同法第 24 條另規定，「企業經營者應依商品標示法等法令為商品或服務之標示」；「輸入之商品或服務，應附中文標示及說明書，其內容不得較原產地之標示及說明書簡略」；「輸入之商品或服務在原產地附有警告標示者，準用前項之規定」。

儘管消保法第 4 條統一要求企業經營者對於其提供之商品或服務，提供消費者充分與正確之資訊，對提供人工智慧商品或服務的企業經營者而言，如何滿足此等消費資訊揭露要求，或有必要進一步另行規範。對此，本研究認為於對應商品或服務的定型化契約規範中進行要求，或較相對務實及可行。

(二)、人工智慧商品或服務之標示說明

從前述有關是否「符合當時科技或專業水準可合理期待之安全性」之討論，可知根據消保法施行細則第 5 條規定，商品或服務是否符合當時科技或專業水準可合理期待之安全性，其認定標準之一係「商品或服務之『標示說明』」。惟學理上認為消保法施行細則第 5 條規定所提出之三款商品或服務是否滿足消保法第 7 條安全性要求之認定標準，事實上僅為「例示性質」，從而實務操作上仍有賴進一步具體化「標示說明」此項判斷因素之內涵。

四、人工智慧與法律責任判斷

(一)、消保法之適用

1、違反消保法第 7 條規定之責任

由於人工智慧系統具有機器學習及自主性等特徵，從而產生其決策結果的不可預測性以及決策過程之不透明性等風險，對使用該系統或接受其服務的消費者而言，恐產生難以預見的損害及訴訟上舉證之困難。

針對違反消保法第 7 條規定所產生的賠償責任，本質上屬於「侵權責任」。論者指出有關商品責任在侵權行為法上之正當化基礎，早在消保法與民法另外明文化制定特殊類型之商品製造人責任規定之前，蓋我國最高法院 78 年度台上字第 200 號判決即明確揭示「商品製作人生產具有瑕疵之商品，流入市場，成為交易之客體，顯已違反交易安全義務，苟因此致消費者受有損害，自應負侵權行為之損害賠償責任」[134]。

違反消保法第 7 條規定所產生的賠償責任，在屬於「侵權責任」之前提下，自應依民法第 216 條之規定填補債權人所受損害及所失利益[135]。

2、消保法第 7 條之舉證責任分配問題

(1)、企業經營者應就其人工智慧商品或服務符合消保法第 7 條第 1 項規定（當時科技或專業水準可合理期待之安全性）負舉證之責

[134] 向明恩，商品「不符合當時科技或專業水準可合理期待安全性」之再認識－以最高法院 109 年度台上字第 2959 號民事判決為例示，月旦裁判時報，第 139 期，頁 23-24，2024 年 1 月。

[135] 臺灣臺北地方法院 107 年消字第 21 號民事判決。

最高法院已多次指出「法院針對『商品製造人責任』事件之處理，如嚴守民事訴訟法第 277 條所定之原則，難免產生不公平之結果，是以受訴法院應視各該具體事件之訴訟類型特性暨待證事實之性質，斟酌當事人間能力、財力之不平等、證據偏在一方、蒐證之困難、因果關係證明之困難及法律本身之不備等因素，透過實體法之解釋及政策論為重要因素等法律規定之意旨，較量所涉實體利益及程序利益之大小輕重，按待證事項與證據之距離、舉證之難易、蓋然性之順序（依人類之生活經驗及統計上之高低），並依誠信原則，定其舉證責任或是否減輕其證明度，進而為事實之認定並予判決」[136]。

依消保法第 7 條第 1 項規定「從事設計、生產、製造商品或提供服務之企業經營者，於提供商品流通進入市場，或提供服務時，應確保該商品或服務，符合當時科技或專業水準可合理期待之安全性」，同條第 3 項並規定「企業經營者違反前二項規定，致生損害於消費者或第三人時，應負連帶賠償責任。但企業經營者能證明其無過失者，法院得減輕其賠償責任」。準此，針對消保法第 7 條規定之違反，歷來實務及學說均認為本條規定係「無過失責任」，最高法院亦曾表示從事設計、生產、製造商品之企業經營者，依消費者保護法第 7 條第 3 項之規定應負連帶賠償責任之事由，為違反確保其提供之商品無安全或衛生上之危險。如其商品有安全上之危險存在，即屬有所違反，應依該條項之規定負其責任，縱令其無過失亦同[137]。

此外，依消保法第 7 條之 1 第 1 項規定「企業經營者主張其商品於流通進入市場，或其服務於提供時，符合當時科技或專業水準可合理期待之安全性者，就其主張之事實負舉證責任」。基此，企業經營者之商品或服務是否符合當時科技或專業水準可合理期待之安全性，即應由企業經

[136] 最高法院 99 年度台上字第 408 號民事判決、最高法院 109 年度台上字第 2747 號民事判決。
[137] 最高法院 87 年度台上字第 242 號民事判決。

營者就該等事實負舉證責任。歷來亦有諸多實務見解指出從企業經營者主張其商品流通進入市場，或其服務於提供時，符合當時科技或專業水準可合理期待之安全性，就其主張之事實，負舉證責任，為消費者保護法第7條之1所明定[138]。

就本研究報告觀點，企業經營者雖負有證明其符合消保法第7條「符合當時科技或專業水準可合理期待之安全性」之責，然而針對人工智慧商品或服務之適用，現階段恐將面臨證明不易或標準尚未臻明確等問題。蓋作為持續發展中的新興技術，無論是諸如歐盟AIA的硬法規定，抑或如美國人工智慧風險管理框架（AI RMF）等軟法機制，包括人工智慧系統衍生風險的判斷（風險等級及其具體所生危害情形），以及企業經營者之人工智慧商品或服務是否已具相當之安全性（是否有效管理人工智慧系統之衍生風險），當前並無放之四海而皆準之標準。

最高法院近年曾於109年度台上字第2959號判決表示「商品符合其交付市場時之科技或專業技術水準可合理期待之安全性，屬不確定之法律概念，其具體化內涵仍需受規範者所得預見，始受拘束，於其未盡該注意義務時，令其承擔賠償責任。市面流通之商品或服務，倘無公認之規格，一般業界所採認之標準，亦可援為參考之依據」[139]，

就本報告觀點，針對人工智慧商品或服務於我國消保法之適用而言，在後續實際出現肇因於人工智慧商品或服務之消費爭議時，企業經營者應如何充分舉證其業已符合當時科技或專業水準可合理期待之安全性，上揭最高法院判決所稱「一般業界所採認之標準」事實上仍有未臻明確之虞，恐易於產生爭議。

本報告建議可採取務實觀點，持續關注國內外實務關聯標準之發展及被認定為「一般業界所採認之標準」之可能性。較值留意者如國際標準

[138] 臺灣高等法院110年度上易字第715號民事判決、臺灣高等法院108年度消上易字第18號民事判決。
[139] 最高法院109年度台上字第2959號判決。

化組織（International Organization for Standardization；以下簡稱 ISO）所發布的「人工智慧管理系統標準」（Information technology — Artificial intelligence — Management system）：ISO/IEC 42001: 2023。依 ISO 說明，ISO/IEC 42001: 2023 是全球首個人工智慧管理系統國際標準，可適用於任何規模的組織，無論是提供或使用人工智慧系統的產品或服務，均可依循此一標準架構，負責任且合乎道德地利用人工智慧技術[140]。

另一可資關注者，為數位發展部：「AI 產品與系統評測制度」與「AI 產品與系統評測指引」。依數位發展部公布資料，AI 評測中心未來將致力於推動國內自行研發 AI 模型功效評測工具，針對不同產品、系統與服務類別，參考對應之國際試驗方法，來發展我國對應之評測工具與系統，符合國內試驗需求[141]，未來或有機會成為一般業界所採納之公認標準。

(2)、消費者則應就人工智慧商品或服務與損害結果兩者存在「因果關係」負舉證之責

就消費者保護法第 7 條規定之從事設計、生產、製造商品或提供服務之企業經營者之賠償責任，應由受害人（消費者）就其損害之發生係因該商品或服務之「通常使用」所致及二者間具有因果關係之事實，負舉證之責，其後方由企業經營者依消保法第 7 條之 1 第 1 項規定，負證明其商品或服務符合當時科技或專業水準可合理期待之安全性之責[142]。

---

[140] International Organization for Standardization, ISO/IEC 42001: 2023, https://www.iso.org/standard/81230.html (last visited Sept. 19, 2024).

[141] 數位發展部，數位發展部「AI 產品與系統評測中心」啟動 推動我國 AI 評測制度與可信任 AI 環境發展，https://moda.gov.tw/ADI/news/latest-news/9295（最後瀏覽日：2024 年 9 月 19 日）。

[142] 臺灣臺北地方法院 109 年度簡上字第 486 號民事裁定。

(二)、民法第 191 條之 1 規定

除消保法第 7 條規定，我國民法亦納入「商品製造人之責任」。民法第 191 條之 1 第 1 項規定，「商品製造人因其商品之通常使用或消費所致他人之損害，負賠償責任。但其對於商品之生產、製造或加工、設計並無欠缺或其損害非因該項欠缺所致或於防止損害之發生，已盡相當之注意者，不在此限」。

學說及實務均認為民法第 191 條之 1 之商品製造人責任，係採取「推定過失責任」，亦即只消存在損害即推定商品製造人有過失，除非其能舉反證免責。而相關免責事由包括：

(1)、對於商品之生產、製造或加工、設計並無欠缺。對此，民法第 191 條之 1 第 3 項另規定若「商品之生產、製造或加工、設計，與其說明書或廣告內容不符者，視為有欠缺」。

(2)、其損害非因商品之生產、製造或加工、設計之欠缺所致，析言之，商品製造人可得證明消費者所受損害與商品之欠缺，兩者之間並無因果關係。

(3)、商品製造人對於防止損害之發生，已盡相當之注意。

(三)、消保法與民法之適用關係

針對商品產生的民事責任規定，我國分別訂有消保法第 7 條及民法第 191 條之 1 規定，採取雙軌規範模式。消保法第 7 條採取無過失（嚴格）責任設計，企業經營者（商品製造人）僅能減輕責任，而不得免責，而民法第 191 條之 1 屬於特別侵害行為態樣之一，性質上為過失責任，民法第 191 條之 1 第 1 項但書設有免責規定，與消保法第 7 條有所不同。

針對消保法第 7 條及民法第 191 條之 1 兩者之間的適用關係，學說上存在「法條競合說」與「請求權自由競合說」等不同看法。多數認為基於消保法第 7 條規定及民法第 191 條之 1 規定，兩者存在著不同的構成要件與相異之法律效果，應解釋「請求權自由競合說」較為妥適。

就本研究觀點，由於人工智慧系統具有機器學習及自主性等特徵，從而產生其決策結果的不可預測性以及決策過程之不透明性等風險，對使用該系統或接受其服務的消費者而言，恐產生難以預見的損害及訴訟上舉證之困難。前述情形也說明了為了歐盟針對人工智慧所涉及的民事損害賠償問題，另行提出歐盟人工智慧責任指令（AILD）草案，並於草案中創設所謂的「因果關係推定」設計，藉以減輕受害者針對人工智慧系統所造成的損害之舉證責任。

對我國而言，由於我國民法第 191 條之 1 原即為「過失推定」設計，從而針對「人工智慧商品」衍生之消費者保護爭議/產品責任問題，似無需考量仿歐盟 AILD 草案制定相近立法並引入其「因果關關推定」機制。但另一方面，由於我國消保法並不以產品責任為限，尚包括服務責任，從而有關「人工智慧服務」所衍生的民事責任問題，便有應否參酌歐盟 AILD 草案並導入「因果關關推定」機制之討論空間。

若決定仿歐盟 AILD 草案制定相近規定，亦須留意 AILD 草案係以「非契約關係」為適用對象，若認為消費者保護立法的適用，係以存在消費關係（消費契約）為必要時，則人工智慧商品或服務造成消費者損害所產生的賠償請求，或無法適用歐盟 AILD 草案。就我國消保法適用而言，按行政院消費者保護會「消費者保護法 Q & A」之說明，消費者並不以「契約關係之相對人」為限，一般權利義務關係，僅存在於具有契約關係的兩方，惟消費者除交易之相對人外，尚包括以消費為目的而為使用商品

或接受服務者，亦即包括契約目的可能實際為消費之人在內[143]，按前揭文義，或係以存在「消費契約」為必要。

若消保法上之消費者，以其與企業經營者之間存在契約關係為必要，縱使我國仿歐盟 AILD 草案制定相近立法，仍無法適用於人工智慧商品或服務衍生的消費爭端之賠償請求與責任分配問題之處理。惟本報告立於充分消費者保護之角度，主張消保法上之消費關係，並不以存在消費契約為必要。基此，若我國仿歐盟 AILD 草案制定相近立法，只消是肇因於人工智慧商品或服務所衍生的民事責任，仍應有該法之適用。

[143] 行政院消費者保護會，消費者保護法 Q＆A（01.總則：014.何謂消費者？），https://cpc.ey.gov.tw/Page/2CC341DED4FBBB94/598b9890-b853-4d34-8fba-07ab69fa7c83（最後瀏覽日：2024 年 8 月 20 日）。

伍、本計畫全程研究成果暨我國消費者保護法制調適建議

一、全程研究成果

(一)、人工智慧/人工智慧系統的概念界定

面對人工智慧發展伴隨而生的各項問題之處理，「自律」與「他律」機制各有擁護者，在人工智慧衍生爭端急遽增加且難以套用既有的監管經驗之下，國際上應對人工智慧的治理與監管思維，也由最初的自律機制在近年加入他律概念，甚至有轉以他律機制為主之趨勢。

人工智慧衍生爭端處理上的首先步驟，便是清楚界定「人工智慧」此一概念。世界智慧財產權組織（WIPO）自技術角度嘗試定義人工智慧，並強調人工智慧並非單一技術，而是包括「機器學習」在內、眾多技術的結合運用。另就監管層面而言，更為重要的定義當推經濟合作暨發展組織（OECD）在其「人工智慧建議書」中提出的「人工智慧系統」（AI System）概念，OECD 將之定義為「一種基於機器的系統，針對明確或隱含目標，根據所接獲的輸入推斷如何產製可能影響真實或虛擬環境之預測、內容、建議或決策等輸出。不同的人工智慧系統實際部署後之自主性與適應性程度各不相同」。人工智慧系統一詞暨其概念受到了諸多國際組織與國家的引用，而甫於 2024 年 8 月 1 日生效的全球首部人工智慧全面性監管專法：歐盟 AIA 亦採用了此一名詞與概念。

(二)、人工智慧/人工智慧系統衍生之消費者保護爭議

在人工智慧技術持續精進並快速滲透幾近各個行為之下，人工智慧/人工智慧系統無疑地催生了龐大的商機。從早期以「管制性行業」為主的應用情形，諸如醫療照護、交通運輸及金融服務等事業，現今整體商業活動及人類生活等層面已有不勝枚舉的人工智慧應用案例出現。而近期「生成式人工智慧」的快速崛起，諸如文字生成工具 ChatGPT 等，更讓多數人首次意識到人工智慧已真實出現在你我的日常生活之中。

惟人工智慧技術發展與實務應用易於引發爭議，主要成因包括了：1、人工智慧系統可能不具可解釋性/透明度；2、人工智慧決策可能存在偏頗/歧視情形；3、人工智慧核心技術「機器學習」仰賴大量的資料蒐集與利用，易於出現不當蒐集與利用個人資料等隱私侵害爭議。而近年蔚為風潮的生成式人工智慧，亦衍生諸如智慧財產權侵害等爭議。

面對人工智慧快速發展與帶來的風險，其相應的治理與監管推動卻面臨若干棘手課題：1、人工智慧監管難以避免規範上出現「空白現象」；2、難以正確框列及評估人工智慧可能衍生之風險；3、難以援引既有的科學與技術監管經驗；以及 4、人工智慧治理推動易於落入所謂的「科林格里奇困境」。特別是人工智慧龐大的發展潛力，使得眾多國家苦思究竟是以發展為主，抑或應以治理為主，踟躕不前下便可能錯失適時介入進行監管之時機。

人工智慧衍生的爭議中，「消費者保護」亦是備受關注之一環。對此，本研究認為日本消費者保護主管機關：消費者廳提出的觀點最具代表性。為因應人工智慧帶來的衝擊，日本消費者廳於 2020 年 1 月成立「消費者因應數位化檢討會之人工智慧小組」並於同年 7 月發布研析成果報告書。日本消費者廳於報告書中提出了當前人工智慧技術發展與實務應用衍生的三大消費者保護議題，包括：1、人工智慧與消費者安全相關議題；2、人工智慧與消費者自主決策相關議題；以及 3、人工智慧與消費者隱私相關議題。

值得留意的是日本消費者廳除梳理上述三大議題外，亦分析各該議題所涉及的日本現行法律規範，可以發現人工智慧衍生的消費者保護爭議，其面向並不以「消費者保護法制」為制，本研究在我國法部分係著重於消保法暨關聯消保規範之適用與調適建議，爰不就消保法以外之立法進行適用與有無規範調適必要討論。

(三)、國際現時關聯法制規範分析

針對人工智慧商品或服務所引發的消費者保護問題，除固有消費者保護法制之適用外，對此一議題直接產生影響的無疑是各國針對「人工智慧監管立法」之推動思維。特別是歐盟甚早即確定將立於「風險管制基準」立場，研議推動全面性人工智慧監管專法，自 2021 年歐盟執委會提出 AIA 草案以降，歷經多年討論，歐洲議會與歐盟理事會於 2024 年 3 月 13 日及 5 月 21 日正式投票通過 AIA，全文於同年 7 月 12 日於歐盟公報發布 ，並於公布後 20 日（同年 8 月 1 日）正式生效。受歐盟影響，現時亦有國家如加拿大及巴西等，刻正推動其全面性人工智慧監管專法。

惟並非所有國家都如同歐盟秉持制定全面性人工智慧監管專法之立場，事實上現時全球人工智慧治理與監管思維可概分為「集中化」（Centralization）與「分散化」（Fragmentation）兩大陣營。而本研究計畫鎖定的四個目標地區/國家中，事實上亦僅有歐盟高舉集中化的全面性監管專法大纛，美國與英國雖未反對針對人工智慧進行立法，但其強調係立於部門固有權責之上進行立法，析言之，美國與英國的人工智慧立法係「部門立法」，同時立法面向亦不以監管為限。而日本為善用人工智慧的發展潛力，更是以「軟法機制」為主，現時並不擬針對人工智慧進行專門立法。

本計畫完整分析歐盟關聯法制，同時掌握美國、英國與日本之規範架構與推動方向。在歐盟法制研析部分，包括最受矚目的歐盟人工智慧法（AIA），以及為解決人工智慧系統衍生民事責任問題提出的「人工智慧責任指令草案」（AILD 草案）與甫完成修正之「產品責任指令」（PLD）。由於歐盟 AIA 係聚焦人工智慧系統衍生風險之應對與監管要求，並未納入民事責任處理規定，爰歐盟執委會除推動 AIA，另行提出 AILD 草案與 PLD 修正草案。

歐盟 AIA 將人工智慧系統可能衍生的風險區分為四個風險等級，包括：1、無法接受的風險；2、高度風險；3、有限風險；及 4、最小風險或無風險。除設定與區分風險級別，AIA 同時根據風險級別的高低，設定其相應之規範密度。若人工智慧系統經判定屬於「無法接受風險」，除符合歐盟 AIA 所臚列的例外條件，將完全禁止此等人工智慧系統之實務應用。若被認定為「高度風險」，該等人工智慧系統於實際應用（進入市場）前，必須恪遵 AIA 所提出之相關嚴格規範。若人工智慧系統被判定為「有限風險」，其應遵循並符合最低限度透明度之要求，以利使用者作出明智決策，同時在實際應用後，使用者亦可得決定是否繼續使用。若人工智慧系統屬於最後之「最小風險」等級，因不存在風險或僅對民眾造成極小之風險，歐盟原則上不會對此類系統進行干預，但鼓勵事業制定「行為守則」落實風險管理。由於我國現時尚無人工智慧專門立法，而國科會提出之「人工智慧基本法草案」，性質上屬於基本法，草案中雖提及「風險分級與管理」概念，但並無具體之分級標準，歐盟 AIA 針對風險的區分標準除具高度參考價值外，對於判斷消保法第 7 條「當時科技或專業水準可合理期待之安全性」之判斷，特別是「安全性」認定部分，應有相當之參考價值。

歐盟執委會繼 2021 年提出 AIA 草案後，為回應歐洲議會之立法要求，執委會於 2022 年 9 月另提出 AILD 草案，針對人工智慧系統所生損

害所涉及的「非契約民事責任」，建立統一規範並期有效解決了人工智慧爭端救濟上所面臨的舉證困難問題。歐盟 AILD 草案的核心宗旨係確保遭受人工智慧系統侵害之人，可得享受與受到其他技術侵害之人相同的保護水平。考量人工智慧技術的複雜性與不透明等情形，歐盟 AILD 草案將創建一套可舉反證推翻的「因果關係推定」機制，藉以減輕受害者針對人工智慧系統所造成的損害之舉證責任。

殊值注意之處在於歐盟 AILD 草案係著眼「非契約民事責任」，立於我國消保法而言，若認為受消保法保障的「消費關係」，係以存在「消費契約」為前提，即使我國訂有類似歐盟 AILD 草案之立法，似亦難以適用該法及其提出之「因果關係推定」機制。反面言之，若認為「消費關係」並不以「消費契約」之存在為必要，則肇因人工智慧商品或服務使用而受有損害之消費者，即可受到「因果關係推定」機制之保障。本計畫認為立於保護消費者之立場，我國消保法下受到保護之消費關係，應不以存在消費契約為必要，從而包括上述歐盟 AILD 草案所擬適用與保障之非契約民事責任。

與歐盟 AILD 草案同步提出之 PLD 修正草案，其主要目的在於解決現行 PLD 規定適用於數位環境之課題。歐盟執委會發布的「產品責任指令評估報告」具體指謫 PLD 在應對新興數位技術，特別是人工智慧的不足之處，包括：1、數位內容、軟體與數據等特定無形元素，對眾多新興產品的有效運作至關重要，但這些無形元素可否被視為 PLD 所稱之產品，事實上未臻明確。2，新興技術往往帶來全新的風險，諸如影響系統安全或網路安全風險等，然而 PLD 僅針對「物理或物質損害」進行賠償。3、人工智慧本身的特性，亦使得因果關係的存在判斷與舉證責任判斷等問題變得愈發困難，並可能導致成員國法院處理人工智慧造成的損害時，採取不同的做法，進而引發歐盟法制出現碎片化現象。

PLD修正草案主要宗旨係著眼製造商針對缺陷產品的嚴格責任規則，進行必要修正，確保過往存在適用爭議的產品，包括數位商品與整新商品等，受害者於此類商品對其造成損害時仍可獲得公平之賠償。此外，草案亦可望助益人工智慧商品所生損害之受害者，向製造商提出更為有效之賠償請求。基此，PLD 修正草案將適度調整有關製造商針對缺陷商品之嚴格責任機制，允許在無需證明過失之情況下賠償消費者所受損害。

二、我國消費者保護法制調適建議

(一)、我國對應人工智慧之專門立法推動概況

在國際高度重視人工智慧治理與監管推動，我國亦高度關注人工智慧發展帶來的正反效益並研商必要規範。在歐盟提出 AIA 草案前，已有立法委員倡議制定人工智慧專法，而伴隨歐盟正式推動 AIA，除立法院持續有委員提案推動「人工智慧基本法」、「人工智慧發展基本法」及「人工智慧發展及管理條例」等不同版本之草案，亦可見由學者集思廣義提出之「人工智慧基本法」草案。此外，在歷經廣泛討論後，國科會於 2024 年 7 月預告「人工智慧基本法」草案，成為當前最為重要之人工智慧專法草案版本。

1、立法院「人工智慧基本法」關聯草案

時間	法案名稱	提案人	草案要點
2019 年 5 月 15 日	人工智慧發展基本法草案	立法委員許毓仁等 21 位委員	• 本法之制定目的。（草案第一條）

			• 人工智慧之名詞定義。（草案第二條） • 人工智慧發展綱領。（草案第三條） • 主管機關與特別委員會。（草案第四條至第五條） • 政府建設。（草案第六條） • 數據資料與隱私、個資保護。（草案第七條至第九條） • 教育預算。（草案第十條） • 沙盒計畫。（草案第十一條） • 人工智慧開發原則。（草案第十二條） • 人工智慧發展之倫理。（草案第十三條） • 施行日期。（草案第十四條）
2020 年 9 月 16 日	人工智慧發展基本法草案	立法委員鄭麗文等 20 位委員	• 本法之制定目的。（草案第一條）

			• 人工智慧之名詞定義。（草案第二條） • 人工智慧開發原則。（草案第三條） • 人工智慧發展之倫理。（草案第四條） • 人工智慧發展綱領。（草案第五條） • 主管機關。（草案第六條） • 補助、獎勵及輔導。（草案第七條） • 個人資料相關法規調整及利用規範。（草案第八條） • 特別委員會。（草案第九條） • 特別審核機制。（草案第十條） • 智慧化政府推動。（草案第十一條） • 教育預算。（草案第十二條）

			• 沙盒計畫。（草案第十三條） • 施行日期。（草案第十四條）
2022 年 9 月 28 日	人工智慧發展基本法草案	台灣民眾黨黨團	• 本法之立法目的、用詞定義、主管機關及其職掌；為協助推動人工智慧發展相關事項，政府得以專責機構辦理相關業務。（草案第一條至第七條） • 通用格式之巨量資料平臺共享機制；人工智慧相關技術之風險分級及其義務。（草案第八條至第十條） • 人工智慧發展之基本原則，包含尊重國際公約規範、環境保護及永續發展原則、兼顧人民權益及資訊透明。（草案第十一條至第十五條） • 人工智慧創新實驗場域之推動及審核、人工智慧產業

			應公開之服務使用條款、人工智慧產品及服務之驗證制度及促進人工智慧產業發展應推動之事項。（草案第十六條至第二十條） • 使用者隱私權保障、個人資料彙集原則及倫理審查機制。（草案第二十一條至第二十四條） • 未揭露服務使用條款、未依個人資料當事人要求提供其通用格式之資料、未經倫理審查而執行應經審查核准之計畫，及未依個人資料保護法規定或未經去識別措施而不當利用個人資料導致個人資料當事人嚴重損害之處罰。（草案第二十五條至第二十七條）

2023 年 12 月 6 日	人工智慧發展及管理條例草案	台灣民眾黨黨團	• 本法之立法目的、適用範圍。（第一條） • 本法之中央主管機關為數位發展部；各地方則為縣市政府。（第二條） • 本法之名詞定義。（第三條） • 主管機關掌理之事項。（第四條） • 政府應寬列預算，由國家發展基金投入人工智慧產業並提供財稅及金融優惠制度，以培植國內人工智慧人才促進人工智慧產業發展。（第五條至第七條） • 政府應針對人工智慧產業發展及相關事項設置專職機構辦理。（第八條） • 政府應創造通用格式之巨量資料分享平台，由政府推廣、確立資料有價之理念，並鼓勵私

			人將巨量資料投入巨量資料分享平台，以建構相當資料利於人工智慧之發展。（第九條、第十條） • 人工智慧之發展原則應以人為本，並善盡環境永續及社會福祉，於發展中倘若涉及資料之處理及利用，亦應善盡個人資料自主之保障；為建構可信賴之人工智慧，應確保其避免歧視之特定以及善盡其可問責性並防止不公平競爭。（第十一條至第十六條） • 人工智慧之使用、研發，涉及個人資料之蒐集、處理、利用及傳輸之行為，亦應善盡個人資料保護之規定，並對應 GDPR 賦予當事人資料可攜權。（第十七條）

			• 人工智慧之發展，應以風險為分級，特別是高風險之內容，涉及較多法遵成本，應由諮詢評估會議議定之。（第十八條） • 高風險人工智慧其研發者及提供產品服務者應由其研發長向主管機關提交安全監測計畫、安全監測報告、建立風險管理系統，並向中央目的事業主管機關提出合乎法規規定之技術文件。（第十九條至第二十二條） • 主管機關針對高風險之人工智慧研發及利用，應設置監測體系，必要時得採取相關措施防止損害。（第二十三條） • 高風險人工智慧應確保其自動記錄功能，並於主管機關

			指定之網站公告相關資訊，確保人工智慧之透明性，以成為可信賴之人工智慧。（第二十四條、第二十五條） • 人工智慧於發生嚴重影響生命身體之事，其研發者或提供產品之人，應立即通報目的事業主管機關。（第二十六條） • 特殊人工智慧系統，因其具備詐欺之風險及特性，無論是否為高風險人工智慧，均有規範之必要，因此針對與自然人互動之人工智慧系統、情緒識別或生物識別之人工智慧系統，或人工智慧系統用於生成影音，而內容易被誤為真實者，明文規定揭露、資料蒐集等義務。

			（第二十七條至第二十九條） • 人工智慧創新實現場域之推動、核准及審查之程序。（第三十條、第三十一條） • 主管機關應推動之人工智慧發展事項。（第三十二條） • 人工智慧之民事責任、政府應建立社會保險制度及無法救濟時應請求人工智慧之國家救濟補償。（第三十三條至第三十五條） • 損害個人資料、違反風險管理系統、提出技術文件、安全監測計畫及報告、記錄功能、人工智慧系統資訊之揭露義務、未依個人資料提供通用格式之資料或其內容有虛偽不實或違反本法之通知義務之

			處罰。（第三十六條至第三十九條） • 政府之法令檢查及完備義務（第四十條） • 本法之施行日期。（第四十一條）
2024 年 4 月 12 日	人工智慧基本法草案	立法委員吳宗憲等 17 位委員	• 本法之立法目的、主管機關及名詞定義。（草案第一條至第三條） • 人工智慧之研發及利用，應以人為本、普惠人民、永續發展及值得信賴為目標，符合自主、保密、安全、包容及透明等基本原則。（草案第四條） • 定明政府應以跨領域或國際合作之方式，落實人工智慧發展之主要政策，由中央主管機關擬訂發展計畫報行政院核定，中央目的事業主管機關應配合擬訂或訂定法規

			或具體方案，辦理所定事項。（草案第五條及第六條） • 中央政府應持續確保預算經費符合推行政策所需，並結合財稅及金融優惠制度，積極協助、輔導人工智慧產業鏈。（草案第七條及第八條） • 關於人工智慧資料之蒐集、處理及利用，應建立必要之保護及監督機制。（草案第九條） • 人工智慧之研發及利用，應落實對於需要協助族群、勞工權益、公平交易秩序之保護，並建立必要之救濟、補償及保險制度。（草案第十條至第十三條） • 人工智慧之研發及利用，應符合國家標準或相關法規。（草案第十四條）

			• 政府對於人工智慧研發及利用之潛在風險，應建立風險評估及監管機制，以確保人工智慧可受信賴。（草案第十五條） • 為確保人工智慧之品質，應訂定品質管理機制，定期進行安全性、穩定性、可追溯性與可解釋性之評估及監督。（草案第十六條） • 為確保人工智慧之安全性，其研發者、提供產品或服務之自然人、法人、機關、機構或團體，有提出並公開技術文件之義務，經評估有風險者，有提出安全監測計畫之義務。高風險人工智慧之安全監測計畫應經核定，並於上市或提供服務後，定期向

			目的事業主管機關提出安全監測報告。（草案第十七條及第十八條） • 發生嚴重影響人民安全、健康、人格法益或財產之情事時，提供者有即時通報之義務。（草案第十九條） • 為有效達成促進人工智慧發展之目的，政府應給予獎勵、補助，並應規劃辦理人工智慧智慧創新實驗環境，強化對中小企業提供者及使用者之協助，鼓勵產業自行制定產業指引及行為規範。（草案第二十條至第二十二條） • 各級政府應於本法施行後，依本法規定檢討並修訂、廢止或改進所主管之法規及行政措施。

			（草案第二十三條） • 本法自公布日施行。（草案第二十四條）
2024 年 4 月 26 日	人工智慧基本法草案	立法委員賴士葆等 28 人	• 確立法案目的，促進人工智慧技術健康發展，保障公民權益。（草案第一條） • 界定本法之主管機關。（草案第二條） • 定義本法所稱之人工智慧。（草案第三條） • 政府應制定全國性策略，明確人工智慧技術發展目標與重點領域。（草案第四條） • 鼓勵政府支持基礎與應用研究，促進公私合作，共建發展平台。（草案第五條） • 強化人才培育，建立完善的教育培訓體系，提升人工智

			慧專業水平。（草案第六條） • 建立安全評估體系，確保人工智慧系統的運行安全與可靠性。（草案第七條） • 制定演算法歧視防範措施，保證人工智慧應用的公平性與正義。（草案第八條） • 加強資料隱私保護，確保個人資料的安全與私隱權益不被侵犯。（草案第九條） • 要求提供決策過程的通知與解釋，增進透明度與可解釋性。（草案第十條） • 保留人工干預的空間，確保關鍵決策可被有效審核與糾正。（草案第十一條） • 明定政府應就人工智慧利用所致之非

			自願性失業者，保障其勞動權益，並依其工作能力，予以輔導就業。（草案第十二條） • 推動國際合作，參與全球人工智慧治理，共同面對挑戰。（草案第十三條） • 要求政府及其機構應對人工智慧負擔監管職責，並建立必要之救濟、補償及保險制度。（草案第十四條） • 明定法案的施行日期。（草案第十五條）
2024 年 10 月 25 日	人工智慧基本法草案	立法委員林宜瑾等 21 人	• 本法之制定目的。（草案第一條） • 人工智慧定義。（草案第二條） • 人工智慧研究發展及應用之基本原則。（草案第三條） • 政府應推動人工智慧研究發展與應

			用。（草案第四條） • 政府應建立或完備人工智慧創新實驗環境。（草案第五條） • 政府應推動人工智慧公私協力與國際合作。（草案第六條） • 政府應推動人工智慧人才培育與素養教育。（草案第七條） • 政府應評估驗證人工智慧防止違法應用。（草案第八條） • 政府應推動人工智慧風險分類規範。（草案第九條） • 政府應強化人工智慧人為可控性。（草案第十條） • 政府應建立人工智慧應用負責機制。（草案第十一條）

			• 政府應保障勞工權益。（草案第十二條） • 政府應落實對於需要協助族群之保護。（草案第十三條） • 政府應保障個資隱私。（草案第十四條） • 政府應提升資料利用性與國家文化價值。（草案第十五條） • 政府公務使用人工智慧之原則。（草案第十六條） • 政府應檢討主管法規。（草案第十七條） • 本法施行日。（草案第十八條）

資料出處：立法院；研究團隊整理製表

2、人工智慧法律國際研究基金會「人工智慧基本法」草案

由學者組成的人工智慧法律國際研究基金會，考量伴隨人工智慧的應用擴大，其所引發之負面效應及風險實不容忽視，諸如隱私侵害、偏見

歧視、不公平競爭、安全性疑慮與工作變遷等。除了兼顧技術深耕及產業發展外，更應當完善運作環境，將道德倫理、法制整備、資料處理及社會變遷等議題，納入人工智慧發展政策。

人工智慧法律國際研究基金會指出為了形塑可受信任的人工智慧發展環境，實現人工智慧之多元利用，實有必要推動制定人工智慧通用法制之基本法，俾使我國高科技發展得以呼應當前之國際規範趨勢，經參酌外國立法例，兼顧國內產業發展脈動，於 2023 年 3 月擬具「人工智慧基本法」草案，全文共計 24 條[144]。其要點包括：

(1)、本法之立法目的、主管機關及名詞定義。(草案第一條至第三條)；

(2)、定明政府應以跨領域或國際合作之方式，落實人工智慧發展之主要政策，由中央主管機關擬訂發展計畫報行政院核定，中央目的事業主管機關應配合擬訂或訂定法規或具體方案，辦理所定事項。(草案第 4 條及第 5 條)；

(3)、中央政府應持續確保預算經費符合推行政策所需，並結合財稅及金融優惠制度，積極協助、輔導人工智慧產業鏈。(草案第 6 條及第 7 條)；

(4)、人工智慧之研發及利用，應以人為本、普惠人民及永續發展為目標，符合自主、保密、安全、包容及透明等基本原則。(草案第 8 條)；

(5)、關於人工智慧資料之蒐集、處理及利用，應建立必要之保護及監督機制。(草案第 9 條)；

(6)、人工智慧之研發及利用，應落實對於需要協助族群、勞工權益、公平交易秩序之保護，並建立必要之救濟、補償及保險制度。(草案第 10 條至第 13 條)；

[144] 人工智慧法律國際研究基金會，《人工智慧基本法草案（芻議)》發表說明會，網址：https://www.intlailaw.org/article_d.php?lang=tw&tb=3&cid=43&id=1938（最後瀏覽日：2024 年 10 月 25 日)。

(7)、人工智慧之研發及利用，應符合國家標準或相關法規。(草案第14條)；

(8)、政府對於人工智慧研發及利用之潛在風險，應建立風險評估及監管機制，以確保人工智慧可受信任。(草案第十五條)；

(9)、為確保人工智慧之品質，應訂定品質管理機制，定期進行安全性、穩定性、可追溯性與可解釋性之評估及監督。(草案第16條)；

(10)、為確保人工智慧之安全性，其研發者、提供產品或服務之自然人、法人、機關、機構或團體，有提出並公開技術文件之義務，經評估有風險者，有提出安全監測計畫之義務。高風險人工智慧之安全監測計畫應經核定，並於上市或提供服務後，定期向目的事業主管機關提出安全監測報告。(草案第17條及第18條)；

(11)、發生嚴重影響人民安全或健康之情事時，提供者有即時通報義務。(草案第19條)；

(12)、為有效達成促進人工智慧發展之目的，政府應給予獎勵、補助，並應規劃辦理人工智慧創新實驗環境，強化對中小企業提供者及使用者之協助，鼓勵產業自行制定產業指引及行為規範。(草案第20條至第22條)；

(13)、各級政府應於本法施行後，依本法規定檢討並修訂、廢止或改進所主管之法規及行政措施。(草案第23條)；

(14)、本法自公布日施行。(草案第24條)。

3、國科會「人工智慧基本法草案」

國科會有鑑於人工智慧技術近年發展快速，為整體產業與社會活動帶來廣泛的經濟和社會效益，並作為我國產業及國家發展之關鍵競爭優

勢。考量人工智慧技術創新之速度和可能面臨的挑戰，建構我國人工智慧技術研發與應用之良善環境，實為政府刻不容緩之責任。

國科會經審慎研議並召開多次溝通會議，凝聚各界共識，於 2024 年 7 月 15 日預告「人工智慧基本法草案」，揭示永續發展、人類自主、隱私保護、資安與安全、透明可解釋、公平不歧視及問責等七大基本原則，以及創新合作及人才培育、風險管理及應用負責、權益保障及資料利用、法規調適及業務檢視之四大推動方向[145]。

「人工智慧基本法草案」全文共計 18 條，其要點包括：

(1)、制定目的（草案第 1 條）；

(2)、人工智慧定義（草案第 2 條）；

(3)、人工智慧研究發展及應用之基本原則（草案第 3 條）；

(4)、政府應推動人工智慧研究發展與應用（草案第 4 條）；

(5)、政府應完善法規調適。（草案第 5 條）；

(6)、政府應建立或完備人工智慧創新實驗環境（草案第 6 條）；

(7)、政府應推動人工智慧 公私協力與 國際合作。（草案第 7 條）；

(8)、政府應推動人工智慧人才培育與素養教育（草案第 8 條）；

(9)、政府應評估驗證人工智慧防止違法應用（草案第 9 條）；

(10)、政府應推動人工智慧風險分級規範（草案第 10 條）；

(11)、政府應強化人工智慧人為可控性（草案第 11 條）；

(12)、政府應建立人工智慧應用負責機制（草案第 12 條）；

(13)、政府應保障勞工權益（草案第 13 條）；

(14)、政府應保障個資隱私（草案第 14 條）；

(15)、政府應提升資料利用性與國家文化價值（草案第 15 條）；

[145] 國家科學及技術委員會，人工智慧基本法草案預告 促進創新兼顧人權與風險，網址：https://www.nstc.gov.tw/folksonomy/detail/87e76bcd-a19f-4aa3-9707-ca8927dcb663?l=CH&utm_source=rss（最後瀏覽日：2024 年 10 月 25 日）。

(16)、政府公務使用人工智慧之原則（草案第 16 條）；

(17)、政府應檢討主管法規（草案第 17 條）；

(18)、施行日（草案第 18 條）。

(二)、法規調適建議：消費者保護法本身

1、人工智慧基本法草案並無實質規範，仍須評估應否就消保法本身進行必要調適

本研究計畫開始執行時，國科會尚未提出「人工智慧基本法」（草案），爰有關人工智慧商品或服務可能引發的消費者保護爭議，以及我國消費者保護法制之適用與調適問題，無可避免地必須檢視我國人工智慧法制具體擘劃方向而定，包括是否參考國際趨勢推動人工智慧專門立法，以及若確定推動專法的話，係屬於基本法抑或為作用法性質等先決事項。

上述先決問題隨著國科會於 2024 年 7 月預告「人工智慧基本法」（草案）後，似獲得解決，惟進一步觀察國科會所預告的「人工智慧基本法」（草案）內容，儘管屬於「全面性」人工智慧專門立法，然相較於歐盟 AIA 係實質監管導向的作用法，明確針對人工智慧系統風險及通用人工智慧進行全面規範，我國「人工智慧基本法」（草案）如同其名稱般，僅係「基本法」性質，該法揭櫫目標之落實，事實上仍有賴各該部會進一步制定實質規範（作用法），甫能有效落實人工智慧基本法草案所要求之事項。

殊值注意者，綜觀人工智慧基本法草案全文內容，事實上並未見任何「消費者保護」或「消費者」字樣。在未明文規定之前提下，本研究認為人工智慧基本法草案與「消費者保護」關係較接近之規定，為草案第 9 條第 1 項與草案第 12 條第 1 項規定。

觀察草案第 9 條第 1 項規定，要求「政府應避免人工智慧之應用，造成國民生命、身體、自由或財產安全、社會秩序、生態環境之損害，或出現利益衝突、偏差、歧視、廣告不實、資訊誤導或造假等問題而違反相關法規之情事」，值得留意者，本條立法理由指出「參考美國總統二○二三年發布之 AI 行政命令（Executive Order on Safe, Secure and Trustworthy Artificial Intelligence）定明政府應避免人工智慧之應用造成國民生命安全或生態環境損害，或出現利益衝突、偏差、歧視、廣告不實、資訊誤導或造假等問題，違反如兒童及少年福利與權益保障法、公平交易法、消費者保護法及個人資料保護法等相關法規之情事」，明文提及「消費者保護法」。

此外，草案第 12 條第 1 項另規定，「政府應依人工智慧風險分級，透過標準、驗證、檢測、標記、揭露、溯源或問責等機制，提升人工智慧應用可信任度，建立人工智慧應用條件、責任、救濟、補償或保險等相關規範，明確責任歸屬與歸責條件」，要求政府應按人工智慧風險分級建立相應之「問責機制」，藉以提升人工智慧應用之可信任度，同時應建立人工智慧之「責任規範，明確責任歸屬與歸責條件。從消費者保護角度而言，前揭問責機制、責任歸屬與歸責條件等，實與消保法高度相關。

就人工智慧商品或服務所涉及的消費者保護而言，對應上述「人工智慧基本法」（草案）要求事項之落實，本研究認為消保法本身之調適評估，關鍵仍在於對應：1、人工智慧商品/服務於消保法上之定性（消保法適用與否之判斷）；2、人工智慧商品/服務所涉及之可合理期待安全性；3、人工智慧商品/服務所涉及之消費資訊揭露；以及 4、人工智慧商品/服務產生消費爭議時之法律責任與責任分配等四項主要議題，就各該議題所涉及之消保法條文評估有無進行調適之必要，抑或維持現行規定即可。

2、對應四項主要議題之消保法調適評估與具體建議

(1)、人工智慧商品/服務於消保法上之定性（消保法適用與否之判斷）

可能為消費者接觸的商品或服務，是否適用消保法，涉及消保法第 2 條及消保法施行細則第 4 條有關「商品」與「服務」之定義。從本研究計畫前揭研究成果，已知人工智慧商品/服務應可認定為消保法所稱之商品或服務；此外，本研究同時認為人工智慧商品或服務，應可直接適用現行消保法與該法實施細則中有關「商品」與「服務」之定義規定。

析言之，現行消保法有關商品或服務之定義，並無須對應人工智慧商品或服務之判斷需求而進行修正。考量人工智慧屬於持續發展中的技術，而其實務應用態樣亦不斷推陳出新，後續於個案判斷上遇有爭議時，應可透過「函釋」方式，具體說明系爭人工智慧應用（人工智慧商品或服務）是否符合消保法之定義規定，並據以判斷其是否受到消保法之規範。

(2)、人工智慧商品/服務所涉及之可合理期待安全性

人工智慧商品或服務在實際適用消保法之前提下，提供商品或服務的企業經營者便應符合該法第 7 條「可合理期待安全性」之要求。蓋消保法第 7 條要求提供商品或服務的企業經營者，應確保其商品或服務符合當時科技或專業水準可合理期待之安全性，若從事設計、生產、製造商品或提供服務之企業經營者違反此一要求，並致生損害於消費者或第三人時，即應負連帶賠償責任。

考量消保法第 7 條規定係針對「所有」受消保法規範的商品或服務進行要求，本研究認為針對人工智慧商品或服務之適用，消保法第 7 條規定應可直接適用而無進行調適之必要。除立法論層面之問題，人工智慧商品或服務在消保法第 7 條規定適用上，尚應確定的兩項重要子議題：其一為針對條文中所稱之「當時」，其具體時間點為何；其二則是如何具

體判斷並確認企業經營者針對人工智慧商品或服務之提供，是否確實符合條文中所稱之「安全性」。

針對第一個子議題，當前無論是學說討論抑或實務見解，咸認為應以「流通進入市場」作為消保法第 7 條第 1 項規定之判斷時間點，此部分較無爭議。爰人工智慧商品或服務是否符合消保法第 7 條第 1 項規定，應以該等商品或服務實際進入市場並可為消費者購買或近用之時間點進行判斷。

針對第二個子議題，本研究認為在通案規範下，消保法第 7 條第 1 項所要求之「符合當時科技或專業水準可合理期待之安全性」，屬於事實認定問題，宜由司法實務依個案進行判斷。析言之，消保法第 7 條第 1 項規定並無須針對「人工智慧商品或服務」之適用，就其所涉及的安全性問題單獨制定判斷標準，而於實務上果發生爭議時，由法院根據當時之科技或專業水準進行判斷為宜。在檢視現時國內相關實務見解後，本研究認為現時可資參考之例如最高法院 109 年度台上字第 2959 號民事判決提出之「技術標準」概念。

然針對可能作為消保法第 7 條第 1 項「符合當時科技或專業水準可合理期待之安全性」之技術標準，相關標準的發展或建立，應非行政院消費者保護處之責。進一步而言，「人工智慧基本法」（草案）第 12 條第 1 項規定亦提及「政府應依人工智慧風險分級，透過標準、驗證、檢測、標記、揭露、溯源或問責等機制，提升人工智慧應用可信任度」，就條文中所要求之「標準」、「驗證」或「檢測」等有助於消保法第 7 條第 1 項規定適用判斷之機制，後續實有必要確認究係由何部會負責，甫利於人工智慧商品或服務產生消保法第 7 條第 1 項規定適用爭議時，可資作為法院個案判斷上之參考。

(3)、人工智慧商品/服務所涉及之消費資訊揭露

觀察現行消保法中有關商品或服務所涉及之消費資訊揭露要求，主要為消保法第 4 條、第 5 條、第 22 條及第 24 條等規定，惟消保法第 4 條與第 5 條屬於消費資訊揭露之原則性規範，而第 22 條及第 24 條則分別側重於廣告真實性與商品標示。另一方面，無論是規定於第一章總則中的消保法第 4 條與第 5 條規定，抑或規定於第二章消費者權益中之消費資訊規範專節規定，如同前述有關安全性之討論，係針對所有受消保法規範的商品或服務之通案性規定，並不宜單獨就人工智慧商品或服務之消費資訊揭露要求，率爾更動現行設計。

事實上對應特定商品或服務的消費資訊揭露要求，歷來多見於目的事業主管機關針對其主管商品或服務所制定的「定型化契約應記載及不得記載事項」之中，爰本研究認為針對人工智慧商品/服務所涉及之消費資訊揭露要求，並無須於消保法本身進行調適，而應思考如何透過既有的商品或服務之定型化契約應記載及不得記載事項之調適，而使其可得充分因應人工智慧所帶來之挑戰。對此，將於後述有關定型化契約規範之調適建議部分，另行說明。

(4)、人工智慧商品/服務產生侵權時之法律責任

由於人工智慧本身所具備的特徵，對於使用人工智慧商品或接受人工智慧服務的消費者而言，恐產生難以預見的損害及訴訟上舉證之困難。考量人工智慧民事侵權問題的處理需求，歐盟也在既有的民事法與產品責任規範之外，針對人工智慧另行推動人工智慧責任指令（草案）。

就我國民事責任規範而言，民法及消保法分別訂有一般過失責任與嚴格過失責任規範，本研究認為相關規範應足敷處理人工智慧商品或服所衍生的民事侵權責任之處理。而在伴隨而生的舉證責任分配部分，觀察

歐盟刻正推動的人工智慧責任指令草案，其最受關注之者在於創設「因果關係推定設計」，俾利消費者舉證。就舉證責任而言，我國消保法原即採取「舉證責任倒置」設計，此外，民法第 191 條之 1 規定亦採納「過失推定」設計，基此而言，在我國民法已有關聯設計之下，或無參考歐盟人工智慧責任指令（草案）制定人工智慧相應責任規範之急迫需求。

另一方面，考量人工智慧技術暨其關聯實務應用仍屬於人們認識有限之事物，當人工智慧商品或服務肇致消費者損害，現階段實務操作上或仍有不易判斷其因果關係之可能，爰參考歐盟立法精神，於消保法或諸如歐盟人工智慧責任指令（草案）之民事責任專門立法中納入相近規定，似亦無不可。本計畫認為初期可評估先於消保法中納入「因果關係推定設計」，並試擬建議條文如下，中長期再行評估有無進一步擴大制定人工智慧民事責任專門立法之必要。

3、建議條文試擬

(1)、民事責任（因果關係推定）

草案內容	說明
第○條　企業經營者所提供之商品（服務）若有應用人工智慧之情形，在滿足下述所有條件之下，可推定企業經營者之過失，與人工智慧系統之輸出，或應輸出而未輸出之間，存在著因果關係： 1、消費者業已證明企業經營者存在過失，包括企業經營者違反用以防止人工智慧商品	一、本條新增。 二、為確保遭受人工智慧系統侵害之人，可得享受與受到其他技術侵害之人相同的保護水平，歐盟繼制定著眼人工智慧風險監管的人工智慧法（AIA）後，另提出人工智慧責任指令（AILD）草案，針對人工智慧系統所生損害所涉及之民事責任，擬建立統一之規範。

（服務）肇致損害之注意義務規定。 2、可得合理地認定企業經營者之過失，影響人工智慧系統之輸出，或導致人工智慧系統應輸出而未能輸出。 3、消費者可得證明人工智慧系統之輸出或未能輸出，確實導致損害之發生。	三、考量人工智慧技術之複雜性與不透明等情形，歐盟人工智慧責任指令（AILD）草案創建可舉反證推翻之「因果關係推定」機制，藉以減輕受害者針對人工智慧系統所造成的損害之舉證責任。 四、本條參考歐盟人工智慧責任指令（AILD）草案第 4 條規定，企業經營者所提供之人工智慧商品（服務）造成消費者損害時，於符合特定條件之下，推定企業經營者之過失，與損害結果之間存在著因果關係。

(2)、隱私資料保護

草案內容	說明
第○條 人工智慧資料之蒐集、處理及利用，應審酌人民隱私、資訊自主及產業發展之均衡維護，建立必要之保護及監督機制。	一、本條新增。 二、人工智慧技術及人工智慧系統之發展，仰賴大量的訓練資料，其中包括可能巨量地蒐集及利用消費者之個人資料，爰就人工智慧商品（服務）之消費者保護而言，確保資料保護實為不可或缺之一環。 三、參考 2024 年 4 月 12 日立法委員吳宗憲等 17 位委員提出之「人工智慧基本法草案」第 9 條規定，使人工智慧資料之蒐集、處理及利

	用，對人民隱私資料有重大影響者，應衡平其與人工智慧相關產業之發展，建立必要之保護及監督機制。。 四、本條參考歐盟人工智慧責任指令（AILD）草案第 4 條規定，企業經營者所提供之人工智慧商品（服務）造成消費者損害時，於符合特定條件之下，推定企業經營者之過失，與損害結果之間存在著因果關係。

(三)、法規調適建議：定型化契約應記載及不得記載事項

1、應併同評估依據消保法制定之定型化契約應記載及不得記載事項之調適必要

我國消費者保護法制如何因應人工智慧帶來之衝擊，除消保法本身之調適評估外，另一應併同思考與推動之處，係處理難度較低而較具彈性之「定型化契約規範」。對此，當前消費者保護實務運作包括了「定型化契約應記載及不得記載事項」與「定型化契約範本」兩者，後者性質屬於行政指導，從而自立法論角度而言，主管機關宜側重於定型化契約應記載及不得記載事項之討論[146]。

[146] 研究團隊針對定型化契約規範之調適，建議側重於「定型化契約應記載及不得記載事項」，但亦可留意特定「定型化契約範本」之調適必要。諸如「手術、麻醉同意書及醫院住院須知參考範例」，因其屬於醫療照護領域，有較高之人工智慧應用可能性，目的事業主管機關於進行相關「定型化契約應記載及不得記載

現階段各部會已依據消保法之授權，制定眾多商品/服務定型化契約應記載及不得記載事項，本研究認為並非全數的定型化契約應記載及不得記載事項，均受到人工智慧影響或有因應人工智慧衝擊而進行調適之必要。務實方向應優先擇定現階段與人工智慧應用關係較為直接或連結較深並已制定「定型化契約應記載及不得記載事項」之領域，包括實務調查顯示人工智慧實務應用相對成熟之行業別，以及數位應用較為顯著之特定商品/服務型態，納入對應人工智慧之規範。

2、優先評估對象一：現階段人工智慧實務應用相對成熟之領域（行業別）

歷來我國各中央目的事業主管機關已根據消保法之授權，就所轄之特定商品或服務型態制定諸多定型化契約應記載及不得記載事項，惟並非所有現時可見的定型化契約應記載及不得記載事項，均有揆諸人工智慧技術發展與實務應用趨勢進行法規調適之必要。本研究認為務實之道，應係先篩選出現時人工智慧實務應用相對成熟的領域，其次再針對所梳理領域下業已制定定型化契約規範的商品或服務型態，檢視有無對應人工智慧增訂或修正相關規定之必要。

本研究基於 Statista 所發布的全球人工智慧實務應用研究進行檢視，並以其所梳理的行業占比排序作為篩選依據。按 Statista 研究成果，現時人工智慧實務應用占比最高的前五大行業別，分別為：1、醫療健康照護（15.7%）；2、金融（13.65%）；3、製造（13.65%）；4、商業暨法律服務（13.6%）；以及 5、交通（10.75%）[147]。其中在製造及商業暨法律服務部

事項」之調適推動時，亦可併同思考此一定型化契約範本因應人工智慧之規調適需求。

[147] Statista, Artificial Intelligence - Worldwide, https://www.statista.com/outlook/tmo/artificial-intelligence/worldwide (last visited Oct. 25, 2024).

分，由於無涉消費者或消費關係，此兩個領域並未見相關的定型化契約應記載及不得記載事項。而在醫療健康照護、金融與交通領域，現時可見的定型化契約應記載及不得記載事項整理如下：

領域	規範名稱	主責部會
醫療/照護	• 養護(長期照護)定型化契約應記載及不得記載事項 • 機構住宿式服務類長期照顧服務機構定型化契約應記載及不得記載事項 • 社區式服務類長期照顧服務機構定型化契約應記載及不得記載事項 • 居家式服務類長期照顧服務機構定型化契約應記載及不得記載事項 • 一般護理之家定型化契約應記載及不得記載事項	衛生福利部
金融	• 個人網路銀行業務服務定型化契約應記載及不得記載事項	金融監督管理委員會

	• 電子支付機構業務定型化契約應記載及不得記載事項 • 消費性無擔保貸款定型化契約應記載及不得記載事項 • 個人購屋貸款定型化契約應記載及不得記載事項 • 個人購車貸款定型化契約應記載及不得記載事項 • 信用卡定型化契約應記載及不得記載事項	
	• 第三方支付服務定型化契約應記載及不得記載事項	數位發展部
	• 商品(服務)禮券定型化契約應記載及不得記載事項	經濟部等九個部會[148]
製造	無	
商業暨法律服務	無	

[148] 按商品(服務)禮券定型化契約應記載及不得記載事項之附表「商品(服務)禮券定型化契約應記載及不得記載事項之主管機關及適用範圍」，主管機關包括：經濟部、農業部、衛生福利部、教育部、國家通訊傳播委員會、交通部、文化部、財政部及國軍退除役官兵輔導委員會。

交通	• 汽車買賣定型化契約應記載及不得記載事項 • 中古汽車買賣定型化契約應記載及不得記載事項	經濟部
	• 公路汽車客運業旅客運送定型化契約應記載及不得記載事項 • 市區汽車客運業旅客運送定型化契約應記載及不得記載事項 • 小客車租賃定型化契約應記載及不得記載事項 • 汽車駕駛訓練定型化契約應記載及不得記載事項	交通部

資料出處：研究團隊製表

3、優先評估對象二：其他可能應用人工智慧技術且數位連結較深之商品或服務型態

規範名稱	主責部會

• 即時通訊軟體服務定型化契約應記載及不得記載事項	數位發展部
• 網路連線遊戲服務定型化契約應記載及不得記載事項	數位發展部
• 零售業等網路交易定型化契約應記載及不得記載事項	數位發展部
• 網際網路教學服務定型化契約應記載及不得記載事項	數位發展部
• 以通訊交易方式訂定之食品或餐飲服務定型化契約應記載及不得記載事項	衛生福利部

資料出處：研究團隊製表

4、具體條文建議

(1)、針對國際關注之消費者知悉權利與風險告知等事項，著眼消費資訊揭露制定相應之定型化契約應記載事項

條文內容	說明
第○條　企業經營者所提供之商品（服務）若有實際應用人工智慧之情形，應於商品（服務）提供前，向消費者明確告知下列事項，並確認消費者確已知悉： 1、企業經營者所應用之人工智慧之具體內容。	一、世界智慧財產權組織（WIPO）指出人工智慧並非單一技術，其包括多個細部技術概念，由於實務上可見的人工智慧應用，其使用的人工智慧技術型態往往按個案情形而存在差異，爰企業經營者所提供之商品（服務）若有實際應用人工

2、企業經營者所應用之人工智慧可能衍生之風險態樣與影響程度。 3、消費者在商品(服務)使用上，針對涉及人工智慧部分所應注意之事項。	智慧之情形，應向費者明確告知經營者所應用之人工智慧之具體內容，俾利消費者知悉。 二、現階段我國尚無人工智慧衍生風險之明確分級標準，然國際可見規範已陸續提出人工智慧風險級別概念。以歐盟人工智慧法為例，便將人工智慧系統衍生風險具體區分為「不可接受風險」、「高風險」、「有限風險」及「最小風險及無風險」等四個風險級別。基此，企業經營者在商品（服務）提供上若有應用人工智慧之情形，應將人工智慧應用上可能衍生之風險型與影響程度，以利消費者掌握可能遭遇之風險，並減少其蒙受風險之可能。 三、人工智慧可能衍生的風險，除人工智慧本身即存在或潛藏之風險外，亦與消費者之使用行為習習相關，爰企業經營者除應告知人工智慧可能衍生之風險態樣與影響程度外，亦應提醒消費者在涉及人工智慧的商品（服務）使用上所應注意之重要事項。

(2)、針對國內可能推動之人工智慧立法及關聯規範，制定相應之定型化契約應記載事項要求企業經營者確實遵循

條文內容	說明
第○條　企業經營者所提供之商品（服務）若實際應用人工智慧，應確實遵循商品（服務）所涉及之人工智慧關聯規範。	一、現時國際上已可見著眼人工智慧所推動的專門規範，諸如歐盟於 2024 年 8 月生效之人工智慧法（AIA），而我國國科會亦於 2024 年 7 月預告「人工智慧基本法」（草案），由於我國專法係基本法性質，後續各部會亦可能根據人工智慧基本法就其權責範疇進一步制定關聯立法，爰企業經營者所提供之商品（服務）若實際應用人工智慧，應確實遵循商品（服務）所涉及之人工智慧關聯規範。 二、除人工智慧立法，現時我國已有部會針對人工智慧實務應用發布行政指導文件，諸如金管會針對金融業所發布之「金融業運用人工智慧（AI）指引」，企業經營者於有實際適用之前提下，亦應一併遵循。

(3)、針對國際關注之人工智慧/演算法可能存在的偏見與歧視問題，制定相應之定型化契約不應記載事項

條文內容	說明
第○條　企業經營者所提供之人工智慧商品（服務），不應存有偏見或歧視情形。	一、現時國際組織及主要國家針對人工智慧提出之法制政策，均共通關注人工智慧實務應用上伴隨而生的偏見、歧視、隱私侵害與其他危害問題，爰要求實際應用人工智慧的企業經營者，不得對消費者產生偏見或存在歧視情形。 二、隱私侵害亦為人工智慧實務應用頻繁被提及之爭議問題，惟現時多數定型化契約不應記載事項，多已針對隱私/個人資料保護訂有相應規範，爰本條規定並未納入隱私/個人資料保護。

針對「定型化契約應記載及不應記載事項」如何因應人工智慧趨進行調適，尚須慮及由於消保法之主管機關係各目的事業主管機關，或可能出現難以強行要求各該主管機關進行修正之情形。歷來多數定型化契約應記載及不得記載事項之制定，除部會主動制定者，大抵係由行政院消費者保護委員會作成決議並責成主責部會進行研訂，經部會法規會確認後，再送交行政院消費者保護委員會審查。在數位經濟發展迅速且人工智慧實務應用持續更迭下，後續或有必要於行政院層級，針對包括消費者保護議題在內的人工智慧整體治理推動，建立具指定權限之統籌機制或強化中央部會間之橫向協調機制，以減少因權責或分工不清，導致部會抗拒或消極不配合推動定型化契約應記載及不得記載事項之情形。

另一後續可併同思考之議題，則是隨著人工智慧應用逐步深入各個行業，中長期或有針對人工智慧商品或服務制定「通案性」定型化契約應記載及不得記載事項之空間，並可由相關目的事業主管機關會銜發布。另面言之，考量人工智慧係持續發展且快速更迭的嶄新技術，而不同行業的應用成熟度亦有顯著差異，爰本研究建議持續觀察人工智慧在技術面及實務應用面之發展情形，務實之道仍係擇定與人工智慧有關的特定商品或服務，對應制定或修正其定型化契約應記載及不應記載事項，而非過快制定通案性定型化契約規範。

(四)、法規調適建議：軟法機制（發布行政指導文件）

1、焦點座談暨深度訪談成果咸建議我國可優先推動軟法機制

本研究計畫於 2024 年 8 月 8 目辦理之「人工智慧(AI)商品或服務之消費者保護焦點座談會」，與會專家多數認為人工智慧尚處於發展階段，現時課予過重規範或恐阻礙產業發展，且亦有規範不易之可能，在平衡人工智慧技發展與風險控管之考量下，過早立法反而阻礙人工智慧之進步，初期或宜採取低度管理策略，先軟法（例如制定指引）而後評估必要法制之介入。而接續焦點座談結論所進行的實務深度訪談，受訪專家亦建議推動軟法機制應較立即進行法規調適務實可行。

針對存在高度共識的「軟法機制」，本研究認為可能方向有二：其一係參酌行政院消費者保護委員會過往針對電子商務衍生的消費者保護議題所發布之「電子商務消費者保護綱領」，思考訂定「人工智慧消費者保

護綱領」之合適性。其二則是參考日本消費者保護主管機關：消費者廳之作法，針對人工智慧發布更為軟性之行政指導文件。

有關研商「人工智慧消費者保護綱領」部分，行政院於 2001 年 12 月發布、2017 年 11 月進行修正的「電子商務消費者保護綱領」，係參考 OECD 於 2000 年 3 月發布之「電子商務消費者保護指南」（Guidelines for Consumer Protection in the Context of Electronic Commerce）[149]，惟 OECD 現階段並未針對人工智慧衍生的消費者保護問題，制定「人工智慧消費者保護指南」或任何以人工智慧為主的消費者保護參考文件，從而我國主動訂定「人工智慧消費者保護綱領」，或非最合適策略。

本研究認為現時最適合我國的作法，係參考日本消費者廳推動經驗，日本消費者廳除成立專門小組，研討及梳理人工智慧具體產生的消費者保護爭議問題外，其亦針對可能受人工智慧實務應用影響的消費者，編撰「人工智慧活用手冊」。立於我國消費者保護主管機關角度，研訂諸如日本消費者廳人工智慧活用手冊之行政指導文件，實不失為可行方向。

[149] OECD「電子商務消費者保護指南」，全文可參見：https://www.oecd-ilibrary.org/governance/guidelines-for-consumer-protection-in-the-context-of-electronic-commerce_9789264081109-en-fr（最後瀏覽日：2024 年 10 月 25 日）；

附錄一、參考文獻

(一)、中文資料

- 王澤鑑，侵權行為法，作者自版，增訂新版，2021 年 11 月。
- 向明恩，商品「不符合當時科技或專業水準可合理期待安全性」之再認識－以最高法院 109 年度台上字第 2959 號民事判決為例示，月旦裁判時報，第 139 期，頁 21-35，2024 年 1 月。
- 朱柏松，消費者保護法論，翰蘆圖書出版，1998 年 12 月
- 林昕璇，初探 AI 自動化決策下之差別待遇－以美國法為鑑，開南法學，第 14 期，頁 79-123，2023 年 2 月。
- 郭戎晉，人工智慧風險治理與監管機制建構之研究－以歐盟監管專法（AIA）與美國風險管理標準為核心，世新法學，第 17 卷第 1 期，頁 109-221，2023 年 12 月。
- 郭戎晉，論人工智慧技術應用、法律問題定位及監管立法趨勢－以美國實務發展為核心，成大法學，第 39 期，頁 180，2020 年 6 月。
- 姜志俊，消費者保護法，國立空中大學，修訂再版，2020 年 8 月。
- 洪誌宏，消費者保護法，五南出版，五版，2021 年 6 月。
- 許政賢，臺灣消費者保護法的創新與挑戰－二十週年的反思，月旦民商法雜誌，第 45 期，頁 38-55，2014 年 9 月。
- 陳煥武，智慧醫材之當時科技水準探究與規範調適—從傳統醫療器材判決出發，高大法學論叢，第 19 卷第 2 期，頁 1-57，2024 年 3 月。
- 陳聰富，民法債編總論（一）：侵權行為法原理，元照出版，3 版，2023 年 11 月。
- 劉靜怡編，人工智慧相關法律議題芻議，元照出版，2018 年 11 月。

(二)、日文資料

- 落合孝文，AI に関連する消費者被害の対応について，消費者のデジタル化への対応に関する検討会 AI ワーキンググループ（第 4 回）会議資料，2020 年 5 月。
- 消費者のデジタル化への対応に関する検討会 AI ワーキンググループ，消費者のデジタル化への対応に関する検討会 AI ワーキンググループ報告書，2021 年 7 月。
- 消費者庁，AI 利活用ハンドブック，2021 年 7 月。
- 消費者庁，AI 利活用ハンドブック：生成 AI 編，2024 年 5 月。
- 消費者庁，第 1 回消費者意識調査結果（AI に対するイメージについて），2024 年 4 月

(三)、英文資料

- Allenby, Braden R., *Governance and Technology Systems: The Challenge of Emerging Technologies*, in The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight (Gary E. Marchant *et al*. ed., 2011).
- Bollier, David, Artificial Intelligence, The Great Disruptor: Coming to Terms with AI-Driven Markets, Governance and Life, y The Aspen Institute (2018).
- Department for Science, Innovation & Technology (UK), The UK Science and Technology Framework (2023).
- Gaske, Matthew, *Regulation Priorities for Artificial Intelligence Foundation Models*, 6 VAND. J. ENT. & TECH. L. 1 (2023).
- Giacobbe, Thomas, *Adapting to Challenges Posed by The Fourth Industrial Revolution: A Regulatory Call to Action Concerning Cybernetic Technology*, 15 WASH. U. JURISPRUDENCE REV. 141 (2022).

- High-Level Expert Group on AI, Policy and Investment Recommendations for Trustworthy Artificial Intelligence (2019).
- Leenes, Ronald et al., *Regulatory Challenges of Robotics: Some Guidelines for Addressing Legal and Ethical Issues*. 9 L. INNOVATION & TECH. 1 (2017).
- Madiega, Tambiama, Artificial Intelligence Liability Directive, European Parliamentary Research Service PE 739.342 (2023).
- McAfee, Rock, Daniel & Brynjolfsson, Erik, *How to Capitalize on Generative AI*, 101(6) HARVARD BUSINESS REVIEW 42 (2023).
- Office for Artificial Intelligence (UK), National AI Strategy (2021).
- PricewaterhouseCoopers, Sizing the Prize What's the Real Value of AI for Your Business and How Can You Capitalise? (2017).
- Stanford Institute for Human-Centered Artificial Intelligence, Artificial Intelligence Index Report 2022 (2022).
- The White House, Guidance for Regulation of Artificial Intelligence Applications (2020).
- The White House, Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People (2022).
- UK Government, A Pro-innovation Approach to AI Regulation (2023).
- United Nations Conference on Trade and Development, United Nations Guidelines for Consumer Protection (2015).
- World Intellectual Property Organization. WIPO Technology Trends 2019: Artificial Intelligence (2019).

附錄二、「人工智慧(AI)商品或服務之消費者保護焦點座談會」紀錄

人工智慧(AI)商品或服務之消費者保護焦點座談會

會議時間	民國 113 年 8 月 8 日下午 2 點	
會議地點	線上會議	
計畫主持人	南臺科技大學郭戎晉	
與會人員	A	陳先生，法律學系教授
	B	計畫協同主持人林昕璇
	C	徐先生，基金會副董事長
	D	黃先生，公會法務長
	E	計畫專家顧問邱映曦
	F	楊小姐，政府機關處長
	G	王先生，消保官
	H	溫小姐，法制處專門委員
	I	呂小姐，政府機關簡任秘書
	J	柯小姐，消保官

發言內容：

計畫主持人：

非常大家感謝百忙之中來參與我們今天的人工智慧商品或服務之消費者保護焦點座談會，我是今天的會議主持人，非常榮幸可以邀請到我們消費者保護團體、學者專家、產業界的先進，以及來自於我們中央跟地方的相關的主管機關包含國發會、臺南市政府、消保官。今天暫定是兩個小時左右的時間，會先簡要介紹與會的貴賓，再用 15 分鐘左右時間，針對我們討論的主題。而 AI 本身我相信大家都已經耳熟能詳的議題，各行各業、各中央部會都一定會受到一個趨勢的影響，所以大家應該也在思考在

自己的一個圈子範圍之內，我們怎麼因應帶來的影響。從消費者保護的角度，在國內消保法這一塊來說的話，從過去的實體到網路的環境，到現在我們談所謂的 AI 全面應用的情況底下，消費者保護法有沒有必要做一些對應的調適，這就是我們今天最主要的討論目的。所以說在前面部分的話，我大概就國際跟國內的狀況做一個初步的一個探討。在目前的話，還是一個進行中的會議，今天大概是偏向初步的意見收集，所以也希望大家不要有任何的顧慮，踴躍提供你的意見，所以我們初步設定一些相關的討論議題，主要針對於我們所看到的人工智慧，對於我們的消費者保護帶來的影響，以及站在我們國內來說的話，我們的消保法有沒有需要做一些對應的調整，那如果有的話，可能的調整方向是什麼？這個大概是我們今天最主要的一個討論方向。

接下來我進行報告之前的話，先介紹一下我們今天的與會的貴賓，今天包括我個人非常尊敬的我們（A）老師，（A）老師本身的話是美國喬治城大學的法學博士，不管是在金融，在公平法在消保法，及科技帶來的一個法治的衝擊，長期都給我們非常多寶貴的意見，第二位來自於學界老師是（B），也是這個計畫的協同主持人，他是美國維吉尼亞大學的法學博士，本身除了公法的憲法行政法的專業之外的話，這幾年對於在人工智慧這一塊的法治的研究也有深入的一個探討，所以這個計畫特別委託（B）老師，可以從 AI、公法角度來看一下，我們在消費者保護可能產生的問題。而第三位，也是我們長年合作的好夥伴，是我個人非常尊敬的學長（C），本身就是在消費者保護領域，在消基會這邊的話，長年投入，目前的話在基金會是副董事長，不管是在實務或法治的角度，我相信（C）都可以給我們非常寶貴的意見。第四位，是我們公會的（D），過去在網路的連線遊戲、網路的教學、定型化契約應記載不得記載事項，法務長在這個部分也長期投入在消費者保護領域，還包括跟產業界的一個相關的互動，所以也會來麻煩法務長可以從產業界或產業趨勢給我們一些相關寶

貴的意見。第五位是（E），本身是政治大學的法學博士，在科技法還有公平法跟消保法也有長期的一個投入。接下來，是在公部門的幾位專家，首先是來自於政府的（F），過去也是臺南市的主任消保官，這次特別商請處長，可以從過去對於消費者保護的經驗，以及從中央角度來看待 AI 對我們產業帶來的衝擊。再來是我們的好朋友（G），因為整個產業特性，過去包括在一些科技產業、整個數位產生的一個消費者保護議題，也都有一些長期的投入，所以我們也非常榮幸可以邀請到消保官參與我們這樣討論。接下來是在整個有關於人工智慧這個法治本身來說的話，就有兩個非常重要的單位，一個是在中央擔任法制協調的（H），以及在整個消保法本身的主管單位消保處的兩位長官，（I）與（J），今天也會分別從整個國發會及從消保處的角度，最後對今天討論議題給我們一些指導。在此非常榮幸今天可以邀請到這麼多各方面的專家來參與我們的討論。

針對於一個人工智慧商品或服務的消費者保護議題來說的話，第一個部分當然就是人工智慧本身是忽然之間變成是一種顯學，其實人工智慧概念出現的時間是非常早，從機器人概念到人工智慧的基本原則，這個名詞在 1956 年開始被界定下來，只要不是人類所表現出來的智慧都可以被歸類為人工智慧。而早期人工智慧比較是屬於這種，所謂的是跟非或給出一個唯一的答案，但這兩年所謂的生成式的人工智慧，從無中生有、創造，不管是文字圖像，甚至程式碼，都可透過人工智慧快速的創造。所以忽然之間人工智慧更加地貼近我們的生活，我們忽然感覺到人工智慧好像是無所不在。而在整個人工智慧本身的話，今天如果看它的議題，第一個就是怎麼去界定人工智慧，早期人工智慧比較偏向從技術的角度，在世界智慧財產權組織（WIPO）就嘗試從技術，因為大家對於人工智慧的話，一般面都會談說，我申請哪些人工智慧相關的專利，所以 WIPO 就把人工智慧，從專利角度去界定有哪些子技術，他強調一個概念就是沒有一個技術就叫人工智慧，人工智慧其實是不同的技術所組合而成的，所以包括

看得到跟看不到的，像是機器人本身有外體，但是機器人怎麼運作，他可能需要大量的機器運算、需靠視覺的辨識，或像我們現在手機裡面的語音助理，他可能需要有很長的一個語音語義的辨識，像很多的即時翻譯、很多的生成式人工智慧，都是透過不同技術的組合。而現在大家慢慢的會去關注，就是我們要來解決人工智慧可能衍生的風險的話，除了人工智慧這樣一個用語之外的話，更多開始被使用叫做人工智慧的系統，那這個用語是從 OECD 在 2019 年的時候，他就說最早對人工智慧認定就是非人類所表現的智慧，所以基於機器的系統，可以根據我們所下的指令給她的目標來創造出預測建議或決策，所以目前的話包括在大家所關心的歐盟的人工智慧法，基本上規範的對象就不是人工智慧這四個字，而是人工智慧實際運用的時候的人工智慧的系統，所以這個在目前的話，包括 OECD、歐盟本身在這個月 1 號正式運作的人工智慧法，他們的規範主體都叫做人工智慧的系統，但是人工智慧到底要不要管，在國際上一直是引發一些爭議，所以早期的話，當生成式人工智慧還沒有被那麼重視之前，有時候我們會覺得人工智慧距離我們還有一些距離，頂多就是下棋下贏人類，當時是比較偏向是從一些科幻電影當中，會看到人工智慧帶來影響，最早期比較偏向是從自律、倫理道德的角度，可是人工智慧越來越進入到生活，所以從自駕車到自動理財的相關程式，到現在的 ChatGPT 生成式人工智慧。忽然之間，大家覺得這個人工智慧應該要立法，所以從自律開始進入到他律，而他律的部分的話又會分成我今天是要全面性的定義一個管制專法還是分散式的立法，還是說比較正在發展的角度，訂一些基本法就好，所以其實在國際上面對於人工智慧的一個立法，目前還是一個分歧的，最大的方向就可以分成，要不要立法跟不立法，在立法的話，又有不同的立法管制密度的選擇，所以這個是一個我們這一次，大概主要選擇 4 個主要的國際組織或國家，包括最代表性的歐盟，從一開始就覺得人工智慧應該要管，而且是要訂一個全面性的監管專法，所以目前的話除了歐盟之外，

我們也看到像加拿大、巴西幾個國家受到歐盟影響，他們覺得應該要定義一個監管專法，美國不反對立法，但他認為這個法本身就根據各個部會的需要，也就是等於是說分散式的讓各個部會決定要不要立法，所以他不是說一定要訂一個所謂的監管的立法，比如說針對租稅、科技研發等，會有所謂的分散式立法。英國、日本，其實跟美國很像，就是這種人工智慧的話，原則上是站在一個比較務實的角度，所以除了部門立法之外，更多的可能會變成是用一種鼓勵的角度，所以這是一個在國際的話，目前有全面性立法的話，以歐盟為主，而且歐盟本身的立法來說的話，並不是一種所謂的基本法概念，是一個作用法，而且是一個高度管制的作用法，所以在整個歐盟本身的話，從 2021 年就開始推動這個立法，中間又經過 2、3 年的討論，在上個月已經正式在歐盟公報發布，發布之後 20 天生效，在這個月 1 號的話，歐盟本身的人工智慧法已開始生效，裡面的話大概是兩個規範的邏輯，第一個就是針對剛剛所提到的人工智慧的系統，它用風險分級的概念，也就是今天在實務上面可以看到人工智慧的應用的話，我就根據所制定的風險分級的標準，看看你落在哪一個等級最嚴格的，我是完全禁止你使用的，相對的風險比較低或沒有風險的話，我就不做管制，所以中間的話就不同的一個管制的力道，另外一塊就是針對 ChatGPT 生成式的人工智慧，這個是歐盟在後期才加進來的概念。一開始他比較偏向是一般的人工智慧系統規範，後來才開始加入生成式人工智慧，所以在整個歐盟本身的規範來說的話，今天對於所規範的人工智慧，就會分成是一般的人工智慧系統，還是生成式人工智慧，而一般的人工智慧本身又會因為處於這 4 個風險等級，而這 4 個風險等級本身來說的話，這邊找了一些案例來做個參考，比如說這種不可接受，會扭曲人類本身的意志的、對人打分數、用來做犯罪的預測或全面性監控的使用等，歐盟是說完全禁止的，有些是可以讓你用的，也就是除了不可接受風險是完全禁止之外，其他你可以用，但是你可能要接受一些很嚴格的規範，所以高度風險像

生物辨識，他就必須要符合裡面，包括一個上市前的監控、持續性的控管，有些風險的話比較自重在所謂的資訊的揭露，那低風險跟無風險原則上是不受管制的，但你可以自願性地去遵循行業所訂的行為準則，所以說這個是在整個歐盟來說的話，針對人工智慧的應用，他用風險分級的概念。在目前的話，8 月 1 號正式生效之後，並不是說所有的人工智慧系統馬上收到管制，因為這是一個非常新的立法，而且我們對於人工智慧的風險分級標準，事實上可能還是會有一些模糊的地帶，所以歐盟他是採取漸進式的做法，也就是在正式生效之後的話，逐步設定一個實施的時程表，包含從 8 月 1 日開始起算 6 個月、9 個月、1 年、1 年半，到整個 2 年、3 年。雖然說 8 月 1 日整個人工智慧法已經生效，但要到半年之後，無法接受風險才會被全面禁止，而生成式人工智慧本身的這個實務操作的準則是在 9 個月之後才開始運作，那高風險要等到 1 年半之後才會正式的進行規範。如果今天國內的立法方向是比照歐盟的話，那就是一個高度管制的作用法。但是我們來看到在國內的狀況，目前的話在國內本身來說的話其實是非常早，大概我從立法院的這一個公報系統，其實 2019 年甚至比歐盟更早，我們當時就立法委員打算訂人工智慧發展的基本法，但是這個部分的話也就決定我們臺灣在人工智慧的法制推動，不管是從立委的版本、學者的版本或上個月國科會所公告的官方版草案來看的話，目前我們的人工智慧本身的立法都比較偏向是屬於基本法的型態，所以在目前的話，國內從立法委員、學者到國科會本身提出來版本是比較偏向是基本法，與歐盟本身的作用法的立法會有一點點定位跟性質上面的一個差異。所以在國科會正式立法之前的話，這一塊到底是自律或他律，行政院本身對於要不要立法，曾經有過相關的討論，先前的話大概是以所謂的自律制定這種行政指導為主，但是在上個月的話，已經有國科會正式公告，當然我們說基本法本身還是比較偏向是一種所謂的促成或比較偏向是一種軟性的立法規範，所以說整個人工智慧的基本法大概有 18 條的規定，裡面

就會提到政府應該做什麼事情，但做什麼事情？怎麼做？可能還是要回到相關的權責部會或目的事業主管機關，所以這個是整個人工智慧基本法草案初步的一個分析來說，條文當中並沒有一個所謂的消費者保護的專條規定，全文本身也找不到任何有關於消費者保護和消費者的字樣，這一個是從整個人工智慧基本法，但裡面也許有些部分規定還是會跟消費者保護有一些關聯性，所以這邊的話，我大概先列出兩個最直接的，包括草案第 9 條為了避免人工智慧的一個風險性，這個部分他要求應該針對這種利益衝突、偏差、廣告不實、資訊誤導或造假問題，應該要盡量的去避免它，但是怎麼避免？到底會涉及到哪些法律的規定，這些法律本身應該怎麼去處理這個問題，這個部分可能就變成是怎麼去落實，作用法之後，各個部會所要思考的，另外一個可能是在第 12 條針對人工智慧部分，參考類似歐盟這樣想法，針對人工智慧，我們應該要進行風險的分級，所以透過標準驗證、檢測、標記、揭露、溯源或問責，這一塊可能會跟當人工智慧產生的法律責任時，這個責任怎麼做分配？同樣的，當人工智慧的商品或服務造成消費者的生命、身體或財產受到損害時，這樣原本消保法裡面的法律責任的設計，是否能對應到人工智慧的商品，可能也會跟我們草案第 12 條產生一些相關的討論。如果今天回到上個月國科會所看到的這個人工智慧，我們臺灣準備要立法，但我們的立法跟歐盟的監管立法，事實上是有一個性質上很大的差異，目前所看到的條文當中，比較沒有完全是對應到消費者保護的，所以今天站在一個消費者保護立場，回來看臺灣本身來說，人工智慧的商品跟服務，可能會碰到的消費者保護問題，這大概是目前研究團隊我們初步所設定可能的一個相關議題。當然是一個初步方向，如果大家有任何想法都可以提出來討論，所以說人工智慧對於整個消費關係會不會產生影響？人工智慧的商品跟服務開始上市之後，要不要有適當的消費資訊或必要的資訊揭露，另外消保法本身安全性的要求，符合當時科技水平的安全性，這樣安全性怎麼去做確保？以及大家所

關心的，除了事前要求之外，當它產生法律責任，事後的問責在消保法怎麼做處理？所以這是一個我們所初步設定的幾個可能跟消費者保護有關的議題，有關於在商品跟服務本身來說的話，目前人工智慧有可能會被界定為是消保法的商品跟服務，另一個是人工智慧本身可能是過去像我們所謂通訊工具的概念，比如說智能客服，可能會促成消費關係的締結，但是人工智慧本身有可能就直接作為一種商品跟服務的概念，包括在歐盟本身的人工智慧法，他其實有提到類似的概念，就是人工智慧本身就是一種商品或人工智慧可能是屬於商品或服務重要的組成部分，比如說他可能是裡面的一個暗控機制或一個重要的功能，所以不管是作為一種機能，還是他本身可以作為商品跟服務，像是語音助理或自駕車本身，人工智慧的確有可能是直接成為消保法所保護或規範的對象作為一個商品跟服務，另外的對於一個消費資訊揭露，我們在整個目前消保法本身來說的話，一個是在總則當中有提到我們應該要向消費者說明商品跟服務的使用方法，或提供消費者充分更正確的資訊，另外的在我們的消費資訊的規範當中的話，比較有關聯的可能是對於廣告內容的真實性、依照這個商品標示要求，做商品跟服務的標示，這樣一個消費資訊揭露，對比歐盟本身的規定來說的話，在這種風險等級，還有不同的風險等級應該所揭露的這樣一個相關資訊本身來說，是不是能夠直接用消保法本身現有的規定來做要求？這可能是後續可以再做思考。還是要透過像定型化契約，因為消保法本身是整體性的對於商品跟服務的規範，不同商品跟服務的種類是不是能夠做到？因為不見得每一種商品都用到人工智慧，如果要求對應的資訊揭露，那是不是更好的做法，是不是回到對應不同商品跟服務的定型化契約當中去做要求會更合適。所以這是在第一個議題，有關於必要資訊的揭露。第三個就是針對於可以合理期待的安全性。因為人工智慧存在風險，為什麼歐盟要立法，一個很重要的考量，甚至包括不同的風險等級，相對的它所帶來的危害跟對應安全性的要求也會產生差異，在我們消保法本身的

第 7 條當中，就提到商品跟服務的提供應該要符合當時的科技或專業水準，可以合理攜帶的安全性，這也對應到我們剛剛看到的，即便臺灣目前要考慮訂的是一個基本法，但基本法當中，我們也提到風險分級或風險的評測。所以說未來怎麼去確認這樣一個人工智慧的商品跟服務到底有沒有符合當時的科技或專業水準，可以合理期待的安全性？這個是我們現有消保法的規定，怎麼去對應這樣子一個有關於安全性的要求。當然我們對於所謂的消保法本身第 7 條裡面的安全性來說。相關的規定包括第 7 條之一當中的舉證責任是由事業、企業經營者這邊負擔，另外一塊，怎麼去確認安全性，我找大概歷來消保法相關的函釋，比較直接的大概是在先前消保處前身的消保會時，曾經做過一個類似函釋，他認為到底有沒有符合第 7 條的話，第一個是看第 7 條之 1 裡面，不可因為事後有較佳的商品跟服務，而被認為不符合，當然這個就是我們第 7 條之 1 第 2 項規定的直接原因，另外也是條文的直接原因，就是未來在判斷人工智慧的商品跟服務來對應第 7 條的安全性要求，大概我們在施行細則第 5 條，這 3 款的規定可能是一個指標，到底有沒有做清楚的標示說明，到底是不是被期待的合理使用或接受，以及他進入市場或提供的時期。這 3 個規定到底能不能完全去充分地反映人工智慧本身可能存在的風險，或它對應的安全性要求，這也是我們在後續會再進一步做了解的，針對現行消保法有關於第 7 條本身的安全性關聯的規定跟函釋，這邊大概初步做了一些整理。所以這是一個我們大概初步所預想的方向，當然這可能不見得完全成熟，所以第一個部分就我們在消保法本身要不要對應的法規調適？目前看起來，按照我們目前所預設的話，在國科會這邊提出並不是一個像歐盟一樣的作用法，因為如果今天是一個非常明確的作用法，也許我們就完全依照這個作用法規定來處理，但是目前我們只是以國科會本身來說，它是屬於一個基本法的性質，而這個基本法本身的要求怎麼被落實？回到消保法本身，我們要不要對應的法規調適？這可能在這一個研究案之後，會提供

給行政院消保處做參考，因為如果以作用法定位來說，可能就不完全能夠依照作用法本身做一個有效的處理，可能還是會回到各個部會或各個法令主管機關的權責範圍之內來做思考。而上個月國科會已經有人工智慧法立法的提出，但並不是一種類似歐盟的作用法，只是屬於基本法的性質，所以說消保法本身。包括我們所看到的關於消費關係的成立、消費資訊的揭露、可合理期待的安全性及法律責任的處理上，現有的規定是不是能夠完全充分對應到人工智慧所帶來的問題，這個可能是一個我們要思考的方向，另外在整個消保法作為一個消費者保護的基本法的情況下，是不是完全立即地適合做變動，還是對應不同的商品或服務的特性，而思考是透過所謂的定型化契約。如果站在我個人立場，我會覺得這反而是更快，而且相對的變動和衝擊影響會比較小的，但是哪些商品跟服務所涉及到的定型化契約有需要針對人工智慧做一些調整，這也可能是我們之後，會逐一地針對定型化契約做一個檢視，所以定型化契約如果要變動的話，一個可能性是在應記載或不應記載事項當中增加對應的規定，比如說應記載裡面，增加資訊的揭露或不應記載事項的話，針對人工智慧這種潛在的風險性，比如說歧視問題或隱私侵害，這些大家比較關心的，是不是列入到不應記載事項，所以在整個定型化契約的話，分別從應記載跟不應記載可能都有一些對應可採取的操作做法。最柔性的做法，當然就是因為人工智慧還是一個發展中的概念，它具體產生的風險到底有多少的商品跟服務可能會受到影響，當都還是不確定性的時候，是不是有可能透過一個比較屬於行政指導軟法的方式，如同過去我們在網路剛開始出現時，一個電子商務的消費者保護綱領，透過一個行政指導的方式給予一個比較屬於建議式的做法，這也是目前初步我們所想到，在不同的一個法規調適做法當中，哪些是比較容易的，哪些是影響比較小的，我們後續也會做一個排序，提供給消保處做參考，以上是我針對今天所討論的議題，做一個初步的法

治研究跟幾個建議方向，所以大概有幾個議題，今天就交給各位學者專家來討論。

（A）：

我覺得 AI 時代的來臨，對我們帶來很多方便，也有很多的問題，現在整個世界的趨勢看起來，AI 實際上是不會被完全禁止，而且會慢慢的發揮影響力來影響到大家，對於 AI 跟消費者保護，我想這個議題是非常重要，尤其是 AI 時代來臨之後，消費者往往會不知不覺地處於一個弱勢的。剛剛主持人也把研究成果一部分展現出來，我覺得這已經非常的完整，我想可能有一些不同切入點的角度，來跟主持人及各位長官學界的學者專家做報告。我認為 AI 跟這個消費者的商業互動模式，可以分為兩類，一種是被動式，一種是主動式的，被動式是消費者實際上他不知道他在被或消費行為的在跟 AI 發生關聯，比如說消費者的個資、生物的特徵、聲音、面貌、影像，還有他的消費偏好及消費者能力，實際上在消費者不知不覺間就會被收集建檔，然後被分析判斷利用，這時消費者實際上並不見得都知道。關於美國其實發生好幾個的例子，像是生物特徵的聲音，在美國就有商店，專門蒐集小孩子的聲音，如果說聽到小孩子的聲音進店裡，馬上 AI 就傳訊息給店員，告訴店員說有家長帶著小孩子進來，店員就會針對小孩子做一些推銷。很多的時候，把小孩的需求照顧好，家長自然就會買單。但涉及到收集小孩子的聲紋，這時到底這樣有沒有問題？在美國的話，就會有兒少保護的問題。這個實際上也是一個例子，今天消費者在消費時，往往並不知道，他其實跟 AI 發生聯繫，這時顯然就隱私跟個人資料保護的問題，消費者知情權有沒有選擇退出權這往往是一個重點。

這邊就提供另外一個例子，這是 2023 年 12 月 9 號，美國的三大藥妝店 Rite Aid，從 2012 年時，就開始偷偷地收集消費者的 AI，消費者的面部特徵，再根據面部特徵建立一套資料庫，而這資料庫有時候還會更新，

因為消費者會來客訴、退貨，消費者就會填上一些自己的資料，甚至成為會員，所以他就把資料庫的面容漸漸地補充起來，就會包含他的姓名及其他個資，使數據越來越完整，而建立資料庫的目的是什麼？就是要抓潛在的小偷，他發現說某些面部特徵，並非已有前科才警示，他認為 AI 能判斷長這個樣子的很可能是小偷。就像剛剛說的兒童聲紋一樣，他沒有辦法人盯人，1 比 1 的配對店員跟客戶，所以必須要把人力用在刀口上，而剛剛那是為了賺錢，你要去照顧小孩子的需求，另外這個是為了防弊，所以他就把有限的人力配置在高竊盜風險的客人，發現可疑舉動時，可以要求搜查、報警。他完全沒有告訴各位有這樣技術，這個技術實際上從 2012 年就有，若去搜尋一下美國海關也有類似的做法，往往於判斷上要不要落地簽證時，就會用面部的特徵、其他方式來判斷可能會有非申請目的拘留，甚至有跳機的問題，這時 AI 的使用就產生很大的問題。

在美國的聯邦貿易委員會當中，比較相信的公平交易委員會，他就跟這個 Rite Aid 達成和解，這個和解就是說今天聯邦貿易委員要求 Rite Aid 在 5 年之內不能再用 AI、也不能再用 AI 面部識別系統。這個採去年年底的故事，就告訴我們 AI 實際上就會影響很多，像這個就是歧視性錯誤性的決定，因為他並不是完全準確，但也有可能補助企業者做出一些歧視性錯誤性的決定。再來 AI 可能也會提供消費者不實的商品或服務資訊，使消費者做了一些錯誤的消費決定，更可能使用暗黑模式。剛剛的簡報，也提到對人性（消費者）的操弄，這個本身也是 AI 的問題。當然 AI 對消費者保護非常的困難，因為在商品上 AI 的使用，如果是純粹應用 AI，像是 Chatbot、ChatGPT，那還比較容易，但今天在商品的製造、運送、販賣、進出口及零售，每一個環節使用 AI 的程度不同，這時如果在任何一個環節中使用 AI，是不是都應該讓消費者知道，譬如說像經銷商、生產商沒有揭露 AI 的使用，誰要負責？在美國也發生一樣的例子，雖然這不是 AI，而是生產商的消費者爭議，但我把它加入 AI，當在生產時，很多

實例也添加電腦化的自動化生產，這時他錯誤的添加一部分麩質成分，由於美國人因體質的關係，很多人對於麩質過敏，但沒有在外包裝標示，進口商也不知道，也沒去檢驗，根本也不知道這食品含麩質成分，結果有一個消費者，因為誤食該產品後嚴重過敏休克，那這樣誰要負責？在美國常常也有發生很多的事，像這一些使得 AI 的規範是很困難的問題，因為今天一個商品或服務的提供，不是單純的使用 AI，可能有一部分使用 AI，那到底要多大部分都要揭露，還是說只要一碰到就要揭露？還是說程度的問題？這時本身就是一個很難的問題。

在英國的例子，在去年的 4 月 25 日向下議院提交《數位市場、競爭和消費者法案》，提到說任何人提供涉及到 AI 的產品或服務，只要有涉及到跟消費者健康相關的解釋必須要清楚，而在消費者使用該商品或服務之前，要事先給消費者告知或同意，把醫療 informed consent 到時候同一運用到這邊，或事先已給了告知或同意後，他可能就會有一個概括授權，但要讓他有機會去撤回先前給的告知或同意。這也是可以讓各位一起來思考、參考，以上的淺見跟各位報告，謝謝。

計畫主持人：

在歐盟本身，現在很多的 AI 法案裡面確實會提到像提供者或 AI 系統的部署者，也就是 AI 本身來說，它是產品或服務提供，還是說他是實際所使用的，而這個對應到我們消保法，這的確是我一開始思考這議題還沒有完全往這方向想，因為我們消保法本身的企業經營者其實範圍很廣，包括設計、生產、製造、輸入跟經銷，所以這的確是未來在人工智慧商品跟服務的話，我們這麼廣泛的企業經營者的範圍跟對應到現在人工智慧的法裡面所規範的提供者，這個範圍到底一不一致？我們之後會納入到我們的一個研究的範圍。

（B）：

如同計畫主持人所報告，我們希望可以把消費者所衍生的這些相關問題，簡單的濃縮人工智慧對消費契約關係締結所生的影響、有關消費資訊揭露的要求、在產品跟服務他在進入市場上所可能造成的一些安全性的疑慮，以及各種暗黑模式的資訊操弄跟虛假問題。目前綜觀各國，大體上在 AI 跟消費者保護議題上，都可以以最大公約數劃約為這四大議題，所以我們會透過這四大議題，進一步的再去觀察，包括日本、英國、歐盟跟美國這四大法系，但其實也可以更進一步簡化為硬法跟軟法。在歐盟透過這種風險層級嚴格、差異化的這種規範模式、訴諸產業自律跟企業自律標準，包括美國、日本、英國，在我們目前的研究發現當中，都採取比較彈性，給予主管機關裁量權限或業者裁量權限這樣的規範模式之間，究竟臺灣適合哪種規範模式，或哪一種規範模式跟臺灣目前現行的消費保護法相關制度能夠更無縫銜接？這也是我們後續會再討論的問題，在這研究過程當中，我們也發現 AI、巨量數據或是 AI 驅動的這些產品跟服務，其實類型化下，它會產生非常多繁複而多元的樣態，我稍微舉個例子，像是一些包含智慧元素的，標榜人工智慧驅動冰箱的智慧家庭設備，但也可能是像 Siri、Google assistant 或 Alexa，他們這種訴諸語音的翻譯或會訴諸一些情感元素跟高度個人化需求的 AI 產品，其實跟智慧家庭設備，在整個規範上面的密度或著重點可能完全不一樣，甚至前一陣子受到各界的矚目的無人車、自動駕駛的問題，他更甚至著重在怎麼樣去提供導航功能能夠兼顧用路人的安全跟防控機制的設計，怎麼樣去控制車輛的特別著重加強跟強調怎麼樣確保進入市場時是絕對具有安全性的。所以這些一語概之的 AI 產品跟服務其實很難以單一的標準，one pick all 方式法規化，所以這個也是在研究推展過程當中發現的一些問題，如何透過差異化或類型化有沒有一個標準可以差異化這種 AI 的產品跟服務？其實各種各樣的 AI 跟產品服務所衍生出來的法律責任跟規則的判斷基準其實也會產生非常大的差異。所以之後也會再借重日本跟美國一些訴訟裁判的經驗，

也就是說這些 AI 商品跟服務。他發生了事故糾紛或是發生侵權行為責任後，他進入到法院體系，法院可能提出什麼樣的裁量標準，後續我們研究團隊會再進一步去深究，而目前研究的進程也稍微觀察的一些美國的產品責任法，因為美國是 AI 的領軍大國，已經有相當多的訴訟案例跟裁判實務，進入法院當中裁判，所以大體上稍微去關注一下，包括伊利諾州、德州、南卡羅萊納州一些地方法院的判決，我們發現特別注重在歸責原則，這些產品跟服務他在進入法院後，它的歸責原則是要採取所謂的嚴格無過失責任，或是要怎麼樣替 AI 的產品跟服務訂立一個過失規則標準，那這個大概都是可以一般性的、通案性的在各個州的法院都可以看到類似的討論。所以目前這個部分，在美國的產品責任法當中，有關 AI 產品的歸責原則也是他們一個很重要的爭議點，目前到底要針對這些軟法的法律標準，最重要被視為到達什麼樣的注意義務，違反什麼樣的注意義務就可以歸責這件事情，還是有一定的爭議性，不過大體上是會採取商品的嚴格無過失責任，這個我們也會再進一步的研究。另外一個是行為跟損害結果怎麼樣去判斷商品跟服務，最後造成的這些人身損害或利益損失兩者之間是具備因果關係鏈結的建立？其實在美國也有一些相關標準，不過美國的法院非常明確的去強調，這也回應他們是訴諸軟法及非常強調業界標準、習慣跟業界實踐的這種證據法則，他們大體上歸納為怎麼認定兩者之間的因果關係，以及這個規則的標準在這個部分業界的標準、習慣跟證據，包括像 ANSI 非政府組織的業界機構，實際上採取的這些習慣跟實踐的證據，通常都會成為法院一個重要的決定性判斷依據，而這些設計的缺陷，同時也會透過消費者期望的測試來評估，比如說法院就會去測試公眾對這樣的一個 AI 產品，消費者合理期望的假設水準到何處，所以這些也會透過消費者期望測試來評估，不過大體上都不是透過硬法，這個還是反映美國他們非常側重，以及貫徹軟法的基準。回到我國的消保法，第 7 條怎麼樣去確保該商品跟服務在符合當時科技或專業水準可合理期待的

安全性這部分，以及在第 7 條第 3 項也有去訂立企業經營者的過失責任歸責基準的部分，我想我們的研究團隊會在繼續去深究一些美國法院，針對這一類型的案件的裁量基準。但目前美國法院針對何謂符合當時科技或專業水準可合理期待的安全性，就如同我剛說的透過一些消費者測試或業界基準來去衡量 AI 的產品是不是已經符合當時的科技跟專業水準可合理期待的安全性，以及這些無過失責任。我們期待在後續的研究當中，也可以從一些美國法制來窺知一二。因為時間的關係，把時間留給後續的專家學者，謝謝。

（C）：

很開心政府終於開始重視到這個問題，AI 對於消費者的權益所產生的影響，我認為已經發展一陣子，業者利用 AI 對消費者的權利已經侵權一陣子，過去似乎政府或業者沒有盡太多的努力在這個方向，因此很開心終於有人重視這個議題。剛剛有聽到（A）和（B）都有介紹到國外的一些立法例、案例的解析，我才知道原來其他的國家早已針對於業者或消費者之間權利的侵害，已經有一些立法例，甚至有些真正的判決出來。反觀我們國內到目前除了消保法以外，還沒有什麼比較能夠適用的一個法律依據，希望我們國內的法治要趕快加油迎頭趕上。

舉幾個例子好了，為什麼說 AI 早已被一些業者利用在他們的服務上，對消費者的權利產生影響。如果說自駕車目前進行到 level two 這個階段，是按照業者的說法，手必須要放在方向盤上，但很多藝高人膽大的消費者，在使用汽車自駕功能時，並沒有遵照業者的指示，業者也很清楚消費者不可能完全遵照，像是新聞中，在高速公路上自駕功能的汽車撞到高速公路上的防撞車造成嚴重的事故，我實在是覺得很奇怪，業者就已經明明知道自駕功能沒有辦法辨識我們高速公路上的防撞車，難道沒有辦法去改善嗎？既然已經發生真實的案例，造成消費者或第三人死傷、財產損失，那

這時責任應該怎麼去釐清？難道業者完全沒有責任？就目前是沒有一個很具體的法律制度可以適用，因此變成每個個案都要由法院具體的個案認定，這樣等於說無形當中，又增加法院的這個負擔，對於消費者來講，我認為是滿沒有保障的，至少就自駕車這個發展的迅速，應該要盡快做出一些規範。不過目前關於車輛的定型化契約，我們現在只有車輛的買賣，對於汽車銷售給消費者後，就沒有什麼定型化契約，所以未來可以思考，可能需要立一個基本法或用其他的方式來做規範。定型化契約應記載事項應該是沒有辦法規範到汽車製造的業者，第二點就是一個很常發生的例子，就是臉書一頁式詐騙，過去已經發生好多年，臉書利用消費者的習慣，收集消費者瀏覽的習慣跟點閱紀錄後，依照消費者習慣去投放相對應的廣告，而這個廣告又剛好是詐騙集團所投放的廣告，這時臉書需不需要負責？我個人認為他應該要負責，不過長久以來，可能是因為是美國業者，臺灣的政府或法院也拿他沒辦法，因此這個情形就一再的發生，無法解決，既然現在政府有新的打詐專法出來，是不是可以考慮在未來的 AI 相關法制當中，增加一些條款來針對這些業者（提供 AI 服務的業者），是不是能夠給予他更多攸關他權力的規範，比方說消費者因點擊你投放的一頁式廣告受騙上當時，臉書也應該要負連帶的損害賠償責任，這樣他才會介意，不然目前他只有收廣告費，不對消費者的損害負任何的責任，對消費者來說非常的不公平。那我先初步的提出兩點看法供各位與會先進參考，謝謝。

計畫主持人：

謝謝（C），針對這個 AI 運用趨勢，看到像自駕車或社交平臺臉書這種的一頁式詐騙，的確這種演算法本身的推播，現在幾乎所有的平臺大概跟 AI 運用都脫離不了關係。剛剛提到的一頁式詐騙背後的 AI 運用，造成消費者受損時，平臺本身要不要來負相關的連帶責任，這個我們之後也

會看一下國際上有沒有相關的案例，而國內打詐這塊的確是可以思考的方向，非常謝謝（C）。

（D）：

前一陣子大家有注意到很多新聞上，都在談 AI、PC 或相關的部分，其實這些問題，當我們業界在想這件事情時。我先提一個例子，臺灣也許很多人認為在 AI 這一塊的實力很強等，是因為現在很多 AI 的應用在實體、硬體的部分，臺灣有一些供應鏈上關鍵的地位，但回過頭來看，在應用層面，不論在 AI 的學習上，甚至系統上，臺灣在這塊並非居於領先的地位。像今天你要在 AI 給他一些訓練跟學習，他有很多需要的 data、模型等，其實臺灣都還在起跑點、學習的階段而已，所以很多人在探討這些問題，現在的法律一些嚴格的規範到底會不會有助於我們在發展 AI 的應用？那必須說多數的看法應該是持的是比較否定的部分。歐盟當然用的是作用法，但他有很龐大的市場力量在支撐他，他希望 AI 部分能夠有意外的效力。但臺灣沒有那麼大的市場上影響力，我們也很難發揮到這種對境外規範的效力，所以這一塊大家很多的看法是說，臺灣應該走向還是比較低度的管理，至少業界的看法應該還是這樣，因為在應用的過程還是需要太多的學習，累積更多的語言模型、演算的能力。再來就是臺灣的 AI 人才不足，這是現實要面對的問題，不過從這個角度來看，產業當然希望在未來相關的法令規範上，應該還是走向低度管理。從剛剛提到的這些的不確定性，甚至過去的規管經驗套用在 AI 上面，臺灣其實是沒有的。沒有這麼好的經驗去做這些規管，在沒有這麼好的經驗做規管時，我們在很多法律上當然要去思考，但是不是馬上要走向一些比較強度的管理，這都是必須要去思考的，這是第一個點。第二個是說，現在到底實際上面 AI 的應用已經在我們的生活裡面，我很讚成剛剛有提到一些責任的問題，特別是生成式 AI 產生之後，有時候會發現一些 AI 的幻覺，產生的這些錯

誤，過去的商品製造人可能無過失責任這塊，是不是能夠再繼續這樣的去適用？而這樣的責任是不是適合？特別像是生成式 AI 這類，甚至很多來自於 user 本身，加入很多的資訊，最後再回饋相關的資訊給你時，因為我個人在使用也常常會覺得當我輸入某些資訊後，他回饋給我的東西，我也是會懷疑資訊的準確度，所以這東西在消保上，似乎在基本法上這塊沒有比較多去談，但我覺得在消保這個議題上，在責任這塊是值得再深入去探討。第三個，法律上要不要修這個東西，還有很長的一段時間，過去不論剛講的演算法各方面的因素，其實大家早就可能都在使用 AI，只是我們不自知，如何讓現在已運用 AI 在實際的商業活動的部分，它的資訊揭露這塊，我覺得可以優先去推動，而到底要揭露什麼？我相信這東西是可以去討論的，剛剛講到的 Facebook 演算法的東西，我相信很多人在使用這些問題時，為什麼經常會給我一些廣告的訊息，他一定是針對我這個人在上面很多的活動，再去收集、判斷後，餵養給我一些他認為我想看的訊息，這部分資訊的揭露，實際上是可以優先去研究的。最終來講，我還是比較傾向現階段在政府的一些相關部門，因應這些 AI 的應用裡面，現在要去訂定型化契約，我認為也很難。因為定型化契約的使用，第一個它的經濟效益，一般消費者要有一定的量及市場上的規模，你才去用定型化契約才會有效益的，如果沒有，不要說什麼，訂都訂不出來。然後你連 AI 會發生什麼問題也搞不太清楚，就想要去透過定型化契約去做一些的規範，我覺得事實上有困難。那不如開始去用一些的指引來看看說。另外產業本身自己也可以透過一些自律的規範，去講說在一些資訊揭露或他使用的一些演算這塊是不是要讓他的客戶、消費者去知道，也許這是我目前看起來的一個方向，簡單做一些的分享。

計畫主持人：

非常謝謝（D）從幾個面向提供的意見，第一個，站在產業公協會的角度來說的話，目前臺灣本身在全球的 AI 發展上，不是說我們臺灣沒有優勢，但是跟 AI 本身的特性比較起來的話，今天在 AI 系統本身的訓練跟學習上，我們比較像一個跟隨者，而不是一個領先者，所以說我們在硬體或某些個別行業的領域，也許有他的優勢，但整體來說的話，產業本身還是比較偏重在發展，所以到底要不要一個立即的用硬法，還是說用比較適合的低度管理？另外在人才方面的缺口問題，其實我覺得這也是一個消費者保護非常重要的，但如果今天回到整個政府的角度來看這個議題來說，這會變成是一個整體性政策的方向，對於 AI 本身治理到底要採取一個立即的全面性嚴格監管，還是比較是屬於混合模式或完全自律的？我相信這要回到整個行政院來做整體性的討論，但（D）這邊提到一些比較重要的是在責任這塊，我覺得這也是我們目前在看消費者保護，在一般的人工智慧商品服務的系統及生成式 AI 系統，確實未來責任可能會有一點不太一樣，以生成式 AI 的話，更多會加入來自於一般使用者的資訊或反饋，而這也是我們後續會再做更進一步討論，像剛剛有提到的生成式 AI，如果是因為來自於回饋意見而造成消費者受損時，他跟一般的人工智慧商品跟服務的責任區分會不會產生不一樣的判斷，這的確是我們會再看一下國際上面的處理。另外在整個建議的資訊揭露優先推動及最後提到的定型化契約，的確今天任何的一個定型化契約的擬定通常要到所謂的一定規模經濟來制定定型化契約才有一個實際的效應。最後的話，有沒有哪些定型化契約？如同剛剛提到對於車輛這塊，若自駕車有一定的規範，在車輛這塊的定型化契約是不是足夠適用，而其他領域的定型化契約是不是暫時的先不考慮，用自律的方式。那這邊也非常謝謝（D）從不同的角度來給我們這些寶貴的意見。

（E）：

人工智慧的類型太多、應用層面很廣，從生活的採買、社交、理財、工作、娛樂創作、知識的取得等，大家都會碰得到，對消費者來講，在線上購物時，客服的對象到底是 AI 還是真人？以及人工智慧創造出來的一些廣告的內容，像很多在探討深偽技術所衍生出來的見證，其實透過人工智慧來調整、修改過，甚至去模仿別人的聲音或影像做出相對應的廣告，也可能是金融服務的理財上建議或消費者運用一些付費的使用 AI 的服務（如生成式 AI）。在實體的層面就有自動車、AI 臉部辨識分析等可能碰到的問題，就現在一些法制趨勢來講，與數位線上環境主要的問題可能會出現在消費者根本就不知道自己在從事消費行為的過程當中是有 AI 的介入，他不知道他獲得的資訊，已經通過演算法的篩選，也不知道自己討論的對象是 AI、曾經看到過已透過 AI 修正的資訊、AI 創作出來的內容，所以從法制趨勢來講，在觀察美國的一些州法，他們會重視在消費者揭露，以及 AI 基本法裡面有稍微提到針對揭露的這個層次。這個部分，尤其是美國有些賓州、科羅拉多州的州法都有提到一些重點，可能強調是說，今天對消費者保護要去進行相對應的揭露，那揭露什麼東西？什麼時間要揭露？是開始從事交易行為之前就要做揭露，而揭露的方式要如何？怎麼樣才叫清楚等，其實已經開始有一些實務上的做法。

再來就是說，你現在正在跟 AI 進行互動，你訂約的相關資訊來自 AI，這種說明、評價，要調整這部份的說明可能都是需要去做處理的，而法治這個層面，我們有看到相對應的做法。另外在 AI 的時候，可能大家會探討的是一些演算法的分析，甚至分析的話就會連動到歧視的問題，這個地方不一定是揭露的問題，反而是我今天提供的 AI 的產品或服務，他如何避免這個歧視及它的風險預防的檢測機制這部分是不是有辦法去建構出來。首當其衝還是要先讓消費者知道說參與服務運用的時候，其實有人會對你做分析。講一個最近發生的事情，在群組裡面討論說我今天車用的手機架，應該買哪一種類型，結果我們討論大概 10 分鐘左右，隔天有個在

群組裡面完全沒有跟我們討論關於手機架的那個人就說，她不知道為什麼一直不斷彈出各種不同 AI 手機架的廣告在他的手機裡面，所以在這種狀況下，大家也不太知道他在什麼樣的環節已經被收集資料、分析，甚至進行目標式的廣告投放，以這個狀況來講，如何去告知消費者，以及消費者如果他不願意去做這樣的參與，怎麼樣去把這個功能關掉，讓他保有自己某程度上的權利隱私層面、有一定的控制權，這其實也是滿重要的一個點。

目前來講，針對 AI 的消保，我覺得是一個非常廣範性的問題，假設就這個計畫需要對消保的主管機關給建議的話，我覺得可能要考慮的是以臺灣這個面向來講，哪些議題是比較能夠對消費者來講很重要，且在現有的法律體制上面可以做處理的，比如說剛剛提到的定型化契約。當然說定型化契約沒辦法解決所有的問題，但對於揭露這件事情來講，也許在某些層次上他是可以運作的，這個地方其實蠻贊同所提出的可以從定型化契約來做揭露。但定型化契約是針對特定的行業，到底哪一個行業？哪一個服務型態？他的定型化契約可以去做這樣揭露？假設今天在線上的情況下，這個電商購物的服務提供者，他有去做人工智慧的這個部分的消費者的分析等相關的做法，這個地方會不會在這個狀況底下，就可以先去做揭露，這也許是一個可以去思考的看法。不過除了定型化契約以外，也許考慮對消費者有影響，

之前曾經看到過麻州的檢察長發現消保的議題在 AI 影響是滿大的，他有提到也許可以把對消費者，可能會影響平等互惠權益最大的幾個項目如何去適用法律這部分，提出一些比較軟性的指引，也許在臺灣目前有一些 AI 服務還沒到一定程度時，透過軟性的做法也許可先解決現階段對消費者保護不太彰顯的這部分相關問題。我先簡單地提供一些建議供參考，謝謝。

計畫主持人：

謝謝（E）在國際上面的觀察，最後回到臺灣來提出一些法制面的想法，所以看到像美國，雖然沒有像歐盟這樣全面性的專法，但在聯邦的草案提出，或像科羅拉多州的確已經有一個全面性的 AI 立法，這也反映在 AI 本身來說的話，到底用什麼樣的一個法制規範跟力道，剛剛有提到如果回來臺灣，也許比較重要是先處理哪些議題相對是重要的，能不能在現有的法治裡面就立即做一些處理，比如說定型化契約或指引的方式。

像剛剛所提到的，在聊天的時候，馬上收到一些相關的推薦，大家會不會懷疑是手機被竊聽，事實上不是只有手機，我們現在也會跟 AI 產生連動，像一些語音助理的產品或有些兒童的玩具，這個在國際上也有引發過討論。像一些兒童的玩具，可能跟兒童產生互動的或家裡獨居老人的居家監控搭配 AI，像長照的商品透過老人的動作或穿戴式裝置（手錶）判斷，來偵測是不是跌倒，但人家會說，這個會無形當中去收集他的資訊之外，會不會有竊聽的問題？其實這種穿戴式裝置或智能的穿戴式設備來說的確一直有存在這種，它是不是會過當或不當的去收集過多的個資，甚至變成是一種行銷的工具，所以這也會反映出來，AI 的範疇很廣，我們怎麼樣的化繁為簡，在這麼多議題當中，哪些可能是真的有一些法規的調適或法制推動，至少從消費者保護，一般民眾會比較有感覺的，我覺得這個會變成是什麼都處理，反而大家會覺得你什麼都沒處理，也許應該是從中去找到一些一般民眾會比較有感覺的部分。

（F）：

我們都知道就資訊揭露這一塊，因為攸關到消費者知的權利，所以就人工智慧這個部分的使用，我很贊同剛才講的 AI 告知權利，因為 AI 這些產品的使用，其實有些消費者在這部分可能是無所知悉的，如果未能課予製造者或企業經營者這樣的告知權利，在消費者他從事一些消費資訊

的判斷和選擇時，這個部分等於他們無從去做一個比較精準或合理的判斷，而在應用人工智慧技術造成的損害，是不是可以構成民法或消費者保護法裡面特定類型的侵權行為或消保法？目前在國內可能還有一些爭議，在這裡面就值得我們討論的一個議題。我提供個人的淺見就是說，以目前人工智慧的發展，如果它是一個國家的政策，消費者權益的保護雖然重要，但這裡面怎麼樣取得一個衡平？確實是有一個難題，如果今天我們課予企業經營者過重的一些可歸責的部分，是採無過失或危險責任。這裡面是不是會意識到我們本身人工智慧這方面的一個技術、量能各方面的處理，跟國家要走的政策是不是能夠符合，就會值得我們去考慮。其實消費者的權益也不能全然不顧，我會比較贊成剛才（D）說的，我們對於企業經營者的責任是不是要課予比較低度的要求，而不是不要求，因為本身我們在人工智慧的發展跟學習，也在努力學習中，對一個國內是比較不成熟的技術，你課予這麼高的歸責是不是會阻礙到國內這方面產業的興起。至於剛才有提到定型化契約這部分，我個人提供一個淺見，其實定型化契約裡面當然可以就這部分去做相關規範，可是定型化契約一般目前在消保的認知中，可能沒有一個法規的拘束力，他頂多就是資訊或參考，所以對企業經營者，或許他會有一個提醒的作用，是不是能夠達到法制上的一個效果？就我們目前來講，常常說應記載不得記載事項，這個就是法規命令，可是定型化契約的範本在這裡面，如果還沒簽訂之前，都只是一個類似指引或參考用的，在這個部分的話，當然也可以嘗試由淺而深去做處理，不過整個發展，還是要透過修法的方式，才能夠達到一個比較積極的目的性，因為時間關係，我就簡短跟大家分享，謝謝。

計畫主持人：

謝謝（F），可以看出來說在整個消費者保護推動，一個很重要就是怎麼去衡平，包括在這產業的發展跟消費者權益的維護。今天不管前面要不

要設強制性的規範，一旦產生消費者保護爭議時，現有的消保法的責任，在無過失跟危險責任，是不是能夠立即套用到人工智慧商品跟服務？

像醫療糾紛（馬偕醫院案子），過去就產生會不會讓醫生不願意去開刀，如果說把人工智慧的商品跟服務在發展過程、責任還不是那麼明確，而直接去套用這樣的無過失或危險責任時，因為現在在醫療本身來說，一些醫療影像的 X 光片的判讀或癌症篩檢，現在越來越多結合人工智慧的醫療產品開始實際的運用，所以在醫療領域也衍生出來 AI 的醫療的器材，它是工具？還是有點類似醫事專業人員？因為變成說，在這樣子的判斷，比很多醫生還要精準，但是一定有百分比誤判的可能性。剛剛講的也讓我很有感觸，一個消保法責任套用到特定行業或特定產品時，過去在醫療所看到，適用消保法的問題會不會再一次出現？這的確是我們在後續，也會把這一點納入到我們的研究討論當中，另外剛剛提到有沒有可能初步用比較低度的要求部分，及最後針對有關於法制、法規調適在應記載不得記載事項跟範本本身的這個部分，在過去這塊無關乎今天的討論議題，在很多涉及這種議題時，我會比較傾向回到各部會去立法，而不是應該藉助消保法本身的定型化契約規範，因為這會有點行政怠惰，因為你不去立作用法，反而到消保法，這一塊過去有些人會認為，在整個消保法本身的定型化契約的規範會不會被濫用而變成把消費者保護推到第一線，反而行政機關躲在後面，這的確是過去在涉及到很多議題上都看到這種情況，因為大家覺得消保法本身定型化契約太好用，把你們都推到第一線。這個在人工智慧應該要回過頭來，中央應該要有一個基本的立場，定型化契約應該達到一定的規模經濟後，我們再作為消費者保護的後盾，這個也勾起我非常多的感觸。

（G）：

聽說 AI 這個議題是一個很新的議題，其實也是一個很舊的議題，因為這個問題早已經在我們日常方面，但大家可能沒有馬上面對這個問題來解決他，所以現在提出來還算是很新。回到時事上，很多人在看奧運說什麼體育即國力，這說法我並不贊成，因為臺灣就算沒有拿到任何獎牌，我們國力也是很強。AI 就代表這個國家的經濟科技的實力，在這方面，各國家在競相發展 AI 的話，消費者保護可能不會是最優先的參考、判斷價值，也可能會因為這樣沒有充分保護到消費者。這個議題很大，坦白說我根本對 AI 的了解不是那麼深，就我自己平常接觸有一些看法，如果我要判斷 AI 這邊對消費者保護的影響的話，我想從消費者的四大權利開始講，在 1962 年 3 月 15 號，美國甘迺迪總統有講到消費者的四大權利，消費者有知的權利、消費者有講求安全、消費者有選擇、消費者表達的四個權利。現在很多 AI 的產品，包括手機、智慧的音箱很多都 AI 功能，比如自駕車有些會記錄你行徑的軌跡，甚至新聞說可用來做為抓姦的根據，但這都是個人隱私，消費者要知道說我的個人隱私有沒有被偷聽、被利用、被鎖定，以前還有個很保守的家庭，他接到一個孕婦的廣告，恭喜你的女兒快要生產，而父母很生氣，我們是最保守的家庭，怎麼會有這種事情，我女兒才 16 歲。業者怎麼會寄這種廣告過來，業者說不好意思，我們的判斷錯誤，後來才發現那女兒真的未婚先孕，因為那女兒可能有上網查一些相關的資料，就被演算法利用判斷出這女兒確實有懷孕，有時候有人講說現在的父母對小孩的了解甚至不如電腦，因為它都有在背後看這個人的想法屬性，所以在臉書上討論的內容都可以判斷你的政黨傾向，這都是一些個資，消費者要知道說自己的個資怎麼被濫用。另一方面，現在 AI 也進步到說可以換臉，有些代言人可能不是他講的話，就是被換臉，很容易就被糊弄過去，消費者要知道說這個代言人是真是假的。另外，AI 還有文字的生成模式，這樣有些人會在 AI 上面找一些資料，那資料是不是正確？消費者應有知的權利，而在 ChatGPT 剛出來時，有人就說問很

多問題，他其實就是一本正經的胡說八道，講的跟真的一樣，所以這部分消費者的識讀能力，有時候可能趕不上 AI 的發展。再來，消費者講求安全的權利，就是消費者的隱私權、消費者不要被竊聽，還有汽車自駕的問題，其實也是滿有意思，因為我碰到真的案子，一個朋友去試駕有自駕功能的電動車，但是中間可能轉彎時有點緊張，不小心踩到煞車後，這個自駕功能自動解除，他以為車子會在即將撞上的時候會自動煞車，其實並沒有，後來車子壞掉了，也就是他只是去試駕一下，就要面對 80 幾萬的賠償，業者說因為前面很多感應器，修起來要 80 幾萬，只算你 30 萬就好。消費者會認為說自駕車不應該有這種情形，AI 應該要聰明到不會讓我撞到，但實際問題相當多。什麼時候是在 AI 階段、什麼時候是輔助階段、什麼時候是人力駕駛階段，這些界限不是很容易劃清。當然汽車若有個記錄的話，會比較容易釐清，對消費者來講也希望業者能夠把資料拿出來，但資料對業者不利的話，他也一定不會拿出來。而這個安全性在 AI 時代也是一個很大的挑戰，尤其是個資及有沒有竊聽的部分。

另外有些人會用 AI 來寫文章，像我有朋友在美國當教授說 AI 寫的文章，英文比我們一般人好很多。如果說有些人用 AI 來寫一些文章，說不定也會有抄襲的問題，因為資料庫可能都是既有的文章，從那邊抓資料可能會有抄襲的問題，而這有沒有授權，都是有一些爭議。在消費者有選擇的權利，由 AI 來記錄資訊更加爆炸，AI 可能也會有所謂的網軍，會有一些洗風向、帶風向的情形，消費者的選擇可能會更茫然，而且 AI 也可以把外國的文字直接翻譯成中文或自己想要的語言，這樣變成說消費者可能選擇更多，可以輕易地去國外的網站買東西，但保障的話，可能有管轄權的問題，他沒有辦法得到像臺灣消費者保護機制這樣的保障，這都是問題。在消費者保表達的權利，當消費者對 AI 有一些不滿，但是問題是很多政府目前在全力發展 AI，他可能不會把消費者保護放在第一順位，所以有些比較民主國家強調個人隱私，AI 發展可能不會比那些共產國家

更快，因為人家要隨便要取得消費者的臉部識別都沒有問題的。而在民主國家可能會有一些爭議，實名制也不會有問題，雖然這樣可以發展得比較快，那國家是不是應該要保護消費者優先，還是發展這個產業優先？這是一個很難抉擇的事情。目前臺灣的發展沒有先進國家那麼快，我覺得不見得是缺點，因為有時候法規是有後發的優勢，等都已經有一些經驗後再參考，比起之間的事務過程可以節省很多的成本，這方面，我也是建議說不一定要定型化契約著手，可能還是要有作用法會比較好一點，立法的話可以參考國外，因為定型化契約的應記載不得記載事項，說實在你要先有一個主管機關，在碰到這種議題，每個主管機關可能都避之唯恐不及，包括之前的個資法，像 Google 的街景可能會侵犯到隱私，主管機關就喬很久，所以這個部分會牽涉到很多業別，主管機關不好喬的話，我們也不用過度期待這個定型化契約應記載不得記載事項，總之 AI 雖然說可能會帶來一些消費者知的權利的挑戰、安全性的挑戰，還有意見的聲音可能會被淹沒及他選擇可能更多，但 AI 對消費者保護有很多好處，包括之前常常會有網路標錯價，如果是不是業者透過 AI 可以把這些明顯不合理的價格避免掉，另外還有強調說契約什麼時候成立，我在想說這契約什麼時候成立，可參考我們網路下單或自動販賣機的例子，基本上可能要探知這個爭議。但是我也想到說以後的未來，AI 越來越有智慧，會不會也給 AI 一個特殊的人格，也是不無可能的發展，因為他的智慧可能超過一般人。最後我想強調說，這個 AI 的問題其實不是一個國家搞定的，因為 AI 無遠弗屆，可能需要國際組織，若未來 WTO 還有功能或 APEC 會議，可能國際組織會慢慢有一個共識出來，我們也不一定要搶在最前面，可以靠國際組織的國際規範、潮流趨勢及國家的發展，在看其他國家立法例的法規衝擊，最後再訂出一個比較妥善的法規，或許後發的優勢也會享有。

計畫主持人：

非常謝謝（G）一些非常寶貴的意見。而這邊提到一個非常重要就是後發者的優勢，的確 AI 從自律開始到他律的時候，其實像美國或英國的話，也有國會議員提案要立法，可是日本是完全沒有任何法，因為他們就覺得說目前是不是透過一些行政機關的指引，在立法是不是等到國際有一定的成熟度。在國際上面，在英國這邊 20 幾個國家的宣言，後來這幾個國家又到韓國開了一個首爾會議，也提到一個首爾宣言，所以在國際組織這塊的共識的確是有，目前的話，在整個人工智慧本身來說，要從自律走到他律，而他律的做法看起來還是會有一些奇異的地方。在剛剛也提到一些包括人工智慧可能產生的一些風險、消費者怎麼樣的給予他一些選擇跟表達的權利，以及法治上面，針對定型化契約，對主管機關的選擇，像在 Google 街景服務行政院出來協調都協調無效，也包含當時的行政院新聞局、NCC 跟經濟部一直沒辦法把整個主管機關定下來，甚至過去在院裡面，處理過同一種商品跟服務，可能會有不同的主管機關，比如說在禮券這塊，所以未來人工智慧的商品，它是一種商品一種服務一個主管機關，還是同樣的一個人工智慧可能會涉及到不同主管機關的權責，這也會讓整個在人工智慧不管是用自律或他律的規範上，在機關權責本身的劃分跟確定，可能都是國內一定會面對到的問題，這邊的話也非常謝謝（G）從各個面向來給予我們很多的寶貴意見。

（I）：

隨著 AI 的發展跟運用越來越廣，對我們的生活影響也會越來越深，本處近年來，有在持續的關注實務的發展，還有國際間的立法趨勢，包括歐盟 AI 責任指令草案，還有產品責任指引的修正草案等，因為對本議題的重視，所以本處今年有 AI 法治的研究委託案，本處今天是主要列席旁聽，非常感謝各位學者專家提供寶貴的資訊跟意見，謝謝。

（H）：

我想這個議題其實也是緣起去年的時候，行政院在 4 月的時候成立一個院層級的數位政策法制協調的專案會議，這個會議成立的目的就是為了因應數位科技的發展所帶來的法制面衝擊，要建立一個我國的人工智慧的法治路徑圖，因為韓國的部分也是有這樣子去布置，希望透過這樣的一個專案會議來讓各個機關自己組成專案小組，通盤解釋自己的業務來因應 AI 發展趨勢，現在或未來可能會遇到的法規調適的議題來進行相關的嚴格規劃，整個專案會議在運作上，當時由 3 個政委擔任共同召集人來進行督導，並且在專案會議下依照 AI 發展可能涉及到的重要議題，包括人工智慧、個資保護，還有資料創新分別設計 3 個法治分組，分別由國科會、個資籌備處及數位部擔任一個統籌協調機關。這樣的好處是可以避免各機關在提出自己的法規調適，可能有涉及到跨部門需要協調時，就可以運用這樣的分組來進行討論，而這 3 個分組會再把各個部會所報上來的法規調適議題，經過統籌協調後，在整體的把相關的規劃網上發到專門會議進行協調。在國發會這邊，因為法治處一直擔任整體國家的法規調適的工作，就是由我們來做這個專案會議的行政幕僚，而消保法規的調適議題，目前就是被納入人工智慧法治分組的部分，主要關注到人工智慧發展會對消保法的制度產生一些影響，像自駕車的商品責任，或考量到使用人工智慧系統跟產品的一些法規調適議題，所以將院消保處理已納進這個專案會議，大家一起來共同努力，而在整個專案會議的運作上，因為人工智慧的發展，我們可以看到人工智慧技術會不斷的演進，為了兼顧整個風險控管，還有產業發展的平衡，避免人工智慧發展過早的訂定法律阻礙他的進步或箝制產業發展，所以在整個具體法規的調適策略上，其實建議採取先指引後法律，那我想這樣的方向也跟剛剛的一些先進是吻合的，我們可以先透過一個軟法，挑選出一些比較重要議題，需要迫切被處理的領域先挑出來，訂定相關的一個指引來協助產業遵循，像剛剛有提到說針對人工智慧應用的透明度和需要強化落實揭露的部分，我想這個部分可以

挑出一些參考國際的標準、挑出一些相關的原則和標準來訂定相關的指引供產業遵循，目前在去年 4 月行政院成立專案會議後，各種機關都有陸陸續續地針對自己的列管的領域訂定一些指令，像是金管會的部分，就有針對金融業運用 AI 的部分定義的指引，而在消保這部分，我想也可以參考這樣的一個模式，先挑出一個最大的公約數，認為就是目前在這個領域參考國際的趨勢，有一些比較需要被迫切先拉出來做處理的部分，我們可以先朝這個方向去做處理，謝謝。

計畫主持人：

非常謝謝（**H**），從國發會本身還有整個行政院在整個 AI 法制本身的一些推動跟協調，就定位跟目前的推動狀況做個說明，也提到在消保這個議題，先指引後法律也許是一個初步比較可行的方向，我想這也跟我們今天整個學者、業界先進、公部門大家的共識基本上是吻合的，今天也非常謝謝各位學者專家的參與。

附錄三、「人工智慧(AI)商品或服務之消費者保護深度訪談」紀錄

訪談紀綠一

訪談時間	民國 113 年 10 月 21 日	
會議地點	線上訪談	
計畫主持人	南臺科技大學郭戎晉	
受訪人	A	基金會副董事長
	B	律師
	C	計畫專家顧問

訪談內容：

計畫主持人：

整個人工智慧本身來說的話，對於這些可能運用到 AI，或者說 AI 本身就是一種商品或服務、在消費者保護來說的話，各國的消保主管機關也開始意識到這些問題，所以說在日本這邊的消費者主管機關，他就提到像是安全、影響消費者的決策、個資保護。這些看起來的話，其實涉及到的面向，當然就不是只有在消費者保護，可能還有涉及到其他的法律議題，我們今天大概就是比較偏重在消保法本身，因為消保本身來說，是一個廣泛的面向，各國也開始思考到針對 AI，歐盟一個全面性的監管專法，美國、英國、日本，目前並沒有說一定要定專法。日本部分，現階段是不打算先訂任何的法。英國本身則是在部會的權責，所以部會要立法修法，還是說既有監管的一個工具這個部分，英國強調就是按目的事業來做客製化的監管。美國在監管是一個自律跟他率，他希望做一個衡平，而比較特別是說另外針對產業標準這一塊。

如果我們今天來談整個消費者保護或人工智慧導致消費者受損的時候，可能產生的法律責任。事實上，在歐盟的人工智慧法，比較注重在監

管，所以針對可能衍生的，特別在民事賠償這一塊的話，它提到一個是既有的歐盟體系或成員國裡面的，如同我們民法跟消保法裡面相關的過失責任，還有包括在商品製造人這邊的嚴格或無過失，這個其實在我們民法跟消保法都有對應的規定，歐盟本身又思考到說，對於人工智慧這種新興的應用，可能會造成消費者難以證明這一個所謂的人工智慧商品或服務跟所謂傷害結果之間的關聯性，所以在他所提出來的人工智慧的責任指令草案當中，就去創設這樣子一個因果關係的推定。

在國內的部分也會談到，歐盟的人工智慧責任指令，我們有沒有參考跟學習的必要，另外消保法本身它說是一個嚴格責任，無過失責任，但是在我們民法當中，其實有一個有趣的設計，就是民法第 191 條之 1 的話，相較於 184 條的這種一般的過失責任來說，這樣子一個因果關係本身的推定來說，是不是直接用我們的民法第 191 條之 1 條就可以，這個是一個在整個，會在後面談到我們國內消保法的部分再做介紹。

我們說人工智慧的商品跟服務涉及到消保議題很廣，如果說我們聚焦在消保法，大概有 4 個比較重要的問題，這是我們第一階段會建議消保處關注的，第一個就是人工智慧商品到底有沒有適用消保法，如果沒有適用消保法，我們先談這些問題，好像就是未雨綢繆。

第 2 部分就是人工智慧本身，我們消保法今天不管是任何的商品跟服務的話，我們消保法之所以會有這麼大的一個規範的作用，就在於要求商品或服務的提供者，你必須要在實際進入市場的時候，必須確保這個符合當時可合理期待安全性，所以這邊會衍生 2 個問題，我們今天任何進入到市面的人工智慧的應用，在進入市面的當時，是不是有符合所謂的可合理期待的安全性，那這邊就會衍生一個問題，因為這個是一個新的技術跟新的應用，所謂的可合理期待安全性應該怎麼做判斷？

第 3 個，既然他有一定的風險性來說的話，這邊對應的資訊揭露要求應該做到什麼程度，以及剛剛我們看到歐盟有所謂的人工智慧的責任

指令，所以人工智慧衍生的一個民事損害賠償的時候，怎麼做一個法律責任的判斷，還有舉證責任這些管理的問題。

所以說在有關於到底我們使用消保法上，我們認為是有適用的，因為包括我們的商品跟服務的定義來說的話，應該還是足夠去把它整個人工智慧的商品跟服務給規範進來。所以兩種可能性，一個就是人工智慧本身就是一種商品服務，或者是人工智慧本身，它是商品或服務的重要組成部分，或者是一個重要的功能，或者是整個結構的一塊，其實在歐盟本身的 AIA 有類似的一個規定。所以說這一塊，過去我們對於商品跟服務的界定的話，大致上也是放得比較寬一點點。

第 2 個部分就是一個所謂的可合理期待的安全性，在我們消保法的第 7 條第 1 項有提到一個，提供商品或提供服務的時候，必須符合當時科技或專業水準的可合理期待安全性，所以這邊就會變成是後續在實務操作的話，所謂的科技或專業水準，以及所謂的可合理期待的安全性，具體應該怎麼做判斷？這部分消保主管機關應該扮演什麼樣的角色？這個部分來說的話，過去我們的消保法施行細則當中，是有提到關於這個第 7 條可合理期的安全性本身的判斷，但我們對這三款的一個判斷標準，還是一種不確定性的概念，所以說這個部分的話，包括一些民法學者都認為說，即便我們有承襲第 5 條，但它屬於一種歷史的概念，還是必須要加以具體化。這個部分的話，我大概看了一下，目前整個實務，針對消保法第 7 條的判斷，最重要就最高法院 109 年一個民事判決，因為它針對一個兒童嬰兒床本身，提出一個技術標準，以技術標準來作為所謂的可合理期待的安全性，而這一個判決本身也引發一些學者的討論，因為我們只要能夠證明符合消保法當中的這個，由企業經營者負舉證責任。等於我們看到第 7 條的第 2、3 項。如果今天有辦法證明他無過失，是可以減輕他的責任。如果可以用技術標準來認定他無過失的話，會不會變成造成業者很容易因為這個技術標準本身到底適不適合作為一個安全性的判斷標準？不過

這個會有點一體兩面，因為太新的東西，如果沒有一個明確的一個判斷依據，好像也會造成業者的責任無限擴大，但因為這個判決當中，引了一個 ISO 標準，只要你拿到這個 ISO 認證，是不是代表你就可以主張你無過失，所以這個會變成有些人認為說，用技術標準來作為這一個可合理期待安全性的話，反而會讓消保法的保護水平低於民法，這個是在 109 年最高法院判決當中所提出來的這樣子，不過至少說，它是一種跟技術有關的，提到技術標準，也許是可以作為第 7 條的判斷因素。

目前我們也看到一些人工智慧的技術標準，包括在 ISO、數位部，也有這樣一個相關的一個國際，或國內相關的一個機制的推動，後續有沒有可能被引用為法院作為第 7 條判斷的一個依據，這個我們可能需要再做一個觀察。

另外在資訊揭露，消保法資訊揭露大概就是比較落在幾條重要規定。在消保法的第 4 條、第 22 跟 24 條，不過第 4 條只有提到，你要向消費者說明這個商品服務的使用方法，並且提供充分跟正確諮詢，是有一個原則性的要求，但具體你要告訴哪些事項，在消保法本身並沒有做這麼細緻的規範，當然也不適合，因為消保法通案性規定，所有的商品跟服務的話，這種具體的資訊揭露要求，歷來大致上，比較可以進一步觀察到的，大概就是落在我們目的事業主管機關所訂的定型化契約的應記載不得記載事項，特別在應記載事項，所以我這邊大概舉了這樣子一個，通訊軟體服務的定型化契約裡面就提到，一般企業經營者的資訊一定會揭露，因為這個是消保法要求的，比較重要，他可能會針對帳號申請、安全維護，另外像網路連線遊戲這個，像過去比較大家比較關心的，這種賬號被盜或續保，所以說一些重要的消費資訊或警訊來說，這個大致上是落在我們的定型化契約的要求，所以在消費資訊揭露本身，如果我們要今天要針對人工智慧消費資訊揭露問題的話，比較務實的做法可能就是往下到，可能會跟人工智慧有關的現行的定型化契約應記載或不得記載的事項，去看看有沒

有增訂對應人工智慧的一個資訊揭露的要求，或有沒有必要，如果未來人工智慧成為通案的話，要不要針對人工智慧制定一個通案的定型化契約規範，不過後面這個，我覺得目前時間可能會太早，所以比較務實是現在已經有訂定定型化契約的商品跟服務當中。有沒有哪些可以考慮優先來處理，跟人工智慧有關的一個資訊揭露要求。

最後一塊就是在整個法律責任，其實這個會跟我們消法第 7 條前面所談的安全性會有一些相關的一個連動關係，所以我們的消保法本身採取一個嚴格的責任，所以說在第 7 條第 3 項有提到企業經營者可以證明無過失的話，可以減輕其賠償責任，前面就是像最高法院 109 年判決當中，他用所謂的技術標準作為業者，今天證明無過失的一個判斷指標來說的話，反而是不是讓業者很容易就可以減輕其賠償責任。不過這邊的話，只有提到減輕，並沒有說要完全免除，這個是一個在我們的消保法規定底下。而這一個部分還包括舉證責任的導致，所以說這是在看整個歐盟本身，特別在歐盟關於民事責任的時候，它創設一個人工智慧責任指令的草案。當然，歐盟是整體性的，從既有的傳統民法上面的一個過失責任，到可能在於所謂的產品這一塊的嚴格責任，對於這個部分他又去創設這樣，一個過失推定，不過在我在我們的民法第 191 條之 1 當中，大概就有針對商品製造人，但這一塊，我們民法第 191 條之 1 跟我們消保法比較起來的話，第一個是只有針對商品，所以說能不能適用在服務，我們民法第 191 條之 1 看起來是會有一個局限性。另外一塊是說，我們的民法第 191 條之 1 的話，就是一個有過失推定的概念，大概是在民法學者這邊，所提出來的一個相關的討論。所以說我們要不要針對人工智慧的民事責任，參考歐盟的這一個責任指令草案來定相關的立法，如果說從我們的民法來看的話，似乎已經有相關的規定，但我們民法第 191 條之 1 是不是足夠適用，這個也是一個在這次研究當中的話，針對這一塊，我目前是比較傾向，我們先不去創設新的，因為民法其實已經有一個類似的一個過失，只是說

他適用在服務的確會容易產生一些爭議。在國內消保法本身的一個適用上面的話，可能會有這 4 個主要的議題，所以說回到法治建議，第一個，如果今天像歐盟一樣有這樣的監管專法的話，本身來說的話，我們就有一些很明確的監管規定走在前面，但是目前國科會的這一部草案當中，比較可惜，他就是基本法，而且基本上是完全的基本法，主要提到政府應該怎麼樣。所以跟消費者保護比較有關的規定，很多都會跟消費者保護會有一些間接的連結，相對比較直接的可能來自於我們消保法。這一個人工智慧基本法草案的第 9 條跟第 12 條，不過這個部分就可以看出來，我們這部草案的設計真的是一個基本法。所以他就提到是哪些部會，他都不願意明講，就只有提到政府應該做什麼。當然我們不是說反對立基本法，但是有基本法，其實關鍵還是在於作用法本身。

對於這個部分也是今天我們訪談比較另外核心，除了讓大家暢所欲言之外，另外一個針對我們國內的法治建議調適方向。我們先針對現有的消保法結構，或現階段所曾經面對到的，第一個他到底有沒有消保法適用，從我們現有的商品跟服務上，對於服務這塊是沒有明確在細則當中做定義，但要把人工智慧商品跟服務認定適用消保法，我想這應該沒有什麼太大的爭議。第 2 個就是合理期待的安全性，所以說這塊來說的話，我們站在消保法本身，是一個消費者保護的通案，或所謂的基本規定來說的話，

你說第 7 條針對人工智慧的部分，再去做更限制化的設計，除非是消保法本身有放這樣分章，否則第 7 條我也認為不適合去做過多的變動，所以這個判斷的時間點跟所謂的當時科技可合理期待的安全性，這個部分也許就是比較適合，由司法實務來個案認定。

109 年最高法院判決所提到的技術標準，之後有沒有可能被延伸應用在人工智慧後續衍生的民事責任，這可能性是在，因為這部分，看起來的話，我相信後續人工智慧商品服務衍生的爭議會越來越多。

第 3 塊，就是消費資訊揭露，我們認為消保法本身不適合做過多的，因為如果考慮到它是一個整體性規範的話，這邊可能比較可以考慮，是不是把它放到定型化契約裡面去做一些規定。有關於定型化契約，後面還有一頁簡報就是針對定型化契約這一塊。在民事責任這部分，我們也認為現有的民法跟消保法本身來說的話，我們在消保法的嚴格責任，跟在民法的一般的過失跟推定過失，應該現階段是足夠來處理這些問題。

在中長期我們一些立法路上的問題，比如說民法本身來說的話，第 191 條之 1 能不能適用在服務，或要不要類似像歐盟一樣，有一個人工智慧專門的民事責任規定，這個可能是在中長期，也許可以考慮來納進來。所以說定型化契約這塊的話，現階段來說的話，先前在消保處啟動審查的時候，他們本身就提到幾個問題，包括第一個我們的目的事業主管機關跟他的產品跟服務的對應關係，再來就是如何去叫動目的事業主管機關，這當然是長期消費者保護的老問題，不過這個部分來說，如果今天建議可以針對現有的定型化契約去考慮增訂消費者保護。在裡面要增訂有關於人工智慧的規定，比如說應記載事項放消費資訊揭露或不應記載事項，因為我們現在很多會關注人工智慧，就是人工智慧的偏見或歧視或隱私保護的問題，所以說一個部分，我們是不是有辦法先優先選定一些特定的機關，跟他制定的定型化契約，再來就是放哪些規定，所以初步我們建議就是可以以產業可能跟人工智慧連結，或數位化連結會比較深的幾個產品或服務，而這邊我大概初步抓 6 個，當然這就是以我們現在已經有的，後續如果說有必要，也許由消保處再去協調目的事業主管機關定新的，但以現有來說的話，大概認為這 6 個是比較合適的，至於訂的話，我覺得如果放太多，反而會變成有點未雨綢繆，比較務實可能是消費資訊揭露放在應記載事項跟不應記載事項，也許可以放一個比較屬於宣誓或比較屬於警示性的規定，要求如果應用到人工智慧的話，確保人工智慧系統本身不應該有偏見歧視，或有侵害消費者隱私的情況。

而這個問題大概就是條例式的，大概主要針對我們目前建議消保處這邊可以考慮的法規調適方向的話，請 3 位專家給我們一些建議。

(A)：

對於剛剛報告的內容，我幾乎全部都讚成，都沒有什麼意見。首先提到關於我國到底要制定一個專法，還是要將人工智慧相關的規範訂在定型化契約應記載事項裡面。這一點我的看法，在剛才見解中，應該是要放在應記載事項裡面，其實我也同意，因為目前消保處的位階不夠高，要訂一個專法的話，這過程可能會非常的冗長，不知道要花費多少年。

大家都知道現在這個人工智慧，技術的腳步進步非常的快，立法是遠遠跟不上技術的腳步，所以可能在現行的應記載事項去做相關規範，應該是比較適合的。我同意這樣的做法。不過關於剛剛提到人工智慧是服務的本身，或服務的重要部分，沒有錯。業者在提供人工智慧服務的同時或之前，應該要同時或事先告訴消費者，現在業者要提供部分的服務內容是由人工智慧提供的，要讓消費者知道，而消費者心裡面就可先有一個準備說，我接受業者提供的服務，可能是人工智慧提供的，而消費者是不是要繼續使用？其心裡面自己要做個判斷，當然繼續使用，可能就代表說消費者接受業者這樣的一些規範。這些業者將人工智慧置入他的服務本身，或是成為其重要部分，把這個服務上市，提供消費者使用的同時，我認為就已經代表說，業者認為人工智慧的技術已經成熟，是可以提供消費者使用。也就是說，只要提供消費者使用，提供上市的，就代表已符合當時科技水準，就應該要已經符合當時科技水準可期待的安全性，如果對於消費者產生任何損害的時候，就代表你提供這個人工智慧的服務是有問題，是不太成熟,就已經把它上市了。對於消費者所受的損害就應該要負責，至少業者必須去舉證證明說，你提供的服務已經符合可合理期待的安全性，那是因為什麼樣的原因對消費者造成的損害？業者必須要盡到舉證的責任。

至於這個剛剛有提到什麼樣的行業，要適用一些定型化契約應記者事項裡面，要先把它放進去，剛剛提到的這些行業我都贊成，但我建議再增加一個汽車銷售這個行業。眾所周知，目前的汽車銷售都會強調他們的自駕系統，而且目前的法規標準也都有針對汽車提供駕駛或行人的安全性，有一定的基準。銷售業者表示說，我們這一台汽車是符合目前 level two 的一個標準，代表說目前已經可以自動跟車、自動煞停，這一種的技術，汽車都已經具備這樣子的功能，而在銷售上售價會比較高。所以業者既然已經提供消費者這樣的服務，當然要就這些人工智慧所提供的服務要負相對應的法律責任，所以我建議，除了剛剛提到的幾個行業外，把汽車銷售也放進去，因為現在絕大多數的車子都由人工智慧，甚至都還要加錢，以上是我先做一個簡單的報告。

計畫主持人：

關於項目的部分，我也會把剛剛（A）所提到的在汽車銷售這一塊。其實在期中審查，他們大概也有提到，因為這個部分我們人工智慧，今天並不是第一天衍生出這些可能的法律問題或爭議或民事責任問題，而是早期的話，比較像剛剛提到的汽車本身，在交通或金融或醫療，因為本身是一種管制性的行業，所以我們也的確看到早期這些走的比較快的這些產業別的話，因為有產業的管制立法在，所以為什麼人工智慧本身全面性的監管專法這幾年才出現，是因為他開始變成不以行業別為限，幾乎變成是各行各業都在使用，甚至未來可能變成一種標配或預載的一個功能在，所以說這個的確是在我們期中審查，消保處就有提到，可不可以先針對這些人工智慧比較成熟的行業別。這邊也謝謝徐律師這邊的提點，就是對應到這個像交通這一塊，自駕系統的確是在車子裡面，或輔助駕駛變成是一種標配，所以我會把這個再納入到我們建議優先增加的一個定型化契約的類別中。

(C)：

我覺得大致上先就這4個主題有幾個部分來分享一下我的一些看法，假設考慮我們國內的消費者保護的法制這一塊而言，就就如同剛剛提到，我們是不是就以現行的這種消保法結構裡面去考慮定型化契約的這個部分，那當然AI的應用真的是範圍還蠻大的，如果你今天要用一概而論的這種消保的邏輯，去訂定單一的相關規範其實是有一點困難。不過這個部分我倒是可以建議是說，實際上而言，對於消費者的角度，人工智慧的應用，其實對它可能會有什麼樣的影響，至少我們在某一些程度上的事務是可以先讓他了解，或對業者有所要求的，舉例來講，像是剛剛講到的揭露義務部分，到底要揭露哪些東西以及他到底是要從哪些層面介入，譬如說他是一個商品類型的揭露，還是他是設計服務的部分，應該如何去做揭露，我想現在目前來講，國際上有很多針對消保議題的討論。

會關注消保讓消費者他可以在使用服務的時候，一開始他碰到這樣一個服務提供者，他是人工智慧的這件事情，他能夠有很明確的知曉這些資訊的這個取得，怎麼樣才能更明確？我覺得這個地方未必是一個定型化契約可以做到，因為如果你是只放在各行各業，其實有時候要分別去訂，還要找相關的主管機關，也許可以考慮去訂一個指引或指導原則這樣的一個部分，把比較共通性，針對人工智慧商品服務提供給消費者共同性的這個部分需要考量的點，比如說它的開發者、部署者等，他們需要考量的點，這個部分把它提示出來，然後可以讓那產業界的人，他可以去follow這樣。

至於說，我們現在目前消保法的規範要不要做某程度上的調整，事實是可以在商品服務的安全度去做一些考量，實際上人工智慧整體的那個風險，其實要討論的議題其實還蠻多的，所以長遠來講其實我還是比較建議，可以有一個比較大的專法，但當然不是現在一蹴可幾，他可能會是一

個長期面向的考量，這個專法會不會是消保處這邊要處理，我覺得這個專法消保處來處理好像有點太過。因為可能涵蓋的面向，不單純只是消費者保護的議題，還有產品整體的相關一些製造、風險控管、隱私等很多面向的議題，甚至權力的取得，包括今天在一開始 AI 在訓練的時候，權力的取得，哪些高風險的 AI 該出現，哪些高風險 AI 應該被禁止，哪些 AI 是可以被運作這個部分，都不單純只是消費者保護的議題，所以長遠來講，應該要有一個比較具體的專法，也許會是比較妥適，現階段也許可以透過指引的部分，來給大家一些指導，所以我就先初步提供這樣的意見，謝謝。

計畫主持人：

剛剛其實有提到，如果中長期我們是不是應該有一個人工智慧的專法。事實上國科會出來立的這一個法本身就有點怪，不過因為先前的一個政策的分工狀況。剛剛也有提到，中長期其實是不是適合有一個專法，那專法本身來說的話，包括它的涵蓋的一個層面跟包括範圍，當然就不是只有在消費者保護這一塊。從這個本身來說的話，我其實同意中長期有需要的話，我們應該有一個這樣的專法，看到像歐盟這樣子一個人工智慧的立法結構，它是有一個全面性的監管專法，再去思考配套的民事責任，再反過來來思考他的產品製造人責任這一塊，是不是有併同做修正的必要，因為這幾年也發現原本的商品責任這一塊，在遇到數位議題，不是只有人工智慧，包括一些數位內容商品本身，就存在一些適用上爭議，因為過去歐盟本身對於商品製造的責任還是偏向，所謂的物理性有形的商品，所以說這一塊來說，怎麼去處理這些數位內容，或資料經濟，由資料這種驅動經濟產生的一個爭議，他們就想說這一次就併同地做一些修正，所以這是一個我們在中長期也可以評估看看國內這一塊。針對人工智慧，我們怎麼樣地去訂定，或基本法接下來要去落實作用法的時候，這一塊怎麼樣的能夠做一個比較有效率或者整體面的一個考量。

另外的剛剛有提到說適不適合去訂一個指引，其實在整個消保處那邊，先前在做報告的時候，我是有看到像日本的消費者廳，他其實有針對整個人工智慧的應用，也提到 3 個消費者保護的重要議題，包括安全性、自動化決策跟隱私本身的影響來說，其實它的面向很廣，所以說這個部分的話，絕對不是只有單純的去修消保法本身就夠，他也認為說，現階段日本政府的立場是先不做任何的修法，所以他也是藉由發布一些行政指導文件的方式。在 2020 年的時候，就針對人工智慧所謂的消費者保護的一個手冊。今年 7 月的時候，針對生成式 AI，另外又編了一本給消費者參考，不過他比較偏向概念宣導，或怎麼去留意這樣的人工智慧可能對你產生的問題。所以這也是目前消保處這邊有興趣的，也許他們也會考慮說後續有沒有可能用這樣一個比較柔性或軟性的文件先行。

（B）：

基本上剛剛大家說的我都相當贊同。我補充幾點意見，第一個，人工智慧是一個太大的概念，而且是一個太粗略的概念，所以我們如果要落實到實際上法律上來說，它是一個非常複雜的技術的體系，在裡面大分類，至少可以分成生成式 AI 和分析式的 AI，分析式 AI 底下的話，又有各種不同的演算法，你可能針對不同的演算法，比如說推薦式的演算法、辨別式的演算法，它都有不同的技術成熟度，所以如果我們在講所謂的合理技術水準，其實這個必須要去看，它具體用的技術是什麼，所以其實不同的技術會有不同的技術上的要求，現在比較成熟的，應該是在分析式 AI 的部分，他可能已經有比較多的檢測工具可以使用，也有比較多的所謂的技術的標準在，所以如果要從消保的角度去做一些規範的話，我其實會特別建議我們針對像是這些分析式 AI，包括演算法、視覺辨識、自駕車，還有蠻多產品裡面都有這些影像辨識的 AI 在裡面，那這些影像辨識的 AI，它應該要遵守哪些規範，可能是可以跟主管階機關先討論，然後看怎麼樣

去訂指引，或訂到定型化契約裡面。第 2 個，我相當贊成現階段沒有辦法針對像歐盟那樣去做一個很全面性的規範，因為比較好的 approach 應該是從下面個別的應用場景底下開始往上去做，因為每一個應用場景，其實它 AI 做的事情不一樣，我們實際上的用法，大家也在調整當中。

而我想特別提一件事，其實 AI 是一個太新的技術，尤其是生成式，我有個問題就是如果產生人權傷害，就是權益傷害的結果，他到底是服務提供商造成的，還是使用者不當行為造成的，我覺得這個是有可能會有一個問題的，像台德開發者蔡宗翰教授和李玉潔老師，就常講一個例子，他就說，大家都知道，你不能把鐵的東西放到這個微波爐裡面，或者說不能把手機放到微波爐裡面去，這個是我們大家都知道怎麼用，但在運用深層式 AI 這件事情底下，其實你在用的時候，有一些用法是不應該的，其實你是不會得到正確的服務的，如果是這一種消費者行為造成的結果的話，在責任的歸屬，我覺得其實會容易產生一些爭議，所以我覺得在消費者的教育這一段，其實也需要更多的提醒跟教育。再者，剛剛有講到兩種可能跟 AI 有關的消費跟服務的態樣，一個是人工智慧本身就是產品或商品或服務，另外一個是人工智慧本身是產品或商品或服務的重要成分，我覺得這 2 個我都相當贊成，但我的觀察，實際上的狀態是現在有一些它是人工智慧產生的商品，這種狀況是不是會去涵蓋到。比方說，現在美國有一個比較嚴重的狀況，前年 Amazon 就出現很多人工智慧產生的書，這些書的內容，有很多可能是沒有經過專家校正，所以有很多錯誤的。這一種結果特別會發生的問題是在，比如說圖鑑，是像蘑菇的圖鑑這種書，可能內容其實整個是錯的，閱讀者買了以後，拿著書去認蘑菇，可能會產生嚴重的傷害。可是這個好像不算是人工智慧，也不是它的重要成分，但這個商品整個本身其實是人工智慧產生的，這個可能也是我們要去討論的某個態樣，比如你的產品本身是人工智慧，參與進去做的產出，我覺得至少要有揭露這件事情，要讓消費者知道說，我現在買到的這個東西，內容或服

務內容是人工智慧去產生的。比如說接下來可能會有很多報業的服務、摘要的服務，裡面如果沒有揭露的話，可能就會有一些問題出現。總結來講的話，我同意現在的消保法可能還不到需要去調整的狀態。比較好的方式是去做指引，再者是說針對定型化契約，在某些服務態樣裡面去做一些修改，在選擇這些服務態樣的時候，我覺得剛剛舉的那幾個例子都蠻好，但也許可以再多看一下比較成熟的這些 AI 的應用方式裡面，也許還有其他的定型化契約，可以先去做一些提醒跟一些更新的，那我大概就先分享到這邊，謝謝。

計畫主持人：

早期我們的確是比較自重在分析式的 AI，在歐盟或更早 OECD 裡面，就把它界定為人工智慧系統的概念，這兩年從這個 open AI 的生成式 AI 之後的話，歐盟本身立法也把通用人工智慧或生成式的 AI 跟加進來，所以說這個分析式的 AI，我們來處理它的消費者保護議題，相對的時間或整個規範上，相對的輪廓會比較明確，生成式 AI 現在怎麼樣。第一個，衍生的爭議是不是已經夠多，或適不適合立即的介入做處理，因為也看到比較多，關於這一塊討論，像是在智慧財產權，或在於它內容的偏誤這塊。所以剛剛也提到一塊，如果我們對於這個要不要適用消保法，如果只是看他本身，比如像分析式的 AI，本身就是一種商品，或整個 AI 是他的在商品或服務的重要組成部分之外的話，要不要把 outcome 把 AI 生產製出來的，像這樣一個圖鑑個例子。所以我也會在關於我們適用消保法本身的話，除了我們所提到兩種情況，它直接作為一種商品服務，以及作為所謂的重要組成部分之外的話，可能是人工智慧的一個產製出來的結果。我覺得這的確是我先前比較沒有特別想到這一塊，所以說這邊也像非常謝謝（B）。其實我們大家都有共識，人工智慧本身，我們應該針對應用相對的比較成熟，所以這一塊提供給消保處的建議我可能也會像 2017 年的時候，我看

的是一個 PwC 的報告，就針對交通、醫療跟金融這一塊。如果一個比較新的這種人工智慧，特別在分析式 AI 應用市場別來說的話，目前醫療保健還是第一名，金融大概是第 2 名，第 3 名現在是製造業，第 4 名是在所謂的法律服務，還有一些相關的服務行業，第五是交通。因為今天這個討論，也許我把這幾個領域先抓出來，把我們現在已經看得到定型化契約，能不能就往裡面丟，也許就是到時候讓消保處可以了解，以整個產業應用比較成熟，或者這個相關的數據所呈現出來百分比的領域當中的話，現有有哪些定型化契約，先放進來這個，到時候讓消保處來評估，看看說這些是不是先針對裡面哪幾個讓目的事業主管機關來評估要不要去增訂他的定型化契約本身的一個條文的增加，或者說修改，那消保處本身可以做的，也許就是像剛剛（B）提到，是不是先用一個指引的方式，做一些比較屬於通案的，有點像是消費者教育的概念，我們先用一個比較屬於軟法或行政指導的方式。

（C）：

我覺得生成式 AI 這件事情，我蠻贊同（B）那邊講到的，AI 應用面向很大，即便是生成式 AI，它也是在不同的領域去做運用的，我現在看到大部分都是針對生成式 AI，比較大面向的一些指引，我覺得在消保這個層次，有些已經處於它的應用面，面對到使用者，所以在這個階段來講，他到底應用在哪個層面，從那個層面去做處理會比較妥適，要不然現在你提一個大的，其實現在大家都在寫，用途好像也沒有那麼大，所以倒不覺得現階段而言，我們就有辦法就單純生成式 AI，這樣一個基本的模型操作去做這樣的一個規制，我覺得是比較困難。假設說今天是要給產業接觸，給消費者一些指導的話，我覺得可以寫一些比較常碰到的面向，甚至有些人反而認為是說生成式 AI，現在對消費者的使用有很多，像是今天去使用 ChatGPT、Midjourney，我今天去使用什麼，現階段大家可以免費或比

較容易去獲取這些服務的層面，消費者他應該注意一些什麼事情，我覺得應該給他一些這樣的一個指導。

計畫主持人：

這些也許到時候，我再評估看看說生成式 AI 是不是立即的，在我們的研究報告要給消保處任何比較屬於實質建議，還是說建議他持續去做關注，因為的確這個連日本他有這樣子，一個針對生成式 AI，還有一些軟法，也都有提到這個部分本身來說的話，面向還是很廣，因為從文字到音樂或影片的生成，甚至到 coding，現在都可以用生成式的 AI。這一塊他們目前的話，還是比較屬於觀察的立場在看，而這個部分的話也許我會比較持保留的看法，或者說寫得比較保守一點點，但是在分析式 AI 的確這一塊的話，這個是已經很現實的。比如說我們對於這種分析式 AI，包括屬於推薦的、鑑別式的，像醫療影像的鑑別或說投資性的、理財機器人等，這一塊有時候也會反映出來在消保法本身它還是一個消費關係。像理財機器人，屬於帶有點投資目的的，也許他就不適用消保法或在醫療影像 AI，也會變成像過去一些像馬偕醫院這一個，就是醫療行為要不要適用消保法。

總結，還是比較回到比較務實，因為 AI 本身還是一個很大的面向，我們怎麼樣去結合現階段產業，大家的共識？產業運作或人工智慧的使用，相對的比較成熟一些領域，還有一些現階段已經可以實際看到或自駕車這一塊。因為這個的確是很現實的，這個已經是我們生活當中可以感知到的，所以最後提供給消保，除了這邊的建議的話，也會把今天 3 位專家的一些看法融入到我們最後所形成的結論。

（B）：

因為我們會提到通常技術水準這件事情，其實評測工具非常重要，現在人工智慧很大一個問題，就是沒有好的評測標準跟工具，所以你要說他到底是有沒有符合那些，比如說準確性、歧視、不歧視、公平，這些其實並沒有一把很好的尺量。從消費者的角度來看的話，其實會非常需要這件事情，這個其實是現在數位部也在做，但可能速度需要更快一點。

計畫主持人：

中研院這邊已經開始針對 AI 的評測這一塊，有持續的推動，不過這一塊，包括歐盟本身，他們像這種人工智慧風險的分級、分類也會遇到類似的問題，就是說這個評測的標準，因為人工智慧風險本身是一種有生命週期的，所以說到這個誰能夠說了算，

所以我們也也蠻期待說，數位部這樣一個評測中心或評測工具。未來能夠扮演它一定的功能跟角色，非常謝謝（B）的提醒，因為這一塊工研院其實也有找過我去討論一些，包括國際性的一個規範，所以說這一塊來說的話，因為這個一體兩面，法院對這塊不夠了解、沒有一個好的標準，或者今天想要找一個所謂的專家鑑定，可能都不想要找誰，所以說這個也可能會讓業者就裹足不前。今天這個可能之後衍生出來的，特別在我們消保法這一個嚴格責任的情況底下，從另外一個角度無法讓消費者享受到這個 AI 產品或服務帶來的一個便利或好處，這個也是很可惜的。這個是到時候會再把它寫到報告當中，謝謝。

訪談紀錄二

訪談時間	民國 113 年 10 月 23 日	
會議地點	國立成功大學	
受訪人	D	法學教授

訪談內容：

（D）：

關於強化人工智慧商品或服務的消費者保護法制，我對於研究團隊所達成的結果非常欽佩，而且我都很贊同。人工智慧本身對於消費者權利的影響，隨著人工智慧的加重跟加深，這個影響一定是越來越明顯。對於消費者保護這一塊，我覺得應該要提早重視起來 我覺得這個研究團隊的想法非常好，又把世界各國目前的法制來做個介紹，又著重來介紹歐盟的法制 那我覺得這個方向是比較契合我們台灣現在的方向。畢竟我們是大陸法制國家，對於歐盟相關法制不僅是在法律規範上或在移植的便利性上都有一定的優勢，所以對於研究團隊來側重歐盟的規定，而密切觀察歐盟的規定，並適當的加以引用，我覺得研究的方向完全的贊同，也非常的肯定。

再來，對於人工智慧今天在運用上，我覺得有一個困擾，有些是專門本身這些商品或服務就是人工智慧主要的結果，譬如自動駕駛，自動駕駛主要都是靠 AI，但像這個問題其實很需要重視，也應該加以釐清，但我想另外一個需要加以釐清的就是，如果說只是在商品跟服務中有參雜一些 AI 的因素，並不是整個商品或服務都是 AI 所提供的，但有一部分借重 AI，這時候該怎麼來處理？舉例而言，AI 這時候可能只是一個輔助，在生產或者在運送中，把 AI 做一個輔助，我覺得研究團隊所提供的關於 AI 要向消費者說明這塊，這個大方向絕對是對的 讓消費者知道他所接受的商品跟服務有一部分其實是 AI，如果是全部的話那比較容易，或有一部分來自於 AI，我覺得讓消費者知道，本身就是消費者保護的一種態樣。這個研究團隊也加以支持，認為要讓消費者在消費之前就知道一部分是 AI 的成果，我覺得這很好。可是我覺得可以適度的加以區隔，也就是說今天一件商品涉及到 AI，到底是指的是生產部分，還是它的功能效能部

分，還是說從生產到運送。如果是國外的話包含進出口，最後到消費者的終端的地方。是不是每一個過程涉及到 AI 都需要說明，這個可能對消費者而言，我覺得至少安全性而言比較沒有需求。今天像生產有 AI 來輔助可能對於產品的安全性會有一些比較大的疑慮，但如果說它生產好了，只是在運送過程中有涉及到 AI，譬如說像運輸的方式、自動化倉儲，這些都會涉及到 AI，還有自動化倉儲的提存，還有路線編排，這些如果都涉及 AI，這一塊可能對消費者權益受到的影響，可能就沒有那麼的明顯。如果說我們的一種規範方式是可以只要涉及 AI 都要揭露，都要讓消費者知道，因為消費者持著權益，這是一種規範方式。另外一種，如果說這個商品跟服務，只是在生產、運送、進出口、經銷、零售方面有遇到有加上 AI 的成分，這時候要不要全部都要跟消費者來揭露，我覺得可能有時候揭露太多，可能消費者會被訊息淹沒，反而會沒那麼重視，因為他發現怎麼到處都是 AI，每個都講的話，他可能就不是那麼在意。另外一個考量是揭露要成本，今天要求的揭露越多，實際上最後還是會轉嫁到消費者身上，所以如果要保護消費者的話，我覺得在台灣還沒有一開始想要保護的時候，建議研究團隊可以考量循序漸進，不要一步到位，若一步到位的話，只要涉及到 AI 通通都要揭露。如果能夠循序漸進，只是先就生產這一塊要先揭露，至於其他的倉儲、運送、進出口，這些可能對 AI 的成分，可能就沒有揭露的急迫性，我覺得研究團隊在已經是很正確、很好的基礎上，可以有再進一步思考的地方，這個是關於揭露的部分。

另外關於資訊的的個人隱私、資訊的流傳、資訊的採用，因為很多時候，AI 其實可以自動收集很多的資訊，而資訊的收集跟保存這一塊，也會跟個人隱私與消費者保護有關。關於這一塊的話，研究團隊的方向有側重到這一點，我覺得也很好。但這個之前我在前一次的專家訪談裡面，講過 AI 實際上其實可以分兩種，一種是主動式的、一種是被動式的，而今天很多時候 AI 是在主動式上，就是消費者主動的使用 AI 或是用 AI 的輔

助完成消費行為。被動式的主要就是去收集建檔，像是消費者的喜好、消費能力的多寡，譬如說這個人到我們店裡來，向來消費都是一兩千起步，這時候就覺得這是可以來多多開發行銷的一個好對象。這其實也是 AI 在收集的，在消費偏好上，譬如說他不吃牛、不吃豬、生物特徵，這個客人一進門還沒講話，後面開始就叮叮叮叮，我們大客戶來，馬上手邊的電腦就跳出這個人的個資，然後就開始熱情地打招呼，就說你來啦，給你有貴賓般的感受，那這當然就仰賴 AI 平常就要收集。像這些都是被動式的 ，跟消費無關，但在消費過程中往往也會有 AI，像這兩個對於被動式的這些要不要告知，這也是一個難題。像我們剛剛講到生產運送的時候，要涉及到 AI 的揭露，可是這時跟你的生產運送沒關。也就是說，今天我們到一家商店去買東西，我偏好買什麼樣的東西，譬如說我比較喜歡紅玫瑰，那我就偏好紅色的花朵，那我不太去買白色的花朵，而這些偏好實際上，跟我這一次的消費沒有直接關係，可是這個是不是重要的資訊？其實也是。或消費能力或他的付款能力或來的頻率。因為有時候像消費可能他一次都可以消費一定的金額，每個月還很頻繁的過來。有些是隔了半個月、一年或兩年，大概過來一次，這種消費頻率，本身也是一種個資，所以像這些資訊的收集要不要揭露，這可能也是一個很難解的問題。因為這個是很容易就可以收集的，但收集這些資訊絕對也是個資。有時候資訊流出去之後，我也不想讓人知道我平常來的時候，我明明到大飯店，可是每一次都只點一碗滷肉飯，卻讓人家覺得我平常都在大飯店吃飯，或者我就只點沙拉、義大利麵，但是別人都以為我來吃大餐，但實際上我在裡面吃貝果，所以像這些其實都是涉及到個人隱私，最理想的情況就是要取得消費者同意或告知。另外就像現在一樣，幾乎我們是沒有管制的，我們法律對這一塊沒有管。對消費者權益上，我覺得值得研究團隊進一步的思考，就是到底該怎麼做，我覺得不妨區隔一下，我們剛剛講的，從生產、運送、販售這幾個點，可以著重在揭露生產這一塊，慢慢的循序漸進，同樣對於個

資的收集，可能也是可以循序漸進，或是不妨在消費者一開始的時候，就告知他可能會收集，就像我們現在打電話給客服，很多時候在電話接通客服之前，他就跳出一段自動語音，就是說本電話為了提供更好的品質，電話可能會被錄音，所以這時候你繼續來使用的話，其實是同意的。類似這樣的做法其實也可以，今天你來這邊的一切消費行為，可能會被列為數據，這種先告知實際上也是一種方式，我覺得只是一個小建議，但研究團隊集體的智慧一定更能夠深入的針對這議題來討論，我只是拋磚引玉讓大家或是讓團隊做參考。

再來，談到我們國科會的所提出的人工智慧的基本法草案、人工智慧發展法，它都是一個基本法的性質，有一個缺點，其實只是方向的指引，細部的規定還是要靠細部的立法或執法來加以落實，當然有規定總比沒有好，但是細部的落實這一塊，我想可能研究團隊也可以試著提出更多的建議，因為目前研究團隊好像就是把這個基本法影響跟消費者保護法做一個合併的觀察，我覺得這當然也很好。譬如說像我們消保法的第 4 條、第 22 條跟第 24 條，這些研究團隊把它做的很好結合，我覺得這個很好。但可能對消費者保護而言，有可能還是不太周到，所以我覺得可以先開個頭，我們把這個人工智慧發展法或人工智慧基本法相關的議題 可以擇一兩條來討論，作為下一次更深入計畫的基礎。因為這個研究計畫有時間性，還有研究計畫當時需求書的範圍所限制，也強烈的建議研究團隊向委託機構建議，能夠讓研究團隊有足夠的時間跟經費來做更細部的研究，尤其對於執法規範方式或立法方面，我覺得這個其實是可以大家琢磨，如何更細緻的可行的來保護消費者的權益我覺得這個其實是一個很重要的。

最後再看一下提綱，現行的消保法跟定型化契約，也是這次研究團隊的重點。而現行的消保法，本身並不是針對 AI 人工智慧來立法，其實是針對所有消費態樣，在立法的時候，可能也沒設想到 AI 後面的蓬勃發展，所以我覺得就現在消費者保護而言，當然有所不足，因為消費者不是像剛

剛提到的資訊的揭露，絕對不是只知道要有使用 AI 而已，他可能需要的是在哪一個部分涉及到 AI，因為剛剛提到消保法第 4 條就是要提供充分正確的資訊來保護消費者，雖然說是比較抽象的原則性的規定，但是在這個基礎上不妨可以訂一個執法，要求商品服務提供者、生產者、銷售者來結合我們之前講到循序漸進的方式，適度的先開始，我覺得這個可以參考的，把他標示清楚，讓消費者在決定要不要購買這個商品跟服務之前，至少有資訊來做判斷。另外，如何標示這也是一個難題，我覺得不妨借鑒那個基因改造食品，往往大家對基改食品可能也有一些疑慮，所以我們要求基改食品要做適當的標示，我覺得可以從基改食品這邊來獲取一些經驗，然後說這實際上是 AI，是有 AI 參與的，這不見得是負面的，搞不好人家看到 AI 會覺得很新鮮，還會增加購買的慾望，所以有時候在政策、宣導上也是可以來說服業者配合，因為這樣搞不好，對於消費者而言，反而是另外一種促進行銷的方式，這個是很好的例子。

再來，我覺得我們消保法採的是無過失責任，這無過失責任可能對於 AI 的使用者來說，可能這涉及到的是政策考量，也就是說，跟我下一個建議可能是可以相輔相成，我覺得建議研究團隊在呈現研究成果的時候，不妨站在行政院的角度，也就是委託單位的角度，可以列一個保護比較強的跟保護比較弱的建議。所謂保護比較強就是所有 AI 要納管，這個當然保護最強，可是所耗費成本最大，不管是政府的監管成本或是業者的法令遵循成本，都是最高的。這個絕對是一種規範方式。另外，相對比較弱的保護強度，就是主動的揭露，這實際上也跟研究團隊的成果，我覺得是之前在談到世界各國的法制，譬如說談到歐盟模式、英國模式、美國模式、日本模式，而不同的模式實際上其實也是不同程度的政策選擇。我們臺灣到底要選擇哪一個，雖然說我贊同民眾團隊，我們可以採比較保護消費者，強度比較強的方式來立法，但是有時候，也可能要兼顧一下現實，太理想性的，可能在推動上可能會有一些障礙，但像研究團隊的成果，我覺得不

妨提供這種政策選擇，藉由我們研究計畫，幫助我們的行政院或幫助我們的政府在制定相關政策，甚至要不要修法來保護消費者在做這樣決策的時候，可以藉由研究團隊的幫忙，提供不同的相關配套規定，當然並不是說要一次解決所有的領域，我覺得不妨可以再細分，可以在未來的研究上，慢慢的一步一步的把它做好，但這個可能是一個思考的起點，就是說我們可能把不同強度的法制，配合研究團隊已經掌握的不同國家的規範方式、不同的強度，我們也提供不同的建議。因為研究計畫執行到現在要做大幅度的增加，可能時間上來不及了，但不妨可以建議行政院，或者最後在建議的時候，可以說這是未來再深入研究的點，最好能夠由研究團隊在既有的基礎上繼續往更深的地方鑽研，實際上也是大家的福氣，所以不妨在研究計畫中也可以談到未來可能，或者加一個章節，就有幾頁，談到未來可能需要進一步研究的哪些點，這個可能也是一個。藉由在之前剛講到的一些，如果時間來得及的話，可以做不同強度的修正建議，或如果時間來不及的話，至少可以單獨列一個章節，就說目前研究團隊的成果已經相當的豐碩，但是因為時間的限制，接下來這些面向，也是有研究的急迫性，但可能就需要在下一個研究的計畫再來完成或未來打算完成，至少我覺得如果目前時間上來不及，不能提出這種不同輕重或保護周密性不同的修法建議，這個沒有關係，至少要把未來就這一塊單獨成一個研究主題，進行研究的可能，可以先把它點出來，這樣的話，也會提醒一下我們的主辦單位，這是急需要研究的，有一定的迫切性，但因為主辦單位或者委託單位可能沒想到或沒有想得這麼清楚，這時候我們的研究計畫可以提供一些建議。這個其實不同的輕重，實際上也點到跟剛剛的問題有一定的連接性，因為剛剛提到無過失責任，很多時候我們在政策上要保護消費者的同時，也鼓勵 AI 的創新發展，這時候就可能要給 AI 一些彈性，如果說我們的政策主要是以消費者保護為主，這時候對於消費者保護這一塊可以多強調一點，可以比較少去考慮到對 AI 產業的成本的增加或負擔，這是

政策選擇的問題。那該怎麼做？至少我覺得研究團隊可以貢獻的是可以來提供一些政策的選項、提供一些學理的支持，讓政府在做決策，到底是要採美國模式、歐盟模式、英國模式、日本模式之前有一些參考，這樣的話，就跟前面剛剛講的幾個點可以來產生一定的連結性。這個是關於政策選擇、責任的問題，還有 AI 產業跟消費者權益要平衡的問題，這些實際上也是研究團隊可以來進一步琢磨。我想這大概就是目前在拜讀這個研究團隊的研究成果，初步的想法，跟研究團隊來分享。

訪談紀綠三

訪談時間	民國 113 年 10 月 24 日	
會議地點	國立臺灣科技大學	
受訪人	E	法學教授

訪談內容：

（E）：

一開始接到你訪談邀請時，先去找了幾篇文章，我發現不同的文章，他們觀察的點，跟我們從法體系出發不是很一樣。舉例他會考慮到 AI 的應用會不會有所謂的價格操控？我跟朋友叫車，我會比較貴，朋友會比較便宜，他會考慮我們的位置、手機，還有我們常常叫車，所以這是 AI 應用可能的負面。除這一篇文章，我發現大部分在看 AI 的時候，所有人都會關注一個議題，就是 data，這一些數據，data、data 跟 data 到底會怎麼樣，他們擔心會不會有歧視偏見或不正確，但我覺得這一篇文章有一個比較有趣的點，他說全部都是 AI 引用後。像有很多客服全部變成不是人以後，我好希望有一個體驗，可以跟著客戶體驗的需求出現，這一篇文章他談的就比較上位，就為了避免 AI 產生偏見，希望除了隱私跟資安以外，

可以併入考慮當事人的自主權，我在消費也好，不管是自駕或購物也好，你有沒有經過我的同意就收集我的資料，甚至要求未來 AI 的開發商，應該負起所謂的社會責任，所以他提出有關 AI 倫理道德的相關的挑戰，要求必須重視客戶的體驗，強化一般人跟人的 social network。就像現在臺科大的孩子有一個很大的問題，不太跟人講話，因為有一群孩子就被認為是後疫情時代，而最近大陸的事業潮很嚴重，這一群孩子被貼上標籤，就是因為他們都不是實體上課，他們是 covid 視訊的孩子，有人認為 covid 視訊的孩子，不管學習的成效怎麼樣，可是跟人互動的頻率是少的，然後 social network 就會變成他們很憂慮的一件事，這一篇文章他談的就是透明度問神意外，還談到所謂的包容性的問題。

撇開這一些國外文章關注的點，我已經閱讀所有的簡報，我覺得你們的簡報基本上是從消保法制體系裡面，基本上會有四大面向的產品責任、定型化契約、特種買賣跟消費秩序，而產品責任的部分，就會呈現在目前的命題，我沒有辦法很清楚的去界定所謂的 AI 跟商品服務的消費者保護。舉例來說，AI 應用在商品，就像提到自駕車。那 AI 的所謂的服務是純粹。還是說我們在做 healthcare 的 logo CT 的輔助軟體，它算是一種產品，還是一種服務？所謂的服務是真的要 AI 來提供服務嗎？像是現在有很多餐廳是 AI 來端盤子，那 AI 來端盤子，如果不小心他的湯、水倒到你身上，我覺得比較難界定的是在既有的消保法裡，針對商品是有定義，可是針對服務是沒有定義，之所以沒有定義是透過函示來解釋，可是並沒有針對 AI 的應用，到底要應怎麼樣才叫做是一種服務的類型或態樣？我覺得這個部分是沒有的。目前本來對服務就沒有定義，更何況對 AI 提供的服務就更沒有定義，我覺得這個部分到底應該怎麼看？舉例，我剛剛說的送餐機器人，他到底是一個產品，還是服務？那個機器人服務人員，如果他把湯湯水倒到小朋友上，一定是找餐廳，而餐廳就會去看，是他設計有問題，還是那個小朋友沒事把腳伸出去，害機器人跌倒，還是場地有問題，

而那個是後面問則跟咎責的問題，跟他是不是 AI 有沒有必然的關係，我覺得這個部分可能需要更多的資訊才能夠去做應用的服務類型，我覺得這個部分可能需要再去思考一下。

如果回歸消保法，基本上不管你提供商品或服務，他的責任基準是以消保法第 7 條第 1 項可合理期待的安全性，從司法實務跟歐盟的相應規範，我們可以建構所謂可合理期待安全性的類似技術標準，不能說是準則，但至少是一個指引。這個部分可能是你這個計畫可以做，而且會有比較大的亮點的部分就是，當所謂的 AI 應用的過程裡面，什麼是我們可以期待的安全性，我們怎麼去檢視它有沒有所謂的沒有辦法滿足消保法施行細則第 5 條裡面可能合理期待安全性，基本上它呈現出來的態樣可能是設計、生產、製造的瑕疵或帶警告的瑕疵，我覺得如果可以扣合這 2 個，從消保法施行細則第 5 條，去解釋可合理期待的安全性，再去建構所謂的瑕疵，或強化消費者保護的類型，我覺得這個部分是可以做得到的。

比較難的部分是舉證的部分，目前消保法第 7 條之 1 的舉證責任，如果要企業經營證明這一件事做得到呢，如果做不到就很像車子會有又要第三方鑑定的問題。我覺得這個舉證這一個部分是難的，除了舉證難以外，還有就是因果關係，原因跟結果的關聯性。以因果關係而言，目前實務才是相當因果關係，可是那這時候，不管是舉證或因果關係，可能要再去思考一下有沒有其他的案例可以來輔助我們，在未來如果發生相應爭訟的時候，舉證責任的合理分配或因果關係應該怎麼認定，目前我是沒有特別看到有針對 AI 有特別去談論這個部分。但我覺得不當使用這個部分也是一定可以做的，就如我們提到的自駕車，它會有分不同的等級，會要求使用者舉例，不可以閉眼睛不可以睡覺，不可以全離手。可是當他閉眼睛睡覺全離手的時候，這時候我們就會問，他是不是有所謂的當使用，而可以適度去過免掉或 balance 掉舉證責任的問題，因為目前舉證責任都在企業競爭，但是使用者會不會有所謂的不當使用這個部分，我覺得可以併

思考，讓權利義務關係降為衡平。至於以產品責任的體系的最後的部分就會是在於損害賠償的計算。計算的前提，我覺得必須建構在誰該負責？那傳統的損害賠償計算有財產上、非財產上跟懲罰性，財產上有所受損害跟損失利益，可是那都是以人為本，但他是 AI 的時候是不是損害賠償計算會不會有不同，舉例精神上的損害賠償，請問 AI 有精神上的損害賠償？就像更換手機跟上一隻手機的語音助理 Siri 告別的時候，要不要考慮？當你從舊的體系去檢視的時候，或許我們可以挑出在既有法體系裡面，有什麼是我們可以去反思或思考的點，但是如果談完產品責任以後，我覺得就目前反對裡面提出來的定型化契約，而團隊提出來的定型化契約在 28 頁，目前幾乎都全部鎖定是通訊交易。我說消保的法體其實是產品責任定性化契約，其實特種交易跟消費資訊的揭露，那定型化契約，如果以你們目前挑出來全部都是通訊交易的話，我覺得他的好處是定型化契約跟特種交易做的法體系的整合，但是它的壞處是沒有什麼亮點。我看了一頁，我會覺得如果以目前挑的這一些定型化契約，它只會在應記載的部分加警語，在不得記載的部分加免責的規定，沒有太多亮點。因為 AI 的應用對他們的產生的衝擊跟影響，並沒有因為產業別而有太大的差異。反過來如果你要問我，針對於 AI 應用比較多的產業下手舉例，健康照護產業金融跟零售業，他們各個產業有不同的特性，而且他管制密度也不同，反而比較容易去凸現出研究團隊去中整這一些定型化契約的價值，舉例零售業，就很擔心那個停損行銷或個資外洩，像韓國支付平臺，把所有資料都給中國支付寶。那金融 fintech 就會銜接到支付，健康照護產業就會牽涉到資安及國安 DNA 外洩，對於非遺傳的基因資訊或許比較不在乎。可是遺傳的基因資訊，他就會被很要求，美國 FDA 針對這一塊也有一些特別的規定，如果你問我，我可能不會按照研究團隊的建議作為優先對象，我也想要切入就是 AI 應用比較多的產業作為 approach 的點，我覺得或許會不太一樣。至於從我一開始說的，到底有哪人工智慧可能產生的問題，我

有稍微寫一下，比如偏見、隱私、資安、自主權、歧視跟濫用，我覺得這一些問題在國外的文章都有討論過，我可以全部留給你，但如果這一些問題要回歸到我們的法體系會呈現在哪裡？產品責任的部分。所謂的可合理期待安全性，我們要不要考量隱私跟資安，因為我們以前在談那個可合理期待安全性通常是在產品本身，可是隱私跟資安是不是會成為一個新的可合理期待安全性的技術標準？我不知道。

第 2 個你們有問的一個問題是我國法治如何去評斷？未來有沒有相關的規範足不足夠？陳如我剛剛說的，目前國科會只有 AI 基本法，裡面只做一些原則性的規範。舉例剛剛 AI 應用的第一名健康照護產業，AI 應用的第一名在 AI 基本法裡面講的還是全部都是基本法，有沒有辦法去區別所謂具有遺傳性質的個人基因資料，還是不去有族群或遺傳特性的 data。舉例 EHR 跟 EMR，這個時候就會出現在我們今年年會理事長特別提到，臺灣是 AI 硬體的強國，目前排名世界第一，可是我們在健康照護底下，我們會變成健康照護軟體的殖民地，理由是什麼？因為我們鎖國，我們的健保資料也不能用。舉例穿戴式裝置的納管，FDA 有一些是不納管的。但如果我們什麼都不能用，臺灣不可能有新創，這個時候就是他很擔心的，會不會我們會融為 AI 的殖民地，什麼的殖民地？健康醫療資訊軟體的。因為目前他們所有收到的 data 都是白人，沒有有色人手，黃皮膚的基本上會是中國新加坡跟臺灣，而中國管制很嚴，新加坡樣本數太少，臺灣具有名客台外四大族群，華人基因的縮影，又有戶籍資料又有健保資料，我們可以有很好的發揮，但如果我們沒有把這一部分去做相關產業跟新創的應用，台灣會失掉自己的市場，然後面對這樣的問題，AI 基本法裡面有沒有？沒有，最簡單就是穿戴式裝置裡面的東西可不可以用？台灣不能，但是臺灣的穿單式裝置有沒有賣到國外去？有。那面對這樣的問題，現有的民法跟消保法夠不夠？不夠，他可能會涉及個資法，甚至於個資法、甚至於個資委員會、GDPR。所以面對這一些跨國的問題，我覺得是應該

要做相應的保護跟準備好，至於剛剛文章裡面有提到透明度，所謂的包容性，我覺得這一題我不知道該怎麼去解釋它，也不知道該透過什麼樣的立法？

就如同我剛剛告訴你，我今天去國科會開會，他們健康臺灣 2 個禮拜前開過會，他們擬 AI 基本法，可是就如同我剛剛講的 AI 應用第一名是健康操照護產業，可是這一些健康數據誰管？他提了幾個，數位部，但數位部不會管這個數位部，頂多參考歐盟把資料做分析好。個資委員會不會管這個。

那天時在 BTC 的會議，有個老師向個資委員會提出，你們可不可以擬一個範本，類似定型化契約，讓所有的健康照護產業大家都很清楚，第一個要做什麼？我需要告知你，我需要尊重你，autonomy 和 privacy 很重要，當我們在產品責任談到資安跟隱私的時候，在定型化契約裡面，有沒有可能把 autonomy 放進去，在收集的時候先取得人家的自主跟同意好，更重要的是要不要讓人家退出的機制。

這禮拜《赫爾辛基宣言》，2024 年 10 月版出現，他有去 Echo 台北宣言，他同意可以做 2 次理由，而面對 HER、EMR 是不是都在做 2 次利用，因為我們原來是看病，可是除了看病以外，如果我們不把這一些資料提供給 AI 做分析，未來在健康照護的領域，我們會被忽略。理由很簡單，未來整個藥物的研發，它不知道我沒有什麼病，不知道我們用藥的術後，也不知道這一些病對我們會有什麼副作用，所以對我們反而不是一個有利的保障。

我明天會去清大開研討會，我們就會有一個倡議，對非遺傳的基因資訊像 EHR、EMR 應該要能夠開放應用，但需不需要把它分類、分期納管？要。剛剛我們在一起的隱私跟資安的保護很重要的一個點。舉例參考 HIPAA 跟 GDPR 時，會有下一個問題，就是臺灣既有的怎麼辦？像回收新病例 EHR、EMR。新收的是一件事，新收的我可不取得告知同意，可

是已經是舊的資料可不可以用推定同意，所以明天我們會提出來的建議就是參考德國跟們日本用推定同意加透出。就是新的是 option in，就是經過 inform consent option in 提供你隨時可以經過你的同意再放進來，但是我保障你退出，舊的我推定你同意，我一樣提供你退出，甚至於我可以在加再同意，這就是我早上被抓去健康臺灣我的問題。

總結來說，這一些資料會從哪裡來？他不一定從醫院來，可能從穿戴式裝置來，而穿戴式裝置這樣的產品，在美國 FDA 有相應的管制規範，他會去隔醫療目的跟非醫療目的，即便是本於醫療目的，在赫爾辛基宣言，面對這一些聲音大數據的應用，我覺得我們應該正視他，所以基本上我已經大概都回答完所有的問題。

附錄四、日本消費者廳人工智慧與消費者保護相關行政指導文件

1、日本消費者廳「人工智慧活用手冊」

日本消費者廳藉由發布「人工智慧活用手冊」，助益消費者了解人工智慧，其包括「基本篇」及「按服務項目別之自我查檢篇」兩大部分，本研究整理其重要內容如下，以作為我國消費者保護主管機關評估與推動之參考。

一、基本篇

(1)、消費者周遭之人工智慧

消費者身邊有許多活用人工智慧的產品與服務，此一技術也被活用於支撐社會的結構之中。包括支持生活與支撐社會在內的相關人工智慧應用，讓人們的生活更加安心與安全，也帶來了便利與豐富[150]。

(2)、人工智慧的便利性

在以往的系統中，「人類」需要事先提出分類所需的條件（模式）並基此進行程式設計，而根據人工智慧，電腦可得分析給定的資料，並自動發現適當的分類條件（模式），其結果則是消費者可得輕鬆做出更為準確的決定，人工智慧透過持續學習資料，當趨勢發生變化時，可以得出反映其變化的分析結果[151]。

---

[150] 消費者庁，AI 利活用ハンドブック：AI をかしこく使いこなすために，頁 2-3，2020 年 7 月。

[151] 消費者庁，AI 利活用ハンドブック：AI をかしこく使いこなすために，頁 4，2020 年 7 月。

如果將人工智慧作為「人類的支持工具」進行利用，則人工智慧在各種場景中都可望作為「好夥伴」加以活用，其示例如下[152]：

利用場景	便利性
可根據人員在場/不在場及其所在位置，操作空調並自動調節溫度與濕度。	• 使生活於舒適空間成為可能。 • 實現了降低電力消耗，以及調節用電高低峰。
兒童與老人的看護支援	• 可以安心外出。 • 更便於參與工作、社區活動等。
由機器人管家推薦新聞、推薦電視節目等	• 在無法騰出手來的情況下，仍可輕鬆搜尋新聞。 • 實際觀賞所擬觀看的電視節目。
根據消費者回家時間預測及自動調節空調，實現家務自動化	• 使生活於舒適空間成為可能。 • 減輕家務負擔。
根據消費者喜好提供食譜建議並訂購食材，實現料理自動化	• 減輕家務負擔。 • 可得輕鬆選擇適合消費者口味的菜色與健康料理。
透過機器人管家控制各種家電與機器人	• 只消有一個機器人管家便可控制家中多個家電與機器人。

(3)、人工智慧是什麼？

人工智慧為 Artificial Intelligence，人工智慧的研究從 20 世紀 60 年代就開始進行，而「人工智慧」的概念也隨著技術的進步而不斷改變，因此人工智慧並沒有固定的定義。

[152] 消費者庁，AI 利活用ハンドブック：AI をかしこく使いこなすために，頁 5，2020 年 7 月。

就當前使用的術語而言，人工智慧實際上係指「機器學習」，因此本手冊將人工智慧解釋為機器學習。現階段人工智慧（機器學習）」大致上具有如下特徵：

1、人工智慧屬於電腦（或使用電腦的系統）：其係使用計算公式等分析輸入資料，並基於人類創建的程式（指令）進行操作之系統。

2、蒐集資料並進行學習：蒐集與累積的高品質資料愈多，人工智慧的分析結果與程式就愈準確。

3、存在蒐集資料的感測器部分與進行思考的大腦部分：感測器部分所蒐集的資料結合出自其他來源的資料，並由「大腦」部分進行分析。

4、一般認為「人工智慧=設備（產品）」，但事實上並非如此：人們所看到的是提供應用程式與服務的智慧型手機和智慧音箱等「設備」，但人工智慧不僅安裝於此類設備之中，還安裝於連接至網路與其他各種場所的伺服器之中[153]。

(4)、人工智慧做得到與做不到的事

人工智慧讓消費者的生活變得更為輕鬆，但人工智慧並非萬能。消費者應根據人工智慧的特點和侷限性使用人工智慧。當前人工智慧不僅可分析數據，還可以分析影像、語言與聲音等各種資料，並從大量不同的資料中，發現模式（特徵）並以較人類更快的速度進行高級分析。

A、人工智慧擅長/可以做到的事：

[153] 消費者庁，AI 利活用ハンドブック：AI をかしこく使いこなすために，頁 5-6，2020 年 7 月。

(A)、從事有明確規則與目標的任務：特別是在將棋與西洋棋領域，由於人工智慧可得立即思考並研究出多種模式，從而人工智慧在此一領域普遍被視為較人類更強。

(B)、蒐集與累積大量數據，並進行複雜的登載與分析工作：諸如擅長自大量資料中提取出不同模式的臉部辨識系統與異常偵測等[154]。

B、人工智慧不擅長/無法做到的事：

(A)、創意工作，應對新興案例：人工智慧不擅長未基於過去資料的創意工作（設計、研究與開發）。

(B)、理解詞彙的意思：人工智慧無法理解語言或上下文，其僅是根據自模型所估計的單字進行應對。

(C)、僅運用少量數據應對個案：在資料較少之下，人工智慧將難以針對個人提供客製化服務[155]。

C、消費者應了解人工智慧的侷限性

(A)、人工智慧並非萬能：人工智慧可以做到的事情，仍然是在程式範疇之內。

(B)、人工智慧所作分析仍未臻完善：人工智慧無法考慮輸入資料中並不存在的元素，而其準確度也將受到待訓練資料的數量與品質之影響[156]。

二、按服務項目別之自我檢查篇

[154] 消費者庁，AI 利活用ハンドブック：AI をかしこく使いこなすために，頁 7，2020 年 7 月。
[155] 消費者庁，AI 利活用ハンドブック：AI をかしこく使いこなすために，頁 7，2020 年 7 月。
[156] 消費者庁，AI 利活用ハンドブック：AI をかしこく使いこなすために，頁 8，2020 年 7 月。

消費者廳針對可能為消費者利用的人工智慧服務，整理了四種類型的自我檢查要點。消費者在實際使用個別服務時，應確認相關要點[157]：

類型	自我檢查項目
1、辨識語音並進行溝通的人工智慧 示例：智慧音箱、互動應用功能	人工智慧可能會錯誤辨識聲音、給予不正確的指令或蒐集關於日常對話之資訊。 □ 消費者應注意故障與隱私風險，並決定何時開啟/關閉電源，以及連接哪些服務（家用電器、網路服務等）。
2、自動操作設備的人工智慧 示例：智慧家電、溝通功能、機器人	人工智慧可能作出與使用者預期不同的舉動。 □ 安全使用考量，消費者應務必仔細閱讀使用說明和使用說明書中包含的其他資訊。 □ 於外出時進行使用應特別留意。
3、提供推薦與建議的人工智慧 示例：飲食/訓練、轉換職業諮商、愛情/婚姻諮商、時尚諮商、投資建議	人工智慧提出的建議，是基於人工智慧所學習的資料範圍內之分析結果，對消費者來說不一定是最好的建議。 □ 消費者應透過評估建議內容及其效果，自行決定是否接受建議。
4、執行審查的人工智慧 示例：就業/錄用審查、貸款審查	若使用於人工智慧的訓練資料存在偏見，則此類偏見可能會反映於審查結果之中。 □ 消費者應確認企業經營者針對可

[157] 消費者庁，AI 利活用ハンドブック：AI をかしこく使いこなすために，頁 9-10，2020 年 7 月。

	能出現的偏見之處理政策（諸如透過人為介入防止偏見）以及其判斷要點。 □ 若消費者有任何疑慮，請考慮使用其他服務。

2、日本消費者廳 2024 年「人工智慧活用手冊－生成式人工智慧篇」

繼 2020 年發布「人工智慧活用手冊」後，日本消費者廳於 2024 年另發布「人工智慧活用手冊－生成式人工智慧篇」：

一、理解生成式人工智慧（生成式人工智慧之定義）

生成式人工智慧為人工智慧之一種，可以根據輸入之指令（文字等）創建文字、圖像、影片或程式等內容。生成式人工智慧也可透過自然對話創建語句或圖像，如同人類之交談。

生成式人工智慧之運作原理，係依據其大量學習之資料（例如文句或圖像），機率性地進行內容之創建，並非藉由實際理解所創建之內容。例如可以生成文句的人工智慧，透過分析選擇最有可能跟隨某個單字之字彙以創建文句。例如，輸入詢問日本的首都，則生成式人工智慧將選擇連結此一問題文句機率最大之詞彙，也就是東京。

對於生成式人工智慧之運用必須特別注意，生成式人工智慧不一定會輸出準確答案，同時若資料來源不盡正確或存有偏見，則生成式人工智慧回應的內容，即可能包括錯誤之資訊。此外，由於生成式人工智慧的回應係基於機率而生，故也可能出現所謂的幻覺現象，亦即出現與現實有所不同之資訊。

生成式人工智慧適用及不適用之用途：其適合之用途包括可用於專業層面，包括協助總結、解釋、翻譯或產生想法。而不適合之用途，則如需要最新且高度精確資訊之情形。

二、生成式人工智慧於社會上之利用情境

生成式人工智慧之實務應用，就使用者端而言，可能是使用者自己運用生成式人工智慧創建內容，或使用者利用提供生成式人工智慧之企業服務，或是使用者接觸由第三人透過生成式人工智慧所創建的內容等三種基本型態。

生成式人工智慧的利用示例存在正反之例，以企業服務為而言，諸如聊天機器人（文章生成運用案例）或虛擬服裝試穿（圖像生成運用案例）等。而反面之運用案例，諸如利用生成內容進行詐騙，包括以生成式人工智慧創建的詐欺郵件，或利用生成式人工智慧偽裝特定人之聲音或偽裝為熟人進行詐騙，其他負面案例還包括運用生成式人工智慧形成虛假圖像、影音或文字，從而影響輿論，或使民眾誤以為其係特定政治人物所發表的言論，從而引發社會混亂。

三、自我檢查表

消費者廳針對可能為消費者利用的生成式人工智慧，整理消費者使用上之自我檢查要點[158]：

自我檢查項目

[158] 消費者庁，AI 利活用ハンドブック：生成 AI 編，頁 4，2024 年 3 月。

使用之前
使用時 □ 請先調查您想使用的生成式人工智慧服務 確認其是否符合政府發布之「人工智慧事業指導方針」，確保其為安全、可靠之生成式人工智慧。 □ 請確認使用條款、隱私政策等內容 切勿使用遭到禁止之使用方式。確認生成圖片或影片之使用條件。
實際使用時
□ 請勿輸入無法被公開之重要資訊 輸入資訊可能被生成式人工智慧應用於學習，並且可能直接提供予他人，或與錯誤資訊結合後進行提供。因此，涉有個人資料等無法為他人知悉之重要資訊，請勿輸入。 □ 請注意所生成之回應內容未必正確 由於基礎資訊的錯誤或偏差，或出於幻覺效應（hallucination）所致，生成式人工智慧的回應內容未必正確。需要專業判斷之內容，應諮詢適當之專家。 □ 針對生成內容公開一事，請根據風險謹慎決定 若有與現有著作相近之情形，可能構成著作權侵害等風險。 □ 當生成式人工智慧推薦購買商品或服務時，請考慮其必要性 對話中可能會引導消費者進行購買。由於可能出現不正確的回應，進行購買時建議保留對話記錄作為憑據。 □ 請勿製作或散播虛假圖片等內容 虛假圖片等可能損害他人名譽或妨礙業務，從而導致法律責任。即使看到吸引人之影片或圖片，請考慮其是否為生成式人工智慧所製作的虛假圖片等內容。在未確認其可靠性之前，切勿輕易進行分享，並謹慎判斷是否適合共享。