編號：(114)012.0901

# 114 年「前瞻數位科技法制政策變革趨勢研析」委託研究計畫

**本研究報告內容僅供本會業務參考**

**國家發展委員會**

**中華民國 114 年 12 月**

編號：(114)012.0901

# 114 年「前瞻數位科技法制政策變革趨勢研析」委託研究計畫

委託單位：國家發展委員會

受託單位：財團法人資訊工業策進會

計畫主持人：陳益智

計畫期程：中華民國 114 年 1 月至 114 年 12 月

**國家發展委員會**

**中華民國 114 年 12 月**

# 目錄

**圖目錄..... VI**

**表目錄.....VII**

**摘要..... i**

**Abstract..... ii**

**第一分項、國內數位法制變革調適與國際趨勢研析.....1**

**項次 1. 113 年焦點議題延續趨勢觀測.....1**

**壹、 AI 著作相關議題國際趨勢.....1**

一、 美國.....1

二、 歐盟.....21

三、 英國.....36

四、 德國.....42

五、 韓國.....45

六、 中國大陸.....53

**貳、 AI 應用之消費者/使用者保護議題國際趨勢.....55**

一、 美國.....55

二、 歐盟.....93

**參、 AI 或演算法運用與勞工權益相關議題.....96**



本報告之智慧財產權歸屬於國發會

一、 美國.....96

**肆、 AI 與個人資料保護及監管相關議題.....124**

一、 美國.....124

二、 歐盟.....142

三、 法國.....153

四、 澳洲.....156

五、 韓國.....168

六、 新加坡.....176

七、 中國大陸.....178

八、 國際合作或會議.....181

**伍、 其他重要趨勢觀測.....183**

一、 美國.....183

二、 歐盟.....203

三、 英國.....224

四、 澳洲.....236

五、 日本.....242

六、 韓國.....254

**陸、 小結.....263**

一、 國際趨勢總結分析.....263



本報告之智慧財產權歸屬於國發會

二、 我國法制整備建議.....272

**項次 2. 國內數位法制調適與變革焦點議題.....280**

**壹、 焦點議題 1：數位科技法規調適—加速法規調適或鬆綁研析 280**

一、 背景說明.....280

二、 近兩年國際發展趨勢重點及歸納.....281

三、 我國法制現況.....328

四、 小結.....343

**項次 3. 前瞻數位科技法制研討會.....353**

**壹、 研討會概說.....353**

一、 背景說明.....353

二、 研討會規劃.....353

三、 議程.....356

四、 其他行政事宜.....358

**貳、 會議報告.....360**

一、 開幕致詞－國發會副主任委員詹方冠.....360

二、 各場次會議報告.....361

**參、 成果綜整.....416**

一、 出席人數及活動意見調查.....416

二、 活動照片及影片.....418



本報告之智慧財產權歸屬於國發會

**第二分項、國內法規環境建構幕僚協助與新興議題因應事宜.....419**

**項次 1. 法制幕僚研析意見.....419**

**壹、 智慧機器人產業推動法制相關幕僚意見.....419**

一、 智慧機器人產業發展背景.....419

二、 國際法制發展狀況.....421

三、 結論.....433

**貳、 跨域資料運用研析.....436**

一、 國際跨域資料運用現況.....436

二、 結論.....458

**參、 國際 AI 運用與著作權刑罰或處罰規範趨勢研析.....460**

一、 國際趨勢發展.....460

二、 結論.....462

**肆、 Cookie 之監督管理國際規範研析.....463**

一、 前言.....463

二、 國際趨勢重點.....465

三、 結論與建議.....481

**項次 2. 工作會議.....484**

**壹、 第一次工作會議.....484**

**貳、 第二次工作會議.....486**



本報告之智慧財產權歸屬於國發會

參、 第三次工作會議.....489

肆、 第四次工作會議.....492

附錄一：114 年度國際趨勢觀測重點法案清單.....495

附錄二：期中審查意見回應說明.....506

附錄三：期末審查意見回應說明.....513



本報告之智慧財產權歸屬於國發會

# 圖目錄

圖 1 現行中央行政機關法制作業程序.....336

圖 2 會議手冊封面.....358

圖 3 現場活動照片.....359



本報告之智慧財產權歸屬於國發會

# 表目錄

表 1 研討會議程.....356

表 2 活動問卷整體看法統計結果.....416

表 3 活動問卷各主題看法統計結果.....416



本報告之智慧財產權歸屬於國發會

# 摘要

新科技運用於創新商業模式對於現行法令體制之適用或解釋產生衝擊，需要充分之討論釐清，甚至進一步法制政策之調整。然而修立法的速度往往無法趕上科技的腳步，此一長久以來的問題，於 AI、高度之算力與超高速網路環境之發展下，更加凸顯。法規調整的速度不但無法因應新興科技之應用，甚至影響新科技創新研發的過程。面對數位科技帶來的數位經濟環境變動，本計畫基於近年來國內外 AI 相關研發應用，及平臺、資料經濟議題所帶來之社會變化與需求，研析法制環境需因應新興科技帶來之影響進行適當之調適。國家發展委員會作為國家整體發展政策協調之角色，掌握國際法制政策脈動，思考國內實務走向或需求，研擬法制政策推動方向。

本年度計畫分為兩個部分:「國內數位法制變革調適與國際趨勢研析」及「國內法規環境建構幕僚協助與新興議題因應事宜」。延續去年重點焦點議題範圍，持續觀測 AI 與著作權、AI 與消費者/使用者保護、AI 與勞工權益及 AI 與個資保護議題，綜整國際法制趨勢發展。同時，為深入探索我國促進資料流通應用及營造友善創新法制環境的法規調和路徑，本計畫透過舉辦研討會，與產、官、學各界專家進行對話，匯聚多方意見及取法國際經驗，為臺灣邁向 AI 之島和實現數位主權，提供平衡創新發展與權益保障的具體法制政策建議。就我國法制整備方向，研析各國於數位科技環境下如何加速法規調適或鬆綁進行，比較我國面對新興數位科技發展法規調適面臨之問題及現況作法，提出可能可強化或提升法規調適效率之建議。



本報告之智慧財產權歸屬於國發會

# Abstract

The use of new technologies in innovative business models challenges the application and interpretation of existing laws, necessitating thorough discussion and clarification, and potentially leading to further legal or policy reforms. However, the pace of legislative enactment and reform often fails to keep up with the development of technologies. This long-standing challenge has been further exacerbated by the rapid development of AI, high computing power and high-speed networks. The pace of regulatory adjustment not only frequently fails to respond to the application of emerging technologies, but may also affect the process of technological innovation and research and development. In light of recent changes in the digital economy brought about by digital technologies as both the domestic and international levels, the rapid development and application of emerging technologies, particularly those related to AI, as well as the social changes and demands arising from platform and data economic issues, this project examines the necessary adaptation of the legal and regulatory framework to address the impacts of emerging technologies. In its role as the coordinator of national development policy, the National Development Council monitors international legal and regulatory policy developments, considers domestic practical trends and needs, and formulates directions for promoting legal and regulatory policies.

This project is divided into two parts: “Evaluation and analysis of the necessity of adjusting domestic digital regulations and research of international trends” and “Assistance in analyzing the domestic regulatory environment in response to emerging issues.” Building upon the key focus issues identified in previous phases, this project continues to monitor issues of AI and copyright, AI and consumer protection, AI and labor rights, and AI and personal data protection. By synthesizing developments in




本報告之智慧財產權歸屬於國發會

international legal and regulatory trends, the project provides advice for strengthening Taiwan's legal preparedness. To further explore the regulatory harmonization pathways for promoting data circulation and application, as well as creating a friendly and innovative legal and regulatory environment in Taiwan, this project convenes a seminar to facilitate conversations among experts from industry, government and academia. By gathering diverse perspectives and drawing on international experience, the project aims to provide legal and policy advice that balances innovation and development with the protection of rights and interests, to support Taiwan's vision of becoming an AI island and advancing digital sovereignty. In addition, the project focuses on examining how other jurisdictions accelerate regulatory adaptation or pursue regulatory flexibility in response to the digital technology environment, and conducts a comparative analysis of the challenges and existing approaches Taiwan faces in adapting its regulatory framework to emerging technologies. Based on this analysis, the project puts forward advice aimed at enhancing and improving the efficiency of regulatory adaptation.



本報告之智慧財產權歸屬於國發會

# 第一分項、國內數位法制變革調適與國際趨勢研析

## 項次 1. 113 年焦點議題延續趨勢觀測

## 壹、 AI 著作相關議題國際趨勢

### 一、美國

#### (一)2024 年 11 月美國提出《人工智慧網路透明度及責任法案》

2024 年 11 月 21 日，美國參議院議員提出《人工智慧網路透明度及責任法案》(Transparency and Responsibility for Artificial Intelligence Networks Act, TRAIN Act)，該法案修正美國著作權法，旨在透過修法增加行政傳票(administrative subpoena)程序，以協助權利人確認其受著作權保護之著作是否已被用於 AI 模型訓練。

依據修法新增之第 514 條(b)款，若法定、實質權利人(legal and beneficial owner)或被授權人(authorized person)主觀且善意的確信 AI 模型開發者或部署者使用一個或多個受著作權保護之著作的部分或全部以訓練生成式 AI 模型，則其有權向美國任一地方法院申請對 AI 模型開發商或部署者發出傳票，要求 AI 模型開發商或部署者揭露足以辨識其用以訓練 AI 模型，且可能係由該法定或實質權利人所擁有或控制之著作權著作的副本或使用紀錄。

該條(c)款規定提出傳票申請時需向法院提交擬議傳票以及聲明。聲明內需說明：

1. 申請人是善意確信模型開發者或部署者使用該法定或實質權利人所擁有之一個或多個著作之部分或全部，以訓練 AI 模型；

2. 申請簽發傳票之目的係為獲取用於訓練生成式 AI 模型之素材副本或足以識別作品使用之紀錄，以確定模型開發人員或



本報告之智慧財產權歸屬於國發會

部署者使用上開權利人之所擁有或控制之受著作權保護的著作；

3. 須記載相關副本及記錄僅用於保護法定或實質權利人之權利。

法案亦規定，AI 模型開發者或部署者在收受法院傳票後，應立即向法定或實質權利人或被授權人揭露傳票中所要求之副本及記錄。若 AI 開發人員未遵守傳票規定揭露相關資料，得推定其已使用受著作權保護之著作進行 AI 模型訓練。

由於現階段僅有極少數 AI 模型開發者或部署者願意揭露其訓練資料，因此該法案透過對 AI 模型訓練紀錄近用之立法，降低著作權人對未經授權使用其著作訓練 AI 模型之擔憂，有助於提升 AI 模型開發或部署者對於著作權保護之透明度及責任感。

■ **資料來源：**


1. Transparency and Responsibility for Artificial Intelligence Networks Act，2024-11-21，https://www.govinfo.gov/app/details/BILLS-118s5379is/ (last visited 2025/01/14)

2. Joseph Cahill, Baker Botts L.L.P.，Senate Introduces TRAIN Act to Enhance Transparency in AI Model Training, 2024/12/09, https://www.jdsupra.com/legalnews/senate-introduces-train-act-to-enhance-2430793/ (last visited 2025/01/14)

3. Congress.GOV, S.5379-TRAIN Act, 2024/11/24, https://www.congress.gov/bill/118th-congress/senate-bill/5379/text, (last visited 2025/01/14)




本報告之智慧財產權歸屬於國發會

## (二)2025 年 1 月美國著作權局發布關於 AI 生成作品之可著作性相關報告

2025 年 1 月美國著作權局(United States Copyright Office, 下稱著作權局)發布繼 2024 年 7 月後之第二份著作權與 AI 報告，該報告是關於 AI 輔助及生成作品是否可受著作權保護(copyrightability)之研析意見。該報告係以 2023 年 8 月著作權局所發布之意見徵詢為基礎，該次徵詢共計收到超過 10,000 多則建議，絕大多數人認為現行著作權法已足夠解釋，僅「人類創作之作品」可受到著作權之保護，而目前法院見解亦未將 AI 生成作品視為使用者及 AI 之共同創作，因此利用 AI 生成內容之作品是否享有著作權保護，需評估人類於創作中之參與程度。

1. 無須改變現行法律

著作權局認為，AI 創作之問題現行法令已可解釋，無須對 AI 作品或成果之著作權保護另訂規範。對於部分使用 AI 組合而成之作品，仍應逐案分析，確定人類於作品之貢獻程度。

2. AI 輔助作品之著作權保護

使用 AI 作為輔助工具之創作，若係協助或增強人類之思想之表達，而非直接取而代之，仍有受著作權保護之可能，如透過 AI 協助建立文學作品之大綱或進行數位音樂之合成等。報告指出，判斷作品是否受著作權保護之關鍵為 AI 系統係如何被使用，而非該系統固有之特性。若有足夠之「人類投入創作」之且滿足原創性等要件，則應受到著作權法之保護，不因過程中使用 AI 作為輔助工具而有所區別。

3. AI 指令(Prompts)



本報告之智慧財產權歸屬於國發會

著作權局於報告中指出，以目前可取得之科技觀之，使用者若僅為單純輸入 AI 指令，並不足以展現足夠之人為控制，而讓使用者得以成為 AI 依循指令產出成果之作者。所輸入之指令僅可被認為係傳達不受著作權保護之想法(ideas)，且依目前之 AI 技術，使用者無法透過指令之對話控制 AI 最終的呈現，即便指令內容經過多次修改，亦無法達到控制將想法表達出來的結果，故使用者並非 AI 輸出內容之創作者，所生成之內容也因而不受著作權之保護。換言之，生成內容是否具備著作權，判斷重點並非指令之複雜程度而是人類對結果之控制程度。

4. 表達性輸入(Expressive Inputs)

表達性輸入是指以文本、圖像、音訊或影片等媒體組合形式輸入至 AI 模型。例如將圖像作品輸入 AI 要求修改顏色或將創作之第一人稱故事輸入 AI，要求將第一人稱轉換為第三人稱視角。若人類創作者將自身受著作權保護之作品輸入 AI，且於 AI 輸出之結果中得識別出原作品，則該創作者應有作品及輸出作品得辨識其作品部分之著作權。

5. 對 AI 輸出之結果進行修改

對 AI 輸出之內容進行有意義之修改、編排之新作品得獲著作權保護。依據報告，如 Midjourney 等 AI 工具允許用戶對 AI 生成之結果進行後製或重新編排，該種修改與單純下指令不同，是使用戶得對單一元素或區域進行選擇與編排，故若能明確指出對生成內容修改之範圍及程度，可能被認定為受著作權保護之著作。而若於人類創作中包含 AI 生成元素之大型作品，即便當中之 AI 元素不受著作權保護，該類大型作品之完整著作權保護仍不受影響。



本報告之智慧財產權歸屬於國發會

報告指出，現行著作權法之保護原則仍具有足夠彈性，目前 AI 技術所生之著作權問題仍可以現行著作權法解決。雖尚未有建立新法或機制之必要，但著作權局仍會持續觀察技術及法律發展，評估是否需採取不同之監管機制。

■ **資料來源：**


1. United States Copyright Office, Copyright and Artificial Intelligence Part 2: Copyrightability, 2025-01-29, https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-2-Copyrightability-Report.pdf (last visited 2025/02/25)
2. Copyright alliance, Summary of the USCO Copyright and AI Report; Part 2: Copyrightability, 2025-02-06, https://copyrightalliance.org/ai-report-part-2-copyrightability/ (last visited 2025/02/25)


(三)2025 年 2 月德拉瓦州地方法院判定 AI 訓練不構成合理使用

2025 年 2 月美國德拉瓦州地方法院對 Thomson Reuters v. Ross 作出「簡易判決」(Summary judgment)。該案係由 Thomson Reuters 公司控告 Ross Intelligence, INC（下簡稱 Ross 公司）未經授權使用其資料庫 Westlaw 做為大型語言模型訓練資料，設計著作權侵權問題之訴訟。德拉瓦州地方法院判定 Ross 公司利用未經授權資料進行訓練並不符合著作權法中合理使用之規定。

Ross 公司為一法律搜尋新創公司，為開發 AI 法律檢索工具而向 Thomson Reuters 請求授權其資料庫 Westlaw 遭拒，轉而使用第三方公司 LegalEase 之「法律問答文件資訊集(Bulk Memos)」，做為 AI 訓練資料。其中大量利用 Westlaw 檢索資訊開頭之題註，故 Thomson Reuters 公司主張 Ross 公司構成直接侵權，而 Ross 公司則主張其用於 AI 利用應可構成合理使用。



本報告之智慧財產權歸屬於國發會

法院認為，Ross 公司之 AI 在訓練過程中使用受著作權保護內容，即便其 AI 未直接輸出 Westlaw 之「題註」，本質上仍是利用受著作權保護著作來建立競爭產品，構成直接侵權。就合理使用四項因素之判斷上，法院認為使用目的與性質以及使用受著作權保護著作之潛在市場影響為較重要之兩項因素。在使用目的及性質中轉化性之判斷上，法院認為 Ross 公司之使用並不具有轉化性，Ross 公司使用 Westlaw 之「題註」作為 AI 訓練資料而開發搜尋引擎，使其能更容易地開發一具競爭性之法律研究工具，目的與 Westlaw 相同，並非轉化性使用。

法院於判決中說明，潛在市場要素為合理使用判斷中最重要之要素，須考量 Ross 公司之複製行為對原作市場（法律研究平台及其衍生市場用於訓練法律 AI 之資料）可能造成之影響。法院認為 Ross 公司所開發之 AI 工具為與 Westlaw 競爭之替代品，會對市場造成影響，無論 Thomson Reuters 公司是否已實際運用該資料訓練其尋引擎。Ross 公司亦無法以公共利益作為主張，因法律判決本身已可自由取得，雖法律本身屬於公共利益，Thomson Reuters 公司係對其進行整理解析，為著作權保護之對象，並非 Ross 公司之創作，其資料之取得係侵害 Thomson Reuters 公司之著作權。

因此，最終法院判決 Ross 公司之利用為直接侵權且並非合理使用。

■ **資料來源：**

1. Thomson Reuters Enterprise Centre GmbH et al v. ROSS Intelligence Inc., No. 1:20-CV-613-SB – Document 547 (D. Del. Sep. 25, 2023), https://www.ded.uscourts.gov/sites/ded/files/opinions/20-613_5.pdf (last visited 2025/12/19)

### (四)2025 年 5 月美國著作權局發布關於 AI 與著作權第三部分報告-生成式 AI 訓練（出版前版）



本報告之智慧財產權歸屬於國發會

美國著作權局於 2025 年 5 月發布著作權與 AI 報告第三部分：生成式 AI 之訓練報告（出版前版）(Copyright and Artificial Intelligence Part 3: Generative AI Training pre-publication version)。本次報告係為回覆國會質詢以及利害關係人所關注之議題，並將於近期發布最終版本，預計實質分析內容及結論並不會有更動。報告重點內容係對生成式 AI 於訓練過程大量使用受著作權保護著作之合法性及風險問題進行分析及說明，著重於 AI 使用受著作權保護資料進行訓練是否得主張合理使用的探討。

1. 初步侵權(Prima Facie Infringement)

依據著作權法，賦予著作權人包含重製、發行、公開演出、公開展示以及其他著作衍生之相關權利。若著作利用要構成初步侵權，需先確定兩項要件(1)有受著作權保護之著作(2)重製著作中具原創性之構成要素。在未取得授權之情形下，開發或部署生成式 AI 系統時，若使用受著作權保護之作著作，且該作為未有可採行之合法抗辯（如合理使用），則可能構成對一項或多項著作權人權利之侵害。

(1) 資料蒐集及整理

本報告指出 AI 開發商於開發 AI 模型時使用受著作權保護著作建立訓練資料集之相關步驟，明顯涉及重製權。上開步驟包含多次下載及複製相關作品、於不同儲存媒介間傳輸資料、將資料格式化或創建副本等。報告中亦指出多數情形下，開發者取得資料之第一步，係從公開可得之來源下載資料，惟不論來源為何，都會進行反覆之複製，即會涉及重製權的問題。

多數意見認同或並不爭執 AI 開發者於獲取及整理資料之過程中涉及重製權議題。雖然有些觀點注意到資料在



本報告之智慧財產權歸屬於國發會

訓練後可能被刪除，但這並不會影響對侵權之認定。且公開之報導亦指出主要 AI 開發者通常會維持其訓練資料庫以供未來專案使用。

(2) 訓練

訓練過程亦會涉及重製權。開發商於模型訓練前階段會需要下載資料集並將其複製於高性能之儲存空間。於訓練過程中，受著作權保護著作之實質部分會被以其所呈現之狀態，批次性的暫時向訓練模型重製。而該重製資料，因所開發之 AI 類型及開發商所使用之特定軟硬體特性，可能導致保留之時間過長，而足以構成對重製權之侵害。

在訓練過程中，包括提供訓練樣本、透過預期的輸出衡量模型之效能，以及迭代更新模型權重(model weights[1])以提高模型效能等過程，亦可能會影響模型中涵蓋各項訓練資料副本之權重。即使是由未參與模型開發之第三方於訓練後重製模型權重，亦可能構成初步侵權。

當一個特定模型可以生成與訓練範例逐字或幾乎完全相同或實質相似(substantially similar)之內容，且該內容之生成無須透過外部提示或其他輸入提供該內容之表達(expression)時，則上開生成之內容，必然已以某種形式存在於模型權重當中。舉例而言，當生成式 AI 接受指令輸入一人名後輸出與訓練資料中一幅肖像幾乎相同之圖像時，則可認定該圖像顯然來自該訓練模型。

於此前提下，重製模型權重將會涉及對模型中記憶範例(memorizes examples)之重製。至於模型權重是否得為重

[1] 模型權重(model weights)係指 AI 模型當中的數值參數，用以確定模型如何回應輸入(input)形成輸出(output)。



本報告之智慧財產權歸屬於國發會

製或衍生著作，著作權局認為，應取決於模型是否保留或記憶相關著作實質受保護之表達。

綜合上述，使用受著作權保護之著作於準備資料集及訓練模型時皆會涉及重製權議題，但重製訓練後之模型權重則僅在其具實質相似之情況下才會構成侵權。

(3) 檢索增強生成(retrieval-augmented generation，或稱 RAG)

RAG 通常有兩種工作方式，一為開發者將材料複製到檢索資料庫中，生成式 AI 系統接取該資料庫檢索資料並將用戶指令一同提供予模型。二為從外部來源如搜索引擎或特定網站檢索資料。兩種方式都涉及受著作權保護之著作的重製，並且該技術為目前 AI 產品的重要功能，相關用途是新媒體及利害關係人特別關注之議題。

(4) 輸出

若經由生成式 AI 輸出作品時與受著作權保護之著作近似，則此類輸出很可能侵害重製權，並且若進行對原作之改編，則可能侵害其他衍生權利。

2. 合理使用

若以受到著作權保護之著作進行訓練可能構成前述之初步侵權，則最基本可用之抗辯為合理使用。法院會依據著作權法第 107 條所列四項非排他因素(non-exclusive factors)依個案判斷是否為合理使用。

(1) 因素一：使用目的及性質，包含該使用是否具有商業性質或用於非營利之教育目的

A. 識別用途



本報告之智慧財產權歸屬於國發會

判斷合理使用之第一考慮因素為被控侵權之著作是否有進階目的或不同之著作特徵。法院在判斷時會依據著作之轉化性(transformativeness)以及商業性(commerciality)進行判斷，且依個案情形有別，同樣之作品用於某一目的時可能構成合理使用，但用於其他目的，則未必構成合理使用。生成式 AI 於開發及佈署過程中會以不同方式使用受著作權保護之著作，著作權局指出，AI 開發及部署過程對作品使用上之不同應分開討論。例如識別 AI 開發過程中複製行為，若該行為目的係為編輯資料集或進行訓練，則其通常並非最終目的(ultimate purpose)。故於判斷生成式 AI 模型是否為合理使用時，需就其整體使用情境判斷。

B. 轉化性

就作品使用轉化性而言，著作權局認為生成式 AI 模型於大量且多樣之資料集上進行訓練可能是具有轉化性的。創作作品本身為人類提供娛樂及教育之目的，而 AI 模型之目的是為執行多種功能，其使用受著作權保護著作進行訓練之目的與該作品原有之使用目的並不相同。

然而模型是否具有轉化性仍不能一概而論，將取決於該模型之功能性及其部署之方式。作品之轉化性為一光譜，光譜一端為該作品用於研究或將其利用限制於不具替代性任務的封閉系統時，此類部署應具有最強之轉化性。而光譜的另一端，則用於訓練可生成實質上與受著作權著作相似之輸出的 AI 模型，此一情形除非原始作品本身被用以作為評論或模仿之標的，否則難將其視為具有轉化性。



本報告之智慧財產權歸屬於國發會

多數模型的用途係介於兩者之間，則需視個案評估。如模型輸出之內容與原訓練作品雖未有實質相似，但可能與原作品有相同之性質或使用目的，此種情形僅可算是具有「輕微轉化性」(modestly transformative)。故於判斷作品轉化性時，並非僅依據模型生成結果與原著作品之相似程度，仍須依其最終使用目的以及生成內容之性質進行判斷。即便 AI 模型並未生成與訓練作品相似之內容，但其使用目的相同，亦可能因缺乏足夠轉換性而不符合合理使用之要件。

有部分意見認為使用受著作權保護之著作訓練 AI 模型本質上就具備轉化性，因使用 AI 模型進行訓練不具表達性。著作權局認為上述觀點本身有誤，若該生成模型被用以創造表達性內容或潛在重現受著作權保護的著作之表達，則該訓練不能公平地被描述為不具表達性，而主張合理使用。此外，本報告亦不同意 AI 訓練因類似人類學習而本質上具有內在轉化性的論點。合理使用並不意味著所有為學習目的而進行之人類行為都可以被豁免。例如學生不能僅主張合理使用，即廣泛重製圖書館所有的書籍促進個人教育，相反其應當以購買或租借方式，合法獲得或使用著作。

C. 商業性

商業性係涉及在不支付慣常價格之情況，利用受著作保護之著作而得獲得經濟利益之潛在不公平性。營利與非營利非區別商業性之關鍵，而取決於特定使用是否服務於商業目的，即使用者是否會從利用受著作權保護之著作而從中獲利且無須支付慣常價格。若



本報告之智慧財產權歸屬於國發會

一個非營利組織可以透過訂閱產品將資料集或模型貨幣化來從事商業活動，這種行為將具有商業性，無論該組織運作是否為慈善之目的，故對於商業性之分析不應取決於實體成立之性質，而應取決於實際上之特定用途是否服務於商業或非營利之目的。

D. 非法獲取

著作權局認為，若明知係使用包含盜版或非法取得作品之資料集，不利於主張合理使用。但目前法院對於作品係善意或惡意取得，與是否可主張合理使用之判斷，仍存在不確定性。

(2) 因素二：受著作權保護著作性質

本報告指出，越具有創作表達之作品如小說、電影或音樂等會比功能性作品如電腦編碼等之利用，更不可能主張合理使用。由於 AI 模型之訓練作品來源多元，實際是否符合合理使用要件，仍須視模型及其具爭議之作品進行個案認定。

(3) 因素三：所使用之部分占該受保護著作整體之比例及合理性

A. 使用數量

該因素須判斷與受著作權保護之著作整體相比，其著作利用比例以及重要性綜合評斷。即使僅重製少部分著作，也可能會因為該複製部分屬於該作品之核心，而無法主張合理使用。著作權局認為，生成式 AI 模型之訓練不盡然需使用完整著作即可達成相同之目的，相較於 Google 搜尋引擎，生成式 AI 模型使用整個著作權著作進行訓練之合理性較低。



本報告之智慧財產權歸屬於國發會

B. 目的之合理性

大型通用 AI 模型之訓練，難以排除需要使用完整著作進行訓練，以達成其高效能表現。於此情形，若具備「轉化性目的」(transformative purpose)，即使利用完整作品進行訓練，亦足以被認定為合理使用。故雖使用完整著作進行訓練通常並無法構成合理使用，但若模型開發者得證明該模型之訓練必須使用大量資料才得完成或該訓練具備轉化性目的，則利用完整著作應可被視為是合理使用。

C. 向公眾提供之數量

當訓練模型能夠採取充分保護措施，有效限制受著作權保護之著作的核心表達部分被輸出，確實防止生成侵權內容之情況下，得視個案狀況權衡其是否可主張合理使用。

(4) 因素四：著作之利用對於潛在市場或該著作價值之影響

此一因素除須考量對原著作之權利侵害外，亦須將對其衍生著作市場之損害納入評估。本報告指出生成式 AI 訓練可能對市場造成之影響大致如下：

A. 銷售損失(lost sale)

此處係指著作權人因潛在購買者選擇重製品而取代購買原作，將會導致權利人失去收入。於生成式 AI 之情形，則是若模型所生成的結果與受原著作相似且具有替代性，可能造成對市場之損害，或是潛在市場之損失。

B. 市場稀釋(market dilution)



本報告之智慧財產權歸屬於國發會

此理論主張生成式 AI 輸出之內容可能會稀釋原有作品之市場，雖此一理論尚不確定，目前為止未經法院檢驗，但著作權局認為，AI 生成內容之速度及規模大於真人作者，將對同類作品市場造成稀釋的風險，也將使原作品之銷售更為困難。此外，作品風格並非著作權保障範圍，若 AI 以受著作權保護作品進行訓練而生成類似風格之內容，即便並非與原作實質相似，亦可能影響原創作者之市場。

C. 失去授權之機會(lost licensing opportunities)

權利人原可就授權作品利用而獲得收益，生成式 AI 將使原著作權人實際或潛在市場的現有收益或未來收益受到影響。

D. 公眾利益

本報告認為不論著作權利保障,抑或生成式AI之運用，皆可為公眾帶來巨大公共利益。但對於使用未經授權之著作進行訓練而帶來廣泛益處，從而改變以合理使用規定平衡著作利用之議題，目前尚無法提出定論。

3. 授權 AI 訓練

著作權局指出，著作權人授權 AI 使用其著作進行訓練是可行的。自願授權 AI 使用著作進行訓練亦越來越普遍，惟自願授權是否能完全滿足 AI 訓練需求仍有疑問。目前透過授權使 AI 得使用作品進行訓練之制度正在發展實踐當中，著作權局建議讓授權制度於未有政府干預之情形下繼續發展。

綜合前述，著作權局認為，作品於 AI 訓練是否屬於合理使用仍需視個案判斷，並非一概而論。須將視作品利用之轉



本報告之智慧財產權歸屬於國發會

化性、來源、目的、AI 產出結果及市場競爭因素等個案事項皆納入判斷。此外，著作權局支持授權制度於 AI 訓練之發展，並認為政府應讓市場持續發展而非於此時進入干預，有效的授權得確保技術創新且不損害智慧財產權，並使開發者、創作者及消費者皆受益。

■ **資料來源：**


1. Copyright and Artificial Intelligence Part 3: Generative AI Training pre-publication version, 2025-05-09, https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-3-Generative-AI-Training-Report-Pre-Publication-Version.pdf (last visited 2025/06/09)
2. Copyright lately, Five Takeaways from the Copyright Office's Controversial New AI Report, 2025-05-28, https://copyrightlately.com/copyright-office-ai-report/ (last visited 2025/05/28)


(五)2025 年 6 月美國聯邦法院裁決 AI 訓練可主張合理使用

2025 年 6 月，美國加州北區聯邦地方法院(United States District Court for the Northern District of California)對三位美國作家向 Anthropic 公司訓練大型語言模型使用受著作權保護書籍提起訴訟一案，作出裁決，認為 AI 訓練可主張合理使用。

1. 案件事實

被告 Anthropic 公司透過掃描購買之實體書籍以及自盜版網站重製取得之受著作權保護書籍，將其以數位化可搜尋之檔案儲存。以此建立一世界所有書籍圖書館，以永久保存。該公司再自其所建「圖書館」中挑選數位書籍之全集及子集訓練其正在開發之大型語言模型（Large Language Model, LLM）。原告作家們主張 Anthropic 公司未經授權大量使用受



本報告之智慧財產權歸屬於國發會

著作權保護書籍訓練其模型之行為，為大規模未經授權之利用。法院以美國著作權法第 107 條判斷 Anthropic 公司之行為是否符合合理使用。

2. 合理使用之判斷

美國著作法第 107 條規定，合理使用須考量四項要素，包含使用目的及性質、受保護作品之性質、使用部分於完整著作之比例及重要性、使用著作對該作品之潛在市場或價值之影響。

(1) 使用目的及性質

AI 模型訓練係透過學習語言結構、邏輯，並非單純複製或重現原作。AI 訓練將大量內容經演算法、向量化，並非為複製或取代原作，其最終創造出不同的內容(create something different)，為一種學習及在創造之過程。法院認為，使用著作進行模型訓練以生成作品之目的以及性質是具有高度轉化性(quintessentially transformative)的。而訓練過程中於 LLM 內部之合理複製行為則屬於轉化性使用。

Anthropic 公司購買書籍並將其掃描儲存為數位可搜尋之檔案，並建立「圖書館」，法院認為，紙本書籍掃描轉換為數位版本之作法符合轉化性，Anthropic 公司有權保留紙本書籍副本，只是其選擇以數位形式保留，並非著作權人合法權利之侵害。

(2) 受保護作品之性質

該要素係要求識別某些作品較其他作品須受到更強之著作權保護，因此於複製該類作品時，合理使用將更難成立。法院認為，本案中之著作接包含表達性元素(contained express elements)，且作品被選入進資料庫即是



本報告之智慧財產權歸屬於國發會

因其表達性。法院認為系爭著作皆為須受到較強保護之著作，但於合理使用之判斷上，仍須就四項要素整體衡量。

(3) 使用部分於完整著作之比例及重要性

法院認為，LLM 之訓練需大量使用內容、書籍，大量書籍之使用為訓練之合理必要，而原告作者群之作品被選為 LLM 訓練時之寫作範例，其所輸出之內容係經過演算法、向量等技術轉化，並未直接複製或重現原作，與單純複製、重製作品並不相同。

(4) 使用著作對該作品之潛在市場或價值之影響

該要素係判斷重製後之作品是否會取代著作權人著作之市場需求。法院認為，訓練 LLM 之複製，並不會削弱作者群原作於市場之需求，且著作權法係為促進創作，而非為保護作者免於競爭。然而，法院亦強調，提供 AI 訓練合理使用不代表其資料來源之適法性為合法，取得盜版圖書，即便經過轉化使用於訓練 LLM，仍然構成著作權之侵害。

3. 結論

法院認為，本案利用著作訓練特定 LLM 屬於合理使用，且涉案技術為相當具有轉化性之技術。然而法院亦強調，雖 AI 訓練屬於合理使用，並不代表盜版取得之資料亦得主張合理使用，即便 AI 訓練構成合理使用，亦不影響非法取得著作之侵權判定。

■ **資料來源：**

1. Bartz et al. v. Anthropic PBC, No. 3:24-cv-05417-WHA, Doc. 231, (N.D. Cal. June 23, 2025)，https://cdn.arstechnica.net/wp-content/uploads/2025/06/Bartz-v-Anthropic-Order-on-Fair-Use-6-23-



本報告之智慧財產權歸屬於國發會

25.pdf (last visited 2025/11/25)

2. 資策會科技法律研究所，美國聯邦法官裁決 AI「訓練」行為可主張合理使用，2025-07，https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=9357#_ftn5 (最後瀏覽日:2025/11/25)

3. The Theverge, Anthropic wins a major fair use victory for AI — but it's still in trouble for stealing books, 2025-6-24, https://www.theverge.com/news/692015/anthropic-wins-a-major-fair-use-victory-for-ai-but-its-still-in-trouble-for-stealing-books (last visited 2025/11/25)

### (六)2025 年 6 月聯邦法院判決 Meta 公司之 AI 訓練屬合理使用

2025 年 6 月 25 日，於 Anthropic 案宣判兩日後，加州北區聯邦地方法院聯邦法院再次對類似案件做出「簡易判決」(summary judgment)。該案為 Meta 公司之生成式 AI Llama 被 13 位作家指控未經授權擅自使用其著作進行 AI 模型之訓練。法院再次就 AI 模型訓練之合理使用做出判斷，最終法院裁決 Meta 勝訴，其訓練為合理使用，惟判決亦表示若原告證據更為完善結果可能不同。

1. 案件背景

Meta 公司為訓練其生成式 AI Llama，其中一部分資料來源為盜版之影子圖書館(shadow libraries)，該圖書館提供包含受著作權保護書籍之內容，在未經著作權人授權之情形下供用戶免費下載。原告作家們主張，Meta 公司未經授權下載其受著作權保護作品訓練大型語言模型，違反合理使用且造成市場稀釋，侵害原作者之著作權。

2. 作品使用目的及性質

該因素重點在於作品之轉化性，Meta 公司使用書籍資料訓練其 AI 模型屬於高度轉化性。其使用書籍之目的係用以訓



本報告之智慧財產權歸屬於國發會

練大型語言模型，並非如原書籍以閱讀、娛樂、教育為目的而使用。法院表示，大型語言模型之閱讀與人類閱讀不相同，其屬於文字間之結合統計，其訓練並非對書籍之重新包裝，未有任何證據顯示大型語言模型能重現超過原告書籍任何超過 50 個單字之大量作品內容。證據僅能顯示 Meta 欲開發能創造特定風格之作品，惟風格並未著作權保護之範圍。

3. 著作權保護著作之性質

該因素欲判斷作品是否屬於應受著作權高度保護之作品。原告之作品多為小說、回憶錄以及戲劇，屬於具高度表現力之作品，為著作權法重視且希望保護之類型。大型語言模型訓練依賴特定語序、詞語選擇、文法及語法，皆為原告之創作表達。

4. 使用著作之數量及實質性(substantiability)

該要素重點為所使用部分之數量及實質性是否與複製目的相符且合理。法院認為，由於 Meta 複製書籍後具高度轉化，即便其複製整本書籍仍屬合理。且大型語言模型之訓練需使用大量資料進行訓練以確保模型品質，故 Meta 有合理必要使用原告之全部作品。

5. 對著作權保護作品潛在市場價值之影響

該要素為本案 Meta 公司勝訴之重要關鍵，法院認為此要素為合理使用最重要之單一元素。法院考慮三項要件進行判斷：

(1) Llama 複製、生成原告書籍之內容，是否替代原書籍之市場



本報告之智慧財產權歸屬於國發會

法院認為該要素並不成立，原因在於 Llama 並不允許使用者生成原作書中任何有意義之部分，即便 Llama 複製原著作微小之部分，亦不會對原告書籍之潛在市場產生有意義或重大之影響。

(2) Meta 公司未經授權使用原告書籍進行大型語言模型之訓練，是否損害原有書籍之授權市場

法院認為，授權市場之存在與否與潛在市場價值判斷無關，因原告無法壟斷授權市場，且原告無法主張「未支付轉化性使用之授權費」為潛在市場損害，這樣的主張將過於偏向權利人，並不符合合理使用中對潛在市場保護之要素。

(3) Llama 大量生成之作品即便作品本身不侵權，是否仍會因大量且快速之生成與原作競爭，造成市場稀釋或間接替代

大型語言模型因使用原著作訓練而快速且大量地生成競爭作品可能導致間接替代效果，亦稱市場稀釋。法官認為，訓練大型語言模型快速大量生成內容，確實會導致市場稀釋，損害原有市場，將減少原作者之銷售，而影響作者之創作動力，為著作權法所欲防止之傷害。但本案中原告無法提出證據證明該理論，因此最終裁決 Meta 公司勝訴。

法院於判決最後說明，大型語言模型之訓練使用著作權保護著作創造出大量競爭作品，對原作市場造損害，難以被認為是合理使用。但本案中原告未能就市場稀釋部分提出有力證據，並無法排除未來在類似爭議中以完整舉證，因市場稀釋效果而不構成合理使用。

■ **資料來源：**

1. Kadrey v. Meta Platforms, Inc., No. 23-CV-03417-VC, 2025 WL



本報告之智慧財產權歸屬於國發會

1752484, (N.D. Cal. June 25, 2025).，
https://storage.courtlistener.com/recap/gov.uscourts.cand.415175/gov.uscourts.cand.415175.598.0_2.pdf (last visited 2025/12/19)

2. LOEB&LOEB, Kadrey v. Meta Platforms, Inc., 2025-06-25, https://www.loeb.com/en/insights/publications/2025/07/kadrey-v-meta-platforms-inc (last visited 2025/12/19)

## 二、歐盟

### (一)2025 年 7 月歐盟發布《通用人工智慧實踐準則》

2025 年 7 月，歐盟執委會發布《通用人工智慧實踐準則》(The General-Purpose AI Code of Practice, 下稱 AI 實踐準則)，旨在協助相關產業能遵守 AIA 中與通用 AI 模型之安全性、透明度及著作權法律義務。AI 模型供應商可透過自願簽署及遵守該準則以證明其符合 AIA 之規定，此舉得減輕供應商之行政負擔並能為其提供法律明確性。

AI 實踐準則分為透明度、著作權以及安全保障三個部分，透明度以及著作權部分係提供通用 AI 供應商遵守 AIA 第 53 條規定之義務及方法；安全保障章節僅與少數最先進(the most advanced)模型之提供者有關，提供其遵守 AIA 第 55 條之相關義務。AI 實踐準則於去年 11 月發布初稿，並於今年 3 月更新第 3 版，此次發布之最終版本較第 3 版精簡，實際內容無太多差異，惟於安全保障部分，將第 3 版之 16 項政策精簡至 10 項並更著重於系統風險管理之具體措施。

#### 1. 透明度

透明度部分共有三項措施，製作及保存最新狀態之模型相關文件、提供相關資訊以及確保資料品質、完整性及安全性。

(1) 製作及保存最新狀態之模型相關文件



本報告之智慧財產權歸屬於國發會

簽署方（即簽署 AI 實踐準則之供應商）應於將其 AI 模型於市場發行時，應至少記錄本實踐準則文件中之所有資訊，簽署方得選擇填寫 AI 實踐準則提供之模型文件表格。該表格之內容包含供應商及模型之基本資料、相關許可證、使用政策、訓練過程等相關資訊。簽署方應確保該些資料為模型之最新狀態資訊，同時仍需保留舊版之文件，舊版文件之保存期限為模型上市後之 10 年。

(2) 提供相關資訊

簽署方應於將公用 AI 模型投入市場時，應於其網站或於未有網站時透過其他方式揭露歐盟 AI 辦公室及下游供應商之聯絡資訊，以提供相關單位或個人取得模型文件資訊或其他必要資料。簽署方應依 AIA 第 91 條或 75 條第 3 項之規定提供模型文件之資訊時，向 AI 辦公室提供其履行職責或國家主管機關為履行 AIA 監管職責所必須之資訊。簽署方應提供最新版本之資訊，並於請求之期限內交付。另簽署方應依 AIA 第 53(7)條及第 78 條之保密條件向下游供應商提供僅屬下游供應商之最新模型文件，並於不違反智慧財產權、商業機密及法律規定之營業秘密規定前提下提供下游供應商額外訊息，除有特殊情況，簽署方應於合理時間範圍內，且最遲不超過收到請求後之 14 天內提供相關訊息。AI 辦公室亦鼓勵簽署方將相關資訊向公眾公開，以促進公共透明度。

(3) 確保資料品質、完整性及安全性

簽署方應確保其記錄資訊之品質及完整性之控制，作為遵守 AIA 義務之證據予以保留，並防止未經同意修改。於草擬、更新及控制資訊及記錄之品質與安全過程中，鼓勵簽署方依照已建立之協議及技術標準執行。



本報告之智慧財產權歸屬於國發會

2. 著作權

此部分措施不影響對歐盟著作權及相關權利法規合規性，僅是列出簽署方得用以證明其於歐盟市場上推出之通用 AI 模型所需之著作權政策合規義務承諾。簽署方仍需負責確認其著作權政策中所列措施是否符合各該成員國對歐盟著作權規定及相關權利之實施，並於執行任何著作權相關行為前確保遵守各該成員國之著作權法規，以避免產生相關法律問題。

(1) 擬定及實施最新之著作權政策

簽署方將制定並保持實施最新之著作權政策以符合歐盟法律與著作權相關之要求，該著作權政策將適用於所有於歐盟市場上推出之通用 AI 模型。簽署方將透過文件說明相關政策，文件中需包含 AI 實踐準則著作權章節之內容，並且簽署方將於其組織內部分配負責實施及監督相關政策等相關職責。另外，AI 實踐準則鼓勵簽署方公開並確保其著作權政策摘要保持最新狀態。

(2) 自網路爬取資料時，僅得重製及擷取合法之內容

若簽署方使用或委託他人使用網路爬蟲，以進行資料擷取或彙編，作為《單一數位市場著作權指令》第 2(2)條所定文字與資料探勘或用於訓練其通用 AI 模型，應承諾以下事項：

A. 不得忽略歐盟《2001/29/EC 與資訊社會中著作權相關權利指令》第 6(3)條所定之有效技術措施，該些措施旨在防止或限制對作品及其他受保護主體之未經授權之行為，尤其應尊重透過訂閱模式或付費牆(paywalls)所加之技術性拒絕或限制存取。



本報告之智慧財產權歸屬於國發會

B. 簽署方於執行爬蟲時應排除向公眾提供內容，且被歐盟或歐盟經濟區內之法院或主管機關認定為持續且反覆以商業規模侵害著作權及相關權利之網站。歐盟將於其官方網站上公開包含上述網站清單之動態連結清單。

(3) 於網路爬取資料時識別並遵守權利保留

A. 為確保簽署方於使用或委託他人使用網路爬蟲進行資料探勘或訓練通用 AI 模型時能符合歐盟《單一數位市場著作權指令》第 4(3)條之機器可讀權，簽署方應承諾以下事項：

a. 簽署方使用可讀並遵循依據「機器人排除協議」(robot.txt)所表達指令之網路爬蟲，且該協議需符合網路工程任務小組(IETF)第 9309 號意見請求書及其後續版本規定，故於遵守上必須為 IETF 證明技術可行且 AI 提供者及內容提供商（包含權利人）可實施之最新版本。

b. 識別及遵守其他適當之機器可讀協議，以根據《單一數位市場著作權指令》第 4(3)條表達權利保留。協議必須為已被國際或歐洲標準化組織採納，或為最新技術及技術上可實施且被著作權人廣泛採用，並由著作權人、AI 提供者及其他利害關係人參與，於歐盟層級達成共識。

B. 前述承諾不影響著作權人原依法享有之保留權利、歐盟法律之適用範圍仍不受影響。權利人以依據《單一數位市場著作權指令》第 4(3)條所享有，以任何適當方式對作品及其他受保護文字與資料探勘用途進行明確保留之權利並不受前述承諾影響。此外，承諾亦



本報告之智慧財產權歸屬於國發會

不影響歐盟著作權及相關權利法規對被第三方自網路擷取或爬取內容，並被簽署方用於文字及資料探勘或訓練 AI 模型之受保護內容之適用。

C. 鼓勵簽署方支持(1)中所提之程序，並自願與著作權人及其他利害關係人討論，制定適當之機器可讀標準及協議。

D. 簽署方承諾採取適當措施，使受影響之利害關係人得獲得簽署方所使用之爬蟲、機器人排除協議功能及其他簽署方為行使權利保留而採取之措施。具體措施包括公開此類資訊並提供相關機制，使受影響之權利人能於資訊更新時自動收到通知。

E. 簽署方若亦有提供線上引擎服務，AI 實踐準則鼓勵其於進行資料探勘或 AI 模型訓練時採取適當措施以確保不會直接導致對該搜尋引擎所表達之權利保留之內容、網域名稱或 URL 之索引編列(Indexing)造成不利影響。

(4) 減緩侵犯著作權之輸出風險

A. 為減緩下游 AI 系統可能造成之風險，簽署方應承諾以下：

a. 採取適當且符合比例之保護措施，以防止其模型以侵害方式重製受歐盟著作權及相關權利保護之訓練內容之輸出結果。

b. 於可接受政策、使用條款或其他同等文件中，禁止模型之侵害著作權行為。以免費以及開源方式發布之通用 AI 模型，在不影響授權之免費及開源性質之前提



本報告之智慧財產權歸屬於國發會

下，應於模型附隨文件中提醒使用者不得以侵害著作權之方式使用該模型。

B. 不論簽署方是否將模型垂直整合進其 AI 系統，或依契約關係將模型提供與其他實體，皆適用前述政策。

(5) 指定聯絡人，並提供投訴管道

簽署方應承諾指定一聯絡人，並建立機制以使受影響之著作權人及其授權代表得透過電子方式提交相關之證明投訴，簽署方必須以公正方式於合理期間內回應投訴。該措施不影響歐盟及會員國原有之著作權利相關救濟及制裁措施。

3. 安全保障

本章節僅適用於具有系統性風險之通用型 AI 模型提供者，要求事業須對 AI 模型進行風險評估及管理，共設有 10 項風險控管建議。

(1) 安全保障框架

簽署方應承諾採取最先進之安全保障框架，該框架之目的系為確保模型所生之系統風險為可接受之風險，所實施之系統性風險管理程序及措施。流程共有建立、執行以及更新框架三個階段。

(2) 系統風險識別

簽署方承諾識別來自模型之系統風險，識別風險之目的包括促進系統性風險分析及決定接受系統性風險。識別系統風險有兩項要件：A. 遵循結構化流程自模型識別系統風險，依據安全保障框架中之風險類型，整理可能源自模型之系統性風險清單，分析風險之相關特性，如性質及



本報告之智慧財產權歸屬於國發會

來源，最後依分析識別該模型所具之系統性風險；B. 為每個識別出之系統性風險制定系統性風險情境，包含數量以及詳細程度。

(3) 系統性風險分析

簽署方應分析每一個被識別之系統風險。風險分析共包含五項要件，各要件間可能會有重疊或需要遞回實施(implemented recursively)之部分，系統分析之五項要件分別為蒐集與系統性風險相關，但不依賴特定模型之資訊，如市場分析、訓練資料審查、專家評價等；模型評估，以評估模型之能力、傾向、可行性及/或影響；系統性風險建模，以風險情境為建模基礎並納入所蒐集之相關資訊進行；評估系統風險，評估系統性風險之損害機率及嚴重性；最後須進行上市後監測。

(4) 決定系統性風險之接受程度

簽署方應具體說明系統性風險之接受標準，並確定模型之系統風險是否為可接受，應依據系統風險接受程度決定是否繼續開發、上市及/或使用模型。

(5) 安全緩解措施

簽署方應於模型完整生命週期中實施適當的安全緩解措施，以確保模型所導致之系統風險維持於可接受範圍內。所謂適當安全緩解措施包含於面對對抗性操作時仍有足夠認應之緩解措施，並應考量模型之發布與策略。

(6) 資安緩解措施

簽署方應於模型之完整生命週期間為模型及其實體基礎設施實施適當之網路安全保護，以確保由於未經授權



本報告之智慧財產權歸屬於國發會

之發布、未經授權之存取及/或模型盜竊而生之系統風險為可接受。

(7) 安全及資安模型報告

簽署方應於將 AI 模型投入市場前，向 AI 辦公室報告有關模型及其系統風險評估及緩解措施之相關資訊，並作成安全及資安模型報告。並且確保該報告須隨時維持於最新狀態，同時須通知 AI 辦公室有關模型報告之更新情形。

(8) 系統風險責任分配

簽署方需於組織內部各層級明確界定相關責任，以管理由模型導致之系統性風險，並且須為已被分配系統性風險管理責任之人員或單位配置適當之資源，此外，亦須於組織內推動並維護健全之風險文化。

(9) 重大事故報告

簽署方須確保實施適當程序及措施，以追蹤、紀錄並即時地向 AI 辦公室及國家主管機關報告模型生命週期間之重大事故相關資訊，以及欲採取之可能矯正措施。並且，簽署方應就相關程序及機制，依據重大事故之嚴重程度及模型涉入程度，提供適當之資源。

(10) 附加文件及透明度

簽署方需紀錄安全保障章節之實施情形，並依據需要發布其框架及模型報告之摘要。

AI 實踐準則於 2025 年 7 月 10 日發布後，於 7 月 30 日，Google 於其網站表示將與包含美國模型供應商在內之幾家公司願意簽署該實



本報告之智慧財產權歸屬於國發會

踐準則，期望能使歐盟公民及企業得獲得安全及優質之 AI 工具，並表示將積極支持有利創新之作法，以實現於歐洲之投資及創新。

■ **資料來源：**

1. European Union, The General-Purpose AI Code of Practice, 2025-07-10, https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai (last visited 2025/08/04)

2. Google, We will sign the EU AI Code of Practice, 2025-07-30, https://blog.google/around-the-globe/google-europe/eu-ai-code-practice/(last visited 2025/08/04)

(二)2025 年 7 月歐洲議會發布生成式 AI 及著作權報告

2025 年 7 月，歐洲議會發布生成式 AI 及著作權報告(Generative AI and Copyright)。該報告分析生成式 AI 對歐盟著作權法核心原則造成之挑戰，及歐洲議會將如何應對。由於 AI 訓練實務與現行資料探勘例外規定的內容並不兼容(legal mismatch)，且 AI 輸出內容之法律地位仍不明確。現行生成式 AI 系統大規模使用含有自然人創意之內容而缺乏對著作權人之公平報酬，對歐洲創意產業產生結構性風險。該報告呼籲依照 AI 系統之運作特性，針對輸入內容與輸出結果進行分析、建立透明度義務、公平的授權及報酬模式，以平衡創新與作者權利。

報告指出，現今之挑戰並非科技創新本身，而係對法律解釋可能扭曲而減弱法律之一致性。相較於使著作權法適應 AI，更應該確保 AI 發展尊重歐盟著作權法之法律核心及政策原則。報告採取兩步驟分析法：首先，評估目前生成式 AI 系統的使用是否符合歐盟著作權法規定；其次是識別是否存在監管或立法不足之處。

1. 資料輸入

於資料輸入層面，報告關注使用受著作權保護著作訓練人工智慧模型之合法性，並檢視文字與資料探勘例外的適用



本報告之智慧財產權歸屬於國發會

界限、退出機制的功能，以及訓練資料透明度所帶來的規範挑戰。

AI 之運作於訓練階段會透過爬蟲或資料庫之提取建立訓練語料庫，過程中會有重製及儲存之行為，而無論是否能於模型輸出中被辨識該作品，皆不影響其可能於輸入階段被重製及使用。因此需討論之重點為重製之發生於著作權法規定之例外及限制下是否被允許。

(1) 資料探勘例外之立法目的與生成式 AI 之差異

資料探勘技術與 AI 語言模型之運作模式具有差異，雖兩者皆涉及重製，但運作方式截然不同。資料探勘屬於資料科學(data science)領域，用於分析既有資料，涉及使用軟體處理大量文本、圖像或其他資料；AI 則是屬於機器學習(mechine learning)領域，除資料分析外，亦涉及大規模資料及處理並依據統計相關性透過演算法合成輸出。AI 訓練與資料探勘技術之差異，使 AI 訓練是否適用歐盟《數位單一市場著作權指令》(Directive on Copyright in the Digital Single Market, DSM 指令）第 3 條與第 4 條之與資料探勘例外產生疑義。

DSM 指令第 4 條授權具備合法取得來源之使用者進行廣泛之資料探勘活動，除非相關權利人選擇拒絕。基此，有論者認為 AI 訓練亦得適用此條規範，然該報告指出，此種解釋過於簡化了法律框架以及基礎技術現實。若對第 4 條進行寬泛解讀以允許 AI 訓練，將扭曲其預期範疇，使其成為「事實上的強制授權」，而無法達到平衡兩者間利益之目標。報告指出，DSM 指令中之資料探勘旨在分析數位形式之文本及資訊以產生資料之任何自動化分析技術，所謂分析係指知識、模式或趨勢之提取，而非表達



本報告之智慧財產權歸屬於國發會

行作品之合成。惟生成式 AI 訓練並非 DSM 指令所定之分析，而是透過內化與重組表達行內容運作，與資料探勘例外規定之預期目的並不相同，不應與合法之分析用途等同視之。資料探勘例外條款係針對不同技術之規範，並不能為生成式 AI 發展提供法律基礎。

(2) 現行資料探勘法律框架於生成式 AI 使用上之限制

如同前述分析，不應將條文範圍無限擴張，因此報告重申作者控制權之重要性，並確保 AI 訓練必須經過事先同意、協商授權及公平報酬。AI 訓練於現行資料探勘例外況架下之限制範圍過窄、退出機制存有缺陷、AI 訓練與資料探勘目標不符以及缺乏權利補償機制。

資料探勘例外條款第 3 條有對科學研究之資料探勘設有不需著作權人同意即使用其文本進行資料探勘之規定。該條之主體為非營利研究機構，然而非營利公共研究機構與私營開發者間之合作日益增長，使科學研究及商業用途之界線日益模糊。AI 系統之運作為在下游商業背景下重新利用原先符合第 3 條規定之資料集，且無須額外取得授權或補償，對著作權人權利有所衝擊。報告認為，應更清楚界定法規中例外之界線、強化監督機制，並於 AIA 中提供進一步指導規範。

就退出機制而言，DSM 指令第 4 條有要求著作權人得保留其權利，要求使用者不以其著作進行資料探勘。然而退出機制於現今技術下仍有困難，尤其是在 AI 模型訓練大型抓取網路資料之情形下更難以執行。現行退出機制僅能向後生效，並無溯及既往之功能，對於未有足夠資源監測作品狀況之小型創作者而言實為傷害。報告認為，應



本報告之智慧財產權歸屬於國發會

考慮是否回歸基於許可之事前同意(opt-in)制度，以保護為預設而非預設允許獲取。

報告亦指出，現行機制於報酬及補償上之不足。DSM 指令中，即便該些內容可能於後續被使用於具有商業價值之 AI 商品中，資料探勘使用資料並不需支付任何酬勞或相關補償。著作權人擔憂補償機制缺乏可能導致之系統性失衡，AIA 之實踐準則中雖有對著作權合規有所說明，其本質上仍屬自願遵守，並未有強制效果；且實踐準則中對資料探勘之權利保留機制排除網路抓取以外資料取得方法，並非取決於受著作權保護著作是否被利用於 AI 訓練進行判斷。實務上，AI 訓練使用之線上內容多為第三方上傳，著作權人難以有效主張其權利，而導致著作於未經真正同意或給付補償之情形下被用於 AI 訓練。

為使著作權人之權利受到保障，除現已提出之自願受權機制、集體授權機制及資料探勘法定報酬機制，透明度亦相當重要。包含 AIA 以及 DSM 指令皆有針對透明度之相關規範，然單就前二法規中之透明度要求，仍無法明確歐盟著作權法政策中確保著作權人著作被利用於 AI 訓練時獲得公平報酬之預期目標。透明度規範仍難以解決談判地位、執行或訴訟管道上之結構性不對等。

報告認為應重新制定著作權基礎設施，如引入專為 AI 訓練設計之集體授權模型，或開發能大規模處理選擇退出集授權請求之歐盟中央權利管理平台。透過強制性集體權利管理、強而有力之公共監督以及 opt-in 機制之框架，轉向一旨在主動保障權利之系統。

2. AI 輸出



本報告之智慧財產權歸屬於國發會

於輸出層面，報告關注重點包含生成式 AI 輸出內容是否可受著作權保護，包含權利所有人、特殊權利之正當性、公平署名與報酬之相關法律及經濟機制以及輸出內容侵權問題之相關疑慮。

(1) 著作權保護對象

歐盟著作權法乃至國際法律體系之普遍共識，著作權僅保護由人類創作之作品，在歐盟法律下，完全 AI 生成，未有實質人類投入之創作並不受著作權保護。儘管對 AI 協作提供保護，歐盟之規範仍係以人為本，保護人類創作。

(2) 區分 AI 協作(AI-assisted)及 AI 處理(AI-processed)

為能確定作品是否能受著作權保護，應區分 AI 協作以及 AI 處理，若人類將 AI 作為工具，由自身做出實質行之創意決定，則該輸出結果仍可能符合著作權保護之資格。報告中引用美國著作權局於 2025 年發布之報告，說明著作權需要足夠之人類作者身分，並排除無實質性人類創意下生成之作品。

在判斷上可透過學術界之三層級模型區分進行分辨：

A. 以極少人類投入建立之輸出，通常不可受著作權保護。

B. 透過有意義人為編輯或策劃所構成之輸出，可能受著作權保護。

C. AI 純粹作為輔助工具以協助人類作者身分之作品，明確受到著作權保護。

該模型雖尚未入法，但已反映出日益增長之共識，可作為未來指引或立法方向之參考。報告認為，任何形式之規則修改，都應優先採用能增強法律明確性及透明度之方



本報告之智慧財產權歸屬於國發會

案，並且同時兼顧歐盟著作權法之基本價值。人類創造力、比例原則及開放性為快速變化環境之 AI 時代下之法律核心原則。

(3) 潛在市場影響

AI 生成內容可能對法律及經濟層面造成影響。自經濟角度而言，生成式 AI 將改變既有之創意價值鏈，產生替代效益，可能侵蝕創作者之收入以及市場地位；就法律角度而言，公平性、署名及競爭框架將產生問題，對於 AI 生成結果及人為參與創作之定義不明確，將使授權報酬機制增加法律不確定性。監管上確保公平競爭以支持著作權人之作品即使被 AI 訓練仍能得到合理報酬，並向消費者確保資料來源之透明。

(4) 侵權責任

生成式 AI 之輸出若直接或間接包含於訓練或生成過程中接觸之既有著作，可能使輸出結果構成著作權侵害。重點在於區分合法靈感(lawful inspiration)以及非法重製(unlawful reproduction)之界線。當輸出內容含有受保護著作之實質部分或可識別部分，即便輸出是由 AI 系統組合，且使用者或提供者無抄襲意圖，仍很有可能構成侵權。AI 輸出之著作權侵權樣態可能包含逐字逐句之重製、公共傳輸以及實質性相似。

A. 逐字逐句重製：訓練作品之一部分被幾乎原封不動地輸出，研究證實，大型語言模型確實會記住(memorize)訓練資料，而產出相當於未經授權副本之內容。

B. 公共傳輸：該類型之重點在於，AI 輸出是否成為受保護著作之功能性替代而干擾原作之利用，依據《資訊



本報告之智慧財產權歸屬於國發會

社會著作權指令》(InfoSoc 指令)第 3(2)條，透過聊天機器人發布之 AI 內容若向新公眾(new public)提供受著作權保護內容，則可能構成侵權。

C. 實質性相似：雖輸出之內容並非完全相同之副本，但其與訓練資料及為相似，當中挪用原作品受保護表達之內容，而非僅是思想、主題或概念。

在責任歸屬上不同階段之角色分別負有相應責任。就 AI 使用者而言，若下達指令要求生成特定受著作權保護著作，導致 AI 生成未經授權之衍生內容，使用者應承擔主要責任。在 AI 提供者部分，若模型被設計為可預期地輸出侵權內容，提供者將可能負有間接責任。AIA 要求 AI 提供者實施高度防範措施以防止非法輸出，AI 提供者若未能防範模型於 AI 使用者於輸入侵權提示詞時，生成侵權內容，則 AI 提供者將因此產生侵權責任。

4. 政策建議

鑒於生成式 AI 發展，模糊現行著作權法之界線，報告認為於政策上應與技術進步以及創意經濟、激勵人類創作間取得平衡。現行監管較集中於訓練過程中使用受著作權保護作品以及相關法律不確定性之問題。雖有論者認為 AI 學習相當於人類閱讀著作之學習，然本報告認為依據歐盟著作權法，此種類比並不成立。生成式 AI 模型運用著作權保護著作進行訓練時，通常會重製並處理作品中之實質表達部分，已超出現行法律對研究或分析之例外允許範圍。實務上，生成式 AI 模型之黑箱問題仍存在，即便模型開發者亦難以理解模型中之元素是如何被處理、儲存或轉換。因此，需以可追溯性及透明度以確保負責任的資料使用。



本報告之智慧財產權歸屬於國發會

著作權法應為確保創新且具有倫理基礎及合法性之手段，若須確保 AI 發展能於尊重基本權利以及公共利益之框架下進行，責任以及公平原則相當重要。因此該報告提出三項政策指導目標：

(1) 法律明確性：明訂 AI 訓練範圍及 AI 生成作品之法律地位。

(2) 透明度及問責：資料集可追溯性及可稽核性，並以事前同意(opt-in)取代事後退出(opt-out)機制作為 AI 之訓練方式。

(3) 公平報酬：建立相關機制以確保著作被用於訓練之著作權人能夠獲得公平補償。

該些目標將具體化歐盟的預防性原則，於大規模、不透明之資料使用產生系統性風險時，預先部署透明度、可追溯性及公平補償之措施。

■ **資料來源：**

1. Nicola Lucchi-European Parliament's Committee on Legal Affairs., Generative AI and Copyright, 2025-07, https://www.europarl.europa.eu/RegData/etudes/STUD/2025/774095/IUST_STU(2025)774095_EN.pdf (last visited 2025/12/20)

三、 英國

(一)2024 年 12 月英國智慧財產局針對著作權及 AI 公開徵詢意見

2024 年 12 月 17 日英國智慧財產局(Intellectual Property Office, IPO)發布《著作權及人工智慧：諮詢》文件（Copyright and AI: Consultation, 下稱諮詢文件），旨在針對政府如何確保英國著作權與



本報告之智慧財產權歸屬於國發會

AI 之法律框架，得以共同支持英國創意產業及 AI 產業所為之公開意見徵詢。諮詢期程為 2024 年 12 月 17 日至 2025 年 2 月 25 日止。

英國現行著作權架構提供著作權人之著作財產權及著作人格權(economic and moral right)，而由著作權人控制其作品如何被利用，故除非有特殊情況，重製作品進行 AI 訓練需要經過著作權人之同意。然而此一現行法制架構無法滿足英國創意產業及 AI 產業之需求。英國創意及媒體組織(Creative and media organisations)擔心其所屬作品於未經許可下被用於訓練 AI，且無法透過協議取得相應報酬。此外，AI 開發人員於使用或獲取內容之方式上缺乏透明度，將使著作權人難以執行著作權法賦予之權利。而對 AI 產業而言，缺乏合法取得訓練資料之明確性規定，將導致法律風險，並阻礙英國 AI 之創新及採用。故本次意見徵詢計畫旨在針對著作權與 AI 之法律架構如何建構，以獎勵人類創造力、激勵創新並為著作權及 AI 領域之長期發展提供所需之法律確定性，見徵詢目標有三：

1. 確保著作權人對其作品是否用於訓練 AI 模型之控制權，及獲得使用報酬之權利。

2. 確保 AI 開發人員得獲得高品質訓練資料，支援英國開發世界領先之 AI 模型。

3. 確保 AI 開發資訊之高透明度，建立創作者、創意產業及消費者間之信任。

本次諮詢文件提出 4 種政策方案，釐清著作權法制架構需要，以實現 AI 及創意產業發展：

1. 選項 0：不採取任何措施，著作權及其他相關法律保持不變

   此選項表示目前對於權利人及 AI 開發人員間之關係仍缺乏明確性。諮詢文件表示，雖該選項將延長創意產業及媒



本報告之智慧財產權歸屬於國發會

體行業與 AI 行業模型訓練之法律不確定性，且無法實現該諮詢文件所欲達成之目標，但仍邀請各界就此選項提出意見。

2. 選項 1：加強著作權保護，在所有情況下皆須取得授權

即 AI 模型僅在獲得明確授權之情形下以著作權著作進行訓練。此選項基本上將現行法律明確化，為英國著作權法如何於 AI 模型發展之適用提供法律明確性，並為創作者提供一明確之報酬取得途徑。然而此種方式將使英國之競爭力不如其他無此類規定之國家（如歐盟及美國），降低英國 AI 發展之吸引力，導致對 AI 領域開發之投資減少。

總而言之，此選項賦予著作權人對其作品有更大的控制權，然而亦會使得 AI 開發人員更難以在英國進行領導模型之開發。進而嚴重損害英國 AI 產業，對著作權人之利益亦有限。

3. 選項 2：建立廣泛之資料探勘例外(data mining exception)

此選項為引入較廣泛之資料探勘例外規定，允許無須取得著作權人許可即得利用著作權資料進行資料探勘（包含進行 AI 訓練）。此例外將允許任何目的之商業活動利用，且限制極少或無限制。

此類廣泛且無限制之例外規定，將改善 AI 開發人員取得訓練資料之機會，並提升對英國 AI 產業之投資。惟此作法將導致著作權人無法控制其作品之使用，或尋求適切之報酬，故難以滿足權利人的需求。

對英國著作權法制架構進行此種極端變化，極可能限制創意與媒體產業之發展。又依據該例外規範之擴張程度，可能使英國與國際法之義務難以一致。



本報告之智慧財產權歸屬於國發會

4. 選項 3:採用允許著作權人保留其權利並以支持透明度作法為基礎之資料探勘例外規定

此選項主要在尋求平衡 AI 開發者使用作品及著作權人對作品之控制需要，同時強化各方之信任與透明度。採行此一架構，AI 開發人員得使用合法取得之資料進行訓練，但僅限於權利人未保留其權利之範圍。換言之，AI 開發人員得在無侵權風險之情形下使用以網路(web-based)為基礎之資料訓練其模型；而著作權人亦得透過有效且可取得之技術，控制其作品如何被使用，並透過許可協議取得相對應之報酬。該方法須以強力措施(robust measures)為基礎以確保 AI 開發人員對模型訓練採用作品維持透明，且著作權人得單獨或集體進行權利保留。同時亦須搭配與現行著作權架構一致或現行著作權架構外之爭端解決機制及監管機制。

此一資料探勘例外規定，允許著作權人保留其權利，並以透明度為基礎，有支持 AI 創新之潛力。此架構將消除法律適用上之模糊性，為著作權人創造授權機會並降低著作權人獲取報酬之障礙。執行上將透過賦予著作權人更大之控制權，規範 AI 事業如何及何時使用其作品以達成諮詢文件所提及之三項目標。同時亦會明確指出是否需支付報酬，並對模型輸入與輸出加強透明度作為支撐。此方法使著作權人得了解其著作如何被運用並得解決現行法規下尋求報酬之不確定性。

本次意見徵詢文件指出，選項 3 具有實現權利控制、著作權作品取得及確保透明度等三項目標之可能性，並能促成授權協議以確保著作權人得獲得適當報酬。因此確保權利得保留、並以開發者透明度為基礎之資料探勘例外規定為此諮詢文件之主要諮詢議題。諮詢文件歡迎各界提出對前述不同選項之意見，並希望能蒐集到關於 AI 創新發展所引發之著作權相關法律問題可能需要關注之意見。



本報告之智慧財產權歸屬於國發會

■ **資料來源：**

1. Intellectual Property Office, Open consultation Copyright and Artificial Intelligence, 2024-12-17, https://www.gov.uk/government/consultations/copyright-and-artificial-intelligence?utm_medium=email&utm_campaign=govuk-notifications-topic&utm_source=bda528c5-6cac-46ce-a9a2-488d2820322c&utm_content=immediately (last visited 2025/01/13)
2. Intellectual Property Office, Copyright and AI: Consultation, 2024-12-17, https://assets.publishing.service.gov.uk/media/6762c95e3229e84d9bbde7a3/241212_AI_and_Copyright_Consultation_print.pdf (last visited 2025/01/13)

### (二)2025 年 6 月英國議會通過資料使用及近用法新增 AI 商業資料透明度相關規範

英國議會於 6 月 11 日通過《資料（利用及近用）法案》之修正案(Data (Use and Access) Bill，[HL] Bill 238)，並於 6 月 19 日經皇室批准正式成為法律，內容係就 AI 業者之透明度予以規範。該規定之修訂是為回應下議院於 5 月 7 日所提出之修正案，該修正案刪除了上議院於 2025 年 2 月提出之原始法案中第 137 條關於爬取著作權作品之透明度規定。此修正案納入相關條款強化與 AI 模型利用相關商業資料(business data)[2]之透明度，確保著作權人能識別其作品被用於 AI 訓練。

該法針對與 AI 模型相關之商業資料透明度作出規定，要求內閣大臣或財政部須對與 AI 模型利用著作相關商業資料的揭露制定規範：

1. 規範對象

[2] 法規中之商業資料依據同條規定，係指:關於交易者所提供或提供之商品、服務及數位內容之資訊；與交易者提供或提供之商品、服務及數位內容相關之資訊；關於商品、服務或數位內容(或其他供應或提供)之回饋資訊；關於依據資料法規向個人提供前述資訊之資訊。



本報告之智慧財產權歸屬於國發會

上開相關規範之規範主體為符合下列條件之交易者(trader)以及商業資料之持有者(data holder)：1.所提供之服務包含提供 AI 模型，以及 2.其服務與英國有關聯。而所謂與英國有關連之服務係指該服務擁有顯著數量之英國使用者，或英國使用者為該服務的目標市場之一。

2. 揭露內容

規範中並要求符合條件之交易者及資料持有者於揭露特定商業資料時，應提供有效的機制，使著作權人得以識別其被用於 AI 模型之預訓練(pre-training)、訓練、微調及檢索增強生成(retrieval-augmented generation)或作為 AI 模型之輸入資料之所有作品。

除用於 AI 訓練之資料外，亦規定交易者若於其 AI 模型提供服務過程中使用機器人(bot)，則應揭露所使用之機器人的相關資訊。此處所稱機器人係指得與系統或使用者互動，並依指令自網站獲取資料之自動化軟體(autonomous software)應用程式，包括爬蟲軟體及擷取器等，其所需揭露之資訊包含機器人之名稱、負責該機器人之法律實體及個別機器人之特定使用目的等。

3. 揭露形式

商業資料之揭露須以特定形式、頻率及方式發布，並且須確保著作權人得請求近用上開資料。

4. 執法時程

內閣大臣及財政部必須於該法案通過後 12 個月內向國會提交本條所要求制定之規範草案以及該規範所須遵循之程序。



本報告之智慧財產權歸屬於國發會

■ **資料來源：**

1. Data (Use and Access) Bill [HL] Bill 238 2024-25 (Lords Amendments to the Bill), 2025-05-12, https://publications.parliament.uk/pa/bills/cbill/59-01/0238/240238.pdf (last visited 2025/06/20)

2. Center For Data Innovation, House of Lords Copyright Amendments Derail Data Access Bill Crucial to UK AI Innovation, https://datainnovation.org/2025/05/house-of-lords-copyright-amendments-derail-data-access-bill-crucial-to-uk-ai-innovation/ (last visited 2025/05/28)

## 四、 德國

### (一)2025 年 11 月慕尼黑地方法院判決 OpenAI 訓練資料侵害著作權

2025 年 11 月，德國慕尼黑地方法院判決裁定 OpenAI 於未經許可下使用受著作權保護歌詞訓練生成式 AI 模型，違反德國著作權法(UrHG)重製權及公開傳輸等規定。

#### 1. 案件背景

GEMA 為德國之音樂著作權協會，於 2024 年 11 月提起訴訟，指控 OpenAI 於訓練 ChatGPT 時，在未獲得授權之情形下，使用其管理 9 名作詞、作曲者等音樂人之音樂著作訓練其模型。並且其模型之訓練已記憶該歌詞內容，致使使用者於 ChatGPT 輸入提示詞後所生成之內容大量、近乎相似之歌詞內容。被告 OpenAI 則以模型訓練並非儲存相關資料而係參數組合，其生成內容為機率非固定形式，以及資料探勘例外合理使用作為抗辯。

#### 2. 訓練資料「記憶」屬重製



本報告之智慧財產權歸屬於國發會

語言模型之「記憶」得透過許多方式進行驗證，若係已知訓練資料，可使用簡單之提示詞並透過足夠之文本長度，將訓練資料與輸出內容進行比對以確定記憶之存在。法院經過比對證明後，認為 ChatGPT 語言模型成功輸出系爭侵權歌詞，其內容幾乎與原作歌詞雷同，故本案歌詞在語言模型中是完整且未經修改地被記憶。

依據德國著作權法第 2 條規定，重製須為直接或間接、暫時或永久、以任何方式及任何形式之複製；且重製並不限於完全再現，變更著作形式亦會屬於重製，如將實體著作數位化，以 MP3 等壓縮格式儲存。本案法官依據德國高等法院之判例，被侵權客體被實體固定[3]（Körperliche Festlegung）及該固定成果對人類屬直接或間接可感知（Wahrnehmbarkeit）之標準審查。

被告 OpenAI 抗辯依語言模型特性，係字元間及回應之機率參數組合，並不包含具體歌詞可辨識之資料庫。且生成之內容為機率性質，特定詞序僅有在輸入特定提示詞時出現，並非實體固定之形式。然法院認為，重製之判斷需依照整體語言模型活動做為行為認定之客體，而非單獨特定之零散參數。語言模型整體足夠精確得被客觀識別，即便其運作參數分散並以機率之形式儲存於模型中，仍不影響其重製之構成。在間接感知之判斷上，作品若得透過使用技術輔助工具備感知時，即滿足此要件。而本案模型即可於工具輔助下，對爭議歌詞或其受著作權保護之部分進行感知，即便為機率性質或需工具之間接感知，都仍屬於可感知之範圍。

本案中法院用於判斷重製之另一項判斷要素係被侵權著作(歌詞)之原創性元素是否得於被控侵權對象(ChatGPT 生成

[3] 指透過實體方式將作品固定，使人類感官能直接或間接感知該作品。如將旋律寫成譜等。



本報告之智慧財產權歸屬於國發會

內容)作品中可供識別。Chat GPT 得依據特定關鍵詞於未經線上搜索之情形下，完整呈現歌詞之核心如創作者之心境、營造畫面、手法、結構感等獨創性要素，法院認為該語言模型係以完成對歌詞可再現地實體化，屬於重製行為。

3. 資料探勘例外之不適用

德國著作權法落實歐盟《數位單一市場著作權指令》(DSM 指令)，於其著作權法第 44b 條訂有資料探勘例外條款，在著作權人未保留其權利之前提下，得重製合法取得之著作進行資料探勘。而 AI 語言模型之訓練屬於此條資料探勘例外之範疇。雖 AI 模型訓練為資料探勘之範圍，惟本案法院認為，OpenAI 之語言模型重製行為已超出資料探勘之規範目的，其訓練資料並非僅被用於評估與分析，而是完全被納入模型參數中，隨時會因使用者輸入而被任意使用與提出，模型中之重製已實質侵害著作權人之權利。

此外，法院認為該案不得以立法者未預見之漏洞及規範事項與待規範事項兼具可比利益為由抗辯，因系爭歌詞被語言模型永久記憶後，對著作權人所造成之損害遠超過僅用於資料探勘文意規範之分析機率與關聯性等用途。

4. 公開傳輸之侵害

除重製以及資料探勘以外，OpenAI 同時違反了德國著作權法之公開傳輸規定。該語言模型之運作方式提供任何擁有網路存取及設備之人使用，有足夠多的人數得存取記憶化之歌詞，屬公開傳輸。於模型內重製未經授權之著作後公開傳輸，係違反德國著作權法之規定，侵害著作權人之權利。

5. 結論



本報告之智慧財產權歸屬於國發會

慕尼黑地方法院認為，OpenAI 並未於訓練時透過合法方式取得著作權資料之授權及給予合理補償，該行為構成不當重製，不得主張資料探勘之合理使用，因此判 OpenAI 敗訴，其仍能提出上訴。

■ **資料來源：**


1. Urteil GEMA gegen Open AI, 2025-11-11, https://www.justiz.bayern.de/gerichte-und-behoerden/landgericht/muenchen-1/presse/2025/11.php (last visited 2025/12/18)
2. GEMA sues for fair compensation, GEMA, 2025-11-13, https://www.gema.de/en/news/ai-and-music/ai-lawsuit (last visited 2025/12/18 )


## 五、 韓國

### (一)2025 年 6 月 30 日韓國文化體育觀光部與韓國著作權委員會發布《生成式人工智慧生成物之著作權爭議預防指南》

於 2025 年 6 月 30 日，韓國文化體育觀光部(Ministry of Culture, Sports, and Tourism, MCST)與韓國著作權委員會(Korea Copyright Commission, KCC)發布《生成式人工智慧作品著作權爭議預防指引》，旨在提供各界關於生成式 AI 產出物可能引發之著作權爭議之預防與應對指導。隨著 AI 技術之迅速發展，AI 生成內容與人類創作之間之界限日益模糊，對著作權之保護與侵害判定產生新挑戰。因此，本指引之目的在於幫助著作權人、AI 使用者及 AI 服務經營者了解相關法律規範，釐清如何識別與預防可能之侵權行為，並提供實務操作指引，確保 AI 技術之發展不會侵害原創作品之合法權益。藉此促進 AI 技術與著作權保護之間之平衡，保障創作自由與智慧財產之合法性。

1. 韓國著作權法概要



本報告之智慧財產權歸屬於國發會

(1) 著作權

指引首先概述韓國著作權法。著作權法所保障之權利包含著作人格權以及著作財產權，著作人格權係為保護著作人名譽及人格利益而設，共有公開權、署名權以及同一性維護三種類型；著作財產權則係為保障著作人經濟利益所設之權利，由重製權、演出權、公眾傳達權、展示權、發行權、出租權及改作權七種類型組成。而著作權財產權之保護期間係依據作品性質，自作品創作完成後至著作人死亡或著作公開之次年 1 月 1 日起 70 年後。

(2) 著作鄰接權

指表演者、錄音製作者、廣播業者得控制其表演、錄音或廣播使用之類著作排他權利，包含重製、發行、互動傳輸等報酬請求權。著作鄰接權之保護期間為公開演出、聲音固定於錄音物及廣播播出那一刻算起，通常 70 年（廣播為 50 年）。

(3) 其他權利

著作權使用者得以專屬地發行、重製或傳輸著作物之權利，受設定專屬發行權者，有排他對第三人主張該著作之排他使用權。受設定專屬發行權之人，無需著作權人代位，即得成為第三人侵害其專屬發行權之原告。

(4) 著作財產權之限制

法定情形下，允許未經著作權人許可使用其著作。該些例外情形如教育用途、新聞報導、引用、非營利表演、私人複製、公眾作品自由使用等。

(5) 侵害著作權救濟措施



本報告之智慧財產權歸屬於國發會

受到著作權侵害之人得對侵權者提出民事救濟及刑事處罰。民事救濟包含停止侵權、損害賠償金（實際或法定損害）、返還不當得利等；刑事部分，若侵害著作財產權得處 5 年以下有期徒刑或罰金 5 千萬韓元，若是侵害著作人格權則是得處 3 年以下有期徒刑或 3 千萬韓元以下罰金。

另外亦設有調解制度，由專家組成之調解委員會，藉調解委員之專業知識，引導當事人達成和解，較訴訟快速且保密。

2. 生成式 AI 與生成作品

生成式 AI 係根據提示詞生成文字、圖像、聲音、影片等之 AI。生成式 AI 生成作品係未有任何人類創作性貢獻之生成式 AI 輸出成果。生成式 AI 應用作品係指人類於創作過程中運用 AI 作為創作工具，且有可被認定為人類創作性參與部分之作品，如對生成式 AI 生成物進行修改增減等。

3. 生成式 AI 生成物侵權之著作權侵害

生成式 AI 分為訓練及服務階段，不同階段可能產生不同法律問題，本指引僅針對生成式 AI 生成物之著作權侵害提供注意事項說明，不包含訓練階段之著作權侵害問題。於生成式 AI 服務階段可能產生之著作權侵害包含重製權、互動式傳輸權(Right to interactively transmit)及二次創作等權利，生成式 AI 作品是否侵權須確認其是否有實質相似。

4. 判定侵權之要素

判斷著作權侵害要素為接觸判斷、實質相似以及侵權主體判斷。



本報告之智慧財產權歸屬於國發會

接觸判斷為判斷是否於侵害他人著作權時曾觀看或接觸過他人著作，於生成式 AI 作品之情形下，須判斷生成式 AI 使用者於生成生成式 AI 作品時已識別該當著作並基於此進行創作或特定著作是否被納入訓練資料中。實質相似判斷，係判斷生成式 AI 作品與現有著作之表現是否相同或相似，該判斷須依據個案而定。侵權主體認定上，一般而言係由輸入提示詞之使用者負侵權責任，惟於特定情形下，如 AI 提供者於訓練過程中使用著作進行訓練或微調，AI 提供者也可能被認定負擔一定程度之侵權責任。

5. 著作權人注意事項

(1) 著作權爭議預防

雖韓國法院目前尚未有針對 AI 學習受著作權保護著作是否構成著作權侵害之判決，惟指引提供著作權人不希望其著作於未經許可下被用於 AI 學習之方法：

A. 著作權人得透過適當方式明示反對其著作被用於 AI 訓練。目前韓國內部及國際上皆在討論如著作權人明示拒絕以及加強 AI 學習透明度等相關政策或技術方案，以確保著作權人權利行使及 AI 產業發展間之平衡。

B. 著作權人得利用技術手段防止其作品被未經授權成為 AI 訓練資料，並預防因此而生之著作權爭議。例如，著作權人得透過於網站或資料庫中設置 robots.txt 檔案限制爬蟲爬取或管理使用權限。

C. 著作權人亦得利用網站如 haveibeentrained.com 檢查作品是否被用於 AI 訓練，並得於必要時提出刪除請求。



本報告之智慧財產權歸屬於國發會

(2) 生成式 AI 作品產生著作權爭議時之應對

A. 著作權人可利用 KCC 之調解制度，調解若成立將具有與法院判決同等效力。

B. 著作權人可採取民事措施如禁制令、損害賠償、銷毀侵權作品。

C. 若情節嚴重，著作權人可提出刑事告訴。

6. 生成式 AI 使用者注意事項

(1) 提示詞輸入注意事項

使用者應避免輸入特定作品(如特定文學作品、歌詞等)之內容或可能導致生成與該著作相同或相似結果之提示詞，於參考著作輸入提示詞時，須注意生成式 AI 生成之作品是否包含該著作之重要部分。另亦應注意人格權、肖像權、商業機密等其他權利之侵害，並應避免損害他人名譽或受保護之技術及機密資訊。

(2) 使用或公開 AI 生成作品之注意事項

若使用者將生成式 AI 生成結果用於營利目的，須確認無侵害第三人權利。個人利用生成式 AI 生成作品可能不構成侵權，但若將其公開或共享。則可能產生著作權侵權問題。

(3) 審閱服務條款之重要性

生成式 AI 業者於其服務條款中多以明確規定生成作品之著作權歸屬以及可否商用之資訊，生成式 AI 使用者須仔細審閱並遵守相關規範。

(4) 生成式 AI 使用者之侵權責任



本報告之智慧財產權歸屬於國發會

原則上係由使用者負擔侵權責任，具體責任範圍及適用依個案而定。

7. 生成式 AI 業者注意事項

(1) 生成式 AI 業者類型

生成式 AI 業者分為 AI 開發者及利用已開發生成式 AI 提供服務者。

(2) 生成式 AI 作品著作權責任

由於生成式 AI 模型訓練、評估及更新為反覆進行之過程，利用基礎模型提供服務之生成式 AI 業者無法完全掌握其模型所學習之所有資料，於著作權侵權行為產生時，通常難以清楚認定責任歸屬。故，不論生成式 AI 開發者或利用者，皆應於簽訂使用合約中，明確規定責任歸屬。對於除著作權以外之權利，生成式 AI 業者亦應充分理解並採取適當措施。

(3) 預防著作權爭議之措施

生成式 AI 業者於建立 AI 模型時，應考慮著作之使用目的、性質以及貢獻等各類情形，生成式 AI 業者可能會因生成式 AI 生成之結果而負有著作權侵權責任，因此須依據業者本身特性，採取必要措施以避免侵害他人著作權，例如利用篩選功能，對可能涉及著作權侵害之請求拒絕回應；或刪除特定關鍵詞，如角色名稱、藝術家之作品等。指引亦建議，生成式 AI 業者於訓練 AI 時，可事先與著作權人簽訂授權契約，以確保合法使用著作內容及避免潛在爭議。

(4) 生成式 AI 服務條款建議



本報告之智慧財產權歸屬於國發會

生成式 AI 業者應透過服務條款明確界定生成式 AI 生成作品之責任歸屬，並提醒使用者避免生成侵權內容。此外，生成式 AI 業者得建立使用者保障機制，於商業使用相關著作權侵權訴訟中，為使用者提供法律保護並承擔相關費用。

8. 附錄要點（Q&A）

(1) 模仿風格（創作方式、繪畫風格等）是否侵害著作權？

著作權為保護表達人類思想或情感之創作物，單純事實、想法非表達形式，非著作權法保護對象。故 AI 若生成作畫手法、畫風等風格相似之作品不構成著作權之侵害。

(2) 生成式 AI 產出之作品是否屬受著作權保護之著作？

受著作權保護著作須為表達人類思想或情感且具有創作性。生成式 AI 生成作品可分為生成式 AI 應用作品以及生成式 AI 生成作品。前者為人類於創作過程中使用生成式 AI 作為工具而生，若人類創作程度受到認可，則屬應用生成式 AI 之著作；後者則是依據人為提示詞所生成，未有人類思想或情感，非著作權法上之著作。但認定上仍須依個案由法院裁定。

(3) 合理使用（Fair Use）判斷要素

合理使用之判斷要素包含：使用目的與性質、著作種類與用途、使用部分於著作中所佔比例與其重要性、著作使用對該著作現有市場及潛在市場或價值所造成之影響。該 4 項判斷要素為依據具體事實及情況依個案適用，並且著作是否屬合理使用，須由法院裁定。



本報告之智慧財產權歸屬於國發會

(4) 未經許可使用生成式 AI 翻唱作品或肖像、聲音等，是否會構成著作權侵權？

歌手之聲音或肖像非著作權保護之對象，惟若未經授權，利用 AI 製作翻唱曲，於製作過程中須對唱片進行學習，過程涉及重製，可能會構成對著作權及鄰接權之侵害。

(5) 如何取得著作使用許可，以及使用費用如何計算？

若欲使用他人作品，須事先取得著作權人許可。著作權人（或代管作品之集體管理組織）與使用者協商決定著作使用費。

(6) 應以哪部法律作為判斷侵權之標準？

外國著作與韓國著作相同或相似而生之著作權侵權問題，原則上，依作品被使之地點決定適用之法律。例如，生成式 AI 生成之作品若於韓國發行或販售，適用韓國法；於美國發行或販售，則適用美國法。網路作品可能同時在多國使用，這時可能會涉及多國法律或跨國訴訟。一般而言，侵權行為發生地或作品實際使用地為決定適用法律之關鍵依據。

(7) 著作權侵害是否成立之判斷主體？

生成式 AI 作品是否侵權，僅能由法院作出最終判斷。政府或相關機構可提供意見或參考案例，但不具法律強制力，僅能作為參考。

■ **資料來源：**

1. Korea Copyright Commission, 생성형 인공지능 결과물에 의한 저작권 분쟁 예방 안내서, 2025-06-30, https://reurl.cc/xKgq1Z (last visited 2025/11/06)



本報告之智慧財產權歸屬於國發會

2. JD SUPRA, South Korean Copyright Office Issues AI Guidance , 2025-07-31, https://www.jdsupra.com/legalnews/south-korean-copyright-office-issues-ai-6591715/ (last visited 2025/11/06)

## 六、 中國大陸

### (一)2025 年 3 月中國大陸國家互聯網信息辦公室發布《人工智慧生成合成內容標示辦法》

2025 年 3 月 7 日中國大陸互聯網信息辦公室、工業和信息部、公安部及國家廣播電視總局共同發布《人工智慧生成合成內容標示辦法》，以促進 AI 健康發展並維護公共利益，該法標準化地要求網路資訊服務提供者於 AI 生成合成內容增加顯示及隱式標示。該法於 2025 年 9 月 1 日起施行。

1. 適用對象

該法適用於以符合《互聯網信息服務法推薦管理規定》、《互聯網信息服務深度合成管理規定》及《生成式人工智慧服務管理暫行辦法》規定之網路資訊服務提供者（下稱服務提供者）對 AI 生成合成內容進行標示。

2. 顯式標示

該法所指 AI 生成內容之標示分為顯式標示及隱式標示。顯式標示係指於生成之合成內容或互動界面中以文字、聲音、圖形等方式標示，使用戶得明顯知悉該內容為 AI 所生成，且服務提供者應於提供生成內容下載、複製、匯出等功能時，確保檔案中包含有符合規定之顯式標示。顯式標示應依據不同類型內容依照下列要求進行：



本報告之智慧財產權歸屬於國發會

(1) 文字內容：於開頭、結尾或中間適當位置增加標示或於互動介面、文字周邊增加明顯提示之標示。

(2) 音訊內容：於開頭、結尾或中間適當位置加入語音提示或節奏提示等標示，或於互動介面上增加明顯之提示標示。

(3) 圖片：於適當位置加入明顯提示標示。

(4) 影片：於開頭畫面及影片播放介面適當位置，應加入明顯易辨識之提示標示，並可視需要於影片中段或結尾處增設提示標示。

(5) 虛擬場景：應於起始畫面之適當位置增加提示標示，或可於虛擬場景持續提供服務之過程中，於適當位置增加明顯提示標示。

(6) 其他生成合成內容服務依據其自身特性增加明顯之提示標示。

3. 隱式標示

隱式標示則是指透過技術手段，將標示嵌入於生成內容檔案之中繼資料(metadata)，隱式標示包含生成合成內容之屬性資訊、服務提供者之名稱或識別碼及內容編號等與製作相關資訊。此種標示相較於顯式標示較不易被使用者察覺，該辦法鼓勵服務提供者於生成合成內容中以數位浮水印等形式添加隱式標示。此外，若為提供網路內容傳播之服務提供者，須檢驗其中繼資料是否含有隱式標示，若中繼資料為 AI 生成，則需於中繼資料上添加顯式標示。

4. 用戶協定

服務提供者須於用戶協定中明確說明生成合成內容標示之方法、樣式及規範等內容，並應提醒用戶詳細閱讀相關標



本報告之智慧財產權歸屬於國發會

示之管理規定。該辦法亦給予用戶權利向服務提供者申請提供無顯式標示之生成合成內容，惟須透過用戶協定明確約定用戶之標示義務及使用責任，並且相關紀錄（包含提供對象資訊）之保留不得少於6個月。

5. 違反規範

若違反規定，由前述包含網路信息、電信、公安及廣播電視等有關主管機關依據職權及法律進行相關處理。

■ **資料來源：**

1. 中华人民共和国中央人民政府, 关于印发《人工智能生成合成内容标识办法》的通知，2025-03-07，https://www.gov.cn/zhengce/zhengceku/202503/content_7014286.htm (last visited 2025/04/15)

## 貳、 AI 應用之消費者/使用者保護議題國際趨勢

### 一、 美國

#### (一)2024 年 12 月俄勒岡州檢察總長發布《俄勒岡州事業人工智慧指引》

2024 年 12 月俄勒岡州檢察總長(Oregon Attorney General, OAG)發布《俄勒岡州事業人工智慧指引》(Guidance on AI for Oregon Businesses)，旨在幫助事業瞭解適用於 AI 之相關監管法律。隨著 AI 之發展，其演算法運算結果之不可預測性，雖可能發現傳統運算模式無法發掘之解決方案，但亦可能導致對公平性、可責性(accountability)及可信度之疑慮。此外，AI 之運用亦為消費者帶來重大之風險，包括隱私、歧視、責任及透明度等核心問題。尤其 AI 通常需要依賴大量個人資料之蒐集與儲存，增加了個資外洩、未經授權使用消費者資料甚至普遍監控消費者之可能性等。



本報告之智慧財產權歸屬於國發會

儘管俄勒岡州並無實質之 AI 立法，但事業使用 AI 仍須受其他法律拘束，如透過之《俄勒岡州非法交易行為法》(Oregon Unlawful Trade Practices Act, OUTPA)、《俄勒岡州消費者隱私法》(Oregon Consumer Privacy Act, OCPA)、《俄勒岡州消費者資料保護法》(Oregon Consumer Information Protection Act, OCIPA)及《俄勒岡州平等法》(Oregon Equality Act, OEA)等法律監管 AI 之運用。該指引提醒 AI 開發者及部署者可能違反前述法令規定之行為，重點摘述如下：

1. 《俄勒岡州非法交易行為法》(OUTPA)

該法禁止於消費交易中為不實之陳述。開發、銷售或部署 AI 技術之事業應確保 AI 產品之透明度，並向消費者提供準確之資訊。縱使未直接向消費者為不實陳述，AI 開發者或部署者亦須為其產品對下游消費者造成之損害負相應之法律責任。

於以下情形，事業宣傳、提供或銷售 AI 產品或服務，或於宣傳、提供或銷售其他產品或服務時採用 AI，則該事業違反 OUTPA：

(1) 於招標或交付 AI 產品時，未向消費者揭露已知之重大缺陷或重大不合格之情形。

(2) 不實陳述 AI 產品或利用 AI 技術不實陳述產品或服務具有其不具備之特性、用途、益處或品質。例如 AI 開發或部署者謊稱 AI 系統具備其實際上不具備之功能，或聊天機器人謊稱其為人類等。

(3) 使用 AI 不實陳述商品或服務具有實際上沒有之贊助、核准、從屬關係或連繫。例如利用 AI 發布虛假之產品評論，或使用 AI 生成影片使原未被代言之產品其看起來似由名人代言等情形，皆係違反 OUTPA 之規定。



本報告之智慧財產權歸屬於國發會

(4) 使用 AI 對降價之原因、存在狀態或金額進行虛假或誤導的事實陳述。例如若全年提供相同或基本相似之折扣，則公司不得使用 AI 生成「限時」或「閃購」之廣告或電子郵件發送於消費者。

(5) 於緊急情形下使用 AI 設定不合理之價格，違反《俄勒岡州反價格剝削法》(Oregon's Anti-price Gouging Law)。

(6) 使用 AI 生成之聲音為自動語音電話(robocall)活動時，扭曲或偽造資料，包含身分及通話目的。

(7) 使用 AI 採取不合理手段，以銷售、出租、或處置不動產、商品或服務，或進行債務催收或執行義務。禁止故意利用消費者無知，或故意允許消費者進行無法獲得實質利益之交易而使用 AI。

2. 《俄勒岡州消費者隱私法》(OCPA)

賦予消費者對其個人資料之控制權，得以知悉事業是否蒐集或處理其個人資料，亦得要求存取自己之資料、更正不正確之資料，以及刪除資料。

使用個人資料訓練 AI 系統之開發者，須於可訪問且容易理解並清晰之隱私聲明(privacy notices)中明確被揭露。於實體使用個人資料開發或訓練 AI 模型前，須先取得消費者明確同意。開發商購買或使用其他事業之資料集為模型訓練時，開發商應視為 OCPA 之控制者，須遵守與最初蒐集資料事業相同之標準。

資料提供者及開發者不得透過事後追溯或被動修改隱私聲明及使用條款，而將使用先前蒐集之個人資料於訓練 AI 模型之作為合法化。相反的，資料提供者及開發者須另就上開資料之任何新用途或二次利用取得同意。資料之開發者及使



本報告之智慧財產權歸屬於國發會

用者，須提供消費者撤回先前同意資料利用之機制。消費者若撤回同意，則資料之開發者及使用者須於接收撤回通知之15日內停止處理其資料。

OCPA並允許消費者得有機會選擇不使用AI模型作成對其具有法律或類似重大影響之決策，例如：教育、購屋或貸款等。OCPA賦予消費者得要求刪除其個人資料的權利，故適用OCPA之組織於使用AI模型時，須考量如何尊重消費者此一權利。

此外，組織在利用資料進行分析，或從事可能對消費者產生更大損害之作為（包括處理敏感性資料）時，應進行資料保護之影響評估。且有鑑於生成式AI模型、專有資料(proprietary data)以及演算法之複雜性，組織應意識到將消費者資料輸入AI模型並進行處理，可能會對消費者帶來更高的風險。而即使為不適用OCPA之組織，若其行為與其公開聲明當中關於如何蒐集、利用或揭露消費者資料之政策相互矛盾，亦可能違反消費者保護法。換句話說，即使是運用AI導致對消費者之誤導，於法律上仍可能被視為詐欺之行為。

3. 《俄勒岡州消費者資料保護法》(OCIPA)

擁有、授權、維護、儲存、管理、蒐集、處理、取得或以其他方式擁有個人資料之AI開發者、資料提供者及資料使用者須遵守OCIPA規定，透過合理之安全措施保護消費者資料，例如：於出現安全漏洞時，通知消費者及OAG，違反本法規定者，將可能依據OUTPA進行執法。

4. 《俄勒岡州平等法》(OEA)

OEA 規定主要係進一步強化俄勒岡州之反歧視保護措施。依據OEA之規定，基於種族、膚色、宗教、性別、性取



本報告之智慧財產權歸屬於國發會

向、性別認同、國籍、婚姻情形、年齡或身心障礙之歧視均屬於違法。OEA 將反歧視之保障延伸至居住及公共設施方面，以確保所有人皆能獲得平等享受相關措施之機會。例如：房屋租賃管理事業使用 AI 抵押貸款審核系統，因使用有偏見之資料訓練 AI 系統，導致持續拒絕提供來自某些社區或種族背景之合格申請人之貸款，該事業則可能違反 OEA。

■ **資料來源：**


1. OREGON DEPARTMENT OF JUSTICE, AG Rosenblum Issues Guidance on AI for Oregon Businesses, 2024-12-24, https://www.doj.state.or.us/media-home/news-media-releases/ag-rosenblum-issues-guidance-on-ai-for-oregon-businesses/ (last visited 2025/01/15)
2. OREGON DEPARTMENT OF JUSTICE, What you should know about how Oregon's laws may affect your company's use of Artificial Intelligence, 2024-12-24, https://www.doj.state.or.us/wp-content/uploads/2024/12/AI-Guidance-12-24-24.pdf (last visited 2025/01/15)


### (二)2025 年 1 月美國聯邦貿易委員會發布對《人工智慧與消費者傷害風險》之政策方向建議

2025 年 1 月美國聯邦貿易委員會(Federal Trade Commission, USFTC)發布對《人工智慧與消費者傷害風險》(AI and the Risk of Consumer Harm)之政策方向建議，旨在解決事業採用 AI 系統及工具對消費者產生之相關風險，並要求事業須於消費者接觸 AI 系統及工具之前及之後採取必要措施防止相關風險之產生。消費者於生活上能經常接觸之AI系統及工具，包含客服聊天機器人、社群媒體動態(social media feeds)之推薦系統、臉部辨識技術，以及消費者是否或以何種條件獲得醫療協助、居住、工作或貸款之工具等。現行法律並無對 AI 之運用給予任何豁免規定，故部署 AI 系統及工具之事業均須遵守現行



本報告之智慧財產權歸屬於國發會

法律，包含 USFTC 執行之競爭及消費者保護相關法規。USFTC 得分析 AI 系統及工具是否侵害消費者隱私，以及是否容易受到惡意輸入(adversarial inputs)或攻擊，而使個人資料面臨風險；其並得檢視用於詐欺、操縱、非自願圖像或其他可能危及兒童或他人之生成式 AI 工具；USFTC 亦得考量用於醫療、居住、就業或金融等高風險環境決策之演算法產品的影響。以下為 USFTC 本次發布建議事業於開發、維護、使用及部署 AI 產品時，須考量之因素：

1. 部署產品之前及之後須採取必要措施防止損害。包含部署前之測試、評估、測量及記錄，以及部署後採取合理之措施，進行監控或測試，評估及減輕潛在之下游損害(downstream harm)，以及解決針對消費者作成決策之相關技術的使用與影響。

2. 採取預防措施，偵測及阻止與 AI 相關之冒充、詐欺、兒童性虐待素材及非自願之親密圖像。USFTC 於 2025 年初曾提出打擊冒充政府與事業行為之規則，而上開冒充行為可能因利用 AI 深度偽造而強化。而 USFTC 對此一議題，發起「語音複製挑戰[4]」(Voice Cloning Challenge)，旨在透過檢測及阻止未經授權用戶濫用語音複製軟體以保護消費者，包含應用有效之即時檢測或監控措施、使用解決方案評估現有內容、防止或阻止 AI 之誘騙及詐欺，以及利用解決方案建構防護機制，提供身分驗證或防止上游損害(upstream harm)。

3. 避免 AI 工具作出欺騙性聲明，導致消費者之金錢損失或使用戶面臨傷害風險：USFTC 近期已處理多起涉及 AI 產品之欺騙性宣傳，例如宣傳 AI 產品能幫助民眾創業或賺錢之宣傳等。同時亦有多起訴訟，涉及關於 AI 安全篩選產品、臉部辨

[4] 該挑戰為美國聯邦貿易委員會發起，對外徵求得保護人類不受語音複製技術欺騙之方法，包含產品、政策已及軟體，並祭出最高 35,000 美元之獎金。



本報告之智慧財產權歸屬於國發會

識軟體、AI 網路訪問工具等之虛假宣傳或陳述，或欺騙使用者帳號停用亦將停止利用使用者過往傳輸之照片或影片，但實際上卻未停用等。

4. 以預設方式確保隱私及安全：

生成式 AI 工具需要大量資料輸入，作為大型語言模型及其他類型 AI 模型訓練過程之一部分，其中資料可能包含高度敏感資料，USFTC 向事業提供有關確保資料安全及保護隱私之指導，例如：《生物辨識資訊政策聲明》(Policy Statement on Biometric Information)。USFTC 得基於職權向未遵守法律義務之事業提起訴訟。

■ **資料來源：**


1. Federal Trade Commission, AI and the Risk of Consumer Harm, 2025-01-03, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2025/01/ai-risk-consumer-harm (last visited 2025/02/18)
2. JD SUPRA, Artificial Intelligence Briefing: Trump 2.0 Executive Orders Revoke, Overhaul Biden Administration's Approach, 2025-02-05, https://www.jdsupra.com/legalnews/artificial-intelligence-briefing-trump-5010481/ (last visited 2025/02/18)


### (三)2025 年 1 月美國加州檢察總長辦公室發布《關於加州現行法適用於人工智慧之法律諮詢》

2025 年 1 月美國加州檢察總長辦公室(The California Attorney General's Office, AGO)發布《關於加州現行法適用於人工智慧之法律諮詢》(Legal Advisory on the Application of Existing California Laws to Artificial Intelligence)，旨在為開發、銷售及使用 AI 之消費者及實體（entities）提供指引，說明其於加州法律之權利及義務，包含於加州《消費者保護法》(Consumer Protection Laws)、《民權法》(Civil Rights



本報告之智慧財產權歸屬於國發會

Laws)、《競爭法》(Competition Laws)及《資料隱私法》(Data Privacy Laws)等。

AI 系統科技屬於產業之最前線，於實現科學突破、推動經濟成長及造福消費者等層面，具備巨大之潛力。AI 雖帶來新的機會，然而其使用則可能產生對特定對象嚴重的偏見或歧視，以及傳播假消息或製造詐欺之風險，對加州人民、機構、基礎設施、經濟及環境將可能造成傷害，故應以合法、安全、合乎道德及符合人性尊嚴之方式，負責任地開發及使用 AI 系統。加州現行法律提供許多可能適用 AI 系統開發及使用之保護措施。開發及使用 AI 系統之實體，包含企業、非營利組織及政府，須確保其開發或利用之系統，及其利用行為符合加州法律，包含保護消費者免受不公平及詐欺待遇、避免反競爭損害、歧視、偏見，並採行防止濫用消費者資料之法律。事業須理解其所使用之 AI 是如何被訓練，系統使用之資料及系統如何生成結果，且須了解若 AI 之使用造成傷害，可能產生之法律責任。AI 開發者需注意對消費者之透明度，須告知消費者其資料是否被作為訓練資料以及其如何透過 AI 做出影響消費者之決策。

以下為現行加州提供適用於開發及使用 AI 工具之法律重點說明：

1. 《不公平競爭法》(Unfair Competition Law)

該法為保護加州居民免受不合法、不公平或詐欺之商業行為或實務侵害。AI 為企業及消費者帶來新的工具，同時亦增加欺騙加州居民之新風險，欺騙或損害消費者之行為屬於《不公平競爭法》之範圍。該法亦規定，違反任何其他州法、聯邦法或當地法律之行為，均可依《不公平競爭法》獨立提起訴訟，《不公平競爭法》之適用範圍廣泛，包含各種情況下可能適用 AI 之法律。

依據《不公平競爭法》，下列情形可能屬於非法行為：



本報告之智慧財產權歸屬於國發會

(1) 虛假宣傳 AI 系統之準確性、品質或效用，如聲稱系統具有其不具備之能力、聲稱系統完全由 AI 驅動但實際上有部分功能為人為控制、聲稱部分功能由人類執行但實際上由 AI 執行，以及無根據地宣稱系統為準確的、執行任務之能力優於人類、具備特定特性、符合產業或其他標準，或無偏見。

(2) 使用 AI 促進或進行欺騙行為，如以深偽、聊天機器人及語音複製之產物，創設從未存在或發生過的人、事及言論。若未揭露使用 AI 創作媒體作品亦可能構成欺騙行為。

(3) 未經當事人事前同意，知情使用 AI 製作他人之姓名、聲音、簽名、照片或肖像。

(4) 出於傷害、恐嚇、威脅或詐欺他人之目的，使用 AI 假冒真人。

(5) 出於收受金錢或財產的目的，使用 AI 假冒真人。

(6) 出於任何非法目的，使用 AI 假冒真人。

(7) 使用 AI 假冒政府官員執行公務。

(8) 以不公平之方式使用 AI，包含以弊大於利之方式，以違反公共政策、不合乎道德、具壓迫或不實之方式，或可能造成重大傷害之方式。

(9) 建立、行銷或散佈不符聯邦或州法律之 AI 系統，包含之規範如《虛假廣告法》(False Advertising Law)、《民權法》、《隱私權法》，以及規範特定產業及活動之法律等。

(10) 事業亦可能因知情或應知情其所提供之 AI 產品將被用於非法行為時負有法律責任。



本報告之智慧財產權歸屬於國發會

2. 加州之《虛假廣告法》

加州之《虛假廣告法》（False Advertising Law）為加州居民提供防範欺詐性廣告之保護，禁止任何個人或企業製作或散佈任何已知或合理可知為錯誤或具誤導性之內容，以誘使公眾進行交易。該法禁止有關 AI 產品之能力、可用性及效用之虛假廣告，禁止將 AI 用於商品或服務，以及禁止任何主題之虛假廣告，無論其是否由 AI 生成。

3. 加州之競爭法

加州之競爭法包含反托拉斯之《加州卡特萊特法》(the California Cartwright Act)，及管制低於成本銷售(below-cost sales)及虧本誘購(loss leaders)等行為之《不公平營業行為法》(Unfair Practices Act)，以保護加州之經濟。AI 開發者及使用者應注意 AI 系統對公平競爭所造成之任何風險，例如定價系統。即使 AI 系統無意對競爭造成損害，也可能違反加州之競爭法；具主導地位 AI 公司之反競爭行為亦可能損害 AI 市場之競爭並違反聯邦或州之競爭法。

4. 加州之民權法

《加州安魯民權法》(the California Unruh Civil Rights Act)保護加州所有人民之自由與平等，不論其性別、種族、膚色、宗教、血統、國籍、身心障礙、醫療情況、基因資訊、婚姻狀況、性取向、公民身分、主要語言或移民情況如何。《加州公平就業及住房法》(The California Fair Employment and Housing Act)亦保護加州民眾免於受到因前述受保護特徵所生之就業或住房騷擾及歧視。AI 系統可能將社會及其他偏見納入其決策，AI 開發者及使用者應警惕這些可能對加州人民(Californians)產生非法影響之潛在偏見。



本報告之智慧財產權歸屬於國發會

其他法律亦要求對公民採取不利行動之實體須提出採取各該不利行動之具體原因，包含因使用 AI 做出判斷之情形。例如聯邦《公平信用報告法》(Fair Credit Reporting Act)及《平等信用機會法》(Equal Credit Opportunity Act)，以及《加州消費者信用報告機構法》(the California Consumer Credit Reporting Agencies Act)均要求行為實體須向因信用評分受到不利處分之加州公民提供明確理由。消費者金融保護局(Consumer Financial Protection Bureau)澄清，使用 AI 或複雜信用模型之債權人於拒絕或對個人採取不利行動時，須提供具體理由。

5. 加州《選舉不實資訊防治法》(Election Misinformation Prevention Laws)

加州相關法律亦為選舉中使用 AI 可能導致違法之多種情形提供指導。例如加州法禁止使用未明示為聊天機器人，且意圖誤導使用者其系統之虛假身分，以鼓勵購買商品或影響選舉投票(Bus. & Prof. Code, § 17941)。亦有法令禁止使用 AI 冒充民選公職候選人或倡議網站(Elec. Code, § 18320)，且禁止於當選後 60 日內，使用 AI 惡意散佈該候選人具有實質欺騙性之聲音或視訊媒體(audio or visual media)，意圖損害該候選人之聲譽或欺騙選民投票支持或反對該候選人(Elec. Code, 20010)。

6. 《資料保護法》(Data Protection Laws)

加州公民本即享有憲法保障之隱私權，無論對於政府或私人實體皆適用之。而資料隱私權(informational privacy)為防止個人之敏感及機密資料被散播或濫用之權益，亦為加州憲法所保障之核心隱私權益。AI 開發者及使用 AI 之實體須監



本報告之智慧財產權歸屬於國發會

控 AI 系統之訓練資料、輸入及輸出，以確保尊重加州居民依據憲法保有之隱私權。

(1) 《加州消費者隱私權法》(The California Consumer Privacy Act, CCPA)，廣泛監管消費者個人資料之蒐集、利用、銷售及分享，包含加強對敏感個人資料之保護。此外，個人資料亦可能包含 AI 系統對加州消費者所做出之推斷。CCPA 賦予個人以下權利：

A. 瞭解企業所蒐集之個人資料，及企業如何利用、共享這些資料。

B. 更正企業持有不準確之個人資料。

C. 刪除企業所蒐集之個人資料。

D. 選擇不銷售或分享個人資料。

E. 限制利用及揭露敏感個人資料。

蒐集及利用加州居民個人資料之 AI 開發者及使用者皆須符合 CCPA 規定，確保其蒐集、利用、保留及分享之個人資料為合理必要且符合目的，禁止出於未揭露之目的而處理個人資料。即使出於已揭露之目的而蒐集、利用、保留個人資料，亦必須與其目的相符。AI 開發者及使用者亦須了解 CCPA 也適用於，利用個人資料進行研究，以及得以輸出個人資料之 AI 系統中之個人資料。

(2) 《加州侵犯隱私法》(The California Invasion of Privacy Act) 限制錄製或聆聽私人電子通訊，包含未經同意之電話竊聽或錄製通訊，以及錄製或攔截行動電話通訊。禁止於未經同意之情形，使用檢查或記錄聲紋之系統以判斷陳述之真



本報告之智慧財產權歸屬於國發會

偽。開發者及使用者應確保其開發或使用之 AI 系統或各該系統利用之資料皆不違反規定。

(3) 《學生線上個人資料保護法》(Student Online Personal Information Protection Act)禁止教育科技服務提供者銷售學生資料、利用學生資料進行目標性廣告，以及除特定學校利用目的外蒐集學生之個人資料，包括家庭或遠距教學服務及公私立學校所利用之程式及服務。開發者及使用者應確保任何教育 AI 系統符規定。

(4) 《醫療資料保密法》(the Confidentiality of Medical Information Act)規範加州居民醫療資料之利用及揭露，適用於提供軟體或硬體於消費者以管理醫療資料、或用於診斷治療或管理醫療情況之事業，包含行動應用程式或其他相關裝置。AI 之開發者及利用者應確保任何用於醫療保健之 AI 系統，包含直接面對消費者之服務，須符合 CMIA 規定。

7. 新興之加州 AI 相關法律

加州頒布多項涉及 AI 使用之立法，於 2025 年 1 月生效，對企業及個人產生廣泛影響，摘述如下：

(1) 《生成式 AI：訓練數據透明法案》(Generative artificial intelligence: training data transparency, AB2013)為針對生成式 AI 資料訓練透明度之規範，要求 AI 開發者應於 2026 年 1 月 1 日起在其網站上揭露有關 AI 訓練資料之資訊，包括用於開發 AI 系統或服務時，訓練資料集之揭露。

(2) 《電信：自動撥號裝置：人工語音法案》(Telecommunications: automatic dialing-announcing devices: artificial voices, AB2905)為針對電信通訊事業自動撥號設



本報告之智慧財產權歸屬於國發會

備採用 AI 聲音之規範，要求使用 AI 產生或經過顯著修改與合成之行銷電話，必須揭露其對 AI 之應用。

(3) 針對娛樂產業及其他領域未經授權肖像使用部分，《違反公共政策之契約：個人或專業服務：數位複製品法案》(Contracts against public policy: personal or professional services: digital replicas, AB2602)，要求於 AI 技術製作之數位複製品中使用個人之聲音及肖像之授權契約，須包含對預期使用之合理具體描述，且須由法律顧問或工會代表該個人。《使用肖像：數位複製法案》(Use of likeness: digital replica, AB1836)則禁止在未經事前同意之情形下，於已故名人去世 70 年內使用其數位複製品，違反者將須給付權利受侵害之人 10,000 美元以上之賠償。

(4) 針對於選舉及競選資料中使用 AI，《1974 政治改革法:AI 政治廣告法案》(Political Reform Act of 1974: political advertisments: artificial intelligrnce, AB2355)法案要求任何使用 AI 生成或大幅修改之競選廣告，皆須揭露該廣告為「使用 AI 生成或進行實質性修改」。《2024 保護民主免受深度偽造欺騙法法案》(Defending Democrary from Deepfake Deception Act of 2024, AB 2655)法案則要求大型網路平臺必須開發並實施使用先進技術的程序，於選舉前後特定期間內，用以識別及移除具實質欺騙性之選舉內容，例如深度偽造。此外，該法案並要求於選舉前後更長之時間內，須就特定額外之內容標記為被操縱、不實或虛假；同時要求平臺須提供加州使用者便利舉報機制。

(5) 《兒童色情法案》(Crimes: child pornography, AB1831, SB1381)，擴大對 AI 濫用之禁止及報告，例如擴大現行兒童色情之刑事禁令(criminal prohibitions)，納入使用 AI 製作對兒童性虐待及性剝削之視覺描述。



本報告之智慧財產權歸屬於國發會

(6) 監管醫療保健環境之 AI 工具層面，醫療保險給付：醫療利用審查法案(Health coverage: utilization review, SB1120)法案則要求醫療保險公司應確保有具備執照之醫師監管對醫療照護服務及保險索賠進行決策之 AI 工具的使用。

■ **資料來源：**


1. California Department of Justice, Office of The Attorney General, California Attorney General's Legal Advisory on the Application of Existing California Laws to Artificial Intelligence, 2025-01-13, https://www.skadden.com/-/media/files/publications/2025/03/state-attorneys-general-may-fill/legal-advisory--application-of-existing-ca-laws-to-artificial-intelligence.pdf?rev=1ddc130e80f041e491cfedf097be8431&hash=63283A39FBC4922139C806C780F67E2A (last visited 2025/03/26)

2. JD SUPRA, California Attorney General Issues Two Advisories Summarizing Law Applicable to AI , 2025-01-17, https://www.jdsupra.com/legalnews/california-attorney-general-issues-two-3958548/ (last visited 2025/03/26)


### (四)2025 年 2 月科羅拉多州 AI 影響工作小組發布報告與建議，提議修改《關於與人工智慧系統互動之消費者保護法案》

2025 年 2 月科羅拉多州 AI 影響工作小組(Artificial Intelligence Impact Task Force)發布建議報告，建議修訂《關於與人工智慧系統互動之消費者保護法案》(Concerning Consumer Protections in Interactions with Artificial Intelligence Systems Act )。上開法案係於 2024 年 5 月 17 日由州長簽署，並將於 2026 年 2 月 1 日生效，旨在要求高風險 AI 系統之開發者及部署者採取合理且謹慎之措施，保護消費者免受高風險 AI 系統中任何已知或合理可預見之演算法歧視風險。經過 AI 影響工作小組考量關於保護消費者及勞工免受 AI 系統及自動偵測系統(automated detection systems, ADS)影響之問題後，本次報告提出相關



本報告之智慧財產權歸屬於國發會

建議，指出此法案可再「澄清、細化及改進」之規範範圍，摘要重點如下：

1. 高風險 AI 系統之「開發者」應遵守此法案所採取之合理謹慎措施：

   (1) 向高風險系統之部署者提供一份聲明，揭露相關高風險系統之特定資料。

   (2) 向高風險系統之部署者提供完成高風險系統影響評估所需之資料及文件。

   (3) 發表公開聲明，總結開發者已開發或意圖大幅修改目前提供予部署者或其他開發者之高風險系統類型，以及開發者如何管理任何已知或可合理預見之演算法歧視風險，此風險可能源於已開發或意圖大幅修改之高風險系統。

   (4) 於發現或收到部署者之可信賴報告(credible report) 90 日內，向檢察總長及已知高風險系統之部署者或其他開發者，揭露高風險系統已造成或有可能造成之任何已知或可合理預見之演算法歧視風險。

2. 高風險 AI 系統之「部署者」應遵守此法案所採取之合理謹慎措施：

   (1) 針對高風險系統實施風險管理政策及方案。

   (2) 完成高風險系統之影響評估。

   (3) 每年審查所部署之高風險系統，確保各該高風險系統不致造成演算法歧視。



本報告之智慧財產權歸屬於國發會

(4) 若高風險系統作出與消費者相關之重要決策，或將成為與消費者相關之重要決策之重要因素(substantial factor)，應向消費者通知特定事項(specified items)。

(5) 提供消費者更正高風險系統作出重要決策時所處理之不正確個人資料。

(6) 於技術可行時，賦予消費者得就因部署高風險系統而導致對消費者不利之重要決策提出申訴之權利，並透過人工審核所提之申訴。

(7) 發表公開聲明，總結所部署之高風險系統類型、如何管理所部署之高風險系統產生之任何已知或可合理預見之演算法歧視風險，以及部署者蒐集及使用資料之性質、來源及程度。

(8) 於發現高風險系統造成演算法歧視 90 日內，向檢察總長揭露。

3. 於本州開展業務之個人，部署或提供旨在與消費者互動之 AI 系統時，須確保揭露消費者與 AI 系統互動之情形。

整體報告以爭議及處理方式有無共識，共計提出 4 大類建議，重點摘述如下：

1. 本次擬議修訂具有明顯共識之問題

對於利害關係人提出相對影響較小之擬議修訂重點已存在共識，在此情況下，除非其他利害關係人提出工作小組未充分考慮之強烈反對意見，否則應納入修改。

2. 需透過額外時間及利害關係人之參與而可達成共識之問題



本報告之智慧財產權歸屬於國發會

諸多領域有利害關係人提出疑慮，雖然所提出之疑慮可能已達成共識，但於修訂細節存在分歧，於此情形下利害關係人應與政策制定者進行溝通，避免產生有不良效應之立法，例如：

(1) 更明確地定義「重大決策」之類型，以確保明確化可能受法律約束之對象。

(2) 重新制定「涵蓋決策系統」定義之豁免清單，及法律對開發者及部署者規定之義務豁免清單，以解決產業及公眾利益之問題。

(3) 針對管理開發者向部署者提供之資料及文件等相關條款提出修改建議。

(4) 對影響評估之時間及觸發事件等提出變更之建議。

3. 達成共識與否取決於是否以及如何對多個相互關聯部分進行變更之問題

於利害關係人間，有部分人員存在一定共識且認為有空間及餘地解決根本之疑慮，但仍有其他利害關係人有相反之疑慮，需解決這些疑慮方能達成共識。例如：

(1) 就建議修改之演算法歧視定義部分，取決於產業及公共利益團體針對開發人員及部署人員於預防演算法歧視方面應承擔之義務，以及如何執行上開義務方面所存在之強烈分歧能否達成共識。

(2) 若可就影響評估之固定間隔達成共識，則建議修正「故意及重大修改」之定義可能變得無關緊要。

(3) 利害關係人是否願意接受關於何時須向檢察總長提供資料之建議修正規定。



本報告之智慧財產權歸屬於國發會

(4) 擬議變更部署者之風險管理計畫的要求可能需與擬議修訂部署者之影響評估義務部分併同考慮。

4. 存在強烈分歧且需相當創造力以尋求解決方案之問題

工作小組已確定有諸多問題，利益團體對於擬議修正之方法，甚至是否進行修正都存在分歧。此類問題，工作小組尚無法提出實質性建議，但認為若利害關係人持續參與，將有機會找到解決之共識，例如：

(1) 「重要因素」(substantial factor)之定義，有助於將受法律約束之 AI 技術範圍明確化。

(2) 開發者與部署者之「注意義務」的定義及機制，或是否繼續納入注意義務之概念，抑或以更嚴格或較寬鬆之義務取代。

(3) 是否保留、最小化擴大目前小企業雇員少於 50 人之部署者免於擔負特定法律要求之豁免規定。

(4) 增訂提供機會於檢察總長執法前修正違規事件之條款。

(5) 擬議變更法律商業機密豁免規定。

(6) 擬議修正(revisions)消費者申訴權規定。

(7) 擬議變更檢察總長制定規則之範圍及法律實施時間。

■ **資料來源：**

1. Colorado General Assembly, Report and Recommendations, 2025-02, https://leg.colorado.gov/sites/default/files/images/report_and_recommendations_0.pdf (last visited 2025/02/13)

2. Colorado General Assembly, Consumer Protections for Artificial Intelligence, 2024-05-17, https://leg.colorado.gov/bills/sb24-205 (last visited 2025/02/13)



本報告之智慧財產權歸屬於國發會

(五)2025 年 02 月美國夏威夷州眾議院提出《關於 AI 法案》

2025 年 02 月美國夏威夷州眾議院提出《關於 AI 法案》(Relating to Artificial Intelligence Act, HB639)，要求從事商業交易之公司、組織或個人，於消費者與聊天機器人或模擬真人互動之技術進行交流互動時，應告知消費者。此外，銷售、廣告或提供聊天機器人的開發者，須揭露該聊天機器人為使用 AI 之聊天機器人，且能模擬真人行為及進行文字或口頭對話。

由於科技之進步，聊天機器人能與使用者進行高度擬人對話，使用者難以分辨其係與真人互動或是與聊天機器人互動。許多聊天機器人被設計用以模仿人類行為及對話，透過與使用者之互動以學習及適應，並且以各種方式影響使用者，從廣告到散播錯誤資訊，甚至得操縱使用者使其洩露個人資料等。惟目前少有法規要求公司或個人對使用者揭露其正在與聊天機器人互動，此類缺乏透明度的情形，可能誤導使用者認為正在與持有證照的專業人士如醫生、財務顧問或治療師對話。基此，夏威夷立法機關認為消費者應有權於與聊天機器人或其他擬真互動之技術互動時知情。故本法要求：

1. 從事商業交易之事業、組織或個人在消費者與聊天機器人或擬人機器互動時應予以告知。

2. 銷售、提供銷售、宣傳或提供聊天機器人之開發者必須揭露其所使用之聊天機器人是否使用 AI 且可模仿人類行為進行文字或口頭對話。

以下為本法案之重點說明：

1. 揭露要求

(1) 任何事業、組織或個人於從事貿易或商業行為時，不得使用 AI 聊天機器人或其他模仿人類行為的技術，並以可能誤導或欺騙使消費者合理相信其正在與真人交談之方式



本報告之智慧財產權歸屬於國發會

進行文字或語音對話，除非事業事先以明確且顯著之方式向消費者揭露其正在與 AI 聊天機器人或模仿人類行為之技術互動。若小型企業於不知情之情形下使用 AI 聊天機器人並不違反本章規定。除非該小型企業已被充分告知本部分之法律義務且被給予合理機會(reasonable opportunity)後仍未遵守。

(2) 任何 AI 聊天機器人的開發者，除非已以清晰顯著之方式揭露該聊天機器人使用 AI，且其能模仿人類行為，可能誤導或欺騙一般理性的人相信其正在與真人進行文字或語音對話，否則不得銷售、宣傳或提供任何 AI 聊天機器人。

(3) 根據本章規定，任何違反本條之行為，即視為不公平或欺騙之行為或作法。

2. 救濟

(1) 除後述(2)另有規定外，任何人因違反本章規定而受到損害，均可：

A. 就其所受之損害提起訴訟，若判決原告勝訴時，應向原告支付不少於 1 千美元或原告所受損害之 3 倍賠償金，以及合理之律師費及訴訟費；以及

B. 以禁止非法行為提起訴訟，若判決原告勝訴，原告將獲得合理之律師費及訴訟費。

(2) 前述(1)規定之救濟措施應適用於集體訴訟及事實上的集體訴訟或訴訟程序，前提條件為：

A. 前述 A.規定之最低 1 千美元賠償額不適用於集體訴訟或事實上的集體訴訟。



本報告之智慧財產權歸屬於國發會

B. 超過補償性損害賠償之 3 倍賠償金部分，應由法院酌情分配，以促進本章之有效執行，並嚇阻違反本章規定之行為。

C. 判決之損害賠償不得超過 1,000 萬美元。

(3) 本章規定之救濟措施為累積性，可於一次訴訟中提出。

(4) 除法律規定之其他救濟措施外，檢察總長及消費者保護辦公室主管得對違反本章規定之任何事業、組織、開發商或個人提出禁制令救濟(injunctive relief)請求。

3. 罰則

任何事業、組織、開發商或個人被發現違反本章規定，應處以不超過 500 萬美元之罰鍰。

除夏威夷州外，2025 年陸續有其他州訂定使用 AI 聊天機器人揭露之相關規定，以下為重點整理：

1. 麻薩諸塞州 2 月發布《要求聊天機器人通知消費者法案》(Requiring consumer notification for chatbot systems, SB 243)，修訂《一般法》(the General Laws)第 93 章，新增第 115 節揭露電腦化通訊(computerized communications)，重點如下：

任何人與消費者為任何形式之商業交易或貿易行為，於消費者在與機器人進行對話或其他互動時，可能誤導或欺騙一般理性的人，使其相信正在與真人進行對話，如未先以清楚明顯之方式告知消費者，其正在與電腦而非真人對話，不論該消費者實際是否受到誤導、欺騙或損害，則違反本第 93A 章第 2 條之不公平及欺騙行為或作法。

2. 阿拉巴馬州 4 月發布《消費者保護：當消費者誤信為與人互動時，使用電腦與消費者互動，為不法商業行為法案》



本報告之智慧財產權歸屬於國發會

(Consumer protection, use of a computer to interact with a consumer when consumer believes the interaction is with a human is an unlawful trade practice, HB 516 )，重點如下：

透過聊天機器人、AI 代理(AI agent)、虛擬化身(avatar)或其他以文字或聽覺進行對話之電腦技術與消費者進行商業交易或貿易行為，可能誤導或欺騙具備理性之人，使其相信正在與真人對話或互動，且符合以下情形，即構成欺騙行為(1)未以清楚明顯之方式告知消費者正在與非真人進行對話或互動；或(2)消費者有理由相信其正在與真人對話或互動。

3. 伊利諾州 4 月發布《消費者詐欺與欺騙性商業行為法修正案》(Amends the Consumer Fraud and Deceptive Business Practices Act, HB 3021)新增第 2HHH 節，商業交易；AI 揭露，該法案目前仍在審理程序中，法案重點如下：

任何人與消費者進行商業交易或交易行為時，不論消費者是否確實受到誤導、欺騙或損害，如出現以下情形即屬非法行為(1)消費者正在與聊天機器人、AI 代理、虛擬化身或其他以文字或聽覺進行對話之電腦技術，進行對話或以其他方式進行互動；(2)誤導或欺騙一般理性的消費者，使其相信正在與真人溝通；(3)未以清楚明顯之方式告知消費者，消費者正在與 AI 系統而非真人對話。

4. 緬因州 4 月發布《確保涉及 AI 消費者交易透明度法案》(An Act to Ensure Transparency in Consumer Transactions Involving Artificial Intelligence, HP 1154)，重點如下：

於下列情形，任何人不得使用 AI 聊天機器人或任何其他電腦技術與消費者進行商業交易或交易行為，其方式可能誤導或欺騙一般理性的消費者，使其相信正在與真人進行交易：



本報告之智慧財產權歸屬於國發會

(1)未以清晰明顯之方式告知消費者並非與真人進行交易；或

(2)消費者合理相信正在與真人對話。

■ **資料來源：**


1. LEGISCAN, Relating To Artificial Intelligence, 2025-02-05, https://legiscan.com/HI/text/HB639/2025 (last visited 2025/05/14)
2. LEGISCAN, Consumer protection, use of a computer to interact with a consumer when consumer believes the interaction is with a human is an unlawful trade practice, 2025-04-03, https://legiscan.com/AL/text/HB516/2025 (last visited 2025/05/14)
3. LEGISCAN, Amends the Consumer Fraud and Deceptive Business Practices Act, 2025-04-11, https://legiscan.com/IL/text/HB3021/2025 (last visited 2025/05/14)
4. LEGISCAN, Requiring consumer notification for chatbot systems, 2025-02-27, https://legiscan.com/MA/text/S243/2025 (last visited 2025/05/14)
5. 132nd MAINE LEGISLATURE, An Act to Ensure Transparency in Consumer Transactions Involving Artificial Intelligence, 2025-04-17, https://legislature.maine.gov/legis/bills/getPDF.asp?paper=HP1154&item=1&snum=132 (last visited 2025/05/14)


(六)2025 年 3 月猶他州州長簽署《AI 消費者保護修正案》

2025 年 3 月猶他州州長簽署《AI 消費者保護修正案》(Artificial Intelligence Consumer Protection Amendments, S.B. 226)，旨在保護消費者對生成式 AI 之使用，要求採用生成式 AI 與消費者互動之實體應向消費者揭露資訊，遵守相關透明度義務、確認涉及 AI 行為若違反《消費者保護法》(AI consumer protection laws)之相關責任、為相關揭露提供安全港(Safe harbor)之規定、授予消費者保護部(Division of Consumer Protection)制定規則及執法之權利、訂定罰則，以及延後《AI 政策法》(AI Policy Act)廢止之日程等。本修正案於 2025 年 5 月 7 日生效。



本報告之智慧財產權歸屬於國發會

以下為修正案之說明：

1. 相關名詞定義

(1)「消費者交易」(Consumer transaction)

A. 係指向個人（或表面上為個人） 出售、租賃、轉讓、授予或以其他書面或口頭之方式，移轉(transfer)或處分(disposition)特定商品、服務或其他有形或無形財產（證券及保險除外）的作為。而該作為之目的係為：

a. 個人、家庭或家戶用途；或

b. 涉及商業機會相關之目的：包含個人須持續向 A.指涉之特定個人支付金錢及財產，或須持續向 B.指涉之特定個人提供服務，且過去未曾受雇於該個人從事該服務。

B. 消費者交易包含

a. 前述 A.之轉讓或處置，包括要約、招攬(solicitation)、協議、或履行協議。

b. 慈善募款（charitable solicitation）。

(2)「生成式 AI」，係指 AI 技術系統：

A. 經過資料訓練。

B. 被設計以文字(text)、聲音(audio)或視覺傳達(visual communication)等一種或多種方式，模擬人類與消費者進行對話。

C. 於有限監督或無人監督之情形下，生成與人類建立之輸出相似之非劇本式輸出(non-scripted outputs)。



本報告之智慧財產權歸屬於國發會

(3)「高風險 AI 互動」(High-risk artificial intelligence interaction)，係指與生成式 AI 涉及以下內容之互動：

A. 蒐集敏感個人資料，包含健康資料、財務資料及生物辨識資料。

B. 提供個人化之建議、意見或資訊，使個人得基於合理之信賴，作出重大之個人決策，包含提供財務法律、醫療及心理健康等相關建議或服務。

C. 其他消費者保護部認定之適用情形。

(4)「許可證」(License)，係指猶他州政府授予個人從事特定職業之授權，包括基於符合州法律規定之個人資格，以及為個人合法從事職業取得報酬前必須取得之資格等。

(5)「受管制職業」(Regulated occupation)，係指符合受商業部管制，以及要求個人須取得許可證或猶他州認證始能從事之職業。

2. 違反《AI 消費者保護法》之責任

生成式 AI 作成以下行為，不得作為違反《猶他州法典》(Utah Code)第 13-2-1 條中所規定，由消費者保護部管理及執行之任何法規的抗辯理由：

(1) 作出違法聲明。

(2) 進行違法行為。

(3) 被用於助長違法行為。

3. 必要揭露義務



本報告之智慧財產權歸屬於國發會

(1) 供應商與消費者交易使用生成式 AI 與個人互動，若該個人詢問或以其他方式提示供應商是否正在使用生成式 AI 時，供應商須明確揭露該個人正與生成式 AI 互動而非真人。前述個人所提出之提示或問題須為明確清楚，並用以確認該個人正與 AI 而非真人互動的請求。

(2) 於受管制職業中提供服務之個人，應注意以下作為：

A. 若使用生成式 AI 提供之服務會構成與高風險 AI 互動之情況，應於提供服務時，向接受服務之個人顯著揭露其何時正在與 AI 進行互動。

B. 透過生成式 AI 提供服務時，應遵守受管制職業之所有要求。

(3) 上述(2)之揭露方式，包含於語音互動時，應於對話開始時以口頭方式提供；於書面互動時，於開始前以書面方式提供。

4. 安全港條款(Safe harbor)

(1) 於生成式 AI 與個人進行消費者交易或提供受管制服務之初，以及在整個互動過程中，若明確且清楚地揭露為與生成式 AI、非人類或為 AI 助理互動之情形，則不會因違反前述必要揭露義務要求而遭受執法行動(enforcement action)。

(2) 依據《猶他州行政規則制定法》(Utah Administrative Rulemaking Act)，消費者保護部與人工智慧政策辦公室(the Office of Artificial Intelligence Policy)得協商制定揭露形式及方法之規則，該些規則得為：

A. 符合前述安全港條款(1)之要求；或



本報告之智慧財產權歸屬於國發會

B. 不符合前述安全港條款(1)之情形。

5. 責任與罰則

(1) 檢察總長應

A. 就消費者保護部於本章所規定之職責提供法律建議。

B. 於消費者保護部履行本章規定職責時，擔任其法律顧問。

(2) 消費者保護部之執法權力

A. 得對違反本章之行為，處最高 2,500 美元之罰緩。

B. 得向法院提起訴訟以執行本章規定。

(3) 違反依本章規定發出之行政命令或法院命令者，每次最高可處 5,000 元美之罰鍰。於消費者保護部提起之任何民事訴訟中，檢察總長得依授權代為執行前述處罰。

■ **資料來源：**


1. UTAH STATE LEGISLATURE, S.B. 226 Artificial Intelligence Consumer Protection Amendments, 2025-03-27, https://legiscan.com/UT/text/SB0226/id/3174279 (last visited 2025/04/29)

2. SheppardMullin, Utah Enacts AI Amendments Targeted at Mental Health Chatbots and Generative AI, https://www.sheppardhealthlaw.com/2025/05/articles/artificial-intelligence/utah-enacts-ai-amendments-targeted-at-mental-health-chatbots-and-generative-ai/, 2025-03-15, (last visited 2025/04/29)




本報告之智慧財產權歸屬於國發會

(七)2025 年 3 月猶他州州長簽署《AI 修正案》

2025 年 3 月猶他州州長簽署《AI 修正案》(Artificial Intelligence Amendments, HB 452)，制定關於使用 AI 技術的心理健康聊天機器人(AI mental health chatbots)相關監管規定，旨在使提供使用 AI 技術的心理健康聊天機器人供應商遵守相關規定，為使用 AI 技術的心理健康聊天機器人之使用者提供保護措施，內容包含相關名詞解釋、對於使用者的個人資料保護、廣告限制、透明度要求以及執法權力等。HB 452 於 2025 年 5 月 7 日生效。

以下為 HB 452 重點整理：

1. 相關名詞解釋

(1) 「醫療保健提供者」(Health care provider)，指服務提供者、醫療或健康服務提供者，及於正常業務過程提供醫療健保服務、開立帳單或收取醫療保健費用之任何其他個人或組織。

(2) 「健康計畫」，指提供或支付醫療服務費用的個人或團體計畫。

(3) 「個人可識別健康資料」，指與個人身心健康或狀況相關之任何資料，不論為口頭或以其他形式或媒介記錄。

(4) 「心理健康聊天機器人」，指符合下列條件之 AI 技術：

A. 使用生成式 AI 與心理健康聊天機器人之使用者進行互動式對話，類似於個人與持有證照之心理健康治療師間之保密談話。

B. 供應商表示或使個人合理相信，可以或將會提供心理健康治療，或幫助使用者管理或治療心理健康狀況。



本報告之智慧財產權歸屬於國發會

C. 不包含以下 AI 技術：

a. 提供劇本式輸出(scripted output)，如引導冥想或正念練習。

b. 分析個人之輸入，以連結個人與真人心理健康治療師。

(5) 「心理健康治療師」(Mental health therapist)，指取得心理健康治療執照之個人，並於個人相關執照法規定之執業範圍內執業，如依法從事心理健康治療業務之醫師、外科醫師或整骨醫師；具有從事心理健康治療資格之心理學家；及具有從事心理健康治療實務資格認證之心理學住院醫師等。

(6) 「供應商」，指賣方(Seller)、出租人(Lessor)、轉讓人(Assignor)、要約人(Offeror)、仲介人(Broker)或其他定期招攬(Regulary Solicits)、從事或執行消費者交易之人，無論其是否直接與消費者交易。

(7) 「猶他州使用者」，指於近用或使用心理健康聊天機器人時，位於猶他州之個人。

(8) 「使用者輸入」，指猶他州使用者提供給心理健康聊天機器人的內容。

2. 心理健康聊天機器人之供應商應遵守之義務

(1) 個人資料保護

供應商不得向任何第三方出售或分享，包含猶他州使用者之個人可識別健康資料或使用者輸入的任何內容。除非由醫療保健提供者要求並獲得猶他州使用者同意、猶他州使用者要求提供於其健康計畫，以及為確保心理健康聊



本報告之智慧財產權歸屬於國發會

天機器人效能，供應商得與簽訂相關功能契約之第三方分享必要個人可識別健康資料。

前述分享必要可識別健康資料時，供應商及簽訂契約之第三方須遵守《健康保險可攜與責任法》(Health Insurance Portability and Accountability Act, HIPAA)所規範之相關隱私及安全規定。

(2) 廣告限制

A. 供應商不得於猶他州使用者與心理健康聊天機器人對話時，使用該聊天機器人向使用者廣告特定產品或服務，除非該聊天機器人清楚且明顯標示該廣告為廣告，以及向使用者清楚明顯揭露該廣告為贊助、商業關係(business affiliation)，或供應商與第三方達成之促銷、廣告或推薦產品或服務之協議。

B. 供應商不得將猶他州使用者輸入用於以下目的

a. 決定是否向猶他州使用者顯示產品或服務的廣告，除非該廣告之對象為心理健康聊天機器人本身。

b. 決定要向猶他州使用者宣傳的產品、服務或產品、服務類別。

c. 以客製化方式向猶他州使用者展示廣告。

C. 廣告限制不禁止心理健康聊天機器人推薦猶他州使用者尋求諮詢、心理治療或其他持有執照專業人士的協助，包含持有特定執照專業人士。

(3) 揭露要求



本報告之智慧財產權歸屬於國發會

心理健康聊天機器人供應商須於以下三種情形，使心理健康聊天機器人清楚且顯著地向猶他州使用者揭露，心理健康聊天機器人為 AI 技術而非真人：

A. 猶他州使用者可近用心理健康聊天機器人功能前。

B. 若猶他州使用者於過去 7 天內未近用心理健康聊天機器人，應於每次互動開始時告知。

C. 任何猶他州使用者詢問或以其他方式提示該心理健康聊天機器人是否為 AI 時。

3. 執法機關

(1) 州檢察長

A. 依據要求向消費者保護部提供法律建議。

B. 擔任消費者保護部之法律顧問，協助其履行本章規定之職責。

C. 得代表消費者保護部提起民事訴訟，以收取本段(3)之罰鍰。

(2) 消費者保護司除了須依據《猶他州法典》(Utah Code) 第 13 編第 2 章「消費者保護部」規定管理及執行本章規定外，額外賦予消費者保護部以下執法權力：

A. 於每次違反本章之行為，得處最高 2,500 美元之行政罰緩。

B. 向有管轄權之法院提起訴訟，以執行本章之規定。

(3) 法院得對違反本章規定之行政命令或法院命令行為，每次處以不超過 5,000 美元之罰鍰。



本報告之智慧財產權歸屬於國發會

4. 積極抗辯(Affirmative defense)

(1) 於訴訟中，心理健康聊天機器人供應商能證明以下情形，則得作為責任之積極抗辯：

A. 建立、維護並執行符合法定方式之政策，該政策須以書面形式為之、清楚闡明心理健康聊天機器人之預期目的、能力及限制、描述供應商所為之相關程序、以及確保遵守安全隱私之相關規範。

B. 保留關於心理健康聊天機器人開發與實施之文件紀錄，包含描述開發中使用之基礎模型、使用之訓練資料、是否符合聯邦健康隱私規則(federal health privacy regulations)、使用者資料蒐集與分享實務，以及持續進行確保準確性、可靠性、公平性及安全性之作為。

C. 供應商依法應向消費者保護部提交政策時，應提供：供應商名稱及地址、供應商所提供心理健康聊天機器人之名稱、書面政策及費用。申請之提出須依消費者保護部所規定之方式進行，以及可向消費者保護部提供備案政策之任何修訂，或供應商選擇提供之其他文件。

D. 於違法行為發生時，已遵守所有已備案政策之所有要求。

(2) 積極抗辯僅適用於違反以下事項之行政或民事訴訟：

A. 違反《猶他州法典》第 58-1-501 條 1 款之非法行為。

B. 違反《猶他州法典》第 58-1-501 條 2 款之不專業行為。

■ **資料來源：**



本報告之智慧財產權歸屬於國發會

1. UTAH STATE LEGISLATURE, H.B. 452 Artificial Intelligence Amendments, 2025-03-25, https://legiscan.com/UT/text/HB0452/id/3170911 (last visited 2025/05/05)

2. SheppardMullin, Utah Enacts AI Amendments Targeted at Mental Health Chatbots and Generative AI, https://www.sheppardhealthlaw.com/2025/05/articles/artificial-intelligence/utah-enacts-ai-amendments-targeted-at-mental-health-chatbots-and-generative-ai/, 2025-03-15, (last visited 2025/04/29)

(八)2025 年 5 月 16 日紐約州頒布針對人工智慧伴侶之新法

2025 年 5 月 16 日，紐約州頒布 AI 伴侶(AI Companion)相關之條款，監管機關注意到 AI 伴侶帶給人們的負面影響，故制訂法律規範 AI 聊天機器人等 AI 伴侶，以促進人類在使用 AI 時之心理健康及安全。此法更新於紐約綜合法（Consolidated Laws of New York）第 20 章（CHAPTER 20）一般商務（General Business）中第 47 節（ARTICLE 47 Artificial Intelligence Companion Models）之第 1700 條至 1704 條。並明定於 2025 年 11 月 5 日正式實施。

以下為重點整理：

1. AI 伴侶之定義：

AI 伴侶定義為利用 AI、生成式 AI 及/或情緒識別演算法(Emotional recognition algorithms)，並且目的為模擬與使用者間持續性之「人類或類人類之關係」之系統，而所謂人類關係不限於浪漫陪伴或交往關係。該模擬係透過存取與使用者先前之互動或使用者輸入之資訊及偏好，達到個人化互動、持續性互動、主動或未經請求提供使用者指令範圍以外之情緒性回應。本法中之 AI 伴侶排除僅用於客戶服務或商業資訊之



本報告之智慧財產權歸屬於國發會

系統、提升效能或研究技術協助之系統、僅供公司內部員工使用之系統。

法條中對 AI 伴侶經營者(Operator)之定義為提供消費者 AI 伴侶之個人、企業、協會、公司或商業實體，前述組織之成員、附屬機構、子公司或實質受益人亦屬之。使用者則是指紐約州內將 AI 伴侶作為個人用途之任何人。而情緒辨識演算法係指用以辨識與解讀人類情緒訊號之 AI 技術，包含文字、聲音、影響或其組合之形式。

2. AI 伴侶經營限制：

AI 伴侶經營者不得忽略使用者表達自殺或自我傷害之跡象，並須提供協議機制等合理努力偵測並提供協助管道，否則不得經營或提供 AI 伴侶系統。協議機制包含但不限於識別及偵測使用者有自殺或自我傷害意圖，並於偵測到前述情形時主動引導使用者聯絡緊急心理諮商服務機構，如自殺預防及行為健康危機熱線等。

3. AI 伴侶經營者之通知義務：

AI 伴侶經營者應於 AI 伴侶與使用者互動開始時，以口頭或書面之方式提供使用者清楚且明顯之通知，說明其並非在與人類溝通，每天無須超過 1 次；若為持續性 AI 伴侶互動，則須至少每 3 小時通知 1 次。

4. 罰則：

紐約州檢察總長若依據證據認 AI 伴侶經營者違反本法之規定,得提起訴訟要求法院禁止該經營者繼續其違法行為。並且亦能要求對違法行為處每日 1 萬 5,000 美元以下之民事罰鍰，及相關適當補救措施。本條所收取之費用及罰鍰應存



本報告之智慧財產權歸屬於國發會

入《州財政法》（the state finance law）第 99-ss 條設立之自殺預防基金。

■ 資料來源：

1. The New York State Senate, Artificial Intelligence Companion Models, 2025-05-16, https://www.nysenate.gov/legislation/laws/GBS/1700 (last visited 2025/07/25)

2. JD SUPRA, Regulatory Trend: Safeguarding Mental Health in an AI-Enabled World, 2025-07-21, https://www.jdsupra.com/legalnews/regulatory-trend-safeguarding-mental-7610166/ (last visited 2025/07/25)

### (九)2025 年 6 月美國德州州長簽署通過《德州負責任地人工智慧治理法案》

2025 年 6 月美國德州州長簽署通過《德州負責任地人工智慧治理法案》(the Texas Responsible AI Governance Act, HB 149)，當中包含監管提供德州居民 AI 系統、產品或服務之開發者或部署者，或於德州推廣、廣告或開展業務之人，以達到以下目的：(1)促進及推進負責任的 AI 系統的開發及使用；(2)保護個人及群體免受與 AI 系統相關之已知或可合理預見之風險；(3)提供開發、部署及使用 AI 系統之風險透明度；(4)提供國家機關使用或考慮使用 AI 系統之合理通知。該法案將於 2026 年 1 月 1 日生效，以下為此法案之重點整理：

1. 向消費者揭露 AI 系統

政府機關若欲提供與消費者互動之 AI 系統，不論一般理性之消費者是否能明顯察覺其正在與 AI 系統互動，都應於互動前或互動時，向每位消費者揭露其正在與 AI 系統互動。揭露方式須為清晰顯著、並使用淺白語言撰寫、不得使用操弄



本報告之智慧財產權歸屬於國發會

性介面設計(dark pattern)。揭露方式得透過超連結將消費者引導至獨立網頁提供。

AI 系統若用於醫療照護服務或治療，該服務或治療的提供者應不遲於首次提供服務、治療之日或緊急情況時，於合理情形下盡快向服務或治療的接受者或接受者的代表揭露其正與 AI 系統互動。此醫療照護服務，指由州或聯邦法律取得執照、註冊或認證之個人所提供與人類健康、疾病或損傷之診斷、預防或治療有關之服務。

2. 不得有操縱人類行為(manipulation of human behavior)

任何人不得以故意煽動或鼓勵他人之方式，開發或部署進行身體自我傷害包含自殺、傷害他人或從事犯罪活動目的之 AI 系統。

3. 社交評分(social scoring)使用之限制

政府機關不得使用或部署依據已知、推斷或預測之社會行為或個人特徵，對自然人或群體進行評估或分類之 AI 系統，且該 AI 系統係以進行計算或分配該人或群體之社會分數，或類似的分類、評價，而已導致或可能導致以下情形：

(1) 在無關察或注意該行為特徵之社會環境中，對個人或群體造成不利或不利待遇(unfavorable treatment)；

(2) 在與觀察或注意該行為或特徵的性質或嚴重性不合理或不成比例之情形下，對個人或群體造成不利或不利待遇；或

(3) 侵害《美國憲法》(the United States Constitution)、《德州憲法》(the Texas Constitution)或州或聯邦法律所保障之任何權利。



本報告之智慧財產權歸屬於國發會

4. 擷取生物特徵資料(capture of biometric data)之限制

生物特徵資料，係指透過自動測量個人生物特徵所產生之資料，包含指紋、聲紋、眼睛視網膜或虹膜，或其他用於識別特定個人獨特性之生物圖案或特徵；不包含實體或數位照片或由實體或數位照片產生之資料、影片或錄音或由影片或錄音產生之資料，或依《1996 年健康保險可攜與責任法》(Health Insurance Portability and Accountability Act of 1996)所蒐集、使用或儲存之醫療照護治療、付款或操作資料。

政府機關不得未經個人同意開發或部署利用生物特徵資料或從網際網路或其他公開來源有針對性或無針對性地蒐集影像或其他媒體，以識別特定個人的 AI 系統，若該蒐集行為將侵害個人依美國憲法、德州憲法或州或聯邦法律所享有之權利。

5. 禁止非法歧視(unlawful discrimination)

任何人不得以違反州或聯邦法律，對受保護族群進行以非法歧視為目的之 AI 系統開發或部署。而本法中之受保護族群係指受到州或聯邦《民權法》(civil rights laws)所保障不受歧視之特徵、品質、信仰或身分之群體或階層，包含種族、膚色、國籍、性別、年齡、宗教或身心障礙。另外，本條規定單純之差別影響(disparate impact)並不足以證明歧視之意圖。

6. 禁止露骨性內容及兒童色情(sexually explicit content and child pornography)

該法規定，任何人不得開發或散布其唯一目的為製作、協助或幫助製作或散佈違反《刑法典》(Penal Code)第 43.26 節規定與兒童從事性行為或為性行為受害者相關之視覺素材(visual material)，或第 21.165 節深度偽造影片或圖像之 AI 系



本報告之智慧財產權歸屬於國發會

統。並且，任何人不得故意開發或散佈冒充或模仿未滿 18 歲兒童進行模擬或描述《刑法典》第 43.25 節定義之性行為的文字對話之 AI 系統。

■ **資料來源：**


1. LegiScan, Texas House Bill 149, 2025-06-22, https://legiscan.com/TX/text/HB149/2025 (last visited 2025/06/26)
2. Texas Responsible AI Governance Act, 2025-06-22, https://www.skadden.com/-/media/files/publications/2025/06/texas-charts-new-path/texas_responsible_artificial_intelligence_governance_act_traiga.pdf (last visited 2025/06/26)
3. K＆L GATES, Pared Back Version of the Texas Responsible Artificial Intelligence Governance Act Signed Into Law, 2025-06-25, https://www.klgates.com/Pared-Back-Version-of-the-Texas-Responsible-Artificial-Intelligence-Governance-Act-Signed-Into-Law-6-24-2025 (last visited 2025/06/26)


## 二、歐盟

### (一)2024 年 12 月歐盟執委會發布《關於瑕疵產品之責任指令》

2024 年 12 月歐盟執委會(European Commission)發布《關於瑕疵產品之責任指令》(EU 2024/2853 on liability for defective products)，簡稱《新產品責任指令》(The new Product Liability Directive, PLD)。本指令旨在更新及調整歐盟對新技術之責任規則，適用於數位時代及全球價值鏈，提供企業經營者(economic operators)更明確之法律確定性，並給予受害者更好的保護，確保受害者因接觸瑕疵產品而遭受損害時，得向製造商提出賠償請求。損害賠償基於以下兩主要原則：(1)製造商須賠償因產品瑕疵所造成之損害；(2)受害者須證明產品之瑕疵及所造成之損害，並證明該瑕疵為造成損害之原因。



本報告之智慧財產權歸屬於國發會

PLD 重點如下：

1. 遭受以下主要損害之一時，即應獲得賠償之類型

(1) 死亡或人身傷害，包含身體及心理傷害。

(2) 財產損失。

(3) 資料破壞或毀損。

2. 主要責任方

瑕疵產品之製造商為主要負責人。若於產品製造商並非於歐盟領域內，該非歐盟製造商仍須依據 PLD 承擔責任，受害者可向其於歐盟境內設置之其他負責代表請求賠償。包括進口商或授權代表(the importer or the authorised representative)；於無進口商或授權代表時，由履行服務之提供者(the fulfilment service provider)負責。

為知悉於歐盟之責任方(the EU-based liable party)為何，受害者得向瑕疵產品之經銷商(the distributor)請求取得歐盟責任方之資訊。若於提出請求後 1 個月內並無獲得任何歐盟責任方之資訊或經銷商無答覆時，受害者得向經銷商請求賠償。

線上平臺為企業經營者之一，對瑕疵產品承擔責任。依《數位服務法》(the Digital Services Act)規定，於特定條件[5]下即使僅為瑕疵產品中介之線上平臺，仍須與經銷商承擔相同之義務。

3. 產品與瑕疵

[5] 依據數位服務法第 6 條，賦予中介平台有條件責任豁免。中介平台在未知悉違法活動或內容、且未察覺足以顯示該違法活動獲違法內容之事實或情況，或知悉或察覺違法內容、情況後立即移除該內容，不負法律責任。故若中介平台明知違法情事卻無處理，需承擔相應責任。



本報告之智慧財產權歸屬於國發會

已投放至歐盟市場之所有產品，無論其類型為何皆須適用 PLD。產品若不能提供可期待之安全性或法律要求之安全性，則該產品將被視為有瑕疵。

PLD 將適用之產品範圍涵蓋至所有類型之軟體，包含應用程式、作業系統及 AI 系統。製造商須對於軟體或 AI 系統發布時存在之任何瑕疵承擔責任，包含發布後因更新、升級或機器學習功能而更為明顯之瑕疵。

經過實質修改(substantially modified)之產品將被視為新產品，而實施修改之人則為 PLD 定義之製造商。

4. 受害人請求損害賠償之時效

企業經營者於產品推出市場後 10 年內須對其瑕疵產品負責；與健康相關之案件，因其損害之顯現所需時間較長，故期限延長至 25 年。

受害者須於知悉或合理應知悉損害、缺陷及可依第 8 條負責之企業經營者身分之日起 3 年內向國家法院提出賠償請求。

5. PLD 其他規定

為確保執法資訊之透明度，國家最高法院及上訴法院須公布其對產品責任案件之判決。歐盟委員會將建立歐盟資料庫，以便法律執業者、學者及公眾查閱相關判決。

PLD 於 2024 年 12 月 8 日生效，適用自 2026 年 12 月 9 日起投放於歐盟市場之產品。歐盟國家須於 2026 年 12 月 9 日之前將該指令轉化為國家法律。

■ **資料來源：**



本報告之智慧財產權歸屬於國發會

1. European Commission, Liability for defective products, 2024-12-08, https://single-market-economy.ec.europa.eu/single-market/goods/free-movement-sectors/liability-defective-products_en#software-and-ai-systems (last visited 2025/01/09)

2. European Union, on liability for defective products and repealing Council Directive 85/374/EEC, 2024-11-18, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402853 (last visited 2025/01/09)

## 參、 AI 或演算法運用與勞工權益相關議題

### 一、 美國

#### (一)2024 年 10 月美國消費者金融保護局發布《消費者金融保護通函 2024-06》

2024 年 10 月美國消費者金融保護局(the Consumer Financial Protection Bureau, CFPB)發布《消費者金融保護通函 2024-06》(Consumer Financial Protection Circular 2024-06)，旨在處理雇主使用 AI 為招聘、晉升及其他就業決策造成偏見或歧視之問題。

通函提出的主要問題，為雇主可否於不遵守《公平信用報告法》(the Fair Credit Reporting Act, FCRA)規定之情況下，透過背景檔案、演算法評分及第三方消費者報告決定是否進行聘僱。關於用於就業目的之消費者報告，通函中指出，雇主如同借貸關係當中之貸款方，有可能以購買消費者報告方式，協助其作出是否進行對特定勞工的聘僱，尤其針對勞工背景有關之資料，檢視該勞工的公眾紀錄，包括是否有犯罪紀錄等。

而現今消費者報告機構或其他背景篩選事業，可向雇主或潛在雇主提供一系列之報告，包括勞工之活動、個人習慣、屬性及生物特徵等資訊之報告。例如，部分雇主透過第三方服務以監督所屬勞工之銷



本報告之智慧財產權歸屬於國發會

售互動情形，或追蹤員工之駕駛習慣、完成任務所需要之時間、發送訊息之數量或記錄其參與會議之數量與持續的時間、監督員工之網頁瀏覽、螢幕截圖及擊鍵頻率以計算員工之離線時間等。而某些情況下，消費者報告機構有可能將因提供上開第三方服務所得之資訊，販售予勞工目前或潛在之雇主。部分公司則可能協助分析勞工之相關數據，以提供雇主包括勞工生產力或風險之評估或評分報告，此類報告並可能被雇主用以自動作出與該工人薪酬相關之建議或決定、預測勞工之行為，或評估有無組成工會或離職之潛在可能性、或用以進行輪班或工作職責之安排、甚至用於警告或紀律處分。

國會通過 FCRA 以回應民眾對於事業蒐集消費者詳細資訊檔案，並將之出售的擔憂，其中包括此類信用報告可能對消費者就業權利之影響。以下為重點整理：

1. FCRA 消費者報告定義：

   消費者報告機構以書面、口頭或其他方式傳達之與消費者之信用價值、信用狀況、信用能力、品格、聲譽、個人特徵及生活模式相關之任何資料，並全部或部分被使用或預期會被使用或蒐集，以確認消費者符合某些目的（包含就業目的）之資格條件。

2. FCRA 對於消費者報告用於就業目的之額外要求：

   (1) 當消費者報告用於就業目的時，須獲得勞工許可。

   (2) 要求雇主於採取不利行動前及採取不利行動時，向勞工提供通知及報告副本。

   (3) 消費者報告機構須依勞工請求，揭露 2 年內出於就業目的使用消費者報告之任何人。



本報告之智慧財產權歸屬於國發會

(4) 消費者報告機構為就業目的呈報公眾記錄資料時，須遵循合理程序確保準確性。

3. FCRA 勞工保護：

(1) 勞工有權知悉消費者報告機構之消費者報告檔案內容，並得對不完整或不準確之資料提出異議。

(2) 消費者報告機構回應異議時，應更正或刪除不準確、不完整或無法核實之資料。

(3) 禁止報告過時之負面資料。

(4) 要求雇主於採取不利行動前及採取不利行動時，應向勞工提供通知。

(5) 嚴格限制消費者報告機構，僅得將消費者報告用於 FCRA 特定允許目的。

4. 審查依第三方消費者報告作出僱用決定之雇主是否受 FCRA 監管時，應考量：

(1) 雇主對消費者報告之資料使用是否出於「就業目的」

FCRA 將「就業目的」定義為用於評估消費者之就業、晉升、調職或留任之報告，適用於最初評估消費者就業性質之資料，以及用於持續就業目的（即晉升、調職或留任）之資料。

(2) 消費者報告是否來自「消費者報告機構」

依 FCRA 蒐集或評估消費者資料，為雇主提供報告用來協助為就業決策之第三方為「消費者報告機構」。



本報告之智慧財產權歸屬於國發會

於實體蒐集消費者資料訓練演算法，為雇主提供關於勞工分數或其他評估時，該實體得依「消費者報告機構」之含義，蒐集或評估消費者資料。

蒐集或評估資料若為消費者與製作報告人間之交易或經驗資料報告，依 FCRA 規定則非屬消費者報告之定義，故提供上述報告之第三人非「消費者報告機構」。

■ **資料來源：**


1. CFPB, Consumer Financial Protection Circular 2024-06, 2024-10-24, https://www.consumerfinance.gov/compliance/circulars/consumer-financial-protection-circular-2024-06-background-dossiers-and-algorithmic-scores-for-hiring-promotion-and-other-employment-decisions/ (last visited 2025/02/11)
2. Orrick, CFPB provides guidance on employer responsibilities and surveillance under the FCRA, 2024-11-01, https://infobytes.orrick.com/2024-11-01/cfpb-provides-guidance-employer-responsibilities-and-surveillance-under-fcra/ (2025-02-11)


### (二)2024 年 12 月美國平等就業機會委員會發布關於《工作場所中之穿戴式裝置：聯邦就業歧視法下穿戴技術之使用》之情況說明書

2024 年 12 月美國平等就業機會委員會(the U.S. Equal Employment Opportunity Commission, EEOC)發布《工作場所中之穿戴式裝置：聯邦就業歧視法下穿戴技術之使用》(Wearables in the Workplace：Using Wearable Technologies Under Federal Employment Discrimination Laws)之情況說明書，旨在為雇主於工作中要求員工配戴穿戴式設備以蒐集員工健康或生物特徵資訊等作為提供指導。「穿戴式科技」或「穿戴式裝置」為嵌入感測器(embedded with sensors)並佩戴於身上之數位設備，可追蹤身體運動、蒐集生物辨識資料及追蹤位置。現在於工作場所中



本報告之智慧財產權歸屬於國發會

使用穿戴式裝置越來越頻繁，例如：員工可能被要求穿戴智慧手錶、戒指等，而智慧眼鏡或智慧安全帽也可能用於偵測腦電波活動(electrical activity)，以追蹤並監控勞工於工作場所之位置、身體或精神狀況。

依據此說明書，《聯邦平等就業機會法》(the federal equal employment opportunity laws, EEO)於特定情況下亦適用於雇主要求員工使用穿戴式裝置之情形，提醒雇主進行此類要求，可能會涉及 EEO 合規性之問題。同時，EEO 並禁止雇主對特定員工因種族、膚色、國籍、宗教、性別、身心障礙、年齡及遺傳資料而為歧視。

雇主要求員工使用穿戴式裝置取得健康相關資料，可能使雇主、其代理人及其他適用 EEO 之實體產生以下法律遵循問題：

1. 使用穿戴式裝置蒐集資料(Collecting Information Using Wearables)

   雇主使用穿戴式裝置蒐集有關員工身體或精神狀況之資料或診斷測試(diagnostic testing)可能構成《美國身心障礙法》(the Americans with Disabilities Act, ADA)規定下之「健康檢查」(medical examinations)。包含：如果雇主指示員工在使用穿戴式裝置提供健康資料，也可能構成 ADA 中與身心障礙相關之詢問(disability-related inquiries)。

   ADA 嚴格限制雇主對員工為與身心障礙相關之詢問或健康檢查。除特定員工於工作相關且符合業務需求之情形，或依美國法典(42 United States Code)第 12112 (d)(4)(A)條規定，雇主須證明為達成工作目的之情形時得要求員工進行相關諮詢或健康檢查。依據美國法典第 12111(3)條規定，所謂工作相關且符合業務需求包含雇主自行評估有健康狀況之員工是否構成重大安全風險，且無法透過合理調整降低風險之情形。



本報告之智慧財產權歸屬於國發會

於少數有限之情形下，允許雇主對員工為與身心障礙相關之詢問或健康檢查，但仍有具體要求：

(1) 聯邦、安全相關法律或法規要求，例如：《職業安全與健康法》(the Occupational Safety and Health Act)。

(2) 擔任影響公共安全職務之員工，例如：消防員、警察。

(3) 雇主可為自願健康檢查，包含自願病歷紀錄，作為工作場所提供員工健康計畫之一部分，旨在合理地促進健康或預防疾病，依美國法典第 12112(d)(4)(B)條(42 USC § 12112(d)(4)(B))及聯邦法規第 1630.14(d)條(29 CFR § 1630.14(d))。

雇主從穿戴式裝置蒐集之醫療或身心障礙相關資料，須依 ADA 要求將資料保存於單獨之醫療文件，並將其視為機密醫療資料。

2. 使用穿戴式裝置之資料(Using Information from Wearables)

雇主使用穿戴式裝置蒐集資料時，須遵守 EEO 非歧視要求，禁止基於以下受保護特徵(protected characteristic)之就業歧視：種族、膚色、宗教、性別、國籍、年齡、身心障礙、或遺傳等資料。雇主使用穿戴式裝置產生之資料進行雇傭決策時，若此決策因上開受保護特徵而產生對員工之不利影響，即違反 EEO 規定。

例如，雇主透過以下方式使用穿戴式裝置產生之資料，違反 EEO 非歧視要求及違反 ADA 對醫療資料保密之要求：

(1) 使用心率、疲勞程度或體溫資料推斷員工懷孕，以此解僱該員工或違背其意願使其休無薪假。



本報告之智慧財產權歸屬於國發會

(2) 依賴穿戴式技術的數據，這些數據對於膚色較深的個體（種族或膚色）產生的結果不太準確，從而對這些員工做出不利的就業決策。

(3) 員工陪同親屬前往血液透析中心時，於午休時間追蹤員工，並詢問或研究前往之目的，進而蒐集員工家族病史及遺傳資料。

(4) 分析心率及皮膚溫度推斷或預測更年期，而後因性別、年齡或身心障礙而拒絕晉升員工。

雇主不得基於受保護之特徵選擇性地使用穿戴式裝置來監控員工，或對從事受保護活動之員工進行報復。例如僅要求西班牙裔員工使用蒐集健康資訊的穿戴式裝置，並基於西班牙裔員工的國籍對其進行差別待遇。

3. 與穿戴式裝置相關之合理調整(Reasonable Accommodation Related to Wearables)

於 ADA 允許雇主使用穿戴式裝置蒐集醫療資料之例外情形，雇主仍須對穿戴式裝置政策為例外處理。依民權法第 7 章(Title VII of the Civil Rights Act of 1964)禁止於僱傭、解僱及其他僱傭條款，因求職者之宗教信仰而為歧視、ADA 或懷孕員工平等法(Pregnant Workers Fairness Act)做出合理調整。例如，雇主遵守 ADA 於蒐集醫療資料之限制，如果員工穿戴裝置有違其宗教信仰，雇主須免除員工穿戴裝置之責任，或提供替代方案。

4. 最終提醒：

雇主應考量因素應包括：



本報告之智慧財產權歸屬於國發會

(1) 穿戴式裝置蒐集哪些資料，包含資料於不同保護基礎之準確性及有效性。

(2) 蒐集資料之儲存方式。

(3) 所蒐集之資料是否及如何用於與就業相關之決策，包含資料使用是否對不同保護基礎之員工產生不同影響。

■ **資料來源：**


1. U.S. Equal Employment Opportunity Commission, Wearables in the Workplace: Using Wearable Technologies Under Federal Employment Discrimination Laws, 2024-12-19, chrome-https://www.eeoc.gov/sites/default/files/2024-12/Wearables_Fact_Sheet_V10_%28002%29_508FINAL.pdf (last visited 2025/03/07)
2. JD SUPRA, EEOC Fact Sheet on Wearable Technologies Indicates Growing Concern Over Employee Monitoring, 2025-01-03 , https://www.jdsupra.com/legalnews/eeoc-fact-sheet-on-wearable-9625859/ (last visited 2025/01/07)


### (三)2024 年 12 月美國德州眾議員提出《德州負責任地人工智慧治理法案》

2024 年 12 月美國德州眾議員 Giovanni Capriglione 提出《德州負責任地人工智慧治理法案》(the Texas Responsible AI Governance Act, HB 1709)，當中包含德州雇主及其他部署者對「高風險 AI 系統」使用之規範。高風險 AI 系統包含作出或促成「重大決策」之 AI 工具，於就業領域用於聘僱、績效、薪資、紀律及解僱之決定。依據此法案，受規範之雇主及其他部署者須採取合理謹慎之措施，防止勞工受到已知或合理可預見之演算法歧視，包含撤回(withdraw)、停用及召回(recall)不合法之高風險 AI 系統。本法案於 2025 年 6 月經由立法機構通過後，



本報告之智慧財產權歸屬於國發會

提交至州長並經州長簽署通過，並將於 2026 年 1 月 1 日生效。以下為雇主及其他部署者應履行責任重點：

1. 即時暫停(Prompt Suspension)

高風險 AI 系統之部署者認為或有理由認為高風險 AI 系統不符此法案之規定時，應立即暫停使用該高風險 AI 系統，直至該系統符合此法案規定時。

2. 人工監督(Human Oversight)

高風險 AI 系統之部署者應指派具有足夠能力、訓練、權限及組織支援之人員，以監督使用高風險 AI 系統所做之重大決策。

3. 影響評估(Impact Assessments)

高風險 AI 系統之部署者應每半年完成高風險 AI 系統之影響評估，或於進行有意圖或實質性修改後 90 日內完成高風險 AI 系統之影響評估。

(1) 影響評估內容

高風險 AI 系統之部署者應每半年完成一次影響評估，並需於對高風險之 AI 系統進行任何有意圖或實質性修改後之 90 日內完成修改後之影響評估。影響評估至少須包括部署者合理已知或可獲得之範圍：

A. 部署者之聲明，揭露高風險 AI 系統之目的、預期用途、部署背景及提供之效益。

B. 分析高風險 AI 系統之部署是否會造成已知或可合理預見之演算法歧視風險，分析演算法歧視之性質，並採取降低風險之措施。



本報告之智慧財產權歸屬於國發會

C. 描述高風險 AI 系統輸入處理之資料類別，及高風險 AI 系統產生之輸出(outputs)。

D. 於部署者利用資料訓練高風險 AI 系統時，概述用於訓練高風險 AI 系統之資料類別。

E. 用於評估高風險 AI 系統之效能及已知可能之侷限之任何指標(metrics)。

F. 描述對高風險 AI 系統採取之任何透明措施，包含於向消費者揭露其正在使用高風險 AI 系統之任何措施。

G. 關於部署高風險 AI 系統提供後採行之監測(the post-deployment monitoring)及使用者保障措施(user safeguards)之說明，包含部署者為解決部署高風險 AI 系統所產生問題，而建立之監督、使用及學習程序。

H. 對於高風險 AI 系統所採取之網路安全措施及威脅模型之說明。

(2) 定期為 AI 工具評估(Regular AI Tool Assessments)

部署者應定期評估高風險 AI 系統，每年進行檢查，確保系統不會造成演算法歧視，並應保存最近完成之高風險 AI 系統影響評估及每次影響評估相關之所有記錄，並於高風險 AI 系統最終部署後至少保存 3 年。

4. 通報之要求(Reporting requirements)

部署者須於發現或知悉所部署之高風險 AI 系統造成或可能造成以下情形後 10 日內以書面通知委員會、檢察總長或監管部署業者之州主管機關之主管，及受影響之消費者：



本報告之智慧財產權歸屬於國發會

(1) 發生對個人或群體之演算法歧視。

(2) 作成不適當或歧視性之重大決策。

若開發者發現或知悉已部署之高風險 AI 系統之使用輸入(using inputs)或提供輸出(providing outputs)違反此法案規定，須停止違法系統運作，並於發現或知悉不可接受之風險 10 日內通知委員會及檢察總長。

此外，本法案另對數位服務提供者或社群媒體平臺有義務之規定，要求其必須盡商業合理之努力，防止服務或平臺上之廣告商於服務或平臺上佈署可能使得該服務或平臺使用者遭受演算法歧視之高風險 AI 系統。

■ **資料來源：**


1. Texas Legislature Online History, Bill: HB 1709, 2024-12-23, https://capitol.texas.gov/BillLookup/History.aspx?LegSess=89R&Bill=HB1709 (last visited 2025/01/22)

2. Texas Responsible AI Governance Act, 2024-12-23, https://www.mba.org/docs/default-source/policy/state-relations/draft_texas-ai_10.28.24.pdf?sfvrsn=9f83267e_1 (last visited 2025/01/22)


### (四)2025 年 1 月美國紐澤西州檢察總長辦公室及民權司發布《演算法歧視指引》

2025 年 1 月美國紐澤西州檢察總長辦公室(the New Jersey Office of the Attorney General)及民權司(the Division on Civil Rights, DCR)發布《演算法歧視指引》(Guidance on Algorithmic Discrimination)，旨在釐清《紐澤西州反歧視法》(New Jersey Law Against Discrimination, LAD)如何適用於因雇主、住房提供者、公共場所及 LAD 涵蓋之其他實體



本報告之智慧財產權歸屬於國發會

(entity)，於使用如 AI 等新興資料驅動技術(data-driven technologies)產生之演算法歧視。

該指引指出，近年來政府及事業使用自動決策工具做出重大決策，如人員聘僱或晉升、金融貸款及醫療服務等資格之決定，雖為受監管實體及公眾帶來潛在之益處，惟不負責任地設計及部署自動決策工具，將會導致演算法歧視之風險。此指引概述使用自動決策工具造成之演算法歧視風險、潛在益處及 LAD 對演算法歧視之保護措施，以下為重點說明：

1. 自動決策工具及演算法歧視：

(1) 自動決策工具

自動決策工具，指任何技術工具，包含但不限於軟體工具、系統或進程，用於促進人類決策程序全部或部分之自動決策。自動決策工具包含不同程度先進性及複雜性之技術，例如生成式 AI、機器學習模型、傳統統計工具及決策樹(decision trees)等。

自動決策工具得使用於各方面，包含協助雇主為聘僱、晉升及降職之決策；決定是否獲得租賃或購買房屋之資格等；亦可用於協助醫療服務提供者做出診斷、分配病患照護資源及決定所服用之藥物；執法機關用於識別嫌疑犯、車牌及選擇巡邏區域；法院用於預測某人是否再次犯罪及設定保釋或釋放之資格。

自動決策工具之開發及部署方式，可能會導致或減少歧視性結果。當實體未能解釋或修正自動決策工具之歧視時，會導致歧視性結果；反之若實體使用自動決策工具時考量到公平性，則會減少歧視性結果。故實體於使用自動



本報告之智慧財產權歸屬於國發會

決策工具時需審慎考量其潛在風險及使用自動決策之益處。

(2) 自動化決策工具如何造成歧視性結果

自動化決策工具之歧視性結果多源自於該工具之設計、訓練或部署方式，且有一定之共通性：

A. 設計：開發人員於設計自動決策工具時所為之選擇可能有意或無意地扭曲該工具，包含開發人員如何將真實世界之問題轉換成自動決策工具得分析之數值。有關自動決策工具提供之輸出、所使用之模型或演算法，以及輸入內容之評估決定，都可能為自動決策工具帶來偏見。

B. 訓練：自動決策工具須經過「訓練」才能使用。開發人員得創建新的資料集訓練自動決策工具，亦得改善及重新格式化已有之資料集。訓練資料可能反映出開發者本身之偏見，亦可能反映出制度與系統性之不平等。當訓練資料有偏差或不具代表性、缺乏多樣性、反映歷史偏見、與將要部署之工具內容不連貫、由其他自動決策工具人工生成(artificially generated)，或包含錯誤，則該工具可能會產生偏見。

C. 部署：部署自動決策工具，可能會因多種原因發生演算法歧視。於自動決策系統工具被用來做出決策而非用來評估時，其部署會擴大工具之偏見及工具外存在之系統性不公正(systemic inequities)。於某些情形，部署可能會揭露自動決策工具之偏見，以及導致反饋循環(feedback loop)。反饋循環係指具有偏見之自動決策工具所為之歧視性決策，又被引入該工具持續訓練，這個循環於每次迭代(iteration)都會加劇工具之偏見。



本報告之智慧財產權歸屬於國發會

2. LAD 禁止之演算法歧視：

LAD 禁止基於實際或認定之種族、宗教、膚色、國籍、性別、性取向、懷孕、哺乳、性別認同、性別表達、身心障礙及其他受保護特徵之演算法歧視。當雇主、住房提供者、公共場所或其他受規範實體使用自動決策工具時，若這些工具造成基於受保護特徵產生之不同待遇或影響，則違反 LAD 禁止之演算法歧視。自動決策工具排除或妨礙提供之合理調整，或為確保人們基於受保護特徵無障礙政策、程序或實體結構之修改，則違反 LAD 禁止之演算法歧視。

(1) 差別待遇歧視(Disparate Treatment Discrimination)

差別待遇歧視，係指實體因某人符合 LAD 受保護類型(protected class)之資格，而給予不同待遇之行為。

於實體設計或使用自動決策工具時，以不同方式對待受保護類型之人，即屬差別待遇歧視。若於實體選擇性地使用自動決策工具評估受保護類型之人時，可能導致差別待遇歧視，此外於自動決策工具無直接考量受保護特徵，但依受保護特徵之近似代理變數[6](close proxy)提出建議，實體使用該工具亦可能導致差別待遇歧視。

(2) 差別影響歧視(Disparate Impact Discrimination)

差別影響歧視，係指自動決策工具無明確依據受保護特徵對人們進行不同評估，並且該工具之使用對受 LAD 保護類型之人造成不成比例(disproportionately)之負面影響。

[6] 近似代理變數(close proxy)係指與敏感資料高度相關但表面上中性之資料，如郵遞區號、學歷等，即使模型未明確使用受保護資料亦可透過近似代理變數進行間接推論，而導致間接歧視。



本報告之智慧財產權歸屬於國發會

LAD 禁止政策或實務作為以非法方式對受 LAD 保護群體產生不成比例之影響，除非該政策及實務作為是為達成實質、合法及非歧視性之利益所必要，且無其他歧視性較低之替代方案能達成相同之利益。

LAD 禁止自動化決策工具提出之建議或促成之決策不成比例地傷害受 LAD 保護群體，而形成差異影響歧視。除非使用該工具是為達成實質、合法及非歧視性之利益，並且須評估是否有其他歧視程度較低之替代方案。

(3) 合理調整(Reasonable Accommodations)

如果自動決策工具之使用排除或妨礙提供合理調整，則可能違反 LAD 禁止之演算法歧視，包含未依某人之身心障礙、宗教、懷孕或哺乳等法律保護特徵而提供合理之調整。因此 LAD 要求實體因某人屬於受保護群體而提供合理調整，該合理調整須為該實體知道或應該知道之必要調整，且不會對該實體造成過度之困難。

合理調整可能為自動決策工具建議之因素，而自動決策工具之建議可能造成差別影響歧視，於自動決策工具未使用包含調整措施之個人資料進行訓練時，則該工具可能沒有識別調整措施之可能性，或可能懲罰擁有或需要合理調整之個人。

(4) LAD 實體之責任

雇主、住房提供者、公共場所及其他實體，須對任何導致違反 LAD 歧視之政策或實務負責。雖然實體使用之自動決策工具，可能主要或完全係依賴第三方開發者建立或執行，但實體使用該自動決策工具造成之演算法歧視，



本報告之智慧財產權歸屬於國發會

不因該工具係由第三方開發，或實體不清楚該工具之內部運作，而得免除責任。

雇主、住房提供者、公共住宿場所及其他實體，以及實體所使用之自動決策工具的開發商及供應商，須於部署自動決策工具前，考量及評估該工具之設計及測試，並於部署後持續分析及評估該工具，以降低產生歧視性結果之風險，從而降低違反 LAD 規定之風險。

■ **資料來源：**


1. Matthew J. Platkin Attorney General, Attorney General Platkin and Division on Civil Rights Announce New Guidance on Algorithmic Discrimination, Creation of Civil Rights Innovation Lab, 2025-01-09, https://www.njoag.gov/attorney-general-platkin-and-division-on-civil-rights-announce-new-guidance-on-algorithmic-discrimination-creation-of-civil-rights-innovation-lab/ (last visited 2025/03/13)
2. Guidance on Algorithmic Discrimination and the New Jersey Law Against Discrimination, 2025-01-09, https://www.nj.gov/oag/newsreleases25/2025-0108_DCR-Guidance-on-Algorithmic-Discrimination.pdf (last visited 2025/03/13)


### (五)2025 年 2 月美國加州民權理事會發布第二次修改《關於自動決策系統之擬議就業法規》

2025 年 2 月美國加州民權理事會(The California Civil Rights Council)發布第二次修改之《關於自動決策系統之擬議就業法規》(Second Round to Initial Text of Proposed Modifications to Employment Regulations Regarding Automated-Decision Systems)，旨在解決企業於使用 AI 為就業決策時，基於受保護之特徵可能產生的就業歧視問題。

企業使用 AI 提升工作效率之方式，包含開發自動決策系統以協助招聘及晉升評估之流程，對於使用自動決策系統為人事決策之雇主



本報告之智慧財產權歸屬於國發會

或其他適用實體，即任何僱主、職業仲介、勞工組織或實習培訓計畫，並受此法拘束之主體，須注意以下規範變更：

1. 代理人(Agent)之新定義擴增至直接或間接代表雇主行事之任何人，行使傳統上由雇主行使之職能或其他受《加州公平就業及住宅法》(California’s Fair Employment and Housing Act, FEHA)監管之活動，包含招聘、申請人篩選、聘僱、晉升或有關薪酬、福利及休假之決定，全部或部分使用自動化決策系統進行之情形。

2. 雇主或其他適用實體使用自動化決策系統為人事決策時，應負較高之舉證責任，證明其已執行反偏見測試(anti-bias testing)或類似之積極措施以防止非法歧視。缺乏證據之主張，得用於指控雇主或其他適用實體無法證明其有進行避免歧視而實施具體措施之作為，證據可包括相關措施之品質、效力、近期性(recency)及範圍，此類測試或其他措施之結果，以及對這些結果之回應。

3. 紀錄保存係指於雇主或其他適用實體處理聘僱實務時，製作或接收任何人事或其他聘僱紀錄，影響求職者或員工之就業福利，應由雇主或其他適用實體自紀錄製作之日或涉及人事活動發生之日起，保存至少 4 年。紀錄包含求職申請、人事紀錄、會員紀錄、就業推薦紀錄、篩選標準、自動決策系統資料，以及雇主或其他適用實體製作或接收之任何影響申請人或雇員福利之其他記錄。

4. 雇主或其他適用實體使用自動決策系統為就業決策，例如分析申請人之語音語調、面部表情或其他身體特徵或行為，可能造成歧視具有身心障礙或受法律保護特徵之個人，為避免違反就業歧視，雇主或其他適用實體須依本法第二章就業歧



本報告之智慧財產權歸屬於國發會

視第 8 條（宗教信仰歧視）及第 9 條（身心障礙歧視）之規定，為申請人提供合理調整。

5. 雇主或其他適用實體使用自動決策系統為人事決策時，使用之標準、測試及其他篩選標準，須確保與工作職位相關及符合業務需要，並且無歧視性之標準、測試或其他篩選標準能有效達到雇主之目標。

此次修改擬議就業法規，公眾意見徵集截止至 2025 年 2 月 24 日。加州民權委員會於同年 3 月 21 日通過此次修改擬議法規，並於同年 6 月已經批准，10 月生效。

■ **資料來源：**


1. Civil Rights Council, Second Round to Initial Text of Proposed Modifications to Employment Regulations Regarding Automated-Decision Systems, 2025-02-07, https://www.callaborlaw.com/_images/blog_files/Second_Modifications_to_Proposed_Modifications_to_Employment_Regulations_Regarding_Automated-Decision_Systems.pdf (last visited 2022/02/27)

2. California Labor & Employment Law Blog, New Proposed Regulations Will Impact How Businesses Utilize AI to Make Personnel Decisions, 2025-02-13, https://www.callaborlaw.com/entry/new-proposed-regulations-will-impact-how-businesses-utilize-ai-to-make-personnel-decisions (last visited 2022/02/27)

3. Civil Rights Council, Final Unmodified Text of Proposed Employment Regulations Regarding Automated-Decision Systems, 2025-03-17, https://calcivilrights.ca.gov/wp-content/uploads/sites/32/2025/03/Attachment-B-Final-Unmodified-Text-of-Proposed-Employment-Regulations-Regarding-Automated-Decision-Systems.pdf (last visited 2025/04/14)




本報告之智慧財產權歸屬於國發會

(六)2025 年 4 月美國加州參議員提出《自動決策安全法案》

2025 年 4 月美國加州參議員修改《自動決策安全法案》(Automated Decisions Safety Act, AB1018)重新提交至委員會，旨在嚴格監管開發及部署可做出或促成重大決策之自動決策系統 (automated decision systems, ADS)，防止系統所為之重大決策於工作場所及其他地方造成歧視。此法案要求 AI 開發者、部署者應遵守相關義務，包含對涵蓋之 ADS 進行性能評估(performance evaluation)、第三方稽核，以及對影響就業、醫療保健、住房及其他領域之 AI 驅動決策主體為透明度之要求。

以下為法案之重點說明：

1. 名詞解釋

(1) 「自動決策系統」，指從機器學習、統計模型、資料分析或 AI 中之計算程序，該程序得用於發佈簡化輸出，包含分數、分類或建議，用以協助或取代人類之自主決策，可能對自然人產生重大影響。自動決策系統並非指垃圾郵件過濾器、防火牆、防毒軟體、身分與近用管理工具、計算機、資料庫、資料集或其他資料之匯集。

(2) 「實質影響個人權益之決策」(Consequential decision)，指對自然人所為之決策，可能對下列任一事項之成本、條件、品質或近用性產生重大影響：

A. 與就業相關之決定，係指雇主直接或透過第三方做成影響工資、福利、其他報酬、工時、工作時間表、績效評估、招聘、紀律、晉升、解僱、工作任務及職責、工作分配、培訓機會、生產力要求、工作場所之健康及安全或其他就業條款或條件之決定。



本報告之智慧財產權歸屬於國發會

B. 與教育及職業訓練相關，包含評量分班、作弊或抄襲之發現、認證、證書發放、錄取及入學、紀律處分經濟援助及獎學金、考試監督等。

C. 與住房及住宿(Housing and lodging)相關，包含租賃或短期住房及住宿、房屋估價、租金補貼、公共支持之住房(publicly supported housing)等。

D. 必要之公用設施，包含水、電、熱能、交通運輸、城市垃圾及汙水處理服務等。

E. 計劃生育、收養服務、生殖服務以及與兒童保護服務相關之評估。

F. 醫療保健及健康保險，包含心理健康照護(mental health care)、牙科及視力。

G. 金融服務，包含抵押貸款公司、經紀人或債權人提供之金融服務。

H. 關於審前釋放、量刑及有期徒刑替代措施之刑事司法制度。

I. 法律服務。

J. 私人仲裁。

K. 調解。

L. 與選舉相關，包含投票、劃分選區以及選舉管理等。

M. 獲得政府福利或服務，或被政府實體處以罰緩。

N. 《民法典》(the Civil Code)定義之公共場所。

O. 保險。



本報告之智慧財產權歸屬於國發會

P. 網路及電信接取。

(3) 「ADS 之範圍」，指設計或使用 ADS 做出或促成重大決策。

(4) 「部署者」，指直接或透過與第三方簽訂契約，使用涵蓋 ADS 做出或促成重大決策之個人、合夥企業、州或地方政府機構、公司或開發商。

(5) 「開發者」，指透過設計、編碼、實質修改或以其他方式產生自動決策系統（直接或透過與第三方簽訂契約達成以設計、編碼、大幅修改或其他之方式製作用於做出或促進重大決策）之個人、合夥企業、州或地方政府機構、公司或部署者。

2. ADS 之開發者義務

(1) 應依據其部署期間對 ADS 為性能評估。對於 2026 年 1 月 1 日前首次部署或潛在部署之 ADS，及使用 ADS 之開發者應於 2027 年 1 月 1 日前對 ADS 進行初步效能評估。並於以下情形進行額外效能評估：開發商對 ADS 進行實質性修改後、對所承包 ADS 進行微調而實質上改變該 ADS 之用途或輸出，以及於開發商前次對 ADS 進行性能評估後不超過一年即將 ADS 進行部署或提供予潛在部署者。而對於 2026 年 1 月 1 日後部署或潛在部署 ADS 之開發者亦須於相同情形下對該 ADS 進行效能評估。

(2) 開發商於進行性能評估時，須與獨立第三方稽核員簽訂契約，評估開發者是否遵守本法案之規定。

(3) 向潛在部署者出售、授權或以其他方式轉讓 ADS，應向部署者提供相關內容，包含最新性能評估之結果、說明應如



本報告之智慧財產權歸屬於國發會

何做出或促進重大決策，以及說明於何種情形應對 ADS 進行微調等內容。

(4) 從適用之 ADS 稽核員接受影響評估之開發者，應向 ADS 之部署者提供資料，包含 ADS 之預期準確度與實際觀測準確度間之任何重大差異，這些差異可能發生之部署條件，以及解釋部署者得採取何種措施緩解差異等資料。

(5) 開發者接收稽核員回饋後應考量並嘗試將該回饋納入 ADS 後續開發。

(6) 須保留未經編輯之相關文件 10 年，包含稽核結果及性能評估等。

3. ADS 之部署者義務

(1) 於做出或促成重大決策前，應向該決策之任何主體提供簡單易懂之書面揭露聲明，告知當事人將使用 ADS 做出或促進重大決策。

(2) 於做出或促成重大決策前，應向該決策之任何主體提供合理之機會，選擇退出使用 ADS。

(3) 於做出或促成一項重大決策後，應於 5 日內向該決策之主體提供簡單易懂之書面揭露，包含 ADS 於最終決策中扮演之角色、是否涉及任何人為判斷，以及最終決策結果可能產生不成比例之影響的關鍵參數等資訊。

(4) 涵蓋 ADS 做出或促成重大決策後，應向該決策之任何主體提供於 30 日內，得更正做出或促進重大決策使用之任何不正確之個人資料，以及對重大決策之結果提出上訴。

(5) 對重大決策主體之個人資料為蒐集、利用、保留及共享應合理必要且符合目的，須以實現蒐集及處理個人資料之目



本報告之智慧財產權歸屬於國發會

的，或用於與蒐集個人資料背景相符之其他目的，且不得以不符合目的之方式進一步處理資料。

(6) 使用涵蓋 ADS 做出或促進於 3 年內直接影響超過 5999 人之重大決策之部署者，應與獨立之第三方稽核師簽訂契約，每 3 年對涵蓋 ADS 進行影響評估。

(7) 須保留未經編輯之相關文件 10 年，包含從開發商收到之任何文件及選擇不使用本法所涵蓋的 ADS 之請求等。

(8) 使用涵蓋 ADS 做出或促進重大決策之部署者，應指定至少 1 名員工負責監督部署者是否符合本法規範。

(9) 受《2018 年加州消費者隱私法》(the California Consumer Privacy Act of 2018)約束之企業部署者亦須遵守相關隱私規定。

4. 受涵蓋 ADS 之稽核員義務

(1) 向涵蓋 ADS 之部署者索取進行影響評估合理需要之任何資料，僅適用於部署者於正常業務過程所蒐集之資料。

(2) 對涵蓋 ADS 進行影響評估後，稽核師應向與其簽訂契約為影響評估之部署者提供影響評估結果，以及於稽核機構網站免費公開影響評估結果之總結摘要(high-level summary)，供使用者查閱。

5. 檢察總長、檢察官、民權部以及僅負責與就業相關之決定之勞工專員等公共實體，得對違反本法案之開發者、部署者或審計師，提起民事訴訟救濟。

■ **資料來源：**

1. LEGISCAN, California Assembly Bill 1018, 2025-02-20, https://legiscan.com/CA/text/AB1018/2025 (last visited 2025/04/10)



本報告之智慧財產權歸屬於國發會

2. JD SUPRA, California Introduces Another AI Anti-Discrimination Bill: What Employers Need to Know , 2025-03-04, https://www.jdsupra.com/legalnews/california-introduces-another-ai-anti-8080739/ (last visited 2025/04/10)

(七)2025 年 10 月加州州長否決《就業用自動決策系統法案》

加州州長 Gavin Newsom 於 2025 年 10 月 13 日以限制過廣等原因，正式否決《就業用自動決策系統法案》（Employment: Automated Decision Systems，下稱 SB7 法案），俗稱「禁止機器人老闆法案」（No Robo Bosses Act）。最早於 2024 年 12 月由參議員 Jerry McNerney 提出，旨在針對雇主在職場使用「自動決策系統」（Automated Decision Systems, ADS）進行規範，建立「預先通知、人類覆核、資料存取與更正、反報復與罰則」等整套治理機制，避免 AI/演算法成為解僱、停職或懲處之唯一裁判標準。然州長在否決書中指出，法案對通知義務與使用限制之適用過廣，連最常見、低風險之日常數位工具亦可能被納入，可能過度影響民眾生活；此外，部分議題已由加州隱私保護局(California Privacy Protection Agency, CPPA)即將推出之規則涵蓋重疊，應先評估其效果，再考慮另立新法。

1. 法案重點內容如下

SB7 法案預計對《加州勞動法典》(California Labor Code)進行修訂，針對雇主在職場使用 ADS 工具之前置義務、禁止事項、重大決策人類核准以及員工資料權與救濟方式等，建立完整 AI 用於就業、職場決策之專章。

(1) 第一章 定義

SB7 法案首先對 AI、雇主、勞工等基礎詞語進行定義，其將 ADS 定義為：任何透過機器學習、統計模型或其他資料分析流程所產出之數值、分類、建議、資訊、假設、



本報告之智慧財產權歸屬於國發會

預測等，用以輔助或取代自然人裁量、並對自然人產生實質影響之系統。其亦將「預測行為分析」定義為任何能夠預測或推斷勞工之行為、信念、意圖、個性、情緒狀態或其他特徵或行為之系統或工具；並將「雇用相關決定」定義為雇主所做的任何影響工資、工資設定、福利、報酬、工時等廣大要件之決定。

(2) 第二章 ADS 系統「使用前通知」(Pre-Use Notice)

此章節規定，雇主若在職場上以 ADS 作為招聘以外之就業相關決策用途時，須向直接或間接向受影響之勞工提供書面之「使用前通知」，包含解釋 ADS 系統用途、用於輸入資料之類型與來源、可能產生重大影響之參數；資料之存取、更正權等。雇主亦必須準備、維護「現行使用中之 ADS 清單」，法案中未說明清單功能，然可合理推測應為資訊揭露或審查用途。若法案生效前雇主已開始使用 ADS，則應於 2026 年 4 月 1 日前向員工完成通知；新部署之 ADS 系統，則須於新部署前至少 30 天通知；若有新員工任職，亦應於到職後 30 天內對其通知 ADS 之使用。使用前通知須以簡明易懂之語言書寫，並以獨立、簡便之方式提供。

(3) 第三章 限制與禁止

根據此章節，法案禁止雇主利用 ADS 來推斷受保護身分(protected status)，如種族、性別、國籍等 ，亦不得對行使合法權利之勞工採取違反聯邦法、州法等勞動法規之識別、分析、預測等不利行為。雇主不得依賴顧客評價作為 ADS 系統進行解僱、降職或懲處之唯一或主要標準；並重申不得違反既有勞工、健康與安全、平權等法律。勞工有權向雇主要求近 12 個月內用於 ADS 雇用決策之資



本報告之智慧財產權歸屬於國發會

料，同時具有 12 個月內得申請該類資料一次之限制，該類資料提供時應以匿名形式呈現。若雇主依 ADS 產生之結果對員工作出紀律處分甚至解雇裁定時，必須有對該 ADS 結果進行人工審查，包含對主管評價、人事檔案、工作成果、同儕評價與客戶評論等進行審核。

(4) 使用後(Post-Use)通知

此章節規定，凡雇主主要依賴 ADS 對員工作出懲處或停職之決定時，應在通知該員工該項決定之同時，向受影響員工提供書面通知。該通知必須以簡明易懂之語言撰寫，並應為獨立文件或訊息，不得與其他公司通訊或文件合併。通知內容須以員工平時接收例行工作資訊所使用的語言提供(如英語)，且應以簡便方式傳達，例如電子郵件、超連結或其他書面格式。

通知內容應包含可聯絡之自然人窗口，供受影響員工就該決定進一步詢問與取得相關資料；通知亦應明確說明雇主在對該員工作出一項或多項懲處、解僱或停權決定時，曾使用 ADS 作為輔助工具。通知應明確告知員工有要求取得自動決策系統所使用之個人資料副本之權利，以及應明確聲明雇主依法禁止因員工行使本章及本法所規定之權利，如資料請求、查詢或申訴等，而對其進行任何形式的報復行為。

(5) 第五章 工作者資料的存取與更正

本章重申反報復條款，即雇主不得因員工行使或嘗試行使本法所保障的權利，而對其採取不利行為；任何員工若因使用或嘗試使用本法賦予的權利、向勞動相關單位提出投訴，指控雇主違反本法時，若因此遭解僱、威脅解僱、



本報告之智慧財產權歸屬於國發會

降職或受到任何形式的歧視與報復，皆屬違法。員工基於協助他人主張本法權利之行為，亦應受同等保護。

本法由加州勞動相關單位負責執行，該類機關得主動或依投訴進行調查，並可採取必要之臨時救濟措施，以防止損害擴大，直至調查或聽證程序結束為止。相關單位可依現行勞動法程序對違法雇主進行裁罰，並得提起民事訴訟。裁罰與執行程序，依既有勞動法規定辦理。除勞動相關單位外，檢察官亦可依相關章節規定對違法行為提起訴訟。

州高等法院審理的任何民事案件中，無論案件發生地或被告雇主事業經營地點，原告均得請求法院頒布禁制令控制損害，並可要求懲罰性損害賠償及合理之律師費、訴訟費用。凡違反本法之雇主，均應處以 500 美元之民事罰鍰。

若雇主已遵守本法關於自動決策系統就業通知的要求，則無須重複遵守其他州法律中內容實質相同的通知規定。但若雇主屬於《加州消費者隱私法》（CCPA）所規範的事業，仍必須遵守加州隱私保護機構依 CCPA 所制定的與 ADS 相關的隱私規範。

此章節後段給予些許豁免條件；若雇主與勞工之間存在合法有效的集體談判協議，且該協議以明確無歧義的方式放棄本法的適用，同時明定工資、工作條件及其他勞動條件，並提供防止演算法式管理的具體保障，則該協議所涵蓋的當事人得免於本法適用。

最後，本法案不得被解釋為限制或禁止任何雇主遵守聯邦政府所規定的法規或合約義務。在雇主提供產品或服



本報告之智慧財產權歸屬於國發會

務予聯邦政府時，如依規定需遵守特定的管理或資訊要求，仍應以聯邦法規範為優先。

2. 加州州長否決之理由

雖然草案內容應可提供加州勞工更多保障，根據 2025 年 10 月 13 日州長辦公室對參議院的正式否決函，州長雖認可 ADS 系統若未妥善控管，將對勞工權益造成損害，然仍提出以下主要反對理由：

(1) 未針對濫用實例對症下藥

州長認為草案並未具焦真正具風險之 ADS 使用情境，連最無害(innocuous)的工具亦被涵蓋，無助於直接處理真正具風險之濫用事件。

(2) 限制過廣

草案對雇主如何使用 ADS 工具過廣，如禁止以顧客評價作為主要輸入參數，然顧客評價可能為辨識高績效員工之可靠依據，若擔憂評價被不當使用，立法應針對該情境修正，而非全面禁止。

(3) 與既有、或將有之規範重疊

根據否決書，部分情境已被加州隱私保護機構（CPPA）現有或即將發布之法令、規則涵蓋，而此類規則亦可令勞工更了解個資如何被 ADS 系統使用，故通過 SB7 草案前應先評估上述規則之有效性，避免重複或矛盾之監管框架，徒增企業合規成本而未有相稱效益。

綜上，州長認為 SB7 草案仍有風險聚焦不足、限制過廣且監管重疊的疑慮，故否決該草案。



本報告之智慧財產權歸屬於國發會

■ **資料來源：**

1. California State Legislature, SB-7 Employment: automated decision systems, 2025-09-17, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260SB7 (last visited 2025/12/08)

2. Office of the Governor, State of California, Veto Message for SB 7 (Employment: Automated Decision Systems), 2025-10-13, https://www.gov.ca.gov/wp-content/uploads/2025/10/SB-7-Veto.pdf (last visited 2025/12/08)

# 肆、 AI 與個人資料保護及監管相關議題

## 一、 美國

### (一)2024 年 11 月美國加州隱私保護局發布關於《加州消費者隱私法》更新、網路安全審查、風險評估、自動決策技術及保險公司之監管規則之修正提案

2024 年 11 月美國加州隱私保護局( the California Privacy Protection Agency, CPPA )發布關於《加州消費者隱私法》( the California Consumer Privacy Act, CCPA ）更新、網路安全審查(Cybersecurity Audits)、風險評估(Risk Assessments)、自動決策技術（Automated Decision-making Technology, ADMT ）及保險公司監管之修正提案(Proposed Regulations)。旨在修訂現行 CCPA，促使事業落實年度網路安全審查與風險評估；於事業使用 ADMT 時，並須落實消費者近用與選擇退出之權利；同時，敘明保險公司須遵守 CCPA 規定之時機。

以下為此修正提案之核心重點：

1. 網路安全審查

(1) 須為網路安全審查事業之要件：



本報告之智慧財產權歸屬於國發會

A. 事業有 50%或以上年度營收來自出售或分享加州消費者之個人資料或將其提供第三方用於跨境行為廣告(Behavioral advertising)。

B. 經 CPPA 調整後，事業年度營收超過 2500 萬美元，且於前一年度達到下列門檻者：

a. 處理至少 25 萬名或以上之消費者或家庭之個人資料；或

b. 處理至少 5 萬名或以上加州消費者之敏感個人資料。

(2) 網路安全審查要求：

A. 使用符合資格、具客觀性及獨立性之審查人員並使用審查專業普遍接受之程序及標準。事業須提供指引以維護審查人員之獨立性。

B. 事業須闡明審查範圍及標準。

C. 審查時須包含審查人員之姓名、從屬關係、相關資格，以及所有審查人員之聲明，證明其獨立性及客觀性。審查報告須包含一份審查人員簽署之聲明，並呈交至事業董事會、管理機構(governing body)或負責網路安全程序之最高主管。審查人員須保留網路安全審查相關文件至少 5 年。

D. 網路安全審查內容須包含辨識、評估及記錄事業網路安全程序如何保護個人資料，避免未經授權之使用、事業網路安全程序之 18 個組成部分，例如：驗證、個人資料之加密及帳戶管理與近用控制等，以及事業採取之保障措施如何提供最低程度之安全性。

(3) 提交網路安全審查：



本報告之智慧財產權歸屬於國發會

事業須每年向 CPPA 提交網路安全審查書面證明，註明審查所涵蓋之 12 個月份，並由負責監督事業網路安全審查法律遵循(compliance)之事業董事會、管理機構或最高層級主管人員簽署。同時包含一份聲明，證明簽署人已審閱並瞭解網路安全審查結果。

2. 風險評估

(1) 擬議規定要求事業若會以「對消費者隱私造成重大風險」的方式處理個人資料，須於實施之前進行風險評估，重大風險行為可能包括：

A. 出售或分享個人資料。

B. 處理敏感個人資料。

C. 使用 ADMT 為與消費者相關之重大決策或個人資料分析。

D. 使用或訓練 ADMT 或 AI(train ADMT or AI)處理個人資料。

(2) 風險評估，旨在判斷特定個人資料處理活動對消費者隱私權侵害之風險是否大於效益，以下為事業進行風險評估需涵蓋之內容：

A. 處理個人資料之具體目的。

B. 識別待處理個人資料之類別，確認其是否包含敏感個人資料，及為維持 ADMT 或 AI 處理個人資料之品質所採取之行動。



本報告之智慧財產權歸屬於國發會

C. 確認處理個人資料之要素，例如：計畫之處理方法及個人資料來源、消費者與事業間之關係、向消費者為相關揭露與揭露方式等。

D. 具體指出處理個人資料對事業、消費者、其他利害關係人及公眾帶來之利益。若事業得因處理個人資料而獲得金錢收益，則事業須識別該利益並於可行之情形下估算預期獲利。

E. 識別處理個人資料對消費者隱私權造成之負面影響，並了解造成負面影響之原因。

F. 對已識別之負面影響須訂定計畫已實施保障措施。保障措施須具體說明將如何解決負面影響及得消除或減少負面影響之程度。於使用 ADMT 之情形下，事業須確認是否對使用 ADMT 進行評估，且事業若是自第三方取得 ADMT，須識別該第三方是對 ADMT 之評估及是否有相關要求或限制，並已實施準確性及非歧視之保障措施。

G. 確認是否觸發風險評估之處理程序。

H. 事業提供 ADMT 或 AI 於其他事業使用時，須提供所有必要事實，協助接收事業為風險評估，並以簡單易懂之語言說明 ADMT 或 AI 技術相關之要求或限制。

I. 於觸發風險評估程序前進行風險評估並記錄，並至少每三年檢閱一次。處理程序有重大變更時，應立即更新風險評估。於程序持續期間或完成風險評估後五年內保留風險評估。

(3) 提交風險評估：



本報告之智慧財產權歸屬於國發會

擬議法規若通過生效，事業須自生效之日起 24 個月內向 CPPA 提交風險評估資料，資料須包含：負責監督公司風險評估法律遵循之最高層級主管簽署之證明、CPPA 提供之風險評估表格、風險評估之完整版本。受監管事業須每年提交上述風險評估資料，並於 CPPA 或州檢察總長提出要求後 10 日內提供完整之風險評估資料。

3. ADMT

(1) 事業於以下情形時，適用擬議 ADMT 規則之要求：

A. 使用 ADMT 作出「重大決策」，包括使用這些技術實質地促進有關招聘、工作分配、薪酬、降職、停職和解僱的決策。

B. 使用 ADMT 對消費者進行廣泛分析 (extensive profiling of a consumer)，包括使用自動處理透過廣泛觀察收集的數據來分析或預測申請人、員工及獨立承包商的特徵。

C. 使用個人資料訓練 ADMT(training uses of ADMT)。

(2) 修正提案對使用 ADMT 事業之要求：

A. 於使用前通知個人隱私權政策，通知須包括使用 ADMT 之目的、以簡潔易懂之語言說明 ADMT 之運作方式、提交選擇退出權與近用權之請求及禁止事業對行使 CCPA 權利之個人進行報復。

B. 提供個人選擇退出之權利及例外情況。擬議的法規賦予加州居民選擇退出 ADMT 所涵蓋之相關用途的權利。但也提供四項退出 ADMT 之例外情況，包括：



本報告之智慧財產權歸屬於國發會

a. 若該 ADMT 之採用為招聘、工作分配、薪酬、晉升、降職、停職或解雇之重大決策有關，而雇主於此類決策提供受影響之個人有就決策結果申訴(overturn)之權利，且處理該申訴之人員有權推翻 ADMT 之決策時，例外無須賦予退出權。

b. 若 ADMT 僅係用於安全、防詐欺或安全目的之例外，且為達成該安全目的所必要時。

c. 運用於重大決策之例外，包括事業無法選擇不使用 ADMT 為招募、分配、工作指派或薪酬之決策時，但僅限於採用 ADMT 為實現上述目的所必須並僅用於上述目的之用途。

d. 運用於工作分析之例外，當 ADMT 僅被用於評估工作能力或表現而為實現該目標所必需時，則例外不適用選擇退出機制。然而，若該評估為評估晉升、降職、停職或解雇之決定（非前述招募、分配、工作指派或薪酬）的關鍵因素，則仍需適用選擇退出權利規定。

C. 提供近用 ADMT 之權利(right to access ADMT)

加州居民有權向事業提出近用 ADMT 之要求，亦即透過請求近用取得 ADMT 利用於那些與個人相關決策等涵蓋用途之資訊。經事業驗證請求權人之身分後須告知驗證身分結果、拒絕近用請求之理由、請求部分拒絕時，揭露其他請求之資料、並於提供個人近用、檢視或接收其要求資料之可攜複本時採用合理的安全措施。

事業使用 ADMT 為不利個人之重大決策時，應於決策之日起 15 日內，通知個人得近用 ADMT 決策



本報告之智慧財產權歸屬於國發會

之權利。包含與個人相關之重大決策、禁止事業對行使 CCPA 權利之個人進行報復、個人有近用權及行使近用權方式，以及消費者得提出申訴與申訴之方式。

4. 保險公司之監管規則

依據《加州保險法》(California Insurance Code)新增「保險公司」之定義。闡明符合 CCPA「事業」定義之保險公司，於蒐集、使用、處理或保留不受《加州保險法》拘束之個人資料時，應遵守 CCPA 之規定。為區隔並劃分 CCPA 與《加州保險法》兩法律架構之管轄範圍重疊之界線，修正提案闡明保險公司得評估於《加州保險法》不適用之情形下，CCPA 應如何適用。

此修正提案徵求公眾評論，截止日為 2025 年 1 月 14 日。

■ **資料來源：**


1. California Privacy Protection Agency, Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies, 2024-11-08, https://cppa.ca.gov/regulations/ccpa_updates.html (last visited 2024/12/11)

2. California Privacy Protection Agency, Notice of Proposed Rulemaking, 2024-11-22, https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_notice.pdf (last visited 2024/12/11)

3. California Privacy Protection Agency, Text of Proposed Regulation, 2024-11-22, https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_text.pdf (last visited 2024/12/11)




本報告之智慧財產權歸屬於國發會

## (二)2025 年 4 月 22 日美國聯邦貿易委員會發布《聯邦兒童線上隱私權保護法》修訂版

於 2025 年 4 月 22 日，美國聯邦貿易委員會(Federal Trade Commission，FTC)依據《聯邦兒童線上隱私權保護法》(Children's Online Privacy Protection Act, COPPA)修訂《兒童線上隱私保護規則》(Children's Online Privacy Protection Rule，下稱 COPPA 規則)，本次 COPPA 規則之修訂目的是為應對技術及網路實踐之變化，加強對兒童個人資料之保護。同時釐清 2013 年修訂以來之內容。更新後之規則將於 2025 年 6 月 23 日生效。

以下為此法修訂之重點整理：

1. 修訂背景

COPPA 於 1998 年通過，旨在保護 13 歲以下兒童(下稱兒童)之線上個人隱私安全，該法規範對兒童個資之線上蒐集、利用及保護。1999 年，FTC 頒布 COPPA 規則，以實際落實 COPPA。COPPA 規則中，要求蒐集兒童個資之網站或線上服務營運商於蒐集、利用或揭露兒童個資前，須直接或線上通知家長，並取得家長同意。此外，線上服務營運商須提供家長透明之資訊揭露並設立資料保留級刪除政策。然而隨著網路與科技之快速演進。為因應技術變化，2019 年 FTC 啟動對 COPPA 規則之檢視，並徵求公眾意見，並於 2024 針對公眾意見稿進行審核。

2. 主要修訂與新增內容

(1) 定義

A. 混合受眾網站或線上服務：



本報告之智慧財產權歸屬於國發會

COPPA 規則於本次修訂增加「混合受眾網站或線上服務」之定義，目的是為提供混合受眾網站及服務營運商於判斷兒童身分時能採取之方式。修訂之規則中，混合受眾網站或線上服務係指「雖針對兒童，但不以兒童為主要受眾，且於蒐集年齡資料或採用其他合理技術手段判定用戶是否為兒童前，除非用於§312.5(c)所列之目的，否則不蒐集任何該用戶之個人資料。且，任何年齡資訊之蒐集或其他判定用戶是否為兒童之手段，必須以中立之方式進行，不得設定特定年齡，亦不得鼓勵用戶提供虛假年齡資料。」

B. 線上聯絡資訊：

新修正之 COPPA 規定，將線上聯絡資訊新增家長之行動電話號碼，該號碼僅得用於向家長發送取得同意之相關簡訊。

C. 個人資料：

自 2013 年修法以來，生物識別技術之快速發展，指紋、手印、視網膜、虹膜及 DNA 序列等生物識別標誌皆可連結至特定個人，故本次修訂中，於個人資料新增生物識別標誌，包含指紋、手印、視網膜或虹膜、遺傳資料如 DNA 序列、面部資料、臉部印模/面部模板、聲紋、步態資料等。並將原先規定之社會安全碼修訂為政府發放之識別標誌，例如社會安全、州身分證、出生證明或護照號碼。

D. 針對兒童之網站或線上服務：

針對兒童之網站或線上服務於定義上係指針對兒童之商業網站或線上服務或其部分，在判斷上有眾



本報告之智慧財產權歸屬於國發會

多因素需要考量。本次修訂將考量因素新增市場行銷、宣傳材料或計畫、對消費者或第三方之陳述、用戶或第三方之評論及類似網站或服務之使用者年齡，以協助更精確地判定網站是否主要針對兒童。

(2) 通知

A. 直接向父母通知之內容：

本次修訂擴大了直接通知家長所需揭露之範圍，包括必須說明將如何利用個人資料；以及網路服務營運商須於將兒童個人資料向第三方揭露時，須通知家長第三方之身分或類別以及揭露之目的，並且，家長須被告知其有權選擇只同意兒童之個資被蒐集而不同意被兒童之個資被揭露與第三方，除非該揭露為網站或服務運作所必要。

B. 網站或線上服務之通知：

新修訂之 COPPA 亦針對線上通知進行增訂。增加規定要求營運商若有向第三方揭露個人資料須於其線上通知提供第三方之身分及特定類別(specific categories)、揭露目的及資料保留政策；亦要求營運商以一般、類別化之方式說明持續性識別碼(Persistent Identifiers)之於其特定內部營運之使用目的；另外，若其網站或線上服務有蒐集含有兒童之聲音之音訊檔案，線上通知中須載明使用此類檔案之方式以及將於利用目的消失後刪除該當檔案。

(3) 家長同意

A. 分別取得同意



本報告之智慧財產權歸屬於國發會

原 COPPA 要求營運商須讓家長選擇同意子女之個資被蒐集但不需同意該當個資被分享給第三方。新規定要求若營運商欲將兒童個資與第三方共享，需另外取得其父母之同意，除非向第三方揭露個資對網站而言是不可或缺的。換言之，營運商須分開取得蒐集利用兒童個資之同意以及分享給第三方之同意。

B. 可驗證家長同意

新法新增可驗證家長同意方法規定。修訂或新增之方法如下：

a. 通知帳戶持有人，原法中，於金錢交易時，使用信用卡、金融卡或其他能向帳戶持有人通知每筆交易之線上支付系統，為驗證家長同意之方法之一。惟新修訂之規定將「金錢交易」刪除，即使未使用金錢交易，亦可透過信用卡、金融卡或其他能向帳戶持有人通知交易之線上支付系統驗證家長同意。

b. 知識驗證（Knowledge-based Authentication），此類驗證需使用猜測答案機率極低之動態多項選擇題，並且問題之難度為 12 歲以下兒童無法合理推斷之答案。

c. 面部識別（Facial Recognition），家長可提供之即時網路攝影機影像與政府發放之身分證件比對，並於驗證後須立即刪除該影像。

d. 簡訊驗證，於不揭露兒童個資之前提下，透過簡訊及附加步驟進行驗證取得家長之同意。

(4) 資訊安全與資料保留強化



本報告之智慧財產權歸屬於國發會

原有之規定要求營運商為保護自兒童蒐集個資之機密性、安全性及完整性須建立並維護合理之機制，而新規定強化了安全性及資料保留要求。首先，營運商須建立資訊安全計畫，該計畫包括所有資料之維護並涵蓋充分保護兒童個資，並須指定特定人員負責計畫之執行，以確保個資之機密、安全及完整，並能控制及評估識別相關風險；另外，營運商僅能於蒐集個資之目的合理必要時間內保留相關個資，若個資不再合理需要時，需採取合理措施刪除該當個資，並且須建立資料保留政策紀錄保留相關個資之業務需求及刪除相關個資之時間表。

(5) 安全港計畫認證經營商公開義務

修訂後規定，每個 FTC 批准之 COPPA 安全港計畫必須在其網站或線上服務公開列出所有認證營運商及其網站或線上服務，且每六個月更新一次。使家長和公眾能夠判斷特定網站或線上服務是否獲得認證。

■ **資料來源：**


1. Federal Register, Children's Online Privacy Protection Rule, 2025-04-22, https://www.federalregister.gov/documents/2025/04/22/2025-05904/childrens-online-privacy-protection-rule (last visited 2025/10/17)

2. Code of Federal Regulations, Art 312—Children's Online Privacy Protection Rule (Coppa Rule),https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312 (last visited 2025/10/17)

3. Loeb & Loeb LLP, Children’s Online Privacy in 2025: The Amended COPPA Rule, 2025-05, https://www.loeb.com/en/insights/publications/2025/05/childrens-online-privacy-in-2025-the-amended-coppa-rule (last visited 2025/10/17)




本報告之智慧財產權歸屬於國發會

(三)2025 年 5 月美國總統川普簽署《刪除法案》

2025 年 5 月美國總統簽署《刪除法案》(Take it Down Act)，旨在禁止於網路上散佈未經個人同意之私密影像(intimate visual depictions)，包含真實拍攝或以數位偽造之方式生成可識別而與個人真實樣貌無區別之影像，以保障個人隱私權利，同時加強對未成年人之隱私保護。該法要求受監管之網路平臺須設立通知及刪除程序，個人得透過程序通知平臺其親密影像被存放於平臺，並要求平臺將影像刪除。而平臺應於接收通知後立即刪除該親密影像。於網路散佈未經個人同意之親密影像為本法所定之犯罪行為，違反本法將受到刑事罰則及罰金併罰。

以下為此法案重點說明：

1. 以刑事規範禁止故意散佈未經同意之私密視覺描繪

應於 1934 年之通訊法第 223 節(Communications Act 47 U.S.C. 223)中(g)款後納入：(h)故意散佈未經同意之私密視覺描繪，並於該小節中進行以下定義：

(1) 「同意」(Consent)係指個人於未受強迫、欺詐、脅迫、虛假陳述或其他強制行為之情形下，所作出肯定、有意識及自願的授權。

(2) 「數位偽造」(Digital Forgery)，指透過軟體、機器學習、AI 或任何其他電腦生成或技術創建任何可識別個人之親密視覺描繪。包含透過調整、修改、操縱或改變真實影像，使一般理性之人(reasonable person)從影像整體觀之，無法區分該影像為真實或偽造。

(3) 「可識別個人」(Identifiable Individual)，指個人全部或部分出現於親密影像中，並且其臉部、肖像或其他顯著特徵，與此類親密視覺描繪有關。



本報告之智慧財產權歸屬於國發會

(4) 「互動式電腦服務」(Interative Computer Service )，指任何資訊服務、系統或近用軟體供應商，可提供或允許多個使用者透過電腦近用電腦伺服器，其中包含近用網際網路的服務或系統，及圖書館或教育機構運作或提供服務的系統。

(5) 「親密視覺描繪」(Intimate Visual Depiction)，該定義係源自 2022 年美國綜合撥款法(Consolidated Appropriations Act,2022 15 U.S.C. 6851)第 1309 條，係指未沖洗之照片及錄影帶、儲存於電腦硬碟或以電子方式儲存可轉換成視覺影像之資料，以及已透過任何方式傳輸且可轉換成視覺影像之資料，無論是否以永久格式儲存，而親密影像之內容包含：

A. 可識別個人之未遮蓋生殖器官、肛門或女性第二性特徵器官等。

B. 展示或傳遞性體液(sexual fluids)至可識別個人身體之任何部位、從可識別個人身體排出，或於可識別個人參與之露骨性行為之情形。

前述任何視覺描繪為可識別之個人身處於公共場所時所製作，且該個人並未自願展示影像呈現之內容或同意影像描述之性行為。

(6) 「未成年人」(MINOR)係指 18 歲以下的任何人。

2. 另於涉及真實私密視覺描繪犯罪及數位偽造犯罪上，區分成年人與未成年人之判斷要件：

(1) 成年人



本報告之智慧財產權歸屬於國發會

任何人於州際或對外貿易時，使用互動式電腦服務故意發布可辨別為成年人之親密影像，有以下情形者，即屬違法。

A. 親密影像為當事人知悉或應知悉，可識別個人具有合理隱私期待之情形下所獲得或創造的。

B. 該影像之內容非可識別之個人於公共或商業情境下自願展示。

C. 該影像內容非公眾關注事項。

D. 發布該親密影像，意圖造成傷害，或對可識別之個人造成包含心理、經濟或名譽傷害。

(2) 未成年人

任何人在州際或對外貿易時，使用互動式電腦服務故意發布可識別為未成年人之親密影像，意圖虐待、羞辱、騷擾或貶低未成年人，或者引起或滿足任何人之性慾。

(3) 前述犯罪不適用以下例外情形：

A. 美國、州或州政府執法機關，以及美國情報局(intelligence agency of the United States)，合法授權之調查、保護或情報活動。

B. 合理及善意揭露，如向執法人員或機關揭露、作為醫學教育、診斷或治療之一部分，或用於合法之醫療、科學或教育目的，以及作為與法律程序相關文件製作或提交之一部分等。

C. 以協助可識別個人為目的之合理揭露。



本報告之智慧財產權歸屬於國發會

D. 個人擁有或發布其本人從事裸體或露骨性行為之親密影像。

E. 發布構成以下內容之親密影像，如《美國法典》(United States Code) 第 18 篇第 2256 節兒童色情 (child pornography)，以及同法第 18 篇第 1466A 節關於兒童性虐待之猥褻影像。

3. 數位偽造相關之犯罪

(1) 成年人

任何人在州際或對外貿易時，使用互動式電腦服務故意發布可識別為成年人之數位偽造品，有以下情形者，即屬違法：

A. 數位偽造品未經可識別之個人同意而發布。

B. 該影像描述之內容非由可識別之個人於公共或商業情境下自願展示。

C. 該影像內容非公眾關注事項。

D. 意圖造成傷害而發布數位偽造內容，或對可識別個人造成包含心理、經濟或名譽之傷害。

(2) 未成年人

任何人在州際或對外貿易時，使用互動式電腦服務故意發布可識別為未成年人之數位偽造品，意圖虐待、羞辱、騷擾或貶低未成年人，或者引起或滿足任何人之性慾。

(3) 前述數位偽造相關犯罪不適用以下情形



本報告之智慧財產權歸屬於國發會

A. 美國、州及州政府執法機關，以及美國情報局，合法授權之調查、保護或情報活動。

B. 合理及善意揭露，如向執法人員或機關揭露、作為醫學教育、診斷或治療之一部分，或用於合法之醫療、科學或教育目的，以及作為與法律程序相關文件製作或提交之一部分等。

C. 以協助可識別個人為目的之合理揭露。

D. 個人擁有或發布其本人從事裸體或露骨性行為之數位偽造品。

E. 發布如《美國法典》(United States Code)第 18 篇第 2256 節兒童色情(Child Pornography)，以及同法第 18 篇第 1466A 節關於兒童性虐待之猥褻視覺影像下規定之親密影像。

4. 注意並刪除未經同意之私密視覺描繪

(1) 「受監管平臺」係指：

A. 指網站、線上服務、線上或行動應用程式，為公眾服務，以及為使用者生成內容包含訊息、影片、圖像、遊戲及音訊檔案等提供論壇，或於貿易或業務過程中，發布、策劃、託管(host)或提供非自願親密影像內容。

B. 受監管平臺不包含 a.寬頻網際網路(broadband internet)服務供應商；b.電子郵件；c.線上服務、應用程式或網站，其主要內容非由使用者生成，而是由線上服務、應用程式或網站之提供者事先選擇，且任何聊天、評



本報告之智慧財產權歸屬於國發會

論或互動功能為附帶性質、與前述預先選擇之內容直接相關或依其所生。

(2) 本法頒布之 1 年內，受監管平臺應建立程序，使可識別之個人得通知受監管平臺，該平臺所發布之親密影像中包含該可識別個人之影像及未經其同意而發布之影像，並且該可識別個人得向受監管平臺提出刪除該些親密影像之請求。

(3) 通知及刪除程序應包含以書面形式為之，內容包含：

A. 可識別之個人的實體或電子簽名。

B. 使可識別之個人辨識親密影像之識別資料，及足以使受監管平臺找到該可識別之個人相關親密影像之識別資料。

C. 簡短聲明，表明可識別個人善意相信依前述 B.所確認之親密影像為未經同意發布，並包含有助於監管平臺確認該親密影像為未經可識別個人同意之情形下而發布之相關資訊。

D. 可識別之個人的聯絡資料。

(4) 受監管平臺應提供清楚顯著（如透過醒目連結提供至另一個網頁）之通知及刪除程序，該程序應易於閱讀且用語淺白，以及提供有關受監管平臺相關責任之資料，如個人如何提交通知及刪除請求之說明。

(5) 受監管平臺於收到可識別之個人提出有效刪除請求後，應於 48 小時內盡快刪除係爭親密影像，並盡合理義務 (reasonable efforts)，辨別及刪除此類影像之任何已知副本。



本報告之智慧財產權歸屬於國發會

5. 罰則

涉及成年人之真實親密影像或數位偽造犯罪，處以罰金、2 年以下有期徒刑，或兩者併罰；涉及未成年人之真實親密視覺描繪或數位偽造犯罪，處以罰金、3 年以下有期徒刑，或兩者併罰。

■ **資料來源：**


1. Congress Gov, TAKE IT DOWN Act, 2025-05-19, https://www.congress.gov/bill/119th-congress/senate-bill/146 (last visited 2025/05/21)
2. Authenticated U.S. Government Information, To require covered platforms to remove nonconsensual intimate visual depictions, and for other purposes, 2025-05-19 , https://www.congress.gov/119/bills/s146/BILLS-119s146enr.pdf (last visited 2025/05/21)


## 二、 歐盟

### (一)2024 年 11 月歐洲個資保護委員會發布《關於個資保護機構於人工智慧法架構所扮演之角色信函》

2024 年 11 月 28 日歐洲個資保護委員會(European Data Protection Board, EDPB)公布致歐盟 AI 辦公室(Artificial Intelligence Office)之信函，回應關於資料保護機關於 AI 架構中之角色，並說明已著手制定一般資料保護規則(General Data Protection Regulation, GDPR)與 AI 法間相互作用之相關指引，期與 AI 辦公室有進一步之討論。

EDPB 表示，為促進資料保護，確保與歐盟其他監管機構之一致性及合作為 EDPB 之政策重點之一。因此，EDPB 相當重視與 AI 辦公室就 AI 監管之合作。EDPB 支持建立相關機制以確保 EDPB、AI 辦公室以及 AI 委員會(AI Board)間業務執行之協作，故邀請 AI 辦公室參



本報告之智慧財產權歸屬於國發會

與其於 12 月之會議，以提供 AI 辦公室以及 AI 委員會之相關資訊。此外，EDPB 提醒 AI 辦公室需充分考量 EDPB 《DPAs 於 AI 法框架角色聲明》(Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework)中對 AI 法第 74(8)條中關於高風險 AI 系統規定之建議。EDPB 依據 AI 法第 64(2)制定關於 AI 模型之 GDPR 意見，意見蒐集至 12 月 23 日，有助於與 AI 辦公室進行交流。

EDPB 於信函最後邀請 AI 辦公室參與其所籌備之技術會議以及公開活動，並表達期於 2025 年第一季之 AI 委員會會議提出對 AI 模型之意見。

■ **資料來源：**

1. European Data Protection Board, Response to the letter on European Data Protection Board (EDPB) statement on the role of data protection authorities (DPAs) in the Artificial Intelligence Act Framework.，2024-11-28，https://www.edpb.europa.eu/system/files/2024-11/edpb-reply-to-the-letter-from-the-ai-office_en.pdf (last visited 2025/01/17)

### (二)2024 年 12 月歐洲個資保護委員會發布《第 28/2024 號關於人工智慧模型中處理個人資料保護意見》

2024 年 12 月歐洲個資保護委員會（European Data Protection Board，下稱 EDPB）發布《第 28/2024 號關於人工智慧模型中處理個人資料保護意見》(Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models)，旨於尋求歐盟範圍內之監管協調，此意見之問題為愛爾蘭資料保護局(the Irish Data Protection Authority)所提出，涉及對社會產生重大影響之快速發展技術，並著重於下列三個問題：

1. 何時及如何將 AI 模型視為匿名(anonymous)？



本報告之智慧財產權歸屬於國發會

該意見指出，AI 模型是否匿名應由資料保護局(Data Protection Authorities, DPAs)依據具體情形為徹底之識別風險評估。只有在滿足下列條件時，才得將 AI 模型視為匿名使用之合理方法：

(1) 不能直接或間接識別其資料被用於訓練模型之個人。

(2) 無自 AI 模型之查詢或分析中獲取個人資料之可能性。

2. 合法利益(legitimate interest)是否及如何為「開發與使用 AI 模型之法律依據」(legal basis)？

EDPB 提供 DPAs 於評估合法利益是否為「處理個人資料以開發及部署 AI 模型之適當法律依據」時，應考慮之一般因素。

於評估特定 AI 模型時，監管機關(Supervisory authorities, SAs)應考量 GDPR 之重要原則：

(1) 問責原則(Accountability principle)

(2) 合法、公平及透明原則(Lawfulness, fairness and transparency principles)

(3) 目的限制及資料最小化原則(Purpose limitation and data minimisation principles)

(4) 資料主體權利(Data subject rights)

於評估及記錄特定個人資料處理時，SAs 應驗證資料控制者是否符合 GDPR 第 6(1)(f)條規定之三步驟測試：

(1) 確定資料控制者或第三方追求合法利益，符合下列三項累積之要件(three cumulative criteria)，則該利益可被視為合法：



本報告之智慧財產權歸屬於國發會

A. 合法利益。

B. 清楚並精確地表達。

C. 真實存在，而非推測性。

(2) 分析資料處理之必要性，必要性評估包含兩元素：

A. 處理是否能達成目的；

B. 是否無侵入性較低之方式達到此目的。

(3) 平衡測試(Balancing test)：

識別及描述利害關係之不同權利及利益，一方為資料當事人之利益、基本權利及自由，另一方為資料控制者或第三方之利益。應考慮案件具體情況以證明合法利益為處理相關活動之適當法律依據。

3. 開發之 AI 模型時使用非法處理之個人資料的後果

要求澄清於開發階段之非法處理個人資料對後續處理或模型運作產生之影響，旨在解決此類 AI 模型處理保留於模型中之個人資料情形，以及於部署 AI 模型時不再涉及個人資料處理之情形 （即 AI 模型為匿名）。

EDPB 建議對以非法處理之個人資料開發的 AI 模型，應採用嚴格的法律審查，包括：

(1) 資料控制者須於開發 AI 模型過程中處理及糾正不符合規定之情形，以免對部署 AI 模型造成影響。

(2) SAs 有權評估資料處理之合法性，依據 GDPR 賦予之裁量權(discretionary powers)，評估可能之違法行為，並依據個



本報告之智慧財產權歸屬於國發會

別情況，選擇採取 GDPR 第 58 條所述之措施中適當、必要並相稱之糾正措施。

■ **資料來源：**

1. European Data Protection Board, EDPB opinion on AI models: GDPR principles support responsible AI, 2024-12-18, https://www.edpb.europa.eu/news/news/2024/edpb-opinion-ai-models-gdpr-principles-support-responsible-ai_en (last visited 2024/12/31)

2. European Data Protection Board, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, 2024-12-18, https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf (last visited 2024/12/31)

### (三)2025 年 4 月歐盟 EDPB 發布《人工智慧隱私風險與因應措施-大型語言模型(LLMs)》

2025 年 4 月，歐盟 EDPB 發布《人工智慧隱私風險與因應措施-大型語言模型》文件，提供大型語言系統(Large Language Models, LLM)之系統開發人員及使用者提供與管理相關技術相關隱私風險之指引及工具，說明相關關鍵技術之概念、風險管理流程、主要風險識別及評估措施，並提供案例，以協助開發者、部署者以及資料保護機關得識別、評估並降低 LLM 之隱私及資料保護風險。該文件共有 10 個部分，第 1 部分為文件架構說明，第 2 部分說明 LLM 之訓練方式、運作原理及其常見之應用。第 3 部分則是關於資料流動以及隱私風險，第 4 部分至第 6 部分為風險評估及控制，第 7 部分至第 10 部分為持續監測及相關實例。

以下就文件中對於 LLM 隱私風險相關之部分說明：

1. 資料流動及隱私風險



本報告之智慧財產權歸屬於國發會

鑒於 LLM 與 AI 系統之高度關聯，該部分說明 AI 系統生命週期於隱私風險管理中之重要性，以及不同類型 LLM 模型中之資料流動以及隱私風險。

許多 AI 系統多是由 LLM 支援，須了解 AI 系統之資料流動，以確保對 LLM 之隱私風險評估。因此本文件參考 AI 生命週期，並以此作為框架提出建議，惟生命週期階段於各組織內部大多相似，但在具體的每個階段仍可能有所不同，並涉及其獨有之隱私風險，因此各組織仍可根據其內部需求及特性制定緩解措施。

本文件建議機構，於 AI 每個生命周期階段皆須實施隱私始於設計政策，有助於自源頭即解決風險而非於後續修復風險。AI 系統生命週期所面對之個人資料風險不盡相同，如於初始資料準備階段需注意敏感資料之匿名化、所蒐集資料可能產生之偏見的調整以及是否須經適當同意，無侵犯著作權或其他法律而蒐集資料；於部署階段則須注意資料之蒐集、傳輸及儲存應採取嚴格控制；最後仍須針對資料模型進行維護及更新維持資料之準確性以及刪除不準確資料以免造成長期隱私風險等。文件強調，機構需考慮各階段可能涉及不同類型個人資料及蒐集、利用及處理方式，以確保能有效實施資料之隱私保護措施。

該文件說明不同類型 LLM 模型之資料流動以及可能產生之風險。封閉模型(closed models & closed weights)係專有模型，不對外提供參數或原始碼之接取，故其風險在於透明度極低，完全依賴提供者之隱私保護措施，若欲獨立驗證資料是否符合法規較為困難；開放模型(open models & open weights)則描述擁有公開可用參數之模型，允許檢查、微調或整合至其他系統中，故其風險則是在於若訓練資料中有涉及敏感或有害內容將可能導致個人資料外洩風險，難以全面檢視訓練



本報告之智慧財產權歸屬於國發會

資料之隱私風險；對於開源模型(open source models)在法律上賦予任何人可以任何目的自由地使用、學習、修改及分配該模型，其風險則與開放模型相同，雖有助於創新但將因模型得被修改而有隱私漏洞或產生原有內建安全機制被移除之風險。

2. 隱私風險評估(Rick Assessment)及控制

風險評估之第一步為風險識別，風險因素(Risk factors)可協助識別 LLM 使用相關之風險。風險因素係指會提高出現不良結果之條件，該些因素得協助識別、評估及確定潛在風險之優先順序。該文件所列風險因素包含：處理目的敏感或具重大影響性、敏感資料之處理、大規模資料處理、處理弱勢個人之資料、低品質資料以及安全措施不足，透過此類風險因素得協助識別於 LLM 系統中之資料保護與隱私是否具備高風險。

除前述風險因素外，AIA 於 AI 系統風險管理中引入基本安全概念，風險之組成包含危害、危害暴露、安全、威脅、漏洞及與基本權利互相影響等，同時為 AI 風險評估提供基礎框架。於識別基於 LLM 系統之風險時，須考慮前述風險對隱私及資料保護之影響，此類風險之識別有助於 AI 系統之風險管理，使 AI 系統符合 GDPR 以及 AIA 之規定，以保護資料主體。系統之預期目的及其情境亦為風險識別之重要部分，預期目的係指 AI 系統設之特定目的及場景，而情境則是指系統運作之環境、使用者基礎及操作設定。由於風險常以非預期目的或於預期外之情境運作下產生，因此清楚界定預期目的及情境將有助於預防錯用並保護使用者。

識別風險後須進行風險評估，此階段預估風險發生之可能性、可能造成之潛在危害及風險可能成為漏洞之因素。由



本報告之智慧財產權歸屬於國發會

於 AI 為跨領域議題，利害關係人於風險評估階段扮演重要角色，於風險評估時透過倫理矩陣(ethical matrix)以識別對利害關係人可能產生直接或間接之影響，確保其觀點被納入風險分類及管理中。下一步須評估風險之機率及嚴重性，並確定是否需進一步處理風險以確保個資保護符合 GDPR 以及 EUDPR 之規範。

最後於風險控制部分，文件說明風險處理(risk treatment)之標準，風險處理是以制定標準之方式以管理已識別之風險，常見的風險處理方式包含緩解(mitigate)、轉移(transfer)、避免(avoid)及接受(accept)。雖並非所有風險都能完全緩解，有些風險可能是固定會產生的，但應至少將風險降低至得接受之水準，並採取管理措施控制風險的影響。此外，建立動態風險登錄(dynamic risk register)可使風險紀錄清楚被保存、可取用並定期更新以確保風險管理之實踐。風險緩解措施需依個案具體情況考量，文件中列出 LLM 於隱私及資料保護風險可行之緩解措施，包含如資料去識別化、紀錄訓練資料來源、定期審核及監督處理資料外洩、偏見或意外之機制、適時採取人為干預及資料最小化等。文件所列之措施僅為一般性建議，並未針對特定案例之背景及目的，此類建議視情況可適用於模型提供者以及部署者。

■ **資料來源：**


1. AI Privacy Risks & Mitigations Large Language Models (LLMs), 2025-04-10, https://www.edpb.europa.eu/system/files/2025-04/ai-privacy-risks-and-mitigations-in-llms.pdf (last visited 2025/05/28)

2. European Data Protection Board, AI Privacy Risks & Mitigations Large Language Models (LLMs), https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/ai-privacy-risks-mitigations-large_en (last visited 2025/05/28)




本報告之智慧財產權歸屬於國發會

(四)2025 年 11 月歐盟執行委員會發布數位綜合法案

歐盟委員會於 2025 年 11 月 19 日公佈「數位綜合法案」(Digital Omnibus Regulation Proposal)。今年年初歐盟委員會提出「競爭力羅盤」(Competitiveness Compass) 溝通文件表示，歐洲於過去 20 年間發展速度一直落後於其他主要經濟體。為使歐洲扭轉局勢，提出三大核心行動以及五大橫向競爭力推動因素，其中簡化監管及行政負擔為首要推動因素，目標係簡化歐盟行政決策之審批流程，目標將企業之行政負擔降低 25%，尤其是針對中小企業之行政負擔降低至少 35%。基於該背景，歐盟研擬修訂整併多項現行法規，包括 GDPR、Data Act 等核心相關法規，以簡化資料立法之框架。其中關於個人資料保護的部分，修訂 GDPR 重點如下：

1. 個人資料與假名化定義之釐清：

修正案前言第 27 段提及：一份資料並不一定被一致性的認定為本法所保護之個人資料。即便可供識別該資料之資料存在，如果資料控制者不存在識別該個人之合理手段(即上述參酌方式)，該資訊對其不應被視為個人資訊。假設該控制者將資訊再次傳送給第三人，則若該第三人具備合理識別該個人之手段，則僅對於該第三人成立個人資訊。針對個人資料定義之規定似乎試圖限縮原 GDPR 對於個人資料之定義，其引入「相對性」概念，認為即使某些資訊可以識別當事人，但若無法直接識別個人資料則可不再視為個人資料。

2. 終端設備資料處理簡化：

為了解決「同意疲勞」問題，提案將原屬於《電子隱私指令》( ePrivacy Directive ) 中關於在個人終端設備上存取或儲存個人資料( 如 Cookie )之規則，整合並新增 Article 88a 及 88b，以實現單一的法律框架管理，具體規定有：



本報告之智慧財產權歸屬於國發會

(1) 在特定風險下，例如僅為測量線上服務的受眾規模且由控制者自行使用，或為提供資料主體明確要求的服務所絕對必需時，儲存或存取終端設備資料將無需徵得同意。

(2) 如果資料主體拒絕同意請求，控制者在至少六個月內不得再次針對相同目的提出新的同意請求，以減少資料主體重複同意。

3. AI 系統開發與個人資料處理之法規鬆綁：

(1) 明確指出為開發及部署 AI 系統或模型而處理個人資料，在適當情況下，可被視為一種正當利益（Legitimate Interest，GDPR 第 6 條第 1 款(f)項）。資料控制者仍需採取適當的保障措施，並提供資料主體無條件之異議權。

(2) 允許在 AI 訓練資料集中處理特殊類別的個人資料(敏感資料)。前提是資料控制者已採取適當措施避免收集此類資料，並在發現後將其移除；若移除需要不成比例的努力，則必須有效地保護這些資料，防止其被用於輸出、揭露或提供給第三方。

(3) 允許處理生物特徵資料以進行身分驗證（verification），前提是相關資料或驗證手段完全由資料主體單獨控制。

4. 資料外洩通報機制變更

在資料發生外洩時，將原須 72 小時內向監管機關通報資料外洩之期限延長至 96 小時。並將通報門檻提升至可能對自然人的權利和自由造成高度風險時才需通報監管機關。

5. 調整個人權利及減輕行政負擔

(1) 處理濫用請求：若資料主體濫用其存取權（Right of Access）時，資料控制者可以拒絕該請求或收取合理費用，



本報告之智慧財產權歸屬於國發會

其實質降低資料控制者證明資料主體請求「過度」（excessive）的舉證責任。

(2) 資料隱私保護影響評估(DPIA)之標準化建立：在歐盟層級內制定單一清單，列出需要和不需要進行資料保護影響評估（DPIA）的處理類型。EDPB 後續將協助準備 DPIA 之共通範本以提供參考。

本法案除 GDPR 修正外，亦提出對 AIA 部分規範之簡化修正，降低風險對 AI 系統發展之影響，重點包括：

1. 免除特定高風險 AI 系統服務提供者之註冊義務

高風險 AI 系統依規定於投放進入市場使用與運作前須進行註冊，但若該系統符合 6 條(3)項之高風險例外者（狹窄之任務範圍、準備程序），由於此類系統不會對人員的健康、安全或基本權利構成重大傷害風險，可免除於 AIA 第 71 條所指的歐盟資料庫中註冊之義務。

2. 擴張歐盟 AI 辦公室之權限與監管範圍

透過 AI 辦公室將監管範圍集中化，減少解釋衝突與分散執法的風險。於歐盟內部，受監管之企業僅須面對單一監管機構，而無須面對各國之監管機關，促使企業更專注於創新和增長，同時減輕各成員國專業人員及監測之負擔。

3. 擴大監理沙盒適用與建設歐盟級沙盒之計畫

新增 AI 系統建立歐盟層級之 AI 監理沙盒。為避免法條實施零碎化，歐盟委員會應通過整體性實施法案，內容包括參與 AI 監理沙盒資格及選擇標準，對於 AI 監理沙盒之申請、參與、監測、退出和終止程序及適用 AI 監理沙盒治理之詳細規則等。



本報告之智慧財產權歸屬於國發會

■ **資料來源：**

1. Digital Omnibus Regulation Proposal，2025-11-19，https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal (last visited 2025/12/05)

## 三、法國

### (一)2025 年 2 月法國資訊自由委員會發布與 AI 相關之個人資料利用指引

法國資訊自由委員會(Commission Nationale de l’ Informatique et des Libertés, CNIL)於 2025 年 2 月 7 日發布兩項關於 AI 使用與個資保護之新建議，旨在促進 AI 領域之負責任創新並同時確保其能遵守歐盟《一般資料保護規則》GDPR 之規定。CNIL 指出，雖某些 AI 模型之訓練資料符合匿名化而不受 GDPR 之約束，但仍有其他大型 AI 模型內(如 LLM 等)可能包含個資，須遵守 GDPR 之規定。

CNIL 提出以下為適應 AI 之建議措施：

1. 目的限定原則：目的之確定可靈活應用通用之 AI 系統，然對於在訓練階段無法明確定義之系統，開發者可描述所開發之系統類型並說明主要潛在功能。

2. 資料最小化原則：利用大型訓練資料集並不必然違反資料最小化原則，惟資料必須經過選擇及清理以優化演算法訓練，同時須避免對個資進行不必要之處理。

3. 資料保存期限：於正當理由且採取適當安全措施之情形下，得延長訓練資料之保留時間。該措施對於需要大量科學或資金投資之資料庫尤其重要，此類資料庫可能成為研究界公認之標準。



本報告之智慧財產權歸屬於國發會

4. 資料庫之再利用：只要資料庫內的資料為合法蒐集（包含取自於現上可得之資料庫的資料），且利用目的與蒐集目的相符，得再利用該資料。

本次發布之兩項新建議分別為「開發者就個人資料被用於訓練 AI 模型之告知義務」以及「當事人之自決權保障」。

1. 開發者就個人資料被用於訓練 AI 模型之告知義務

告知義務係為確保個人資料處理過程之透明度，適用於因 AI 開發訓練而處理之所有個人資料，包括直接或間接蒐集之個人資料。機構於處理個人資料以開發及訓練 AI 模型或系統，而該資料可能被利用於 AI 模型之訓練時，須告知資料當事人，提供必要資訊，使當事人理解機構利用其個人資料之原因，並給予合理之時間，使當事人得以行使 GDPR 賦予之權利，包含異議權(Right to Object)、近用權(Right to Access)、更正權(Right to Rectification)等。而於自大量公開來源蒐集資料之情形下，基於執行告知之可行性，CNIL 建議，機構僅須提供訓練資料之類型或大致資料來源，無須個別通知當事人。例如，若 AI 模型使用自眾多媒體網站取得之資料進行訓練，則依據 CNIL 之建議，機構僅需通知當事人該些資料來源為「線上新聞媒體」而不須標示特定媒體。

對於較敏感之個人資料，考量到模型訓練後可能因技術限制導致當事人較難行使其權利，並因該限制造成風險，CNIL 建議機構應於當事人接受告知至資料實際納入資料庫及模型訓練之間，設定一個合理期間，以利當事人於期間內得行使其權利。

2. 當事人自決權之保障



本報告之智慧財產權歸屬於國發會

機構應確保當事人針對訓練資料庫及AI模型行使GDPR所保障之權利，包括查閱、更正及刪除其個人資料等，以確保當事人對其資料之自主控制權。由於AI模型運作可能涉及哪些個人資料，於技術上較難以識別、定位或刪除，權利行使之風險及成本較高，故 CNIL 建議機構應採取務實且符合比例之作法回應當事人請求，例如向當事人充分說明模型是否可識別其資料，若無法識別，可向當事人說明需要提供其他附加資訊以協助識別，此處之執行可能會因資料控制者是否仍保有訓練資料而有所別。CNIL 鼓勵事業開發可協助當事人對已開發 AI 模型主張權利之技術或作法，然在尚無有效率的處理技術或方法時，現階段較能杜絕爭議可能有兩種做法，最有效者為重新訓練，刪除或修正模型核心資料，然若無法重新訓練，則可考慮使用篩選器解決某些模型運作可能帶來的效應，而無須由模型中刪除本身之資料等。

CNIL 建議機構落實隱私始於設計(privacy by design)，於 AI 系統開發階段即將隱私保護納入考量，並盡量以匿名化(anonymisation)或假名化(pseudonymisation)等替代措施補足現行 AI 系統無法完全讓當事人行使權利之限制。同時建議機構開發創新解決方案以降低 AI 模型洩漏個人資料之風險。CNIL 認為由於目前可用之技術解決方案並無法令人滿意的讓當事人充分行使 GDPR 賦予之權利，故呼籲供應商應優先對訓練資料進行匿名化處理。若無法做到此點，則應確保 AI 模型於訓練後對於資料揭示皆為匿名。

■ **資料來源：**

1. Commission Nationale de l’ Informatique et des Libertés, AI and GDPR: the CNIL publishes new recommendations to support responsible innovation，2025-02-07，https://www.cnil.fr/en/ai-and-gdpr-cnil-publishes-new-recommendations-support-responsible-innovation (last visited 2025/04/09)



本報告之智慧財產權歸屬於國發會

## 四、 澳洲

### (一)2024 年 10 月澳洲資訊委員辦公室發布《隱私及使用市售人工智慧產品之指引》

2024 年 10 月 21 日澳洲資訊委員會辦公室(Office of the Australian Information Commissioner, OAIC)發布《隱私及使用市售人工智慧產品指引》(Guidance on privacy and the use of commercially available AI products)。澳洲《隱私法》(Privacy Act)適用於所有涉及個人資料之 AI 使用，而此次發布之指引旨在協助組織於使用市售 AI 產品時能遵守隱私保護義務，並協助組織挑選適當之 AI 產品。該指引亦涵蓋對免費 AI 產品，如供公眾使用之 AI 聊天機器人的使用指導。雖該指引適用於所有涉及個資之 AI，但尤其適用於生成式 AI、通用型 AI 工具及具較高不利風險影響之 AI。另須注意，該指引並未涵蓋所有應注意之隱私問題及義務，在 AI 工具使用上仍須與隱私法及澳洲隱私原則指引(Australian Privacy Principles guidelines)搭配考量。

本次指引之五項重點如下：

1. 隱私保護之義務適用於輸入至 AI 系統之任何個人資料，以及包含個資之 AI 生成輸出資料。

2. 事業應更新其隱私政策及通知，提供關於其 AI 使用方式更清楚透明之資訊，包括確保向客戶等外部使用者得以明確識別公開使用之 AI 工具，如 AI 聊天機器人。

3. 若 AI 系統被用於生成或推斷個人資料，包含圖片，則該類涉及已識別或合理可識別個人之資訊則構成個人資料，需遵守《澳洲隱私原則》(Australian Privacy Principles, APPs)第 3 章(APP3)關於蒐集個人資料之規定。



本報告之智慧財產權歸屬於國發會

4. 若個人資料將被輸入至 AI 系統，《澳洲隱私原則》第 6 章(APP6)要求實體(entity)僅能基於蒐集資料之主要目的，利用或揭露相關個資。

5. OAIC 建議，組織不宜將個人資料，尤其是敏感資料，輸入於公開可用之生成式 AI 工具。

指引內文架構則分為五部分：

1. AI 及隱私

事業在考慮使用 AI 產品時，須先了解潛在之隱私風險。若欲選擇使用 AI，需考量所涉 AI 產品之開發是否或於使用時將會涉及個資。若確實涉及個資之處理，必須確保在選擇及使用 AI 產品時將隱私保護納入其系統當中。

使用傳統 AI 或生成式 AI 可能造成之重大隱私風險，包括偏見及歧視、缺乏透明度、透過資料洩漏個資之風險及資料當事人對其資料失去控制權。

而生成式 AI 可能會造成特定之隱私風險，如濫用生成式 AI，惡意行為者可能出於不正當目的開發或使用 AI 系統，對個人隱私造成負面後果，例如透過深偽技術(deepfakes)生成虛假資訊或詐騙及身分竊取等犯罪活動。此外，訓練資料品質以及以生成式 AI 模型預測性質相關之問題，導致輸出「似乎可信但不準確」之內容時，將可能產生名譽損害、資訊錯誤或不公平判斷。

機構須注意，使用 AI 系統對兒童及弱勢群體之影響可能較為嚴重，多數案例顯示由 AI 演算法之偏見而導致之個人受到歧視，例如資料集常無法適當反映對原住民族等弱勢團體之歷史偏見。



本報告之智慧財產權歸屬於國發會

2. 與自願性 AI 安全標準(Voluntary AI Safety Standard)之關係

澳洲國家 AI 中心已開發自願性 AI 安全標準以幫助機構於澳洲安全且信賴地開發及部署 AI 系統。該標準由 10 項自願護欄(voluntary guardrails)組成，適用於整個 AI 供應鏈中之機構，協助機構依據現有澳洲法律部署及使用 AI 系統。

3. 組織於選擇 AI 產品時需考量之重點

指引提及，機構於選用 AI 產品時應確保了解所欲使用 AI 產品之運作原理以及包含隱私風險在內之潛在風險。而隱私始於設計以及隱私影響評估皆為機構於使用 AI 產品時得採行以因應風險之措施。在 AI 產品挑選上，指引列出機構應考慮商品是否符合預期用途、潛在之安全風險以及近用 AI 系統數據之權限，但亦提及該些事項並非全面，各機構仍應考慮其他可能產生之相關義務或盡職調查需求。

4. 需採取之透明度及治理措施

透明度為《隱私法》中規定機構須遵守之義務。機構必須確保對 AI 系統相關個人資料之處理保持透明，並能以透明之方式管理 AI 之使用以確保履行 APP 之義務。機構於使用 AI 系統時應告知個人其與 AI 相關資訊之使用方式及隱私政策聲明、具體說明與個人資料相關之 AI 系統蒐集及使用目的及個資揭露、確保能對 AI 之輸出進行解釋以及培訓內部員工了解 AI 產品之生成、蒐集、利用及揭露個人資料。

5. 須持續之驗證流程

機構應於 AI 產品之完整生命週期中制訂驗證流程，以確保產品得持續可靠且符合其預期用途。包括制定 AI 使用內部政策，明確規定允許及禁止之用途，建立明確流程對 AI 輸出



本報告之智慧財產權歸屬於國發會

進行人類監督及驗證，對產品進行定期審查及對員工進行特定產品功能、特定限制與風險等之培訓。

■ **資料來源：**

1. Office of the Australian Information Commissioner, Guidance on privacy and the use of commercially available AI products，2024-10-21，https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-the-use-of-commercially-available-ai-products#section-top-five-takeaways (last visited 2025/01/17)

### (二)2025 年 3 月澳洲聯邦監察員發布《自動化決策最佳實務指引(2025)》

於 2025 年 3 月，澳洲聯邦監察員(Commonwealth Ombudsman)更新發布《自動化決策最佳實務指引(2025)》(Automated Decision-making: Better Practice Guide)，旨在協助政府部門於導入自動化決策系統時，兼顧效率、合法性與公平性。自動化系統能提升服務品質與一致性，但同時可能影響人民之權利與隱私，因此應於創新以及確保自動化決策系統適當使用間取得平衡，即便使用新興科技，民眾仍須為機構服務之核心。該指引內容涵蓋行政法規範、隱私保護、治理與風險管理、透明度、品質保證與救濟措施等面向，並提出一套檢核清單，協助機關在規劃、執行與持續監督自動化決策系統時遵循。

這份指引最初於 2007 年基於行政審查委員會(Administrative Review Council, ARC)第 46 號報告：《行政決策中之自動化協助》(Automated Assistance in Administrative Decision-Making)發布，當中包含 27 條最佳實踐原則，以確保自動化決策符合行政法。2025 年由聯邦申訴專員(Commonwealth Ombudsman)、資訊專員辦公室(the Office of the Australian Information Commissioner)及律政部(Attorney-General's Department)更新，仍著重於提供各政府機構實務指引，以確保其遵守



本報告之智慧財產權歸屬於國發會

行政法與隱私規範，同時參考過去機構監管數位計畫之經驗，並加入補充資源。以下為此指引中與個人資料隱私保護相關之重點整理：

1. 「自動化系統」之定義：

自動化系統所涉範圍廣，本指引之自動化系統係指部分或完全自動完成行政決策之電腦系統。自動化系統可被用於不同之行政決策過程，包含：

(1) 直接做出決策或對決策提出建議。

(2) 可能包含決策協助系統，如於決策過程中為決策者提供相關法律等。

(3) 為個人或決策者提供摘要或初步評估。

(4) 能對決策過程中可能影響後續決策之某些部分進行自動化事實調查。如透過自其他來源之資料或個人直接上傳至系統之資料進行分析。

2. 核心原則：

自動化系統必須遵守與行政法原則中之合法性、公平性、合理性、透明度，並且亦須符合隱私要求以及人權義務。除此之外，良好之公共管理應為高效、容易近用、準確，並且需考量弱勢以及非數位使用者之需求。而行政法、隱私以及人權法規將協助公務機關設計自動化系統，以確保不會造成如偏見、不準確決策等等風險。此外，於自動化系統設計與審查過程中，亦應將行政法、隱私要求以及人權義務整合於其中。

因應大數據及 AI 使用日益頻繁，機構亦應遵守 AI 使用相關之國際規範。澳洲於 2019 簽署經濟合作發展組織 OECD 之 AI 原則(OECD Principles on Artificial Intelligence，下稱 OECD 原則)，該原則於 2024 年 5 月進行更新以考量新興技



本報告之智慧財產權歸屬於國發會

術以及政策發展。該原則將 AI 定義為基於機器系統，能依據輸入內容針對明確目標生成輸出之系統。OECD 原則包含：

(1) AI 系統應透過促進包容性成長、福祉、可持續發展及完永續以造福人類及地球。

(2) AI 系統之設機應尊重法治、人權、民主價值及多樣性，並應包含適當之保障措施。

(3) AI 系統應保持透明且負責任地揭露，以確保用戶正在與 AI 互動，並且能對 AI 結果提出異議。

(4) AI 系統於生命週期內需以穩定、安全之方式運作，並且應持續評估及管理潛在風險。

(5) 開發部署或使用 AI 系統之組織及個人應對依照 AI 原則正常運作 AI 負責。

除如 OECD 此類國際規範外，澳洲工業、科學與資源部於 2019 年發布 AI 倫理原則(AI Ethics Principle, 下稱澳洲 AI 倫理原則)，其內容包含：

(1) AI 系統應於其完整生命週期中，惠及個人、社會以及環境。

(2) 人本價值，AI 系統應於生命週期中，尊重人權、多樣性以及個人自主。

(3) 公平性，AI 系統於完整生命週期中應具包容性及可及性，並不應有對個人、群體之歧視。

(4) 隱私保護以及安全，AI 系統應於完整生命週期中，尊重並維護隱私、資料保護以及資料安全。



本報告之智慧財產權歸屬於國發會

(5) 可信任及安全，於 AI 系統生命週期間，應能可靠地依據其用途運作。

(6) 透明度及可解釋性，AI 系統應有透明度以及資訊公開，使大眾能了解受到 AI 重大影響之時點，以及何時正在與 AI 系統互動。

(7) 可爭議性，AI 系統對個人或社群產生重大影響時，應有即時軟體使大眾能對 AI 系統之使用或結果提出質疑。

(8) 問責性，識別 AI 系統各階段之人員，並且該些人員需對 AI 之結果負責，同時亦須確保 AI 系統受到人類監督。

澳洲 AI 倫理原則可用於 AI 及自動化系統之完整生命週期中，以降低 AI 之負面影響及風險。該些核心原則將於本指引之不同章節中，以自動化系統之重要特徵進行討論。

3. 評估自動化之適當性：

指引中列出不得透過自動化系統處理之行政行為，包含：

(1) 違反行政法之合法性、公平性、合理性及透明性規定。

(2) 違反隱私、資料安全、人權義務或其他法律義務。

(3) 犧牲決策中之準確性。

(4) 明顯弱化公眾對政府管理之信任。

此外，對於評估自動化系統適用性之評估，指引亦列出需考量之因素供各公務機構依據其使用自動化系統時，確認自動化系統適用性所須採取之步驟並將相關內容至於附錄。

當中應考慮之因素如系統是否符合澳洲 AI 倫理原則、系統是否能維護行政法之合法性與公平價值、尋求法律建議並



本報告之智慧財產權歸屬於國發會

確保自動化決策系統及使用符合法律、建立跨領域團隊，就與自動化行政決策及自動化系統開發提供建議、進行風險評估與隱私影響評估、於進行決策前通知受影響個人、建立相關機制以確保於能識別自動化系統造成之錯誤並快速修正與補救以及對相關人員進行培訓等多項確保系統安全性、透明性及對個人權利保障之因素。

4. 法律與裁量問題：

於立法授權層面,雖自動化系統不必然需依賴人類判斷,惟各政府機構仍應指定負最終決策責任之人員或職位，並確保系統設計及後續自動化決策，均依據法律明確授權及允許進行。

就政府機關作出裁量而言，依據澳洲行政審查委員會2004 年所發布行政決策使用自動化輔助之原則見解，直接做出決策之自動化系統僅能是用於非裁量(non-discretionary)之決策，因若使用自動化系統進行裁量，可能使決策者之裁量權受到限制或產生不合理、非理性之結果、錯誤處理等導致權力不當行使之結果。政府機構於使用自動化系統必要時應尋求外部獨立法律專家之意見，以確保具裁量性之行政決策之合法性及公平性之維持。

5. 隱私與個資保護：

政府機構於開發或重新開發自動化系統時，若涉及個人資料之蒐集、利用或儲存，應思考如何於系統設計以及業務流程中保護個人資料，機構於設計自動化系統業務及工作流程時，應選擇符合業務需求且對隱私侵害最小之方式。政府機構應依據《隱私法》(Privacy Act 1998)要求，全面了解隱私義務依據《2017 年澳洲隱私原則》（Privacy (Australian Government Agencies – Governance) APP Code 2017），政府機



本報告之智慧財產權歸屬於國發會

構對於高隱私風險之專案或計畫,都必須進行隱私影響評估。處理個資之自動化決策系統應屬其中之一。另外，隱私始於設計亦應成為機構於開發或審查使用自動化決策時，定期風險管理及流程規劃之一部分。

指引中依據澳洲隱私原則說明當中涉及自動化決策執行之注意事項。

(1) 隱私原則一(APP1)－公開透明

APP1 是為確保機構能以公開且透明之方式處理個人資料。APP1 要求機構採取合理措施，以建立及維護內部慣例、程序及系統。而於 2024 年隱私法修法中，增訂了提高對重大自動化決策可能顯著影響個人權益之透明度規定,要求機構於其隱私權政策中說明其所使用之決策類型及所處理之個人資料種類。

鑒於自動決策系統之複雜性,當事人對於系統所利用之個資何時被蒐集或正在被利用等皆無法察覺。因此，APP1 是要求政府機關能說明其處理個人資料之方式，使資料當事人能理解，以保護個人資料，並且能夠建立大眾之信任,對改善自動化決策系統之結果及促進創新亦能有所幫助。

(2) 隱私原則三(APP3)—僅蒐集合理必要之資料

APP3 為對機構蒐集個人資料之相關規定。要求機構僅能蒐集與其業務或活動合理必要或直接相關之個人資料、蒐集必須為合法公平、且原則上需為自個人所蒐集。APP3 係為平衡個人資料隱私以及自動化決策間取得平衡。



本報告之智慧財產權歸屬於國發會

(3) 隱私原則五(APP5)— 於蒐集個資時，需告知當事人資料將被處理

APP5 要求機構採取合理手段通知當事人或確保當事人了解機構之資訊、蒐集之目的理由、該蒐集是否經法律授權、若不蒐集當事人個資之後果、該機構之隱私權政策以及是否將個資向他國揭露等資訊。

由於於自動化決策之使用情境下告知當事人上述資訊可能具有困難，故機構需以清楚且簡易之方式將相關資訊載於隱私權政策，使當事人能理解。機構亦可透過科技輔助告知當事人，如於當事人輸入其個資時於螢幕上提供相關資訊。

(4) 隱私原則 6(APP6)—利用或揭露授權目的

APP6 說明機構得利用或揭露之個人資料，個人資料僅能用於主要或次要目的。惟於自動決策之情境下，數據分析將可能使資料以不同目的被受到利用。因此實務上，機構必須判斷個人資料之利用是否與最初目的相同，並且有進行隱私權政策說明或通知，若資料利用目的不符，必須將相關資料依據 APP6 進行揭露。使用自動化決策系統因盡量減少當事人對其資料被利用情形不清楚之狀況，指引建議機構應選擇隨時更新隱私權政策，當中包含自動化決策使用之項目，以確保資料當事人能了解其個資之預期用途。

(5) 隱私原則 10(APP10) — 利用之資料須為準確、最新且完整

依據澳洲《隱私法》，機構必須採取合理措施，確保其所蒐集、利用及揭露之個人資料為準確且為最新完整



本報告之智慧財產權歸屬於國發會

的。由於資料分析、AI 及機器學習或自動化決策皆有可能因模型訓練之資料類型不準確或因來源多元而導致其結果產生偏見、歧視等不合理或不準確之結果，故機構應採取嚴格措施確保所蒐集到之個人資料及演算法所建立之相關資訊之品質，確保對個人做出之決策不會因此有不準確或歧視偏見之產生。

另外，機構亦應使當事人能理解 AI 或自動化系統之運作，以協助當事人理解做出自動化決策之原因。於利用個人資料進行自動化決策前，機構應建立資料檢驗流程，驗證非自當事人直接蒐集之資料，並建立相關監控程序及記錄以協助確保資料之準確性。

(6) 隱私原則 11(APP11) —個人資料安全處理

APP11 要求機構採取合理措施避免個人資料遭到濫用、干擾及遺失，以及未經授權之存取、修改或揭露。自動化決策系統會同時建立資料龐大之資料庫，於建立資料庫之過程中，會有將資料來源未經授權修改或存取之可能，因此，機構應採取合理措施保護其所持有之個人資料，包含外部及內部風險。而需處理大量個人資料進行自動化決策之機構，需進行資訊安全風險評估以及資料戶影響評估。另外，若發生資料外洩，需依情形判斷通報澳洲個人資料保護委員會。

6. 治理與設計

自動化系統須建立適當治理框架，確保於系統開發過程中之法律、政策以及服務設計相關部門之參與。於開發系統時，機構應以高標準資訊技術方式進行，並且若自動化系統中有使用 AI，須遵循澳洲政府之負責任使用 AI 政策，並且亦須遵守澳洲政府之隱私框架。



本報告之智慧財產權歸屬於國發會

政府機構若使用自動化系統進行行政決策，必須確保其系統之驗證流程能確認指定之決策者是否有相關權限，而於自動化決策行使過程中，若涉及價值判斷等裁量，必須由有權限之人員進行，且自動化系統必須明確提醒決策者最重決定應自行判斷。此外，涉及裁量或價值判斷之自動化系統，應內建紀錄與保存決策者推理過程之能力，以確保自動化系統之稽核紀錄能完整呈現決策節點。

於資料安全層面，機構應有適當程序，準確蒐集並安全儲存自動化系統所需資料，並且注意資訊安全應始於設計，另外機構亦須確保其自動化系統為符合法律要求及機構之資料安全框架。而在若所設計使用之自動化系統涉及 AI，須遵守澳洲政府之 AI 負責任使用政策及其他政府所發布或更新之其他框架以及政策，並且機構須隨時審查及修正自動化系統以確保其與政府之政策框架保持一致。

7. 透明度與問責制度

行政透明為行政法核心價值之一，且為政府問責之重要要素。因此，政府機構使用自動化系統須注意自動化系統之基本資訊須易於理解，並將相關資料向大眾公開。於使用上，若遇作出對當事人法律或其他重大權利產生實質影響之決策時，應告知當事人。自動化系統之設計應考慮資訊公開以及外部審查，包含決策作成之人、授權、以及決策如何作成。政府機構須能以非技術性之方式顯示其決策之作成為合法且能被認為是公正的。

民眾有權對自動化系統作出或輔助作出之決策提出異議，一旦提出異議，政府機構應進行內部審查，並向當事人提供外部審查之方法，例如向澳洲聯邦監察員提出投訴或將事項提交給仲裁庭或法院。政府機構須確保系統能記錄及保存



本報告之智慧財產權歸屬於國發會

決策者於行使價值判斷相關決策時之審議以及推理過程，並確保相關紀錄為可近用且易於理解。

救濟層面，自動化系統若作出錯誤、不正確或無效之決策，政府機構應抱持即時且合理之補救意願。由於自動化系統可能產生大規模行政風險，於補救上將耗費大量資源及時間，故政府機構應於自動化系統開始使用前即針對大規模行政錯誤制定相關因應計畫，同時制定即時、公平且合理之補救策略，並應能涵蓋所有可能風險，以確保能修正錯誤並防止錯誤再發生。

**■資料來源：**

1.Australian Government Architecture, Automated Decision-making: Better Practice Guide, 2025-03, https://architecture.digital.gov.au/design/automated-decision-making-better-practice-guide (last visited 2025/08/29)

## 五、 韓國

### (一)2025 年 1 月韓國個人資料保護委員會發布 2025 年政策願景及任務：以安全使用個人資料為後盾之可信任 AI 時代

2025 年 1 月 13 日，韓國個人資料保護委員會(Personal Information Protection Commission, PIPC)宣布其 2025 年將以「安全使用個人資料為核心之可信賴 AI 時代」為年度願景。為實現此願景並使個資保護得與 AI 時代接軌，PIPC 將透過全面修訂隱私法規以因應 AI 對隱私所造成之侵害，並希冀能與 AI 政策相互配合。

PIPC 2025 之政策願景以三大戰略及其下之六項關鍵任務組成：

1. 為基於資料及信任之 AI 發展奠定基礎



本報告之智慧財產權歸屬於國發會

(1) AI 時代隱私框架之監管創新

透過建立安全利用個資之法律基礎，協助 AI 及資料生態系發展，以開發對社會有益之 AI 模型。PIPC 將依據韓國《個人資料保護法》(Personal Information Protection Act, PIPA)，推動建立關於使用未經處理原始資料之特殊案例集，例如當企業或研究人員發現於開發 AI 自動駕駛時僅使用假名技術難以實現研究目標時，應採取何種適當之保護措施。同時，考慮到 AI 部署及開發者之合法利益及公共利益，PIPC 將進一步為合法處理個資建立相關法律依據。

(2) 促進創新，為新興產業建構可持續發展之基礎

PIPC 將會透過建構與變化快速之科技發展相適應之制度及基礎建設（包含 AI 模型），為產業創新奠定基礎。

監控設備之資料影像及生物識別技術之管理為 2025 年政策重點之一。鑒於影像資料之特性，此類設備於捕捉隨機行人影像時難以取得當事人之同意，故將推動制定與影像監控設備之安裝及操作相關法律。此外，PIPC 亦將具體處理如個人面部或指紋等生物識別資料之原則，並尊重當事人之權利，以利生物識別技術之傳播。

而為促進假名化(pseudonymization)資料之利用，PIPC 將成立假名化審議委員會，並透過假名化資料支援平台對非結構化之資料進行假名化。此外，PIPC 將著重於包含 AI 在內之新興科技產業之隱私增強技術(Privacy-Enhancing Technologies, PET)發展，並計畫透過對中小企業之技術轉型實現 PET 商業化。

2. 強化於全球資料隱私規範領域之領導地位



本報告之智慧財產權歸屬於國發會

(1) 主動參與全球隱私規範制定討論

PIPC 將在 AI 時代率先參與全球隱私規範制定之討論，2025 年全球隱私大會(Global Privacy Assembly, GPA)預計 9 月韓國首爾舉行，PIPC 預計透過反映亞太地區及其他地區之資料隱私觀點以引領 GPA 上全球隱私規範制定之討論。GPA2025 之討論議程包括設定全球 AI 隱私及資料規範、強化全球網絡及振興國內隱私生態系統。

此外，PIPC 亦致力於加強韓國與歐盟間之資料跨境傳輸合作，其於 PIPA 中增加等效認可計畫之新規定，透過類似歐盟適足性認定之標準，用以評估其他國家及組織之資料保護水準。PIPC 期望透過等效認可計畫建立與歐盟互相承認之系統，以獲得歐盟個資保護適足性認定(adequacy decesion)。

(2) 開創 My Data Scheme 時代，實踐資料可攜

於資料可攜方面，PIPC 將透過於與生活密切相關之醫療保健、電信及能源領域全面實施 My Data Scheme。該計畫將使賦予當事人資料控制權，得請求於不同平台間傳輸個人資料。PIPC 首先推出之服務主要為健康領域、電信服務以及旅遊資料之標準化，未來 My Data Scheme 將逐步擴大該些領域之適用範圍，並規劃將其規範適用於更多行業如教育、就業及娛樂。

而為建立一透明且安全之資料傳輸生態系統，PIPC 計畫建立平台以支援 My Data，使用戶得於平台上查看歷史資料紀錄、撤回資料傳輸、以及執行其資料可攜權利。未來將指定專門機構管理個資，並且由該機構制定相關指導指引，促進 My Data Scheme 之正向發展。



本報告之智慧財產權歸屬於國發會

3. 改革隱私保護框架以因應數位化轉型

(1) 發揮隱私控制塔之關鍵功能

為強化隱私控制塔(Privacy Control Tower)之作用，PIPC 將加強其預防職能及調查能力，徹底改革其調查及處理系統以應對資料轉型之快速變化。為達成此目的，PIPC 將從較容易違反 PIPA 規定之民生相關領域、新興技術與產業以及公共部門三項領域著手，進行事前檢查。民生相關領域包含分享平台、數位金融、住房及教育科技；新興技術產業領域包含自動決策 AI 及其他 AI 服務；公共服務領域則係整合管理系統以及大學教育。

為建立調查能力，PIPC 將於 2025 年成立「數位取證實驗室」，透過專業團隊進行資料外洩證據之分析及保護，並對相關事件進行專業調查，同時亦將組成專門之訴訟團隊以處理相關行政訴訟案件。

行政罰鍰部分，針對國外經營者透過拒絕提供收入資料以規避行政罰鍰，PIPC 未來將要求國外經營企業指定 1 名國內代理人負責，以維護當事人之權利。對中小企業，則將建立較輕微之違法行為調查及行政罰鍰豁免標準。

(2) 建立結構完善且有效之隱私安全網

為積極面對數位時代之隱私侵犯，PIPC 將強化隱私保護及監管措施。PIPC 計畫擴大目前試行中之隱私始於設計(Privacy by Design)認證制度，並計透過修訂個人資料保護法(Personal Information Protection Commission Act, PIPA)將此制度法制化，該機制之適用範圍為網路攝影機(Internet Protocol (IP) cameras)及其他 IT 設備。



本報告之智慧財產權歸屬於國發會

而為提升公部門之資料保護標準，將全面公開違反 PIPA 之公部門相關資訊。針對發生大規模資料外洩之公部門，PIPC 要求其於制裁生效後 3 年內接受額外檢查，提升監管強度，根據機構之資料處理規模、行政制裁紀錄等擴大納入資料保護評估之範圍。

PIPC 對監控設施之隱私保護將透過國家認證資格制度(Nationally Accredited Qualification Scheme)推動影像資訊顧問測驗(Video Information Advisor tests)，以強化公司部門相關人員之專業能力。對於涉及大量個資處理、與民生高度相關之產業(如不動產、旅遊業等)，PIPC 將提供客製化合規指導，依據各產業特性及規模推動「共同監管機制」以提升隱私保護水準。

■ **資料來源：**

1. Personal Information , 인공지능•디지털 시대, 전 국민의 디지털권리 보장을 위한「디지털포용법」제정，2024-12-26，https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=2763 (last visited 2025/03/27)

### (二)2025 年 8 月 6 日韓國個資保護委員會發布《生成式 AI 處理指引》

於 2025 年 8 月 6 日，韓國個資保護委員會（Personal Information Protection Commission, PIPC）舉辦「AI 與隱私公開研討會」，並於研討會上發布《生成式 AI 個人資料處理指引》(생성형 인공지능(AI) 개발·활용 위한 개인정보 처리 기준 제시한다)，以解決生成式 AI 生命週期中《個人資料保護法》（Personal Information Protection Act，下稱 KPIPA）適用之不確定性，並促進企業及機構自願遵守。過去，由於公開資料中往往可能包含姓名、地址、甚至敏感之個人資訊，生成



本報告之智慧財產權歸屬於國發會

式 AI 業者在蒐集與使用資料時面臨法律模糊與隱私風險。此指引之核心精神係於保障人民個資與隱私之同時,減少企業之法律不確定性,使業者能放心投入生成式 AI 技術研發與應用，進而推動創新與產業發展。

指引將生成式 AI 之生命週期分為 4 階段，分別為目的設定、政策制定、AI 訓練與開發，以及應用與管理。此指引確立在每個階段之法律義務，提出需要實施之必要技術及組織措施，並於最後提出以隱私長(Chief Privacy Officer, CPO)為中心之 AI 隱私治理框架。以下是為此指引之重點整理：

1. 目的設定：

   模型開發人員及部署者須定義開發或使用生成式 AI 之目的,並依據個人資料類型以及來源確定訓練 AI 模型之合法依據。對於不同來源之資料,須提供各來源之合法依據,例如:可公開取得之資料、自用戶蒐集之資料等。

2. 政策制定：

   此階段需透過機制之制定,以類型引導風險緩解措施。生成式 AI 之開發與應用策略應與個人資料最小化、隱私加強技術等隱私始於設計(Privacy by Design)原則。而隱私影響評估(Privacy impact assessment, PIA )則可作為將隱私始於設計融入 AI 產品與服務之實踐手段，對公務機關而言，於法定條件下須強制執行 PIA。對於提供大型語言模型(LLMs)服務之類型及使用方式，應提供專門之注意事項指導，確保開發與使用過程安全且符合規範。

3. 生成式 AI 訓練與開發：



本報告之智慧財產權歸屬於國發會

針對資料中毒等風險，制定多層次保障以及 AI 管理措施。於生成式 AI 訓練與開發階段，應採用微調(fine-tuning)和對齊(alignment)技術來提高安全性，並實施針對對抗性攻擊或模型反演攻擊的保護措施，以確保模型達成預期目標，並能減輕意外風險。生成式 AI 之訓練有永久記憶之技術特性，因此原始資訊可能於輸出結果時呈現或能用於推測敏感資料，而有侵害資料當事人權利之可能。因此，於生成式 AI 訓練及開發階段需就資料、模型及系統加強隱私安全措施。需考量之措施如下：

(1) 資料管理：為確保模型之效能以及可信度，故須系統性地應對資料不準確等問題。而訓練資料為防止資料外洩風險之起始，因此考量到生成式 AI 之既定用途與功能，若將訓練資料進行假名或匿名化即可達成防止資料外洩之目的，且指引建議應於資料蒐集後立即進行假名或匿名化處理。而對於識別風險高之資料，以及依 KPIPA 須有特別保護之如居民登錄號碼等唯一識別資料，須於 AI 訓練前刪除或進行假名或匿名化處理。

(2) 模型水準：為補足無法完全消除之之個人資料風險，並使 AI 模型生成安全且準確之回復，指引建議透過微調及對齊等技術，進行額外安全保護措施。

(3) 系統安全：即便已於資料及模型層面實施隱私保護措施，生成式 AI 模型於部署及應用之系統環境下，仍有可能存在個人資料洩漏之漏洞。因此應建立 AI 系統之保護，如限制權限於事先認定之主體、於 AI 系統輸入及輸出階段加裝過濾器分析，避免使用者之提示詞具有惡意或誘導生成敏感資訊。



本報告之智慧財產權歸屬於國發會

(4) 持續評估：生成式 AI 之安全及可靠難以靠一次學習及部署及達成，故應於開發過程中將訓練及評估並行設計，以持續檢查及補充安全性。此外，由於個資保護、偏頗、輸出可靠性等因素將影響資料訓練或模型結構之變化，因此指引建議應定期依照基準測試等方法進行評估。

4. 生成式 AI 系統部署與管理：

在生成式 AI 系統完成開發後，須進行最終檢查，確認系統是否能達成預期目標。於系統部署及應用後，仍須持續檢視系統之功能及安全性，並監測是否有發生對資料當事人之權利侵害，保障當事人權利。業者得於系統發布前測試階段，依據確認之隱私風險，將生成式 AI 之使用目的、禁止行為等記載並公開於「可接受使用政策(acceptable use policy, AUP)」等文件中，透過公開之 AUP，於生成式 AI 發布後，可預防系統濫用並且得以 AUP 為依據，對違反規定之使用行為採取相應措施。業者應於系統中設置資料主體提出異議或意見之功能，以便及時修正偏頗、歧視或權利侵犯之事項，並持續監督及修正系統。

同時，亦須制定相關措施，以保障資料當事人之個資保護權利，如個資之查詢、修改或刪除等。指引建議業者應公開其資料來源、處理目的及 AI 處理過程等事項，並透過措施以及文件問答等方式，協助資料當事人行使其權利。

5. 生成式 AI 隱私治理框架：

由於生成式 AI 之資料處理日趨複雜，風險控管之需求增加，故各業者應以隱私長為中心，以個人資料相關法規、風險管理，建立內部管理制度，使隱私長能於生成式 AI 生命週期中履行管理及監督責任，以確保個資處理之合法性及安全性。



本報告之智慧財產權歸屬於國發會

■ **資料來源：**

1. PIPC, The PIPC Sets Out Personal Data Processing Criteria for Generative AI, 2025-08-14, https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do (last visited 2025/08/21)

2. LEXOLOGY, PIPC Issues Guidelines on the Processing of Personal Information for the Development and Use of Generative AI, 2025-08-14, https://www.lexology.com/library/detail.aspx?g=0dccf02d-b8c5-4fad-b867-c3127f7401be (last visited 2025/08/21)

3. PIPC, 생성형 인공지능(AI) 개발·활용 위한 개인정보 처리 기준 제시한다, 2025-08-06, https://pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId= 11410#LINK (last visited 2025/11/14)

## 六、 新加坡

### (一)2025 年 7 月新加坡發布新工具，協助企業保護資料，並於可信賴的生態系統中部署 AI

2025 年 7 月新加坡資訊通信媒體發展局(Infocomm Media Development Authority, IMDA)發布三項新措施 1.《新全球 AI 信任沙盒》(the new Global AI Assurance Sandbox)；2.《新 PETs 採用指引》(a new PETs adoption guide)；以及 3.《新加坡資料保護標準》(Singapore Standard for Data Protection)，旨在為事業創造最大限度的創新空間，同時提供適當的保護措施，使大眾得安心使用這些技術，以及強化資料保護，使 AI 於不損害個人隱私權益的情形下，基於資料來源進行訓練。以下為重點說明：

1. 《新全球 AI 信任沙盒》

於今年巴黎 AI 行動峰會發布《全球 AI 認證試驗計畫》(Global AI Assurance Pilot)後，AI 驗證基金會(AI Verify Foundation, AIVF)及 IMDA 擴大試驗範圍，以涵蓋新的原型



本報告之智慧財產權歸屬於國發會

(new archetypes)，如代理 AI，以及資料洩漏及容易受到提示注入(prompt injections)影響等風險。

沙盒預計開放於想要發展及取得 AI 治理或測試指引實際回饋的行業監管者。沙盒的見解(insights)將提供政策指導，以發展測試人員認證。並導入 IMDA 近期發布之大型語言模型應用安全測試工具包，以提供測試人員更標準化及結構化的操作方式。前述做法與新加坡以風險為基礎的 AI 實務方法一致，透過適當的保護措施，最大化創新與採用，以建立可信賴的生態系統。

2. 《新 PETs 採用指引》

2022 年，IMDA 及新加坡個人資料保護委員會(Personal Data Protection Commission, PDPC)共同發布隱私強化技術(Privacy Enhancing Technologies, PETs)沙盒，以促進企業使用 PETs。《新 PETs 採用指引》基於 PETs 沙盒用例取得的見解，旨在支援企業採用 PETs 以發揮更大的商業價值，如使 AI 及機器學習能夠更廣泛地取得資料，並與多個相關利益者交叉分享見解。本指引提供以下兩種資源：

(1) PETs 用例評估工具，旨在幫助組織依其特定業務需求確定及評估合適的 PETs 解決方法。

(2) 執行清單(Implementation Checklist)，強調將針對組織採用 PETs 之各階段，從初步評估到永續執行，提出所須考量的關鍵領域，以確保安全及有效地部署 PETs，促進安全的見解分享。

此指引及資源將隨著加入 IMDA PETs 沙盒的新用例及企業回饋而不斷改進。

3. 《新加坡資料保護標準》



本報告之智慧財產權歸屬於國發會

隨著全球資料保護的持續發展，IMDA 與新加坡企業發展局(Enterprise Singapore, ESG)及新加坡認證委員會(the Singapore Accreditation Council)合作，將資料保護信任標誌(the Data Protection Trustmark, DPTM) 提升為新的新加坡標準(SS 714:2025)，向全球資料保護基準及國際最佳實務看齊。企業得申請新的 SS 714:2025 新加坡標準進行認證，以證明其負責任的資料保護實務，為卓越的資料保護設定基準。

SS 714:2025 新加坡標準於第三方管理及跨國傳輸等關鍵領域，為企業提供更明確的資料保護要求，並協助取得認證的企業證明其對資料有效保護的承諾。新加坡認證委員會將對認證機關進行監督，確保 SS 714:2025 標準評估以專業方式進行，符合全球公認標準，並簡化流程從申請到取得認證的整個過程中，只須單點聯絡直接與評估機關合作。消費者可透過 Trustmark 確認通過 SS 714:2025 認證的組織於保護個人資料方面遵循世界級實踐。

■ **資料來源：**

1. Infocomm Media Development Authroity, Singapore launches new tools to help businesses protect data and deploy AI in a trusted ecosystem, 2025-07-07, https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2025/singapore-launches-new-tools-to-help-businesses-protect-data-and-deploy-ai-in-a-trusted-ecosystem (last visited 2025/07/14)

## 七、 中國大陸

### (一)2025 年 3 月香港私隱專員公署發布《雇員使用生成式人工智慧指引清單》



本報告之智慧財產權歸屬於國發會

香港私隱專員公署於 2025 年 3 月 31 日發布《雇員使用生成式人工智慧指引清單》，旨在協助機構制定雇員於工作時使用生成式 AI 之內部政策或指引，並同時遵守《個人資料（私隱）條例》之相關規定。此外，機構於制定指引或內部政策時應依據機構自身情形、符合其自身價值觀，並且須定期檢視所制定之政策及指引，以因應實際運作上及技術上之變化。

1. 準用生成式 AI 之範圍

機構於其內部政策或指引中需明訂：

(1) 準用之 AI 工具，包含公開之生成式 AI 工具、應用程式或內部開發之生成式 AI 及應用程式等；

(2) 準用之用途，機構須清楚明訂可使用生成式 AI 進行之活動或工作，如起草、總結資訊或生成文本、影像內容等；

(3) 政策或指引之適用對象，明定該些政策適用之範圍為整個機構、指定部門、特定職級或是指定雇員。

2. 保障個人資料隱私

機構於制定政策或指引時須注意確保個人資料安全，需明訂得輸入種類以及數量，及禁止輸入至生成式 AI 之資料種類（例如個人資料、機密資料、專有資料或受著作權保護之資料）。私隱公署建議，若機構允許雇員將個人資料輸入至生成式 AI 工具，機構於適當情形下，得要求雇員於輸入資料前將個資進行匿名化，並提供清楚指示。

機構對於生成式 AI 輸出之內容需針對該些內容之准許用途以及儲存方式給予清楚指示。包含生成內容准許之用途且對於進一步使用生成內容之個人資料亦需說明雇員應否、何時及如何於使用前匿名化該些個人資料。機構須要求雇員



本報告之智慧財產權歸屬於國發會

依照相關資訊管理政策儲存資料，並依照其資料保留政策刪除生成式 AI 生成之資料。此外，須確保生成式 AI 相關政策需與機構內部其他與資訊安全及個人資料處理相關政策一致。

3. 合法並符合道德之使用及預防偏見

機構須於其政策中明訂不得將生成式 AI 用於非法或有害之活動，且雇員有責任確保 AI 生成之結果符合機構之道德價值及標準。雇員必須對 AI 所提供之資訊進行校對及查核，確保資訊之準確性，亦須更正及報告帶有偏見及歧視之 AI 生成結果，並且明訂何時及如何於 AI 生成結果加上浮水印或標示。

4. 資料安全

政策或指引須明訂雇員得使用哪些生成式 AI 之裝置（例如由雇主所提供之裝置），私隱公署亦建議雇員於工作裝置上使用生成式 AI 時，應僅限於工作用途。明訂得使用生成式 AI 之雇員，包含需要接受相關培訓或是否需事先經過批准等，亦需確保用戶憑證之安全性以及於生成式 AI 輸入資料之嚴格安全設定。對於涉及 AI 之資料外洩事故、未獲授權下輸入個人資料、異常之生成結果或可能涉及違法之生成結果，應要求雇員依據機構之 AI 事故應變計畫進行報告。

5. 違反政策或指引

機構應於其政策內明訂違反使用生成式 AI 政策或指引可能產生之後果，私隱公署建議機構得參考《人工智能(AI)：個人資料保障模範框架》之制定管理框架及措施。

除該指引清單外，私隱公署亦於同日推出「AI 安全」熱線，供機構查詢相關資訊。



本報告之智慧財產權歸屬於國發會

■ **資料來源：**

1. 香港個人資料私隱專員公署，雇員使用生成式 AI 的指引清單，2025-03-31，https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/guidelines_ai_employees.pdf (last visited 2025/04/10)

2. 香港個人資料私隱專員公署，私隱專員公署發表《僱員使用生成式 AI 的指引清單》，2025-03-31，https://www.pcpd.org.hk/tc_chi/news_events/media_statements/press_20250331.html(last visited 2025/04/10)

## 八、 國際合作或會議

### (一)2025 年 2 月法國、韓國、澳洲、愛爾蘭及英國於巴黎峰會發布 AI 隱私保護之聯合聲明

2025 年 2 月 AI 全球峰會(AI Action Summit)於巴黎舉行，作為其附屬活動，經濟合作暨發展組織(Organization for Economic Cooperation and Development, OECD)、法國資訊自由委員會(CNIL)及韓國個人資料保護委員會(PIPC)共同舉辦 AI 發展下國際資料治理以及隱私之高階圓桌論壇。該論壇重點為推進 AI 資料治理及隱私影響之政策討論，並進一步將資料治理及隱私政策及相關規範定位為可信任 AI 治理之戰略基石。參與此圓桌會議之澳洲資訊委員辦公室(Office of the Australian Information Commissioner, OAIC)、英國資訊委員辦公室(Information Commissioner’s Office, ICO)及愛爾蘭資料保護委員會(Data Protection Commission, DPC)與 CNIL 及 PIPC 共同發布關於 AI 隱私保護之聯合聲明。

該聲明首先說明目前 AI 發展下所產生之風險以及相關資料治理之需求。AI 之發展除為人類、科學創新及經濟提供大量機會，同時於資料保護及隱私規則層面也存在重大風險。此外，歧視、錯誤資訊等亦是因資料處理不當所生之問題。聲明指出，AI 之開發及部署皆須符



本報告之智慧財產權歸屬於國發會

合隱私規則及相關規範，包含自最初階段即引入隱私始於設計系統，並實行資料內部治理框架，將技術及程序保障措施納入框架中，以確保 AI 系統於完整生命週期內皆能被有效管理及降低風險。此外，AI 於開發及部署過程中所涉及之資料極具複雜性，相關資料涉及眾多領域且為 AI 系統大規模運行之核心，處理上較為複雜，因此需要提高透明度以保護資料隱私及基本權利。

基於前述考量，該聲明承諾：

1. 明確資料處理之合法標準及要求

確保 AI 訓練資料之處理為有合理法律依據所為，如基於合法同意、契約必要或法定利益等。同時須注意 AI 開發之目的、必要資料之特性、當事人之合理期待以及相關風險之因應策略。

2. 資料共享之安全措施

資料共享需建立於符合比例原則之安全措施，且該些措施需有嚴謹之科學及實證基礎，並依據不同應用場合進行調整，同時需因應 AI 資料處理技術與實務改變而定期更新。

3. 關注 AI 技術及其對社會之影響

持續監控 AI 技術之發展以及其所產生之社會影響，並盡可能利用資料保護機構及其他如非政府組織、企業或學術機構等相關實體之專業知識及經驗，處理與 AI 相關之政策事務。

4. 鼓勵創新並減少法之不確定性

資料處理為 AI 開發及部署相當重要之一環，因此應減少法律之不確定性並確保技術創新空間。透過建立基於公眾信



本報告之智慧財產權歸屬於國發會

任且符合隱私保護相關規範之制度或方法，如監管沙盒機制或分享最佳實踐工具等，以確保創新及法之確定性。

5. 強化與不同部門間之合作

強化與其他相關部門（包括競爭法、消費者保護及智慧財產權機構）間之溝通，以促進跨部門於 AI 系統、工具及應用程式之一致監管框架，並能共同合作，同時亦鼓勵 AI 生態系中不同參與者之參與及對話。

■ **資料來源：**


1. Joint statement on building trustworthy data governance frameworks to encourage development of innovative and privacy-protective AI, 2025-02-11, https://www.cnil.fr/sites/cnil/files/2025-02/joint_statement_on_data_governance.pdf (last visited 2025/04/18)
2. Commission Nationale de l'Informatique et des Libertés, Data governance and AI: Five Data Protection Authorities Commit to Innovative and Privacy-Protecting AI, 2025-02-11, https://www.cnil.fr/en/data-governance-and-ai-five-data-protection-authorities-commit-innovative-and-privacy-protecting-ai (last visited 2025/04/18)


# 伍、 其他重要趨勢觀測

## 一、 美國

### (一)2025 年 4 月美國白宮發布《關於消除聯邦機構人工智慧使用及採購障礙之情況說明書》

2025 年 4 月美國白宮(the White House)發布《關於消除聯邦機構人工智慧使用及採購障礙之情況說明書》(Fact Sheet: Eliminating Barriers for Federal Artificial Intelligence Use and Procurement)，說明美國管理及預算辦公室(Office of Management and Budget, OMB)與總統



本報告之智慧財產權歸屬於國發會

科技助理(the Assistant to the President for Science and Technology)發布2項修訂政策，《第M-25-21號備忘錄「透過創新、治理及公眾信任加速聯邦使用人工智慧」》(Memorandum M-25-21 Accelerating Federal Use of AI through Innovation, Governance, and Public Trust, M-25-21 )及《第M-25-22號備忘錄「促進有效率採購人工智慧」》(Memorandum M-25-22 Driving Efficient Acquisition of Artificial Intelligence in Government, M-25-22)，旨在落實第14179號總統行政命令《消除美國人工智慧領導地位之障礙》(E.O.14179, Removing Barriers to American Leadership in Artificial Intelligence)，促進負責任地AI採用，改善公共服務，使機構變得更加靈活及提升經濟效率，並增強美國於 AI 創新領域之全球主導地位。

以下為M-25-21及M-25-22之重點說明：

1. M-25-21

旨在提供各機構指導，賦予機構採用 AI 創新所需之工具，提供美國公民隱私、民權及自由之保護，促進人類的繁榮、經濟競爭力及國家安全，以及廢除並取代《第M-24-10號備忘錄「針對使用人工智慧之機構，促進治理、創新及風險管理 」》 (Memorandum M-24-10, Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence)。

(1) 改善AI治理，各機構將授權於AI領導者，消除AI創新之障礙。

A. 重新定義機構首席 AI 官之角色，使其成為改革推動者及AI倡導者，而非層層官僚架構下之監督者。



本報告之智慧財產權歸屬於國發會

B. 首席 AI 官之任務為促進整個機構之 AI 創新，採用風險較低之 AI，降低影響較大之 AI 風險，並就機構之 AI 投資及支出提供建議。

(2) 各機構將制定 AI 應用成熟度評估，更有效地追蹤進展及需求。

(3) 政策引入高影響 AI 類別，追蹤因可能影響美國人民權利或安全而須加強盡職調查之 AI 用例。

(4) AI 之問責(Accountability for AI)將依照現行政府之資訊科技使用程序，而不須建立新的審核層級(layers of approvals)。

(5) 於尋求新的 AI 解決方案時，將最大程度地使用美國之 AI。

2. M-25-22

旨在為各機構提供簡潔有效之指導，以快速、有競爭力並負責任地獲取優良 AI 之能力，以及廢除並取代《第 M-24-18 號備忘錄「促進政府負責任地併購人工智慧」》(Memorandum M-24-18, Advancing the Responsible Acquisition of Artificial Intelligence in Government)。

(1) 各機構須支持具有競爭力之美國 AI 市場，最大限度地使用美國之 AI 系統及服務，以支持美國之 AI 領導地位、人類繁榮、經濟競爭力及國家安全。

(2) 此政策承認競爭之重要性，傳達明確及具體之要求，以避免供應商鎖定(vendor lock-in)。

(3) 新方法消除繁重之機構報告要求，並優化採購流程(the acquisition process)，同時持續保護隱私，以及確保政府資料之合法使用。



本報告之智慧財產權歸屬於國發會

(4) 各機構將運用以績效為基礎之技術，以最佳方式利用快速發展之 AI 市場，並建立資源及工具之線上共享儲存庫(online shared repository)以協助 AI 採購(AI procurement)。

3. 美國聯邦機構將 AI 之益處發揮極致，以促進人類繁榮、經濟競爭力及國家安全。舉例說明如下：

(1) 退伍軍人事務部 (Department of Veterans Affairs，VA)透過 AI 工具優化病患照護，協助識別並標準化退伍軍人之照護，如退伍軍人事務部使用 AI 支援肺癌篩檢，以識別及分析肺部結節，協助臨床醫生進行診斷。

(2) 司法部(The Department of Justice, DOJ)透過利用 AI 保護美國公眾，進而改善公共安全。DOJ 利用 AI 瞭解全球毒品市場及非法毒品對社區及個人之影響，以進一步調查販毒活動，保護美國公眾。

(3) 美國國家航空暨太空總署(The National Aeronautics Space Administration, NASA)利用 AI 擴展人類安全探索火星之能力。NASA 於 Mars2020 火星探測車使用 AI，幫助探測車於來自地球之方向有限情形下進行導航、用以最佳化探測車感應器之科學發現，以及確保探測車安全穿越火星之危險地形。

■ **資料來源：**

1. The White House, Fact Sheet: Eliminating Barriers for Federal Artificial Intelligence Use and Procurement, 2025-04-07, https://www.whitehouse.gov/fact-sheets/2025/04/fact-sheet-eliminating-barriers-for-federal-artificial-intelligence-use-and-procurement/ (last visited 2025/04/09)



本報告之智慧財產權歸屬於國發會

(二)2025 年 7 月美國總統發布人工智慧行動計畫

2025 年 7 月 23 日，美國總統川普(Trump)公布「人工智慧行動計畫」(America's AI Action Plan)，為使美國之 AI 技術領先全球，贏得 AI 技術國際競爭，特設立此計畫以規範 AI 技術在軍事、商業、科技等各領域之運用、建設與創新。此計畫設有加速創新、建設 AI 基礎設施以及引領國際外交及安全三大支柱，以下為此政策的重點整理：

1. 加速 AI 創新（第 1 支柱）

(1) 廢除政府過度限制的條款

AI 現在位於重要的發展階段的初期，不應該被官僚主義所扼殺，因此川普總統於上任後即撤銷了前總統拜登之行政命令(Executive Order 14110)。聯邦政府不應該將與 AI 相關之聯邦資金流向對 AI 發展有過多限制之州政府。然而，聯邦政府也不應過度干涉州政府制定審慎且不過度限制創新之立法的權利。建議政策如下：

A. 由美國白宮科技政策辦公室(the Office of Science and Technology Policy, OSTP)主導，向企業與公眾發出訊息請求，了解當前妨礙 AI 創新及採用的聯邦規定，並與相關聯邦機構合作採取適當行動。

B. 由美國行政管理及預算局(Office of Management and Budget, OMB)主導，並根據 2025 年 1 月 31 日的第 14192 號行政命令「放寬管制，讓經濟更繁榮」(Unleashing Prosperity Through Deregulation)，與各聯邦機構合作，識別、修訂或廢除不必要且妨礙 AI 發展或部署之法規、備忘錄、行政命令等相關文件。OMB 亦將與擁有 AI 技術相關之可裁量資金計劃的機構合作，於確保法律適用之前提下，確保該些機構之資金



本報告之智慧財產權歸屬於國發會

分配決策有將各州之 AI 監管環境納入考量，若該州之 AI 監管可能削弱資金效益，則應限制資金或資助。

C. 由美國聯邦通訊委員會(Federal Communications Commission, FCC)主導，評估各州 AI 法規是否干擾該機構依據 1934 年通訊法履行其義務與權限之能力。

D. 審查在前一屆政府下開始的所有聯邦貿易委員會(Federal Trade Commission, FTC)調查，以確保它們不推進過度負擔 AI 創新的責任理論。此外，審查所有 FTC 最終命令、同意法令及禁制令，並於適當情形下，修改或撤銷任何對 AI 創新構成阻礙之命令。

(2) 確保 AI 保護言論自由及美國價值

AI 系統必須建構在言論自由的基礎上，必須確保在 AI 時代的言論自由仍蓬勃發展，並且，聯邦政府採購之 AI 系統必須呈現真相，而非用於推動社會工程之工具。建議政策如下：

A. 由美國國家標準與技術研究院(National Institute of Standards and Technology, NIST)透過商務部(United States Department of Commerce, DOC)主導，修訂 NIST 的 AI 風險管理框架，以消除對錯誤訊息、多樣性、公平性與包容性以及氣候變化的參考。

B. 更新聯邦採購指導方針，以確保政府僅與確保其系統客觀且不受上而下意識形態偏見影響之前瞻(Frontier)大型語言模型(LLM)開發者簽約。

C. 由美國國家標準與技術研究院的 AI 標準與創新中心(Center for AI Standards and Innovation, CAISI)主導 DOC，進行研究，並在適當的情況下，發布對來自中



本報告之智慧財產權歸屬於國發會

國大陸前瞻模型之評估，以檢視其與中國共產黨之論點及審查制度的一致性。

(3) 鼓勵開源及開放權重之 AI

開源及開放權重的 AI 模型使任何人都能免費下載及修改。新創公司得更靈活地使用且不必依賴封閉模型供應商。同時也讓企業和政府能在不將敏感資料交予封閉模型供應商的情況下使用 AI。對學術研究來說，常依賴近用模型權重以及訓練資料以進行嚴謹之科學實驗，故開放模型不可或缺。相關建議政策如下：

A. 改善大型電腦運算之交易市場，以確保新創事業及學術界能獲得大規模之運算能力。目前大多數新創公司及學者負擔不起大型運算資源，因為需要簽昂貴的長期合約。政府可與業界合作，仿照商品市場機制，建立靈活的「運算交易市場」，讓大家更容易取得所需的運算資源。

B. 與業界領先之科技公司合作，增加研究社群對世界級私部門電腦運算、模型、資料與軟體資源的訪問，作為全國 AI 研究資源(National Artificial Intelligence Research Resource, NAIRR)試點之一部分。

C. 建立精簡及持續性之 NAIRR 營運能力基礎，以將人數上升之研究人員與教育工作者與全國範圍之重要 AI 資源串連。

D. 透過發佈由 OSTP 主導之新國家 AI 研究與發展(R&D)戰略計劃，繼續促進下一代 AI 突破，以指導聯邦 AI 研究投資。



本報告之智慧財產權歸屬於國發會

E. 在美國商務部之國家電信暨資訊管理局(National Telecommunications and Information Administration, NTIA)主導下，召集利害關係人，幫助推動中小型企業採用開源與開放權重模型。

(4) 推廣採用 AI

組織內部對 AI 之有限及緩慢採用為目前 AI 發展之限制。若聯邦政府能有效協調，於美國業界建立勇於嘗試之 AI 文化，將有助於推動 AI 發展。建議政策如下：

A. 在全國建立監理沙盒計畫或 AI 研究中心，使研究人員、新創企業及成熟企業能夠快速部署及測試 AI 工具，同時承諾開放共享資料及結果。

B. 由 DOC 下之 NIST 主導，啟動針對特定領域之 AI 推動計畫，例如醫療、能源與農業，邀集政府、企業與學界各方利害關係人代表參與。計畫目標是加快制定全國性的 AI 標準，並評估 AI 於實際領域中提升生產力之成效。

C. 在美國國防部(Department of Defense, DOD)與國家情報總監辦公室(Office of the Director of National Intelligence, ODNI)合作下，定期更新 DOD 與情報社群對美國、其競爭對手與對手國家安全機構採用 AI 工具之比較水準之聯合評估，並根據這些評估建立 AI 最新情報資訊。

D. 優先處理、搜集與分發可能涉及國家安全之外國前瞻 AI 項目情報，並透過情報機構、DOE、OSTP 等相關部門之協作實施。

(5) 支持以勞工為優先



本報告之智慧財產權歸屬於國發會

政府支持勞工優先之 AI 政策。透過加速生產力並創造全新產業，AI 可以為美國勞工提供更多經濟機會之經濟環境，但也同時改變勞工之工作方式，因此政府將針對勞工政策作出回應以協助勞工適應此過度期。主要政策係推動一系列優先行動，以擴大 AI 素養及技術能發展，持續評估 AI 對勞動市場之影響以幫助勞工於 AI 經濟中成長。建議政策如下：

A. 由美國勞動部(United States Department of Labor，USDOL)、教育部(U.S. Department of Education，ED)、國家科學基金會(National Science Foundation，NSF)與美國商務部主導，將 AI 技能發展作為相關教育與勞動力資金流的核心目標。

B. 由財政部主導，發佈指導意見，澄清 AI 素養與 AI 技能發展計畫可能根據《內部稅收法》(Internal Revenue Code, IRC)第 132 條符合合格教育援助的條件，因 AI 對各職業所需任務與技能之廣泛影響。在適用的情況下，這將使雇主能夠提供免稅的 AI 相關培訓補助，並幫助擴大私營部門對 AI 技能發展的投資，保護美國勞工的工作。

C. 由勞工統計局(U.S. Bureau of Labor Statistics，BLS)與美國商務部透過人口普查局與經濟分析局(Bureau of Economic Analysis, BEA)主導，利用他們已搜集之資料研究 AI 對勞動市場的影響，例如人口普查局在其商業趨勢與展望調查中追蹤的公司層面 AI 採用趨勢。



本報告之智慧財產權歸屬於國發會

D. 在 USDOL 下建立 AI 勞動力研究中心，領導持續的聯邦努力，評估 AI 對勞動市場的影響以及美國勞工的經驗。

E. 由 USDOL 主導，適當時利用可用的自由裁量資金，為受到 AI 相關工作流失影響之個人提供快速再培訓。

F. 在 USDOL 與 DOC 迅速試點新的方法來應對 AI 帶來的勞動力挑戰，這可能包括由勞工流失驅動的快速再培訓需求與入門級角色的技能要求變化等領域。

(6) 支持新興製造業

AI 將促進實體世界中之各種創新，如自主無人機、自駕車、機器人以及其他尚未存在術語的發明。美國及可信賴盟友必須成為這些下一代技術之世界級製造商至關重要。

A. 透過聯邦機構及相關資金投資於開發及擴展基礎、轉化製造技術。

B. 由 DOC 主導透過 NTIA，召集產業及政府利害關係人，以識別美國機器人及無人機製造的供應鏈挑戰。

(7) 投資 AI 驅動之科學科技、建立世界級科學資料庫及推進 AI 科學

A. AI 驅動科技的政府機構應與民營機構互相合作，透過簽訂長期協議支援專責研究機構或類似實體使用 AI 及其他新興科技以促進基礎科學進步，考量研究人員過去獲資助之研究，鼓勵研究人員公開更多高品質資



本報告之智慧財產權歸屬於國發會

料集，並要求聯邦資助的研究者揭露在研究與實驗過程中被 AI 模型使用的非專屬、非敏感資料集。

B. 國家科學技術委員會(National Science and Technology Council, NSTC)機器學習及 AI 小組委員會就生物學、材料科學、化學、物理學與其他科學資料模式在 AI 模型訓練中的最低資料品質標準提出建議。2018 年《機密資訊保護及統計效率法》(Confidential Information Protection and Statistical Efficiency Act of 2018)中之管理與預算辦公室(Office of Management and Budget, OMB)規範，當中包含可訪問性及擴大安全近用措施之規定，這將降低障礙並打破存取聯邦資料之壁壘，於保護機密資料免於不當存取利用之同時促進機構更有效地運用 AI。

C. 優先投資於理論、電腦運算及實驗研究，以保持美國在發現新變革性範例方面之領導地位，並在即將發布之國家 AI 研發策略計劃中反映此優先事項。

(8) 投資於 AI 可解釋性、控制及穩健性突破

目前前瞻 AI 系統的內部運作尚難以理解。技術專家對大型語言模型運作有高層次之理解，但往往無法解釋為什麼模型產生特定的輸出。這使得預測任何特定 AI 系統的行為變得困難，預測困難使用於防禦獲國家安全領域之應用更為困難。若能於這些研究問題上取得突破，美國將能夠在高風險的國家安全領域充分利用 AI 系統。建議政策如下：

A. 啟動由國防高級研究計畫局主導的技術開發計劃，與 DOC 的 CAISI 合作，以促進 AI 可解釋性、AI 控制系統與對抗穩健性。



本報告之智慧財產權歸屬於國發會

B. 於即將到來的國家 AI 研發戰略計畫中，優先考慮 AI 可解釋性、控制性與穩健性的基本進展。

C. 國防部、能源部(Department of Energy, DoE)、商務部的 CAISI、國土安全部、國家科學基金會(NSF)以及學術夥伴應協調舉辦 AI 黑客松活動(AI hackathon initiative)，以徵集美國學術界的最佳人才，測試 AI 系統的透明度、有效性、使用控制及安全漏洞。

(9) 建立 AI 評估生態系統

評估為 AI 產業用以評估 AI 系統性能與可靠性之方式。

A. 提供 AI 評估指南：幫助政府機構依據其特定任務集運作對 AI 系統進行自主評估，確保符合法律要求。

B. 發展 AI 評估科學：由多個聯邦單位合作，推動 AI 模型測試與評估之發展。

C. 定期舉辦交流會議：每年至少舉辦 2 次會議，讓政府與學界互相分享建立 AI 評估之學習及最佳實踐。

D. 建立 AI 測試平台(testbed)：投入資源建立安全及真實之測試環境，使研究者得設計新的 AI 系統原型能並轉化推向市場。

E. 召集 NIST AI 聯盟，推動新型測量科學之合作，識別經驗證之技術及指標，促進 AI 發展與互通。

(10) 加速政府採用 AI

AI 工具之使用得提高聯邦政府之服務效率。



本報告之智慧財產權歸屬於國發會

A. 正式成立首席 AI 官委員會 (Chief Artificial Intelligence Officer Council, CAIOC)，作為採用 AI 之跨機構協調與合作之主要平台。

B. 創建人才交流計畫，旨在快速調派聯邦員工到其他需要專業 AI 人才之機構。

C. 創建由總務署 (General Services Administration, GSA) 管理的 AI 採購工具箱，與美國行政管理及預算局協調，促進聯邦企業最大範圍內的統一性。

D. 與 GSA 實施先進技術轉移與能力共享計畫，以快速在機構間轉移先進的 AI 能力及使用案例。

E. 強制所有聯邦機構確保所有工作可能受益於接觸 AI 模型的員工都能獲得這些工具的使用權限及適當的培訓。

F. 由行政管理及預算局召集提供關鍵公共服務的政府機構，一起試行並推廣 AI 的使用，以提升政府對民眾的服務品質。

(11) 推動國防部 DOD)內之 AI 採用

AI 有潛力改變 DOD 的戰鬥與後勤運作，因國防部於聯邦政府內有獨特運作需求，因此需採取具體政策推動 AI 之採用。建議政策如下：

A. 衡量 DOD 的人力資源所需之人才與技能，並制定人才發展計畫，以滿足 AI 人力資源需求。

B. 於 DOD 建立 AI 與自動化系統虛擬驗證場。



本報告之智慧財產權歸屬於國發會

C. 於 DOD 內部開發精簡流程，對主要作戰與支援功能中之工作流程進行分類、評估及最佳化，以制定優先利用自動化之工作流程清單。工作流程成功自動化後，DOD 應盡快將該工作流程永久過渡至以 AI 實施。

D. DOD 要優先與雲端服務商、運算基礎設施業者，以及其他相關的民間企業簽訂協議，確保於國家緊急狀況下能優先使用所需的之電腦運算資源，以於重大衝突期間使用相關技術。

E. 強化高級軍事學院(Senior Military Colleges)，將其發展成 AI 研究、開發與人才培育中心。推動 AI 相關課程，包含 AI 的使用、開發，以及基礎設施管理等，融入各主修領域的學習中。

(12) 保護商業及政府之 AI 創新

政府與美國主要 AI 開發者合作，使私營部門能夠積極保護 AI 創新免受安全風險，包括惡意網絡行為者、內部威脅等。

(13) 打擊法律系統中的合成媒體(Synthetic Media)

深偽技術(deepfake)為 AI 風險之一，雖川普總統已簽署《刪除法案》(Take it Down Act)，仍需就深偽技術採取進一步行動。AI 合成媒體可能對司法系統帶來新挑戰，如虛假證據之使用，因此行政部門必須給予法院與執法機構克服這些新挑戰所需的工具。建議政策如下：

A. 國家標準與技術研究院會考慮將法醫證據深偽評估計畫做成正式指引與配套之自願性標準。



本報告之智慧財產權歸屬於國發會

B. 司法部(Department of Justice, DOJ)將發布指引，使審判機構能用統一標準來處理深偽證據。

C. 美國司法部法律政策辦公室會對聯邦證據規則中有關深偽技術的修訂提出意見。

2. 建立美國 AI 基礎設施（第 2 支柱）

(1) 簡化資料中心、半導體設備及能源基礎設施之許可流程，並確保安全

A. 建立新的分類，將不會對環境造成重大影響之資料中心納入，盡量採用其他機構已建立之分類，已確保各相關機構得以高效率工作。

B. 確保資料中心之建造合規。尋找合適場地進行建造，確保聯邦土地可用於建造資料中心及其發電基礎設施。

C. 確保安全護欄以防止敵人於該些基礎設施輸入敏感資料，確保 AI 運算為基於美國產品進行，並確保相關基礎設施非使用外國對手資料及通訊技術。

D. 擴大應用 AI，已加速及改善環境評估。

(2) 開發與 AI 創新速度相當之電網

A. 穩定現有電網，避免過早關閉發電設施，確保各地供電穩定又平價。

B. 提升電網效率，使用新技術強化輸電、管理用電，讓電力更充足、更可靠。

C. 優先考慮可靠、可調度電力來源的互聯互通，並接受技術前瞻之新興能源發電來源(例如，增強型地熱、核



本報告之智慧財產權歸屬於國發會

裂變與核聚變)。並對電力市場進行改革，使金融與電網穩定之目標一致，確保電力投資能反應系統需求。

D. 制定策略藍圖，以因應 21 世紀複雜的能源局勢。

(3) 恢復半導體製造

將半導體產業重新導回美國，增強技術領導地位，保護美國供應鏈不受國外競爭對手干預。為使《晶片與科學法案》(CHIPS and Science Act, CHIPS)補助更有效率，應刪除與晶片補助及半導體製造無關之政策限制。此外，國務院及相關聯邦機構應合作簡化相關法規，加速半導體製造。檢視補助及研究計畫，確保 AI 技術能加速用在晶片生產上。

(4) 為軍事與情報社群建設高安全性資料中心

AI 系統適合用於處理原始資料，且其能力可能於未來擴張，亦可能包含利用美國政府之敏感資料，因此部署之模型中心應須能抵禦強烈攻擊，並制定高安全性的 AI 資料中心標準。此外，應推動機構使用機密運算環境以支援安全執行 AI 任務。

(5) 為 AI 基礎設施訓練具備技能之勞動力

A. 由政府帶領倡議 AI 相關基礎設施建設所必要之高度優先職業，並由政府創建 AI 基礎設施相關產業之職業培訓計畫。

B. 推廣中學生與高中生參與 AI 基礎建設相關職業的早期體驗與實習計畫，激發興趣並銜接職業訓練，向州及地方職業技術教育系統提供指導，更新課程，並加強職業教育內容。



本報告之智慧財產權歸屬於國發會

C. 由勞動部主導，擴大註冊學徒制，著重於簡化優先產業及職業中新計畫之啟動，並透過簡化註冊流程或中介機構以減少雇主之用人障礙，並使設計及雇主需求保持一致。

(6) 加強關鍵基礎設施之網絡安全

成立 AI 安全情報共享中心，促進關鍵基礎設施之政府部門間之 AI 威脅資訊交流，並由美國國土安全部(Department of Homeland Security，DHS)提供私部門 AI 安全漏洞應對指引。聯邦政府亦須適時與私部門共享已知之 AI 漏洞資訊，利用現有安全資訊平臺促進合作與整合。

(7) 推廣安全設計的 AI 技術與應用

政府有責任確保其使用之 AI，尤其於國家安全應用上，能防範虛假或惡意輸入，故應促進安全 AI 開發及部署。包含由國防部與商務部之國家標準與技術研究院及國家情報體系(national intelligence community, NIC)合作，持續完善國防部之負責任 AI 與生成式 AI 框架、路線圖與工具包，以及由國家情報體系與美國國防部及美國商務部 AI 標準與創新中心合作，依據情報社群指令發布 AI 保障標準。

(8) 促進聯邦對 AI 事件之成熟應對能力

AI 技術於系統失效時可能會對關鍵服務或基礎設施造成影響，為使影響降至最低，政府應增強對 AI 事故之應對能力，並將相關標準納入現有事故應對之實踐中。商務部之國家標準與技術研究院（含 AI 標準與創新中心）應與 AI 及資安產業合作，確保 AI 納入資安標準與事故應變工具中。此外，政府應更新資安事件應變手冊，加入 AI 系統相關內容，要求資安長、AI 長及隱私長員間之協作。國



本報告之智慧財產權歸屬於國發會

家安全方面，應由國防部、國土安全部與情報總監辦公室，配合其他政府單位，推動負責任分享 AI 漏洞相關資訊，加強國家資安。

3. 在國際 AI 外交與安全中領先（第 3 支柱）

為於全球 AI 競爭中取得成功，美國除於其國內推動 AI 外，亦須推動美國 AI 系統運算硬體及標準於全球採用。美國應運用其於資料中心建設及電腦運算軟硬體方面之優勢建立全球聯盟，並同時避免競爭對手搭便車享受其創新及投資之行為。

(1) 將 AI 技術出口至盟友

必須將完整之 AI 技術，包含軟硬體、模型、應用標準等，出口至有意願加入美國 AI 聯盟之國家。透過技術分配及擴算，阻止盟友依賴競爭對手之技術。美國商務部將設置專門計畫，蒐集產業團隊提出之完整 AI 出口方案。商務部將與經濟外交、貿易發展、出口銀行、國際開發金融公司與國務院合作，幫助推動符合美國安全標準的合作案。

(2) 對抗中國大陸於國際治理機構之影響力

由國務院及商務部帶領，利用美國在國際外交與標準制定組織的影響力，積極推動符合美國價值觀、促進創新並抵制威權主義的國際 AI 治理方式。

(3) 強化 AI 出口管制

AI 對經濟以及新型軍事能力之順利推動相當重要，為防止國外競爭對手獲取相關資源，並基於地緣戰略競爭以及國家安全原因，應開發創新之出口管制方式。



本報告之智慧財產權歸屬於國發會

A. 商務部、白宮科技政策辦公室與國家安全委員會(National Security Council, NSC)為首與產業合作，利用先進 AI 運算晶片之定位驗證功能，確保晶片不流向敏感國家(countries of concern)。

B. 商務部將主導新計畫，與情報機構合作加強全球晶片出口管控，加強全球晶片出口管制之執行。包含監控 AI 晶片技術發展，確保涵蓋可能發生晶片轉運之國家或地區，以提升對高風險國家之終端用途(end-use)監控，尤其是沒有駐地工業及安全局出口管制官員之國家。

(4) 填補現有半導體製造出口管制漏洞

為維持美國於半導體產業領先全球之地位，仍需持續進行開創性研發，同時亦須防止競爭對手利用美國之創新技術，以損害美國國家安全之方式達成目的。因此需以新措施應對半導體製造出口管制之漏洞並加強執法。將由商務部主導制定新的半導體製造子系統出口管制，因目前美國與盟友只對主要製造系統進行管制，對於零件子系統還未施加管制。

(5) 全球統一防護措施

美國對敏感技術施加嚴格之出口管制，並鼓勵貿易夥伴及盟友亦遵循美國之管制以實現國際一致性。

A. 由商務部及國務院帶領，與國安委員會、能源部、科學基金會合作，推動技術保護，防止敏感技術落入競爭對手手中。



本報告之智慧財產權歸屬於國發會

B. 國務院主導制定 AI 聯盟外交策略，促使盟友採用與美國配合的 AI 保護及出口管制，避免技術流向競爭對手。

C. 推動 AI 技術堆疊[7](AI tech stack)之多邊合作管控，避免僅依賴多邊條約機構，確保美國與盟友間之管制標準一致，維護公平競爭環境。

D. 由商務部及美國國防部帶領，與盟友協調確保其採納美國之出口管制措施，並禁止競爭國家向盟友之國防供應鏈供應或取得控股。

(6) 確保美國政府在評估前瞻 AI 模型之國安風險方面處於領先地位

A. 由商務部的 AI 標準與創新中心領導，與具備化學、生物、放射、核、爆炸(CBRNE)與資安專長之政府單位合作，評估前瞻 AI 系統可能帶來之國安風險，並與 AI 開發公司共同進行評估。

B. AI 標準與創新中心也會與國安機構合作，檢視敵對國家的 AI 系統是否在美國重要基礎設施或經濟領域中被使用，評估是否存在後門或其他惡意行為，並比較美國與對手的 AI 技術能力、使用情況與競爭態勢。

C. 政府將優先延攬頂尖 AI 研究人員加入相關機構，包括國家標準與技術研究院、AI 標準與創新中心、能源部、國防部及情報單位，以確保政府能持續提供前瞻 AI 風險評估與分析。

[7] AI 技術運作及應用所需之所有技術層次以及架構，如硬體、軟體、模型等。



本報告之智慧財產權歸屬於國發會

D. AI 標準與創新中心將與國安單位與研究機構合作，建立並定期更新與國安相關的 AI 評估資料，維持風險掌握的前線優勢。

(7) 投資於生物安全

A. 要求所有接受聯邦資助從事科學研究之機構，必須使用具備「完善基因序列篩查」及「客戶驗證」程序之核酸合成工具與服務供應商。並針對此要求設立強制執行機制。

B. 由美國白宮科技政策辦公室主導，召集政府與產業代表，共同建立資料共享機制，使核酸合成業者能合作篩檢潛在欺詐或惡意的客戶。

C. AI 標準與創新中心將持續與國安機構與研究單位合作，建立並更新與國家安全相關的 AI 風險評估系統。

■ **資料來源：**


1. AI.GOV, America's AI Action Plan, 2025-07, https://www.ai.gov/action-plan (last visited 2025/07/30)
2. The White House, White House Unveils America's AI Action Plan, 2025-07-23, https://www.whitehouse.gov/articles/2025/07/white-house-unveils-americas-ai-action-plan/ (last visited 2025/07/30)
3. 科技新報, 白宮宣布美國 AI 行動計畫，「聚焦三大支柱」誓言奪回 AI 主導權, 2025-07-24, https://technews.tw/2025/07/24/trump-ai-plan (last visited 2025/07/30)


二、歐盟

(一)2025 年 2 月歐盟執委會發布《人工智慧系統定義指引》，促進《人工智慧法》規則應用



本報告之智慧財產權歸屬於國發會

2025 年 2 月歐盟執委會(European Commission, EC)發布《人工智慧系統定義指引》(Guidelines on the definition of an artificial intelligence system)，旨在協助提供者及其他相關人員確定軟體系統是否構成 AI 系統，促進《人工智慧法》(AI Act, AIA)規則之有效應用。AIA 並不適用於所有系統，僅適用於符合 AIA 第 3(1)條定義之 AI 系統，故 AI 系統定義為理解歐盟 AIA 適用範圍之關鍵，AI 系統定義不應被機械式的應用，須依系統之具體特點進行評估。此指引不具拘束力，將依時間推移而發展，須依實際經驗、新問題及出現用例進行更新。 以下為此指引所定義 AI 系統之七個要素重點：

1. 以機器為基礎之系統(Machine-based system)

「以機器為基礎」係指 AI 系統利用機器開發並於機器上執行，機器包含 AI 系統運作之硬體與軟體元件，所有 AI 系統皆以機器為基礎，以機器實現其功能。例如：模型訓練、資料處理、預測建模及大規模自動決策。「以機器為基礎」這一要素強調 AI 系統須具備以運算驅動並基於機器操作之事實。

2. 自主性(Autonomy)

AI 系統被設計以不同程度之自主性運作，「不同程度之自主性」指 AI 系統被設計為於某種程度上獨立於人類參與之行動，以及於無人類干預之情形運作之能力。AI 系統之推斷能力，即產生可以影響實體或虛擬環境之預測、內容、建議或決策等輸出之能力，為實現自主性之關鍵。自主性核心概念為「人類參與」及「人類干預」，以及人機互動。自主程度為決定系統是否有資格成為 AI 系統之必要條件，於設計上能有合理程度獨立行動運作之系統，即符合 AI 系統定義之自主性條件。

3. 適應性(Adaptiveness)



本報告之智慧財產權歸屬於國發會

「適應性」指 AI 系統於部署後可能展現之自我學習能力。適應性允許系統之行為於使用中改變，對於相同之輸入，適應系統之新行為可能會產生與先前系統不同之結果，故指引使用「可能」一詞，係因 AI 系統於部署後可能具備自我學習能力，但不一定須具備適應能力或自學習能力才能構成 AI 系統。系統自動學習、發現新模式或識別資料中超出最初訓練之能力為選擇性條件，非判斷該系統是否符合資格成為 AI 系統之決定性條件。

4. AI 系統目標(AI system objectives)

AI 系統之設計依 1 個或多個目標而運作，系統之目標得為明示或暗示。明示目標為開發者直接編碼至系統之明確目標；暗示目標為無明確說明，得從系統之行為或潛在假設中所推斷出來之目標，這些目標可能來自訓練資料或 AI 系統與環境之互動。

AI 系統之目標與特定情形 AI 系統之預期目標不同，AI 系統之目標為系統內部為執行任務之目標及結果；AI 系統之預期目標為提供者預計使用 AI 系統之用途，預期目標不僅須透過系統內部運作達成，亦須透過其他條件協助達成。

5. 使用 AI 技術推斷如何產生輸出(Inferencing how to generate outputs using AI techniques)

AI 系統須從接收到之輸入內容推斷如何產生輸出，AI 系統關鍵特徵之一為「推斷能力」。推斷能力為獲得輸出之過程，例如：輸出可以影響實體或虛擬環境之預測、內容、建議或決策，亦指 AI 系統從輸入或資料推導出模型或演算法(algorithms)，或兩者兼具之能力。



本報告之智慧財產權歸屬於國發會

6. 可以影響實體或虛擬環境的輸出(Outputs that can influence physical or virtual environments)

AI 系統為可以影響實體或虛擬環境之輸出，包含預測、內容、建議或決策四類。

(1) 預測，為 AI 系統最常產生之輸出，亦是最少人工參與之輸出，預測為提供於系統之已知值對未知值之估計。使用機器學習之 AI 系統能發現資料複雜模式，並於高度動態及複雜環境下做出準確之預測。

(2) 內容，為 AI 系統產生之新材料，包含文字、影像、影片、音樂和其他形式之輸出。儘管內容為一種輸出類別，從技術角度可理解為一連串之「預測」或「決策」，但內容輸出於生成式 AI 系統非常普遍，故將其列為單獨之輸出類別。

(3) 建議，依使用者之偏好、行為或其他資料輸入，向使用者提出特定行動、產品或服務之建議，與預測類似，基於 AI 及非基於 AI 之系統皆可以設計來產生建議，例如：以 AI 為基礎之推薦系統得利用大規模資料適應使用者行為，提供高度個人化之建議，並隨著資料集之成長而有效擴充。於其他情形下，建議為潛在之決策，例如：招聘系統僱用之候選人，由人類進行評估，倘建議被自動應用時，即成為決策。

(4) 決策，為系統作出之結論或選擇。輸出決策之 AI 系統，將傳統由人類判斷處理之流程自動化，過程中系統周圍之環境產生一定之結果，不須任何人為干預，完全自動化之過程。

7. 與環境的互動(Interaction with the environment)



本報告之智慧財產權歸屬於國發會

AI 系統之輸出得影響實體或虛擬環境，強調 AI 系統並非被動，而積極影響其部署之環境。實體或虛擬環境表示 AI 系統之影響可能是有形之實體物件，例如：機械手臂或虛擬環境，如數位空間(digital spaces)、資料流(data flows)及軟體生態系統(software ecosystems)。

■ **資料來源：**

1. European Commission, The Commission publishes guidelines on AI system definition to facilitate the first AI Act's rules application, 2025-02-06, https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application (last visited 2025/02/25

### (二)2025 年 2 月歐盟執委會發布《人工智慧法定義之人工智慧禁止行為指引》

2025 年 2 月 2 日歐盟 AIA 已部分生效，歐盟執委會於同月 4 日發布《AIA 定義之 AI 禁止行為指引》(Guidelines on prohibited artificial intelligence practices established by AI Act)，旨在確保 AIA 於歐盟範圍內一致、有效及統一地應用，此指引雖不具拘束力，惟釐清歐盟 AIA 第 5 條規定之 AI 禁止行為，提供法律解釋及實際範例。該指引協助 AIA 下之主管機關進行執法活動，亦協助確保 AI 系統供應商及部署者遵守及履行 AIA 之規定義務。AIA 第 5 條規定，禁止 AIA 風險分級制度中不可接受風險(Unacceptable risk)之 AI。該規定適用於於歐盟市場內提供或部署 AI 系統之企業。

以下為指引對 AIA 第 5 條禁止行為之概述：

1. 操縱、欺騙及剝削(manipulation, deceptive and exploitation)

禁止提供或使用利用潛意識(subliminal)、故意操縱或欺騙之技術，以及利用因年齡、身心障礙或特定社會經濟狀況



本報告之智慧財產權歸屬於國發會

產生之弱點的 AI 系統，此 AI 系統技術對自然人或弱勢群體之行為造成實質影響及重大損害性。目的為保護個人之自主權、決策權及福利，免受操縱、欺騙及剝削性 AI 行為之侵害。

例如，禁止具有顯著危害之潛意識操縱，如透過 AI 神經技術，允許由使用者使用檢測大腦活動之頭戴式設備控制遊戲，並於用戶不知之情形下秘密訓練用戶大腦，從而取得、洩漏或推斷出具侵害性及敏感之資料。禁止 AI 系統依個人資料建立及部署具說服力之資訊，或利用其他個人弱點以影響個人之行為或選擇，造成重大損害。禁止 AI 聊天機器人使用合成聲音冒充個人之親友，並試圖假扮該親友進行詐騙，造成重大損害。而偶然提供虛假或誤導性資訊之生成式 AI 系統不屬於本條所規範之欺騙。禁止 AI 驅動之玩具，利用兒童天生之好奇心及渴望獎勵之弱點，促使兒童做出可能造成嚴重身體損害之危險行為。

2. 社會評分(social scoring)

社會評分係指依據個人或群體之社會行為或個人特徵，對個人或群體為評估或分類。AIA 禁止提供或使用 AI 系統為「社會評分」，導致當事人受到有害或不利益之待遇，尤其當資料源自多個不相關之社會背景，或相關處理方式與社會行為之嚴重性不成比例(disproportionate)時。對社會評分之禁止不僅限於特定領域或行業，亦廣泛適用於公共及私人領域；目的為保護人性尊嚴及民主、平等（含平等獲得公共或私人服務）等其他基本權利，包含不受歧視及平等權、資料保護權、隱私權、家庭生活，以及相關社會經濟權利。對此，指引當中亦提供檢視原則，明示實踐行為須滿足特定要件，方會被認定為應禁止之行為，包括必須已構成對 AI 系統之市場投放、投入使用或使用。且該 AI 系統必須有對自然人或群體以其社



本報告之智慧財產權歸屬於國發會

會行為、已知、推論或預測知個人或個人特質等進行評估或分類，且可能導致有害或不利之待遇等。

禁止使用的情境例如，公共勞動機構使用 AI 系統對失業人員進行評分以確認其是否符合國家就業補助資格。該評分機制係基於個人特徵，如年齡及教育程度判斷，但該機制同時自所獲得之資料或情境中蒐集或推斷與評估目的無明顯關聯之資訊，如婚姻狀況、慢性病健康資料等。

3. 個人犯罪風險評估及預測(individual risk assessment and prediction of criminal offences)

禁止 AI 系統僅依分析或評估人格特質及特徵，預測自然人實施刑事犯罪之風險。例如，禁止執法機構使用 AI 系統僅依個人之年齡、國籍、地址、汽車類型及婚姻狀況等無關犯罪行為之個人特徵，預測特定個人可能於未來犯下恐怖主義等刑事犯罪行為之可能性。

若 AI 系統係用於協助人類對於特定自然人是否涉及犯罪行為之評估，且該評估是基於與該犯罪行為直接相關之客觀可驗證事實時，則非屬此法規禁止範圍。然而若此類非本法禁止而用於犯罪評估之 AI 系統，係由執法機關或其執法者所使用，且用於評估分析自然人之犯罪或再犯罪之風險，則該 AI 之運用仍將被歸類為「高風險」AI 之範圍，須遵守高風險 AI 之相關要求與規範，包括須有人為監督等。

4. 無目標性的抓取臉部影像 (Untargeted Scraping of Facial Images)

禁止自網際網路或監視器錄影無針對性地擷取臉部影像，以建立或擴大臉部辨識資料庫為目的，將 AI 系統投入市場、投入特定目的之利用或其他對 AI 系統之使用。限制此類行為，



本報告之智慧財產權歸屬於國發會

主要著眼於無目的性的地自網路或監視器錄影擷取臉部影像，已嚴重侵害個人之隱私權以及資料保護之權利，同時亦剝奪了個人保持匿名的權利。

例如，禁止臉部辨識軟體公司從社群媒體平臺上（如 Facebook 或 YouTube 等）使用自動影像採集器擷取臉部影像，建立臉部辨識資料庫及關連資料，包含影像來源、地理位置及個人姓名等。

AIA 禁止之臉部辨識 AI 系統不包含無針對性抓取臉部影像以外之生物特徵資料（如：語音樣本），亦不包括無 AI 系統介入擷取影像資料的情形。非用於識別特定人之臉部影像資料庫，亦不在規範範圍內，例如資料庫內影像僅係用於訓練 AI 模型或用於測試之目的，無法識別特定人員等。同時，此限制亦不適用於自網路大量蒐集之面部影像以生成虛構人物新圖像之 AI 模型，因該類模型無法識別真實人物。

5. 情緒辨識(emotion recognition)

禁止利用 AI 系統於工作場所及教育機構用以識別自然人之情緒，除非該系統之利用係基於醫療或安全之原因。情緒識別技術包含偵測、蒐集、分析、分類、反應、互動及學習個人情緒，以推測自然人之情緒。此處限制之系統並非直指 AIA 第 3 條第 39 點所定義用來識別自然人情緒或意圖的「情緒識別系統」(emotion recognition system)[8]，而係僅限可用於推斷自然人情緒之 AI 系統，然而兩者間應有相當之關聯。具備情緒識別技術 AI 系統，存在關於其運作之有效性或準確性的質疑，其運作可能導致歧視結果或侵害人性尊嚴、自由及

[8] AIA 第 3 條第 39 點定義之情緒識別系統，係指該 AI 系統旨在依據自然人之生物特徵資料，識別自然人之情緒或意圖。



本報告之智慧財產權歸屬於國發會

隱私等基本權利，尤其於工作場所及教育機構，員工及學生皆處於特別弱勢地位，故需予以禁止。

例如，禁止於招聘過程使用情緒識別 AI 系統。禁止電話服務中心使用監視器及語音識別追蹤員工之情緒；若為個人訓練目的部署情緒辨識系統，須於不會與人資負責人分享結果且不影響受訓人員之評估或升遷等情形下，方得允許使用情緒辨識系統；或禁止教育機構使用情緒識別 AI 系統推斷學生之興趣及注意力等。

若是出於醫療或安全原因使用之情緒識別 AI，係非屬本禁令之高風險系統，例如用於治療用途(therapeutical use)之系統。基於此類高風險 AI 對基本權可能造成之損害，故此處例外之治療用途系統，於解釋上必須非常限縮，而應被理解為限於帶有 CE(CE-marked)標誌之醫療器材的用途。

6. 生物特徵分類(Biometric categorization)

禁止生物特徵分類系統，主要係透過 AI 模型運作將自然人分類，推論其種族、政治意見、工會會員身分、宗教信仰、性生活或性取向等。此禁止規定不包含歐盟或國家依法律而取得之生物特徵資料集的標籤、篩選或分類。生物特徵資料得提取或推論出個人敏感資料，並針對當事人加以分類，對人性尊嚴、隱私及不受歧視等其他基本權利構成重大風險。

例如，禁止使用 AI 系統分析個人於社群媒體所發布照片之生物特徵資料，依政治取向對群體為分類，並向其發送具有針對性之政治資訊或廣告。

■ **資料來源：**

1. European Commission, Commission publishes the Guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI



本報告之智慧財產權歸屬於國發會

Act, 2025-02-04, https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act (last visited 2025/03/04)

### (三)2025 年 8 月 6 日歐洲保險暨職業養老金管理局發布《人工智慧治理及風險管理意見書》

於 2025 年 8 月 6 日，歐洲保險暨職業養老金管理局(European Insurance and Occupational Pensions Authority, EIOPA)發布《人工智慧治理及風險管理意見書》(Opinion on Artificial Intelligence Governance and Risk Management)，針對保險業使用 AI 系統之監管原則提供指引，強調風險導向與比例原則，明確各國監管機構於 AI 背景下對現有保險法規如《保險分銷指令》(Insurance Distribution Directive, IDD)及《償付能力 II 指令》(Solvency II Directive)之解讀，而為避免監管複雜性，被歸類為高風險 AIA 所禁止之 AI 系統並非本意見書之建議範圍。該意見書未新增法律規定或改變包含 AIA 等其他現有部門立法，意見書明確現有治理及風險管理原則旨在確保資料治理、記錄保存、公平性、資訊安全、可解釋性與人工監督之管理，以平衡 AI 帶來之效益與風險。以下為此意見書之重點整理：

1. 風險導向與比例原則

「風險導向與比例原則」之核心精神，是先評估 AI 系統可能帶來之影響與風險，再依其高低決定治理與監管之嚴格程度。若 AI 系統涉及大量或敏感資料、影響眾多或弱勢客戶、具高度自動決策能力，或可能動搖公司財務與聲譽等評估結果顯示可能造成較高風險，需採取更嚴謹之資料管理、偏差檢測、可解釋性分析與人工覆核等措施；反之，對風險低、影響有限之系統，可採較簡化之管理方式，以確保資源集中於真正重要之風險，同時兼顧安全與創新效率。



本報告之智慧財產權歸屬於國發會

2. 依據前述法規，為確保負責任地使用 AI 系統，業者應依據風險建立相對應之治理與風險管理系統，並考慮以下層面：

(1) 公平性及倫理

A. 公平對待客戶

業者與分銷商必須誠實、公平且專業地行事，以符合客戶最佳利益。EIOPA 於 2023 年針對差異定價實踐及監管之聲明中，說明不符合公平原則之差異化定價做法，並提供業者所需制定之治理及風險管理措施，以減輕風險。

B. AI 運用需以客戶為中心

於 AI 系統之完整生命週期中採用以客戶為中心之方式，以確保公平與客戶最佳利益，並建立包含倫理與公平之企業文化與相關員工培訓。

C. 健全資料治理

去除資料偏見，避免使用可能引發歧視之變數(proxy)，並確保 AI 輸出之可解釋性以識別及減緩偏見。

D. 監測與審計

定期檢查 AI 系統之結果，必要時使用包括公平性與非歧視性之指標進行審計。

E. 申訴與救濟

建立足夠之救濟機制，以便客戶得於受 AI 系統損害時獲得救濟或尋求補償。



本報告之智慧財產權歸屬於國發會

F. 第三方系統

即使 AI 系統由外部供應商開發，業者仍須負最終責任，惟業者應自 AI 系統供應商取得關於 AI 系統特性、能力、訓練及測試之資料及使用限制等充分資訊，並實施補充治理措施如訂立契約條款、進行外部稽核與盡職調查等機制減輕可能的風險。

(2) 資料治理

A. 條文與法規要求

a. 《執委會授權法規 2015/35》(Commission Delegated Regulation 2015/35)第 260(1)(a)(ii)條：風險管理系統應包含關於承保與準備金計算所需資料之充分性與品質政策。

b. 《償付能力 II 指令》第 82 條：用於計算技術準備金之資料必須是完整、準確且適當。

c. 《執委會授權法規 2017/2358》(Commission Delegated Regulation 2017/2358)第 6(1)條：保險商品製造商應適當測試其產品，包含於相關情形下進行情境分析。

B. 風險導向與比例原則

業者應針對 AI 系統實施資料治理政策，並遵守適用之保險及資料保護法規。

C. 資料品質

AI 系統訓練及測試所用資料應為完整、準確且適當。且該些資料限制都應充分紀錄並處理，相關機構應合理努力依據政策消除資料偏差。



本報告之智慧財產權歸屬於國發會

D. 生命週期之資料治理

在 AI 系之完整生命週期間，對蒐集資料、處理資料到利用資料，都應實施嚴謹且妥善之資料治理。另外，若使用第三方提供之外部資料，應同樣遵守資料品質標準。

(3) 保存文件及記錄

歐盟法規要求業者妥善保存業務與內部組織紀錄，並詳細記錄產品審核過程中之相關行動，這些紀錄須供審計與主管機關查閱。此外，亦應保存訓練、測試資料及模型方法，以確保可重現性與追蹤性。

(4) 透明性及可解釋性

業者須用清楚且易於理解之方式，向客戶說明保險產品之客觀資訊，以協助客戶做出明智決定，且所提合約需符合客戶需求及要求。公司也要建立完善之資訊系統，提供關於業務、責任承擔及風險資訊之完整資訊，並須選擇適合目標市場之銷售通路。

使用 AI 時，業者應確保 AI 系統之結果能被有意義地解釋。例如使用可解釋之 AI 演算法，或將複雜 AI 系統用於調整傳統數學模型，並記錄相關假設與限制。若 AI 系統太複雜無法完全透明，應加強風險控管及人為監督。

解釋內容應依據對象調整，監管機關及稽核人員需得到完整說明；客戶則應被告知他們正與 AI 互動，並能用簡單明瞭之語言了解 AI 對他們重要決策之影響。保險中介也應被通知，以履行對客戶之法律責任。

(5) 人工監管



本報告之智慧財產權歸屬於國發會

業者必須於內部各層級建立有效之內部控制系統。依照風險及比例原則方法，於 AI 系統之完整生命週期中建立有效之內部控制系統，並於政策文件中明確之規定升級程序及相關人員參與 AI 之必要步驟。管理層負責 AI 系統之整體運用與風險認知，合規、稽核部門確保符合法規，資料保護官負責個資合規，精算部門則負責相關技術控制。

業者可根據自身需求設置額外組織架構，如聘請 AI 專員、成立 AI 委員會，或與員工代表討論 AI 使用影響。並需針對相關員工提供足夠訓練，確保人員能有效監督 AI 系統，防範偏見，並設置防護機制保障 AI 系統運作正常、尊重客戶權益及維持安全標準。

(6) 準確性、穩健性及網絡安全

業者應建立有效之內部控制系統，依據資訊性質保障資訊安全、完整性與機密性，並遵守金融業資訊與通訊科技之風險管理要求，包括制定與測試業務連續性計畫。

業者應針對 AI 系統設定準確度、穩健性與資訊安全標準，確保系統在完整生命週期內穩定運作，不論系統是自建或外購。應使用合適指標（如準確率、公平性指標）監控系統表現，及時發現並修正問題。

測試 AI 系統時，應評估與其他系統介面連結之安全性與效能影響。AI 系統需防範未授權第三方利用系統漏洞之攻擊（如資料污染），並確保有完善且更新之 IT 基礎建設與備援計畫，保障業務之連續性。

3. 後續監管



本報告之智慧財產權歸屬於國發會

此意見書發布 2 年後，EIOPA 將檢視各國監管機關狀況，已評估各國監管之一致性。本意見中之 AI 治理框架，EIOPA 未來將對特定 AI 系統或保險中使用 AI 系統所生問題進行更詳細之分析，並提供進一步指導。

■ **資料來源：**


1. EIOPA, EIOPA publishes Opinion on AI governance and risk management, 2025-08-06, https://www.eiopa.europa.eu/eiopa-publishes-opinion-ai-governance-and-risk-management-2025-08-06_en (last visited 2025/08/13)
2. EIOPA, Opinion on Artificial Intelligence governance and risk management, 2025-08-06, https://www.eiopa.europa.eu/publications/opinion-artificial-intelligence-governance-and-risk-management_en (last visited 2025/08/13)


### (四)2025 年 9 月 26 日歐盟執委會發布《人工智慧法案第 73 條—事件通報指引草案》

於 2025 年 9 月 26 日，歐盟執委會發布《人工智慧法(歐盟)第 73 條—事件通報指引草案》(Draft Guidance Article 73 AI Act – Incident Reporting)，說明並統一 AIA 中高風險 AI 系統「嚴重事故通報」之具體執行原則與程序。並且致力於與 OECD 之 AI 事件監測通用報告框架保持一致，尋求跨國一致之 AI 事故監測與資訊共享，最終實現 AI 安全、負責與以基本權利為核心之治理體系。

#### 1. 背景與目的

根據 AIA 第 73 條，高風險 AI 系統之提供者有義務通報「嚴重事故」(serious incidents)。而事故通報之目的係為建立早期警示系統，使市場監管機關能及早識別高風險 AI 系統潛在之危害模式或重要風險；強化責任歸屬，確保 AI 提供者(以



本報告之智慧財產權歸屬於國發會

及部分使用者）建立明確問責制度，確保其能對產品之正常運行及安全負責；促進即時矯正措施，主管機關能於事故發生時迅速採取行動；及增加 AI 系統運作之透明度，透過適當監督建立社會對 AI 技術之信任。另因應國際上陸續有相關報告之發布，該指引草案之內容將盡量與 OECD 之《AI 事故監測與共同通報框架》(AI Incidents Monitor and Common Reporting Framework)保持一致。

AIA 第 73 條適用範圍為高風險 AI 系統之嚴重事故與廣泛侵權事件(widespread infringement)，而 AIA 第 55 條第 1 項(c)款所規定具系統性風險之一般用途 AI 模型之重大事件報告，並不包含於本次指引草案之範圍內。

2. 定義與解釋

(1) 嚴重事故依《人工智慧法(歐盟)》第 3 條第 49 款定義，若 AI 系統之事故或故障直接或間接導致以下情況即屬之：

A. 造成個人死亡或嚴重健康損害。

B. 嚴重且不可逆之關鍵基礎設施運作中斷。

C. 違反保護基本權利之歐盟法規義務。

D. 對財產或環境造成嚴重損害。

(2) 廣泛侵權依 AIA 第 3 條第 61 項，係指任何違反歐盟法律之作為或不作為，且該作為或不作為：

A. 已損害至少兩個以上成員國個人集體利益。

B. 已造成、正在造成或可能造成對個人集體利益之損害，其情形具有共同特徵，如涉及相同不法行為或相



本報告之智慧財產權歸屬於國發會

同利益受到侵害，且為同一業者於至少三個成員國內同時或相繼發生。

(3) 「事故」與「故障」區分

A. 事故(Incident)

事故並未於 AIA 中有明文定義，惟於歐盟多個監管框架中皆有依其所管業務特性定義事故，事故通常依據其實際或潛在之負面結果定義，為一種表現特徵上之非計畫偏差。而依據 OECD 之定義，AI 事故為 AI 系統開發或使用導致實際傷害之情形。

B. 故障(Malfunction)

AI 系統功能未如預期運作或性能不符設計目標。

AIA 實務上，兩者並無嚴格區分，均屬應於事故監控下說明之方式，實際之事故/故障範例如：分類錯誤或辨識失準、系統準確度大幅下降、系統臨時停擺或非預期行為。

(4) 直接或間接因果關係

AI 系統之事故需與所造成之損害具有因果關係或可能具有因果關係，若無該事故即不會發生或合理可能不會發生損害，則該事故具因果關係；此外，亦有可能為間接因果關係，如：

A. 醫療 AI 誤判影像導致醫師誤診對病人造成傷害。

B. 信用評分 AI 誤將申請人標示為不可靠，導致貸款遭拒。



本報告之智慧財產權歸屬於國發會

C. AI 招募系統於瀏覽履歷時，因性別或種族而排除實際上優秀的應徵者。導致招聘公司僅能就通過 AI 初步篩選之人員進行聘用。

直接或間接因果關係僅限於 AI 系統於預期用途及合理可預見之誤用範圍內使用之情形，並且事件非由系統使用者之錯誤、義務使用所致。

(5) 嚴重健康損害

嚴重健康損害包括但不限於：

A. 危及生命之傷病。

B. 身體結構或功能之永久或暫時性損傷。

C. 導致住院或延長住院。

D. 須進行醫療或外科手術防止損害惡化。

E. 慢性疾病或嚴重心理疾病。

F. 胎兒死亡或先天缺陷。

(6) 關鍵基礎設施嚴重營運中斷

關鍵基礎設施係指提供基本服務所必要之一項資產、設施、設備、網路或系統或其一部分，而嚴重之營運中斷如：

A. 對生命安全或基本供應造成威脅。

B. 關鍵基礎設施之破壞。

C. 社會經濟活動中斷。



本報告之智慧財產權歸屬於國發會

此外，所造成之中斷需為不可逆，判斷該中斷是否為不可逆需考慮：

A. 需重建物理基礎設施或破壞無法輕易取得之專用設備。

B. 重要紀錄喪失或損毀且無法恢復或重建，如病歷、戶籍資料等。

C. 關鍵節點永久性失效，如鐵路交匯處、電力站等，需花費數年修復。

D. 太空資產喪失，如全球導航衛星系統。

(7) 違反保護基本權利之歐盟法律

僅限大規模且顯著影響歐盟《基本權利憲章》所保護權力之違規行為屬 AIA 第 73 條需通報之嚴重事件，例如：

A. AI 招募系統依性別或種族排除應聘者。

B. 信用評分系統排除特定類別之人如特定族群或居住於特定社區之人。

C. 生物識別系統經常錯誤識別不同族裔背景之人。

(8) 嚴重財產或環境損害

評估財產損害是否屬於嚴重事故，應考慮：

A. 修理更換之費用，若損壞程度影響財產預期用途且使其無法再用於原有用途，視為嚴重損壞，且修復或替換成本超過 5%購置價。

B. 財產之文化或歷史意義。



本報告之智慧財產權歸屬於國發會

C. 財產損失或損害對個人或社群之生活品質或生計造成影響之程度。

D. 損害之永久性及損害之連鎖效應。

(9) 嚴重傷害環境

AIA 中並未定義何謂嚴重傷害環境，故係參考其他相關法規進行定義。環境犯罪指令第 3 條第 5 款定義於評估損害或可能損害是否嚴重時需考慮：

A. 受影響環境之基線狀況。

B. 損害之時間長短、範圍以及可逆性。

3. 責任主體之義務

(1) 高風險 AI 系統提供者

A. 通報義務

高風險 AI 提供者須向事故發生地之成員國監管機構通報，原則上須於得知重大事故後 15 日內進行通報；若為廣泛侵權或關鍵基礎設施中斷則須最遲於得知事故 2 日內通報；若發生人員死亡，不得遲於提供者得知事故之 10 天後通報。

B. 調查義務

AI 提供者須立即對事故所涉 AI 系統進行必要調查，包含風險評估及矯正措施。於通報主管機關前，不得因調查而改動 AI 系統或進行其他可能影響事件後續評估之調查。

C. 合作義務



本報告之智慧財產權歸屬於國發會

AI 提供者必須於調查期間配合主管機關及認證機構，提供必要資料、立即回覆主管機關要求，並與認證機構合作。

(2) AI 系統部署者

若發現嚴重事故，應立即（24 小時內）通知提供者、進口商或分銷商，並通報監管機關。若無法聯繫提供者，則由部署者代行提供者之義務。

(3) 市場監管機關

監管機關須自收到通報之日起 7 日內採取適當措施，而涉及基本權利之通報，須通知國家執行保護基本權利之機關。

(4) 國家主管機關

須立即將嚴重事故通報歐盟執委會。

4. 與其他歐盟法規之互動

若 AI 系統同時受其他歐盟法（如《歐盟實施高度共通程度之資安措施指令》(NIS 2 Directive)、歐盟《關鍵實體韌性指令》(Directive on the resilience of critical entities，CER)、歐盟《數位營運韌性法案》(Digital Operational Resilience Act，DORA)、GDPR 規範，通報僅限於基本權利侵害部分，避免重複通報。

而關於特殊豁免之情形，AIA 第 2 條第 2 款特別規定，若 AI 系統為某些產品之一部分，而該些產品已受其他歐盟法律管理，則該當 AI 系統不須再依 AIA 之事故通報規定（包含第 73 條）進行通報。換言之，該些產品已有其完整監管制度，故不需要重複適用 AIA 之通報義務。



本報告之智慧財產權歸屬於國發會

■ **資料來源：**

1. European Commission, AI Act: Commission issues draft guidance and reporting template on serious AI incidents, and seeks stakeholders' feedback, 2025-09-26, https://digital-strategy.ec.europa.eu/en/consultations/ai-act-commission-issues-draft-guidance-and-reporting-template-serious-ai-incidents-and-seeks (last visited 2025/10/15)

2. JD SUPRA, The European Commission Publishes Draft Guidance for Serious AI Incidents Under the EU AI Act, 2025-10-10, https://www.jdsupra.com/legalnews/the-european-commission-publishes-draft-9085095/ (last visited 2025/10/15)

## 三、英國

### (一)2025 年 6 月英國資訊委員辦公室發布《預防傷害，增進信任：我們的人工智慧與生物辨識策略》

2025 年 6 月英國資訊委員辦公室(Information Commissioner's Office, ICO)發布《預防傷害，增進信任：我們的人工智慧與生物辨識策略》(Preventing harm, promoting trust: our AI and biometrics strategy)，旨在提升 AI 及生物辨識技術應用之信任度及透明度，以及如何於支持負責任創新的同時保障大眾之權利。

AI 發展已融入於日常生活中，其影響決策方式、服務交付方式，以及透過生物辨識技術識別身分之方式，AI 的適應性(adaptability)、可擴展性(scalability)及解決複雜問題的能力，可推動科學、公共服務及經濟領域之進步，且由 AI 驅動之生物辨識技術，得協助組織(organizations)更有效率、更安全地營運，並協助執法部門保護人民安全。為實現上述目的，組織應使英國人民信任其能夠負責任及合法地使用 AI 及生物辨識技術，並達成以下要求：

1. 對使用之個人資料應保持透明度；



本報告之智慧財產權歸屬於國發會

2. 公平地使用這些個人資料；並且

3. 採取適當注意(appropriate care)，制定管理及技術措施，以避免大眾受傷害。

組織利用個人資料缺乏透明度時，將使大眾對 AI 及生物辨識技術缺乏信任，進而不願支持或參與 AI 服務，並對英國經濟體系之負責任地採用 AI 造成障礙。如於警務領域，大眾擔心臉部辨識技術會影響其自由並侵犯隱私權益；於招聘方面，大眾認為雇主會過度依賴 AI 並擔心 AI 對其個人表現之評價會較人類決策者所為之評價差；以及於公共服務領域，大眾對使用 AI 來確認社會福利資格有所擔憂。

為解決此障礙，ICO 提供相關策略，確保組織於符合資料保護法之情形下，使用複雜且不斷演進之 AI 及生物辨識技術，以幫助公私部門確保其對於個人資料之管理及使用能夠實現負責任的創新、預防損害及增進信任，創造更公平之競爭環境，並確保大眾獲得強而有力之保護，以下為 ICO 提供之相關策略之說明：

1. 透過為開發或部署 AI 及自動決策(Automated Decision-making, ADM)之組織制定法定行為準則設定負責任的 AI 之明確期待，以確保於保護隱私之同時實現創新。

2. 透過與開發人員合作，確保於訓練模型時負責任且合法地使用個人資料，從而穩固大眾對生成式 AI 基礎模型之信任。

3. 確保自動決策系統之公平管理及使用，並專注自動決策於招聘及公共服務中之使用方式。

4. 確保公平、適度地使用臉部辨識技術(Facial Recognition Technology, FRT)，並與執法部門合作，確保該技術有效且人民之權利受到保護。



本報告之智慧財產權歸屬於國發會

隨著技術的演進，新的風險也逐漸浮現，AI 系統之自主行動能力的增強，即為所謂之代理 AI (Agentic AI)，同時產生了關於問責性(accountability)與補償(redress)之問題。部分系統會依據人們的身體或行為特徵，推測其意圖或情緒，這些發展皆須仔細審視。ICO 將持續回應新出現之問題，並於工作重點調整時保持透明。

■ **資料來源：**


1. Information Commissioner's Office, Preventing harm, promoting trust: our AI and biometrics strategy, 2025-06, https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/artificial-intelligence-and-biometrics-strategy/ (last visited 2025/06/19)
2. BABL AI, UK Data Regulator Unveils Strategy to Build Trust in AI and Biometrics , 2025-06-10, https://babl.ai/uk-data-regulator-unveils-strategy-to-build-trust-in-ai-and-biometrics/ (last visited 2025/06/19)


(二)2025 年 7 月 31 日英國司法部發布《人工智慧司法行動計畫》

2025 年 7 月 31 日英國司法部(The Ministry of Justice of the United Kingdom, MoJ)發布《人工智慧司法行動計畫》(AI action plan for justice)，司法部認為 AI 有潛力能提供更快、更公平、更容易取得之司法資源，減少法院案件壓力、擴充監獄容量、促進受刑人重返社會以及為被害者服務。惟 AI 發展之同時，仍須將確保公共信任、人權與法治置於核心，並妥善管理 AI 可能帶來之風險。

此計畫為司法部針對法院、法庭、監獄、緩刑及支援體系中負責任且合適地使用 AI 之方針。司法部在制定此計畫時，有與獨立之法官及法律監管單位討論，未來也會與內政部、皇家檢察署、工會等司法相關部門夥伴一起合作推動。此計畫亦是政府讓公共服務更現代化之一部分，希望能發揮英國在全球法律服務、資料科學及 AI 技術上之優勢。此計畫將聚焦於鞏固 AI 技術基礎、將 AI 融入司法系統及投資 AI 技術人才及合作夥伴三大重點策略。



本報告之智慧財產權歸屬於國發會

1. 鞏固 AI 技術之基礎

(1) 強化 AI 技術之管理，成立專責 AI 司法部門

首先，司法部已任命 AI 長(Chief AI Officer)，提供策略領導，加速司法系統中負責任 AI 之採用。AI 長擁有非公務機關 AI 開發與公務機關創新之經驗，將協助吸引頂尖人才，建立高效之跨領域團隊，確保 AI 之倫理、有效與負責任地使用。此外，司法部成立跨領域之司法 AI 單位，協調計畫執行並與相關團隊合作，並安全地將 AI 整合至各部門及機構，確保於維持公眾信任與透明之同時最大化 AI 之潛力。

司法部正與獨立司法機關密切合作，且司法機關已公布其自身之 AI 指引。此合作係為確保司法需求與核心價值能於負責任 AI 部署中充分體現。同時，司法部亦與線上程序規則委員會(Online Procedure Rule Committee, OPRC)合作，相關單位合作，確保 AI 驅動之數位司法服務具備一致性，以使用者為中心且具備健全之法律基礎。

(2) 建立完善之治理機制，以引導並追蹤 AI 之推動與進展

司法部已成立由司法部內各領域高階主管組成之 AI 指導小組(AI Steering Group )，共同監督 AI 採用情形並管理相關風險。該小組負責制定跨領域倫理、資安及營運標準，管理部門之 AI 風險登錄，並定期審查 AI 推動進度及協處各類相關問題。小組會與政府內外之相關機構合作，確保 AI 在司法系統中安全、合法且透明地落實。皇家法院暨仲裁庭(Her Majesty’s Courts Service Tribunals Service, HMCTS)有建立專門之治理與審查機制，避免不當偏誤、保障法律權利，確保 AI 使用方具透明度及問責性。



本報告之智慧財產權歸屬於國發會

而鑒於科技快速發展，司法部保持其治理模式之彈性及敏捷，並持續更新指引、政策及風險管理規範，以遵循現有之數位與資料治理流程進行監督並配合政府發布之 AI 指引。

(3) 透明度為 AI 使用之重要原則

司法部將提供專門之 AI 聯絡計畫(AI Communication Plan)，主動與員工、合作夥伴以及大眾保持互動，以大眾能理解之方式清楚說明司法部之 AI 計畫內容、重點與影響。司法部將以其新架設之網站作為主要平臺，定期發布司法部正在研究、試行及推廣之 AI 應用。並於適當情況下開放原始碼工具及解決方案，促進使用及合作。

司法部將遵守政府之透明度要求，透過「演算法透明記錄標準(Algorithmic Transparency Recording Standard，ATRS)平臺」公開相關之 AI 使用案例，促進公眾監督，提升問責，也促進各領域之創新。

(4) 擴大 AI 與資料倫理框架之適用範圍，確保負責任之建置與採購

為確保 AI 之開發與部署安全、公平且負責任，司法部與研究單位合作，推出「AI 與資料倫理框架」，提供內部團隊在開發與應用 AI 時之實用指引，並將全面推廣使用。該框架還有 5 大核心原則：永續性、問責性、公平性、可解釋性及資料責任。

鑒於司法資料之高度敏感性，司法部高度重視隱私與資安，將與資料保護及資安專家於完整產品週期間進行合作。確保達到或超越法律標準及監管標準，遵守英國 GDPR、政府安全要求、加強控管並定期稽核。



本報告之智慧財產權歸屬於國發會

外部 AI 供應商也須遵守司法部之標準，司法部期望取得其模型與服務之適當存取權限，以確保完整供應鏈皆能落實負責任 AI 實務。為處理演算法偏誤，司法部將持續監測模型輸出、採用去偏見技術，並運用代表性資料集，以確保 AI 僅用於輔助，而非取代人為判斷。

(5) 將資料品質之提升作為推動 AI 應用之前提條件

現行制度下，各機關資料零散且不一致，個人化服務、風險管理及決策速度受到限制。為解決相關問題，司法部正規劃一系列資料計畫，以提升資料品質、治理、互通性及基礎建設。

A. 透過 BOLD 與 Data First 計畫，跨系統連結罪犯資料，提升公共安全、更生、青少年司法、預防及受害者服務。

B. 與內政部(Home Office)及檢察署(Crown Prosecution Service, CPS)合作，推動刑事司法系統資訊流通，推動「安全街道」任務。

C. 強化資料治理、工程及分析流程，提升司法部各機關之資料基礎，加速決策能力並建立司法領域間之一致標準。

D. 與線上程序規則委員會(Online Procedure Rule Committee, OPRC)共同制定資料標準，確保爭端解決機構與 HMCTS 間之互通性，並促進創新及更快速之案件處理。

資料品質之提升將奠定 AI 轉型之基礎。於刑事司法領域為個人建立單一且安全之身分資料，將使 AI 能產生動態風險評分、制定個人化更生方案，並依據健康、教育



本報告之智慧財產權歸屬於國發會

或就業經歷給予個人化協助；於民事、家庭法院或仲裁庭中，一致、準確且可共享之資料可使 AI 進行分流及建議，促進當事人於適當情形下採用相關工具並公平和解，同時亦能擴大司法之可及性。

(6) 解決基礎設施問題，提升 AI 應用準備度

穩定之數位基礎設施為司法系統 AI 應用之重要因素。雖已改善法院及監所之 Wi-Fi、IT 系統及雲端資源，但仍有不足。司法部將強化連線、安全與運算能力，確保 AI 能真正落地並提升法院、監獄及更生之效率。例如，新推出之 ARNS(Assessment, Referral and Notification System)工具將取代舊有風險評估系統，提升管理品質並支援未來 AI 服務所須知基礎設施。

(7) 解決採購 AI 時之財務與商業障礙

AI 需長期監控、更新及維護，需穩定之多年度資金模式，才能真正落地與廣泛運用。司法部將與財政部及科學創新及科技部(Department for Science, Innovation & Technology, DSIT)合作，研究新的資金機制並投資跨部門數位轉型計畫，並且亦將研究彈性採購模式，及早與供應商合作，並擴大創新資金，使新創公司亦得加入。

司法部將不會於初期即投入全部資金，而是計畫採取測試-學習(test-and-learn)之商業模式。首先執行短期價值驗證試點，包含內部及外部開發方案，當中包括與 AI 供應商及中小企業合作，藉此得快速於實際情境中驗證效能；接著透過明確之衡量指標評估結果，評估標準包括準確度、使用者滿意度、成本效益等；最後依據結果進行調整，待方案產生實質價值後再延長相關契約及資金之投入。



本報告之智慧財產權歸屬於國發會

此種商業模式將簡化採購流程、主動與供應商合作，並確保此種商業框架能符合 AI 之特殊需求。司法部認為，政府不只是 AI 之使用者，也能透過採購與合作方式，引導 AI 發展符合社會價值與公共利益。

2. 將 AI 融入司法系統

(1) 在司法系統中擴大使用 AI 生產力工具以增加效率

A. 為每位員工配備安全之 AI 助手

司法部已經在多個部門試用 AI 助理（像是 Copilot 及 Chat GPT Enterprise），幫助員工寫信、整理資料、排行程、製作報告等，節省大量時間。效果顯著，因此，司法部計畫於 2025 年底前，使每位員工都能使用安全之 AI 助理，並提供配套訓練，提升工作效率，並能專注於以人為本之任務。AI 系統亦能協助司法官簡化工作流程，如資料整理、摘要撰寫等，目前針對日常行政工作推廣 AI 工具至各級具領導職務之法官。

B. 運用 AI 搜尋與知識擷取工具，提高資訊掌握效率

司法系統經常需處理大量非結構化之文件，傳統搜尋之效率不足。AI 驅動之搜尋技術能透過理解語意與上下文，更快速搜尋所需之資訊，節省時間、提升決策效率。司法部將於司法服務中逐步推廣此類工具，以降低行政效率，提升服務品質。

C. 利用 AI 語音與翻譯，減少基層人員行政負擔

透過 AI 協助進行逐字稿及會議紀錄，目前已開始於部分地區之緩刑服務中試行 AI 轉錄工具，減輕



本報告之智慧財產權歸屬於國發會

行政負擔並提升錄音品質。此外，於其他司法系統如法院，亦有經司法部驗證之 AI 轉錄翻譯工具試行，該些工具能協助減少延誤、改善司法可及性，並減少對外部供應商之依賴。AI 翻譯工具試行亦包含於監所內之非法律性質口譯及外部出版品之翻譯。

D. AI 代理自動化重複性行政工作

AI 代理能自動執行填表、核對、排程等多步驟任務，提升自動化程度，司法部採取試驗與學習策略，於安全環境用模擬資料測試低風險任務，並嚴格控管安全與權限。法院目前已利用機器學習與電腦視覺技術自動處理每年超過 8 百萬份之紙本表單，顯著提升速度與準確度，未來將擴大應用。

(2) 研議如何透過 AI 改善排程及提高資源使用效率

AI 工具能即時分析人力、風險、容量與優先順序，快速產出最合適之排班或行程。英國國民保健署(National Health Service，NHS)已透過此技術提高手術排班之效率，亦可能應用於司法系統之管理。AI 能根據變動自動更新行程，減少人工作業時間，並維持安全與服務品質，司法部將持續研議該技術應用於監所容量管理、協助法院排程之可行性。

(3) 研議 AI 提升個人教化方式

司法部正在研議如何利用 AI 學習平臺，為員工與受刑人提供客製化之教學內容，解決監所中師資不穩之問題，並協助受刑人提高知識水準，使其能重新融入社會及就業。2025 年春季，司法部試行利用 AI 生成教材，透過



本報告之智慧財產權歸屬於國發會

虛擬學習平臺教授地理、歷史、數位技能等課程，未來將持續評估 AI 如何協助監獄與緩刑中之個別學習。

(4) 研議透過 AI 助理改善司法可及性

AI 聊天機器人可幫助民眾了解法律程序、獲得補償指引、處理家事糾紛，提升司法可及性。司法部正與 DSIT 合作，測試並部署 AI 系統於司法部客服中心，以簡化案件處理並提升服務品質。

(5) 透過 AI 改善政策制定及策略決策

司法部將研議並試用 AI 工具，協助政策與策略部門更快速、智慧且包容地制定決策。機器學習可以分析複雜資料（如社會、經濟、環境資訊），偵測風險或受影響群體；生成式 AI 能整理利益相關者意見之共通主題；情境模擬則能測試不同方案對財務、運作或公平性之影響。這些工具減輕分析與預測之負擔，讓公務員能專注判斷、價值觀與協調合作，同時讓決策更有根據。

(6) 非生成式 AI 得幫助司法系統精準決策

統計模型、深度學習及預測機器學習等非生成式 AI 仍為司法系統數位轉型之重要基礎，且應用上較生成式 AI 合適。司法部現有之資料風險評估及資源分配工具，持續幫助判斷再犯風險與安排矯正方案。其他深度學習模型則協助評估監禁中之暴力風險或從非法通訊中擷取重要證據。司法部將持續監控、評估這些工具，並研究改進方法。

(7) 定期評估成效，靈活調整 AI 推行策略



本報告之智慧財產權歸屬於國發會

司法部將以明確之量化指標評估 AI 解決方案，包括對部門目標之影響、準確度、使用者滿意度、覆蓋範圍、節省時間以及投資回報。每個專案自最初即訂定指標，並持續透過 AI 監控團隊，必要時進行調整或擴大規模。

3. 投資 AI 技術人才及合作夥伴

(1) 吸引、培養及留住技術人才

司法部推出司法 AI 獎學金計畫，吸引專家加入，確保服務能運用最新研究與創新。同時招募專業技術人才，支援 AI 從試點到全面推廣。政府招募 AI 人才面臨薪資競爭與流程緩慢挑戰，司法部將與相關單位合作，推動更快招聘流程、競爭待遇及明確職涯，吸引並留住 AI 專業人才，包括技術與非技術角色。司法部亦將推出「司法 AI 學院實習計畫」，透過吸引頂尖畢業生參與實務挑戰，培養未來 AI 專家，並提供轉為正式職員之機會。

(2) 強化司法部所有員工之 AI 知識及技能

透過 AI 培訓，提升員工技能並加強跨部門合作。並配合宣導及 AI 大使支持，增進信任，確保 AI 負責任使用。

(3) 以員工為主導，積極推動 AI 工作轉型

司法部將與主管與工會合作，支援員工適應 AI 帶來之工作變化，推動培訓、工作再設計及鼓勵措施，確保 AI 為輔助而非取代人力。同時提供多元溝通管道，供員工分享意見與疑慮，參與 AI 之負責任運用及改進。

(4) 促進 AI 產業成長



本報告之智慧財產權歸屬於國發會

司法部致力支持 AI 創新，透過活動與合作強化與新創公司連結。計劃將開放高價值之資料集，透過國家資料庫提供予研究人員與企業，依據標準，創造優質研究與創新環境，加速與創新及改善司法成果。此外，將透過提供穩定政策框架，協助公部門資料之取得，推行彈性採購試行，協助本土 AI 公司成長。

(5) 與監管機構合作，推動法律界負責任之 AI 採用

AI 發展快速，可能超越現有法律規範，讓法律專業面臨不確定性。司法部將持續與法律監管機構合作，推動負責任之 AI 使用，並提供適當培訓。期許監管能保持彈性與科學依據，保障公眾信任與法治，同時支持創新發展。

4. 司法 AI 落實規劃

司法部之 3 大策略優先項目將在未來 3 年內同時推進，並採用「掃描—試點—擴展」之方式，持續調整完善路線圖，並與司法系統其他夥伴合作。

(1) 第 1 年（2025 年 4 月起）：建立基礎，提升能力，推動早期成果，如推出全系統之 AI 生產力工具，並試行聊天、搜尋、語音轉錄等專業應用。

(2) 第 2 年：擴大成功應用，將 AI 深植於轉型計畫中，讓前線服務與決策更有效率。

(3) 第 3 年：全面推動互通之 AI 解決方案，使 AI 成為日常運作核心，支援前線及後勤工作，連結完整資料，充分利用生成式 AI 之預測與決策輔助能力。

■ **資料來源：**

1. Ministry of Justice, AI action plan for justice, 2025-07-31,



本報告之智慧財產權歸屬於國發會

https://www.gov.uk/government/publications/ai-action-plan-for-justice/ai-action-plan-for-justice (last visited 2025/08/08)

2. babl, UK Ministry of Justice Unveils Landmark AI Action Plan, 2025-08-06, https://babl.ai/uk-ministry-of-justice-unveils-landmark-ai-action-plan/ (last visited 2025/08/08)

## 四、 澳洲

### (一)2025 年 10 月 21 日澳洲國家人工智慧中心發布《人工智慧政策指導與範本》

2025 年 10 月 21 日，澳洲國家人工智慧中心(National Artificial Intelligence Centre，下稱澳洲 AI 中心)發布《AI 採用指引》(Guidance for AI Adoption)，指引更新澳洲政府於 2024 年發布之自願性 AI 安全標準(Voluntary AI Safety Standard)並參考相關國際標準。澳洲 AI 中心持續過與產業界合作檢討後，將原先之 10 項防護原則(guardrails)精簡為六項關鍵實踐。而由於制定 AI 政策為 AI 治理之基礎，為協助組織撰寫 AI 相關政策，澳洲 AI 中心同時發布《AI 政策指導範本》(AI Policy: Guide and Template，下稱指導範本)，以提供機構於制定 AI 政策時之參考。該指導範本符合 AI 採用指引之內容，並透過範例文字以及完整涵蓋 AI 生命週期之政策制定範例，供機構參考並自行依其業務進行調整，以使其 AI 政策能反映機構之價值觀、產業標準及法律義務。

#### 1. AI 採用指引

AI 採用指引中含有六項關鍵實踐，為技術團隊以及非技術之決策者提供明確之指引。AI 採用指引分為基礎以及實作兩種，基礎指引提供剛開始採用 AI 治理之組機構，協助其將 AI 使用與其目標達到一致，理解 AI 治理以及管理風險；而實作指引則是提供深入技術指導，強化治理、改善監督並將



本報告之智慧財產權歸屬於國發會

負責任的 AI 融入系統、流程與決策中，適用於欲擴大 AI 採用或正在開發 AI 等較專業或較熟悉 AI 治理及高風險使用情境之機構。剛開始採用 AI、對 AI 治理尚未具有經驗或以低風險方式使用 AI 之機構得先參考基礎指引，後續得再參考實作指引獲得更詳細之逐步指導。

AI 採用指引之六項實踐分別為：設定責任、了解 AI 之影響並據此規劃、衡量及管理風險、分享重要資訊、測試及監控以及保有人類控制。

(1) 設定責任

AI 之複雜性可能導致無明確負責人之情形，故問責制為機構使用 AI 之第一步。機構應指派一資深領導人擔任 AI 治理之負責人，該負責人須有足夠決策權限並具備對 AI 能力及風險之理解，以監督機構內之所有 AI 使用。此外，應制定一份 AI 政策，當中說明機構如何負責任地使用 AI，並確保政策有向員工提供相關風險及管理建議。

(2) 了解 AI 之影響並據此規劃

AI 之高速運作可能放大其潛在影響，單一 AI 系統可能造成廣泛之負面效果，因此為能負責任地使用 AI，機構須了解、規劃並監控 AI 系統可能造成之影響。機構須進行利害關係人之影響評估，識別可能受 AI 系統影響之族群及類型，並評估潛在影響，如不公平決策及提供不準確資訊等。此外，須建立申訴管道，供利害關係人回報問題、挑戰 AI 決策或提出疑問。此類管道之強度應與 AI 可能造成之影響相符，並且亦應確保 AI 系統對個人造成負面影響時，機構能採取適當措施進行補救。

(3) 衡量及管理風險



本報告之智慧財產權歸屬於國發會

AI 風險將隨 AI 類型之複雜程度而有所變化，風險通常與 AI 系統之不同使用情境相關，故為能負責任地使用 AI，機構須能識別並管理相關風險。機構應建立風險篩選流程，識別並標記不可承受之風險或須額外治理關注之 AI 系統以及使用情境。

(4) 分享重要資訊

機構應告知使用者以及利害關係人何時以及將如何與 AI 互動，使用者或利害關係人應知道其正在與 AI 互動並能理解 AI 決策可能對其造成之影響。機構應建立並保有 AI 名冊，紀錄機構內部開發以及採購之所有 AI 系統、使用方式以及其他重要資訊。機構亦應公開其使用 AI 之狀況，明確向利害關係人說明機構使用 AI 之標準實踐方式。

(5) 測試與監控

因應 AI 系統可能隨時間改變或以較難以預測之方式運行，機構應持續測試以及監控 AI 系統。若機構內之 AI 系統為購買之系統，須向開發者或供應商要求提供 AI 系統已經測試之證明。於部署 AI 系統前，應先進行測試，並於部署後監控系統，機構須建立一間空流程，偵測 AI 系統之效能及運行變化。最後機構須將其資料治理以及資安實踐擴及至 AI 系統，以應對 AI 之特殊需求。

(6) 保有人為控制

為確保 AI 安全運作，機構應確保所使用之 AI 系統有適當之人類監督，並且監督者應要理解如何正確進行監督，及於系統出現異常時應採取何種措施介入或覆寫系統運作。人為監督應為有意義，確保人員以符合系統自主權



本報告之智慧財產權歸屬於國發會

及風險高低，低風險採用自動化監督，而於高風險決策強制人工審查。

2. AI 政策指導範本

因應 AI 採用指引中提及，AI 責任之設定為機構使用 AI 之基礎，而責任之設定須自制定機構之 AI 政策開始。故 AI 中心同時發布 AI 指導政策範本供機構於制定 AI 政策時作為參考。

(1) 目的

AI 政策應該從高層次之目標開始說明組織使用 AI 之策略性目標。指導範本建議機構於撰寫政策目的時得以列點之方式撰寫，以符合機構之 AI 策略目標。並且政策目的部分須包含版本資訊以及更新日期。

(2) 政策範圍

明確說明 AI 政策適用之範圍，範圍應與組織架構相符，並且反映預期之涵蓋範圍，如跨部門、職能或整個組織範圍。指導範本建議組織依據其架構以及實際需求，調整政策第一部分之內容及適用範圍。若修改 AI 政策中 AI 系統之定義，須確保修改後之定義仍能涵蓋可能之 AI 風險，如資料偏誤、可解釋性不足等，以符合政策之管理目的。指導範本中有提供簡化之 AI 定義，機構仍得修改成適合組織之定義。

(3) 政策聲明

政策聲明為 AI 政策之核心。該部分列出指導 AI 於組織中設計、採用及使用之原則與期望。指導範本以常見之 AI 倫理框架作為範例，惟組織應確保其政策聲明能反映



本報告之智慧財產權歸屬於國發會

組織之具體價值觀、行業標準、其他政策及法律義務並確保該聲明能轉化為實質行動。

指導範本之聲明範例內容如下：

A. 倫理與以人為本

AI 必須尊重人類尊嚴，不能操控或欺騙，並且最終決策仍須由人類負責。

B. 清楚問責

每個 AI 系統都有指定負責人，若涉及外部供應商，應明確劃分責任。

C. 風險與影響評估

評估上線前必須進行風險評估，並考量弱勢族群影響。

D. 品質、可靠性與安全

系統須經測試並持續監控，處理敏感資料之 AI 必須符合隱私與安全規範。

E. 公平與包容

AI 不得造成歧視，並應促進多元與可及性。

F. 透明與可申訴

若 AI 對人造成重大影響，應讓利害關係人知情，且 AI 系統須登錄在 AI 清冊中，決策紀錄可供查閱。

G. 人類監督與控制(Human oversight and control)



本報告之智慧財產權歸屬於國發會

AI 系統須可被人工暫停、覆寫或關閉，關鍵服務仍需保留人工備援流程。

(4) 治理與法遵

治理與法遵部分為說明關鍵政策內容，明確機構內之角色分工以及責任。並且亦應包含機構對 AI 使用案例之處理流程及對事故管理之處理方式。機構應依據其規模以及現有治理架構制定相關規則，規模較小之組織可能會需要由一人擔任多個角色。

(5) 新 AI 使用情境評估

任何 AI 使用情境都可能產生新風險。故機構應先記錄評估該些使用情境之方式以及流程，並可透過篩選工具協助於採行 AI 前完成相關評估。

指導範本中所提供之範例文字包含說明所有 AI 使用情境須進行篩選檢查，以識別治理方式以及確保 AI 使用是否可能構成無法承擔之風險，並且篩選過程會針對 AI 使用情境進行分類、產生結果決定風險評估、監督及批准之水準。機構得依據該範例文字撰寫其內部之規定。

(6) 事故管理

該部分係要求機構須說明其管理 AI 事故之方式，並且應與機構現有之事故管理框架整合。

依據指導範本中之範例，機構得撰寫如：任何涉及 AI 違規或事故都須向系統擁有者及/或監督者進行報告，並依照機構內之事故應對程序進行管理。機構將確保於必要時得將 AI 下線，並有文件化之手動程序作為備援以確保營運。



本報告之智慧財產權歸屬於國發會

(7) 政策審查

由於 AI 技術發展迅速，機構應制定明確之政策審查週期。指導範本建議機構得依其情境以及使用 AI 技術之變化速度，訂定審查之頻率以及條件。

指導範本舉例機構得於政策審查部分撰寫如：AI 政策須進行每年檢討，並得因重大 AI 相關事件、新興且有影響力之 AI 技術、相關法規調整等情形進行臨時檢視。

■ **資料來源：**


1. National Artificial Intelligence Centre, Guidance for AI Adoption, 2025-10-21, https://www.industry.gov.au/publications/guidance-for-ai-adoption#resources-and-downloads (last visited 2025/10/22)
2. National Artificial Intelligence Centre, Guidance for AI Adoption, 2025-10-21, https://www.industry.gov.au/publications/guidance-for-ai-adoption/guidance-ai-adoption-foundations| Department of Industry Science and Resources (last visited 2025/10/22)
3. National Artificial Intelligence Centre, AI policy guide and template, 2025-10-21, https://www.industry.gov.au/sites/default/files/2025-10/ai_policy_guide_and_template.pdf (last visited 2025/10/22)


五、 日本

(一)2025 年 6 月日本公平貿易委員會發布《關於生成式人工智慧報告 1.0》

2025 年 6 月日本公平貿易委員會(Japan Fair Trade Commission, JFTC )發布《關於生成式人工智慧報告 1.0》(About the Report Regarding Generative AI, Version. 1.0)，生成式 AI 為經濟及社會帶來許多益處，如提升企業生產力等，但同時亦存在各種風險，包含侵害著作權、假訊息之散播，以及網路攻擊等安全風險，從而擾亂社會秩序。自競爭



本報告之智慧財產權歸屬於國發會

法政策角度來看，其中一些風險被指出為潛在風險，例如開發生成式 AI 所需但近用受限之運算資源(computational resources)。有鑒於此，JFTC 展開市場研究，分析由徵求意見及聽證會等所蒐集的資料及意見，選出主要主題，提出具針對性之《關於生成式人工智慧報告 1.0》，旨在維護日本生成式 AI 市場公平自由的競爭環境、確保技術永續發展以促進創新，以及以健全的方式整合生成式 AI 以利經濟與社會等角度，了解生成式 AI 市場的實際情形。以下為本報告之重點整理：

1. 生成式 AI 的市場結構

(1) 基礎架構層(Infrastructure Layer)

A. 運算資源，如圖形處理器(Graphics Processing Unit, GPU)

於 GPU 市場，NVIDIA 的 GPU 於全球有相當大的占比，主要為開發環境及統一計算架構(Compute Unified Device Architecture, CUDA)等因素。隨著供應量增加，供需動態發生變化，於提供計算資源方面，尤其於訓練階段，NVIDIA 的 GPU 將可能持續維持其領導者的地位。另一方面，與訓練階段相比，受新興業者出現等因素所驅動，推理階段計算市場的競爭更為激烈，進而促使市場各廠商的創新。

B. 資料

對於資料的要求不僅關乎「數量」且關乎「品質」，取決於情況及用途。然而，目前難以判斷訓練資料分布不均是否會產生競爭優勢，需要多少日語資料才能訓練出高效能的日語模型，以及日語資料的可用性會帶來什麼影響，這些問題都需要持續密切監測。

C. 專業知識（專業人才)



本報告之智慧財產權歸屬於國發會

隨著生成式 AI 對專業技術人才的需求增加，國內外人力資源的競爭日趨激烈。於此情形下，大型科技公司以其財力及研發資源為後盾，期望於專業人力資源的競爭中佔有優勢。日本國內企業雖然面臨一些挑戰，如薪資水準低及缺乏研發資源等，然而亦有優勢，如容易訓練及招募當地人力資源。

(2) 模型層(Model Layer)

A. 大型語言模型(Large Language Models, LLM)的趨勢

LLM 由各公司自主研發，主要用於通用用途(general-purpose use)。日本國內公司已開發出通用 LLM，但開發此類模型須投入大量的計算資源、蒐集大量資料，以及投入大量專業的人力資源，並須長期耗費時間開發，故具有雄厚資金及技術能力之大型科技公司較佔有優勢。

另外，日本國內公司與新創公司亦有利用其他公司提供的基礎模型(如開源模型)，針對日語性能方面進行研究，或提高計算資源效率並適應特定用途（醫療、金融、法律、製造業等)，以此與大型公司開發之通用模型做出區別。有企業指出，擁有高效能基礎模型之大型科技公司，於發展專用模型仍具有優勢。

B. 生成式 AI 模型的其他趨勢

生成圖像、語音及影片等的生成式 AI 模型開發之競爭日益漸增。這些模型面臨著與 LLM 發展相同問題，亦觀察到此種模型有些特有情況，如圖像生成模型與 LLM 開發一樣需要大量計算資源，LLM 開發領域已有全球性科技公司（如 Google)，日本企業難



本報告之智慧財產權歸屬於國發會

以競爭，惟圖像生成模型開發領域尚未有佔據優勢之公司，且有大量的開放資料，因此日本企業於全球競爭並不困難。

生成式 AI 應用範圍已擴展，從 LLM 轉向多模態 AI (multimodal AI)，多模態 AI 能整合及處理文字、圖像、語音及影片等不同類型資料，預計將其應用擴展至醫學、藥物研發、教育、娛樂等領域，並提升其在推理及分析等通用任務(general tasks)的處理能力。多模態 AI 及其相關產品的競爭將加劇，進而推動生成式 AI 市場的成長。

C. 模型開發方法

生成式 AI 於高度精確技術背後，面臨需要大量的模型、參數及計算資源的挑戰。為了能於資源受限的環境中運行，須縮小模型體積並提高推理效率，使用以下方法，以解決此問題：

a. 提煉(Distillation)，指將預先訓練的生成式 AI 模型所學到的豐富知識移轉至另一個更小、更有效率的生成式 AI 模型的方法。預先訓練的生成式 AI 模型通常需要大量的參數及計算資源，而經過提煉的生成式 AI 模型得在低成本及加速推理的環境中，達到與預先訓練的生成式 AI 模型相同或接近的效能，故經過提煉的生成式 AI 模型為被廣泛應用的最佳方法。

b. 混合專家模型(Mixture of Experts, MoE)，指將單一大型模型分解成多個「專家」子網路(subnetworks)，並對每個輸入選擇最適合的專家來產生輸出的方法。此方法可降低生成式 AI 模型的訓練及推理相關的計算成本，並擴大規模、降低功耗及提高速度。透過此機



本報告之智慧財產權歸屬於國發會

制，每位專家得專注研究於輸入的特定領域或特徵，於維持整體高表現力時，得減少計算量。

(3) 應用層(Application Layer)

A. 應用層市場趨勢

日本從大型科技公司到新創企業，皆提供了各式各樣的生成式 AI 產品，並為滿足多樣化的用戶需求，競爭日益漸增。包含內部及外部使用的聊天機器人、搜尋系統、文字生成、圖像生成及語音生成，且已商業化並投入市場。

B. 與現有數位服務的功能整合(integration)

生成式 AI 產品與現有數位服務（如搜尋服務、雲端服務或社群網路工具等）的功能整合趨勢正在興起。大型科技公司透過數位服務，於特定市場及領域佔據優勢地位。生成式 AI 產品與現有數位服務間的功能整合，可能提升現有數位服務的競爭力並進一步鞏固其市場地位。

C. AI 代理(AI Agent)[9]

近年來，AI 代理成為備受關注的新興技術，現已有能力取代部分或全部日常流程任務。被賦予角色或具體人格特質之個人代理 AI，也正投入實際應用。於日本，AI 代理服務正在被引入，用以提升業務效率及創建新商業模式擴張。

[9] AI 代理，指有能力自主運作及不須人類介入之 AI 系統。其特點為得連接及操作現有的 IT 系統，以及確定特定任務所需的操作自主運作，使特定任務的元件精簡模型(Compact Model)更易於使用。



本報告之智慧財產權歸屬於國發會

(4) 其他超越層級的生成式 AI 特定議題與考慮因素

A. 雲端服務

由於生成式AI模型及生成式AI產品的開發者主要局限於大型科技公司及其他擁有大量運算資源的大型企業，因此許多企業都從提供生成式 AI 雲端服務的企業取得 GPU 及其他高效能晶片。外國雲端服務企業，尤其為大型科技公司，以其雄厚的資金確保運算資源，並提供針對生成式 AI 開發最佳化的雲端服務，由於營運這些雲端服務的資料中心以及處理所產生的大量熱能的冷卻系統須大量資金，故外國雲端服務企業之GPU雲端服務於日本持續擁有高市占率。

B. 開發環境的轉換及遷移

於開發生成式 AI 模型時，開發環境之變更不易，如硬體或雲端環境的變更，因重建整個系統、重新導入軟體及遷移資料等，皆須成本與時間。雖然轉換雲端提供者於技術上是可行的，且涉及轉換成本，但目前難以確認是否會構成障礙，這個問題仍需要密切監測。

C. 開源/閉源(Open source/closed source)

生成式 AI 模型產品分為兩種類型

a. 開源：開源模型被預期透過降低開發及使用生成式 AI 產品的進入門檻以確保競爭環境，尤其是針對難以負擔高成本的新進入者與新創企業。此外，因其開放之特性，任何人都可進入檢查及修改，促進了安全問題之驗證及技術進步。然而其缺點在於因技術規格



本報告之智慧財產權歸屬於國發會

(technical specifications)開放，事業可能難以維持競爭優勢，易於使用有可能導致被惡意利用的風險。

b. 閉源：由於技術規格未揭露，事業與研究機構可獨立管理與限制生成式 AI 的使用，得降低遭第三方濫用風險，缺點為可能阻礙創新，以及技術缺乏透明度。

D. 合作關係(Partnership)

於生成式 AI 市場中，日本正積極於國內外建立跨層次合作關係，此類合作關係得為開發生成式 AI 模型的新創公司帶來益處並提升競爭力，如透過投資取得開發資金、於生成式 AI 市場取得開發資源，以及取得相關技術。合作關係亦會使大型科技公司與其他於數位市場擁有優勢地位的公司，提升自身於生成式 AI 市場的地位，或削弱競爭。

2. 生成式 AI 的《公平交易法》(Antimonopoly Act)及競爭政策問題

(1) 近用限制與排除競爭者

開發生成式 AI 時所需之 GPU 及資料目前都集中於大型科技公司，於此情形下，如果實施近用限制或排除競爭者，將剝奪其他競爭者進入市場的潛力，進而影響競爭。

(2) 搭售(Tying)

如果於某項服務上具有領導地位的企業，使用自己的 AI 模型作為提供該服務的條件，可能影響 AI 模型的競爭。

(3) 其他問題

A. 自我偏好(self-preferencing)



本報告之智慧財產權歸屬於國發會

如果提供生成式 AI 模型的企業於開發模型時，於推斷結果上對自己的商品及服務比對其他商品及服務更為優待，則影響商品及服務的競爭。

B. 使用生成式 AI 為平行行為(parallel conduct)

儘管價格競爭會因生成式 AI 的價格調查(price surveys)而增加，但共同使用潛在(underlying)資料及演算法可能會導致相同或類似的定價策略、生產目標等，進而影響競爭。

C. 透過合作獲取專業人才

如果合作關係之目的為獲取專業技術人才，且該合作關係產生的效果與業務轉讓效果相似，則可能會影響競爭。

3. JFTC 的未來行動

對於生成式 AI 市場中可能的負面影響，JFTC 將積極與相關部門及機關密切協調與合作以確保競爭環境之公平。於生成式 AI 市場中，部分競爭實體的營運規模遍及全球，JFTC 將持續與各國及地區之競爭主管機關進行意見交流，並利用國際競爭網路(the International Competition Network, ICN)及經濟合作暨發展組織(OECD)等論壇，持續與外國相關主管機關合作，以改善競爭環境。

本報告非本市場研究的最終報告，JFTC 將持續密切監測生成式 AI 市場，並持續於 JFTC 網站徵求廣泛的資料與意見。於生成式 AI 市場中，影響市場結構的變化與技術創新每日都在發生，未來市場環境亦可能發生劇烈變化，故掌握市場趨勢極為重要。JFTC 將持續進行市場研究，希望於公平、自由競爭的環境下，持續發展生成式 AI 市場。



本報告之智慧財產權歸屬於國發會

■ **資料來源：**

1. Japan Fair Trade Commission, About the Report Regarding Generative AI, Version. 1.0 , 2025-06-06, https://www.jftc.go.jp/en/pressreleases/yearly-2025/June/250606.html (last visited 2025/07/07)

### (二)2025 年 5 月日本通過《人工智慧相關技術研究開發及應用推動法》

2025 年 5 月 28 日，日本參議院通過《人工智慧相關技術研究開發及應用推動法》(人工知能関連技術の研究開発及び活用の推進に関する法律，下稱日本 AI 法)，為日本為推動 AI 之研發以及運用基本政策所定之法律。

日本 AI 法於第 1 條說明目的：鑑於 AI 技術是日本經濟社會發展的基礎技術，該法就推動 AI 相關技術研發及運用之相關政策，制定基本原則及 AI 相關技術研究開發及利用推動之基本計畫等事項。此外，政府將設置人工智慧戰略本部，並結合科學技術・創新基本法（科学技術・イノベーション基本法，平成 7 年法律第 130 號）及數位社會形成基本法（デジタル社会形成基本法，令和 3 年法律第 35 號）等相關法律措施，旨在達成推動 AI 相關技術之整體研究開發及利用及計畫，從而改善國民生活、確保國民健康的經濟發展。

目前頒布共 2 章 17 條（總共為 4 章 28 條，目前頒布第一章、總則及第二章、基本措施)，剩餘 2 章（第三章、基本規劃及第四章、人工智慧戰略總部）還在進行討論及制定中，預計於 2025 年底頒布。以下為此法之重點整理：

1. 已施行之部分：

第一章、總則（第 1 條至第 10 條）



本報告之智慧財產權歸屬於國發會

(1) 定義

本法所定「AI 相關技術」係指為實現以人工方式取代人類認知、推論及判斷等智力能力功能所需之技術，及為實現該技術處理輸入資料，並輸出結果之功能所需之資料處理系統相關技術。

(2) AI 之發展與政府責任

中央政府負責全面、系統性地制定及實施與促進 AI 相關技術研發及利用相關措施，也應積極推動行政機關運用 AI 技術。地方政府有責任制定並實施結合地方政府所在地區特點的自主措施。

(3) AI 的發展與研究機構的責任

大學、《科學技術和創新創造活性化法》第 2 條第 9 款規定之研究開發公司，以及進行 AI 相關技術研究及開發之其他組織，應積極致力於 AI 相關技術研發、成果傳播，並培養具有專業和廣泛知識之人才。政府於制定相關政策時，除努力激發研究機構關於 AI 領域的研究亦須尊重研究人員之自主。研究機構也應發展跨領域及綜合性的研究。

(4) AI 發展與事業經營者之責任

欲開發或提供利用 AI 相關技術之產品或服務者，或其他有意於其事業活動中運用 AI 相關技術者，應依基本原則，積極透過 AI 相關技術之運用，提升業務活動之效率及精密化，並促進產業創新。

(5) AI 發展與個人責任



本報告之智慧財產權歸屬於國發會

國民需加深對 AI 相關技術的理解及興趣，並遵守國家所實施有關 AI 之規範。

第二章、基本措施（第 11 條至第 17 條）

(1) 促進研發：

政府應推動 AI 相關技術基礎研究至實用化研究之一致性研發，建立研究機構內部成果移轉體系，並提供 AI 研發成果相關資訊及必要措施。

(2) 保障措施：

為保障 AI 相關技術之研究、開發及利用，應依據國際標準，規劃適當的保護措施。

(3) 人才管理：

中央及地方政府、研究機構及利用 AI 之企業應密切合作，針對自 AI 相關技術基礎研究至國民的生活及經濟活動中應用各個階段，採取必要措施，確保、培養提升所需專業及廣泛知識之各領域人力資源。

(4) 國民教育：

政府應採取必要措施，如教育學習、公共活動等，教育國民關於 AI 的相關技術，加深國民對於 AI 之理解及興趣。

(5) 風險因應：

政府應蒐集有關日本或海外 AI 技術研發相關資訊及動向，分析因非法目的或不正當研究方法利用 AI 技術而侵害公眾權利之案件，以制定因應對策，並進行有助推動



本報告之智慧財產權歸屬於國發會

國內 AI 技術開發之調查及研究。並依其結果對研發機構、企業等，提供建議及指導。

(6) 國際接軌：

政府應提供 AI 研究機構有關 AI 之國際規範、符合國際規範的正確指導，促進研究機構與國際合作、參與國際規範制定，並促進與國際間之合作。

2. 尚未施行之部分：

第三章、基本規劃（第 18 條）

政府應依據本法條上述之準則制定推動發展 AI 之計畫。

第四章、AI 戰略總部（人工知能戦略本部）（第 19 條至第 28 條）

(1) 成立宗旨：

為全面推動有關 AI 之研究，並執行「AI 基本計畫」，政府成立「AI 戰略總部」，作為最高指揮單位。

(2) 組織：

總部成員有總部長、副總部長及成員，成員由所有的國務部長所組成。總部長由總理任命。

■ **資料來源：**

1. E-GOV, 人工知能関連技術の研究開発及び活用の推進に関する法律, 2025-06-04, https://laws.e-gov.go.jp/law/507AC0000000053?tab=cited#Mp-Ch_2 (last visited 2025/07/18)

2. note, 日本の AI 法案の全文をみてみよう！～「人工知能関連技術の研究開発及び活用の推進に関する法律」→2025/6/4 施行,



本報告之智慧財產權歸屬於國發會

2025-03-31, https://note.com/informationlaw1/n/nea72aa2e6b7e?utm_source (last visited 2025/07/18)

3. 国際航業株式会社, AI 推進法とは？（人工知能関連技術の研究開発及び活用の推進に関する法律, 2025-06-04, https://www.enegaeru.com/aipromotionact?utm_source (last visited 2025/07/18)

4. 知产财经官网, 附译文下载┃日本通过首部人工智能法案, 2025-05-30, https://www.ipeconomy.cn/kechuang/9459.html?utm_source, (last visited 2025/07/18)

## 六、韓國

### (一)2024 年 12 月韓國科學技術情報通訊部發布國會通過《關於人工智慧發展及建立信任基礎之基本法案》

2024 年 12 月韓國科學技術情報通訊部（Ministry of Science and ICT，下稱 MSIT）發布國會通過《關於人工智慧發展及建立信任基礎之基本法案》簡稱《AI 基本法》(인공지능 발전과 신뢰 기반 조성 등에 관한 기본법안,AI 기본법)。隨著科技發展 AI 成為決定國家經濟及安全之關鍵，各主要國家為推動 AI 創新及建立國際 AI 領導地位陸續制定利於國家之相關法規。韓國考慮到經濟及社會情形，認為應制定基本法提升國家 AI 競爭力，為可信賴之 AI 應用奠定基礎，因此推動頒布《AI 基本法》。《AI 基本法》於 2020 年 7 月提出，歷經四年討論及蒐集各方意見，於第 22 屆國會達成協議，經過科學技術、資訊、廣播與通訊委員會及法律事務委員會審議後，全數通過。

下為《AI 基本法》之重要內容：

1. 建立促進國家 AI 發展體制之信任基礎體系



本報告之智慧財產權歸屬於國發會

(1) 制定 AI 基本計畫：MSIT 部長蒐集相關部會及地方政府之意見，每 3 年制定並實施國家 AI 基本計畫，以提升國家 AI 競爭力，內容包含 AI 政策基本方向、培養專業人才、建立信任基礎等相關事項。

(2) 成立國家 AI 委員會：審議並決定關於促進 AI 產業發展之主要政策相關事項。委員會得向機關部會首長及 AI 事業提出意見及法令或制度之建議。

(3) 設立 AI 安全研究院：為專業且有效地保護公民生命、身體及財產免於 AI 可能引發之相關風險，並維護 AI 安全信賴基礎而設立之專門組織。

2. 促進 AI 技術開發及產業發展

(1) 政府協助建立 AI 產業基礎建立。包括支援 AI 技術研究開發、標準化、學習資料政策的制定。

(2) 促進 AI 技術開發。包括支援 AI 推行與運用、專業人才保障、努力促進中小事業參與 AI 產業、促進創業及產業整合、培育及吸引人才及國際合作等。

(3) 產業活化機制。指定 AI 集中園區、促進 AI 資料中心政策及促進 AI 融合以支持 AI 生態系統之創新發展。

3. AI 倫理及可信賴性之確保

(1) 政府應廣納社會各界意見，確立 AI 倫理原則，確保 AI 安全性及可靠性驗證。

(2) 為遵守倫理原則，AI 研究機構、AI 事業者、其他與 AI 技術相關之機構得設置民間自律 AI 倫理委員會。



本報告之智慧財產權歸屬於國發會

(3) 確保 AI 透明度義務：AI 經營者使用高影響力 AI 或生成式 AI 提供產品或服務時，須先告知用戶；於提供產品或服務時，須表明係由生成式 AI 所創建之結果；於 AI 系統提供與現實難以區分之虛擬結果時，須告知或標示使用戶清楚知悉。

(4) 確保 AI 安全性義務：為確保 AI 系統之安全，用於學習之累積計算量超過法規範標準，AI 服務提供者須為風險識別、評估及緩解等事項。

(5) 高風險 AI 之相關事業者之責任：AI 事業者提供高風險之 AI 或使用 AI 之產品及服務時，須採取措施確保安全可靠。

(6) AI 影響評估：AI 事業者使用提供高風險 AI 產品或服務，須事先評估 AI 對於基本權利之影響。國家機關使用具有高風險之 AI 產品或服務，須優先考慮已為影響評估之產品及服務。

《AI 基本法》於 2024 年 12 月通過後於 2025 年 1 月公布，並將於 2026 年 1 月生效。

■ **資料來源：**


1. Ministry of Science and ICT, 인공지능 시대의 새로운 서막, AI 기본법 국회 본회의 통과，2024-12-26，https://www.msit.go.kr/bbs/view.do?sCode=user&mId=307&mPid=208&bbsSeqNo=94&nttSeqNo=3185321 (last visited 2024/12/30)

2. KBS, ‘AI 기본법’ 국회 본회의 통과…2026 년 1 월 시행, 2024-12-26, https://news.kbs.co.kr/news/pc/view/view.do?ncd=8139129 (last visited 2024/12/30)

3. Chosun Biz, Korea passes AI Basic Act, second globally, 2024-12-26, https://biz.chosun.com/en/en-it/2024/12/26/66W2Z3RX6FE7FMPXMR73T26SKY/ (last visited




本報告之智慧財產權歸屬於國發會

2024/12/30)

4. 법률신문,「AI 기본법」개정안의 주요 내용과 시사점, 2024-12-19, https://www.lawtimes.co.kr/LawFirm-NewsLetter/203936 (last visited 2024/12/30)

### (二)2025 年 11 月 12 日韓國科學技術情報通訊部發布《關於人工智慧發展及建立信任基礎之基本法案施行令（草案）》

2025 年 11 月 12 日，韓國科學技術情報通訊部發布《關於人工智慧發展及建立信任基礎之基本法案施行令（草案）》，為了支持 AI 之健全發展，並建立 AI 社會之信任基礎，保護國民之權利，提高生活品質與國家競爭力，依據《關於人工智慧發展及建立信任基礎之基本法案》制定此施行令，以具體規定該法所委任事項及其執行所需之細節。

1. 適用範圍（第 2 條）

本施行令適用之 AI，係指僅用於以下業務之 AI 系統（由韓國情報化振興院長、國防部長或警察廳長指定）：

(1) 由韓國情報化振興院長指定之業務：

A. 經濟安全供應鏈預警系統。

B. 國安保密研發任務管理。

C. 資源與能源安全之網路防禦體系。

D. 情報及反恐、防諜業務等。

(2) 由國防部長指定之業務：

A. 國防資訊化建設與管理。

B. 武器及支援系統之開發與運用。



本報告之智慧財產權歸屬於國發會

(3) 由警察廳長指定之業務：

A. 國家尖端戰略技術外洩防制調查。

B. 反恐及國防產業技術保護相關偵查業務等。

2. 國家人工智慧委員會

(1) 第 3 條（AI 基本計畫之制定與變更）

A. 若僅為小幅度修改如錯誤修正、機構變更或法律修訂反映，可不經委員會審議。

B. 計畫制定或修改後，應公告於韓國科學技術情報通訊部網站，並通知各中央行政機關及地方政府。

(2) 第 4 條（委員會之組成）

由主要中央部長組成，含財政部、教育部、外交部、國防部、產業部、就業及勞動部、中小企業部等 13 位官員。委員資格可因職務不適任、品格損害等原因被解除。

(3) 第 5 條（委員會經營）

得聽取專家意見、要求資料、進行研究或舉辦公聽會等。

(4) 第 6 條（支援團）

設支援團長 1 名，由委員主席指定，負責執行委員會業務與協調中央機關人員派遣。

(5) 第 7 條（改善建議之履行）

接獲委員會建議之國家機關、公營機構，須在 3 個月內提出改善方案並回報。若難以在期限內完成，可申請延長。



本報告之智慧財產權歸屬於國發會

(6) 第 8 條（分科及特別委員會）

委員會下設「分科委員會」、「特別委員會」、「顧問團」及「AI 責任官協議會」。顧問團由約 20 名 AI 專家組成，協議會由各部次級官員參加。

3. AI 政策與安全機構

(1) 第 9 條（人工智慧政策中心指定）

可指定下列機構為「人工智慧政策中心」:

A. 韓國智慧信息社會振興院。

B. 大學附屬研究所。

C. 公共機關。

D. 政府出資研究機構。

E. 經認可之 AI 非營利法人。

(2) 第 10 條（AI 安全研究所經營）

研究所可執行業務包含 AI 安全諮詢與培訓、安全評估系統建構、資料安全蒐集與分析、統計與資訊共享。並得要求國家機關提供資料或派遣人員支援。

4. AI 技術與資料支援

(1) 第 11 條（AI 技術開發與安全應用支援）

包含 AI 研發基礎建設、國際合作、及其他必要支援事業。

(2) 第 12～14 條（學習用資料支援及統合系統）



本報告之智慧財產權歸屬於國發會

支援項目包含 AI 學習資料生產與加工技術、資料蒐集、管理與流通、法律制度研究與標準契約開發。

5. AI 技術導入與產業發展

(1) 第 15 條（AI 技術導入與應用支援）

包含資訊提供、教育訓練、基礎設施建設等，並得與地方自治團體共同推動。

(2) 第 16 條（國際合作與海外市場支援）

中央機關可委託具 AI 國際合作經驗之機構代辦，並公告委託事項。

(3) 第 17 條（AI 綜合園區指定）

指定標準包含是否符合基本計畫、區域整合效果、就業機會創造、重複性與連結性等。並須經委員會審議與公告。

(4) 第 18 條（園區專責機構）

必須符合為公營機構或地方出資法人、具專業人員 10 人以上、位於園區附近、有辦公設施與資訊系統等條件，且須每年報告計畫及預算。

(5) 第 19 條（AI 驗證基地設立）

開放之實驗設施可由公營研究院、大學、地方公營機構提供。韓國科學技術情報通訊部須公開設施種類、使用條件與費用。

6. AI 安全與透明

(1) 第 21 條（AI 安全性與信賴性認證支援）



本報告之智慧財產權歸屬於國發會

支援項目包含驗證認證標準與培訓、品質診斷、國際合作等。政府得補助中小企業檢驗與認證費用。

(2) 第 22 條（透明性義務）

業者於提供 AI 產品或服務時，須以明確方式告知 AI 使用者：

A. 可於合約、說明書、說明介面或公告場所標示。

B. 若為生成式 AI，須提供至少一次提示訊息或語音說明。

C. 須考慮使用者之年齡與身體條件。

D. 內部用途或明顯可辨之情況可豁免。

(3) 第 23 條（安全性確保義務）

適用對象為訓練運算量超過 $10^{26}$次浮點運算之 AI 系統。具體運算量計算方式由韓國科學技術情報通訊部公告。

(4) 第 24～25 條（高影響 AI 之確認程序與專門委員會）

業者得申請確認是否屬高影響 AI。韓國科學技術情報通訊部須於 30 日內答覆，可延長一次。業者若不服結果得於 10 日內申請再確認

(5) 第 26 條（高影響 AI 業者之責任）

業者須執行風險管理、說明義務、使用者保護等措施，並保存文件 5 年。並須於網站公開主要政策、聯絡人等（營業秘密除外）。

(6) 第 27 條（高影響 AI 影響評估）



本報告之智慧財產權歸屬於國發會

內容包括受影響基本權之識別、社會經濟影響、使用行為、風險預防與改善計畫等。業者得自行或委託第三方實施。

7. 監督與罰則

(1) 第 28 條（國內代理人指定）

適用對象：

A. 營收超過 1 兆韓元。

B. AI 服務營收超過 1 百億韓元。

C. 平均日用戶超過 1 百萬人。

D. 因違法造成安全事件者。

(2) 第 29 條（實態調查與統計）

調查範圍包含 AI 產業現況、企業營收、人力資源、研究動向、投資與法律趨勢等，並需於網站公開。

(3) 第 30 條（業務委託）

韓國科學技術情報通訊部可將部分職權委託給公共機構或 AI 協會，包括 AI 產品開發支援、啟動資料中心、產業調查、倫理推廣等。亦可委託 AI 安全研究所執行高影響 AI 審查事務。

■ **資料來源：**


1. Ministry of Science and ICT, (과학기술정보통신부 공고 제 2025-1000 호) 「인공지능 발전과 신뢰기반조성 등에 관한 기본법 시행령」 제정안 입법예고, 2025-11-12, https://reurl.cc/eVmgXb (last visited 2025/11/13)
2. Dailysecu, 과기정통부, 인공지능 기본법 시행령 입법예고… “AI 산업 성장 지원과 보안·안전성 강화 병행 추진”, 2025-




本報告之智慧財產權歸屬於國發會

11-12,
https://www.dailysecu.com/news/articleView.html?idxno=202311
(last visited 2025/11/13)

# 陸、 小結

## 一、 國際趨勢總結分析

隨著 AI 之快速發展，各國之法制政策於近兩年內持續修正。本案延續去年 AI 著作權、AI 消費者保護、AI 勞工權益保護、AI 個資保護之焦點議題之更新政策發展。整體而言，各國均力求平衡 AI 所帶來的創新效益與潛在的倫理、安全等風險。在技術面要求更多的透明度與人類控制，在治理面採取風險分級和國際協調的方式。相關議題聚焦於建立更具針對性的風險分級和特定應用監管、將 AI 基礎設施和人才培育納入國家發展政策、提升訓練資料來源的透明度、加強要求 AI 系統（如聊天機器人）的身分揭露、保護有人類創作貢獻的人機協同著作、避免 AI 自動決策系統影響消費者和勞工權益、針對高風險 AI 與自動化決策技術提升個資隱私之監管、擴大 AI 系統產品責任範圍，以在推動 AI 發展的同時，有效地應對隨之而來的社會和法律挑戰。總結觀測說明如下：

### (一)AI 著作權法制發展

AI 創作的著作權保護取決於人類創作性的貢獻程度，於國際間已形成共識，即單純輸入 AI 指令缺乏人為控制，其生成內容不受著作權保護。同時，美國、歐盟、英國已逐步以法令或政策表態要求 AI 開發者應提高訓練資料來源的透明度，減輕權利人對其作品被用於模型訓練的擔憂。此外，如歐盟、韓國亦透過發布指引或實踐準等軟法(行政指導)方式，協助產業在現有法律框架有效揭露與預防潛在的著作權爭議。



本報告之智慧財產權歸屬於國發會

但在 AI 訓練是否構成「合理使用」方面，各國態度仍未一致。美國聯邦法院在司法案例中裁定 AI 訓練具有高度轉化性，屬於合理使用，但前提是資料來源須合法。相較之下，歐盟則側重於透過「通用人工智慧實踐準則」要求通用 AI 模型提供者遵守著作權及 TDM 限制，例如在網路爬取資料時應尊重付費牆等技術措施。英國則傾向透過修法建立一個允許著作權人保留權利並以透明度為基礎的資料探勘例外規定，以平衡創新與報酬。此外，在輸出內容的透明度表示及標示的條件、實作方式，各國的要求或期待亦已各自逐漸細部展開：

1. 美國就 AI 相關著作權法制發展上，以立法搭配司法案例並行之策略，重點仍聚焦於訓練資料之合理使用與透明度。美國新增行政傳票程序，期待透過修法使權利人向地方法院聲請，以傳票要求 AI 開發商或部署者揭露其作品被用於 AI 模型訓練之資訊，同時提升 AI 模型開發者對著作權保護之透明度責任。在運用 AI 創作之作品是否得受著作權法保護，美國著作權局強調現行法律已明定僅「人類創作之作品」可受保護，而簡單之 AI 指令輸入缺乏人為控制不受著作權保護。在 AI 訓練是否構成合理使用議題上，美國聯邦法院判決認定，大型語言模型訓練過程是具有高度轉化性 (quintessentially transformative) 的，屬於合理使用，因其目的並非單純複製或取代原作，且不會削弱原作品的市場需求。

2. 歐盟針對通用 AI 模型提供者應遵守著作權及透明度之義務，建立上下游間法遵政策與實踐之措施。更為重要的是，歐盟要求在網路爬取資料時必須遵守文字與資料探勘之限制。此外要求簽署方採取適當之保護措施，減緩模型輸出侵害著作權之風險，並提供權利人相應之救濟管道。

3. 英國於今年之發展著重於促進 AI 創新與著作權益保護之平衡。從去年英國智慧財產局提出之諮詢文件，有意採用允許著作權人保留其權利並以支持透明度之作法為基礎資料探勘



本報告之智慧財產權歸屬於國發會

之例外規定。此諮詢旨在消除法令模糊性，讓 AI 開發人員得以使用合法資料進行訓練，而著作權人則可透過授權協議獲得報酬。更進一步於今年通過之 DUAA 新增對 AI 商業資料之透明度規範，要求與英國相關之 AI 模型提供者，必須提供有效機制，使著作權人得以識別作品被 AI 模型所訓練。

4. 韓國主要透過指引之方式協助預防潛在之法律爭議。其將作品區分為生成式 AI 應用作品以及生成式 AI 生成之作品，即區分是否有人類創作貢獻性，若僅依提示詞生成，未有人類思想或情感則非著作權所保護之著作。指引建議著作權人可透過明示反對或使用相關技術防止其著作被用於訓練。同時對於 AI 服務業者，建議可透過服務條款明確界定責任歸屬，並採取必要措施避免侵害他人著作權，例如事先與著作權人簽訂授權契約。

5. 中國之趨勢發展在於建立網路服務 AI 生成內容標示規範的操作，要求網路諮詢服務提供者對 AI 生成合成內容實施顯式表示及隱式標示。顯式標示要求在文字、音訊、圖片、影片等不同類型內容的開頭、結尾或互動介面上，以明顯方式提示用戶該內容為 AI 生成。隱式標示則是透過技術手段，將標示（如服務提供者名稱、內容編號等）嵌入於生成內容檔案的中繼資料 (metadata) 中。該辦法也規範了服務提供者須在用戶協定中說明標示方法及規範，並要求對提供無顯式標示內容的申請進行記錄保留。

(二)AI 消費者保護法制發展

隨著人工智慧技術深入日常消費場景，AI 與消費者的互動日益頻繁。為保障消費者權益，各國法制在 AI 消費者保護領域聚焦於強化互動透明度、落實反歧視原則以及針對高風險領域的監管。



本報告之智慧財產權歸屬於國發會

關於強化透明度，各國多認為消費者有權知道他們正在與誰互動，以避免消費者被擬人化的 AI 技術誤導或欺騙，例如美國夏威夷州的立法提案「關於 AI 法案」為例，該法案針對從事商業交易的公司設下明確義務：當消費者與聊天機器人進行互動時，必須「事先」以「明確且顯著」的方式，揭露該消費者正在與 AI 聊天機器人或模仿人類行為的技術進行互動。韓國在其關於人工智慧發展及建立信任基礎之基本法第 22 條規定業者於提供 AI 產品或服務時，所須告知 AI 使用的資訊與方式，包括：可於合約、說明書、說明介面或公告場所標示、若為生成式 AI，須提供至少一次提示訊息或語音說明、須考慮使用者之年齡與身體條件、內部用途或明顯可辨之情況可豁免。

在 AI 演算法可能產生的偏見與歧視的問題上，各國傾向於利用既有的消費者保護法與民權法框架來應對。例如：美國俄勒岡州發布的指引認為如果事業體利用 AI 進行不實陳述，例如聊天機器人謊稱自己是真人，或者是利用 AI 大規模發布「虛假產品評論」，這些行為都將被視為違反該州的非法交易行為法（OUTPA），將 AI 的違規行為納入傳統欺詐與不公平交易的監管範疇，嚴格禁止 AI 成為歧視或欺詐的工具。

對於 AI 造成損害的高風險領域與責任制度，歐盟透過修訂「新產品責任指令」（PLD），將產品責任的適用範圍大幅擴張。該指令明確將「所有類型的軟體」，包括作業系統與 AI 系統，納入產品責任的規範對象。更具突破性的是，歐盟將「資料破壞或毀損」納入可請求賠償的損害類型。如果 AI 系統導致消費者的重要資料遺失或損壞，製造商必須承擔賠償責任。而針對特定具有心理或情感影響的高風險應用，美國也有針對性規範。例如美國紐約州特別關注「AI 伴侶」的風險，要求此類系統的經營者必須為使用者提供緊急心理危機的諮詢服務機構資訊。

總結來說，各國皆致力於提升透明度與反歧視，但在監管架構上，歐盟則致力於構建一套統一、全面且具有最高強制力的法規體系，增



本報告之智慧財產權歸屬於國發會

訂瑕疵產品責任指令，將軟體之責任範圍擴大。而美國則依賴各州的分散立法與特定領域的指引。美國雖未有聯邦層級之法制規範，各州仍在現有法律框架下納入監管機制或使用風險指引，協助保護消費者權益。

(三)AI 勞工權益保護法制發展

針對 AI 勞工權益保護，聚焦於防止 AI 或演算法在重大就業決策，例如聘雇、晉升、薪資確定和解僱中，產生偏見或歧視並加強透明度、人工監督、風險管理為核心的共通趨勢。例如美國聯邦政府發布指導文件，將雇主依據消費者報告進行招聘、晉升及就業決策造成偏見或歧視的問題，納入「公平信用報告法」（FCRA）的監管範圍，要求雇主遵循通知與許可要件。例如美國聯邦相關機構（如 CFPB 和 EEOC）的指導文件指出雇主不得利用穿戴式裝置的數據來推斷員工的受保護特徵（如懷孕或更年期），並以此做出不利的就業決策。同時，EEOC 特別關注與健康相關的數據蒐集，對於工作場所使用穿戴式裝置蒐集健康或生物特徵資訊，提醒雇主強制要求員工使用穿戴式設備蒐集健康相關資料，可能構成 ADA 嚴格限制雇主對員工為與身心障礙相關之詢問或健康檢查。

在各州政府層面就自動化決策系統或 AI，被用於就業領域如聘僱、績效、薪資及解僱等重大決策，如何避免演算法歧視，並保障勞工權益等，提出多項監管法案、建議、相關規範文件。例如德州眾議員提出 HB 1709 法案，要求高風險 AI 系統的部署者應每半年完成高風險 AI 系統之影響評估，或於進行實質性修改後 90 日內完成影響評估，並須立即暫停使用不符規定的系統。紐澤西州的「演算法歧視指引」明確指出，雇主對演算法歧視負有責任，即使自動決策工具由第三方開發，亦不能免除實體責任。加州民權理事會發布的就業法規修正建議，要求雇主使用 ADS 為人事決策時，應負較高之舉證責任，證明已執行反偏見測試或類似積極措施以防止非法歧視。而各州立法也在積極推動透明度義務，例如加州有議員提出「自動決策安全



本報告之智慧財產權歸屬於國發會

法案」詳細列出部署者應揭露 AI 在重大決策中所扮演的角色、提供更正不正確個人資料、第三方稽核、透明度要求等義務。

綜上，僅管防止 AI 歧視勞工是共通方向，美國聯邦政府主要係以「指導文件」提供方向，而各州政府則傾向制定具體的「監管法案」，強力直接課予企業法律義務。但由於缺乏統一標準與美國聯邦層級的硬性法規，各州在具體實施細節、問責機制以及部署者義務的劃分上，呈現差異化發展。紐澤西州的指引在責任認定上，明確指出即使自動決策工具是由第三方軟體公司開發，雇主實體仍須對演算法產生的歧視結果負起最終責任。德州的立法則側重於持續性的風險監控與強制停用機制。科羅拉多州也要求部署者必須每年審查所部署之高風險系統，確保企業不會因為系統長期運行而忽視演算法可能隨時間產生的漂移或偏見。加州則不僅關注系統端的合規，更賦予受決策影響的主體（勞工）實質的救濟權利。勞工不僅是被決策的對象，更是有權挑戰決策的主體。

(四)AI 個資保護法制發展

在 AI 與個人資料保護的交匯領域，各國的重點觀注「強化高風險 AI 的隱私監管」，採取透過「強制要求風險評估」及推動「隱私始於設計（PbD）」等措施進行防制。由於各國認知到 AI 系統對個資的處理量大且複雜，傳統的事後監管已不足以應對風險。因此，開始要求組織在導入或訓練 AI 系統之前，執行資料保護影響評估（DPIA）或風險評估。以促使企業在 AI 開發階段就識別並緩解可能對個人權利與自由造成的重大影響。例如前述美國加州 CPPA 的修正提案要求，企業若要使用自動化決策管理科技（ADMT）來做出「重大決策」，或者是使用個人資料來訓練 ADMT，都必須在實施前進行詳盡的風險評估。

針對「隱私始於設計（PbD）」，韓國個人情報保護委員會發布的生成式 AI 指引中，針對如「居民登錄號碼」等唯一識別資料提出嚴格



本報告之智慧財產權歸屬於國發會

要求，規定這些資料必須在 AI 訓練階段之前就進行「刪除」或進行「假名化、匿名化」處理，確保原始的敏感個資不會被輸入模型中，澳洲的指引亦有類似建議。新加坡則積極推動使用隱私強化技術（PETs），並將資料保護信任標誌提升為新的新加坡標準。法國 CNIL 亦建議機構落實隱私始於設計(privacy by design)，於 AI 系統開發階段即將隱私保護納入考量，並盡量以匿名化(anonymisation)或假名化(pseudonymisation)等替代措施，補足現行 AI 系統無法完全讓當事人行使權利之限制。澳洲亦建議不宜將敏感資料輸入公開可用的生成式 AI 工具，以防止這些資料被模型記憶並在未來被意外輸出。

其他在創新與個資保護平衡上，歐盟自 2024 年起即著手連結 GDPR 與 AI 法令之間相互作用之法制協調。依據 2025 年 11 月 19 日公佈「數位綜合法案」(Digital Omnibus)草案，針對 AI 模型中之個人資料處理規範，進一步將個人資料之定義引入「相對性」概念，認為即使某些資訊可以識別當事人，但若該資料控制者無法直接識別個人資料，則該資料可以非個人資料被利用。另為解決同意疲勞之問題，簡化無須取得同意及減少資料主體同意頻率之規定，並於 GDPR 中直接增修對於 AI 系統開發與資料處理之相關鬆綁，包含對正當利益、敏感個資之利用、生物特徵之驗證、資料外洩通報機制變更等規範之調整。法國 CNIL 基於執行告知之可行性，建議多來源的訓練資料之揭露，僅須提供類型或大致資料來源，亦無須個別通知當事人。

國際間對於弱勢群體、民生受眾的個資權益保護也日益加強。美國透過修訂「聯邦兒童線上隱私權保護法」（COPPA）特別針對兒童隱私大幅擴大個人資料的定義範疇，強化家長知情的通知與同意要求，並明定資料安全維護計畫的建立與執行義務。韓國推動在醫療保健、電信和能源等領域全面實施「My Data Scheme」，賦予當事人資料控制權和資料可攜權。

整體而言，各國針對高風險 AI 與自動化決策技術，多開始以政策、規範、技術標準提升個資隱私監管之強度，但為平衡監管與資料



本報告之智慧財產權歸屬於國發會

運用，仍然透過重新解釋關於假名化及自動化決策之相關定義等方式，前提下在符合隱私保護規範之架構下鼓勵創新發展，並減少法律之不確定性。

(五)其他重要趨勢觀測

1. AI 法制政策提升至國家戰略層級

除了上述具體的議題外，觀察國際間在 AI 治理上已形成以國家戰略為導向，並致力於平衡技術創新與安全風險的共通態度。各國普遍意識到，AI 是關乎未來數十年國家競爭力與國家安全的關鍵場域，因此紛紛透過發布國家級行動計畫或制定基本法，確立 AI 的優先發展地位。例如：歐盟則開始透過假名化定義、通報機制、中小企業簡化措施等做法，鬆綁「人工智慧法」（AIA）的限制。美國發布「人工智慧行動計畫」，勾勒美國維持 AI 霸權的藍圖，計畫指出優先推動「開源及開放權重（open source/open weight）」的 AI 模型發展，同時強調聯邦機構採用 AI 技術以提升效能，並且必須解除對企業的「不當監管」，明示美國試圖透過開放生態系來鞏固其技術標準的全球影響力。

韓國於 2024 年底通過「人工智慧發展及建立信任基礎之基本法案」（簡稱 AI 基本法），為「可信賴的 AI」應用奠定法律基礎。韓國透過立法建立高層級的「國家 AI 委員會」及專業的推動機構「AI 安全研究院」，試圖以強化國家競爭角度，保障 AI 產業的穩健發展。日本則於 2025 通過「人工智慧相關技術研究開發及應用推動法」，重點揭示其 AI 政策在於「推動」而非「管制」。日本政府將積極推動行政機關運用 AI 技術，確保、培養提升所需專業及廣泛知識之各領域人力資源，蒐集有關日本或海外 AI 技術研發相關資訊及動向，分析因非法目的或不正當研究方法利用 AI 技術而侵害公眾



本報告之智慧財產權歸屬於國發會

權利之案件以制定因應對策，並進行有助推動國內 AI 技術開發之調查及研究，促進研究機構與國際合作、參與國際規範制定，以全面、系統性地制定及實施與促進 AI 相關技術研發及利用相關之措施。

2. 不同領域的應用與監管規範開始深化

英國司法部發布的「人工智慧司法行動計畫」，目標是在 2025 年底前，使每位司法體系的員工都能使用安全的 AI 助手，顯示各國開始著力於將 AI 轉化為實際提高公共服務的工具。同時在各應用領域中，透過小組制定跨領域倫理、資安及營運標準，管理部門之 AI 風險登錄，並定期審查 AI 推動進度及協處各類相關問題，並持續更新指引、政策及風險管理規範，以遵循現有之數位與資料治理流程，確保 AI 的安全、合法且透明地落實。

同時在國家競爭角度上，亦顯示各國不僅在意 AI 技術本身的風險，同時也擔心 AI 科技的壟斷阻礙創新，例如日本的公平貿易委員會密切監測生成式 AI 的市場結構，關注優勢是否過度集中在基礎設施層（例如 GPU 晶片供應）。韓國則對高算力系統有特殊關注。在其「AI 基本法」的施行令草案中，韓國政府引入具體的量化監管標準，規定凡是高運算量超出其標準的 AI 系統，必須遵守安全性確保義務。這種針對超大規模模型的特別監管，顯示韓國試圖精準針對可能帶來系統性風險的 AI 模型，而非對所有模型一視同仁。

綜上所述，各國的共同點在於都認識到 AI 對國家安全和經濟競爭力的關鍵影響。因此，各國皆於積極制定法規，平衡 AI 所帶來的創新效益與潛在之倫理、安全等風險，建立更具針對性之風險分級與特定應用監管，並注意 AI 之 基礎建設與人才培育策略。



本報告之智慧財產權歸屬於國發會

## 二、 我國法制整備建議

依據國際趨勢的觀察，歸納著作權、消費者保護、勞動權益、以及個人資料隱私等四大議題的共通趨勢，初步提出於我國法制需強化的重點議題，以及適當的敏捷法制整備方式，說明如下：

### (一)著作權議題

AI 訓練定性與合理使用的爭議，國際間普遍認為訓練過程涉及對受著作權保護作品的下載、儲存與複製，本質上構成「重製行為」。AI 訓練在傳統著作權法（例如我國著作權法第 65 條）的合理使用判斷上，先天處於不利地位，特別是因為其具有高度商業化、海量且完整的利用特性。美國聯邦法院雖在個案中裁決 AI 訓練具有高度轉化性（quintessentially transformative），得主張合理使用，但前提是訓練資料來源必須是「合法取得」。然而，AI 訓練讀取的是將資料轉換而成的數值向量，進行的是數學運算，並非傳統著作權法所保護的「表達」（expression），而是更接近轉化成概念或想法。但若訓練過程可無須取得授權，可能導致著作權人成果被收割，從而打擊創作的動機。因此，國際趨勢正朝向建立「公平合理的利益分配制度」，使創作者能獲得應有的報酬，而非僅是無償的合理使用。即便賦予 AI 開發者資料探勘合法使用權利，也呈現出透明化義務、權利保留，例如尊重付費牆等技術性拒絕或限制存取、賦予著作權人「退出權」（Opt-out），以保障創作者的自主性與控制權，應是較為平衡兼顧創作發展與權利保護的做法。

於立法政策上，宜評估擬針對 AI 訓練給予此特定情況下，有較大的資料使用空間，建議制訂 AI 發展專法，增訂「AI 訓練專屬合理使用」；如評估認為具有通案需求，則考慮修訂《著作權法》，增訂「資料探勘例外」，使 AI 模型訓練的行為得以賦予明確可循的合法條款時，但建議應採行以下立法原則：



本報告之智慧財產權歸屬於國發會

1. 不限制於非營利性：多數的 AI 發展皆帶有營利目的，若將例外規定限制於非營利性，將對我國 AI 產業發展造成極大限制。或者考慮以實際是否營利為區分，將 AI 模型開發的「基礎模型訓練」階段與後續「商業應用」(如結合最新新聞進行分析)階段明確區分；單純僅為資料探勘，視為對基礎模型訓練的一部分，納為例外規定，而非於此階段即應洽談授權。

2. 要求 AI 技術開發者負起透明性揭露義務：該義務可透過專責機構或中介服務，定期通知權利人，使創作者得知作品是否被利用，作為後續合理補償的基礎。

3. 賦予創作者事前保留（例如透過 robots.txt 等技術或聲明方式）與事後退出的選擇權：保障創作者的主體性與控制權，但仍須將事後退出在技術執行及驗證上，可能於目前仍存在困難的情況，納入立修法條文研擬之考量事項。

4. 生成階段的過濾義務：課予 AI 服務與系統提供者在生成階段實施合理的著作權過濾機制的義務，以防止模型輸出內容侵害著作權。若開發者已盡到過濾義務，而使用者繞過機制生成侵權內容，則侵權責任應主要由使用者負擔。

5. 檢討刑事責任：我國《著作權法》對侵權行為設有刑事責任，確實對涉及巨量資料利用的 AI 開發者而言，風險責任可能不符比例，而對創新發展造成寒蟬效應。建議評估在利用人已履行透明性義務，並提存或支付合理報酬的前提下，考慮將 AI 訓練行為「除罪化」。若將 AI 訓練行為除罪化，則相關民事責任應回歸《民法》第 216 條的損害賠償規定處理。

於立法或修法之前，建議以輔導措施鼓勵建立商業授權機制，例如：扶持資料平臺，補助大型資料庫業者或內容產業公協會，建立可信任的資料源，並推動一站式集中授權服務，包括透過概括授權並搭



本報告之智慧財產權歸屬於國發會

配超微分潤支付系統，確保創作者獲得累積的合理報酬。亦應鼓勵公協會自訂自律規範或行為準則，建立爬蟲遵循規範、標記系統、並提供調解機制。同時發布函釋或行政指導性的指引文件，表示目前政策上對於在現行《著作權法》框架下，AI 訓練行為主張「合理使用」的邊界與條件，以降低產業的法律不確定性。

(二)消費者保護

國際上普遍認為 AI 系統的運用可能導致消費者被擬人化的技術誤導或欺騙，因此針對高風險應用的特定監管，應強化互動透明度，是消費者保護的核心趨勢。因此，諸多立法例要求從事商業交易的實體，在消費者與聊天機器人或模擬真人互動時，必須以「清晰顯著」的方式「事前」揭露其正在與 AI 系統互動，而非真人。在使用者出現自殺或自我傷害跡象時，必須提供協議機制以偵測並主動引導使用者聯繫危機緊急心理諮商服務機構。而利用 AI 謊稱產品功能、發布虛假評論，或聊天機器人謊稱自己是人類，應被視為欺詐或不公平的商業行為。同時擴大消費者保護的範圍，將資料的錯誤或損壞列為軟體產品之瑕疵；且在特定條件下，線上平臺（Online Platforms）也可能承擔與經銷商相同的責任。

針對在企業經營者資訊提供義務，我國消費者保護法第 4 條已有企業經營者對於其商品或服務，應提供消費者充分與正確之資訊之規定，同法第 5 條亦規定企業經營者應本誠信原則從事商品或服務之設計、製造、銷售或提供。同時，第 21 條要求不得為虛偽不實或引人錯誤表示。若企業刻意設計「擬人化 AI」誤導消費者誤認為真人，理論上可構成違反前揭規定，但仍非法條之明文，實務上仍需搭配主管機關解釋，未必能形成「事前必須揭露」的明確法定義務，也欠缺事中風險預防或事前風險評估的要求。建議我國應推動沙盒機制進行高風險測試，對於此類情感互動功能的 AI 系統的透明度、可解釋性、反歧視機制等進行嚴格的測試與驗證，據該經驗評估義務要求的可行性。因此，可先行推動由相關主管機關（例如數位發展部、衛生福利部）



本報告之智慧財產權歸屬於國發會

針對特定高風險領域的 AI 應用（如醫療、金融、心理諮詢等），發布行政指導性指引，以利有效補充現行法令之具體適用疑義，重點包括：

1. 強化透明揭露義務：確要求商業用途的 AI 系統（特別是聊天機器人或擬人化服務）必須履行「事前清晰揭露」的義務。

2. 揭露模式必須是清晰、顯著且不可迴避的（例如文字或語音互動開始時即告知），避免使用易誤導消費者的設計。

3. 問責窗口：要求提供 AI 服務的供應商必須明確提供聯絡窗口，讓消費者得就 AI 系統的決策或輸出結果提出質疑或申訴。

4. 主動預警設計：要求業者應在使用者出現自殺或自我傷害跡象時，必須提供協議機制以偵測並主動引導使用者聯繫危機緊急心理諮商服務機構。

5. 明確宣示現行《消費者保護法》及《公平交易法》可適用於 AI 相關的詐欺或不公平競爭行為。例如，針對利用深度偽造（deepfake）技術進行詐騙、假冒身分、或使用 AI 發布虛假產品評論的行為，可依法追究責任。

(三)勞動權益

AI 在涉及勞工重大決策中（如招聘、晉升、薪資、解僱）產生演算法歧視的預防與問責，是國際趨勢焦點，包括雇主不能 AI 系統是由第三方軟體公司開發而免除責任。甚至要求採取定期的影響評估和反偏見測試措施，以防止已知或可預見的演算法歧視。同時賦予強化勞工知情權與程序保護，針對使用 AI 進行就業決策，保障勞工的程序性權利，包括知情、存取資料、申訴與人工覆核，例如勞工有權在 AI 系統被用於做出影響其工資、福利、工時、績效、紀律或解僱等「僱用相關決定」之前，獲得書面通知；當雇主依賴 ADS 系統對員工作出



本報告之智慧財產權歸屬於國發會

懲處或解僱等重大裁定時，必須有人工介入審查的程序，以避免 AI 成為唯一的裁判標準。

我國在《性別平等工作法》第 11 條與《就業服務法》第 5 條，分別有禁止因懷孕、生育而給予差別待遇，及禁止因性別、性傾向、婚姻、年齡、種族、宗教、身心障礙等因素，對求職者與員工給予差別待遇之規定。雖並無 AI 自動決策系統的管理專法或專章，但亦不致於完全無法規範而對勞工產生權益損害的風險，故透過跨部會合作、指引制定或函釋，由勞動主管機關與未來個人資料保護委員會、數位發展部等機關強化橫向協調，共同發布就業或勞動條件自動化決策系統使用指引，或為目前效率與效益兼俱的法制整備方式。其重點建議包括：

1. AI 自動決策系統的管理：包括如何進行評估指標設定、如何對抗訓練資料中的偏見、以及如何設置有效的人工監督機制。

2. 明確宣示現行《就業服務法》中的反歧視條款適用於演算法歧視。同時，透過教育訓練，強化勞檢員對 AI 系統運作原理及潛在偏見的理解，確保在勞動檢查中能夠有效識別和處理演算法歧視案件。

3. 對於被認定為高風險的自動決策系統（即用於做出或促成重大就業決策）要求影響評估：要求部署者定期完成影響評估（例如每半年或每年），並公開或向主管機關提交摘要報告。

4. 明確規定涉及懲處、降職或解僱的自動決策決策，不得僅依賴演算法的結果，必須經過具備足夠權限與訓練的人工監督與覆核。

5. 通知與申訴權：雇主使用自動決策作出或促成重大決策時，必須以簡明易懂的書面通知勞工，並提供對決策結果提出申訴的權利，且申訴必須由人工審核。



本報告之智慧財產權歸屬於國發會

6. 舉證責任倒置：發生疑似演算法歧視的爭議時，應對使用 ADS 進行人事決策的雇主賦予較高的舉證責任，要求其證明已執行反偏見測試或類似的積極措施來防止非法歧視。

7. 除非有明確的法律依據或基於工作安全絕對必要，應禁止雇主蒐集與員工工作無關的健康或生物特徵資料。

(四)個資隱私

AI 系統對個人資料的處理具有高複雜性和高風險，因此於國際上開始逐漸考量將強制風險評估與事前管理，做為風險預防措施。特別是做出「重大決策」或利用個人資料訓練，常見要求必須在實施前進行隱私影響評估（DPIA）。以權衡資料處理對消費者隱私權侵害的風險與其帶來的效益，並要求制定詳細的保障措施，包括隱私始於設計與技術強化（Privacy by Design），在開發之始即確保敏感資料不被模型吸收並洩露。另外隨著 AI 系統集中大量資料，國際趨勢也致力於增強個人對其數據的自主控制與可攜權。

考量建立制度化且持續運作的 AI 個資保護機制，涉及不同產業、資料來源、資料性質、機關構性質、規模大小不同等考量，必須較周嚴的橫向議題整合，搭配更具體的意見徵集、實務調查及法制政策回應追蹤機制，以及監理沙盒機制的運用，以指引既有法規下提供最大限限度的明確規範釋明。同時，提出負責任開發的明確期待，例如要求使用 AI 的公務機關或企業公布 AI 倫理準則、揭露 AI 使用情況、並實施內部治理框架，以推動產業自律，提升社會信任和透明度。同時，評估是否先行核心處理影響較廣泛的個資法修法議題，例如：

1. 明確區分假名化與匿名化，並合理調整事故通知義務

鑑於現行法對於「無從識別特定當事人」之概念界定過於抽象，致使實務操作上難以判斷適用界線，建議於第 2 條中明文引入並區分「假名化」與「匿名化」之法律定義。另考量



本報告之智慧財產權歸屬於國發會

經假名化或匿名化處理之資料，在通常情形下已難以識別特定個人，且實際上亦無從確認事故通知之對象，可評估於第12條第1項中，明確規定該等情形得免除個人資料外洩之通知義務，以兼顧風險比例原則與實務可行性。

2. 放寬學研例外與利用目的之明確合法利用基礎

因應資料驅動創新發展之實際需求，同時建立更具彈性之合法利用，可考量擴大學術研究相關例外之適用範圍，刪除現行對資料利用主體之限制（不再限於公務機關或狹義學術機構）外，並將得利用之目的明確擴展至「統計、科學研究或技術開發」。(第6條、第9條、第16條、第19條及第20條)。

3. 以公務機關為起點推動資料保護影響評估制度

考量公務機關長期掌握大量高度敏感個人資料(如戶政、醫療、財稅資料等)，且在法規影響評估與行政程序方面已具相當經驗，建議明定公務機關負有進行DPIA之強制義務；未來亦可參考指定由專業機構協助執行與審查 DPIA，使行政資源得以集中運用於高風險案件之諮詢、指引與標準建構。

4. 建立自動化決策之拒絕、控制權與程序性保障

建議新增賦予當事人於其權利義務或重大利益係僅由「自動化決策或分析機制」作成時，享有拒絕該等決策之權利，並同步保障其知情權、異議權及請求人工介入審查之權利，藉此在促進資料合理運用與確保個人權益保障之間，建立制度性平衡。

5. 引入資料可攜權並保留制度彈性



本報告之智慧財產權歸屬於國發會

現行個資法第 3 條已有當事人得請求將其個人資料複製本製給的權利，但文義上並不及於傳輸予指定之第三方。建議可於該條或另新增資料可攜權，並就其涉及的互通技術標準、格式及資安風險管理等問題，授權訂定子法規範。



本報告之智慧財產權歸屬於國發會

# 項次 2. 國內數位法制調適與變革焦點議題

## 壹、 焦點議題 1：數位科技法規調適—加速法規調適或鬆綁研析

### 一、 背景說明

數位經濟在網際網路、雲端資料發展到如今 AI (Artificial Intelligence)、超級電腦等新興科技高速發展，新興服務型態與商業模式亦變化迅速。尤其新科技運用於創新商業模式對於現行法令體制之適用或解釋產生衝擊，需要充分之討論釐清，甚至進一步法制政策之調整。然而修立法的速度往往無法趕上科技的腳步，此一長久以來的問題，於 AI、高度之算力與超高速網路環境之發展下，更加凸顯出來。法規調整的速度，不但常無法因應新興科技之應用，甚至更可能影響新科技創新研發的過程，例如影響科技研發所需資源之取得（如各類 AI 訓練所需資料資源），以及研發方向之適法性等問題。

近年來國內外面對數位科技帶來的數位經濟環境變動，AI 相關研發應用為首之新興數位科技發展與應用，以及平臺、資料經濟議題所帶來之社會變化與需求，無不絞盡腦汁尋求於法制政策面之因應之道。其中歐盟近年來推動一系列新興之立法，延續歐盟單一數位市場之發展軸心，逐步發布囊括各項配套立法之資料戰略、AI 政策白皮書等大型政策文件，並依循計畫陸續通過引領國際立法先驅之各項數位立法，諸如數位市場法(Digital Market Act, DMA)、數位服務法(Digital Service Act, DSA)、資料治理法(Data Governance Act, DGA)、資料法(Data Act, DA)、人工智慧法(Artificial Intelligence Act, AIA)、媒體自由法(European Media Freedom Act, EMFA)以及各項數位經濟環



本報告之智慧財產權歸屬於國發會

境相關指令或指引等規範或指導，更是加速各國對數位議題法制化之探討與重視。

主要重點國家，如鄰近之日韓、美國以及澳洲近年來亦多有對於 AI 等數位科技引發之議題，以及對經濟社會之影響，陸續於法制政策面向有相當之因應與成績。經由觀察，可以發現日、韓近年來與歐盟類似，皆有發布具整體性之科技政策，提出長短期政策規劃並納入法制政策面之搭配，以利法制政策依循推動。美國近年來則主要透過總統布達具體行政命令之方式，快速對於新興科技議題或國際重要議題因應之方向或進一步之措施，要求各級政府配合推動及落實。相關作法必然與各國政府體制、法制政策形成之程序正相關。而面對比過往更快速之科技變遷，既定法制政策研議之體制或程序可能難以快速因應，是否有其他法規調適之方式或因應做法讓歐盟或上開國家得以有效率推動各項新興修立法的發展；或有無在規範制定上，針對科技應用之不確定性有對應之做法或策略等，值得予以了解，以作為我國評估因應晚近高速新興科技發展之法規調適作法的參考。

本次焦點議題分析，將蒐整近年來投入科技法制政策發展成績卓著之歐盟、美國、日本、韓國及澳洲，了解其基本法制政策形成之機制，以及是否對於科技或數位科技影響法制政策之因應，有對應之作法。同時，OECD 於 2021 年對於其成員國亦有針對法制政策監管層面如何保持敏捷與彈性，提出建議原則，亦可作為我國後續評估相關機制之參酌，併予納入說明。最終比較我國面對新興數位科技發展法規調適面臨之問題及現況作法，提出可能可強化或提升法規調適效率之建議。

## 二、 近兩年國際發展趨勢重點及歸納

### (一)OECD



本報告之智慧財產權歸屬於國發會

經濟合作暨發展組織(OECD)於 2021 年通過《敏捷監督治理以促進創新之理事會建議》[10]（Recommendation of the Council for Agile Regulatory Governance to Harness Innovation，下稱 OECD 建議）並於 2025 年公布完整文件。該建議旨在協助各成員國政府制定及實施敏捷且有彈性的法制監督機制，並促進機構間之合作以使創新活絡。此文件當中對於「監督」(regulation)的定義，涵蓋政府對於事業及人民提出要求之各種方式，包括法律的制定、正式或非正式之命令、次級規則、行政程序以及非政府機構及自律機構所發布之規則。而所謂之「監督管理工具」(Regulatory management tools)，則是指可以用於實施各項監督政策及提升監督品質之不同工具，包括影響評估、利害關係人評估及事後評估等。至於「監督政策」(Regulatory policy)則是指政府為制定、管理及評估相關法規而建立之一系列規則、程序或成立之機構等，合先敘明。

此建議文件，主要係 OECD 於面對新興科技、氣候變遷、環境變化及因應環境緊急變化對社會及全球的挑戰，認為應該協助各國調整並建立所需監管政策以及治理模式。此建議評估之過程，主要考量到要在高度不確定性之環境中充分發揮創新，強化創新為社會帶來的利益，並適切的因應風險，必須要有更靈活與前瞻性的做法。同時也必須考量所採取之策略做法，必須依循證據的評估，確保廣泛及持續之利害關係人參與，並對落實之結果施以密切的監督，創造社會認同。OECD 之監督政策委員會(Professional Regulation Commission, PRC)綜合長期以來之監管經驗，提出以下四項支柱作為本次敏捷、彈性監督機制建議之核心。

[10] OECD, Recommendation of the Council for Agile Regulatory Governance to Harness Innovation, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0464, last visited: 2025/3/5.



本報告之智慧財產權歸屬於國發會

1. 建議調整法制監管工具以確保相關法規適合未來需求

政府應建立更具適應性且更為動態、靈活之監督機制並縮短法制政策評估之週期，同時透過對於科技方法的運用，改善法制政策評估所參酌之證據品質。尤其法制政策監管之流程必須有所調整，改採適應學習(adapt-and-learn)的方式，適時發現及理解創新技術對現有法規之潛在影響，或更進一步識別其對所涉公共價值可能產生之影響。尤其可以考量縮短法制政策制定過程的時間結構(timeframes)，採取更具備活力、適應性及重複採用性(iterative)之監督監管工具[11]。政策制定週期，得活用監督影響評估(Regulatory Impact Assessment, RIA)、利害關係人參與及事後評估等工具，以適時調整監督之方式[12]。

為確保利害關係人及社會各界得充分理解創新技術可能對政策法規產生之影響，並建立可受信任之政策，政府應增加公眾及利害關係人之參與機制。自政策制定前開始至制定過程中皆應持續與公眾溝通，包括透過公聽會或線上平臺等數位方式蒐集意見，且應特別注意公民、公民組織、學術及科學界及新創公司等相關潛在對象之意見。公眾參與過程可以強化監管透明度及參與度，促進針對相關議題之社會實質性對話及審議[13]。

[11] Id at 9.

[12] Id at 10.

[13] Id.



本報告之智慧財產權歸屬於國發會

而為提供成員國更為具體之監督治理適例，OECD 於 2022 年發布敏捷治理以促進創新之案例分析[14] (Case studies on agile regulatory governance to harness innovation)文件，透過無人機(Drones)以及生物技術解決方案(Bio-solution)兩項具體案例，說明各國面對新興技術，所採取之不同監管措施。其中有部分案例反映出動態、靈活之特性；但也有部分案例則是對於新興科技法規調適採取更為審慎評估之作法。

就動態、靈活適例層面，例如，於無人機之議題，英國民航局係選擇較為創新友善之方式，即透過創新監理沙盒機制(Innovation Sandbox)，建立並啟動創新中心，提供創新發展之測試環境。此作法不但協助政府掌握相關風險，也讓創新者能夠獲得民航局專業的協助、指導與法規之說明，使其得以了解可能面對之監管挑戰，也可預測創新領域可能對於法規監管的影響，促進新政策與法規之擬定，使監管與創新得以調和[15]。類似的概念，如韓國對生物技術解決方案之作法，其於 2020 年宣布 10 項產業之監理沙盒，生物技術即為其中之一，政府於特定條件下授予事業豁免權以就其計畫進行試驗，事業於試驗後會取得暫時或正式之核准，得於韓國商業化相關產品或服務，以此方法促進產業創新及政府監管之調整。

於提高法規調適之適應性部分，挪威考量新興政策法規擬定應審慎評估以使之符合需求，乃於民航局提出修法建議及對應之 RIA 分析後，再由優化監管委員會(Norway's Better

[14] OECD, Case studies on agile regulatory governance to harness innovation: Civilian drones and bio-solution, https://www.oecd.org/en/publications/case-studies-on-agile-regulatory-governance-to-harness-innovation_0fa5e0e6-en.html, last visited: 2025/5/6.

[15] 同前註，頁 22。



本報告之智慧財產權歸屬於國發會

Regulation Council, NBRC)對民航局對此議題之法制修訂提供諮詢意見。NBRC 之聲明中對於民航局之修法建議與搭配之 RIA 分析，則係明確指陳應需改進之關鍵領域，以利主管機關予以因應。除此之外，NBRC 也在聲明中表達，政府機關應有一個法規評估之策略，強調法規之「可預測性」對於受影響之事業非常重要，須與其他政府機構及利害關係人充分溝通，並與採用該無人機相關技術之事業有所合作，制定出得讓相關人員清晰易懂之規則[16]。

德國則是於生物技術相關議題部分，成立一個獨立機構－生物經濟委員會(Bioeconomy Council)，主要任務在針對國家生物經濟研究相關戰略等，提供政策及法制如何落實之建議。同時支持以知識為基礎之生物經濟研究及發展，並透過舉辦論壇、座談會等方式蒐集產學界多元利害關係人之意見。其主要亦透過獨立機構之職權，統整重要議題之政策方向，避免政府部門之政策碎片化，並促進政府間橫向溝通及與產業界之協作，共同建立適切之監管框架[17]。

此外，OECD 建議並指出法規政策之制定應參考國際條約、指引等國際標準，或從國際論壇獲得更多的資訊，尤其是對於與目前政策目標正相關之國際條約、指導文件或最佳實踐(best practices)，以確保政策得與國際接軌[18]。並且對於國內監管尚不足以應對創新科技時，亦得透過國際合作、協定之方式建立聯合監管。

---

[16] 同前註，頁 23。

[17] 同前註，頁 39。

[18] Id at 11.



本報告之智慧財產權歸屬於國發會

2. 建議可建立跨組織功能及跨管轄區域之監督合作機制

為避免因政策監管缺乏一致性而導致之監管失敗，政府應強化內部跨部門之協調及合作，建立跨部門之合作機制，落實資料共享，確保各部門間對於跨領域監督政策之一致性，並使彼此間對於創新相關之監督政策與框架維持一定程度之關聯性[19]。因此必須設計適當的機制，預測創新發展可能帶來的風險與機會，建立聯合監督之方法或機制。此外，為便利事業與政府間之溝通，並提高政府部門間之協調，OECD建議可採取一站式(one-stop shops)服務窗口[20]。同時於適當之情形下，可以考慮支持各機關間共享監督之方法，例如透過跨機關、領域之監理沙盒(cross-sector regulatory sand boxes)，以及資料驅動之通用監督機制等。

此外，政府須加強雙邊、區域或多邊之監管合作，以因應跨國政策之影響並確保同時對於國內監管不足以應對創新技術時，得透過雙邊、多邊或區域協定之方式建立國際合作監督機制[21]。對於促進創新領域可用之國際合作監督工具，可以包括資訊交換、相互承認、平等協議、聯合文件之制定、國際論壇之參與、或對於相關能力建設之識別與需求之合作等。尤其必須維持並促進與其他司法管轄區域之對話，確保對創新技術之發展變革層面之監督政策有一定之透明度，同時促進資訊交換，確保監督合作與政策之一致性。針對具備跨國影響之發展，則需要考慮與其他司法管轄區域合作訂定

[19] Id.

[20] Id.

[21] Id, at12.



本報告之智慧財產權歸屬於國發會

聯合之監督方法，或利用多邊或區域論壇，對於國內尚未確立監督政策方向之新興領域有系統的予以評估。

3. 調整治理框架以實現敏捷及適應性法制政策監管機制

為實踐創新之敏捷及適應性監督，須建立得靈活應對技術變化並具前瞻性之監督體系，確保法制政策不會對技術創新造成阻礙。政策制定時得透過實施漸進式之戰略以預測新興技術趨勢，並定期檢討監督機制。同時需要強化相關機關能力之發展，使之得以相互合作分工以進行系統性與協調性之水平掃描與情境分析，有效預測及監控相關監管機制對創新可能產生的影響，並持續強化學習與適應。

建立更加重視成果導向(Outcome-oriented)之監督方法，以關鍵成果或目標取代過度詳細之法律規範，將規範的制定限於必要情況下，尤其在確保法律確定性之情形，使事業於創新技術開發上得更具彈性，同時亦能確保監管目標之明確性[22]。根據公共政策之目標設定績效指標，透過定期審查確保政策與目標之一致性並衡量監督成果；提供明確之實施指引，於適當情況下鼓勵產業採用自願性之規則、標準或非法律性之文件，以責任法(liability law)或條款支持此類規則或文書之效果，降低成果導向之監督可能造成法律遵循之不確定性[23]。

不具法拘束力之標準亦得作為監督工具之替代或補充措施，使政策之執行具較高彈性以因應創新科技之不確定性。惟政府應積極追蹤相關資料及監控執行成效。同時亦須

[22] Id, at13.

[23] Id.



本報告之智慧財產權歸屬於國發會

考慮共同監管(co-regulation)與創新業者合作機制，促進業者之參與意願，或以發布指引之方式，減少監管之不確定性[24]。

監理沙盒、測試台(testbeds)、創新空間以及實驗室之機制亦得降低事業之創新風險，並使政府先期了解其可能之發展以制定合適之法制政策。監理沙盒允許事業進行新想法、產品或商業模式之實驗、測試，並且於適當情境下獲監管豁免，促進創新產業監管政策之適應性。而政府於試驗設計、實施及評估過程中，應積極與事業、監督機構以及公眾保持溝通，以兼顧創新與公共利益[25]。

4. 調整監管執法策略以維護公共利益

鑒於創新科技之快速變動，政府應採取以風險(risk-based)為導向之監督方式，先行加強對高風險事業之監管。透過資料驅動監管，加強實測、資料蒐集與分析，優化資源分配並改善風險評估，提高效率及採取更具彈性之執法[26]。同時亦須適時調整風險治理框架，並依風險比例制定明確執法指引。於調查層面，應促進調查機構與主管創新科技之國內外部門透過資料交換、聯合調查等方式進行合作，以防止事業之非法行為。

(二)歐盟

1. 整體科技政策評估

[24] Id at 14.

[25] Id at 15.

[26] Id, at 15.



本報告之智慧財產權歸屬於國發會

歐盟執委會於 2020 年提出《歐洲資料戰略[27]》(European data strategy)，以建立歐盟單一資料市場為目標，提出系列政策規劃，目的在促使各類資料能於歐盟境內及跨部門間順利流通並有效運用。尤其工業及商業資料為數位經濟中相當重要之一環，因此該戰略亦期待得以促使更多的類型之資料，能在維持資料控制者之控制權的前提下，於經濟社會中被利用。

歐盟資料單一市場之框架包含資料得於歐盟境內跨部門流通並有利於所有人；全面遵守歐盟內部相關規則，尤其資料隱私以及競爭法等規範最為重要；最終並須搭配建立公平、可行且明確之資料近用規則。而為達成前述單一資料市場框架，除制定相關規則外，歐盟亦將透過投資、提供新技術、建立歐洲資料空間等方式為配套，多管齊下相互配合以達成目標。而歐盟資料戰略下規劃之法制建構藍圖，最為重要也帶動國際立法討論者，為 2022 年生效之《資料治理法[28]》(DGA)，以及 2024 年生效之《資料法[29]》(DA)。而為實質上促進歐盟境內資料流通之根本立法，並與 2022 年與其後提出之各領域歐洲共同資料空間相互搭配[30]。

歐盟整體政策目標之建構，主要係由歐洲議會(European Parliament)、歐盟理事會(the Council of the European Union)以及歐盟執委會(the European Commission)共同制定。政策大方

[27] European Commission, European data strategy, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en, last visited: 2025/2/27.

[28] EU, Data Governance Act, https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng, last visited: 2025/3/9.

[29] EU, Data Act, https://eur-lex.europa.eu/eli/reg/2023/2854, last visited: 2025/3/9.

[30] European Commission, Staff working document on data spaces, https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces, last visited: 2025/2/27.



本報告之智慧財產權歸屬於國發會

向及目標之建構或調整，主要由各國之元首或代表組成之歐盟理事會，每 5 年進行一次歐洲戰略議程(EU strategic agenda)之訂定。

在過去 5 年間，AI 為全球關注之議題，故歐盟於 2019 年即提出「值得信任的人工智慧倫理指引（Ethics Guidelines for Trustworthy AI）」，並於「2020 年發布人工智慧白皮書」（White Paper on Artificial Intelligence），隨後於 2021 年 4 月起起草 AIA 並於 2024 年 7 月通過。2024 年後歐盟執委會在新的 5 年任期開始之際，再度提出政治指導方向，依該核心優先事項進行立法及長期預算規劃，制定 2024-2029 年政策指引文件[31]。而執委會則會於每 5 年新的任期開始時由主席擇定該任期之優先事項。執委會主席會於每年之歐盟國情咨文上與歐洲議會進行辯論，說明前一年度所達成之事項，並說明下一年度計畫所欲採取之重點措施。

執委會之議題擇定需與歐洲議會以及歐盟理事會討論，並且歐洲議會或歐盟理事會亦得就其認為重要之事項提案。執委會於其 5 年新任期之初確定優先事項後，主席即會向歐洲議會提交相關政策方針以及各機構之權責。歐盟提出相關政策所服務之對象為歐盟公民、事業及相關利害關係人。因此於提出新政策或立法前，執委會必然會向公眾或利害關係人徵詢意見並進行影響評估[32]，此為歐盟政策與相關推動計畫行程之基本程序。

---

[31] POLITICAL GUIDELINES FOR THE NEXT EUROPEAN COMMISSION 2024−2029, e6cd4328-673c-4e7a-8683-f63ffb2cf648_en ,last visited 2025/2/19.

[32] European Commission, Decision-making process in the Commission, https://commission.europa.eu/strategy-and-policy/decision-making-process-commission_en , last visited: 2025/2/19.



本報告之智慧財產權歸屬於國發會

2. 通常法案形成與立法程序

(1) 立法評估

歐盟法律規範之研議，係由執委會負責規劃、準備及提案，而除了執委會自行提案外，亦可回應歐盟理事會及歐洲議會之建議或公民倡議作為提案。

執委會在提出一項新的提案時，會針對法案可能產生潛在經濟、社會及環境影響進行評估，並透過公眾諮詢讓公民、事業及利害關係人得參與決策過程。執委會之提案過程皆是公開透明，公民及利害關係人都可透過公共諮詢平台 Have Your Say[33]提出意見及建議。執委會下設監管審查委員會(Regulatory Scrutiny Board)負責所有政策之影響評估(impact assessment)、適切性檢討(fitness checks)及特定審查(selected evaluations)。提案經執委會委員團(College of Commissioners)同意後，執委會會發布法律草案以及該草案之影響評估報告(impact assessment paper)，並且開放公民及利害關係人提供回饋。

(2) 立法流程

歐盟之立法程序由代表歐盟公民之歐洲議會、代表歐盟政府之歐盟理事會以及代表歐盟整體利益之歐盟執委會參與。歐盟政策須透過立法程序由三機構達成一致共識建立。

[33] 公眾諮詢平台 Have Your Say, https://ec.europa.eu/info/law/better-regulation/have-your-say_en



本報告之智慧財產權歸屬於國發會

依據歐盟運作條約(Treaty on the Functioning of the European Union, TFEU)第 289 條之規定，立法之程序分為通常程序或普通立法程序(Ordinary Legislative Procedure)以及特別程序(Special Legislative Procedure)。

在通常程序之情形下，執委會提交法律草案後會由歐洲議會以及理事會共同審查，必要時得提出修正案。若執委會不同意修正案，歐盟理事會僅能一致決定否決執委會之決定，若執委會同意修正案之內容，則有權撤回其提案。二讀會於三個機構無法就最終版本達成一致時進行，執委會及理事會得再進一步提出修正案。惟歐洲議會有權阻擋其不同意之理事會提案。修正後之法案會於歐洲議會及理事會同意後通過並公布於歐盟官方公報。若無法達成共識，將會成立協調委員會(conciliation committee)進行協商，歐洲議會及理事會仍可於此階段阻擋法案。

特別程序屬於普通立法程序之例外方式，原則上係針對較為敏感之法制政策領域，並未於 TFEU 具體描述，使用時機根據特定條約逐案而定，而由理事會為唯一立法者。就其程序而言，仍是由歐盟執委會發動，分為同意及諮商兩種形式，前者係由歐洲議會就提案以絕對多數(absolute majority vote)投票同意，且不得修改其內容，理事會無權否決議會此時之意見；後者則是由理事會在議會提交意見後通過立法提案，過程中議會可以批准、拒絕或提議對立之修正案，但理事會於法律面無需考慮議會



本報告之智慧財產權歸屬於國發會

的意見，但不得於未收到議會意見的情況下作成立法與否之決定[34]。

3. 因應社會變遷之規範或機制

歐盟為跨國性的國際組織，故其相關政策或法令規範的形成基本上係透過前述政策與法律形成之程序進行，著重於達成成員國間之共識，並未對於新興議題而有不同的程序規範。然而，其法律規範或法制政策的形式可以相當多元，強制力亦有所區別。其中對於各成員國皆直接產生強制力者，為「規則」(Regulations)，一旦完成立法程序則直接於全歐盟成員國適用。前述資料戰略規畫之兩項修法，包括 DGA 與 DA，以及近期歐盟陸續通過之 DSA、DMA、AIA、EMFA 等，都是規則的性質，具備最高的強制力，有助於針對密切相關之跨國事務，建立一致性的執法原則。

規則之下，常見之法制政策措施尚有「指令」(Directives)、「決定」(Decisions)、「建議」(Recommendations)、「意見」(Opinions)等法制政策類型。其中指令亦是以法案方式提出，走前述之立法程序，然而通過之指令如何於歐盟會員國實現，則需要各國依據國情另外再訂定或修訂內國法，使內國法符合指令指引之方向或要求。至於決定，則主要係針對更具體之個案所為之決定，可能僅針對特定國家所作成，例如 2023 年 1 月發布准許克羅埃西亞採用歐元之決定等。最後之建議與意見，則皆非有拘束力之法制政策，兩者皆是對於特

[34] European Council, Special legislative procedures, https://www.consilium.europa.eu/en/council-eu/decision-making/special-legislative-procedures/ , last visited 2025/3/26



本報告之智慧財產權歸屬於國發會

定事務提出看法，但不會對特定機構或對象提出強制性的要求[35]。

而歐盟面對數位科技相關議題之發展，主要還是依循原有法制政策形成之程序進行，並將歐洲單一數位市場實況與需求納入影響評估，選擇應採取哪類型之立法模式進行法制面之規劃。同時係以歐盟整體政策利益與戰略，作為法制藍圖擘劃之基礎，也是推動整體法制，凝聚共識之源頭。

(1) 建立多元政策參與工具，適時掌握應評估之法制政策

歐盟於法制政策層面與許多國家相同，有提供個人、事業、利害關係人、國家主管機關或其他組織等向歐盟提出建議或參與立法的管道。常見包括針對特定議題或政策規劃於網站進行公眾諮詢[36]，其中即包括法律修正草案之意見徵集。而除了對於執委會提出的政策或法制草案表達意見外，歐盟另有建立公民倡議管道，讓民眾得以呼籲執委會採取政策或法律之行動[37]，而對於如何發起倡議，必有論壇說明即專家協助，以利群眾提出有效之倡議，此部分做法與我國目前已實施之公共政策網路參與平臺概念類似。除此之外，歐盟亦有一個特殊的網路平臺－SINAPSE，以會員制網路社群之方式允許有共同興趣或專才之專家群體透過社群進行意見交換或研究，最終亦可能形成對政策或法律之建議。最後歐盟亦曾於 2021

[35] European Commission, Types of legislation, https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en, last visited 2025/3/26

[36] European Commission, Have your say-Public Consultations and Feedback, https://ec.europa.eu/info/law/better-regulation/have-your-say_en, last visited 2025/3/26

[37] European Commission, European Citizens' Initiative, https://citizens-initiative.europa.eu/_en , last visited 2025/3/26



本報告之智慧財產權歸屬於國發會

年 4 月至 2022 年 5 月嘗試舉辦一系列由公民主導對於如何塑造歐洲的未來進行辯論及討論。其中包括國家小組與歐洲公民小組，共計向歐洲議會及理事會提交包括 49 項提案之最終報告，主題涵蓋氣候變遷及環境、健康、更強大的經濟發展、社會正義及就業、歐盟與世界、價值觀與權力、法令規範、安全、數位轉型、歐盟民主化、移民、教育、青年與運動等多元議題。此一機制與前述機制不同之處，在於其並非常態性之意見討論，然而相關提案亦能被執委會納入年度工作計畫，從參與式民主的機制，快速且直接獲得法制政策需求與走向的提案，亦不失為即時有效取得政策或法制需求方向之機制[38]。

(2) 面對科技不確定性之新興法制規範模式

由於科技發展變化快速，法律制定之速度難以完全與技術發展變化相應，歐盟近年來在數位科技相關新興法制研議，已成為國際之領頭羊，其為何可以屏除各國面對發展快速且影響難以掌握之數位科技，尤其 AI 之發展與應用，直接且果斷的進行新興立法。除立法過程成員國意見充分討論以及立法前充分之影響評估外，規範當中嵌入之特別評估要求，亦可能係其得以直接投入前瞻性立法之保護機制。例如 AIA[39]、DGA 以及 DA 之通過，皆附加了對於法案影響評估之定期檢視或調查之條款，且規範模式日益具體，給予立法者足夠的空間，得以先行

[38] European Commission, Conference on the Future of Europe, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/conference-future-europe_en , last visited 2025/3/26

[39] Artificial Intelligence Act, https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng, last visited: 2025/03/10.



本報告之智慧財產權歸屬於國發會

就現況可評估之事務進行立法，再透過法制執行過程之調查與評估，滾動修正相關法制規範，使其更能貼近立法當時所無法預期的科技影響，逐步達到規範之綜效。相關規範舉例說明如下：

A. AIA 第 112 條

歐盟 AIA 於 2024 年通過，為全世界第一部具體以風險為規範基礎之 AI 監管法律框架。然而 AI 技術類型多元，應用層面廣泛，且變化快速。國際上許多國家未立即針對 AI 進行全面性之立法，即是考量 AI 發展與應用對經濟、社會、人民之影響有高度之不確定性。而面對此一預期影響高度不確定之技術發展，歐盟於 AIA 第 112 條特別設置因應技術發展之檢視修正以及法規滾動式調整特別規定，值得思考。

依據該條規定，執委會須於 AIA 生效後每年一次評估是否需修改附件三高風險 AI 系統以及第 5 條禁止 AI 作法之清單，並且須將評估結果向歐洲議會及理事會提交。而 2028 年 8 月前及此後每四年，執委會都需評估是否需修改現有法規分項標題或增加附件三之高風險 AI、評估是否需修正第 50 條需特別透明度措施之 AI 系統清單，以及評估是否需提出提高監管及治理有效性之修正案。此外亦須於相同時限、頻率下提出 AI 節能開發標準化之成果發展審查報告。2028 年 8 月前及此後每 3 年，執委會須就自願性行為準則之影響及有效性進行評估。



本報告之智慧財產權歸屬於國發會

於監管機構運作方面，同條第 5 項要求執委會須於 2028 年 8 月就 AI 辦公室之運作進行評估，確定 AI 辦公室是否有足夠之權力及能力達成該法所要求之任務。於整體法律層面，執委會則須於 2029 年 8 月，向歐洲議會以及理事會提出關於 AIA 整體之評估及審查報告，內容須包含該法之執行狀況評估以及機構於執行時解決或發現之缺陷或需求，並提出相關建議。

B. DGA 第 35 條

DGA 第 35 條規定亦設有對相關法規之執行後審查機制。該條規定，執委會須於 2025 年 9 月 24 日對法規整體進行評估並向歐洲議會、理事會及歐洲經濟及社會委員會提交調查報告，必要時得附立法提案。調查報告之評估重點內容包含該法處罰規則之適用及運作情形、非歐盟成立之相關事業組織遵守該法之程度、對非歐盟成立之相關事業組織執行處罰之可行性及程度、註冊利他主義之資料類型以及資料共享之公共利益目標概述。

C. DA 第 49 條

DA 第 49 條規定則要求執委會於 2028 年 9 月 12 日前向歐洲議會、理事會及歐洲經濟及社會委員會提交對該法之評估報告，包含特定章節之執行狀況、適用本法之訴訟提起次數及結果、自願資料共享機制之影響、對經濟資料利用之影響如資料貨幣及資料中介服務等、對智慧財產權之影響等法規整體適用執行上



本報告之智慧財產權歸屬於國發會

之影響評估。此外，該法尤其重視對中小企業供應商所生之影響，除須關注中小企業於創新能力、歐盟使用者可用資料處理服務及履行義務之負擔是否因法規之執行造成影響，亦須就其於定價及歐盟內部提供之資料處理服務多樣性提出影響評估報告。

綜上，AIA 針對不同項目設定相關時限以及頻率，要求執委會進行調查、審查、及修訂評估，並向歐洲議會及理事會提出報告。DGA 以及 DA 則是要求法規整體執行及應用狀況進行審查評估，必要時也需要附上立法提案，且 DA 特別要求特別關注中小企業之執行情形。前述三法皆是透過於法制面直接明定執法評估之期限與審查機制，有助於適時且循證進行法規調適。

(三)美國

1. 通常法案形成與立法程序

美國聯邦政府之憲政體制為三權分立，司法、行政及立法權利各自獨立並依憲法相互牽制。

美國憲法明確規定立法權歸屬於國會，由參眾兩院依職權進行立法提案，法案經國會通過後經由總統簽署方能生效。一般性法案可於參議院或眾議院提出，然而，依據美國憲法第 1 條第 7 項規定[40]，涉及徵稅、增加政府收入之法案，則必須由眾議院提出。美國總統並不能直接提出立法草案，

[40] The Constitution of the United States of America, https://www.senate.gov/about/origins-foundations/senate-and-constitution/constitution.htm#a1_sec6 , last visited 2025/2/24.



本報告之智慧財產權歸屬於國發會

但依據美國憲法第 2 條第 3 項規定[41]，總統得經常向國會報告有關聯邦政府運作之狀況，並以總統本人認為適當且必要之政策措施，向國會提出建議。故美國總統可透過國情咨文向國會提出立法政策層面之建議或意見，長期運作之下逐漸形成一種非正式之立法提案形式，但總統建議並不具任何法律上的拘束力，仍需經過國會正式之立法程序。實務上，除總統建議外，亦有可基於行業代表、公民、政治利益團體、選民或私人機構之要求提出起草建議，然而仍須將欲提出之法案，提供予可代表其意見之參議員或眾議員，才可正式提出立法議案。

(1) 政府立法政策評估體制

美國國會於立法前通常會對於個別法案進行評估，評估面向包括政策研究分析、預算與經濟影響分析、法令及憲法之審查、與利害關係人之協商以及立法預審公聽會等前期評估工作。

A. 政策研究分析(Policy Research & Analysis)

國會研究服務處(Congressional Research Service, CRS)是國會委員會及議員共用之專家人員所組成。CRS 共有 400 多名來自法律、經濟、外交事務、國防與國土安全、公共管理、教育、醫療保健、移民、能源、環境保護、科學和技術領域之政策分析師、律師及專業人士。其內部共分為 5 個研究部門，包括美國法律(American Law)、國內社會政策(Domestic Social

[41] Id, Art II Sec 3.



本報告之智慧財產權歸屬於國發會

Policy)、外交國防及貿易(Foreign Affairs, Defense and Trade)、政府及金融(Government and Finance)、資源科學與工業(Resources, Science and Industry)[42]。CRS之專家會從不同角度提供美國國會及議員於立法起草階段之政策影響報告或評估[43]。

除 CRS 對於立法起草進行之評估外，政府問責署(Government Accountability Office, GAO)作為獨立審查與評估聯邦政府支出、計畫及政策之監督機關，亦可能介入影響立法之過程。GAO 主要係就新法案對於經濟、環境或社會之潛在影響，協助國會評估是否可能制定更符合公共利益之法令。而國會審查法(The Congressional Review Act, CRA)為加強國會對聯邦機構規則的監督，要求聯邦機構在規則生效之前，必須向國會兩院和 GAO 總審計長提交一份關於每項新規則的報告以供審查。對於符合「主要規則」條件的規則，GAO 必須向國會提交一份報告，以確定該機構提交的檔是否符合所需的程序及步驟[44]。

B. 預算與經濟影響分析(Budget & Economic Impact Analysis)

國會預算辦公室(Congressional Budget Office, CBO)大部分由經濟學家或擁有高學位公共政策分析

[42] CRS Areas of Research, Areas of Research - Congressional Research Service (Library of Congress), last visited 2025/3/10.

[43] About CRS, About CRS - Congressional Research Service (Library of Congress), last visited 2025/3/10.

[44] Congressional Review Act (GAO), Congressional Review Act | U.S. GAO, last visited 2025/3/10.



本報告之智慧財產權歸屬於國發會

師等專家組成，並聘請律師、資訊技術專家、編輯及具有其他專業領域之人員。其中預算分析部門（Budget Analysis Division）負責分析新法之成本估算，及對各州、地方及私營部門等的成本評估[45]。

C. 美國國會聽證會(U.S. Congressional Testimony Pre-Legislative Hearings)

美國國會調查權乃自國會立法權衍生之一種監督權，其目的在確保國會有效、正確行使憲法賦予之職權。是以國會行使調查權之事由可包括對行政機關之監督、立法準備、政策形成、揭弊與報導、行使人事同意權及行使彈劾權等[46]。立法聽證主要係公開蒐集立法意見，並對立法之必要性及可行性作出判斷。另透過事前聽證會可先聚焦公眾對該立法之焦點議題及參考輿論對立法之支持程度。美國國會立法聽證會由國會委員會舉行，一般需準備該立法背景、相關法規及判決或學術論文等資料。立法聽證會由相關工作人員選擇來自不同背景的證人表達事實與意見，包括國會成員、政府官員、利益團體及學者精英。公民權益可透過聽證會直接或間接的被提出並影響後續立法。

(2) 立法程序

[45] CBO Organization and Staffing, Organization and Staffing | Congressional Budget Office, last visited 2025/3/10.

[46] 立法院編印，《97 年度立法院「美國國會調查及聽證制度運作實務」專案參訪報告》，97 年 9 月，頁 4。



本報告之智慧財產權歸屬於國發會

就聯邦立法之審議程序上，參議或眾議任一議院所做之決議，須提交給另一議院進行審議達成共識。如參眾兩院意見有歧異，則會進入協商委員會進行協商。協商成功則做成共識報告，並經兩院簽署後，送請總統於 10 日內簽署始可生效，總統享有否決法案之權利，但若經兩院覆議後，各院仍有 2/3 以上議員同意該項法案，則該法案仍可通過成為法律[47]。參眾兩院都設有具專業分工之附屬委員會，個別法案提出後會由參眾兩院之程序官員負責將提案分配至負責相關事務之委員會審議及研析，委員會則會於此階段召開公開聽證會，聽取各方代表意見後進行審議，決定是否提出此法案或決定擱置[48]。

作為聯邦制國家，美國政府各州及地方政府，並非為聯邦之下級機關，其享有高度之自主權。但在聯邦層級法令與州法相牴觸時，州憲法及州法律應以聯邦憲法或法令為優先。

各州之立法機構經選舉而產生，基本由上（參議）、下（眾議）兩院所組成。州議會主要負責制定、修改或廢除法律。法案通過後州長亦有決定是否簽署通過及否決之權利。

由於各州擁有高度獨立性，且因文化、經濟、產業、技術發展程度各不相同，所關注之立法議題亦有所差異。但相對於聯邦立法而言，修正或通過州立法之流程較為快速。例如近期為因應 AI 之發展，2024 年 4 月美國康乃

[47] US Constitution Article I, Section 7, Clause 2.

[48] United States House of Representatives, Consideration by Committee, https://www.house.gov/the-house-explained/the-legislative-process/in-committee , last visited 2025/3/26



本報告之智慧財產權歸屬於國發會

狄克州參議院即率先通過 AI 監管法案，透過制定保障措施，消除演算法之歧視風險。故就各州所關注之焦點議題，率先以州立法進行保護於美國為常見之法制現狀。

2. 因應社會變遷之規範或機制：美國總統行政命令

基於美國立法權專屬於國會，因此若要將特定事務以立法方式處理，則需要向國會進行遊說。常見影響是否提出立法之意見來源，包含政黨政策方向、媒體關注議題、利益團體游說、以及總統行政命令(Executive Orders)。而當行政命令之出現起因於國內遭逢之特殊狀況，且國家政策方向較為一致時，例如發生戰爭、經濟大蕭條、重大災害等，立法部門通常會有一定配合，包括加速使立法通過。

由於進入現代化社會之經濟及技術快速變遷，冗長之立法程序往往使社會關注度高且影響重大之問題無法可依，美國亦非成文法國家，無須所有事務皆走向法制化，行政措施或規則的建立亦可達成政策目的。美國總統作為行政權之最高領袖，可透過美國憲法第 2 條所賦予之廣泛的行政與執法權力，發布行政命令決定如何執行法律或管理聯邦政府部門之資源與人員。

如近年 AI 技術之快速發展，美國聯邦參眾兩院，針對 AI 議題實已提出多項立法提案，但皆未正式通過，無法立即處理 AI 開發及運用引發之諸多問題。對此，當時之 Joe Biden 總統即於 2023 年 10 月 30 日簽署通過第 14110 號[49]關於安全可靠且可依賴之開發及使用人工智慧之行政命令，旨在尚未

[49] Presidential Executive Order 14110 of October 30, 2023, FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence | The White House, last visited 2025/2/24.



本報告之智慧財產權歸屬於國發會

立法之狀況下先建立 AI 安全之新標準，確保美國於 AI 技術上成為國際領導地位，並保護美國人民免受 AI 風險之影響，同時要求相關部會分別於 90 至 180 日不等完成行政命令所要求之任務。然也因為行政命令之性質並非法律，雖於部分情況下有等同於聯邦法律之效果，但可能因為政權更迭而被推翻，相對不穩定，例如前述行政命令於 Donald Trump 總統上任後隨即予以撤銷[50]，且若總統所行之行政命令屬於國會授權予總統之權力範圍而非憲法賦予總統發布之行政命令，則國會可立新法將其撤銷[51]。故此一權限可以是美國因應新興科技議題得以由政府部門快速因應之管道，但亦有其不穩定之特性。

美國總統頒佈之行政命令可以由政府部門、管理及預算辦公室(Office of Management and Budget, OMB)或者總統（白宮）起草。OMB 並將進一步審核該行政命令若頒布，對財政預算可能產生之影響，並會同司法部下設的法制辦公室（office of legal counsel）審查其形式及合法性，最終由司法部長審核其合憲性及合法性。

行政命令設置之初，大多涉及日常之行政管理，例如組建重大組織行政議題或是人事事務。但有些行政命令已超出內部行政領域的範疇，造成直接或間接之外部效果時，雖不具備立法效果且未經過立法審議，但實則已有制定類法令框架，其中尤以直接透過行政命令建立規則制定及監管審查爭

[50] Trump 總統認為政府應鼓勵創新而非設置限制，故於 2025 年 1 月 20 日撤銷第 14110 號總統行政命令。

[51] US Congress, Executive Orders：An Introduction, https://www.congress.gov/crs-product/R46738 , 2021.03.29, last visited 2025/3/26



本報告之智慧財產權歸屬於國發會

議最大。故自 1970 年代起，美國開始建立跨部會管制分析監督小組(Regulatory Analysis Review Group, RARG)。

1974 年由於當時美國通膨嚴重，Gerald Rudolph Ford 總統發布「通貨膨脹影響聲明」的第 11821 號行政命令，旨在將經濟分析引入機構規則制定過程，要求聯邦機構發佈聲明，評估主要立法和擬議規則的通貨膨脹影響。爾後 Jimmy Carter 總統於 1978 年所頒布之第 12044 號行政命令[52]，要求針對新的管制規定進行經濟分析，並創建跨部會「管制分析監督小組」(RARG)檢視確認經濟分析狀況。1980 年因「日常文書工作減量法」(Paperwork Reduction Act of 1980)的制定，在 OMB 之下成立「美國資訊與管制事務辦公室」(the US Office of Information and Regulatory Affairs, OIRA)，其內部由約 45 位非政治任命之專家成員組成，包含經濟學、法學、政治分析、統計、資訊技術等背景。

OIRA 最初成立目的係為減少政府部門在資訊處理中之負擔，但在 Bill Clinton 總統於 1993 年發佈第 12866 號行政命令[53]後，OIRA 之職權開始逐漸轉向為檢視行政機關為履行其執掌所訂定之管制性規範（reviewing agencies' implementing regulations）。12866 號行政命令授權 OMB 應審查所有新舊重大監管行動，並要求 OIRA 在行動生效前進行審查，以避免規範出現不一致、不相容或重複之狀況，同時

[52] Presidential Executive Order 12044 (Jimmy Carter, 1978), Presidential Executive Order 12044 (Jimmy Carter, 1978) - Ballotpedia, last visited 2025/2/24.

[53] Presidential Executive Order 12866 of September 30, 1993, EO_12866.pdf, last visited 2025/2/24.



本報告之智慧財產權歸屬於國發會

亦要求各機關對於規範之收益與成本進行分析。依據該行政命令，啟動監管行動之重大法規政策行為包括[54]：

(1) 對經濟活動每年產生 1 億美元以上影響(現已提升至 2 億美元[55])，或對經濟部門、生產力、競爭、工作、環境、公共健康與安全，或對州、地方、部落等各級政府產生影響。

(2) 造成與他機關欲採取之行為嚴重扞格或干擾；

(3) 實質改變預算項目或受益人權利義務；

(4) 引發新法律及政策議題。

於審查規則之角度觀之，第 12866 號行政命令明確指出，每個機關必須在法律允許範圍內調整法規政策，將相關法規政策對社會造成的負擔最小化，並同時確保法規政策目標不變。而制定法規政策草案之機關，於提交 RIA 前需尋求其他機關之建議，如當法規政策與健康保險、移民、教育、能源、民權和勞工等議題相關時，法案擬定機關即會與國內政策委員會(Domestic Policy Council, DPC)進行草案之討論[56]。法案擬定機關提交 OIRA 後，其亦會根據法規整體之主題徵詢各機關對法規政策之意見。

2011 年 Obama 總統於 2011 年頒布第 13563 號行政命令[57]，重申並補充第 12866 號行政命令，以進一步改進規則制

[54] 法規政策影響評估制度之成本效益分析方法與實證個案—以美國為例, https://www.ndc.gov.tw/nc_1871_37797, last visited 2025/2/26.

[55] Presidential Executive Order 14094 of April 6, 2023, https://www.federalregister.gov/documents/2023/04/11/2023-07760/modernizing-regulatory-review , last visited 2025/2/26.

[56] 同前 54 註。

[57] Presidential Executive Order 13563 of January 18, 2011, Federal Register Notice, last visited 2025/2/24.



本報告之智慧財產權歸屬於國發會

定與監管審查機制[58]，並要求聯邦政府應以公眾參與、簡化、靈活、科學及回溯等五項原則制定法規。

該制度經長期運作及修改下，對於行政機關所擬規則制定和監管審查制度，實則已形成一套評估機制。相較於立法須通過參眾兩院冗長之立法審議程序而言，透過總統行政命令搭配OIRA審查制度，對特定或緊急議題之處理更具彈性。

(四)日本

1. 通常法案形成與立法程序

(1) 法制草擬及評估之流程

日本內閣設有內閣法制局，其職權為協助內閣審查提交內閣府之法案、政令、條約或進行法律規範之解釋，首長由內閣直接任命[59]。內閣之下設置內閣府，協助內閣處理各項政策事務，以不同政策領域區隔，由不同局/室襄理各政策領域事項，並依據不同子政策再設有相關會議或委員會，定期就所負責之政策領域舉行會議，制定政策方針以及計畫，必要時亦會提出相關法案建議。

內閣府下各省廳或行政單位就其所管之行政事務或施政目標之執行，若欲訂立新法或進行修法，需提出建議之法律案，為法律案之初步提案（法律案の第一次案）。初步提案會再依據相關省廳或行政單位之意見進行調整，視需要舉辦公聽會蒐集專家學者或利害關係人之意

[58] OIRA, About OIRA | The White House, last visited 2025/2/24.

[59] 內閣法制局，https://www.clb.go.jp/recent-laws/process/，last visited: 2025/03/21.



本報告之智慧財產權歸屬於國發會

見。最後由提案單位整合前述資料進行法案之起草（法律案の原案）。

法案起草後由提案之主管單位將法案提交予內閣法制局進行審查，審查內容包含法案之合憲性、是否牴觸現行法、法案內容之法律效力、立法目的是否明確、法律結構以及文字審查。經內閣法制局審查後之法案會進入內閣會議（閣議）[60]進行決議，經由內閣會議通過後即由總理大臣將法案提交至國會。

(2) 立法程序

日本之立法提案可由議員或內閣向議長提出。前者需由眾議院 20 人以上及參議院 10 人以上贊成提出，惟若為預算相關之提案則需眾議院 50 人以上、參議院 20 人以上贊成方得提出；後者則由各省廳提案，經過內閣會議決定後由內閣總理大臣提出，惟提案需經執政黨批准[61]。

法律草案提交後，會由議長將草案提交予相關委員會，全體議會得決定是否省略委員會審查之步驟。此外，重要之法律案則可舉辦公聽會、專家意見聽證會及相關委員會之聯合審查。前述程序結束後，法律案會進入審查階段，由兩院進行，基本進行程序為由議長報告、討論以及表決，若兩院之意見出現歧異，則會召開聯席會議進行協調，法案會於兩院達成協議並批准後成為法律。法律會由眾議院議長送交內閣，於國會通過 30 天內由首席國務

[60] 由內閣總理大臣及國務大臣（內閣幕僚）進行之會議。

[61] 參議院，參議院のあらまし，法律ができるまで，https://www.sangiin.go.jp/japanese/aramashi/houritu.html，last visited: 2025/03/10.



本報告之智慧財產權歸屬於國發會

大臣編號、簽署，並由首相會簽後發布，再於官方公報上公佈[62]。

2. 因應社會變遷之規範及制度

(1) 數位時代之規則及制度方法

2022 年 2 月，日本經濟產業省事務局於經濟產業政策創新小組委員會之產業結構第 4 次審議會中提出《關於數位時代之法規及系統[63]》之報告，該報告旨在檢視現行面對數位時代法制政策制定之現狀，檢視是否有必要進行調整，並提出得以因應數位時代發展之制度檢討方向。期望解決因數位技術發展，無法直接適用現行法之狀況以及無法及透過法律解決問題之困境。此次經產省之分析，實已提及日本早期於 2014 年起，為提升整體產業之發展，曾經透過《產業競爭力強化法》提出「新事業特別制度」、「灰色地帶消除制度」，及為促進新技術法規之修訂，便利實證測試以及數據之取得，而導入新技術實證之監理沙盒制度[64]。透過事業與政府間之合作，進行安全風險之測試[65]。上開制度是日本因應新興科技採用彈性法制體制之先驅機制。

A. 灰色地帶消除

---

[62] 內閣法制局，法律ができるまで，https://www.clb.go.jp/recent-laws/process/ ，last visited: 2025/03/10.

[63] 經濟產業省，事務局說明資料（デジタル時代の規制・制度のあり方について），https://www.meti.go.jp/shingikai/sankoshin/shin_kijiku/pdf/004_05_00.pdf，last visited: 2025/03/10.

[64] 同前註，頁 2。

[65] 同前註。



本報告之智慧財產權歸屬於國發會

此一制度主要係針對現行法規之規定於新興技術或事業活動之適用不明確，惟為使業者得展開其業務，透過法律特別規定新興技術或事業活動之相關事業，得依據其具體商業計畫，事先就規範之適用進行確認。如無人旅館業者透過住宿資料及消費者之臉部資料連結系統，進行消費者身分確認。因法規未有明確規定，故業者於法規修訂前透過灰色地帶消除機制，事先確認該行為並不違反「旅館業法」。

灰色地帶消除機制共分為事前諮詢、諮詢書提出以及主務大臣確認/回覆三個階段[66]。現行法主要規範於《產業競爭力強化法》第 7 條之規定，可由打算進行新技術或新商業活動之事業，提出期望就與其新技術、新事業活動相關適用之法令或命令等規定進行適用性之解釋。此一制度之落實，首先，須由事業向經濟產業省（經產省）之負責窗口(單一窗口)提出諮詢申請（亦可採取線上諮詢方式），不論欲諮詢之業務是否已開始實施，皆可進行諮詢。經產省收到事前諮詢申請後，會協助業者準備諮詢書，內容包含具體欲諮詢之相關法律/規定[67]。同時經產省窗口將負責與該議題所管相關省廳進行事前協調。諮詢書做成後會向負責該領域之主務大臣提出，主務大臣將於諮詢書受理後 1 個月內回覆事業。此外，針對該管大臣之回

[66] 經濟產業省，規制対応・規制改革参画ツールの活用に関するガイダンス-みんなの規制対応・規制改革，頁 17，https://www.meti.go.jp/policy/jigyou_saisei/kyousouryoku_kyouka/shinjigyo-kaitakuseidosuishin/press/20241217.pdf，last visited: 2025/05/02.

[67] 經濟產業省，新事業活動に関する規制について規定する法律及び法律に基づく命令の規定に係る照会書，https://www.meti.go.jp/policy/jigyou_saisei/kyousouryoku_kyouka/shinjigyo-kaitakuseidosuishin/250401_example_yoshiki9.pdf，last visited: 2025/05/02.



本報告之智慧財產權歸屬於國發會

覆，經產省並提供表單供申請者以及可能受該回覆影響之相關事業提出意見或需求。

B. 監理沙盒制度

此一制度主要用於檢驗創新技術於實際應用之可行性，並自演示中之資料來檢視法規之適用性[68]。例如新藥開發時之臨床監管制度，透過沙盒進行遠端資料蒐集並透過區塊鏈保存資料，經實證後確認該制度可行，且亦透過灰色地帶消除制度確認該作法並未違法，故得透過該方式進行新藥開發之試驗。

日本於 2018 年推出《生產性向上特別措施法》作為新技術實證監理沙盒機制的法源，該法於 2021 年廢止，廢止後依據該法所定之監理沙盒制度納入《產業競爭力強化法》中[69]。於第二章新技術實證、新事業活動示範之特別監理措施之第 6 條，針對新技術示範或新商業活動，亦可向主務大臣請求制定新法規之特別措施，分別依據第 8-2 條(新技術實證計畫)及第 9 條(新事業活動實證計畫)獲得主務大臣之批准。前者針對新技術之示範計畫，即為日本政府所認定之監理沙盒制度。而主務大臣於該計畫實施後，亦可依據該法第 14 條規定，評估特別管制措施適用情形、技術進步之狀況等事宜進行審查，並依據審查結果廢除或放寬所需之立法或其他措施。

[68] 參註 50，頁 3。

[69] 經濟產業省，「産業競争力強化」に向けて果敢な未来投資を後押し，https://www.meti.go.jp/policy/economy/kyosoryoku_kyoka/index.html），last visited: 2025/05/02.



本報告之智慧財產權歸屬於國發會

監理沙盒制度由內閣官房負責，事業可向內閣官房之窗口(單一窗口)提出諮詢，該單一窗口會協助事業撰寫申請內容以及重點整理，必要時諮詢相關主務大臣進行調整。其後由事業正式提出實證計畫認定申請。相關主務大臣（事業所管大臣、規制所管大臣）收受計畫並評估後，原則上須於受理申請 1 個月內將其意見提交至內閣府之新技術等效果評估委員會（新技術等効果評価委員会）審議。委員會審議完畢將意見回覆後，相關主務大臣須於 1 個月內須進行計畫核定[70]。核定後之實證計畫，於實施期間須進行定期報告，並於期限終了提出最終報告，由相關主務大臣進行審查，決定是否採取必要之法制措施或其他措施，包括廢除或放寬相關規定等事宜。

監理沙盒並未限定得申請之領域，主務大臣會聽取新技術等效果評估委員會之意見，並以以下任一條件進行判斷：(1)符合基本方針之適當性(2)預期新技術等實證計畫將能順利且確實進行(3)新技術等計畫內容不得違反《產業競爭力強化法》及其他相關法令[71]。目前已執行之計畫如電動滑板車共享事業行駛、區塊鏈技術臨床資料監測系統及不動產租賃契約電子化等案例。

C. 新事業特別制度

[70] 內閣官房，規制のサンドボックス制度(新技術等実証制度)について，頁 6-7，last viewed: 2025/05/02.

[71] 同前註，頁 9。



本報告之智慧財產權歸屬於國發會

以「事業為單位」，在確保安全及其他因素之前提下，為欲從事新興業務活動之事業提出特別措施及特別適用制度[72]。例如，事業欲提高電動自行車之輔助器倍率，使之超過道路交通法令所規定倍率必須設定於 2 以下的規範，而已特例制度測試將倍率設定為 3，最終於此特別制度測試實施後確認結果是安全的，即可將倍率 3 從特別措施轉變為一般性措施。

除前述已實施之機制確實已給予新興技術發展與應用模式之法制適用一定程度之彈性，然而仍有可加強的空間，故經產省本次報告亦提出五項促進革新之法制政策改善措施：

a. 確保法規及制度隨時更新

因應數位技術之更新，法規、系統及框架應不斷更新，以更有效地實現法律目標，早日實現數位化社會。為此，臨時數位調查委員會（デジタル臨時行政調查会）提出 5 項法制政策層面應遵守的「數位原則」，包括數位化完成及自動化、敏捷治理、官民聯合（公私協力）、互通性之確保以及共用基礎設施等。並考慮設立數位法制局（デジタル法制局）作為數位原則相關法規執行及審查之主管單位。

b. 強化法律及非法律規則之近用

考量數位技術發展難以全面以法律進行規範，政府應透過建立由國家設立之監管機構，及

[72] 同前註。



本報告之智慧財產權歸屬於國發會

與民間服務間的合作,提高法律及制度之可及性。法律及規定分為國家制定之法律、政令、省令以及告示通知、指南、指引等；國家以外制定之規則則包含獨立行政法人或法定團體之規則、指引等、民間團體之標準及技術規格等。

c. 法律機能強化戰略

加強政府之諮詢及支援系統，透過專家支援以加強中小企業及新創公司之法律功能，並利用制度框架促進相關法規之改革。具體作法包含設立以法規改革及新市場創造為核心之「顧問團」，讓專家協助創業、加強對地區中小企業及新創公司之法律支援以及強化經濟產業省及各省廳之諮詢制度運用。

d. 新興技術機構改革

針對新興科技領域，尤其對社會有重大影響之非同質化代幣(NFT)及無人載具領域,日本將綜合實施數位改革監管以及機構之改革，並以示範活動促進創新[73]。於 NFT 領域，經濟產業省與金融廳及數位廳等監管部門就法律議題共同合作。而於無人載具部分則是透過數位廳及各省之合作,建立特定區域,於其內進行無人載具之示範,並同時具體化相關技術及開發之規則。

e. 建立以資料法規為基礎之框架

[73] 同前註，頁 9。



本報告之智慧財產權歸屬於國發會

由於新興技術可能無法於現有法規框架下進行討論或一體適用於全民或消費者，因此應建立一全體國民及消費者資料都得以適用之法規[74]。

(2) 已知之因應措施及作法

A. 召集數位相關制度改革審查委員會

基於前述改進方案之評估，2023 年即由數位廳組織並召集數位相關制度改革審查委員會，以 2023 年 11 月 22 日為第一次會議。主要功能在檢視及推動日本相關法律規範與前述數位原則之一致性，建立檢視流程與機制。截至 2024 年 9 月 25 日已共計召開 7 次會議，逐步確保各級政府相關法規與政策機制符合數位原則，提升政府行政效率，促進資料之流通運用，並使法案符合時代所需。

B. 以指引調適新科技規範

此外，於具體法律建構之外，透過非法律軟法方式達成政策目的，亦是因應上開檢討而為日本政府近年來對應 AI 等數位科技快速發展之主要做法。例如，鑒於 AI 發展及國際上 AI 法制之建立，日本自 2023 年 5 月 AI 戰略會議開始陸續針對 AI 相關之監管進行政策研擬，以促進相關技術之發展同時亦提供安全之使用環境。2024 年 7 月以來，政府已於 AI 戰略會議下舉行 7 場 AI 制度研究會，研究會集結相關研究學者、地方政府、利害關係團體及公眾意見之蒐集針對 AI 制度之執行方式進行討論。2025 年 2 月，內閣

[74] 同前註，頁 14。



本報告之智慧財產權歸屬於國發會

府發布 AI 戰略會議期中總結[75]，為 2024 年之會議做出目前日本於 AI 政策方面之相關說明。

依據該期中報告，日本目前對於因 AI 而產生之問題，是以該領域之主管機關依據其內容以法律或軟法之方式進行對應。為能同時確保技術創新以及面對風險，日本政府目前傾向於法律以及指引等軟法之適當組合進行管理。原則上尊重業者自律，僅在業者無法自主應對之情形下透過法律進行規範[76]。若需要在既存規範以外之領域制定規範，則須注意新制度所對應之場合、對象以及可能造成之影響、風險以及對於必要權利之保護。

該期中報告亦指出，政府應制定普遍適用之 AI 指引，並鼓勵事業確保透明度及適當性。例如，日本總務省於 2024 年針對 AI 事業發布《人工智慧事業者ガイドライン（第 1.0 版）》[77]，並於同年 11 月增修 1.01 版。該指引對象為 AI 事業，包含開發、部署以及使用三類，並未包含非商業使用目的之 AI 使用者。該指引給予事業有效使用 AI 及管理風險之建議，包含應注意 AI 運用可能產生之歧視及偏見、個人隱私之保障、資訊安全以及相關問責義務等，期待能創造 AI 公平競爭之環境以及於各領域之合作及創新。此外，政府應調查並掌握各種風險之應對狀況及實際

[75] AI 戦略会議・AI 制度研究会，中間とりまとめ，https://www8.cao.go.jp/cstp/ai/interim_report.pdf，last visited:2025/03/09.

[76] 同前註，頁 10。

[77]総務省/経済産業省，AI 事業者ガイドライン（第 1.01 版），https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20241122_1.pdf，last viewed: 2025/05/02.



本報告之智慧財產權歸屬於國發會

使用條件，若出現或可能發生嚴重問題，應依據現有法規採取相應措施並給予必要之支援[78]。並且由於 AI 技術快速發展，政府應建立能快速響應之系統。政府於 AI 採購、利用及基礎服務應先透過各領域法規或指導方針做應對並持續與業界對話，AI 之風險治理需要透過公私合作建立。

(五)韓國

1. 整體科技政策評估

韓國自進入 20 世紀起即提出要以科技立國為理念，開始轉型自主研發。為提供科技發展強而有力之保障，韓國於 2001 年頒布制定「韓國科技基本法」(Framework Act on Science and Technology)[79]。該法案明確訂定科技政策與促進制度指定之規範。依據該法第 13 條，政府應定期預測未來科技發展趨勢以應付隨之而來之社會變化，並將該預測結果反映於科學技術政策中。基於此規定，政府通常需於科技基本計畫之前，就近期環境變化提出分析，並預測未來 5-10 年之科技趨勢，擬定前瞻報告提供韓國社會中長期需求及政策法令方向制定之參考。以最新 2022 年發布之韓國第六期科學技術前瞻報告(2021-2045)[80]為例（下簡稱前瞻報告），其由四個委員會進行，包含未來前瞻執行委員會(Future Forecast Executive Committee)及未來前瞻小組委員會(Future Forecast Sub-Committee)，由科學與技術、社會科學的專家組成，負責

[78] 同前註。

[79] Framework Act on Science and Technology, https://elaw.klri.re.kr/eng_service/lawView.do?lang=ENG&hseq=68217, last visited 2025/3/3.

[80] The 6th Science and Technology Foresight (2021-2045), https://www.kistep.re.kr/board.es?mid=a20401000000&bid=0046&act=view&list_no=42923, last visited 2025/3/3.



本報告之智慧財產權歸屬於國發會

檢視及協調整個科學技術前瞻調查的主要議題、為技術引爆點分析選擇目標、審視未來技術結果清單等。另外兩個委員會則是未來技術執行委員會(Future Technology Executive Committee)及未來技術執行小組委員會(Future Technology Sub-Committee)，主要負責未來技術選擇準則[81]。其委員會成員大部分為科學技術或社會科學領域之專家，本次報告預測未來 5 大趨勢及 12 項趨勢，並預測關鍵技術之引爆點，觀測何時這些技術將擴散普及，根據重要程度提醒政府優先採取之行動及提供政策法令方向之準備。而前瞻報告所提之相關預測內容通常會被反映在每 5 年制定之科技基本計畫(Basic Plan for Science and Technology)中，例如 2022 年 12 月公佈「2023-2027 年第五期科學技術基本計畫」(下簡稱第五期科技基本計畫)即提出包括量子科技、尖端機器人、AI 等 12 項國家重點培育科技，引入以任務為導向之創新研發系統等[82]。

依據現行「韓國科技基本法」第 7 條規定，韓國科學技術情報通訊部 (Ministry of Science and ICT, MSIT)部長應於每 5 年根據前述中長期政策目標制定中央行政機關之科技基本計畫，並經科學技術諮詢審議會(下簡稱「審議會」)後予以確定，相關中央行政機關首長及地方政府首長應依據有關規劃，制定並執行年度實施計畫中。科技基本計畫內容包括科技政策目標、新興技術推動方向、確保有前景之技術、人才投資推進策略、以及完善鼓勵科技創新制度或法律規定，例如依據第五期科技基本計畫，MSIT 應於 2024 年 2 月制定

[81] 科技發展觀測平台，科技議題「韓國第六期科學技術前瞻(2021-2045)」, https://outlook.stpi.narl.org.tw/index/tdop/4b11410082b117250183b06fac0c7a5f, last visited 2025/3/3.

[82] 科技發展觀測平台，焦點報導「韓國第五期科學技術基本計畫(2023-2027)」, https://outlook.stpi.narl.org.tw/index/focus-news/4b11410088c17ad40188c1b0a4cf00b4, last visited 2025/3/3.



本報告之智慧財產權歸屬於國發會

工作計畫，提出四大策略及 12 項關鍵任務，包含提升研發、推動創新、引領 AI 及數位轉型及加強數位技術包容性等措施，並提出法規調適重點應包括完善國內因應數位安全及監管之相關法令、制定 AI 基本法及數位包容法等法律配套措施建議等[83]。故韓國近期對於 AI 基本法等科技發展相關立法，與其科技基本計畫之政策評估密切相關。

2. 通常法案形成與立法程序

(1) 立法評估

科技基本計畫所規劃之各項政策目標，包括創新制度或法律規定，皆需回歸行政機構制定工作計畫以為因應，同時對於相關監督措施或法令規範擬定依據韓國「行政規制基本法」(행정규제기본법)[84]第 7 條第 2 項規定進行監管之影響分析與自我審查機制評估規範之方向或有無必要予以調整。法案立法公告期間，涉及該法案之中央機關首長必須將影響分析報告對外公布，並對所蒐集之意見進行審閱以於後續補充影響分析。且中央機關首長對於影響分析之結果，確定監督之對象、範圍及方式，經自律審查委員會審議後，須就法案之合法性進行審查，過程必須充分蒐集專家意見並於審查中切實反映。

所有中央機關在制定或修改法令時，須接受規章改革委員會之審查，準備前述影響分析，並經中央行政機關內部自律審查委員會審查後，提交規章改革委員會，其依

[83] MSIT's Work Plan for 2024, https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=964&searchOpt=ALL&searchTxt= , last visited 2025/3/3.

[84] 행정규제기본법,규제개요 > 관련법령 > 행정규제기본법 | 규제정보포털, last visited 2025/3/12.



本報告之智慧財產權歸屬於國發會

據所提交之影響分析審查新法規及法規調適之有效性，並建議必要時應撤銷、調整或改進新法案。未經規章改革委員會之審議者，不得制定或調整法規，法案經法務部審查並提交國務院時應附上規章改革委員會之審查建議[85]。

(2) 立法流程

韓國與美國同為總統制，該國雖沒有聯邦與州政府之區分，但立法需透過國會進行。

提案階段若是與科技相關之法令通常由相關部門（如科學技術情報通訊部）或國會議員提出，同一議題可能具備多個提案版本。國會對於各版本應進行多方討論及意見蒐集，確保朝野皆充分表達意見，最終將各版本進行合併後，將草案提交國會並由相關委員會進行審議及修正。

委員會審議後將法案提交國會全體進行表決，需半數以上在籍議員出席，並有過半數議員贊成後才可通過。如 2024 年年底所通過之韓國 AI 基本法，其共計合併 19 部提案，歷經 4 年時間才全部整合通過。與美國相似，法律於韓國國會審議通過後，須提交總統簽署，總統可於一定時間內簽署或退回國會要求再議，若總統簽署通過則法律會被公布並生效。

3. 因應社會變遷之規範或機制

綜上，韓國政府要提出修法建議並推動於國會通過，亦須經過複雜的過程，若要處理新興科技引發之法制需求，往

[85] 중앙 행정기관의 규제 영향분석 및 자체심사,규제개혁위원회 > 규제심사 > 심사절차 | 규제정보포털, last visited 2025/3/12.



本報告之智慧財產權歸屬於國發會

往無法及時反應。故除正規之立法程序外，亦搭配了其他相關機制，以確保在法令規範尚未修訂或訂定之前，提供產業研發及測試之安全環境。

(1) 監理沙盒

韓國於前述規章改革之審查架構之外，另有區隔領域別之監理沙盒機制，其特點係採取「臨時許可」的方式，允許事業經營者於訂限制條件（期間、地點或規模限制等）且並非適用全部或部分現行法規之情形下，讓採用新技術之新產品或服務得以於市場推行並進行測試實證，實證過程中並須蒐集相關資料以利後續合理的修訂相關法規系統。依循此一機制，韓國可以發給事業「臨時許可證」。有別於部分國家對於監理沙盒係以金融為主，韓國之監理沙盒類型範圍極大，繼 2017 年 12 月韓國引入此一制度，而於 2019 年開始實施後，以目前所公布的專業劃分沙盒領域，即包括 ICT 融合、產業融合、監管自由特區、移動性監理沙盒(透過移動之方法、基礎設施、服務或技術展開業務者，包括自駕車、無人機、共享移動服務、智慧人行道等)、循環經濟、創新金融、智慧城市、研發特區等。

韓國監理沙盒機制之推行涉及持續性多項法令之修訂及補充。自 2018 年 3 月開始已經陸續修訂包括「資訊通信融合法」(정보통신융합법)、「產業融合促進法」(산업융합촉진법)、「監管自由區法修正案」(규제자유특구법개정안)、「金融創新支援特別法制定法」(금융혁신지원특별법제정안)，及「行政基本規範法」(행정규제기본법)等規範。上開法令主要係規範各領域或



本報告之智慧財產權歸屬於國發會

類型監理沙盒機制之導入及運作、提供應用及諮詢之義務、授權監理之快速確認與例外規定、法律或法規修改申請制度、同案及類似案件快速處理通道等各項事宜進行規範之建構。上開規範，有部分係以特定產業領域作為規範範圍，如資訊通訊、金融創新等，亦有以產業發展型態劃分者，如產業融合促進法規範之沙盒，係以涉及該法所定義之產業融合新產品，也就是經產業融合產生的、具有顯著經濟技術帶動效應、性能品質優良的產品或服務為標的，所提供之沙盒機制，相關產業可就其所開發之產品或服務申請臨時許可。至於監管自由區法，則是以區域作為規範之標的，依該法第 3 章第 2 節可進行免監管特殊區域之劃定與臨時許可，提供新創事業或戰略產業可申請於該區域內進行所擬定之事業推動。

為支持具有技術能力但缺乏資金之中小或創新事業運用沙盒，2020 年 5 月建立「韓國商會監理沙盒支援中心」(대한상공회의소규제샌드박스지원센터)以提升事業諮詢及提出申請之便利性，降低產業利用門檻。自 2019 年起自 2024 年已指定 8 次監理自由區[86]。

(2) 為促進 AI 發展對應之做法

為執行科技基本計畫針對法令調適之方向，並因應近年來 AI 技術快速發展，韓國 2024 年 12 月通過「人工智慧發展及建立信任基礎的基本法」[87](Basic Act on the

[86] 監理沙盒歷史, https://www.sandbox.go.kr/sandbox/info/sandbox_intro#tab_login_02, last visited 2025/3/13.

[87] Basic Act on the Development of Artificial Intelligence and the Establishment of Trust, Korea passes AI Basic Act, second globally, enhancing national AI competitiveness - CHOSUNBIZ, ast visited 2025/3/13.



本報告之智慧財產權歸屬於國發會

Development of Artificial Intelligence and the Establishment of Trust，下簡稱韓國 AI 基本法)，整體對於 AI 之發展及監管做出規範，其中明確支持 AI 技術之發展，提出指定 AI 產業園區、建構 AI 實證基礎、設立 AI 資料中心等特殊配套機制，以協助促進技術開發及產業活化。

該法第 23 條透過指定 AI 產業園區，促進國家及自治團體從事 AI 事業之研發，提供相關資源及集中管理之環境，並提供行政及技術之支援，政府得設立或指定綜合支援相關業務專責機構協助並補助所需執行費用。就有關 AI 產業園區指定及撤銷、專責機構之設立或指定等必要事項，將由總統令後續定之。

該法第 24 條規定建構 AI 實證基礎，為支援 AI 事業開發或技術移轉實證、性能測試，建構並營運試驗、評估等所需之設施、設備及裝備等基礎設施建設並開放給 AI 事業者使用。有關實證基礎設施等建構、營運及開放等必要事項，將由總統令後續定之。

為解決資料訓練問題，韓國政府推進建構及營運用於 AI 開發與應用之資料中心。政府得提供建置資料中心所需財政及行政支援，協助中小企業及研究機構得以建置或使用 AI 資料中心等相關基礎設施，以促進區域均衡發展。

上開 AI 基本法為韓國科技計畫法制層面落實之展現，從其規範可以看出，其實際上亦考量到 AI 發展之不確定性，故於基本法當中鼓勵建構相關園區與試驗機制，為 AI 研發建立可測試開發之環境，並以特別規定建立國家投入之資料中心。惟其實際將如何運作，以及開發試驗



本報告之智慧財產權歸屬於國發會

事宜如何反應於法制政策層面，由於韓國 AI 基本法於 2024 年底通過，上述特殊機制之子法及配套措施尚未公布，執行成效尚無法評估，故有待追蹤後續法規、執行狀態與相關措施落實之成效。

(六)澳洲

1. 通常法案形成與立法程序

澳洲為習慣法體系(Common Law)之三權分立國家，依據澳洲憲法三項權力互相獨立並制衡。而澳洲之內閣主要係由內閣首相(Prime minister)及各部會首長（部長）(Ministers)組成，該制度為澳洲之慣例及實踐，並非依據憲法或任何法律，僅需滿足其集體責任及團結之原則。首相得決定其內閣組成之形式、結構以及運作模式[88]，內閣會議會針對政府認為須解決之議題進行討論，並做出代表內閣整體之結論。各部會之首長皆同時具備執政黨之參議員或眾議員身分（多為眾議員），故政府之政策或立法推動會透過內閣會議決定，並由相關部長以其國會議員身分於國會提出法案[89]。

(1) 立法流程[90]

澳洲之法源有由議會制定之成文法(statute law)、由行政部門（總理及部長）或政府機構制定之授權法(delegated law)以及由司法機構（法院）制定之習慣法

[88] Department of the Prime Minister and Cabinet, Cabinet handbook 15th Edition, at 5, https://www.pmc.gov.au/sites/default/files/resource/download/cabinet-handbook-15th-edn-august-2024_1.pdf.

[89] Id, at 17.

[90] Parliamentary Education Office, https://peo.gov.au/understand-our-parliament/how-parliament-works/bills-and-laws/sources-of-law#:~:text=Australia%20is%20governed%20by%20laws%20which%20are%20made,law%20is%20made%20by%20the%20Judiciary%20%E2%80%93%20courts., last visited: 2025/03/11.



本報告之智慧財產權歸屬於國發會

(common law)，而國會有權推翻授權法並制定推翻習慣法之成文法。

成文法之法案(Bill)由眾議院提出，經過眾議院三讀通過後交付參議院進行三讀程序，參議院通過後由澳洲總督(Governor-General)簽署成為法律。議會得於其成文法下授權行政部門或政府官員訂立法律，即為授權法。授權法與成文法具相同法律效力，其制定與修正不須經過議會同意，較為有效率，此類法律得減輕國會負擔並較能應對緊急情形或快速變化。授權法之類型包含規則(regulations)、決定(determinations)、地區條例(ordinances of territories)等[91]。惟議會之委員會有權審查授權法，並得推翻授權法。習慣法則為法官於法庭上作成之判決先例，成文法位階高於習慣法，故僅有在無成文法之情形下得適用習慣法。

2. 因應社會變遷之規範或機制

(1) 澳洲法律改革委員會

澳洲法律改革委員會(Australian Law Reform Commission, ALRC) [92]為一獨立機關，其主要功能在提供政府對於法律或政策上之改革建議。

[91] Parliament of Australia, Chapter 15 Delegated legislation, scrutiny and disallowance, https://www.aph.gov.au/About_Parliament/Senate/Practice_and_Procedure/Odgers_Australian_Senate_Practice/Chapter_15 , last visited: 2025/03/21.

[92] Australian Law Reform Commission, https://www.alrc.gov.au/about/ , last visited: 2025/03/21.



本報告之智慧財產權歸屬於國發會

澳洲政府於執行聯邦法律(Commonwealth Law)時若認為其因以下原因（包括但不限於所列原因）而需進行法案之審查或修改時得要求 ALRC 進行調查：

A. 公眾認為需要進行法律改革程序之議題。

B. 近期事件或法律案件顯示法律有缺漏。

C. 因科學或技術發展有法律增修之必要。

此外，澳洲檢察總長(Attorney-General)亦得依其認為需要改革之法律領域要求 ALRC 進行調查。ALRC 會將其調查範圍公開於其網站上，並於調查結束後發表最終報告。

調查開始時，ALRC 會組成諮詢會議或專家小組向利害相關人進行諮詢，對象可能包含相關政府單位、法院、學者、非政府組織、特殊利益團體、具特定專業或可能受該法影響之人。ALRC 會於個別案件成案後組成諮詢委員會或專家小組，委員會的組成會與各該案件所需之法律領域或相關特定領域專業知識進行拔擢。諮詢委員會協助 ALRC 釐清個案關鍵問題，並於研究或諮詢過程中提供評價。諮詢委員會於程序進行中就問題或提案等提供建議，但不會直接於 ALRC 所進行之調查中提出意見，最終建議仍是由 ALRC 根據職掌與法定流程提出。

ALRC 只要發布諮詢文件即會正式徵求各界意見，透過所回收的意見回饋，ALRC 可了解國內相關人等對於現行法之看法，以及可能需要如何調整法令規範。ALRC 並可就想要提出之法令修訂建議提案，於最終提出之前，透過此一諮詢機制向利害關係人測試其提案之可行性。



本報告之智慧財產權歸屬於國發會

ALRC 對於建議之評估，則必須盡可能確保其建議可以消除現行法令規範之缺漏、能簡化、更新法令規範或提供更適當之法制途徑。

最終報告做出後必須提供予檢察總長，而檢察總長須於收到最終報告後 15 個國會開會日內提交至國會，正式送交國會後方得公開。報告公開後，澳洲政府得決定是否執行部分或全部之報告建議，並針對報告給予回應。ALRC 並未規定政府回應之期限，惟其仍會於年度報告中追蹤政府之執行情況並給予建議。

(2) 為促進 AI 發展相對應之做法－指引訂定

2021 年於工業科學及資源部下設 AI 中心[93](National Artificial Intelligence Centre, NAIC)，支援及加速澳洲 AI 行業，協助事業開發及使用可信任、安全且負責 AI。

NAIC 發布《自願性 AI 安全標準[94]》(The Voluntary AI Safety Standard, VAISS)，協助機構得安全且負責地開發及部署 AI。該標準包含 10 個得用於 AI 供應鏈之護欄(guardrails)，包括透明度及問責性要求，並且說明於開發及部署 AI 時之注意事項。該標準及 10 個護欄為自願性安全標準，目的是促進 AI 產業之發展及產品信任度，並非創設新的法律義務，因此機構於開發部署 AI 時仍須注意遵守現有法律。

[93] NAIC, https://www.industry.gov.au/science-technology-and-innovation/technology/national-artificial-intelligence-centre.

[94] The Voluntary AI Safety Standard, https://www.industry.gov.au/publications/voluntary-ai-safety-standard.



本報告之智慧財產權歸屬於國發會

在 AI 隱私方面，涉及個資處理之部分都須符合隱私法及隱私原則規範。針對 AI，澳洲資料專員辦公室(Office of the Australian Information Commissioner, OAIC)於 2024 年 10 月發布兩份指引，分別為《開發及訓練生成式人工智慧指引[95]》(Guidance on privacy and developing and training generative AI models)及《隱私及使用商用人工智慧產品指引[96]》(Guidance on privacy and the use of commercially available AI products)。兩部指引皆指出 AI 技術之資料驅動將造成顯著之隱私風險，因此必須謹慎管理。同時強調對機構而言，於開發 AI 系統時必須採取隱私始於設計以及進行隱私影響評估、減輕 AI 生命週期之潛在風險。雖是針對事業在使用 AI 工具時須注意之事項給予指引，內容依然是要求業者必須遵守澳洲隱私法以及隱私原則之規定，以保護個人資料。

三、 我國法制現況

1. 通常法案之形成與立法程序

(1) 立法體制

我國為五權分立之體制，即行政權、立法權、司法權、考試權、監察權。其中就法案的形成，五院皆可依其職權提出法律案[97]，只是最終須由立法院依其立法權進行審議

[95] Guidance on privacy and developing and training generative AI models, https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-developing-and-training-generative-ai-models, last views: 2025/03/11.

[96] Guidance on privacy and the use of commercially available AI products, https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-the-use-of-commercially-available-ai-products, last visited: 2025/03/11.

[97] 立法院，立法程序，https://www.ly.gov.tw/Pages/List.aspx?nodeid=151 ，最後瀏覽日：2025/3/27



本報告之智慧財產權歸屬於國發會

並通過，立法院通過法律後送總統及行政院，若行政院未就通過之法律提出覆議，則總統須於收到後 10 日內公布。

(2) 提案來源

行政院之提案權屬行政機關全體，依據憲法第 58 條規定「行政院設行政院會議，由行政院院長、副院長、各部會首長及不管部會之政務委員組織之，以院長為主席。行政院院長、各部會首長，須將應行提出於立法院之法律案、預算案、戒嚴案、大赦案、宣戰案、媾和案、條約案及其他重要事項，或涉及各部會共同關係之事項，提出於行政院會議議決之。」故行政院提案須經行政院會決議後提出。

依據立法院議事規則第 8 條規定，立法委員提出之法律案，應有 15 人以上之連署；其他提案，除另有規定外，應有 10 人以上之連署。連署人不得發表反對原提案之意見；提案人撤回提案時，應先徵得連署人之同意。依據立法院組織法第 33 條規定，立法委員依其所屬政黨參加黨團，每一政黨以組成一黨團為限，每一黨團至少須維持有 3 人以上。符合立法院組織法第 33 條規定之黨團，除憲法另有規定外，得以黨團名義提案，不受本法有關連署或附議人數之限制（立法院職權行使法第 75 條）。因此，此等黨團亦具有提案權。

(3) 法案草擬階段



本報告之智慧財產權歸屬於國發會

依據「中央行政機關法制作業應注意事項」[98]，法規草擬應先確立政策目標並檢討現行法規狀態，若有現行法規可適用，得以修正現行法規不必草擬新法規。若無現行法規可適用者，方須草擬新法規。草擬時，涉及相關機關權責者，應會商有關機關；必要時，應諮詢專家學者之意見或召開研討會、公聽會；對於法案衝擊影響層面及其範圍，應有完整之評估。

而依據「行政院所屬各機關主管法案報院審查應注意事項」第 4 點規定，各機關研擬法案時，應先整合所屬機關、單位及人員之意見，整合後再徵詢及蒐集與法案內容有關之利害關係，或關注相關議題之機構、團體或人員之意見。必要時，並應諮詢專家學者之意見或召開研討會、公聽會。草擬法案後並須與其他相關之機關或地方自治團體協商，未能達成共識時，應將不同意見及未採納之理由附記於法案說明欄內。研擬法案時應由法制人員參與，並提請法規會或法制專責單位討論及表示意見。國家發展委員會(下稱國發會)已於國內推動法規政策影響評估機制(Regulatory Impact Analysis, RIA)機制。我國目前就 RIA 之實踐，自 2004 年起業針對行政機關制(訂)定、修正法律與法規命令，先後於「中央行政機關法制作業應注意事項」及「行政院所屬各機關主管法案報院審查應注意事項」等，將法案衝擊影響評估等機制融入法制作業程序。其中法律案，行政院業於 2013 年訂定「法案及性別影響評估檢視表」（下稱檢視表），納入 RIA 報告應具備事項，包括問題界定、政策目標、公眾諮詢、成本效益分

[98] 「中央行政機關法制作業應注意事項」，746635CEACE71002，（最後瀏覽日：2025 年 3 月 4 日）。



本報告之智慧財產權歸屬於國發會

析及評估結果等，並要求各機關將法律草案陳報行政院時，須併附檢視表。

為因應臺美貿易協定之良好法制作業規定，國發會亦曾發函各部會提醒應採取適當步驟進行法規影響評估並予以揭露。而我國參考澳洲、紐西蘭、英國、加拿大等政府及歐盟之操作手冊，曾建議各機關 RIA 遵循作業步驟分為 2 階段共 8 步驟進行[99]，並製作 RIA 報告：

A. 第一階段：形成政策階段

a. 政策分析

I. 步驟 1 描述政策背景：行政機關於提出法案時，應就所規劃之政策願景完整說明，陳述政策影響評估作業可能涉及的主題或方向，以利於後續諮詢與分析工作之進行，俾確認政策目標是否具正當性與合理性。內容應包括背景發展及現況說明、政府介入之必要性、政府過去迄今之作為及政府作為或不作為之效果。

II. 步驟 2 釐清政策問題：應釐清問題現況之核心，以及提供具體數據或方式呈現該問題未來之變化發展，推估後續問題之嚴重性，並列出所涉重要利害關係對象，並釐清問題主要成因。

III. 步驟 3 設定政策目標：釐清政策問題後，必須清晰地設定政策目標。政策目標是評估各預擬對策方案的最終指引，由於政策目標就是阻止問題惡化的反

[99] 法規影響評估之作業流程及步驟（附件 2），https://www.ey.gov.tw/File/414EF7B1C1460728?A=C ,last visited 2025/3/13.



本報告之智慧財產權歸屬於國發會

義詞，因此政策目標設定的最重要原則，乃根據政策預期解決的核心問題，陳述政策未來所欲達成的願景狀態。所設定的政策目標，建議為「結果型」，或至少為「產出型」的目標，才能真正與欲解決之問題間緊密相扣，政策目標本身也會更具有正當性，獲得社會民眾支持。政策目標如均為「過程型」，未來將難以評估所選定對策的執行成果，是否能真正減少問題的惡化。

IV. 步驟 4 研擬對策方案：對策方案因其主要內容可歸類為管制類或非管制類工具。管制類對策方案之共同特點是，政府機關對於人民自由行使基本權利或自由從事經濟商業活動，必然施予一定程度的限制，且違反限制者必然受到行政處罰或刑罰。非管制性的對策方案則是依賴經費補助、獎勵、教育宣導、資訊提供、技術協助、價值訴求等方式，鼓勵人民接受政策方案。

b. 影響評估分析

V. 步驟 5 預評估對策方案：了解比較相關對策方案可能影響之程度，俾供後續決定適切對策方案外，亦可藉此程序強化國家預算支出效率之正當性與合理性，具體說明各方案之影響、指出主要利害關係人之影響狀況，對政策方案之進行質化或量化之成本效益影響分析。

VI. 步驟 6 諮商利害關係者：機關應先思考哪些利害關係者應該列為諮詢對象，包括產業組織、勞工組織、倡議組織、公民個人、智庫、專業顧問公司、大學



本報告之智慧財產權歸屬於國發會

研究機構、地方政府等代表，並秉持資訊透明公開化原則，辦理各種諮商，將踐行前述步驟 1 至步驟 5 分析所得結果與相關資料作成諮詢文件。機關應視諮商的開放程度模式，選擇一種以上適合的方法，例如公聽會、研討會、焦點團體討論、面訪、專家會議、調查、問卷徵詢、聽證會或商議民主方法中的特定諮商技術等等。隨著資訊科技的普及，機關亦可積極使用網路作為平臺。為確保諮商能獲得有意義的意見資訊，並取得外界的信任，建議至少提供 1 個月以上諮詢期。

VII. 步驟 7 選定最終執行方案：經諮商公眾意見，決定最終方案後，其 RIA 報應注意於此階段就前述步驟 1 至步驟 5 所撰之諮詢文件內容不得變更，僅得於報告中補充原方案預評估之質化或量化方析、採用公眾諮商所提方案之分析，並於報告中敘明諮詢過程中之蒐集意見採納與不採納之理由。

B. 第二階段：形成法規草案階段

VIII. 步驟 8 預告法規草案：當機關完成 RIA 政策分析與影響評估作業，最終決策擇定方案，並據以制（訂）定或修正法規，形成法規草案後，應進行法規草案預告（現行預告要求詳（4）報院審查前流程說明）。為強化與國際規範接軌，落實開放透明政府，俾利對外洽簽國際投資及經貿協定，各機關研擬之法律或法規命令草案，一併公告於「公共政策網路參與平臺」徵集意見。

(4) 報院審查前流程



本報告之智慧財產權歸屬於國發會

依據中華民國 114 年 2 月 19 日院臺規長字第 1145002532 號「法律、法規命令草案預告前及法律草案報院前之控管機制」函文[100]公告，考量法律、法規命令草案涉及社會高度關注之重要或敏感議題之重大事項，不論外界有無爭議，均有必要於辦理預告前及法律草案報院前通報行政院。規範內容如涉及社會高度關注之重要或敏感議題之重大事項，應於預告前填具「涉及重大事項之法律或法規命令草案預告前通報單」，另若涉及重大政策之事項或具時效性，應於報院前填具「重大或具時效性法律草案報院前通報單」。前述通報單應於草案預告前先行提交行政院，並於通報時一併檢附擬預告草案。

若不屬前述類型之法案，無需經過行政院預告前通報審查，則草案研議完成，應進入草案預告之流程。草案於預告階段，各機關應徵集公眾意見，並將意見製作成意見表。依據中華民國 112 年 10 月 23 日院臺規長字第 1125021127 號「法律及法規命令草案之預告期間」函文[101]公告，法律草案預告期間之相關規定如下：

(一)法律草案與貿易、投資或智慧財產權有關者，應至少預告 60 日。但情況急迫者，得免預告；有下列情形之一者，得另定較短期間，並應於草案內容公告時，一併公告其理由：

[100] 法律、法規命令草案預告前及法律草案報院前之控管機制，https://www.ey.gov.tw/File/7B19FD9A2624D0F?A=C，最後瀏覽日：2025/5/6。

[101] 法律及法規命令草案之預告期間，https://www.ey.gov.tw/File/F9C54E3AB7C69FCF?A=C，最後瀏覽日：2025/5/6。



本報告之智慧財產權歸屬於國發會

1. 為遵行國際條約、協定或國際組織之決議、為維護公共利益之必要、為避免發生安全、衛生或環境保護等相類之緊急問題，有儘速施行之必要。

2. 法規內容係授予民眾利益或對民眾權益無實質性影響。

3. 單純文字修正。

4. 配合其他法規修正或廢止。

5. 其他為配合重大政策經主管機關審認有必要之情形。

(二)法律草案與貿易、投資或智慧財產權無關者，各機關得衡酌是否辦理預告。

待完成預告後，應將相關文件報行政院進行審查，審查通過後則進入立法審查程序。依據「行政院所屬各機關主管法案報院審查應注意事項」第 6 點，各機關報院審查時，應檢附下列資料：

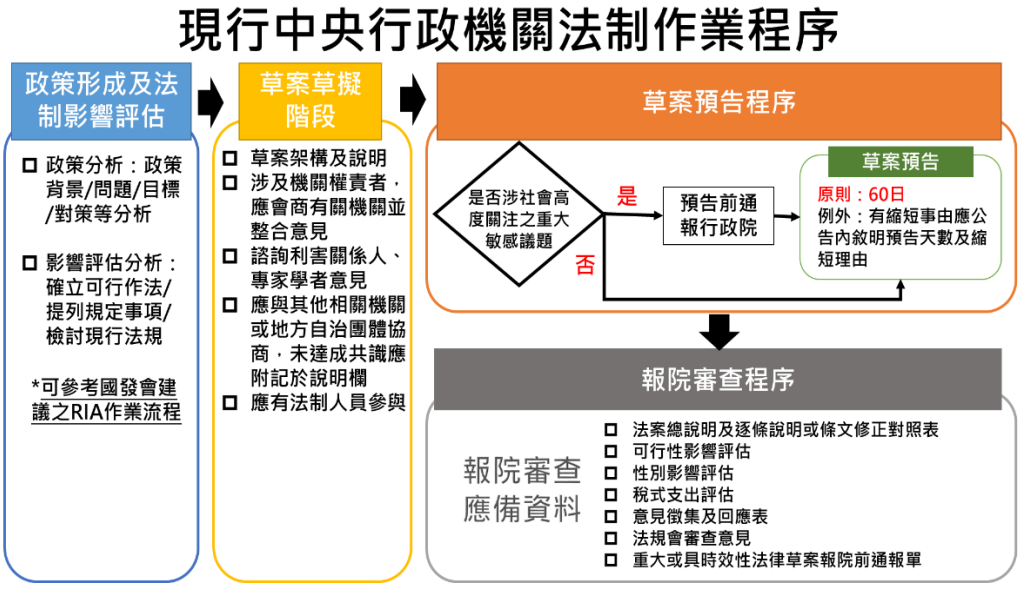
1. 總說明及逐條說明（制定案）或條文對照表（修正案）。

2. 第 3 點各款規定及已踐行第 4 點所定程序之相關文件及其他參考資料。包括草擬階段之可行性評估、性別影響評估、稅式支出評估、法規會或法制單位審查意見、草案預告期間意見回應表等。

前項法案為法律制定案或修正案者，應於報院函中敘明是否英譯，並副知法務部全國法規資料庫工作小組。



本報告之智慧財產權歸屬於國發會




資料來源：本研究自行繪製

圖 1 現行中央行政機關法制作業程序

(5) 立法審議

立法提案草擬完成後，在送立法院審議前，各機關可依據情況先經過內部討論，或可舉辦公聽會，讓利害關係人得以表達意見，連同草案預告蒐集之意見適切回應後，將法案提交行政院進行後續審查及送立院審議相關程序。法案送交立法院後，則係依據立法院議事規則第 15 及 16 條規定，提交程序委員會編列議程、報告及討論事項，進行法案排程，進入一讀審查程序，進行立院表決，若各委員會針對法案進行實質討論及修正，則交由立法院內各委員會審查進入付委程序，此時可能舉辦公聽會邀請相關利害關係人出席，針對較有爭議之法案，各委員會還可決定是否送交黨團協商，避免政治立場不同致議事癱瘓。但依據立法院職權行使法第 8 條第 2 項，若經



本報告之智慧財產權歸屬於國發會

立委 20 人以上連署或附議，並表決通過則不用再經過委員會審議，逕付二讀程序。進入二讀流程將逐條針對條文進行深入討論及表決，若通過二讀則法案基本已定型，進入三讀定稿程序通過後，送交總統及行政院，若行政院無覆議則由總統公布生效。

2. 因應社會變遷之規範或機制：法規調整規定

為因應全球國際環境之變動，加速相關法規調適、提高彈性及機動性，自 2017 年起，行政院推行「啟動法規鬆綁-從函釋開始」之政策，認為各部會應以人民幸福有感、排除投資障礙及減輕遵法成本為目標，檢討鬆綁函釋、行政規則及法規命令等管制措施，從函釋開始建立便民之法制環境。

(1) 法規鬆綁方式[102]：

A. 優先檢視鬆綁令釋（函示）、行政規則及法規命令等規定。包括：

a. 令釋（函示）指依行政程序法發布之第 2 類具外部效力之令函、依行政裁量所作之解釋及目前各機關以個案函示做為通案援用者。

b. 行政規則指本於職權訂定之內部作業規範。

c. 法規命令指法律明確授權訂定者。

B. 強化機關法規自主檢視機制，以人民有感為鬆綁目標並採行效益管考方式，機關須說明法規影響對象及因鬆綁可受惠之對象及人數等。

[102]國家發展委員會 106 年 10 月 26 日發布「啟動法規鬆綁-從函釋開始」政策懶人包，https://www.ey.gov.tw/File/8B509B59F76570F3?A=C，頁 3，(最後瀏覽日 2025 年 3 月 13 日)。



本報告之智慧財產權歸屬於國發會

(2) 法規鬆綁方向[103]：

A. 簡化行政程序（例如申請及審查流程）。

B. 在符合法律前提下，針對於新興商業模式未涉法律禁止或限制規定者，應優先考量採取管制以外之管理措施。

C. 行政機關因執行法令就具體個案所為之函示，應考量個案事實間之差異，不宜逕將個案函示當作通案處理。

D. 逾越法律授權訂定過多管制規範的函釋，應即廢止。

E. 法律所授權訂定的「其他相關管理事項」，目前各部會在此授權下訂定過多管制規範，應重新檢討，刪除不符立法意旨的內容。

F. 為執行法律所訂的內部行政規則規定，應朝彈性處理。

國發會對於法規調整之推動已行之有年，也為此成立新創法規調適平臺窗口，推動各部會啟動並持續進行法規調整作業以排除投資障礙，多年已有相當之成果。

(3) 現行面對新興科技發展與應用法規調適所遇到之問題

近年來因應科技快速發展，尤其高速網路、演算法、平臺與 AI 之出現與迅速發展，使得國內法制適用不斷面對各項衝擊，而法案研商與修訂之速度往往無法符合實務所需，甚至有新興利法草案一出現，即備受爭議之情

[103] 同前註，頁 4，(最後瀏覽日 2025 年 3 月 13 日)。



本報告之智慧財產權歸屬於國發會

形。觀察近年來相關科技法制適用、規劃或提案所面臨到之問題，大致有以下幾點：

A. 科技政策之提出未必併同納入法制政策配套藍圖

依據我國「科學技術基本法」(簡稱科技基本法)第 10 條規定[104]，政府應考量國家發展方向、社會需求情形及區域均衡發展，每 4 年訂定國家科學技術發展計畫，作為擬訂科學技術政策與推動科學技術研究發展之依據，並應參酌中央研究院、科學技術研究部門、產業部門及相關社會團體之意見，並經全國科學技術會議討論後，由行政院核定。前述全國科技技術會議，每 4 年由行政院召開之。另依該法第 9 條[105]規定，政府應每 2 年提出科技技術發展之遠景、策略及現況說明。於實際運作上，「國家科學技術發展計畫」形成中長期科技政策之後，環顧國內外趨勢、科技與社會狀況及各界需求等，2 年後運用科學技術白皮書(或科技發展策略藍圖)進行檢視並調整科技政策的方向，透過不斷地與時俱進，建立完善的科技政策循環機制。

除中長期科技政策外，行政院自 2016 年起啟動「數位國家・創新經濟發展方案(2017-2025 年)」(簡稱 DIGI$^{+}$方案)，為因應未來智慧國家發展願景，更名為「智慧國家方案(2021-2025 年)」，訂定「2030 實現創新、包容、永續之智慧國家」為願景，將資源整

[104] 科學技術基本法, https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=H0160028, 最後瀏覽日 2025/3/24。

[105] 同前註。



本報告之智慧財產權歸屬於國發會

合聚焦於四個主軸構面：「數位基盤」、「數位創新」、「數位治理」及「數位包容」，以促進社會整備(Society Ready)為核心之目標，為實現主軸目標，行政院核定包括「前瞻基礎建設之數位建設」、「臺灣 AI 行動計畫」、「資安產業發展行動計畫」、「臺灣 5G 行動計畫」、「臺灣顯示科技與應用行動計畫」、「台灣運動 x 科技行動計畫」、「臺灣 AI 行動計畫 2.0」等跨部會合作之重大數位政策[106]。

整體而言我國與韓國相同，有科技基本法引領之全國科技技術會議及政策研議，也有如同歐盟之發展戰略，針對新興數位科技或數位國家整體發展，提出的整體政策發展規劃。然我國在相關科技政策規劃過程當中，法制政策配套層面之考量，則未必有納入整體藍圖的評估，或雖有部分納入方案或計畫文字，卻欠缺對應之執行方案，或僅有點到為止說明有推動之必要性，卻沒有納入執行計畫等。其可能原因在於政策方案或行動計畫之提出，主要是由各部會就國家特定政策目標由下而上所提出，雖有部分議題由上而下提出指導，卻未必在技術研發或產業推動考量下納入法制需求評估之層面，以致到最終技術要落實或進一步開發時，才發現於適用法律產生障礙。

B. 法令制定過程未充分溝通致使爭議過大無法推行

雖然我國推行法規政策影響評估機制已行之有年，惟評估之方式及成效仍須仰賴各法案研議主管機

[106] 智慧國家推動小組簡介，https://digi.nstc.gov.tw/Page/A1701D7654C6B83C，最後瀏覽日 2025/3/24。



本報告之智慧財產權歸屬於國發會

關之落實。近年來面對歐盟快速且持續通過各項數位平臺法案，我國部分機關為因應整體國際發展趨勢，亦曾快速提出修法草案，然而卻因為欠缺事前充分討論及意見溝通而無法順利通過。例如國家通訊傳播委員會(NCC)於 2022 年曾參考歐盟 DSA 發布之「數位中介服務法」草案，望藉由法規促使大型線上平臺之透明化，並要求平臺負起「守門人」的監督責任，對其服務內容及言論加以規範。然而，該法案因所涉資訊服務業者範圍極大，並未考慮國內產業狀態與歐盟市場狀態之差異，而未於預告前充分調查、討論及溝通，而於預告後引發高度爭議。雖於後續舉辦 3 場公開說明會邀集業者表達相關意見，但仍因法條不夠明確與技術層面之質疑、是否會限制言論自由、資料調取權等議題造成社會重大不認同，甚至被質疑為「強推草案」，最終由行政院要求 NCC 暫緩草案之推動，要求應積極溝通獲得大眾共識再予提出[107]。

C. 法制政策建構欠缺彈性/敏捷之調適機制

我國目前已有極為完整且行之有年之法制作業程序，且亦已引入架構清晰之 RIA 機制，就立法及法規影響評估之層面，相較於本文前面整理之國際法制政策形成機制，並未有很大的落差。然而，面對新興科技的議題，法規調適之需要如何被迅速發現及因應，除近年推動之公共政策網路參與平臺機制，給予

[107] 數位中介服務法草案爭議問題，https://ai.iias.sinica.edu.tw/controversial-draft-digital-intermediary-service-act/，最後瀏覽日 2025/3/24。



本報告之智慧財產權歸屬於國發會

民眾提案之管道外，尚未有其他進一步可取得或評估法制需求或政策之彈性或敏捷因應之機制。

OECD 提到「為實踐創新之敏捷及適應性監督，須建立得靈活應對技術變化並具前瞻性之監督體系，確保法制政策不會對技術創新造成阻礙。政策制定時得透過實施漸進式之戰略預測新興技術趨勢，並定期檢討監督機制」。歐盟於 AIA 中已有納入針對 AI 之技術發展必須滾動式進行修正之條文，澳洲法律改革委員會亦有針對科學或技術發展有法律增修之必要納入啟動評估之項目，提供政府對於法律或政策上之改革建議。我國目前新興立法則較為仰賴政府部會及其智庫幕僚自行發掘，或專家、產業呼籲等非制度化之作法進行處理或評估，以致法制政策反映較為緩慢。

D. 主管機關各自為政，無法形成法制政策之橫向連結

晚近許多涉及數位科技研發與實務應用發展產生之法制問題，基於數位匯流高度發展之跨領域產業型態，以及技術應用之多元化，與傳統國內目的事業主管機關之分業管理邏輯已有極大差距。導致新興議題應有何機關著手評估法規調適之需要，形成最大的爭執。且所涉之法制議題，亦未必屬於單一機關主管法律所能處理，尚需進行藍圖式之法制整備，此時則可能因為缺乏主導機關而無法有效率的形成共識，並有效進行法制因應。故如何規劃適切之模式促進不同主管機關於法制政策面之合作與橫向連結，將十分關



本報告之智慧財產權歸屬於國發會

鍵。例如 OECD 建議應建立跨組織功能及跨管轄區域之監督合作機制即是適例。

E. 除少數領域外，欠缺足夠之監理沙盒相關機制

因應科技發展，部分國家採取程度與類型不一之監理沙盒機制，以降低法制政策因無法預期科技應用或上市之影響，而無法適時或適當修訂，或採行適切因應措施（如函釋或指引）之問題。我國目前於監理沙盒層面，有包括金融科技[108]、無人載具[109]及產學合作[110]三類領域可開放申請創新實驗，併有相關法規進行規制。然隨著科技發展迅速，以及類似科技可應用之範圍或領域日漸廣泛（如 AI 相關應用），僅有少部分侷限領域之監理沙盒是否符合需要，則有必要予以檢視。上開韓國之沙盒制度雖有針對產業，但對於技術融合及產業領域設定極廣，且持續因應新技術進行擴增。日本之沙盒制度亦非係針對特定產業領域而來，而係只要技術應用市場化，有企業創新發展之需求皆可提出申請，其可動之法規調適之檢視範圍，較我國為廣。

四、 小結

(一)國際趨勢綜整

整體而言，國際主要國家或國際組織，即使面對新興科技發展帶來的社會經濟變化，原則上並未改變其法制評估與建構之機制。具體

[108] 金融監督管理委員會於 2018 年 1 月 31 日制定「金融科技發展與創新實驗條例」。

[109] 經濟部於 2018 年 12 月 19 日制定「無人載具科技創新實驗條例」。

[110] 教育部於 2021 年 5 月 28 日制定「國家重點領域產學合作及人才培育創新條例」。



本報告之智慧財產權歸屬於國發會

法規之研析與調整，仍須依據法定之立法程序與體制進行處理。只是各國因政府組織體制與權限上之差異，而可對於急迫性之法規調整或跨領域之議題，有相關協商與較為快速之處置方式，或為新興科技所需法制政策之發現，採取不同管道提高發現問題，與研析解決方案之效率。此外，於法制本身之研議上，面對科技影響之高度不確定性，則有如同歐盟近期科技立法之作法，明確規範不同法制執行評估之時間與重點。或於整體政策面向具體評估技術及產業發展所面臨之問題，同時對應所需建構或修訂之法制規劃，並按照所規劃之法制政策藍圖具體落實。

1. 科技政策整體推動規劃，納入法制層面之評估及意見徵集，對應提出法制推動藍圖

   歐盟每 5 年透過歐洲戰略議程擬訂未來 5 年之政策大方向，就重點政策提出相關研究或工作報告，並提出訂立相關指引或立法建議。歐洲執委會則進一步確認立法規劃，並就新立法提案進行影響評估報告，並開放公民及利害關係人提供回饋意見。

   韓國則係透過科學戰略會議，確認其政策方向及因應該政策應進行哪些相關之法令調適。日本則是以內閣向下之政策領域分工，並依據不同子政策再設有相關會議或委員會，定期就所負責之政策領域舉行會議，制定政策方針以及計畫，必要時亦會提出相關法制提案，就提案徵集各界意見。

   足見主要國家多數認為，因應新興科技的影響，整體政策推動必須納入法制面的評估與思考，且透過公眾意見的取得，會是最為貼近實際需求也經濟之方式。

2. 選擇彈性較大之法制政策手段處理新興急迫之重要議題



本報告之智慧財產權歸屬於國發會

各國對於立法程序皆採嚴謹之審查程序，以確保法律之制定不致造成社會經濟過度之損傷，並能有效達成政策目標。故即使是涉及科技之議題，亦並未調整法律建構之流程與做法，已如前述。然而，並非所有科技引發之法制適用問題，皆需要透過最高層級且最嚴格之立法手段來進行，而各國於其不同之政府組織與權限體制下，多仍有可彈性運用之方法，可迅速解決問題或至少降低法制適用上之疑慮或障礙：

(1) 美國總統行政命令，利用行政權快速解決法制障礙

美國基於其總統制與憲法賦予總統之職權，對於如同 AI 等新興科技帶來的影響，可以先行透過總統行政命令方式，對於各機關相關因應作為提出要求，雖非法律但具強大的行政執行力。但也因為其並非經過國會正式通過之法律，國會可以透過訂定新法予以撤銷，新上任之總統亦法發布新的行政命令取代前手頒布之行政命令，故此一作法雖具有彈性但卻相對不穩定。

(2) 制定相關指引，擇定彈性作為提供產業依循方向

針對科技新興議題，在尚未立法確定前，各國皆嘗試訂定相關指引，以協助已正在運用之大眾，予以相應提醒。以日本為例，其通常應對新興科技時，是以該領域之主管機關依據其內容以軟法之方式提供相關利害關係人參考。日本政府傾向於以軟法之方式，原則上尊重業者自主，僅在業主無法自主應對之情形下才透過法令進行規範。



本報告之智慧財產權歸屬於國發會

OECD 於敏捷監督治理之建議當中，亦提示監督的方式可以包括法律制定、正式或非正式命令、次級規則、行政程序以及非政府機構及自律機構所發布之規則等等各種可以達到監督目的的作為。要採用可以實現敏捷與適應法制政策之監管機制，確保監督政策不致對於技術創新造成阻礙。因此選擇有彈性工具或方式很重要，甚至包括不具法拘束力的標準或監理沙盒都是選項。

(3) 彈性法制監理促進科技產業發展：監理沙盒

當新興科技之創新應用對社會或經濟可能產生之影響尚無法預測，也無法確認是否可能對於現行法律適用造成障礙時，若僅一味因懷疑或違法可能性而不允許創新投入，對科技創新可能產生不當之阻礙。已有相當之國家，包括 OECD 案例分析文件提及之英國及本文整理之日本、韓國以及我國等，都有採取程度及規則不等之沙盒或類似沙盒之機制，允許創新科技應用於特定原則下，得以先行投入特定範圍之市場進行運作，透過運作的觀察與分析，確定該技術創新應用模式可能之影響以及法制面之需求。然而沙盒機制運用範圍之廣度，可能影響其效能。日本之制度並未針對特定產業，而是以解決產業法規適用之灰色地帶消除、監理沙盒與新事業特別制度搭配，視個案需求進行運用，可以用以確認法律適用之疑慮，並評估修立法的需要，讓不同之科技應用皆有機會突破現況進入市場。韓國之監理沙盒機制亦是具備相當之彈性，可適用領域與事物類型廣泛，並可透過臨時許可證方式讓特定領域事業可以在並未完全符合所有法令規範情況下，先行於設定之範圍及條件內進行測試，再反饋回法制



本報告之智慧財產權歸屬於國發會

面之配套作為。兩國皆係採取較為擴大之監理沙盒機制作為促進產業創新發展及法制建構平衡之重要手段。

3. 滾動檢視評估機制納入法律規範

面對新興科技發展與應用的不確定性，歐盟近年來多項科技立法，皆於規範當中設置特定期限之評估與檢視條文，包括歐盟 AIA、DGA 及 DA 皆已納入定期檢視及滾動修正之條款。其中 AIA 之規定最為複雜，要求於該法生效後每年需對高風險之附件清單及禁止 AI 作法之清單進行評估，至 2028 年後每 4 年執委會需重新評估現有法規分類。DGA 則要求執委會需於 2025 年 9 月 24 日就法規整體狀況進行評估並提交調查報告。DA 則要求執委會於 2028 年 9 月 12 日向歐洲議會、理事會及歐洲經濟及社會委員會提交對該法之評估報告等。

(二)對國內做法之建議

綜整對於國際主要國家與國際組織之作法，可以發現其基本上對於法制之形成，並未因為數位科技之變化，而降低法制評估與研議之嚴謹度，或因而調整簡化立法的過程。然而，面對新興科技對經濟社會帶來的衝擊，不容忽視。貿然走進完整的立法，未必會是最好的做法，尚須有相關機制的搭配，包括進一步之調查、意見徵集或透過沙盒實驗之方式，實際發覺與評估創新科技應用產生的影響。即使晚近大量立法的歐盟，亦是已進行多年之影響分析，方能陸續提出各項法制草案進行審議。當然，如何啟動對於科技影響之法制政策評估，以使政府得以快速因應，採用敏捷治理之方式解決問題，亦十分重要。

我國長期以來已如同國際先進國家，建構並累積極為完整之法制作業程序，其中亦包括詳盡明確之 RIA 要求與程序，故在法制風險之



本報告之智慧財產權歸屬於國發會

影響評估機制上，已有相當之完備。科學技術研發應用之法制建構速度無法趕上技術發展需要，未必為通常法制作業程序本身之問題，而是需要考量可以強化法規調適議題發現，以及具面對快速變遷得以彈性且敏捷因應問題之作法或機制。對應國際作法以及國內近期法制建構面臨之問題，似可從以下幾個角度切入進行制度面之思考：

1. 強化法規調適議題發現機制，提高政府對新興科技創新法制需求之敏感度，以利早期啟動法制藍圖之規劃

我國實質上具備與主要國家相同之國家科技政策建構機制，惟政策制定之過程往往忽略將法規調適具體納入搭配之政策評估，且即便政策層面曾提及應同時考量需要之法律規範，但並未強化相關技術研發推動與法制間之鏈結，導致技術研發、推動、應用與實際法制研議之走向未必可以相互搭配。故若能於科技政策與計畫規劃之初，即具體納入 RIA 之評估作業，實質進行意見徵詢、調查與分析，提出得以對應科技政策與計畫之法制修定配套藍圖，則可使相關法制需求提早納入考量，有助法制建構與政策、計畫推動進程之搭配。歐盟、韓國及日本近年來之法制修定之速度及相關法制政策與發展戰略之密切連動，即為我國可參考之適例。

歐盟為多國家組織，對於相關政策需要之發現，採取多元政策參與工具之利用，包括對於法律修正草案正式提出前之意見徵集外，並透過設置之公民倡議管道、特定領域專家論壇之設置，以及塑造歐洲未來等相關意見溝通活動，以發掘並探討歐盟所需要之法制政策。上述做法包括前期之需求發現、建議作法，以及法制政策研議中期進一步之意見調查與社會發現等，最終達成共識提出最適切之法制方案。



本報告之智慧財產權歸屬於國發會

而我國近年來推動公共政策網路參與機制，不但法案預告須提上公共政策網路參與平臺徵集各界意見，亦允許公眾得以透過此一機制提案進行法制政策修訂，可以算是歐盟所提出之公民倡議管道，相較過往已更能快速取得民眾對於議題之看法與建議。專家議題討論，亦有透過政院顧問或各部會委辦計畫邀集專家座談或論壇等方式進行，惟相關之操作卻未必對應出具體之法制政策評估或建構。此部分除了涉及政府單位對於民眾意見提案性質之認定外，也涉及不同意見管道是否有統合整理、評估及進一步整合意見提出具體法制政策規劃建議之機制。

於法規調整之推行部分，國內實務運行雖有統一之法規調適平台，但卻未將其制度化，導致現行之法規調整係由各部會自行提出改善鬆綁之項目，實務上未有較為橫向之法規需求檢視。故也有必要考量建構一個制度化且持續運作之科技法制評估機制，搭配科技重點發展，滾動檢視法令條文及相關配套機制是否對科技或產業發展產生過度限制等。

參考澳洲 ALRC 的操作，可以發現 ALRC 作為獨立的法規改革評估單位，係基於獨立於其他主管機關角色之定位對於科學或技術發展有需要進行法律增修之需求進行深入的調查、了解與分析，並提出因應之具體建議，供聯邦法律建構之參酌。因獨立於各主管部會之外，故評估係以澳洲整體法制政策思考，並透過具體諮詢機制，對於各類利害關係人盡可能與以諮詢或測試提案之可行性。我國目前有數位政策法制協調平臺，透過平臺分組方式由特定主持部會主導法制政策之規劃，惟部會僅以所管法規層面思考之模式，則無法勾勒法制需求之關聯藍圖。且亦無相關單位及機制得以切實



本報告之智慧財產權歸屬於國發會

做到實質之利害關係人與公眾意見之深入取得、分析與評估。

因此我國相關意見徵集或法制政策討論機制，所欠缺的是更具體深入之調查、分析與建議。此部分需要有獨立於各部會立場之角色機制進行更制度化的操作。於數位政策法制協調專案會議，可強化此機制之運作，透過行政院與指定部會幕僚進行橫向議題整合，搭配更具體之意見徵集、實務調查及法制政策回應追蹤機制及跨部會法制政策藍圖建構，強化整體面之法制政策需求發現、確定與具體落實。

2. 強化跨部門法制監督合作，確保法制政策鏈結不中斷

因科技所涉領域廣泛，政府各機關依其職權於某些領域重疊，政策方向與法制規範容易發生扞格。根據 OECD 建議「各國政府應強化內部跨部門協調及合作，建立跨部門之合作機制，確保各部門或政府間針對新興科技法制政策應有一致性」。然而相關議題仍須有領頭之主管機關進行較為全盤的討論與規劃，如同日本，指定由數位廳召開數位相關制度改革審查委員會，進行推動各級政府法制政策符合數位原則之事務，而相關機關須予以實質配合，方能收其綜效。此部分實際上亦可透過數位政策法制協調專案會議機制之進行，強化領頭部會對於整體法制政策面向規劃與監督的權限以及其他部會配合的責任。運作模式上設置任務分組，分別針對 AI 法制、資料治理、個人資料保護、數位經濟相關法規等進行跨部會協商，並於灰色地帶之法規適用問題協調主責機關，並透過該會議確保各部會所釋出之法規或指引符合政府政策，推動立法共識，確保行政院整體數位政策之一致性。



本報告之智慧財產權歸屬於國發會

該會議採定期及不定期會議。針對緊急須解決之事項，得召開臨時會議，並協調相關部會協作，及時處理重要議題。

3. 以指引、監理沙盒等釐清法規適用，提高產業創新彈性之作法，提升問題處理之敏捷度

OECD 建議各國應建立可靈活應對技術變化並具前瞻性的監管體系，以確保法制不會對技術創新造成阻礙。採用之法制監管模式未必採取強制性立法，亦可透過提供明確之實施指引或解釋之方式，降低產業創新法律適用之不確定性。另不具法律拘束力之監管工具亦可替代及補充法律，例如透過相關標準之採行，亦可達成監督之目的。例如日本對於 AI 或資料治理法制議題之處理，近年來則主要以指引等軟法之建構以為因應，必要時方進行法律面之部分修訂。我國目前已推行從函釋開始啟動法規鬆綁之政策，可以更具體透過相關指引之訂定，於法制建構尚待評估階段，給予產業創新具體的建議與指導，降低產業嘗試錯誤之成本或因對於法律適用不確定性而趨於保守發展之不利益。

監理沙盒、測試台、創新空間等機制基本上亦為可彈性面對科技創新衝擊之作法，並可協助政府及事業以實際測試之結果，具體發現法制面之限制或需要，有利目標性的達成法令建構、調適或鬆綁之目的。目前國內監理沙盒機制僅限於三種類型，無法滿足科技產業創新發展的需求，可考慮擴大監理沙盒機制運用之範圍及配套法制之建構，給予未來產業創新有更彈性之空間，也給予法令建構一定之實證機會與緩衝期。

4. 針對新興科技立法加強滾動檢討評估之要求，降低法制建構對於科技影響不確定性之疑慮



本報告之智慧財產權歸屬於國發會

如前所述，歐盟近期新興科技相關法制建構，面對 AI 及資料治理等議題之不確定性，皆具體於法律規範當中嵌入就不同風險或執行疑慮滾動檢視之要求，且多具體指出應檢視之時間及重點。此一作法，基本上可以降低在涉及科技議題之法案研議過程中，常會出現對於相關技術影響層面不確定，而導致無法對於管制重點與強度進行有效擇定之問題。我國過往之法制建構雖沒有如此明確之滾動檢討規範，但仍有出現過提醒特定事項得由主管機關視社會經濟強況及實際需要調整之規定（如電子支付機構管理條例第 9 條第 2 項電子支付機構最低實收資本額之規定），足見透過明確於法律規範進行滾動檢視要求，有其可行性。建議可針對涉及新科技議題之立法，規劃具體滾動檢視調整之規範，以降低法律建構方向擇定之疑慮。



本報告之智慧財產權歸屬於國發會

# 項次 3. 前瞻數位科技法制研討會

## 壹、 研討會概說

### 一、 背景說明

因應人工智慧(AI)科技高速發展，國家發展委員會刻正偕同相關部會規劃「AI 新十大建設推動方案」，透過「智慧應用」、「關鍵技術」及「數位基磐」三大面向，擘劃我國 AI 生態系的發展圖像，以展現政府發展 AI 的承諾與決心，並落實賴總統「創新經濟、智慧國家」國政願景，推動臺灣成為 AI 之島。

鑑於 AI 應用場域日漸普及，引發生成式 AI 訓練資料取得合法界限、巨量分散資料授權困境、資料共享互利發展等監理挑戰，如何在促進創新發展的同時，建立適切的法律框架以保障各界權益，將是形塑產業競爭力的重要課題；另觀察部分國家嘗試藉由 AI 監理沙盒機制，提供新創業者測試 AI 商品及技術可行性之實驗場域，並觀察監管需求及挑戰，以消弭科技發展與現行法規落差，值得借鏡。

本次研討會透過產、官、學各界代表的深度對話，期盼匯聚多方意見及取法國際經驗，探索我國促進資料流通應用及營造友善創新法制環境的法規調和路徑，並為臺灣邁向 AI 之島和實現數位主權，提供平衡創新發展與權益保障的具體法制政策建議。

### 二、 研討會規劃

(一)會議總覽

・主題：實現人工智慧之島—營造友善創新法制環境



本報告之智慧財產權歸屬於國發會

・日期：114 年 10 月 29 日（週三）

・時間：09:30 - 16:40 (含報到、茶敘、午餐、綜合討論)

・地點：集思交通部會議中心國際會議廳 3-4 樓 (臺北市中正區杭州南路一段 24 號)

(二)主題與議題規劃

・主題一：AI 監理沙盒機制與創新治理

與談講題：

1. 監理沙盒是法規驗證、修改法規、優化機制、創新實驗場域？國際推動 AI 監理沙盒態樣或相關新技術研發/法規適用沙盒等成功經驗?對臺灣建立 AI 監理沙盒制度的啟示？

2. 目前我國既有監理沙盒（金融與無人載具）創新實驗運作經驗?似無因實驗案件而修正相關法規之原因?針對未來設立 AI 監理沙盒建議？

3. 產業不願進入沙盒或僅止於實驗而無法落地之考量為何?如何增加誘因、配套及簡化行政流程，鼓勵業者參與未來 AI 監理沙盒？

・主題二：生成式 AI 訓練資料的著作權挑戰

講題(一)：生成式 AI 訓練資料之著作利用合法界限與條件

與談議題：

1. 透過現行法令解釋，針對「為訓練 AI 模型於網路爬取



本報告之智慧財產權歸屬於國發會

受著作權法保護資料」行為所劃定之「合理使用」界限為何？對於我國 AI 發展及相關著作權人保障的影響為何？

2. 對於訓練生成式 AI 所面臨之資料授權取得困難，或個別授權管理不易等困境，是否可能在一定前提條件下，透過授權機制，如法定授權等方式加以解決？

3. 對於增訂資料探勘例外或 AI 訓練專屬合理使用規定的看法為何？如規定，其目的是否應限於非營利性？

4. 除上述作法外，國際上是否有發展趨勢或法規調適策略值得我國借鏡？

講題(二)：友善生成式 AI 發展之法制配套初探

與談議題：

1. 倘修法明定資料探勘例外、法定授權或 AI 訓練專屬合理使用規定等，必要採行之配套措施為何（例如：課予利用者透明性義務、賦予權利人退出權）？若法制上尚無法解決時，有何其他配套措施可予採行？

2. 如何建立合理之利益分配制度，以兼顧創作人之私益及公眾接觸人類智慧之公益？

3. 針對為訓練生成式 AI 取用資料所導致之侵害著作權行為，AI 開發者及部署者應負擔的責任為何？是否應就現行實務狀態與資料運用情形之需要等，評估現行民、刑事規範之合理性及有效性，例如評估行為輕重規範不同刑度，或進行民刑責任之搭配或調整等？



本報告之智慧財產權歸屬於國發會

三、 議程

表 1 研討會議程

| 時間 | 議程 | 主持人/講者 |
|---|---|---|
| 9:30-10:00 | 報到 | |
| 10:00-10:10 | 開幕致詞 | 國家發展委員會 |
| 10:10-11:30 | **主題一 AI 監理沙盒機制與創新治理** | 主持人：<br>詹方冠 國發會副主任委員<br>與談人(按姓氏筆畫排序)：<br>王偉霖 文化大學法律系教授<br>施宜君 金管會創新處副處長<br>陳奕廷 景翊科技股份有限公司總經理<br>雷震台 無人載具計畫辦公室主任<br>戴豪君 世新大學法律學系副教授 |
| 11:30-11:50 | 交流討論 Q&A | |
| 11:50~13:00 | 午餐時間 | |
| 13:00-14:20 | **主題二 生成式 AI 訓練資料的著作權挑戰**<br>講題(一)：生成式 AI 訓練資料之著作利用合法界限與條件 | 主持人：<br>王勁力 資策會科技法律研究所所長<br>與談人：<br>尤騰毅 城邦出版社法務副理<br>陳仁偉 實踐大學企業管理學系副教授<br>陳啟桐 律果科技執行長/律師 |



本報告之智慧財產權歸屬於國發會

| | | |
|---|---|---|
| | | 章忠信 東吳大學法律學系兼任助理教授<br>廖怡苓 台灣微軟法務副總經理 |
| 14:20-14:40 | 交流討論 Q&A | |
| 14:40-15:10 | 下午茶敘時間 | |
| 15:10-16:40 | **主題二 生成式 AI 訓練資料的著作權挑戰**<br>講題(二)：友善 AI 發展之法制配套初探 | 主持人：<br>林豐文 國發會法制協調處處長<br>與談人：<br>李佩昌 六合法律事務所主持律師<br>李姿儀 國立臺灣科技大學專利所助理教授<br>徐秋華 公共電視總經理<br>樊晉源 國家實驗研究院科政中心組長<br>賴文智 益思科技法律事務所所長 |
| 16:40-17:00 | 交流討論 Q&A | |
| 17:00 | 會議結束 | |

資料來源：研究單位繪製



本報告之智慧財產權歸屬於國發會

四、 其他行政事宜

執行團隊協助以人工智慧等數位科技法制為主題規劃實體研討會，邀請產官學研等利害關係人參與交流，並協助研討會相關行政作業整理如下：

(一)研討會會議手冊彙編

本次會議手冊由執行團隊彙編，整理各位與談專家之個人履歷及與談資料。

資料來源：本研究自行繪製

圖 2 會議手冊封面



本報告之智慧財產權歸屬於國發會

(二)與談人及主持人聯繫及會前議題溝通會議

此次研討會執行團隊蒐集近年在 AI 創新發展實驗場域或 AI 著作權有相關研究之講者，整理推薦名單提供委託機關確認，並協助聯絡邀請與談人。

確認與談專家後，執行團隊協助安排會前溝通會議，並規劃研討會進行流程表，提供委託機關與專家進行事前溝通。

(三)會議場地及設備事務

本次研討會執行機關租借可容納 150 人之集思交通部國際會議中心(國際會議廳)，協調必要設備提供講者所需之相關配置。並進行會場佈置及流程控管，提供現場活動餐飲。

資料來源：本研究自行繪製

圖 3 現場活動照片

(四)主持人及司儀建議講稿

執行團隊協助研擬部分主持人及司儀講稿，並於會前提



本報告之智慧財產權歸屬於國發會

供委託機關確認。

## 貳、 會議報告

### 一、 開幕致詞－國發會副主任委員詹方冠

AI 的發展可謂下一次工業革命，許多國家包含美國於 2025 年 7 月發布其 AI 行動計畫，以及韓國李在明總統上任後即宣布投資百兆韓元希望於 5 年內成為全球 AI 第三大國，可見很多國家都正致力發展 AI。我國於 AI 硬體有很大的優勢，於全球供應鏈中有不可取代的地位，但 AI 真正應用於社會或生活使人民有感的層面上，仍有待精進的地方。目前國發會與各部會合作推動 AI 新十大建設，主軸是透過 AI 產業發展讓百工百業及人民生活都能導入 AI。為達到此目的，仍有許多準備工作，如矽光子等攸關下一代 AI 發展的晶片、伺服器等技術須掌握，以及智慧機器人技術的發展、AI 基礎建設包含算力、資料、資金、人才等的完備等。

國發會除推動 AI 新十大建設之外，同時擔任行政院數位政策法制協調專案會議的幕僚單位，主要是為解決 AI 於法制上的問題，與相關單位共同推動。AI 興起導入許多法制需要調整，故今天將探討兩個主題:一為在智慧應用方面,於法制環境還沒完全相容的情形下，我國已於金融及無人載具方面透過監理沙盒推動，然現行模式於 AI 時代是否有檢討或借鏡國外經驗；二為訓練資料，眾所周知 AI 的訓練需要資料，故資料議題相當重要，尤以現今 AI 的發展可能 2 至 3 年內資料都會被大型語言模型訓練完畢。而資料的訓練及運用會涉及到著作權法制的議題。希望今天研討會的議題能對各位有所幫助及收穫。



本報告之智慧財產權歸屬於國發會

二、 各場次會議報告

## ■ 主題一：AI 監理沙盒機制與創新治理

**主持人：**

詹方冠 國發會副主任委員

**與談人：**

王偉霖 文化大學法律系教授

施宜君 金融監督管理委員會金融市場發展及創新處副處長

陳奕廷 景翊科技股份有限公司總經理

雷震台 經濟部產業技術司無人載具科技創新實驗計畫辦公室主任

戴豪君 世新大學法律學系專任專技副教授



本報告之智慧財產權歸屬於國發會

(一)主持人開場及提問第 1 題

AI 發展會觸及許多法制環境面的問題，在過去，較為創新的技術，是否可以在尚未修法前，透過監理沙盒的機制，先試營運，藉此觀察法制或環境面要做哪些調整。臺灣已經在監理沙盒機制上有一定經驗，包括金融領域以及無人載具的相關法規。

面對 AI 的發展，無論是監理沙盒的制度，或如何與 AI 發展調和，想請教是否有國際經驗可以參考？

(二)與談人回答第 1 題

1. 戴豪君老師

(1) 監理沙盒機制並非全新概念，過去於各領域如金融、交通、能源或個資都有監理沙盒。近幾年針對 AI，國際上亦開始逐步導入 AI 監理沙盒機制。今年 OECD 關於監理沙盒的報告中，對監理沙盒有完整的定義，並將監理沙盒分為兩種：

A. 創新者驅動

業者碰到問題，主動提出希望法規有所調整。例如日本企業經營特許制度即是由業者主動提出，如針對送貨三輪車豁免駕照要求。

B. 監管者驅動

基於政府監管需要所設，如我國無人載具以及金融科技沙盒。



本報告之智慧財產權歸屬於國發會

(2) 監理沙盒機制的法制趨勢：

A. 英國的監理沙盒機制最早從金融、交通開始，最近針對 AI 涉及個資推動監理沙盒規範。例如在向銀行進行理財諮詢時，會需要評估風險等級，透過與聊天機器人得對話並透過過去推動開放銀行的驗證，確定風險等級。

B. 韓國針對兩種特定行業，即金融及資通訊，有監理沙盒規範，另針對其餘產業訂有整體性的監理沙盒法令（即產業融合促進法），以避免每個產業都需要訂定一套監理沙盒機制。同時，另有政府行政程序上如何配合監理沙盒推動的法律（行政管制基本法），並且有地區型的專業化發展特區法，以及推動智慧城市監理沙盒法案。上述相關法令組成韓國的監理沙盒六法。

C. 德國規範較為務實，先從法令開始，設有實驗性沙盒法條的撰寫指引，說明如何撰寫監理沙盒的法條。今年(2025)推動聯邦層級監理沙盒法案，並設有政府監理沙盒創新網頁。

D. 日本法制架構分為三層次：第一層次為國家戰略特別區域法，針對區域型監理沙盒；第二層次為創新者驅動的企業實證法；最後一層則是生產性向上法是針對特定技術，如區塊鏈、物聯網以及近期之 AI。

(3) 監理沙盒案例，目前全球已有超過 60 個國家推動監理沙盒，其中 59 個國家推動國家層級的 AI 監理沙盒：



本報告之智慧財產權歸屬於國發會

A. 法國，推動針對個資的部分，首先為對個人就業輔導，包含轉職及業務處理等。另外是針對地鐵的監控，透過新影像擷取技術對個人侵擾性較低視覺呈現偵測特定事件，做到 AI 交通監控，確保沒有公共危險事件發生。

B. 西班牙因應歐盟立法，推動 AI 立法。與歐盟 AI 法(AIA)一致，分為高風險、有限風險、低風險以及被禁止 AI。主要是針對高風險部分，有實驗案例，除立法外，成立人工智慧局，於今年成立負責監督 AI 監理沙盒的專家小組。其中一個實驗以香菸自動販賣機為例，導入 AI 生物特徵辨識驗證年齡；以及在機器設備(如飛機)設有 AI 聊天機器人，能詢問操作方向等。

C. 歐盟於 AIA 中定有監理沙盒規定，要求各會員國於 2026 年 8 月前成立國家層級 AI 監理單位。監理沙盒最重要的是責任豁免規定，歐盟規定下，未豁免民事責任損害賠償，但豁免行政責任，各會員國不得對 AI 監理沙盒內的行為有任何行政處罰。另外允許個資之目的外利用，前提是必須是合法蒐集。

(4) 另外於監理沙盒後段設有真實世界測試，歐盟以技術準備度分級(PRL 0-10)，技術較前期的部分不能進入沙盒僅能透過法規諮詢；Level3-7 原型以及測試時建議進入監理沙盒，Level8-10 準備上市時則要求進行真實世界實驗，會請真的試用者進入實驗，因此會需要徵詢試用者的同意。

2. 陳奕廷總經理



本報告之智慧財產權歸屬於國發會

(1) 聚焦 AI 時最重要的是資料，若資料不正確會使 AI 產生幻覺，歐盟已注意到這點，我國透過監理沙盒機制，討論新的驗證計畫。沙盒機制係希望針對先進科技，於落地測試過程中最重要的是需有廠商、場域以及法規豁免，例如 Uber 在進入我國市場時被法規所限制，直至法令修正後才允許多元計程車。

(2) 各國在數位監理沙盒方案中，有對應的主管機關，沙盒機制另外一項重點是公私協力，因此資料相當重要。歐盟為此訂立資料治理法(Data Governance Act)，以此法為框架，下設各項行動方案去執行各項資料交換等法規。歐盟各成員國政府須設有國家級樞紐(national hub)以及資金準備，並且與民間進行協調資料的取用。

(3) 歐盟有 GAIA-X 計畫，有對於基礎設施的定義，以及服務法規框架標準的定義；另外 International Data Spaces Association (IDSA)，則是定義技術框架以及資料交換的各項法規。

(4) 綜整歐盟的公私協力運作機制，公部門定願景、法規以及資金協調；GAIA-X 定行業規範及標準；IDSA 負責技術框架以及實施模型部分；私營部門則是實際建立資料空間等。

(三)主持人提問第 2 題

對於我國沙盒實施，是否有推動上的狀況及經驗分享，尤其在後續法規上是否有做出那些調整？以及對於未來 AI 金融監理沙盒有什麼看法？



本報告之智慧財產權歸屬於國發會

(四)與談人回答第 2 題

1. 施宜君副處長

(1) 金融科技發展與創新實驗條例(下稱實驗條例)於 2018 年公布施行，至今累計申請 17 件，核准 10 件，落地 4 件，可發現比例並不是那麼高。隨後於 2019 年訂定銀行業、保險業及證券期貨業申請業務試辦作業要點，與實驗條例雙軌並行，因試辦比較能於真實世界中小規模運行，至今年 8 月已經有 134 件申請案，其中核准超過 110 件。若將雙軌並行兩者一起看，是有一定的成效。

(2) 在前述 4 件落地之沙盒案，較著重在普惠金融及多元金融服務創新，在法規修訂部分有兩個例子（屬於非金融業者直接申請沙盒案例）：

A. 沙盒成功落地且運行成功：

過去外籍移工的匯款費用太高，導致走向地下金融，因此開放移工匯款的監理沙盒，並於實驗結束後修正「電子支付機構管理條例」及訂定「外籍移工國外小額匯兌業務管理辦法」，目前本會已核准 5 家非電子支付機構辦理外籍移工跨境匯款的公司。

B. 業者正在調整落地商業模式中：

國外債券投資部分，外國債券投資門檻較高，因此有業者申請將其碎片化成為小額投資單位，讓投資者以較少的金額參與國外債券投資。本會亦進行法規調適，已修正發布「證券商設置標準」等相關規定，並開放證券自營商得辦理「自行買賣特定外國債券業務」。



本報告之智慧財產權歸屬於國發會

(3) 對於沙盒的建議，若牽涉到法律或法規命令，修法過程會比較冗長，導致花費較多時間，可能跟不上社會型態的快速變化，建議可以採「軟法」方式，例如金管會於 2024 年發布金融業申請業務試辦作業要點(下稱試辦要點)，整合銀行業、保險業及證券期貨業三業的試辦要點，在試辦要點中只要不涉及法律或法規命令的部分，如行政規則、公會自律規範或周邊單位的規定等尚未開放部分，金融業皆可申請試辦。另業務試辦之法規調適較快、有彈性且時程較好掌握，故建議制度設計上應有分級管理方式。

(4) 沙盒實驗之前的輔導及法規釐清也相當重要。金融科技業者及金融業者若有創新想法，得透過金管會金融市場發展及創新處(下稱創新處)的諮詢輔導會議，或金融科技創新園區的「監理門診」等管道進行諮詢，創新處將與相關業務局共同研議輔導，若議題涉及跨部會權責，將再洽相關部會意見，以降低業者前期摸索、法規釐清的時間及成本。

(5) 建議未來推動 AI 監理沙盒時，產官學研可一同合作，若沙盒實驗牽涉跨部會議題，可考慮是否由主責單位設單一窗口，必要時由窗口洽其他相關部會意見，讓業者於實驗創意發想時無需重複與不同單位說明。

2. 雷震台主任

(1) 無人載具涵蓋自駕車、無人機以及無人船的類型，包含未來可能的新型載具。這些載具在上路實驗時可能會與法規有所牴觸，因此需要沙盒實驗機制讓實驗順利進行。



本報告之智慧財產權歸屬於國發會

(2) 無人載具係我國第一個以科技產業的沙盒實驗，並參考金融沙盒實驗的經驗。整個實驗分為兩階段：前端計畫審查是由經濟部透過跨部會合作機制，邀集中央各部會、地方政府以及產學研的專家共同審視。計畫核可後，上路實驗牌照的發放會由交通部依據無人載具科技創新實驗計畫牌照核發辦法執行。

(3) 計畫執行以不超過 1 年為限，得展延最多 4 年。若計畫過程中有碰到需要法規調適的部分，會於展延期進行調整。基本上計畫會以最多 4 年為限。

(4) 實驗審視主要有兩個重點，即創新具備以及實驗安全。計畫中除審視創新性、可行性，亦會針對實驗過程中的風險評估、因應方式、安全措施(如安全保護設施或保險等)，能夠透過相對機制涵蓋實驗中的不可預期狀況並做出補償。

(5) 計畫自 108 年 10 月至今 6 年間，有 24 件上路實驗，包括 18 件自駕車，以及自駕船及無人機各 3 件。自駕車涵蓋類型包括物流、都會運輸以及園區觀光接駁；船的部分以觀光接駁為主；無人機則有物流運送相關實驗。

(6) 目前延續案例為台積電臺南廠區的接駁，包括員工以及供應商於廠區內的活動，以自駕車於廠區進行。目前階段實驗非常順利，已累積近 15,000 趟次的接駁實驗、載客超過 87,000 人次。未來實驗範圍將持續擴大，從現有廠區到跨廠區，以及從廠區到員工宿舍，長期部分要推動自廠區至南科火車站之長距離的接駁。



本報告之智慧財產權歸屬於國發會

(7) 法規調修部分，交通部將自駕公車做為推動目標，透過沙盒實驗讓交通部瞭解自駕技術於國內運行中能掌握到的對應情境以及運用的場合進行法規調修。然而實驗雖有 6 年，但對自駕產業而言仍屬於初期，因此於法規修訂前先訂定「自駕公車安全指引」，涵蓋運行安全、聯網、運行服務的指標規劃，並於後續沙盒實驗運用。待運行情境更為成熟後，將該指引轉換為法規，供廠商做為依循。

(8) 就自駕車實驗而言，涵蓋各產業及部會，包含交通部、內政部、數發部等不同部會。故目前實驗過程中，就跨部會的整合是以計畫媒合。建議未來 AI 沙盒機制設計時，若涉及相關部會，需要有充裕前置時間，將計畫目標、分工及執行方式讓各部會對沙盒實驗相關資訊有完整瞭解，在資訊同步的狀態下進行溝通洽談。

(9) 在計畫審查部分，會將審查重點先與業者溝通，使計畫完整性較高時再送審查，時效上會較有效率。不論是跨部會或業者，先前的溝通都相當必要。

3. 戴豪君老師

(1) 我國未來若要推動監理沙盒需要思考的面向，首先，我國目前係以行業別做為規範，但 AI 新十大建設會需要各產業都使用 AI，若未來不同產業都有沙盒需求，是否會有分散式立法的問題。另外，是否需要針對特定技術或地區型的 AI 產業實驗，如日本愛知縣的無人車運行區域，以及美國的 Waymo 也是在特定的區域試驗，故我國是否也應考慮建立區域式的 AI 監理沙盒法制設計，否則未來將可能面臨分裂式監理沙盒挑戰。舉例而言，我國將成立個資會，現在 AI 的發展最重要即為資料管理，那未來針對



本報告之智慧財產權歸屬於國發會

AI 發展是否可能出現個人資料監理沙盒？一個沙盒既要面對行業管制、又要符合個資法的規定，建議體例上可設計如韓國制度，即建立一套普遍適用各行業的監理沙盒法規。

(2) 在無人載具科技創新實驗條例以及金融科技發展與創新實驗條例中，皆要求應遵循個資法，故無法排除個資法之適用；於 AI 應用上，欲提供個人化服務，會需要一定的個資，但於此二法律中，對 AI 而言相當重要的個資實驗卻是禁止的。歐盟有超過一半以上的會員國以個資主管機關為 AI 監管機關，可見 AI 與個資的關係相當緊密，歐盟的 AIA 亦有排除個資保護的相關規定。

(3) 我國於進入沙盒後，除非有政府補助案，政府並未提供其他資源。歐盟則提供算力資源，軟體、資料及單一實驗基礎等 6 至 7 種 AI 工具，支援 AI 監理沙盒。我國目前仍是以法規監管角度思考，尚未思考進入沙盒後須提供產業支援。監理沙盒有一重要目的是扶植中小企業，但目前我國幾乎沒有中小企業進入監理沙盒。他國為扶植中小企業有規定，對於中小企業進入監理沙盒，政府得給予簡化之審查，或給予優惠費用；我國亦應有中小企業的監理沙盒，並且對於相關政府人員，應有一定培訓。

(4) 另外，可導入如歐盟的技術成熟度標準，將技術分等級，不需要一開始即進入沙盒，初步想法可先透過諮詢，較完整的技術可做上市前驗證，屬於兩者中間階段的再以沙盒進行。

(5) 監理沙盒法規為政府設計予企業使用，但政府本身若想進行監理沙盒，則未有任何豁免規範。公務機關若需要創



本報告之智慧財產權歸屬於國發會

新服務，會比較猶豫進入沙盒，因此可考慮是否政府單位自身設有公共服務的監理沙盒，可借鏡歐盟國家於公共服務設有監理沙盒的經驗。

(五)主持人提問第 3 題

我國推動各式監理或計畫都較以單點的實驗，但要推動整個產業的發展，還是必須從點、線到面全面的發展才有更進一步幫助。而監理沙盒在我國推行的件數上偏少，故想請教各位專家，在沙盒推動上，為何我國業者會不願意進入沙盒或難以落地？

(六)與談人回答第 3 題

1. 王偉霖老師

(1) 我國金融監理沙盒相關規定很早建置，以落地率而言有超過百分之二十，並不算差。可以再思考的部分，例如因申請需為主管機關核准的特許金融業務，因此非金融業者申請沙盒須與金融業者合作；沙盒內容多與傳統金融業有關，如加密貨幣等新興領域相對來說較少。金管會為主管機關，沙盒為金融相關內容無可厚非，但以國家推動 AI 產業的角度而言，若各部會皆分散式立法，會產生戴老師所提及的問題，且對業者的成本相當高，以推動 AI 角度而言應不太合適。

(2) 金管會訂定的金融業申請業務試辦作業要點，俗稱「輕量沙盒」，係鼓勵法規尚未開放但尚未違法的創新做法。建議沙盒應進行分級，需要排除法規適用以及需要灰色地帶解釋空間的狀況，可有不同的處理。在未來推動 AI 監



本報告之智慧財產權歸屬於國發會

理沙盒的過程中或許可參考金管會的輕量監理沙盒，達到比較好的結果。

(3) 目前 AI 監理沙盒較大的問題為資料，而資料中最重要的為個人資料。以個人資料而言，目前相關的兩個沙盒都沒有辦法排除個資法的適用，需思考未來將如何解決此問題；另外 AI 發展中尚有著作權侵權的問題。若我國目前的法制不處理個資及著作權相關問題，於 AI 推動上將會面臨限制以及挑戰。

(4) 日本著作權法第 30 條之 4 將 AI 模型訓練視為合理使用，此非透過沙盒機制，而是直接規定於著作權法中，從而排除著作權法侵權風險。歐盟於 AIA 第 59 條得暫時放寬 GDPR 法規要求，允許特定目的外利用，但於沙盒中仍對個資利用仍有明確要求。或許可參考 AIA 第 59 條規定，適度開放個資的豁免、同時確保於沙盒內個資運用仍有完整規範。

(5) 期待有國家層級 AI 監理沙盒，避免分散式立法，並降低立法及業者成本。另外，在著作權侵權及個資法部分是否能整合意見，推動建立豁免機制，以幫助 AI 的發展。

2. 陳奕廷總經理

(1) 法規未規範之灰色地帶部分，業者都會想辦法突破並找到應對方式，並開始推行。例如泳池溺水偵測，透過人員姿態而非臉部監控，以迴避 GDPR 規定；前段時間關於 Lawsnote 用爬蟲造成侵權的案件，在美國也有類似案例，但判無罪的原因是被告購買書本再掃描及轉換格式等處理才放入資料庫，因此類似狀況未必皆構成侵害著作權。



本報告之智慧財產權歸屬於國發會

(2) 沙盒實驗一定有效果，但不是百分之百會成功。無人機於無人載具沙盒實驗中數目少，係因為軍用商規無人機，軍方提供 150 億資金，讓廠商做實驗後可購買，因此大公司皆轉至預算較高的軍方實驗。金融方面，新創公司若能與評價好的大廠整合，不須監理沙盒即可執行。

(3) AI 應用遠超於現在能想像，但我們仍使用較基本的角度想像。對廠商而言若符合未來趨勢，灰色地帶會盡量去突破並執行想法。

(4) 美國未運用監理沙盒，而係訂定通行規範，包括強制保險、裝載多少人等。歐盟則是訂定通用型規範，並搭配民間聯盟，為政府與民間聯盟組織及企業串連合作。日本於 2012 年已開始推動亞洲區域的 international data space hub。日本 data space 由大企業主導，因 AI 所需資料龐大，需要企業間整合，於信任框架中交換資料。

(5) 希望我國能訂定通用型法規，並針對公務人員有豁免規範，以降低其提供資料而伴隨的行政風險，另明確主責單位並由其協助跨部會進行協調亦是推動上需要考慮的部分。

3. 雷震台主任

(1) 沙盒，實驗一定會有不可預期的結果，沙盒既然是實驗，應關注造成結果的原因。若達標，要確切知道成功的原因為何；若未達標，則更要釐清未達成原因（目標設定過高？場域條件未預期？），以提升後續沙盒實驗品質。

(2) 沙盒實驗最初設計是為讓業者可以合法上路實驗，以自駕車為例，上路需要車輛、系統、安全設施等，於實驗初



本報告之智慧財產權歸屬於國發會

期成本高、不確定性等，並無配套措施減輕業者負擔；後續才加入實證運行補助機制，針對實驗營運服務為前提提供補助。

(3) 未來 AI 實驗會有各種不同類型，如何收斂實驗能達到預期想法，或自實驗資料或心得及後續因應方式，都是寶貴的資訊。建議 AI 沙盒規劃對中小企業或新創可提供小額補助，若欲以新創及中小企業為主力，則應給予誘因，如透過分級補助，提供資源使其於沙盒實驗更有動力。

(七)交流討論

金管會進行金融沙盒 2.0，在法令通過需要較為冗長的情況下，目前金管會是否有能快速推動的想法？

1. 施宜君副處長

(1) 有關研議優化金融科技發展與創新實驗條例之方向，目前仍屬金管會內部討論階段。例如 AI 訓練與個資相關，因個資於金融部分牽涉到財產，須更為謹慎。目前金管會已發布函釋，若是銀行間為防範金融詐騙或犯罪，其個資利用為增進公共利益所必要，可不受個資法特定目的利用的框架限制，並於適當防範及去識別化下小規模執行。

(2) 公私協力部分，金管會與金融總會於今年 2 月 19 日成立金融科技產業聯盟，由大型金融機構帶領，分成技術應用、法規、跨業整合、投資四個小組，較具體的成果為防詐及阻詐部分。過去銀行間為保護個資難以追蹤金流，因此透過金融機構去識別化資料的交換，於聯盟內研究技



本報告之智慧財產權歸屬於國發會

術，並與數發部合作，利用 AI 及早識別警示帳戶及金流履歷，來保護民眾財產安全。

(3) 在國際上，個資利用的放寬亦是從公益部分著手，因此突破的方向可評估以小規模試行。

(4) 支持新創企業的部分，除於實驗前提供諮詢輔導，金融科技創新園區也提供分級輔導機制；針對實驗後落地的法規調適問題，金管會研議未來規劃設計於實驗進行中申請人即可向相關主管機關提出修法建議，以利主管機關提早評估實驗落地的法規調適方向。

2. 王偉霖老師

我認為在法規層面上要因應 AI 發展，著作權法及個資法的鬆綁仍為關鍵因素。著作權法部分或許可透過主管機關解釋或提供指引等方式，讓業者比較放心。雖無法完全拘束法院，但我國法院通常尊重主管機關解釋，若主管機關的解釋夠明確，對業者於執行上較為容易。但個資部分較有難度，其為法律層面的管制，較難透過解釋或函釋，且目前我國兩個沙盒機制皆未排除個資法的適用，故後續仍需透過修法處理相關問題。

3. 陳奕廷總經理

我國若要發展主權 AI 需要很多資料，面臨很大的問題為著作權，全世界皆有類似問題。日本發展主權 AI 面臨此問題時，因考量法規需花費較長時間，採用架構性方式，透過科技方式(NCP 架構)，替代法律尚無法解決的問題。

4. 戴豪君老師



本報告之智慧財產權歸屬於國發會

個資部分，臉書於歐盟提出兩種選項，1.臉書服務免費，但使用者的個資須供臉書蒐集投放廣告；2.付費訂閱，但不蒐集個資投放廣告。歐盟於今年 5 月依據數位市場法，認定臉書違反守門人義務，未取得當事人真正同意，且並未提供等效替代方案，以當事人係被迫同意而裁罰臉書。同年 8 月，愛爾蘭同意臉書使用 GDPR 第 6 條(f)的正當利益，得不需取得同意蒐集個資，德國因此以緊急機制暫停愛爾蘭的同意。臉書被裁罰後仍以不同方法取得個資，可見個資對 AI 而言相當重要，但若難以透過行政規則排除適用，如何於嚴格管制下有所突破為接下來需解決的問題。



本報告之智慧財產權歸屬於國發會

## ■ 主題二：生成式 AI 訓練資料的著作權挑戰-講題一：生成式 AI 訓練資料之著作利用合法界限與條件

**主持人：**

王勁力 資策會科技法律研究所所長

**與談人：**

尤騰毅 城邦媒體出版集團法務副理

陳仁偉 實踐大學企業管理學系副教授

陳啟桐 律果科技股份有限公司執行長/律師/專利師

章忠信 東吳大學法學院兼任助理教授

廖怡苓 台灣微軟股份有限公司法務副總經理/律師



本報告之智慧財產權歸屬於國發會

(一)主持人開場及提問第 1 題

AI 訓練涉及的著作權問題，主要源自龐大的資料需求，每一筆受著作權保護的資料單獨取得授權，在現實操作上幾乎是不可能的任務。目前國際上已有例如日本修正著作權法，讓訓練資料的取得有「合理使用」的空間，但我國現行的著作權法並未針對「AI 訓練」這種新興的利用模式有明確的規範。雖然 AI 訓練是一種「學習」，並非為了重複再現既有內容，學理上可稱為具有「高度轉化性」，但當 AI 系統將網路上的文章、圖片下載並儲存於伺服器中來進行模型訓練時，在法律上可能被認定為「重製」他人著作。若 AI 輕易將網路上的文字圖片下載並儲存於伺服器中進行模型訓練，在我國著作權法下，可能會被認為是重製他人著作的行為。雖 AI 系統開發者得以主張其行為符合我國著作權法第 65 條之合理使用，但 AI 訓練幾乎是商業、完整且海量利用他人著作的情形，是否符合著作權法第 65 條第 2 項判斷標準，如利用之目的及性質、著作之性質、所利用之質量及其在整個著作所占之比例、利用結果對著作潛在市場與現在價值之影響等，是否能讓這些大量取用資料的 AI 訓練者、開發商真正主張合理使用，其實有很大的疑問。

第一個問題想請教與談專家：透過現行法律的解釋，針對為訓練 AI 模型在網路爬取受著作權保護的資料的行爲，如果將之劃定爲合理使用，其界限在哪裏？對於我國 AI 的發展及相關著作權人之保障會有哪些影響？

(二)與談人回答第 1 題



本報告之智慧財產權歸屬於國發會

1. 陳啟桐律師

(1) 我國著作權法合理使用的因素，立法時沒有設想 AI 之訓練，所以沒有預測到 AI 發展的情況。如主持人所述，傳統的著作權法合理使用判斷標準，包括利用的目的及性質。雖然 AI 的目的不是去享受、欣賞作品，而是去轉化作品，但它的性質卻又是商業化的使用居多。以使用目的及性質來談，商業上使用就比較難主張合理使用。

(2) AI 訓練階段與 AI 應用階段的著作權議題不一樣，應區分討論。AI 訓練所需之著作是海量的，如去年 Pre-train 計畫，訓練資料量有 5000 億中文字之多，很可能著作權人所有資料都已被 AI 爬取進行訓練；以訓練階段所利用著作的質與量而言，很難主張合理使用。

(3) 「利用結果對著作潛在市場與現在價值之影響」部分，我認為應持中立立場，視個案而定。有時候 AI 不是要重現原著作，但是會不會對原著作的經濟價值有影響，就需要個案判斷。整體而言，我認爲在多數的個案情況下，應該是很難去主張合理使用。

2. 陳仁偉老師

(1) 著作權法基本上允許合理使用，限制的是商業運用。在 AI 模型訓練，如果依照著作權法的精神，屬於重製行爲。而重製行爲從著作權法第 44 條到第 65 條，依我個人從資訊運作的角度解讀，並沒有太大的限制。在歐盟法制下，允許資料探勘(data mining)，但提供拒絕選擇，允許 AI 的建模處理。日本，如同主持人所述，是更開放的運作。



本報告之智慧財產權歸屬於國發會

(2) Opt-in/Opt-out 在歐盟與美國意見不同。歐盟認為是 opt-in，即搜尋資料必須經過權利人的同意；美國認爲是 opt-out，即若權利人拒絕則不可搜尋其資料。歐盟於 AI 時代，轉向選擇 opt-out 之模式，趨勢上對 AI 時代用資料建模態度已有改變。

(3) 在搜尋時代，會連結到著作權人個人網頁，可以此獲得利益。但在 AI 時代，AI 綜合出多個著作權人的著作才提供答案，所以原著作權人完全被忽略，除了稀少性或有特徵性之著作資料外，多可透過技術模糊化去除掉資料，無法追溯到資料有被引用，法律難以全面保護。

(4) AI 可以產生很多資料，但是 AI 不是自然人，其產生之資料沒有著作權，若以 AI 產生之資料進行建模，就不會有著作權議題。未來 AI 產生的著作量會大於人類著作，在著作權議題上需要再思考。例如 AI 可以模擬「大師風格」寫出幾可亂真之作品，若不揭露為 AI 生成會以為出自該大師之手。更進一步，即便沒有用到原文，也可以寫出一樣風格的內容，但著作權法目前並沒有把「風格」當作受保護客體；就算把文本改寫再拿去建模，也難以辨識。

(三)主持人提問第 2 題

AI 訓練需要海量資料的情況下，就算能夠逐一取得授權，如何有效追蹤、管理數十億筆不同來源、不同授權條款的資料，也幾乎是不容易完成的任務。這個問題不是 AI 時代才出現，例如傳統廣播電台播放音樂、有線電視重播節目，要電台或電視台向每一位詞曲創作者、歌手或製片人取得個



本報告之智慧財產權歸屬於國發會

別授權，無論在管理或成本上都是不切實際的。因此，法律出現「法定授權」的機制，讓著作使用者在符合法律規定（例如支付一定費用或滿足特定條件）後，即可合法利用他人的著作，而無需逐一取得授權。

接下來請教各位與談專家：對於訓練生成式 AI 所面臨的資料授權議題，或者是個別授權管理不易。有沒有可能在一定的前提條件之下，比如以透過法定授權機制，解決這些困境？

(四)與談人回答第 2 題

1. 章忠信老師

(1) AI 的訓練涉及大量且完整地利用很多作品，那這樣的行為會是「合理使用」嗎？我認為絕對不是合理使用。許多人認為 AI 的訓練可被視為「資料探勘（data mining）」，而資料探勘在歐盟屬於合理使用；但歐洲議會今年 7 月的報告特別指出，把 AI 訓練比照資料探勘，是錯誤的法律連結（legal mismatch）。

(2) 何謂資料探勘？舉例而言，我們稱對岸為「匪區」後改稱「大陸」、「中國大陸」，現稱「中國」；把大量文獻全文丟進 AI 做探勘，開始知道用詞在什麼時候改變，這種統計趨勢分析才是資料探勘。資料探勘最終成果並沒有用到內容本身，而只是找出某種趨勢而已；相較之下，AI 訓練結果是產生足以與原內容相競爭之成果，不是資料探勘、亦不是合理使用，必須要取得同意或授權。



本報告之智慧財產權歸屬於國發會

(3) 任何人有問題，應該請教專家，而不是隨便去問路人。在AI 訓練取得授權方面，應以期刊、專書、論文為內容，而不是網路資料隨便抓。既然資料庫的建立都可以取得授權，那 AI 的訓練要取得授權，應該也不是那麼困難。AI 訓練者甚至還可考慮與資料庫業者合作，因為資料庫業者已將資料處理完畢，品質與授權問題都能被控制。

(4) 著作利用的基本原則，需要先取得授權再作利用，並非可以未經授權就加以利用後，再由著作權人要求退出；歐盟的資料探勘，若是非營利、學術性質，著作權人是無法退出的，只有營利的性質，著作權人可以要求退出。問題是AI 訓練的資料利用，看起來根本就不是資料探勘，應先取得授權才能利用。

(5) 實務上，資料庫業者取得授權，都是找粽子頭角色的期刊、雜誌或出版社，只要向它們取得授權，下面的每一個粽子，也就是每個作者們，就全部搞定了，不可能一一與每一個作者們洽商授權。生成式 AI 若要能生成優質成果，應該找老師的作品而非路人的作品。不過，生成式 AI 的訓練，在利用著作方面，一旦利用了，就不可能刪除或遺忘，如同學生上大學後將高中課本丟掉，並不會喪失其高中程度，因為已經學習過了。因此，著作權人將來在授權時需要思考，並非是要討論授權多久，而是每年都需要分錢給著作權人，因為讀過著作權人著作後，即便拿掉著作，模型也已記住著作內容知識、已得到如同著作的程度，且不會喪失。討論授權時，需思考這些問題。

2. 陳仁偉老師



本報告之智慧財產權歸屬於國發會

(1) 「法定授權」舉證實務非常困難。關於 opt-in 或 opt-out 的問題，即便權利人拒絕被使用，若是模擬出相似風格，再以模擬出的風格進行建模，在訓練時執法相對困難。以爬蟲為例，若下載完不超過一天內刪除，隔天再重新爬取或搬到別的機器，就幾乎找不到「我保留了你的資料」之證據。法令要解決現行狀況，重點應該是利益分配，有沒有機構可以作合理分配？

(2) AI 時代的資料是跨國資料，跨國資料的授權更困難，不同法域、不同來源，要如何取得授權、計價收費？即便彼此都願意授權與付費，處理授權應由哪個機構負責，也是問題。

(3) 另外，若爬取的資料屬營業秘密，大部分公司沒有那麼嚴謹資料保護。舉例而言，律師訴狀風格其實是訴訟策略，AI 是可以寫出訴狀(風格)幫你生成這些文書。雖然大型雲端或平台（如微軟）承諾不會用你的資料來訓練，但建模「風格」仍可能在雲端過程中被學習，進而影響到著作權人的權益。

(4) 著作權法除了保障著作權外，亦要促進社會公共利益。有能力的 AI 建模者，需要授權，也不會留下違法跡證。資安產業有關資料取得與利用，有詳細分工，包含資料的蒐集、整理、處理，甚至已形成市場。看似無用的資料，對資料市場而言都是很重要的，例如步伐資料，手機裡看似瑣碎的資訊，都可能很有價值，這部份很難用法律規範。google 現在的資料相當豐富，是很好的建模工具，再加上資通安全已是高度分工的產業，現在再進行規範，對 AI 業者似是沒有影響。



本報告之智慧財產權歸屬於國發會

(5) 保護著作權人及社會權益的法律觀點，我建議回到商業機制。鼓勵與促進可信任的 AI，因為 AI 資料偽造太多，應區隔何為可信資料，建立授權來源可信任的 AI。接著鼓勵業者公示資料來源，鼓勵大型資料庫業者，讓資料產生業者願意加入，以取得授權。一旦使用資料就進行分潤，或建立超微支付系統，例如一次 0.001 元的 Token，若集合全球用量，也是很可觀的收益。回到金流商業機制，並立法協助商業機制，才能真正保護創作者權益。

(6) 回歸到商業機制，就是歐盟的 opt-in/opt-out，即預設授權，除非當事人拒絕；因為即使不預設授權，AI 公司也拿得到。各位每天都在授權，舉例來說：手機的使用、上傳 PDF 解密、轉檔，仔細看網頁條款其實都包含授權；論文傳上 AI 修改，也已經授權。蘋果手機條款中，用戶資料，除其個資以外，廠商皆有權使用，現下已很難阻擋。建議從鼓勵的角度，國家可以透過回饋機制，讓大家願意主動授權，並且可以拿到微利，累積起來也是很龐大的。可由 AI 公司或搜尋引擎的公司說明運用比例分配，讓多方利益衡平。

(7) 因為建模後即不需原始資料，吸收到模型裡後，可以組裝改寫而難以辨別，無法證明是源自於著作權人的資料；因此建議透過商業化機制，預設授權、分潤等方式，由國家鼓勵扶持大型資料庫業者，以利我國發展主權 AI，並有大型與臺灣有關的語料庫、圖片庫可以出售。

(五)主持人提問第 3 題



本報告之智慧財產權歸屬於國發會

由於「利用之質量與比例」、「對著作市場的影響」這些都須個案判斷，而且 AI 訓練有大規模、無差異複製整個著作的特性，在合理使用的解釋上先天就不利開發者。相較於歐盟已通過《數位單一市場著作權指令》(Directive on Copyright in the Digital Single Market)，明確為「資料探勘」設立例外條款；日本修改著作權法，讓為資料分析而重製的行為合法化。我國《著作權法》並未明確將「資料探勘」(Text and Data Mining, TDM）或 AI 訓練行為納入「合理使用」的範疇。如果我國後續推動修法，可能需要參酌這些立法例的經驗，在放寬 AI 訓練須事先取得授權的同時，避免對創作者造成「不當損害」或「市場替代」。故想請教各位與談人：對於資料探勘的例外或 AI 訓練專屬合理使用規定的這種看法。如果要規定的話，這個規定的目的是不是應該限於所謂的非營利性？

(六)與談人回答第 3 題

1. 廖怡苓副總

(1) 這個議題目前在全球都有非常多的討論。我從產業的角度，特別是生成式 AI 業者的角度，與大家分享一些觀察。首先是著作權的兩個重要概念及精神，著作權保護的是表達（expression），而不保護概念、想法及趨勢。第二，著作權法保護著作權人的利益，同時也重視知識的散布。我們保護著作權人，是希望鼓勵創作，讓更多作品產出，使社會能累積更多知識與利益，讓社會更蓬勃。因此，當我們討論 AI 時，也要重新思考這兩件事帶來的意義。



本報告之智慧財產權歸屬於國發會

(2) 討論該議題前，需先釐清生成式 AI 模型訓練過程中，讀取的是數值，而不是文字或內容。用以訓練生成式 AI 的模型，是先進複雜的演算法模型，是將資料做成 token，將文字、字詞、內容分段，進入神經網路學習內容彼此間的模式，學習資料間的關聯，並非讀取文字。學習到模型後，就可以進行預測，模型建好、交給使用者使用時，依照使用者輸入的內容，可預測後輸出結果。與傳統認知的重製不一樣，AI 輸出的東西稱為數值向量，模型做的是數學，而非文字的重製。

(3) 其次要釐清，當建模後被使用者拿去使用，例如當你輸入提式詞後跑出的結果，過程中不需要再讀取訓練的資料；在過程中所使用的模型，是就已學習的趨勢及知識，予以產出內容。因此，這個議題不應該當作著作權上表達的保護，而是想法、概念，可以思考這是否受著作權保護。

(4) AI 是下一個十年的新興科技，需要注意如何讓 AI 散布知識，讓更多人取得知識並利用這項工具。須確保模型建模過程中，是負責任的 AI，美國稱為可信任的 AI。為了讓 AI 產生的結果是無偏頗且正確的，有必要大量讀取資料，這個過程不適合只讀取部分資料，亦即不太適合以營利/非營利作為區分。

(5) 因此，對於著作權人的權利保護，現行有一自願性的產業標準(robots.txt)，若著作權人不希望著作被利用，鼓勵著作權人可透過相關系統，保護自己的著作物，業界也有類似工具，微軟的搜尋引擎(Bing)亦有發布此類工具，保障著作權人的權利。微軟對個別使用者產出的生成式 AI 內容，針對付費企業及客戶，其承諾若有著作權人覺得權利



本報告之智慧財產權歸屬於國發會

受到侵害並對微軟企業客戶主張，微軟會以自己的費用為企業客戶辯護並依終局法院判決負責。

(6) 法定授權及強制授權的部分，可行性有限。為了負責任的AI，會需要讀取大量資料，若要找到對的著作權人進行授權，即便是強制性授權，實務上有點不切實際。例如在音樂產業中，一首歌的作詞、作曲、編曲、錄音都有不同權利人，要整合授權相當困難。即使建立強制授權機制，實務上最終著作權人得到的分潤也有限。因此，我們建議主管機關思考整個立法目的，包含著作權原本要保護的目標、著作權的精神，原來要散布知識以及如何與著作權人達到平衡的角度，在著作權法做出例外的規定，讓建模合法化。這也是另一個可以幫助國家發展的方法，可以協助所有 AI 產業及供應鏈，進而嘉惠使用者。

(7) 最後分享一個案例，從微軟發布的使用者案例中，AI 可以用在很多好的地方，其高度算力讓許多醫療產業及科學研究有高度的進步。以冰島為例，他們政府利用 ChatGPT 保存冰島語言文化的資產。現在於全球的討論已經不再是 AI 如何使用，而是朝更進階的高風險 AI 應如何進行管理。其發展每年倍速成長，因此，當我們討論 AI 尤其是修法時，應該都要納入思考。

2. 尤騰毅副理

(1) 從媒體出版的實務上來看，我們在 2022 年、2023 年與外國出版社簽訂授權契約時，發現契約中出現「不要將本書內容提供予他人進行 AI 訓練」的條款，此時大概是 AI 開始流行的始點，當時僅有部分大型出版社有相關規定，但到 2025 年，幾乎大部分的外國出版社都有這樣的規定。



本報告之智慧財產權歸屬於國發會

看得出來內容業者對 AI 訓練有所防備，但規定在合約內是較為被動的。近期在美國有包含美術著作、圖形著作或音樂著作等內容業者對 AI 公司提出訴訟的相關新聞，初步統計到現在應有超過 30 件。這是屬於內容業者較主動，對 AI 訓練模型進行防禦。

(2) 目前臺灣尚未有相關爭訟。但今年智財局的電子郵件函釋中，主管機關對 AI 訓練過程如資料蒐集、欲處理及優化等行為，可能涉及「重製行為」。此為基於著作權法框架下的解釋。若 AI 模型訓練可能涉及重製，會需要取得權利人授權。

(3) 若是討論 AI 模型資料爬蟲屬於合理使用，現階段會需要修法，因為現行著作權法條文難以突破。若修法，對著作權產業會造成衝擊。以語文著作而言，假設開放 AI 訓練為合理使用，會造成替代效果，內容業者的成果會直接被收割，長期將造成惡性循環，也會降低創作者創作的動力。

(4) 亞洲其他國家近幾年 AI 相關著作權訴訟，以鄰近國家韓國及日本為例，韓國於 2025 年初，新聞網站對入口網站提起訴訟；日本在同年 8、9 月，日本讀賣、日經等老牌新聞媒體對美國 AI 業者提起訴訟，主張 AI 業者爬梳其資料且免費提供予 AI 用戶使用，且可能涉及 AI 越過付費牆蒐集新聞資料提供給 AI 訂閱者。

(5) 目前，內容產業對 AI 的模型訓練及合理使用，不論是要透過解釋或修法，我個人持保留態度，應該要循一般商業契約取得授權比較好。案例上，可看到美國 Open AI 與美國、德國、法國加拿大的出版集團或新聞集團取得授



本報告之智慧財產權歸屬於國發會

權。我國正在發展主權 AI，需要大量文本，可考慮例外的情況下透過法律授權；考量修法時程，亦可尋求直接與內容業者對話取得授權，對發展主權 AI 的效果會比較好。

3. 陳啟桐律師

(1) 今年 7 月我協助處理一件中央社控告臺大博士生的案件，簡單說明案情：中央社發現臺灣有一個公開資料庫，透過臉書(FB)連結即可看到約 14 萬筆中央社新聞的全文。對中央社而言，14 萬筆是很大的數量，這涉及重製，以一個 Dataset（資料集），可以看到新聞全文，不像一般 AI 訓練只看到成品。以著作權法觀點，這樣大筆的資料難以主張是合理使用。臺大博士生主張，整個資料庫不是他自己爬的，而是國外大型爬蟲計畫 Common Crawl 所蒐集；其中資料量以 TB 計算，他只是基於研究目的，自其中擷取繁體中文，形成次資料集，中央社內容只占約 0.3%，比例極低；而且來源是公開開源資料，也採開源釋出，為何會構成侵權？

(2) 案例可見，AI 訓練需要極大量資料，以研究者的角度，幾乎不可能完全不侵權，若要求完全不侵權，往往會綁手綁腳。身為法律科技業者，理解法律有強烈的在地特性，以著作權法為例，同樣事實，在臺灣可能有民、刑事責任；在歐洲可能是民事責任；在美國可能不構成責任。因此在中文 AI 訓練上，我們需要大量繁體語料做訓練，包含合約、法學期刊論文等，但這些資料都有著作權，難以合法取用，因此也就無法訓練出有差別、領域性的模型。



本報告之智慧財產權歸屬於國發會

(3) 能夠訓練的公開資料，最大筆的是臺灣的法規資料庫以及司法院的法學判決。若要使用這些資料會需要花大量時間爬蟲，雖不致有違法疑慮，但也不能爬他人已整理好的資料庫，否則可能會侵害他人編輯著作。

(4) AI 的訓練還是可以再區分。如果是資料集，訓練後是否可散布公開？訓練完後，若不會取代或重現原來的著作，我認為有合理使用的空間。但於現行法下並不能直接適用，仍然需要修法，或可參考如日本著作權法第 30 條之 4 以及歐洲資料探勘的例外作為修法方向。

(5) 若將 AI 訓練限制於非營利，對臺灣的 AI 發展是很大的限制。所有發展很好的 AI 都是有營利行為的，因此，合理使用若要修法，不能限於非營利；但修法上可以透過配套去限制相關利用，例如：

A. 不得重現原著作，如不得公開完整訓練資料集。

B. 不得取代著作權人的經濟利益，若侵害須提供補償，如授權機制，可參考專利領域的標準必要專利(SEP)，其所搭配的是公平、合理、非歧視(Fair, Reasonable, and Non-Discriminatory，FRAND)的授權承諾，著作權也可參考該授權機制。

C. 我國著作權刑事責任需要檢討，近期有案件以爬蟲行為被判觸犯刑法第 359 條無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄罪。未來修法，也應有配套排除刑責，如透過權利金授權等，避免 AI 研究人員因為刑責疑慮，進而使我國在地繁體中文 AI 發展受限。

(七)主持人提問第 4 題

當我們在運用資料進行建模與訓練時，應該採用什麼樣的授權機制？是否有資料探勘等例外可以適用？現行著作權法的規範下，是否能妥善定位合理使用？這些問題目前仍有相當多的爭議與討論，也是我們今天邀請各位專家提供專業意見的初衷。

剛才每位專家都分享到技術面的脈絡；我們也都知道，當前 AI 的技術進展，主要來自業界長期投入大量資源一步一步推進。如果 AI 的建模與訓練、語言模型的運作並不會直接與原始著作品產生競爭，它不是要取代我們對作品的欣賞或利用，如同廖副總所提，這整個過程本質上是數學向量化等程序。

回到法制面，我們最關心的是：AI 訓練本身既然不直接產生與原始著作競爭的產品，是否有什麼突破性的權利或義務設計，可以讓臺灣的 AI 產業能參與國際主流競爭，但又合理分配利益予資料提供者。就美國 Anthropic 公司與作家間的巨額和解案，似乎顯示市場有朝向「回歸授權」模式發展的趨勢。故除上述作法外，國際上是否有發展趨勢或法規調適策略值得我國借鏡？

(八)與談人回答第 4 題

1. 廖怡苓副總

(1) 微軟認為 AI 的建模行為本身不屬於著作權法上「表達」的範圍。不過，我們也非常理解著作權人對自身權益的擔憂。為了更明確釐清這樣的爭議，微軟目前在全球對各國



本報告之智慧財產權歸屬於國發會

主管機關的建議，是希望在修法上能夠有所努力與調整。就我們觀察到的國際修法趨勢，有幾項值得借鏡：

A. 日本與新加坡都已經將文字與資料探勘例外納入著作權法，這是滿好的立法作法。

B. 美國透過現有合理使用條款，認可 AI 建模屬於合理使用。

(2) 身為 AI 業者，我也要再次強調，雖然我們認為 AI 建模並非著作權客體，但所有人，包含我們自身，都應尊重、遵守著作權法並尊重著作權人的心血。

(3) 舉例來說，微軟在澳洲曾經參與媒體議價相關討論，我們是支持的。不只是媒體議價，我們尊重每個著作權人的權利，如果有權利侵害，對於大型企業客戶，如先前所提，我們會站在客戶後面，並且若有著作權人主張，我們也會負責。

(4) 我們的觀點是，AI 建模是推動第四次工業革命的重要基礎。它不僅能協助產業升級，就個人而言，如想出國留學的學生，AI 技術能讓他更快速、更有效率地取得相關知識與資料，幫助知識的散布；另外在經過轉化後，AI 的應用亦能促進各行各業的發展，進而帶動國家的整體成長。這些都是修法上需要思考的角度。

2. 章忠信老師

(1) AI 會這麼聰明，一定是有讀過他人的作品，如果沒有重製或閱覽既有的作品，AI 不可能透過演算法演算出這麼



本報告之智慧財產權歸屬於國發會

棒的成果。生成式 AI 生成的結果未必會重製或改作既有的作品，但是訓練過程當中，一定有利用到既有作品，即使技術上可能最後沒有在系統中重製既有著作，而僅是從中擷取某些素材，轉成演算依據所需要之參數，但仍有著作之利用。生成式 AI 的研發者並非公益慈善團體，不能以爲了促進國家文化發展及知識的散布為由，主張可以免費利用他人的作品。

(2) 著作權法並非保護著作權，而是在做創作者與利用人之間的適當利益分配。當 AI 的研發者利用他人的作品獲得很多收益，是否應與創作者進行利益分配？至於如何分配，則為技術上問題，可能透過立法，或透過合意授權。既然資料庫業主可以與大型出版社、媒體集團、雜誌期刊取得授權，不必跟每一個作者取得授權，即可使用優質的內容，後續再進行利益分配，則 AI 的研發者要取得授權，應該也不會有太大困難。我認為這樣的做法才能讓 AI 的成果是優質的。

(3) 另外要思考一個問題，人買書、看書，可以解決重製權的問題。這些書的內容記在腦海裡，跟權利人無關。但 AI 這麼聰明，資料內容被 AI 記住，那麼人類閱讀與 AI 閱讀在法律制度的價值上相不相等？又例如，研究所畢業賺錢領了薪水，不需要跟作者進行利益分配，但 AI 學習後收錢回答問題，應不應該與創作者進行利益分配？

(4) 每一個國家對於 AI 發展是有各自的策略及政策。對美國來說，他們的 OpenAI 到世界各地去征戰，美國人無法反而在國內跟他要求應取得授權，所以會認為利用著作訓練 AI 是合理使用。歐盟則有很清楚的利益分配概念，認



本報告之智慧財產權歸屬於國發會

為應該要儘量方便讓作品受到利用，並獲得利益合理分配，但歐盟的議會已經在檢討這件事。所以長遠而言，應該要建立一個公平合理的利益分配制度，創作者要獲得利益，利用者可以方便的利用，這應該才是著作權法最主要的核心。著作權法第 1 條規定，保護著作權人，調和社會公共利益，促進國家文化發展。基本上第一個(保護著作權人)不會爲了保護後面這兩個(保護著作權人、調和社會公共利益)而不見。

(九)交流討論

1. 陳仁偉老師

(1) 提出兩個情境供大家思考：

A. 人看了幾本書寫了書評，人類會有著作權；但若 AI 看了同樣的書(技術上是將其轉成文字關係的向量)，並且寫了書評，是轉譯、改寫，那麼 AI 的公司是否有著作權？因已轉成數學向量，且產出內容不可能與原書一模一樣。

B. 若將書本拍照上傳到網路上、雲端硬碟，雲端硬碟業者有權整理該資料，並將照片解析轉成向量。例如學校有電子書授權，使用者將電子書傳給 AI 要求做摘要，這些過程都會涉及重製。若一本書每個人拍不同部分上傳，並且都已被轉成向量，公司是否有著作權？



本報告之智慧財產權歸屬於國發會

(2) 科技會在法律之前，法律制定出來時，技術通常已經過去。資訊時代的所有權，假設我擁有翠玉白菜並以高解析度拍照，即便我將翠玉白菜賣掉，仍然擁有該照片的著作權。



本報告之智慧財產權歸屬於國發會

## ■ 主題二：生成式 AI 訓練資料的著作權挑戰-講題二：友善 AI 發展之法制配套初探

**主持人：**

林豐文 國發會法制協調處處長

**與談人：**

李佩昌 六合法律事務所主持律師

李姿儀 國立臺灣科技大學專利所助理教授

徐秋華 公共電視總經理

樊晉源 財團法人國家實驗研究院-科技政策研究與資訊中心政策研究組組長

賴文智 益思科技法律事務所所長



本報告之智慧財產權歸屬於國發會

(一)主持人開場及提問第 1 題

有關友善 AI 發展配套的法制初探，我國的「人工智慧基本法」草案已於行政院審查通過，後續將送到立法院審查，其中該草案第 1 條即指出立法目的係為促進以人為本之 AI 研發與應用，保障國民人格尊嚴及權利，提升國民生活福祉、維護國家主權、安全及文化價值，增進永續發展及國家競爭力。為因應 AI 發展，法制為重要的議題。

關於生成式 AI 訓練著作權問題，不僅為法律的挑戰，也是產業發展的關鍵，著作權的法律界線可能影響到 AI 業者合法取得資料的意願，阻礙了技術的研發，但若未提供足夠的保障，又可能損害到創作者的權益而打擊到創作的動力，故此議題為雙向平衡的挑戰，需要找到一個解決方案。想詢問在場專家學者的第一個問題：倘修法採取資料探勘例外、法定授權或 AI 訓練專屬合理使用規定等，必要採行之配套措施為何？若法制上尚無法解決時，有何其他配套措施可以採行？

(二)與談人回答第 1 題

1. 樊晉源組長

(1) TAIDE 為首個政府推動可信任生成式 AI 的相關計畫，而國研院科政中心扮演資料蒐集的角色。2022 年 OpenAI ChatGPT 問世時，推動 TAIDE 遇到許多困難，今天並不是要跟大家講解決問題的方式，而是把我們經歷過的問題和大家分享，也嘗試是否可以從這幾年的研究經驗找到平衡的作法。



本報告之智慧財產權歸屬於國發會

(2) 首先，資料授權取得不易，在 2022 年尚未有資料法規時候，TAIDE 團隊是逐家談資料授權；資料持有者多數質疑若生成式 AI 所取得的都是有價資料，未來是否會被 AI 所超越或取代，因此最後達成的授權數量不多，且多限於單方面授權，也就是授權 TAIDE 的資料只能用於模型訓練。以模型訓練的角度，研究者會希望模型能上到開放的平臺，讓更多人下載其研究成果；但以資料持有人的角度而言，則希望能夠保護資料。因此，為從中取得平衡，當時科政中心針對每個單位，撰擬不同的說帖，或以購買的方式取得資料，並且向各單位說明清楚。

(3) 第二點，就資料抓取部分，OpenAI 可以自網路抓取資料，為何 TAIDE 不行？因為 TAIDE 是以國科會名義製作的模型，故須受到法規嚴格的拘束以及外界的檢視，故即便是公開資料(CCS)，我們還是會詢問是否可以使用。資料授權是提供大家閱讀使用，但模型能否使用，又是另外一回事，當時遇到的問題是資料訓練的型態與授權方式的細節不清楚。

(4) 即使取得資料，但授權時間不同，資料衍生應用也受到限制，例如期刊願意授權，但期刊論文作者是否願意授權仍為問題，資料持有者與權利人概念混雜不清。大型語言模型需要高品質資料，這些公開資料並非如文章或圖形等敘述不易使用。教模型像教小孩子，必須要說明非常清楚，才能訓練；若只有片段，模型容易會臆測，或若只有數值等公開資料的數據、統計資料，雖可抓取，但對模型訓練



本報告之智慧財產權歸屬於國發會

並無意義。因此，在資料授權的範圍中，是否可以不包括授權他人使用，或重新授權，為當時遇到的困境。

(5) 三年前上述問題較為嚴峻，以近年的趨勢發展來看，我國第一部的「人工智慧基本法」草案已在立法院，加上國際上討論聲量很多，後續受到的限制可能會逐漸變少。

(6) 建議由 AI 訓練者的角度出發，若未來著作權法能夠修法納入資料探勘的例外，或 AI 訓練專屬的使用規定，我們樂見其成。AI 模型的著作權有分階段，因為 AI 生成的資料會註明參見某資料，真正應該取得授權的是網頁或是資料的部分；基礎模型只是在訓練模型瞭解資料特性，需要資料探勘之例外規定或 AI 訓練專屬合理使用規範。基礎模型如同教導小孩理解是非與人事物，更進一步的功能，如結合最新的新聞等其他資料進行分析時，則會需要與各個資料庫合作及搭配，因此有營利的商業模式時，應須取得授權；而非於資料探勘時，即要求處理授權問題，未來法令上須有明確要件及界線以利判斷。

(7) 資料的使用是否有超出合理使用範圍，在基礎模型上最新的新聞，一定要加上資料庫來源時，應向該資料庫取得授權；若只是詢問模型為人或貓或狗，或是理解音樂樂理，此為不同層級的問題，應進行清楚切分。若單純僅為資料探勘，建議視為對基礎模型訓練的一部分。

(8) 上個月歐盟專利智慧財產權研討會，因應 AI 訓練資料非常龐大，歐盟建立權利人事後退出的機制，讓著作權人事先保留某些權利，避免著作被用於 AI 訓練的作法，可供參考。歐盟 AI 通用實踐準則，建議在爬取網路資料時得以識別並遵守權利保留。此機制雖在研究層面上認為技術

可以執行，但實際上操作相當困難，因為模型難以完全遺忘訓練後的資料。

(9) 最後建議考量在不同著作領域中利害關係人合理利益的分配，期待標準亦應不同。依據具體用途著作權人及著作權使用者雙方進行協商，並且協商地位平等及授權效率，或可考慮第三方集體管理團體，代表著作方與使用者方所屬單位或機構進行協商。

2. 李姿儀老師

(1) 我最近對於 AI 訓練資料的著作權議題，提出一個資料探勘例外的著作權修法提案，希望能和大家分享想法，以找到文化永續發展及技術發展並進的衡平方式。

(2) AI 的發展非常迅速，生成式 AI 正在重新定義創作，一方面降低創作門檻但一方面也大量未經許可使用既有作品作訓練。對我國的挑戰嚴峻，因全球大型語言模型，73%來自美國與中國，95%是以英語為主，中文數量較少而其中繁體中文又更少。在 AI 時代下，台灣創作者內容有可能出現被邊緣化的危機。繁體中文的文化與表達方式，恐難以得到代表與再現。故希望能透過適當法制創新，重新定位創作者的角色，並讓技術得以並進。

(3) 現行著作權法的困境第一是創作者的資訊不對稱，創作者不知作品何時被訓練，訴訟時又會碰到舉證的問題。第二是談判不對稱，有些較有倫理觀念的開發者可能會想與創作者取得授權，但個別創作者與中小型技術開發者間談判能力不對稱。更不用說大型語言模型，其基本上不會與個別的創作者進行談判，而是與大型的內容創作者談判。最



本報告之智慧財產權歸屬於國發會

後是，即使創作者發現作品被使用，但舉證困難，事後救濟成本高。另一方面，對開發者而言則是法制上的不確定性，雖著作權法有合理使用，但須個案認定。現行著作權法制最大的危機，為內容雙重集中化的問題：大型開發者與大型內容的控制者有談判的能力，但中小型或個別的創作者因為缺乏談判能力，因此會造成文化內容集中化、同質化。對於人類創新及文化多樣性不是太樂觀的發展。為避免雙重集中化情形，故「負責任的 AI」是現今我們需要的應發展方向，不僅為倫理要求，亦為永續的必要條件。透過機制設計提升社會接受度，讓機制更透明化，讓雙邊都有一個協調的機制處理，以提升 AI 的發展及創作間的信任程度，並符合國際趨勢，超越技術開發與創作者間的零和的思維。

(4) 技術的開發訓練與後續的生成階段分開。資料探勘於不同國家有不同程度的例外機制，各國都希望能發展新興的技術。我們有後發者優勢，可在其他國家的經驗之上，進一步改良出適合我國的法制設計。資料探勘的技術，指透過數學統計方法，發現文字或圖像間的向量關係。大型語言模型會產生幻覺，因其為分析字元與字元間的關係，而非理解文字本身的內容，此與人類理解作品、聆聽音樂與閱讀是不一樣的意義。資料探勘雖涉及著作權法上的重製的可能性高，但不同於人類的欣賞作品；而是藉由統計與數學運算，統計語言結構，向量或像素間的關係，與傳統著作權上的盜版或抄襲，有本質上的差異。

(5) 在上述前提下，我提出著作權法資料探勘的例外條款的修法提案，希望能搭配創作者保護機制，透過公共利益考量，



本報告之智慧財產權歸屬於國發會

彌補現行著作權法上合理使用及授權高度不效率的情形，並能平衡創作與創新間的機制，促進國際競爭。

(6) 以「資料探勘例外免責」為核心，相關機制設計上有幾個重要支柱做搭配：

A. 支柱一為透明性，資料探勘若要免責，AI 技術開發者需賦予透明性的義務，功能在於可以提供資料來源的溯源，讓創作者得以得知作品是否有被利用，並作為後續合理補償機制的基礎。知道作品如何被使用，才有後續補償可言。機制尚可配合國際上鼓勵開源 AI 的作法，透過政策鼓勵，或針對 AI 業者不同規模，設計透明機制程度高低作搭配。

B. 支柱二為合理報酬及退出機制，針對商業性與營利性的使用，規劃相關機制，以表現對於人類創作勞動的尊重；並提供創作者退出的選擇，事後退出與事前保留提供創作者的主體性與控制權。

C. 第三支柱為於生成階段作搭配，前述訓練的階段應用資料探勘的機制，後面生成階段可透過機制上提供著作權合理的過濾機制，如各位在使用 CHAT GPT 已無法 AI 生成迪士尼受著作權保護之圖樣，因為現行技術已可以做到合理的過濾機制。雖然這部分但可能會有言論自由辯證空間，但現在僅先討論生成式 AI 著作權議題做討論。作為資料探勘例外的重要要件之一，係「於生成階段賦予 AI 服務及系統提供者合理過濾機制的義務」，否則無法享有豁免的例外。而此機制義務的侵權的責任會落到使用者身上，亦即若 AI 的使用者，想辦法繞過過濾機制，騙過 AI 做出侵權



本報告之智慧財產權歸屬於國發會

內容，使用者須負直接侵權責任；而 AI 系統或服務提供者則課以間接侵權責任。

(7) 整體而言，分成輸入與輸出階段，從文化多樣性與 AI 技術發展並進的角度，形成正向循環資料經濟機制。著作權法適當的修改，可以引導負責任 AI 的發展，需要技術開發者及提供資料的創作者共同使 AI 朝向更負責任的方向進行。

3. 李佩昌律師

(1) 正體中文的資料被邊緣化，也是我們最近在思考的問題。AI 的運用已為趨勢，無法阻擋，像近年來律師事務所諮詢的人，許多都先問過 AI，再來找我們。可能是因為英文合約的開放資料較多，近期 AI 產出的英文合約進步幅度驚人，已可生成許多較高品質的英文合約；而 AI 產出的正體中文合約，雖然最近也有開始進步，大概差不多有 3 年律師經驗的成果，但相較於英文版本合約，仍有較大的進步空間。基於 AI 的能力驚人，趨勢上不可能阻擋 AI 的發展和應用，對於業者取用正體中文資料來訓練 AI，也應該建立透明可信賴的機制，使正體中文領域的資料權利人的權利能被合理照顧，權利人的接受度也就提高。

(2) 贊成透明性義務及賦予退出權。但如果法制上無法做到明訂資料探勘例外，提出幾個層次的建議供思考：第一，是否將資料探勘除罪化。但前提為維護資料安全與個資去識別化。



本報告之智慧財產權歸屬於國發會

(3) 第二,在利用人已履行透明性義務並提存合理報酬之前提下，把利用人的 AI 訓練利用行為除罪化。我國著作權法的侵權人有刑事責任，但歐美多僅為民事責任。

(4) 第三,在利用人已履行透明性義務,並且提存或對集管團體支付合理報酬的情形下， AI 訓練行為不負著作權法第 88 條第 2 項與第 3 項之損害賠償責任,而回歸民法第 216 條請求損害賠償進行處理。

(5) 呼應資料分層級，重點是 AI 產出所引用的資料是否符合合理使用；若已經超過合理範圍，是否利用人從 AI 利用創作產出端進行技術上控管或限制，或者，從 AI 創作產出端揭露及已提存合理報酬之情形下，把 AI 訓練行為除罪化，回歸民法第 216 條請求損害賠償。技術上沒問題，重點為是否要進行過濾。

(6) 產業公協會可自訂自律規範或行為準則,如建立爬蟲遵循規範、標記等，亦可經營集中作品平臺提供一站式授權集費率計算服務，並可提供調解機制，處理退出、補償與下架申訴處理服務。

(三)主持人提問第 2-1 題

AI 的利用不僅能夠提升效率及精準分配資源,還能促進公共服務的普及，例如透過智慧輔助系統提供醫療診斷、教育輔導、或在災害預警和環境檢測中都可提高公共服務的效能。而公視作為一個以服務公共利益為宗旨的電視媒體，在公共領域扮演舉足輕重的角色，想問一下公視徐總經理對於 AI 在公共服務扮演的角色有哪些經驗得以分享？



本報告之智慧財產權歸屬於國發會

(四)與談人回答第 2-1 題

1. 徐秋華總經理

(1) 法律對於文創者為重要的基礎,尤其做節目與著作權脫離不了關係。AI 開始發展後，很多影視從業人員產生一些憂慮，如 AI 其實已經可以開始寫劇本，其劇本也是從過去很多人的創作中做轉化，做為基礎，大家擔心 AI 是否擷取過去成功的劇本，創作者的權利為何。AI 也可以生成人物，對演員而言，會擔心未來是否還有工作機會。

(2) 如何創作 AI 友善環境，以及 AI 能為我們做些什麼，就公共廣電立場,希望能運用 AI 擴大公共服務的能力。2023 年公視率先公布 AI 使用準則,不論新聞、節目或是動畫，如有使用 AI，須予以揭露，自行建立倫理標準。2024 年公視與工研院合作研發 AI 虛擬手語氣象主播，因手語人才庫不足,不可能臺灣每一個新聞臺都有人力,若虛擬主播能扮演這個角色，未來對聽障人士是很大的福音。

(3) 因為正體字的資料不足，我們於 2025 年 9 月 1 日啟動與中央社、中央廣播電臺、原民臺、華視、客家電視臺合作的計畫，結合所有資料庫，建立新聞的 AI CHAT BOT，希望未來若要搜尋臺灣的新聞,能提供一個可信度的正體資料庫。計畫有三個目的，一為提升可信資訊的傳播力，二為加速公共媒體的數位轉型，以及三發揮 AI 科技的正面潛能並創造科技應用的示範效應。在授權方面，我們已取得正當性。

(4) 各臺的新聞資料須進行數位儲存與數位轉化,這是加速數位轉型相當重要的一步。公視與中研院古老師合作，未來



本報告之智慧財產權歸屬於國發會

開放全民使用，並能提供正確且有說服力的內容，降低 AI 的幻覺率。希望能與國際語言模型團隊建立合作管道，發揮中文世界的影響力。

(5) 在 AI 手語部分，公視是更早開發的。於國家語言發展法中，手語也是語言之一，因公視已有 27 年手語新聞經驗，是公視最棒的資料庫。最開始是與日本的 NEP 合作，因其於 2025 年聽障奧運有手語的虛擬主播服務，故進行技術合作；後續與工研院合作，AI 手語更為細緻。預計今年 12 月在公視主頻道可以看到虛擬氣象主播，虛擬氣象主播已讀進所有氣象相關語彙，只要輸入一些字，即可轉換為手語主播的呈現。

(6) 工研院做過 AI 影像辨識技術，在科學上或影像上，讓新聞能即時，經由 AI 即時的翻譯。未來順利上線，期望可達到每節新聞都有 AI 手語即時翻譯的服務。

(7) 另外公共服務的應用服務整合天氣速報，現在為文字或廣播的聲音，對視障或聽障可以用 AI 的方式，提供即時公共服務。在英國與法國的公共場所，都有提供公共訊息的手語服務。

(8) 公視現階段成果，已收錄三千多筆的氣象單詞，以及每日新聞與中央氣象署的錄影，虛擬主播的樣子亦已選出。並邀請 200 名聾人參與調整，並於今年 11 月東京達福林匹克(聽障奧林匹克)運動會提供選手的應援服務。

(9) 預期成果為建立臺灣手語資料庫，擴大手語服務，並培育聽障影視人才與製各類節目。同時整合手語翻譯、骨架生成集影像生成模組系統，打造 AI 手語虛擬主播。



本報告之智慧財產權歸屬於國發會

(10)公視提供的每一項服務，最後都會與法律相關。包含手語服務的資料庫建立，都是有來源、創作者等，涉及著作權的議題，於開發過程中以公共服務為出發點，但若未來有其他用途，在著作權議題上亦須非常小心。

(五)主持人提問第 2-2 題

謝謝徐總經理的分享，讓我們瞭解 AI 可以為大眾帶來的具體公益，但要最大化 AI 可以帶來的公益，卻不能忽略權利人私益的保障。AI 可能有很大的公共利益，但如何使用它，早期著作權為合理使用，但範圍為爭議的問題。有些專家提到資料探勘，似乎有點像行政法上的徵用或徵收，因有使用需求進行資料提供，但給予利潤的分配作為補償，這些都涉及憲法第 15 條對人民財產權的保障，即如何合理的限制及合理的補償。勞動基準法第 9 條之 1 有競業禁止的規定，其中一個重要的條件為合理的補償。若需要使用他人著作權內容，如何給予合理的報酬，以兼顧公益與私益？

(六)與談人回答第 2-2 題

1. 賴文智律師

(1) 如果 AI 像人一樣讀書學習知識、自我成長，會不會有問題？我認為著作權一直走在追求動態平衡的路上。依據著作權法第 1 條「為保障著作人著作權益，調和社會公共利益，促進國家文化發展，特制定本法」，故著作權法係人類依據社會發展所設計，並非完全為保障著作權人而存在的法律，著作權法制是為追求不同利益的平衡。



本報告之智慧財產權歸屬於國發會

(2) 新的技術需要大量的資料訓練，且需為多元、完整、高品質的資料。在著作權層面，一種是認為若未經過權利人授權即是違法；另一種是將其列為對著作財產權的限制(合理使用)。傳統著作權法的設計，要不就是權利人的權利，要不就是要求權利人容忍利用的行為。可想像為光譜的兩端，但光譜不一定有絕對的兩端，一定會有中間的部分。當遇到著作權權利的限制與權利人權利的範圍不是很清楚時，正常商業機制是先取得授權，避免侵權。

(3) 著作權制度的選擇，不只是 AI 訓練，還有後續的利用。現行設計若不是著作權人的權利，則為對著作財產權的限制。AI 生成對後續的利用，可能為著作權的侵權，或為對著作財產權的限制。歐盟著作權指令中資料探勘(TDM)的規定，其制訂背景為資料庫的年代，資料庫服務必然跟隨資料，因此資料探勘為資料庫服務提供前之必然前置行為，但探勘有一定成果對外提供服務時，需與資料的權利人談授權。故該規定是於中間階段給予例外，因最後階段仍需要取得授權。

(4) 但生成式 AI 不一樣，不需要原始的訓練資料，單靠模型即可提供服務。因此歐盟某些主張認為 TDM 的規定不適用於 AI 領域。若要修著作權法，不見得要完全照歐盟的規定，因其解釋不同，目的也不同，要先選擇方向。著作權制度有很多中間性規定，例如過往針對影印機、印表機、錄音機等，設有著作權「補償金」機制，亦可能用強制授權或集管團體延伸的「集體授權」機制，因此制度要考慮實踐可能性。其實沒有好壞，制度選擇後要承擔後果。



本報告之智慧財產權歸屬於國發會

(5) 不論選擇何種機制，「降低交易成本」是重要的概念，選擇著作財產權的限制，不一定能降低交易成本。著作財產權限制的風險，是著作權運用幾乎難以說清楚，若直接照歐盟 TDM 規定，難以解決現在 AI 訓練到後續提供服務的所有免責。若選擇權利集中授權，可能很多人不提供著作至平臺。若選擇傳統管理機制，沒有一定的商業規模，是很難發展的。著作權的補償金機制，交完錢仍要有人分配。選擇一個將交易成本降至最低的機制，所謂交易成本，亦包含違法的成本。

(七)主持人提問第 3 題

日本、韓國著作權主管機關，於 AI 指引皆有提示、引導要求 AI 開發者揭露其訓練資料的來源、使用的資料類型，以及相關的著作權處理方式，增加產業透明度。同時，透過技術手段，阻止侵權內容的生成，並在 AI 生成內容中嵌入浮水印或識別碼，方便追溯內容的來源。

AI 發展固然帶來很多便利及幫助，但也有很多不法之徒利用 AI 詐欺、洗錢等犯罪行為，或其他侵害法律之行為。在法律的制度上，應如何設計較為恰當，例如訓練生成式 AI 取用資料所導致的侵害著作權行為，AI 開發者及部署者應負擔的責任為何？生成工具希望有商業價值，能讓大家使用。但若用於犯罪途徑，或因利用而造成他人權益的損害，此時責任的分配與法律應做怎樣不同的規範？在民刑事責任上須如何調整？



本報告之智慧財產權歸屬於國發會

(八)與談人回答第 3 題

1. 李佩昌律師

(1) 著作權法第 1 條規定的重點在於動態平衡，固然著作權人的著作權益很重要，但也講究平衡調和公共利益，最終目標是促進國家文化發展。依據目前的 AI 條款，輸入進 AI 的內容常被視為授權 AI 使用，一時的方便對產業的衝擊很大，但是大家覺得好用就會用，很難阻擋。 AI 已經是大眾獲取知識最快速的來源之一，網路時代已經擋不住這種速食性的成果享用，擋不住公眾使用 AI 生圖生文。當圖文創作人自身都在運用 AI，AI 生圖生文的資料來源又是廣泛的大眾，法律的限制或禁止是否有用？

(2) AI 的部署者與開發者主要承擔的責任，可能是部署及開發 AI 時違反著作權法的責任。在開發或部署 AI 時，包含資料探勘，若涉及權利管理電子資訊移除或變更，就已經觸法了。例如圖庫業者的圖被其他媒體利用，但浮水印還在，若刻意移除可能會有權利管理電子資訊移除或變更的問題，會有刑事與民事責任。

(3) 關於資料探勘，還可能涉及對於著作權法規定防盜拷措施（科技保護措施）的破解、破壞或規避。接觸著作資料者，若未經合法授權或不符合理使用，都不得規避防盜拷措施，此為民事責任，開發者與部署者會遇到此問題；另外，若涉及不法重製行為，則有民、刑事責任。上述為目前著作權法，開發者及部署者可能涉及的侵權責任。

(4) 不一定需要移植歐盟的規定，但仍需考慮著作權法除罪化，使用 AI 時，有沒有換位置換腦袋？以律師的立場，



本報告之智慧財產權歸屬於國發會

會平衡多方，尋求和解。因為 AI 議題的討論，從權利人立場會反對資料開放供 AI 訓練及利用，但權利人同時也會是利用人，也使用 AI 來作為創作的助力，所以，應在權利人與利用人之間尋找平衡點。另一方面，AI 開發者也應展現相應的誠意，如是否建立產業的自律機制、相關宣導是否足夠等。

(5) 刑事責任部分，若利用人已履行透明性義務，並提存或對集管團體支付合理報酬的情況下，宜將 AI 訓練行為除罪化，民事責任部分則應回歸民法第 216 條請求損害賠償。另外在利用人從 AI 創作產出端予以技術上控管或限制，或從 AI 創作產出端予以揭露及已提存合理報酬的情形下，也可回歸民法第 216 條請求損害賠償規定。

2. 賴文智律師

(1) 有關責任，生成式 AI 需要基礎模型訓練，需要的資料不是大量，而是巨量；即使全臺灣資料都拿去訓練，也訓練不出好的基礎模型，更何況未予訓練。AI 訓練需要多元的資料，例如 AI 依據讀到的英文文獻，可能將中文描述的「原住民」族，生成出印地安人的圖像；或如 AI 從曾經讀過的資料裡看過蝙蝠俠的描述，即使沒有看過蝙蝠俠的照片，也能生成類似的畫面。亦即，有時我們的作品未被利用，反而造成更嚴重的情況。我國狀況有點類似，即希望市面大型語言模型訓練繁體中文的資料，OpenAI 也未必想花 Token 訓練。

(2) 但若欲鼓勵臺灣的業者拿臺灣的資料進行訓練，就不得不需要解決權利保護的問題。目前問題是，不太可能期待一個一個的授權，權利碎片化到非常細；於資料庫年代，因



本報告之智慧財產權歸屬於國發會

大部分的資料庫為特定的領域服務，資料量有限，較能個別談取授權；但現在 AI 的資料量已經達到巨量，難以達到個別談取授權的期待。

(3) 至於制度如何修改，應思考「期待開發者做到什麼事情」。倘期待都不使用著作權人的資料作訓練、期待資料訓練需揭露或補償、或是期待後設地禁止生成特定 IP、或需要有模組禁止 AI 服務生成與原始資料相同或近似度為多少比例的內容等，要引導開發者達到社會各界的期待，可透過減輕責任的方式，引導開發者採取措施。有點像過去談 ISP 責任限制時，先談論部署者可先採取什麼措施始得免責。可以朝這個方向設計。應先有對 AI 開發者、部署者、應用者各別要做到的事情達成共識，再透過制度設計如免責機制等，引導其往該方向進行。

(4) 刑事制度應優先於民事制度作檢討，於我國是有必要的。凡事都走向刑事，對開發者不見得公平，為了一、兩個著作未經授權，即涉及刑事責任，可能有點過頭了，尤其是涉及巨量資料利用的情形。AI 普及應用後，若允許 AI 開發者抓取他人資料作訓練，會不會影響創作？但是原本沒有著作權法時，大家還是創作，雖然 AI 訓練確實會影響，但是此為價值取捨的問題。

(5) 即使反對 AI，沒有使用 AI 不代表未享受 AI 的利益，例如 AI 的技術讓醫療技術更精進無形中間接受益。整體人類的發展，皆享受科技帶來的好處，科技有好處也有壞處。沒有一定反對或贊成 AI，共識凝聚不容易，但與其談是否應授權，不如談如要鼓勵 AI 的開發者，在臺灣希望他們能做什麼，以此角度思考，較易引導出合理的法制規範。



本報告之智慧財產權歸屬於國發會

若 AI 發展對人類利益是好的，由免責的角度思考，從而產生解決的方法，並非一定要從授權或著作權限制二選一。

3. 李姿儀老師

(1) 針對侵權責任，在我提出的修法提案架構下，同意刑事責任應免除，同時呼應前面兩位律師，修法提案希望透過免責做為誘因，去要求 AI 開發者負責任的開發技術。負擔透明性揭露義務，該義務不見得要對公眾開放，但可透過如專責機構等中介服務，對權利人為定期通知，以為合理補償的基礎。這些合理補償可限制於商用資料探勘之目的。

(2) 為保護著作權人創作自主權，事前保留與事後退出機制，應該要存在。雖仍有實務上爭議，但一旦要求，相信技術開發者可以做到，這是免責對於開發者的誘因。免責於使用者端提供負責任使用的條件，當開發者盡到著作權合理使用的過濾機制，那麼侵權責任會落在使用者。因此，民事責任在技術開發者，應盡到前述相關義務及著作權合理過濾機制提供後，若使用者仍然繞過著作權的內容，而生成明知會侵害他人著作的內容，應該要負著作權法中的民事責任。若權利人仍認為免除刑事責任保護不足，則可能於現行仍有刑事責任的情形下，對明知道生成之內容會侵害他人著作權的使用者責任，或許仍可保留刑事責任，整體而言還是傾向除罪化。

(3) 希望能透過這樣免責誘因的機制設計，讓創作者於 AI 發展環境中與技術開發者並進，讓不同的立場的利害關係



本報告之智慧財產權歸屬於國發會

人，更瞭解這些技術的本質，以及對社會的影響，一起達到可以讓個人及社會公共利益，更往前進的方向。

(九)交流討論

退出權的部分，讓著作權人透過有效方式明確反對作品被用於 AI 訓練，能有效兼顧著作權人意願，又不會阻礙 AI 產業的發展。現行的退出權規劃是否有效？

1. 李姿儀老師

(1) 以實務上經驗而言，有些著作權人透過 robot.txt 的方式控制搜尋引擎爬取範圍，於業界較常見。但實務上 AI 開發者睜一隻眼閉一隻眼，雖有作事前保留但不使用。係技術開發者因資本較強大，看準個別創作者無法個別主張權利。因此我認為相關法制應有更好的設計，讓創作者不是完全限制 AI 的開發去利用自己的著作，而是用更能互相理解、可以並進的方式處理，可能是比較可行的方式。

(2) 事後退出部分，我的修法提案，若著作人的著作已被利用進去成為參數，於事後退出的效力是對未來產生效力，也就是不溯及既往，讓技術開發不會與實務進行衝突太大。

2. 樊晉源組長

退出權對產業是好的，但是沒有照顧到科技弱勢者，因為他們不懂這樣的權利。例如現行網路服務的使用者條款，多數人是不會去閱讀的。

3. 李佩昌律師

退出權對產業是好的，但是不一定會照顧到科技弱勢者，因為他們通常不懂這樣的權利。例如現行網路服務的使用者條款，多數人是不會去閱讀的。所以，仍應有配套機制，給予臂力用人合理的報酬或補償。

4. 賴文智律師

(1) 事前退出比較像機制，事後退出已非權利行使而似懲罰。事前要如何退出，現在歐盟也不清楚，像 robot 的方式，要如何很清楚排除抓取的資料不能用作 AI 訓練？事實上，AI 的訓練也有很多種。事後退出更困難，因其退出可能導致整個 AI 參數變化不明且事後難以查明。即使行使事後退出權利，AI 還是可以騙過人，光是如何評定退出完成是很困難的。除非要求 AI 訓練每天或每段時期都保留一個版本，要行使權利時，依據訓練版本回復到資料加入之前的參數，後續重新訓練，否則有點像是被遺忘權的行使，技術上似乎不太可行。

(2) 另一個問題是，為什麼一定要遺忘掉，有時候需要思考，權利人的權利到底有多大？著作中所描述的內容，不見得都屬於著作權人的。例如哈利波特一書運用許多西方歷來的魔法概念，倘因要遺忘本書，這些歷來概念都要遺忘嗎？或是可釐清哪些是本書特有的？因此我對退出權沒有很大的期待，因為執行或驗證都不是那麼容易。但法制上的事前排除，是一種安慰劑，實際上能不能知道著作被利用，例如透明度部分，歐盟有要求開發者提供摘要，但是上有政策下有對策，開發者繳交的摘要也難以完全核實。「退出權」制度上可以考慮，但不需要有太大的期待，因為執行和行使權利都不容易。



本報告之智慧財產權歸屬於國發會

## 參、 成果綜整

### 一、 出席人數及活動意見調查

報名人數：157 人，實際參加總人數：127 人。

回收有效問卷數：59 份。

(一)對(10/29)的整體看法

表 2 活動問卷整體看法統計結果

| | 本研討會主題設計 | 本研討會時間安排 | 本研討會活動流程 | 會議地點與環境 | 活動現場各項服務 |
|---|---|---|---|---|---|
| 分數 | 4.54 | 4.46 | 4.49 | 4.64 | 4.63 |
| 總分(平均) | 4.55 | | | | |

資料來源：研究單位繪製

(二)對(10/29)各主題的看法

表 3 活動問卷各主題看法統計結果

| | 主題一<br>AI監理沙盒機制與創新治理 | 主題二<br>生成式AI訓練資料的著作權挑戰 |
|---|---|---|
| 議題設計 | 4.56 | 4.63 |
| 時間掌握 | 4.54 | 4.49 |
| 講者安排 | 4.49 | 4.58 |
| 對於增進本主題之理解 | 4.54 | 4.64 |
| 總分(平均) | 4.53 | 4.58 |

資料來源：研究單位繪製



本報告之智慧財產權歸屬於國發會

(三)建議與反饋

■ 主題一：

1. 獲益良多，謝謝。
2. 應該多一點互動。
3. 可惜時間有限，以致講者沒法深入討論議題。
4. 講者提到應用到台灣情境，各自訓練 AI 在領域內學習、而非想像強大 AI 做所有事，開放 API 交換的提議，感覺最務實而且科學。

■ 主題二：

1. 獲益良多，謝謝。
2. 全球皆要面對的議題。
3. 能找到不同立場的與談者，提供很棒的腦力激盪。
4. 建議可邀請著作權法主管機關與談，俾進一步瞭解未來政策方向。
5. 應該多一點互動。
6. 時間有限，以致講者針對本主題沒法更深入討論。再者，針對此主題與我國目前行政院通過的「人工智慧基本法」草案中之關聯部分亦無介紹提及，有點可惜。
7. 律師、出版業與微軟的討論營造出對立論，認為對議題探討還有中短期未來發展思考較沒有建設。律師講者因個人主見



本報告之智慧財產權歸屬於國發會

太過鮮明，對於此議題思考方向可能有所侷限。建議下次多增加一位律師專業，但有不同觀點的另一方，擴增思考範疇。

(四)對未來辦理研討會主題建議或其他意見

1. 有尋找產業、學者、官方等提供不同角度建議。
2. 可針對個資與 AI 運用的衝突與共榮進行討論。
3. 希望未來政策有不同觀點時，可以多舉辦這類研討會激盪想法。
4. 希望可以舉辦導入人工智慧的經驗分享或策略研討會。
5. 主辦單位相當優秀！
6. 對此次研討會之主持、與談者之內容，非常滿意。無其他意見。
7. AI 及個資法。
8. 希望未來能辦理關於人工智慧基礎設施、主權 AI 等相關國際及國內法制之介紹及因應的研討會主題。感謝！
9. 重要議題而且趨勢火速改變，建議每六個月或一年辦一次研討會。

二、 活動照片及影片

本次活動委請專業攝影團隊拍照及攝影，執行團隊已於活動結束後整理提供委託機關。



本報告之智慧財產權歸屬於國發會

# 第二分項、國內法規環境建構幕僚協助與新興議題因應事宜

## 項次 1. 法制幕僚研析意見

## 壹、 智慧機器人產業推動法制相關幕僚意見

### 一、 智慧機器人產業發展背景

為解決因出生率下降、人口高齡化之社會問題所造成之人力短缺，自 2010 年以來機器人已廣泛運用於各領域。其中製造業工廠中等多使用工業型機器人。而對於食品供應、車站、機場或清潔等服務業相關之產業則多有使用服務型機器人之事例。早期由科幻作家艾西莫夫(Isaac Asimov)提出著名的「機器人三法則」[111]：一、機器人不得傷害人類，或因不作為使人類受到傷害[112]；二、除非違背第一法則，機器人必須完全服從人類命令[113]；三、在不違背第一及第二法則下，機器人必須保護自身安全[114]，此三原則於機器人研發及法令發展歷程中被沿用至今。

然 2017 年後伴隨 AI 技術發展日益精進，打破長久以來機器人僅係「服從人類命令」之規則。歐盟 2023 年修訂公布之「機械規則」[115]前言第 12 點即指出，目前市場上已推出更先進之機器，它們對於人類操作之依賴程度較低。這類機器雖係執行定義的任務，並於結構化之

---

[111] The Three Laws of Robotics (often shortened to The Three Laws or Asimov's Laws), presented to be from the fictional "Handbook of Robotics, 56th Edition, 2058 A.D."

[112] A robot may not injure a human being or, through inaction, allow a human being to come to harm.

[113] A robot must obey the orders given it by human beings except where such orders wo uld conflict with the First Law.

[114] A robot must protect its own existence as long as such protection does not conflict wi th the First or Second Law.

[115] European Union, Regulation (EU) 2023/1230 of the European Parliament and of the C ouncil of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parli ament and of the Council and Council Directive 73/361/EEC, Regulation - 2023/1230 - EN - E UR-Lex, Last visited 2025.1.21.



本報告之智慧財產權歸屬於國發會

環境中作業，卻可於該環境中學習執行新的作業，從而變得更加自主。可以說機器之進一步改造及進化已在進行中或已可被預期，其中包括即時資訊處理、問題解決、移動性、感測系統、學習性、適應性以及得以在非結構化環境（例如建築工地）中運作之能力。歐盟執委會於2020 年 2 月 19 日曾提出關於 AI、物聯網及機器人技術之安全和責任影響報告即指出，AI、物聯網及機器人等新興數位技術的出現，於產品安全層面帶來新的挑戰。該報告即認為當時產品安全相關法規，包括機械指令(2006/42/EC)，與上開數位技術推展而引發且須處理之產品安全問題，仍有相當之差距，需有進一步建立規範，以應涵蓋新數位技術產生的安全風險，此報告即為 2023 年機械規則建立之基礎。

因此，基於機器人之技術演變，可以認為所謂之智慧機器人，係有別於傳統機器人，而運用新興科技提升自主執行任務能力之機器人。韓國智慧機器人發展及促進法（詳貳韓國專法摘要），則定義「智慧機器人」是指能夠辨識外部環境、判斷情況並自主運作的機械裝置（含機器運行所必須之軟體），足見從傳統依據固定指令運作之機器人，走向智慧機器人發展，其差異主要在於機器人已因 AI 等數位技術之應用，走向能夠更精確地感知、辨識、判斷、自主運作甚至有分析的能力，對傳統對機械安全規範有相當之衝擊，並與晚近 AI 監管法令產生某程度之關聯性。亦即，對原工業型及服務型機器人時代之監管，主要規制之產品投入市場前安全標準、測試要求等規範。進入與 AI 結合之時代，需進一步考量 AI 演算與自主運作帶來的風險、與 AI 基本倫理之符合性，以及其他與 AI 運作相關之法令關係（如個人資料相關規範等），上開議題已成為近年國際機器人法制討論之重點。以下主要針對近三年國際間對於智慧機器人法制政策層面，較為直接且具體之法制及標準層面，進行重點摘整。



本報告之智慧財產權歸屬於國發會

## 二、 國際法制發展狀況

目前以通用、非針對特定領域之機器人法制政策來說，國際上直接對於智慧機器人發展與推動有專法制定者主要為韓國「智慧機器人發展及促進法」，歐盟過往對於機器人之產品安全及責任，有機械指令之適用，而面對 AI 等相關技術應用，具備自我學習、判斷與自主性之機器人發展，則於 2023 年將機械指令進行規範之增訂，並升級為機械規則。專法或機械規則較屬於直接之法制面規範，此外亦有包括歐盟、日本及美國，至於特殊領域部分，發展較多者為與自駕車相關之規範，然若討論智慧機器人，則主要是自主移動機器人之發展及應用，有部分之法制討論。基於本次主要是蒐集對應機器人之相關法制，故專注於自駕車部分之法制則暫不予列入，而主要整理對智慧機器人較直接之法制或標準，並補充部分自主移動機器人之資訊。

### (一)制定專法：韓國「智慧機器人發展及促進法」

#### 1. 法令背景

針對勞動及高齡化社會之需求，韓國大力發展機器人產業，並於 2008 年 9 月即制定通過第一版之「智慧機器人發展及促進法」（지능형로봇개발및보급촉진법）[116]（簡稱「韓國機器人法」）。該法旨在促進機器人之開發與佈局，奠定推動機器人產業政策發展之法令基礎。該法嘗試對於智慧機器人進行定義，透過要求政府對智慧機器人制定推動發展之基本計畫，支持產業發展並同時確保產品安全。除促進產業發展外，該法隨著機器人產業之持續推動，陸續進行多次修訂，其中並有參考歐洲議會所提出「機器人民法

[116] 지능형 로봇 개발 및 보급 촉진법,https://www.law.go.kr/, Last visited 2025/1/22



本報告之智慧財產權歸屬於國發會

規則」[117](Civil Law Rules on Robotices)，並引入「智慧機器人倫理憲章」之概念，於規範當中建立包括對智慧機器人之開發人員、製造商及消費者等所應遵守之準則，於促進開發的同時，降低及防止智慧機器人基於其功能，而對社會可能衍生之危害。

2017 年伴隨 AI 之興起，機器人之發展已從原先完全依靠人類指令，逐步進化成可能脫離人類操控而有相當自主判斷與運作之技術，其可能產生之風險已與過往純粹指令引導之機器人有相當之差異。

韓國會議員曾經於 2017 年 7 月 19 日提出「機器人基本法草案」（로봇기본법），期望可以因應智慧機器人發展可能產生之風險。該草案於倫理道德及責任分配歸屬之風險控管上提出相關建議機制，然當時多數意見認為過早訂立監管規範，可能扼殺新創技術或產品之發展，故議會最終並未通過該草案，但已為後續之修法埋下伏筆。

2018 至 2023 年為因應自動駕駛電動車及無人載具等技術之應用及發展，韓國機器人法陸續進行了 5 次修法。最新 2023 年之修正，新增戶外移動機器人之定義，明確允許可於人行道通行之機器人上路，透過安全認證機制確保人行安全，並規範強制保險以應對戶外移動機器人可能對人身或財產可能產生之損害。本次修正同時刪除對於智慧機器人投資公司之相關內容，取消智慧機器人公司須經特許之相關規範，以利持續擴大機器人產業之永續發展。

[117] Civil law rules on robotics, https://www.europarl.europa.eu/RegData/etudes/ATAG/2017/599250/EPRS_ATA(2017)599250_EN.pdf, Last visited 2025/1/22



本報告之智慧財產權歸屬於國發會

2. 法令架構及內容重點

現行韓國機器人法涵蓋定義、基本計畫、推廣、實驗場域（機器人園區）及推動法人與罰則等方面，與智慧機器人推動較為相關之規範重點，摘要整理如下：

(1) 明確智慧機器人之定義

2023 年修法將第 2 條「智慧機器人」定義修正為識別外部環境並可自主判斷情況之機械裝置（包括機器運行所必須之軟體），並進一步於第 4 條(2)新增「戶外移動機器人」之定義，指能夠自主操作（包括遠端控制）進行送貨等工作的智慧機器人。由此可看出，韓國智慧機器人之定義已包含運用 AI 技術之機器人產品。

(2) 每 5 年制定機器人政策之基本計畫

與韓國其他科技法令類似，韓國機器人法同樣要求政府應制定機器人基本計畫，並由機器人產業政策審議會協助審議，該基本計畫應每 5 年制定 1 次。

(3) 確保產業發展之所需及保障人民權益

韓國 2023 年修法仍保留產業通商資源部對於制定「智慧機器人倫理憲章」之授權，內容包含關於機器人技術倫理之發展方向，開發、製造及使用機器人時所必須遵守之道德與行為準則。

除機器人倫理外，2023 年修法新增第 19 條之 2 針對智慧機器人損害保險業務，指定可提供相關保險服務之事業，並對於戶外移動機器人部分，提供保險服務之事業若認為有必要，可以請依據第 40 條之 2 規定受指定之安全



本報告之智慧財產權歸屬於國發會

認證機構，提供運行安全認證有關之資料，該指定安全認證機構不得拒絕，以利對於戶外移動機器人損害保險提供之評估與落實。

(4) 建立機器人創新園區，提供研發環境

韓國致力於發展機器人產業，故自 2012 年起修訂機器人法創建機器人園區，以提供該產業實驗與技術開發之場域。從土地開發區之指定、實施計畫之批准、工程開發與竣工確認、園區使用、費用收取到園區管理等皆有對應之規範，提供產業開發之相關支援。

(5) 新增戶外移動機器人運行安全認證等相關安全要求

隨著 AI 技術之發展，自駕車、無人載具技術已逐漸成熟並進入市場，伴隨而來則是安全問題。故韓國於 2023 年修法新增第 40 條之 2 至第 40 條之 4 就戶外移動機器人之操作安全認證之規定，要求戶外移動機器人若要進入市場，必須獲得指定安全認證機構之安全認證。取得安全認證者，得展示安全認證標示並用以宣傳；反之，若未獲得安全認證者，則不得展示相關安全認證或類似標誌，亦不得宣稱已取得安全認證。而安全認證之標準，以及認證機構之指定，將由產業通商部負責。若所提供之商品不符合安全認證，產業通商資源部可採取責令改正等相關必要措施。於第 40 條之 3，並規定產業通商資源部可以取消安全認證之情形，包括以虛假或詐欺手段取得認證、不符合認證標準、生產不適當之戶外移動機器人而有對行人等造成嚴重傷害之風險、不遵守產業通商資源部之改正命令等情形。已獲安全認證之業者，則需對可能於人行道等區



本報告之智慧財產權歸屬於國發會

域，因機器人運作可能造成人身、財產損失之情形，依法進行投保。

(6) 推動機構、相關配套措施及罰則

為有效率、有系統地推進智慧機器人產業振興項目，支持智慧機器人產業相關政策的制定與推行，韓國於 2010 年即依據機器人法第 41 條，成立韓國機器人產業振興院（以下簡稱「機器人振興院」[118]）。該組織為類似行政法人之組織，主要功能在促進及落實機器人產業政策、產業發展趨勢研究、落實機器人倫理憲章、支援機器人國際合作與海外拓展、機器人發展之認證項目、產品標準之研發與發布、支持機器人產業創新及成長、專業人員培訓等各項與機器人、智慧機器人發展推動有益之任務。2023 年修法對於新增戶外機器人安全認證部分，並有對應罰則之訂定，以強化安全認證之落實。

(二)國際組織規範或國際相關標準

1. 歐盟 2023 年機械規則

2023 年 6 月，歐盟理事會發布「機械規則」[119](Regulation 2023/1230/EU – machinery)，此一規則，基本上取代了歐盟於 2006 年發布之「歐盟 2006 機械指令」(Directive 2006/42/EC - machinery directive)，將更具強制力，且將直接適用於各會員國，機械規則除少數條文陸續於 2023 及 2024 年實施外，將於 2027 年 1 月起全面適用。

[118] 韓國機器人產業振興院（한국로봇산업진흥원）成立目的與歷史，https://www.kiria.org/portal/intro/portalIntHistory.do, last visited: 2025/1/23.

[119] European Union, REGULATION (EU) 2023/1230, supra note 115.



本報告之智慧財產權歸屬於國發會

2023 年機械規則與 2006 機械指令相同，主要係就機械產品進入歐盟市場之基本健康及安全需求建立標準，旨在使機械及其相關產品進入市場並確保人員之健康及安全。

由 2006 年指令進化到 2023 年之規則，主要是鑒於數位科技之高度發展，機器(包括機器人)之運作對人類之依賴度逐步降低，部分智慧機械並提高自主資料取得、學習與判斷之能力，包含即時資訊處理、問題解決、移動性、感測系統、學習性、適應性以及得以在非結構化環境（例如建築工地）中運作之能力等等技術發展，都較過去進步。2006 年之機械指令已不足以應對當前科技技術之發展。2023 年機械規則為彌補原有指令之不足，特新增可涵蓋新興數位技術之相關規定，尤其包含自主移動機械(autonomous mobile machinery)、物聯網設備及 AI 運用相關智慧設備所產生之安全風險。機械規則之適用範圍為機械產品本身及其相關產品，包含可互換設備、安全元件、起重配件、鍊條、繩索與鐵帶以及可拆卸之機械傳動裝置，並包含部分完成之機器。惟機動車輛及其拖車、用於遊樂場之特定設備或專為研究所設計製造之實驗室臨時使用之機械並不適用。

依據機械規則第三章之規定，製造商於設計及製造機械及相關產品時必須符合附件三之基本健康及安全要求(Essential Health and Safety Requirements, EHSR)，包含如材料、照明設備、人體工學等與產品設計及運作相關之要求。製造商在證明其機械及相關產品符合規則要求，則需擬定歐盟符合性聲明並於機械貼上 CE 標章。製造商於符合基本健康及安全要求後欲將產品投入市場前，必須依照第四章之規定進行合格評定程序(Conformity Assessment)。合格評定程序是對產品進行檢測確保其符合相關法規及標準。該規則允許製造



本報告之智慧財產權歸屬於國發會

商進行自我評估以證明其產品符合相關要求。惟附件一第一部分(Annex I Part A)所提及之高風險產品則須強制由第三方機構進行檢驗或認證，不得再像過往採取自我聲明之方式。此部分即係包括與 AI 應用相關之兩種機械：使用機器學習方法確保安全功能且具自我進化行為(self-evolving behavior)之安全組件，以及設有機器學習方法確保安全功能且具自我進化行為之嵌入式系統機械等，皆被列為附件一中具高風險之產品，於進行合格性評定程序時需強制由第三方機構進行認證(規則第 4 章第 25 條第 2 項規定)，智慧機器人即屬於此類機械。

因此歐盟 2023 年機械規則對於智慧機器人之適用而言，主要係針對該機器人已經具備自我進化能力，且係以機器學習等技術確保安全功能時，為確保該類自主機械設備之風險受到適當之管控與監督，透過強制第三方檢測與驗證，提升安全風險控管之效能。

2. 日本主導服務型機器人運行國際標準之制定及發布

日本社會正面臨出生率下降及人口老齡化造成之人力資源不足問題，因此各類服務型機器人開始積極進入各產業之應用，如送餐機器人、車站及機場之清潔、安檢或醫療設施之護理機器人等。為確保機器人在運作過程中不會對人員造成傷害。2023 年 11 月由日本經濟產業省主導制定之「服務型機器人運行國際標準」[120]（サービスロボットの安全な運用に関

[120] 日本經濟產業省，日本発のサービスロボットの安全な運用に関する国際規格が発行されました，https://www.meti.go.jp/press/2023/11/20231113001/20231113001.html，最後瀏覽日：2025/1/22。



本報告之智慧財產權歸屬於國發會

する国際規格，ISO 31101），順利於 ISO 正式發布，日本並以此標準進行服務型機器人標準化之推動。

於上開標準訂定之前，已有對服務型機器人製造商之安全要求，但尚未有對於使用服務型機器人之企業及其安全操作建立之國際標準。故上開標準旨在建立服務提供者透過機器人提供服務就安全運行管理層面所應具備及落實之基本要件，尤其應確保對機器運作知識較不足人員之安全。該標準規定服務提供者應實施之作為，如應識別機器人服務可能產生之相關風險及可能之原因，並進行風險評估以避免或降低相關風險之發生，且須具體實施員工訓練。

標準當中對於服務機器人利用與管理之要求及建議，包括需有機構高層之參與、服務提供者須進行風險評估及採行降低風險之措施、須提供得以建立及實施安全措施所需之資源、須進行服務營運期間之規劃、管理以及績效評估，並須持續改進。

3. 美國

(1) 機器人安全標準

美國並未針對機器人開發與產品，進行聯邦層級之專法規範，然而其對於機器人安全層面，從早期之工業機器人、協作機器人等皆透過與 ISO 整合之國家標準制定，進行安全層面之原則要求。2020 年後並考量自主移動機器人（Autonomous Mobile Robot, AMR）特性，研議公布新的機器人安全標準。部分州別則就其需求有法制面之考量，簡述如下：



本報告之智慧財產權歸屬於國發會

美國國家標準協會(American National Standards Institute, ANSI)針對工業機器人以及協作機器人之應用皆有制定相關標準，分別為「工業機器人安全標準」[121] (ANSI/RIA R15.06-2012 Industrial Robots and Robot Systems - Safety Requirements)以及「協作機器人應用之安全指導」[122] (RIA TR R15.606-2016 Technical Report - Industrial Robots and Robot Systems - Safety Requirements)。兩標準皆係內化 ISO 機器人相關標準所制定，但尚未涵蓋特別針對智慧型機器人安全標準之內涵。

「工業機器人安全標準」規定了工業機器人之安全設計、保護措施及使用資訊之全面要求，該標準基於 ISO10218-1 及 ISO10218-2，旨在使美國之安全規範與全球標準接軌。該標準適用於工業機器人之設計、製造、整合及使用完整生命週期之安全性，並針對不同階段訂定對應之安全要求，例如於設計階段要求機器人應內建緊急停止功能、速度監控緊急停止功能等。此外，該標準亦有規定風險評估，包含機器人系統需有識別危險之功能並能夠評估風險及採取風險降低措施，且根據 ISO13849 對機器人有控制系統之安全設計。

「協作機器人應用之安全指導」是規範協作機器人系統及工作環境的安全要求，該標準是以前述「工業機器人安全標準」為基礎並參考 ISO/TS 15066 制定，規定了協

[121] ANSI, ANSI/RIA R15.06-2012 Industrial Robots and Robot Systems - Safety Requirements, ANSI/RIA R15.06-2012 - Industrial Robots and Robot Systems - Safety Requirements (CONTAINS CORRIGENDUM), last visited: 2025/1/22.

[122] ANSI, RIA TR R15.606-2016 Technical Report - Industrial Robots and Robot Systems - Safety Requirements, https://webstore.ansi.org/standards/ria/riatrr156062016#:~:text=This%20Technical%20Specification%20specifies%20safety%20requirements%20for%20collaborative,supplements%20the%20requirements%20and%20guidance%20on%20collaborative%20indust, last visited: 2025/1/22.



本報告之智慧財產權歸屬於國發會

作機器人之設計、安全評估及應用。協作機器人依據該標準之定義為能夠與人員共享工作空間且無須物理隔離之工業機器人。為確保人員之安全，對於協作機器人軟體本身以及工作環境皆須進行全面評估，並考慮於與機器人協作運用時之人體工學優勢，而在風險評估以及人體容許力及壓力限制部分，需依照 ISO 15066 之規定進行。

故美國雖有自行訂定針對機器人安全運行之標準，惟其標準內容亦仍是參考或以 ISO 標準為基礎，以使其機器人之生產及產品運作符合國際標準。目前則尚未於機器人相關之上述國家標準中特別針對智慧型機器人特性進行增補，然而早期工業用機器人之安全標準設計，係針對固定式之機器人，故若應用於晚近開發之具移動能力之機器人(Mobile Robot)，則尚有不足。

為因應得以移動或自主移動之機器人發展，美國國家標準協會(ANSI)即於 2016 年成立 R15.08 標準之研議之委員會其中涵蓋多位參與 ISO 機器人標準制定之成員，於 2020 年，美國公布 ANSI/RIA R15.08-1:2020 標準中首度定義了自主移動機器人，同年 ISO 亦公布 ISO 3691-4:2020 標準，皆納入考量自主移動機器人特性之安全規範。

(2) 加州對話機器人揭露法案

為防範「利用對話機器人誤導消費者其係與真人進行溝通，並誘使消費者進行不公平交易」，加州於 2018 年通過「對話機器人揭露法」[123](Chatbot Disclosure Law，SB-1001 Bots: Disclosure)，該法案於通過後被收錄於「商業與

[123] California Legislative Information, SB-1001 Bots: disclosure, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001, last visited: 2025/1/22.



本報告之智慧財產權歸屬於國發會

專業法典」(Business and Professions Code)第 6 章中。該法所定義之機器人，係指非由人為操作或發表貼文之自動化線上帳戶；而人之定義除自然人外亦包含公司、有限責任公司、合夥企業、合資企業、協會、政府等法律實體或組合。若任何人使用機器人與加州之其他人在線上通信或互動，並意圖以虛假身分誤導他人以達成故意欺騙他人進行交易或影響選舉之目的者，皆屬於非法行為。除非使用機器人之人已揭露其是使用機器人進行互動。此處所謂揭露，則是需以清晰、醒目且設計合理之方式告知與機器人通信或互動之人。

(3) 麻州議員提案之負責任使用機器人法案

麻州眾議員 Lindsay Sabadosa 及參議員 Michael Moore 於 2023 年提出一份確保負責任之使用先進機器人科技之法案(An Act to ensure the responsible use of advanced robotic technologies[124])，此法案主要著眼於先進機器人之發展，若該類機器人被用於裝載武器，將可能對於公眾安全產生高度影響。故要求透過法案限制麻州機器人、無人機或其他無人機器人設備，裝載相關武器，並禁止使用機器人設備進行威脅、騷擾或其他對人的身體拘束。目的在確保先進機器人設備被用於對經濟及公眾生活有益之用途，禁止不當之濫用[125]。此項法案提出當時受到包括波士頓動力機械公司及國際無人駕駛車輛系統協會等之支持。該法案於 2023 年至 2024 年經過聽證及議會之討論後，於 2024 年 7

[124] An Act to ensure the responsible use of advanced robotic technologies, Bill S.2483

[125] State Representative Lindsay Sabadosa & Senator Michael Moore File Bill to Ensure the Responsible Use of Robots, https://www.senatormikemoore.com/new-blog/2023/9/13/state-representative-lindsay-sabadosa-amp-senator-michael-moore-file-bill-to-ensure-the-responsible-use-of-robots, Last visited：2025/1/24



本報告之智慧財產權歸屬於國發會

月重新修訂更改為與公民權利及科技相關之法案(An Act Relative to Civil Right and Technology[126])，該法案將所謂之機器人設備(Robotic device)定義為一種能夠移動、導航或飛行之設備，可以根據命令、回應感測器資料或兩者之組合，於遠離控制者或監督者之位置，進行運動、導航、移動或飛行的設備，包括但不限於無人駕駛之飛機或車輛。其規範則主要係明列不得以機器人設備從事之行為及罰則，規範除了部署機器人設備之一般事業外，對於執法機構採用機器人設備進行調查之特定作為，包括透過該類設備進入私人資產或進行監視、位置追蹤等，皆須有相當之令狀要求等限制。

(三)特定領域之規範建構：以個人自動貨運裝置為例

個人自動貨運裝置(Personal Delivery Device, PDD)之概念係由美國提出，屬於自主移動機器人實務運用之一類，主要係以電池及電動馬達為動力，可於行人區域移動（部分情況可行駛於一般道路），係為專門用以運送貨物而設計之自動化機械。此類貨運裝置已在多國出現，如歐洲所稱之人行道自動貨運機器人(Sidewalk Autonomous Delivery Robot)、日本所稱之自動行走機器人（自動走行ロボット）及韓國所稱之戶外移動機器人（실외이동로봇）。此類機器人因已進入市場運用，故國際上已有部分國家對其實務影響訂定對應之規範，然定義或歸類上則有差異。如美國州法（如路易西安那州等，自 2017 至 2022 年已有超過 20 州訂定關於 PDD 之規範）對於 PDD 之規定，大多將其列為非車輛（歸屬行人或其他獨立類別），若認為歸屬於行人，則要求 PDD 須遵守行人相關之規範，禮讓具有路權且行為合法之行人或其他交通主體（含車輛），並有針對其上路（行駛／運行）安全與保險等之

[126] An Act Relative to Civil Right and Technology, Bill H.4832, https://malegislature.gov/Bills/193/H4832, last visited：2025/1/24



本報告之智慧財產權歸屬於國發會

要求。而日本則認為其應屬於小型車類型，若於人行道移動，應確保不對行人造成危害。日本警察廳於 2021 年曾對此類機器人之道路試驗訂定使用許可基準[127]，以確保該類機器人於研發過程所需進行之道路實證，符合一定之規範要求。日本並於 2022 年修正道路交通法，要求該類機器人無論實驗階段或進入商用階段，皆需要申請道路許可[128]。韓國則係於 2023 年韓國機器人法當中將戶外移動機器人之安全認證機制等監督規範納入規定，已如前述。

## 三、 結論

為解決高齡化等社會問題造成勞動力逐年下降之現實，許多國家投入發展機器人產業已有相當之歷史。2017 年以前，機器人之運用主要在工業機器人及自主運作程度較低之服務型機器人層面。2017 年以後隨著 AI 之興起，各國開始投入先進之機器人技術研發，包含運用 AI 相關之概念及技術，開發具高度感測、資料蒐集、分析與逐漸自主運作之機器人，並有部分產品已進入市場運用，如前述各國已關注且建立必要規範之自主移動機器人。而隨著歐盟對於 AI 監管通過專法，現有機器人相關法制，對應到蘊含 AI 元素之智慧機器人時，AI 監管規範與機器人法制間即可能產生交互之關係，尚須進一步觀察。以目前已知之國際規範來看，大致可歸納出以下法制政策之走向：

### (一)對機器人產業發展訂定專法或促進實驗場域運用之規範，非國際常見作法但有相關事例。

目前對於智慧機器人之研發、推動與監督有訂定專法者，主要有韓國機器人法，其係自 2008 年開始推動機器人產業以來，即伴隨發展

---

[127] 特定自動送貨機器人公路試驗道路使用許可基準（特定自動配送ロボット等の公道実証実験に係る道路使用許可基準），https://www.meti.go.jp/shingikai/mono_info_service/jidosoko_robot/pdf/004_04_02.pdf, 最後瀏覽日：2025/1/24

[128] 道路交通法の一部を改正する法律（令和四年法律第三二号），https://www.sn-hoki.co.jp/article/pickup_hourei/pickup_hourei2104043/ ，最後瀏覽日：2025/1/24



本報告之智慧財產權歸屬於國發會

進程以及技術演變，持續進行修訂，直至 2023 年將智慧機器人之特性納入考量，並將已進入市場運用之戶外移動機器人之安全認證機制納入規範。該法主要重點尚包括對於機器人政策之研議、推動與落實，並透過機器人創新園區之建構，提供機器人產業發展所需之實驗場域，並設置法定推動機構機器人振興院，進行整體規劃與推行，包括相關之政策資源、標準研議與人員培訓等，可以看出其長期發展機器人之高度企圖心。

日本雖並未針對機器人訂定專法，而主要是針對服務機器人安全層面推動國際標準的制定，然而由 PDD 的法制規範，可以看出日本政府對於特定領域機器人發展仍有相當之法制支援，例如 2021 年警察廳公布之特定自動送貨機器人公路試驗道路使用許可基準，則是允許開發自動送貨機器人測試之實務實證的規範事例。透過特定領域智慧機器人發展所需，研議對應之法制方案，亦不失為可參考之作法。

(二)多數國家或國際組織主要係著眼於機器人技術之發展進程，對應進行標準或安全規範之研議或修訂。

歐盟、美國及日本，對於智慧機器人之發展，主要皆係從產品或服務安全之角度出發，訂定相關標準或規範。歐盟 2023 年機械規則係於機械發展之法制要求層面，考量機器人等機械設備已進入到涵蓋機器學習與自我進化之技術應用，將引發更高且為早期機械指令無法處理之安全風險，故對相關規範予以修正、增訂並提升規範強度，同時對應 AIA 對於高風險 AI 產品之監督與要求，於新興規則當中分離出需要經過第三方查核驗證之高風險產品類型，以強化即確保該類產品進入市場之安全。而美國同時從國家標準與 ISO 國際標準之促進著手，除早期對於工業機器人或協作機器人建立安全標準外，並針對近年發展之自主移動機器人建立新興安全標準等。加上前述韓國專法當中對於戶外運送機器人安全認證之要求，可以認為對於機器人之監督，主要國家或國際組織所重視的，尤其涉及可能進入市場運用之智慧機器



本報告之智慧財產權歸屬於國發會

人發展，將係以安全之確保為最優先之法制政策考量，無論是透過較為強制性之法制規範，或透過國家標準、國際標準之制定與採用等。

(三)對於相關規範之競合，以及法制規管之切入與分工，應係下階段機器人法制政策需要關注的重點。

目前所看到之機器人相關法制或標準，主要通過之時間點皆為2023 年以前。然而 2024 年伴隨歐盟 AIA 之通過，涉及 AI 之法制監管議題開始受到各國重視。除歐盟外，韓國亦於 2024 年底通過 AI 基本法，預計將於 2026 年 1 月生效。韓國 AI 基本法之規範雖然並未如同歐盟 AIA 進行高強度之監管，但也參考歐盟 AIA 規範，認為應該要建立相當之機制，確保高風險 AI 之安全可靠。而美國亦有部分州別，陸續建構 AI 監督或消費者保護之相關法制。足見涉及 AI 監督或發法制建構已逐步受到重視。

智慧機器人之發展與 AI 之運用具高度相關性，故對於 AI 技術、產業促進或監管之相關法制，亦可能與智慧機器人之發展與應用產生相當之關聯。包括涉及高風險 AI 運用之機器人研發等，於歐盟即須同時符合 AIA 之監督，並於機械規則正式生效後，亦須符合機械規則對於安全監督或第三方檢測之要求。而智慧機器人亦可能運用於不同之場域，涉及不同場域原有之法制規範，例如前述 PDD，於上路提供服務，則需要確定其定性是否為車輛或行人，決定其可適用之規範，並搭配其運作特性，進行現行法制（如日本修訂道路交通法）之調整等。

此外，智慧機器人之發展及運作基本上亦會涉及資料之蒐集、分析與傳遞。此與 AI 發展與運作相同，亦可能涉及資料隱私、情緒操控以及虛假、錯誤引導之問題，視其發展之類型與適用之情境將有不同法律規範之影響需予評估予配合。故未來推動上對於不同規範之競合，以及法制規管之切入點予分工，將有必要視推動重點及涉及領域與情境進一步予以評估。



本報告之智慧財產權歸屬於國發會

# 貳、 跨域資料運用研析

## 一、 國際跨域資料運用現況

### (一)美國

#### 1. 資料及 AI 相關法令脈絡

美國早於 2011 年即由其國家科學技術委員會(United States National Research Council, NRC)[129]，成立「智慧揭露工作小組」(Task Force on Smart Disclosure)，並於 2012 年提出促進消費者市場資訊透明化與效率之相關報告，透過標準化和可讀性之資料格式，使消費者得以更輕鬆獲取市場資訊，並鼓勵企業與政府部門提供清晰之產品服務諮詢，幫助消費者作出明智之選擇，從而增強市場競爭力。該份報告為美國資料治理政策奠定基礎，強調在資料經濟中，透明度對創新科技及消費者保護之重要性。爾後，於 2018 年美國發佈聯邦資料戰略(Federal Data Strategy, FDS)，制定包含資料可獲取性、共享性、透明度及責任等方面，提供政府清晰之資料管理框架，並於 2020 年提出行動計畫(Federal Data Strategy 2020 Action Plan)[130]，內容包含機構行動、跨機構行動及社區參與行動三類主體、20 項行動計畫，透過結構化之行動方案提升政府部門資料管理能力，促進公眾參與及信任。

然而由於美國並未如歐盟訂定與資料相關議題之專法，即使是個人資料保護議題，亦未有聯邦層級之法律規範，而係針對特定領域資料運用等需要訂定專法，例如 1996 年即通

[129] Informing Consumers through Smart Disclosure，https://obamawhitehouse.archives.gov/sites/default/files/omb/inforeg/for-agencies/informing-consumers-through-smart-disclosure.pdf, last visited 2025/2/17.

[130] Federal Data Strategy 2020 Action Plan, https://strategy.data.gov/action-plan/, last visited 2025/2/17.



本報告之智慧財產權歸屬於國發會

過施行的健康保險可攜與責任法(Health Insurance Portability and Accountability Act, HIPPA)。故其雖於 2019 年至 2022 年間針對 AI 議題，頒布或通過多項行政命令及法規，包括關於維持美國人工智慧領導地位之行政命令 13859（2019 年）、推動聯邦政府使用可信賴人工智慧之行政命令 13960（2020 年），但因缺乏明確、統一之細部執行規則與監管機制，導致實務落實過程情形不佳。雖陸續有關於 AI 聯邦層級法案提出，但目前皆尚未通過，僅有零星州別於 2024 年陸續通過與 AI 相關的監管法案，故亦無針對 AI 相關跨域資料運用之規範提出。

2. 資料隱私保護

如前所述，美國尚無聯邦層級之隱私或個人資料保護專法，而係針對特定領域或由各州依其需要訂定州法。加州消費者隱私法(California Consumer Privacy Act, CCPA)[131]2020 年 1 月 1 日生效，是美國首部由州訂定之隱私法，旨在增強加州居民對其個人資料之控制權。該法適用於年營收超過 2500 萬美元；每年購買、接收、販賣或分享超過 5 萬筆加州消費者個資；或年收入 50%以上來自販賣加州消費者個資者。其規範了消費者有知情權、刪除權以及選擇退出權、不受歧視權，並可對違規企業進行裁罰。在 CCPA 以前美國尚未有關於資料隱私等相關規範，該法透過賦予消費者更多控制權及透明度，促進企業在資料管理上之責任感，並在日益被關注之資料隱私問題上提供美國相關立法基礎。

[131] California Consumer Privacy Act, https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/#section1, last visited 2025/2/17.

由於資料之運用，除本國資料外，跨境資料流通亦是重要一環。由於歐盟與美國基於 GDPR 之限制流通不易，故美國及歐盟執委會於 2022 年 3 月 25 日宣布將建立新的跨大西洋資料保護框架(Trans-Atlantic Data Privacy Framework)[132]，以促進美國與歐洲之間的資料流通。歐盟執委會並於 2023 年 7 月 10 日通過對歐盟－美國資料隱私框架適足性認定[133]，促進兩地人民得以安全且適法的持續流通資料。

在此基礎上，2022 年 7 月 20 日，美國眾議院能源與商務委員會通過資料隱私和保護法案(American Data Privacy Protection Act, ADPPA)[134]，使該法案得以進入眾議院大會審議，目前尚未進一步通過。該法案旨在建立聯邦層級統一之資料隱私保護規範，性質上類似歐盟 GDPR。規範範圍包括資料蒐集最小化原則、消費者查看、修正及刪除等權利規範、企業處理個資透明度義務及隱私政策告知義務等。

3. 特別領域資料之機制或措施

美國對於大數據及 AI 之發展較早，且由於其分散式之管理模式，並未如歐盟有統一之資料戰略，但在特殊領域則有促進資料流通之相關措施。例如於地理區域層面，為推動區域內資料流通運用，而發展「國家空間資料基礎建設」(National Spatial Data Infrastructure, NSDI)，促進地理資料共享。由聯邦政府主導建立技術、政策、標準及人力資源之相關框架，並訂

[132] TRANS-ATLANTIC DATA PRIVACY FRAMEWORK, https://ec.europa.eu/commission/presscorner/api/files/attachment/872132/Trans-Atlantic%20Data%20Privacy%20Framework.pdf , last visited 2025/2/17.

[133] The EU-US Data Privacy Framework, https://www.data-privacy-framework.com/ , last visited 2025/2/17.

[134] H.R.8152 - American Data Privacy and Protection Act, https://www.congress.gov/bill/117th-congress/house-bill/8152, last visited 2025/2/17.



本報告之智慧財產權歸屬於國發會

定特別法，即「2017 年地理空間資料法」(Geospatial Data Act of 2017, GDA 2017)。該法主要係根本性的將所測量(Survey)及製圖(Mapping)成果皆解釋成地理空間資料(Geospatial Data)以利監督應用。而 2018 年接續修訂調整該法，並於 2018 年通過 GDA 2018，明確指陳地理空間資料應保障隱私管理及安全性，並建制全球空間資料基礎建設。至於對於健康、醫療等高敏感性特種資料的部分，更是著重隱私之保護，即使 AI 發展如火如荼之現在，涉及醫療保健領域之 AI 資料應用仍須符合 HIPPA 之標準與原則，以保障當事人隱私。其中包括必須確保資料處理從儲存至傳輸皆須安全，並須符合資料匿名化與去識別之要求；對於敏感資料之存取則需要有明確存取規則及授權，且須持續對於 AI 系統潛在違法行為進行監督。

## (二)歐盟

### 1. 歐盟資料戰略相關法案

#### (1) 歐盟資料戰略相關法案

歐盟為推動資料單一市場，於 2020 年提出歐盟資料戰略(European Data Strategy)[135]，並於戰略中勾勒推動資料流通運用所需之法律建構。其中即包含目前已通過之資料治理法(Data Governance Act, DGA)[136]及資料法(Data Act)等。除此之外，並提出歐洲資料空間之規劃，作為促進資料內部流通之配套機制。

---

[135] European Data Strategy, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en , last visited 2025/2/17.

[136] Data Governance Act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868 , last visited 2025/2/17.

惟歐盟推動資料單一市場規範相關資料新興規範之基礎，為其 2016 年已通過之歐洲一般資料保護規則(GDPR)。無論是何種資料之流通應用，只要涉及個人資料，皆以遵守 GDPR 規範為前提，例如以 GDPR 第 20 條規範之資料可攜權為基礎，於 DGA 進一步賦予個人更能控制自己被政府及企業所掌握之個資之權利，並規定公部門所持有含有個資之資料，於進行跨境傳輸時，需確保接收國必須具備與傳輸國同等保護之相關措施。

Data Act 主要係規定資料持有者可基於物聯網之使用者指示，提供第三方或公部門相關資訊，此部分係物聯網使用者於購買商品時就以契約協議，故涉及個資提供之層面仍是由當事人自主決定提供之情形。另規定公部門於緊急情況下，有強制私部門提供資料之相關例外規範，如在發生自然災害或人為引起之重大災害等公共緊急情況時，歐盟有權自私部門取用其持有之資料，但於特殊情況下資料持有者應獲得合理補償。緊急目的消失後上開資料即必須被刪除。

除上開資料法令係以 GDPR 規範為基礎進一步進行資料流通應用之配套規範外，GDPR 本身實際上也有規定於特定情況下，可較為彈性放況個人資料之利用的情形。例如，根據 GDPR 第 9 條(2)(j)，若符合第 89 條規定「為實現**公益利益、科學或歷史研究目的**或**統計目的**建檔所做必要之處理」的情況，且該處理符合尊重資料保護本質並採取適當且具體之保護措施確保當事人基本權利及利益時，則可對所蒐集之特種個資予以處理。然前述利用之前提已採取適當措施，必須符合資料蒐集最小化、進行資料影響評估等原則、並已採取假名化處理，亦即採用使資料



本報告之智慧財產權歸屬於國發會

無法識別或無法再識別當事人之技術手段。另根據 GDPR 第 9 條(4)規定，會員國可以維持或採用對於基因資料、生物特徵資料或健康相關資料的處理條件或限制之進一步規定。

(2) AIA 法案[137]

歐盟 AIA 法案於 2024 年 8 月 1 日正式生效並分階段實施。AIA 之法令重點在於透過制度監管建立可信賴之 AI 運用，包含最重要之風險分級制度及對於通用 AI(General purpose Artificial Intelligence, GPAI)提出需符合透明度要求之相關規範，其草擬之文件包含訓練資料、測試過程及評估結果等制定必須符合著作權指令(Copyright Directive)之政策，公佈用於訓練內容之詳細摘要。

除規範風險控管外，為支持創新，AIA 第 57 條明定歐盟會員國應確保其主管機關在國家層級建立至少一個 AI 監管沙盒(regulatory sandboxes)，亦可建立區域或地方層級之監管沙盒。監管沙盒建立目的主要係將可控風險集中於實驗場域，在此環境中測試並識別可能產生的風險，包括對於基本權、健康、安全、法令規範義務層面之風險。

然而涉及個人資料的部分，AIA 第 59 條亦有相關規範與限制：

A. 在 AI 監管沙盒中，為了其他目的合法蒐集的個人資料，僅在滿足以下所有條件時，才可為了在沙盒中開發、訓練及測試特定 AI 系統之目的進行處理：

[137] Artificial Intelligence Act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401689 , last visited 2025/2/17.



本報告之智慧財產權歸屬於國發會

a. AI 系統可以於以下一個或多個領域，由公務機關或其他自然人或法人為維護重大公共利益而發展：

I. 公共安全及公共衛生，包括疾病檢測、診斷、預防、控制和治療以及改善醫療保健系統；

II. 高水準的環境保護及品質改善、生物多樣性之保護、防止污染、綠色轉型措施、氣候變遷減緩和調適措施；

III. 能源永續性；

IV. 運輸系統及移動性、關鍵基礎設施及網路之安全性與韌性；

V. 公共行政及公共服務的效率與品質；

b. 處理的資料對於符合第 3 章第 2 節中的一項或多項要求是必要的，且這些要求無法透過處理匿名、合成或其他非個人資料有效實現；

c. 存在有效的監控機制，以識別在沙盒實驗期間可能出現的對資料主體之權利及自由的之任何高度風險，以及迅速降低這些風險的應對機制，並在必要時停止處理；

d. 在沙盒中處理的任何個人資料，都處於由預期之供應商控制的功能上獨立、隔離且受保護的資料處理環境中，且只有授權人員才能存取這些資料；

e. 供應商只能依據歐盟資料保護法進一步分享原始蒐集的資料；於沙盒中建立之任何個人資料皆不得於沙盒外分享；



本報告之智慧財產權歸屬於國發會

f. 在沙盒中處理任何個人資料，既不會導致影響資料主體的措施或決定，也不會影響其在歐盟資料保護法中規定的權利之適用；

g. 在沙盒中處理之任何個人資料，都應透過適當的技術及組織措施加以保護，並在參與沙盒終止或個人資料達到其保留期限後刪除；

h. 在沙盒中處理個人資料的日誌應在參與沙盒的整個期間內保存，除非歐盟或成員國法律另有規定；

i. 應保存對 AI 系統之訓練、測試及驗證背後之過程與理由的完整而詳細的描述，以及測試結果，作為附件四所指技術文件的一部分；

j. 應在主管機關的網站上發布在沙盒中開發的 AI 專案、其目標及預期結果的簡短摘要；此義務不應涵蓋與執法、邊境管制、移民或庇護機關之活動相關的敏感操作資料。

B. 為了在執法機關的控制和責任下，預防、調查、偵查或起訴刑事犯罪或執行刑事處罰，包括防範和預防對公共安全的威脅。在 AI 監管沙盒中處理個人資料應基於特定的歐盟或國家法律，並符合第 1 款中提及的相同條件。

C. 第 1 款之規定，並不影響排除因明確提及之目的以外之其他目的而處理個人資料之歐盟或成員國法律；且不影響針對處理個人資料之基礎要求之歐盟或會員國法律。該處理對於開發、測試或訓練創新 AI 系統



本報告之智慧財產權歸屬於國發會

或任何其他法律基礎是必要的，且須符合歐盟資料保護法。

2. 歐盟其他相關機制

(1) 歐盟創新議程(New European Innovation Agenda)[138]

歐盟執委會於 2022 年 7 月 5 日通過「新歐洲創新議程」，藉由引領創新，特別是在「深度技術」(Deep Tech)，例如 AI、量子科學、光子技術等領域之創新，強化歐洲在綠色轉型和數位轉型的中心角色，並為氣候變遷及網路威脅等迫切的社會問題，提供創新的解決方案，以減少能源依賴、改善民眾健康，並繁榮歐洲經濟，並提出重視實驗場域及創新採購之倡議，提出讓創新的企業可藉由「監理沙盒」(Regulatory Sandbox)等實驗場域(experimentation spaces)驗證其概念，政府則加強對創新產品和服務的公共採購(public procurement)，促進創新研發。

(2) 歐洲共同資料空間(Common European data space)[139]

為快速流通資料，歐盟透過計畫建立歐洲共同資料空間，目標在使空間內之私領域資料可有效被利用。自 2022 年建制以來已有 14 個領域之相關空間建制。然在空間內如欲利用資料，除需滿足統一技術標準及資料庫互通性外，仍需遵守 GDPR、DGA、Data Act 之相關規範。

以健康資料空間為例，除空間建立外，亦有對於該空間之運作建立規範。2025 年 1 月 21 日歐盟理事會通過歐

[138] New European Innovation Agenda, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0332, last visited 2025/2/17.

[139] Common European Data Spaces, https://digital-strategy.ec.europa.eu/en/policies/data-spaces, last visited 2025/2/17.



本報告之智慧財產權歸屬於國發會

盟健康資料空間規則(European Health Data Space regulation)[140]。其旨在提升歐盟層級內跨國存取個人健康資料並促進資料安全共享之公益利益。該規則提升個人對其數位健康資料之存取與控制權，同時也允許某些資料重新用於研究與創新之目的。故其實質提供特定於健康之資料環境，以確保歐盟境內跨境存取數位健康資料之服務。其主要規範有：

A. 使個人更容易取得健康資料

該規則係為使病患於不同醫療健保系統仍得以電子方式存取個人健康資料，包含病例摘要、電子處方、醫學影響、實驗結果等，並允許衛生專業人員於施行特定醫療行為時，有權存取病患資料。依據該規則，成員國被要求必須設立數位健康管理機構來落實。

B. 提升健康資料之研究潛力

為方便研究人員及創新者取得健康資料，在符合嚴格的歐盟資料安全、存取標準、基本權利保障及網路安全下，允許共享基於公益目的之匿名化或假名化健康資料。但目的限於：研究、創新、政策制定、教育及病患安全之公益範疇，禁止出於廣告或評估保險目的共享資料。

C. 確保互通性

[140] European Health Data Space regulation , https://data.consilium.europa.eu/doc/document/PE-76-2024-INIT/en/pdf, last visited 2025/2/17.



本報告之智慧財產權歸屬於國發會

目前各成員國之健康資料數位化程度存在差異，使得成員國跨境共享資料存在困難，故規則要求各國建立國家健康資料存取服務，並制定電子健康資料共享格式、品質、安全性及互通性等交換格式規範，確保資料於歐盟層面得以安全互通。

D. 權利要素

a. 選擇退出：成員國可以允許患者選擇退出對其健康資料之利用，無論是由醫療專業人員作為主要用途還是在嚴格條件下之二次利用，但出於公共利益、政策制定、統計及研究目的除外(符合 GDPR)。

b. 受限資訊：如果患者選擇限制資訊，醫療保健專業人員將只能在至關重要的情況下存取受限的健康資料。

c. 敏感資料：成員國可能會制定更嚴格的措施，管理對某些敏感資料之研究目的，例如基因資料。

d. 可信任資料持有者：為了減輕行政負擔，成員國可以建立可信任資料持有者之規定，以安全地處理存取健康資料之請求。

e. 臨床意義之發現：如果研究人員將可能影響患者健康的發現告知健康資料訪問機構(health data access bodies, HDAB)[141]，而患者資料被用於科學研究，則 HDAB 可以通知受信任的資料持有者，後者必須將這些發現告知患者或相關的醫療專業人員。

[141] Health data access bodies, https://health.ec.europa.eu/ehealth-digital-health-and-care/eu-cooperation/health-data-access-bodies-community-practice_en, last visited 2025/2/17.



本報告之智慧財產權歸屬於國發會

## (三)韓國

### 1. 資料法制脈絡

韓國於2022年9月由科學及資通訊部(Ministry of Science and ICT, MSIT)發佈「韓國數位戰略」，確立五大策略目標，即建構領先數位能力、促進數位經濟發展、創建包容性數位社會以及打造數位平臺政府及創新數位文化，並重點投資六大數位領域：AI、半導體、5G/6G、量子技術、元宇宙及網路安全。基於戰略目標，韓國逐漸完備數位法制建構：

(1) 數位權利法(Digital Bill of Right)[142]

韓國於2023年9月由MSIT發佈數位權利法案。該法主旨在確保數位環境下之自由與權利，強調安全、信任及持續創新。該法案認為在確保個體享有穩定之網路環境下，可隨時平等的使用各項數位服務，並可自由表達其意願但不可侵犯他人權利與社會道德，要求非歧視性的取得資訊之數位存取，並保障個資之查閱、更正、刪除及傳輸之權利，對平臺勞動、遠距辦公等自有資訊、資訊存取及控制等進行規範，並重視數位創新與國際合作。

(2) 人工智慧發展與建立信任基本法(Basic Act on the Development of Artificial Intelligence and the Establishment of Trust, 韓國AI基本法)[143]

---

[142] Digital Bill of Right, https://beingdigital.kr/front/digital_rights_new_en.do, last visited 2025/2/17.

[143] Basic Act on the Development of Artificial Intelligence and the Establishment of Trust, https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_R2V4H1W1T2K5M1O6E4Q9T0V7Q9S0U0 ,last visited 2025/2/17.



本報告之智慧財產權歸屬於國發會

韓國於 2024 年 12 月 26 日於第 22 屆國會全體會議上通過，並於 2026 年 1 月起實施。本法框架分為總則、推動體系、技術研發及產業培養、AI 倫理及可靠性確保以及附則五大部分。

其立法目的旨在透過規範 AI 建立信賴基礎，並提高國家 AI 之競爭力。立法體例上屬 AI 相關之特別法，於政府推動 AI 之組織結構上，新增設立國家 AI 安全委員會，負責審議 AI 政策及風險規範事項，並由 MSIT 負責統籌設立 AI 政策中心，每 3 年制定 AI 基本計畫，另再設立 AI 安全研究所，負責 AI 技術標準化、風險定義及評估方法等相關措施。

技術研發及產業培養上，建立政府政策支援研發規定，包括促進 AI 聚落建立、AI 資料中心政策等，另針對中小企業及新創給與資源及補助，培養 AI 人才。根據該法第 23 條規定，國家及地方應為振興 AI 產業及強化 AI 開發與應用之競爭力，得促進從事 AI 及人工技術研究與開發之企業、機構或團體在其功能、物力及地域方面進行集中化管理。該集中化必要時得依總統令規定指定 AI 集中園區，並提供行政、財政及技術支援。而第 25 條規定，政府應採取必要政策，推進用於 AI 開發與應用之資料中心的建置及營運，提供財政支援、為中小企業與研究機構等之 AI 資料中心利用提供支援、為該資料中心等 AI 相關基礎設施區域提供促進均衡發展的支援。而第 26 條則提出應設立 AI 振興協會，依其任務看似為促進推廣 AI 產品、培養人才及與國際合作等相關任務之法人。

在 AI 倫理及可靠性上，韓國有提出針對高風險之 AI 指定監管機制，包括確保透明度義務、安全義務等，亦有



本報告之智慧財產權歸屬於國發會

安全驗證及 AI 影響評估等配套措施，針對違反告知義務者，設有相關罰則。

由於該法於 2026 年 1 月才施行，就相關促進資料運用之 AI 集中園區及 AI 開發與應用之資料中心之運作模式尚待持續觀測其發展，但韓國似有針對 AI 之資料運用係希望透過政府建置資料中心予以解決。

(四)日本

1. 資料流通相關機制

(1) 協調性資料加值運用之資料管理框架

日本經濟產業省於 2022 年公布「協調性資料加值運用之資料管理框架－透過確保資料可信度創造資料價值之新路徑[144]」(協調的なデータ利活用に向けたデータマネジメント・フレームワーク～データによる価値創造の信頼性確保に向けた新たなアプローチ)文件，於網路及實體空間高度融合之工業社會中確保資料可靠性，並提出確保資料可信度之方法，以確保資料於不同組織間流通時之完整性及可靠性。

該框架將資料管理定義為「將資料屬性依所涉法令或組織規章及因蒐集處理利用移轉等活動而改變之過程，視為一生命週期加以管理。」。資料管理會受到三大元素影響，分別為屬性(資料種類、揭露範圍、利用目的、資料管理主體及資料權利者)、場域(各國或地區之法規、組

[144]協調的なデータ利活用に向けたデータマネジメント・フレームワーク～データによる価値創造の信頼性確保に向けた新たなアプローチ，https://www.meti.go.jp/policy/netsecurity/wg1/DataManagement-Framework.pdf



本報告之智慧財產權歸屬於國發會

織規範及組織間之契約等）以及事件（生成、取得、處理、利用、轉讓、儲存及處置），並依據此三要素建立個別資料管理模型。

該框架期待藉由此三要素依序透過資料處理流程（事件）視覺化、整理必要制度之保護措施（場域），如個人資料保護相關規範等、資料屬性具體化最後識別每個事件之風險之步驟，使利害關係人間之資料共享及治理更易進行。

(2) 資料信託功能認定指引 3.0[145]

2018 年日本總務省發布《資料信託功能認定指引第一版》（情報信託機能の認定に係る指針 Ver1.0），期望藉此推動其國內資料銀行之發展，並促進資料流通及利用。第一版主要為資料銀行所需具備之功能以及規範個資管理及向第三方提供資料之條件；第二版於 2019 年發布，對第一版之內容進行修正及重新定義；2023 年推出第三版，內容包含與健康及醫療領域之敏感個資處理相關之要求。依據指引，資料銀行係指於個人有效參與（可控性）下，有效促進個人資料分配及利用之系統，其廣泛採用將有望為公眾帶來便利生活。資料銀行為符合國家標準之可信賴實體，管理其委託人（利用者個人）之個資，並於個人同意之範圍內將資料提供與第三方[146]。該制度是建立於日本個人情保保護法中有效同意之基礎上，由個人與資料銀行簽訂委託契約，明示其業務內容、資料銀行之義務等

[145] 総務省，「情報信託機能の認定に係る指針 Ver3.0」の概要について，https://www.mhlw.go.jp/content/10904750/001168027.pdf，last visited 2025/2/14.

[146] 総務省，情報銀行の取組，https://www.soumu.go.jp/main_content/000791752.pdf，last visited 2025/2/14.



本報告之智慧財產權歸屬於國發會

相關資訊。並且資料銀行須定期向包含外部專家在內之資料倫理審查委員會就契約內容、資料利用狀況進行報告，審查委員會亦會於必要時對相關部門進行調查。

依據修正前之指引，處理個人敏感資料之企業不得被認證為資料銀行，惟鑑於健康及醫療領域為個人及社會利益而利用敏感個人資料之需求較高，因此就處理相關資料之業者進行認證，透過包含由健康及醫療領域專家所成立之敏感個人資料工作組之討論，就敏感個人資料進行定義並限制其利用範圍。本次修正透過認證特定資料庫促進資料之安全及分配利用，使利用人得使用符合自身情況之安全醫療保健服務。

A. 利用目的限制

於提供敏感個人資料予第三方時，必須對利用者有「明確之利益」，並且無任何不利風險；當將資料用於利用者個人以外之目的時，其他人之利用必須符合公益目的。

B. 敏感個人資料之範圍

該些資料之範圍為個人健康紀錄(Personal Health Revord, PHR)指引中所訂之健康紀錄，包含接預防接種、健康診斷及用藥資訊等，為用戶得充分理解之醫療資訊；而資料是否為資料銀行得處理之範圍將於資料倫理審查委員會進行討論。

C. 醫療專業人士之參與

於認證資料或進行更新時，資料之蒐集及提供須有醫療專業人士參與；鼓勵利用人於提供資料予資料



本報告之智慧財產權歸屬於國發會

銀行時向其保健醫生等專業人士尋求建議，以做出準確判斷。

D. 安全管理措施

除本指引外，亦須遵守其他醫療資料取得相關之規範。

2. 日本國家戰略特區

(1) 超級城市及數位田園健康特區[147]

日本自 2022 年起推動「超級城市」（スーパーシティ）以及「數位田園健康特區」（デジタル田園健康特区），並指定特定城市為施行地區。超級城市係透過促進數位技術之監管及運用及相關制度改革推動各項服務，以實現未來社會，並解決地區上各領域與日常生活相關之問題。目標於 2030 年前後實現居民參與及居民角度出發之未來社會，重點內容包含：於日常生活相關領域提供數位服務，利用 AI 及大數據等新興技術提高行政效率、交通、醫療及教育等領域之便利性；各領域間之資料流通，將透過「資料協同平臺」（データ連携基盤）連結並共用各類資料；推動同步、整體且全面落實先進政策所需之制度改革。數位田園健康特區為因應日本人口少子化及高齡化所設，聚焦於利用數位技術解決健康及醫療問題，該計畫由大學、醫療機構以及相關數位產業共同合作，透過制度及數位技術之運用解決地區所面臨之醫療健康領域問題。

[147] 内閣府国家戦略特区，スーパーシティ・デジタル田園健康特区，https://www.chisou.go.jp/tiiki/kokusentoc/supercity/openlabo/supercitycontents.html#jump，last visited 2025/2/14.



本報告之智慧財產權歸屬於國發會

資料協同平臺之資料活用為推動超級城市及田園健康特區之核心基礎，於超級城市而言，該平臺將蒐集、整理、提供政府、民間企業等資料持有者所提供之資料於交通、物流、醫療、防災等各領域提供服務；而對田園健康特區而言，將醫療院所、地方政府及民間服務等持有之健康資料（電子病歷、健康資料、活動資料等）標準化，以落實資料配合運用。為保障資料安全及通用，資料協同平臺之資料將經內閣府調查及審查確保所處理資料之安全性及準確性之措施，包含如資料匿名化及符合個資法之相關資料安全及隱私之措施，以便以安全可靠之方式連結各類資料。

## (五)英國

### 1. 資料共享法規

#### (1) 資料共享協議

英國資料委員會(Information Commissioner's Office, ICO)於資料共享方面訂有資料共享守則[148](Data Sharing Code)，為英國資料保護法(Data Protection Act 2018)下之規範，提供公私部門於合法情形下公平且合理共享其所持有個人資料之依據。依規定，當組織考慮共享資料時，需遵守資料保護相關法規，ICO 亦建議須於共享前進行隱私影響評估(Data Protection Impact Assessment, DPIA)，並且簽訂資料共享協定為佳。該法所涉及共用之資料為資料控制

[148] Information Commissioner's Office, Data Sharing Code, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/executive-summary/, last visited 2025/2/13.



本報告之智慧財產權歸屬於國發會

者間之個人資料共享，於個人資料共享過程中之程序皆須符合英國 GDPR 之規定，該資料共享須為不同組織間之資料共享，若是組織內部之資料流通則不屬於此規定下之資料共享。資料控制者間亦得以資料池(Data pooling)之方式共享資料，以用於特定目的，惟須確立其為獨立控制者或聯合控制者，若為聯合控制者則須依據英國 GDPR 簽訂相關契約明示各控制者之角色及責任。

資料控制者及接收者間得選擇透過簽訂資料共享協議以確保雙方之責任歸屬，任何形式之協定或合約皆可做為資料共享協議，惟備忘錄、清單或採購協定不得作為資料共享協議。資料共享協議中將明確說明雙方之角色、資料共享之目的、參與資料共享之組織（包含 DPO）、共享之資料內容、法律依據、資料於其生命週期之狀況及資料治理之相關安排。

2. 沙盒機制

(1) ICO 監管沙盒

ICO 於 2019 年建立沙盒計畫[149](ICO Sandbox)，提供以安全且創新方式開發個人資料產品及服務之組織，得於安全可控且不排除資料保護法規之開發環境下，透過提供關於降低風險及資料保護始於設計(data protection by design)之專業知識及建議以降低法遵風險。有意參與之業者得向 ICO 提出申請，由 ICO 審查及邀請與其目前所關注議題相符，且產品能為公眾提供潛在明顯利益之組織參與。組織參與沙盒計畫得獲得多重優勢，包含 ICO 之專業

[149] Information Commissioner's office, ICO Sandbox, https://ico.org.uk/sandbox, last visited 2025/2/13.



本報告之智慧財產權歸屬於國發會

知識及協助、得增強其對自身產品之信心、更加了解資料保護框架及其對組織業務之影響、了解積極主動之資料保護方式，以提高消費者對產品服務之信賴、為 ICO 之未來指引提供資訊並為開發符合公益之產品做出貢獻。沙盒之最長時間為 12 個月，將依據申請組織之需求及其內部時程而定。

組織向 ICO 申請加入沙盒後將會收到 ICO 所制定之沙盒計畫，當中可能包含分階段之指導、對產品或測試之非正式監督、對文件之審查包含 DPIA、隱私聲明及資料共享協議及對設計風險降低之指導等。ICO 目前關注之重點為新興技術領域議題，ICO 監管沙盒協助組織就利用新興技術進行創新並防止其餘過程中對個人資料隱私造成侵害。沙盒過程中之經驗除可提供 ICO 發展新興技術之新觀點外亦得於最終減輕企業之負擔。新興科技領域下議題包含物聯網(IoT)及個人化 AI(Personalisaed AI)等。

(六)澳洲

1. 資料共享法規

(1) 政府資料共享

自 2022 年「澳洲資料可用性及透明度法」（Data Availability and Transparency Act 2020）通過後，所有組織皆可透過資料位置(Dataplace)要求澳洲政府資料[150]。政府之開放資料皆由 data.gov.au 免費提供，所提供之資料包含澳洲、州及地方政府機構之資料庫、公共資助之研究資料

[150] Office of the National Data Commissioner, Share Data, https://www.datacommissioner.gov.au/share-data, last visited 2025/2/13.



本報告之智慧財產權歸屬於國發會

及符合公共利益私營機構之資料。該法案規定資料僅得於「提供政府服務」、「通知政府政策及計畫」及「研究開發」相關目的時共享，且不得於涉及國家安全或執法相關目的時共享。

(2) 消費者跨域資料共享

2019 年澳洲財政修正法案[151] (Treasury Laws Amendment (Consumer Data Right) Act 2019)增訂消費者資料權(Consumer Data Right, CDR)於競爭及消費者法(Competition and Consumer Act 2010)，為聯邦層級之法律。

依據該法第 AA 款，CDR 賦予指定行業之消費者資料自主權，消費者得要求其個資於指定行業領域被安全、有效且便利地揭露予消費者或適格者(Accredited person)。CDR 並非強制權利，消費者資料權為一選擇權(opt-in)，消費者得選擇是否同意將資料共享，並能全面了解資料共享之對象以及目的。依據該條第 AC 款規定，澳洲財政部得指定相關部門針對 CDR 制定具體規定，而與「澳洲競爭與消費委員會」(Australian Competition and Consumer Commission, ACCC)及「澳洲資訊委員公署」(Office of the Australian Information Commission, OAIC)共同合作執行 CDR 相關政策及制度。

依據《競爭消費者規則 2020》(Competition and Consumer (Consumer Data Right) rules 2020)規定，請求消費者資料之方式分為「商品請求資料」、「CDR 消費者請求其消費者資料」及「消費者請求授權他人請求消費者資料」

[151] Treasury Laws Amendment (Consumer Data Right) Act 2019, https://www.legislation.gov.au/C2019A00063/asmade/text, last visited 2025/2/12.



本報告之智慧財產權歸屬於國發會

三種。消費者資料權行使僅限於消費者同意，且以機器可讀形式進行，資料控管者不得對資料使用附加任何條件之限制。此外，依據《消費者資料權認證指引》(Consumer Data Right accreditation guidelines)規定，僅有經過 ACCC 認證過之業者得利用消費者資料提供服務或產品。目前 CDR 多用於銀行以及能源產業，非銀行業貸款將作為第三個開放之領域。消費者得選擇與經認證之資料接收業者共享其銀行或能源資料（如交易紀錄、利率或用電量等），CDR 能使消費者於產品比較及選擇上更加便利[152]。CDR 之運作方式係由消費者透過 APP 或網站給予同意，允許供應商得存取其個人資料或業務相關資料，並經過身分驗證後與供應商之網站產生連結，並且消費者得隨時查看資料及撤銷其同意。

(七)紐西蘭

1. 資料共享協議

紐西蘭之資料共享是以協議方式進行，依據其數位發展部門(Digital Government)建議，資料共享協議為用於紀錄資料共享活動之協定，內容包含確保機構共享資料之原因、內容及方式；確保各機構了解其責任及義務；說明各機構對資訊共享採取隱私始於設計方法，並確實考量資料共用之目的及

[152] Australia Government, Consumer Data Right, https://www.cdr.gov.au/, last visited 2025/2/13.



本報告之智慧財產權歸屬於國發會

實現目的所需之個人資料；提高透明度，建立民眾對機構共享個人資料方式之信任並定期安排審查[153]。

資料共享協議有「資料共享協定(information sharing agreement)」、「經批准之資料共享協定(AISA)」及「資料媒合協定(information matching agreement)」三種主要類型，機構於前述協議外亦可能簽訂關係協議以規定機構間同意合作之方式。其中 AISA 為紐西蘭《隱私法》(Privacy Act)下之資料共享規定，為受隱私專員批准以提供公共服務之資料共享協議[154]。AISA 多為政府部門間之資料共享，由隱私專員批准後公布於隱私委員會(Privacy Commissioner)之網站。

## 二、 結論

綜上，觀察主要國家對於促進資料共享之作法，可以發現多數國家或國際組織（除美國外）基本上資料流通應用之策略，若涉及個人資料，皆係以保障個人資料與隱私為根本，再進行機制面之規劃或特別法之建構。以歐盟為例，GDPR 作為整體資料戰略相關法制藍圖之基礎規範，後續規範之資料治理法、資料法甚至針對醫療空間之規則，皆是以個資法為基礎再延伸進行規定。相關規範原則上僅少打破 GDPR 對個人權利已建構之保障，而係就所涉及之資料與推動目的，進一步強化流通機制、權利要素、規格、標準等要求。例如 EHDS 建立之選擇退出權、資訊限制權利、敏感資料控管措施等各項特別規範。澳洲則較為特別，於保障個人資料自主之前提下，進一步規範消費者

[153] DIGITAL. GOVT.NZ, Information sharing agreements, https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/information-sharing/information-sharing-agreement/types-of-information, last visited 2025/2/13.

[154] Privacy Commissioner, Approved Information Sharing Agreements, https://www.privacy.org.nz/privacy-act-2020/information-sharing/approved-information-sharing-agreements/, last visited 2025/2/13.



本報告之智慧財產權歸屬於國發會

資料權，讓消費者透過同意方式願意提供資料於指定產業領域共享，亦是以保護個人資料為基礎再變化之資料流通促進規範。

然而對於技術開發過程之資料應用，則亦有相關措施予以搭配，例如各有特色之沙盒機制或規定。例如歐盟 AIA 法案，特規定 AI 監管沙盒，使 AI 研發過程之風險得以集中於特定實驗場域，並對於監管沙盒當中所合法蒐集之個人資料，得於符合規定條件之情況下用於開發、訓練及測試 AI 系統，以平衡 AI 開發資料運用之需求，以及對個人資料之保護。英國 ICO 也建立沙盒計畫機制，協助產業於產品服務之開發，降低法律遵循之風險。日本則是透過特區之機制進行服務與技術落地之評估，並以資料協同平臺機制促進各領域間之資料流通。紐西蘭則推動資料共享協議機制，促進資料跨域應用，而共享協議之批准則需以符合隱私法為前提。此外，韓國 2026 年 1 月施行之 AI 基本法，則規定須建立促進資料應用之 AI 集中園區，以及 AI 開法與應用資料中心，其運作尚待觀察。足見除特別法制建構外，透過配套之沙盒機制、資料中心、資料平臺或合法之共享協議等機制推動資料流通，亦為廣受認可之作法。



本報告之智慧財產權歸屬於國發會

# 參、 國際 AI 運用與著作權刑罰或處罰規範趨勢研析

## 一、 國際趨勢發展

基於保護著作權人為目的，各國著作權皆有不同程度之責任規範（含民、刑事或行政責任規範）。然隨著 AI 之快速發展，大量訓練資料取得之需求，以及訓練成果之權利等問題，與各國現行著作權保護法制皆產生程度不等之衝突。其中包括無法取得訓練資料之著作權授權，或因不確定所需訓練資料之著作權的權利狀態而產生侵害著作權之情形，或對於 AI 產出結果是否構成著作權侵權無法評判等問題。觀察近期國際法制趨勢，國際上針對 AI 運用而衍生之著作權侵權，是否對應之刑罰或行政罰的調整或鬆綁，大致整理如下：

### (一)歐盟：AIA 針對運用 AI 之著作權侵害，設有高額之行政罰鍰

2024 年 8 月，歐盟通過 AIA 法案，其表明尊重歐盟各國國內著作權法之責任規範，並針對 AI 訓練資料規範相關義務及罰則。要求「通用 AI 模型提供者」(GPAI 模型提供者）之訓練內容應公開透明，並依據該法第 101 條規範，若 GPAI 模型提供者故意或過失違反著作權義務，則可處以不超過上一財政年度全球營業額 3%或 1500 萬歐元之罰鍰。故歐盟 AIA 針對著作權侵權，於 GPAI 層面設有高額行政罰鍰，其他著作侵權責任則依據各國國內著作權法處理，近期並未觀測到歐盟成員國針對 AI 相關事宜修訂著作權法。值得注意的是英國智慧財權局於 2024 年 12 月針對著作權及 AI 議題公開徵詢意見，針對是否修訂著作權法或加強保護、是否建立廣泛資料探勘例外規定、是否採用允許權利人保留並支持以透明度為基礎之資料探勘例外規定等議題進行公眾意見徵詢，後續是否有進一步發展則可持續關注。

### (二)日本：雖修正著作權法放寬 AI 訓練資料運用之限制，但仍不得「不正當損害著作權人之利益」，並仍需承擔侵權責任



本報告之智慧財產權歸屬於國發會

為提高機器學習之資料取得與利用之便利性，日本於 2018 年修正其著作權法，於第 30 條之 4 規定在下列情況下，若著作利用之目的並非為自己或他人感受作品中表達的想法或感情，於依據作品之種類、目的和使用方式，不會不當損害著作權人利益的情況下，可於必要範圍內以任何方法應用該作品：1.用於測試與錄音、錄影或其他著作權作品使用相關的技術的開發或實際應用；2.資訊分析，即從大量作品等大量資訊中提取構成訊息的語言、聲音、圖像等要素相關的資訊，並進行比較、分類等分析。依據該修正，當時日本著作權法修正對於 AI 訓練資料採取較為寬鬆之規範，但仍附帶條件以不損害著作權人之利益為優先。2024 年 4 月日本文化廳文化審議會著作權分科會法制小組提出之「關於 AI 與著作權之思考」，說明即使為無須授權之資料訓練仍然不得「不正當損害著作權人利益」，例如出於資訊分析（AI 學習）等目的，從出售的資訊分析資料庫複製著作權作品或 AI 開發者或 AI 服務提供者明知或可得而知蒐集包含盜版或其他侵權之作品複本者，仍應負著作權法相關之侵權責任。故以日本而言雖有部分放寬資料訓練，但若面臨侵害現有著作權人之權益上，仍有可能面臨賠償或刑罰處罰等，處罰規範並未有所放寬。

(三)美國：部分州提出運用 AI 之管制措施，雖與著作權相關但並非從著作權法保護之角度提出，其著作權局亦無修法之規劃

美國近年由於深偽等 AI 之利用已造成民眾困擾及眾多社會問題，田納西州於 2024 年 3 月提出「確保肖像、聲音、圖像安全法案」，要求第三方若利用生成工具重製肖像、圖像、聲音須取得授權之規範。該法為美國首部禁止他人未經授權使用或重製權利人之聲音以提供訓練 AI 模型或採用深偽技術之州法。然該法雖部分與著作內容使用相關，但並非從聯邦著作權法角度進行之規範調整，而係個別州法層級之區域性保護。



本報告之智慧財產權歸屬於國發會

面對 AI 開發、部署及運用過程相關作為，與著作權保護規範適用之衝突日益加劇，美國著作權局雖尚無修正著作權法，但針對 AI 系統引發的一系列著作權法和政策問題發佈意見徵集，並於 2024 年至 2025 年分別發佈 3 份「著作權與 AI」主題性報告，分別為：2024 年 7 月發佈之第 1 份「著作權與 AI 分析 AI 引發的著作權法及政策議題」、2025 年 1 月發佈之第 2 份「關於 AI 輔助及生成作品之著作可保護性(copyrightability)」及 2025 年 5 月剛發佈之「關於生成式 AI 之訓練」。其中第 1 份報告美國著作權局認為形象或聲音的複製在美國各州的法律存在不一致和不足之處，不同的管轄要求導致對於誰可以尋求救濟產生差異，結果是形成一種保護拼湊的局面，救濟措施的可用性取決於受影響個體之居住地或未經授權使用之發生地，因此應該於聯邦層級建立法律規範。而第 2 份報告則認為現行法令已可解釋，無須擴充對 AI 作品成果著作權保護另訂規範，對於部分使用 AI 組合而成之作品，仍應逐案分析，確定人類於作品之貢獻程度。而近期所發布之第 3 份報告則對於訓練內容是否可以形成合理使用及使用多少比例才算合理使用等作出了較為保守之判斷，此與現行川普政府之政策相左，故後續美國將在開放與保護之間如何選擇尚待後續觀測。但就目前趨勢來看，美國著作權局之報告並無修正現行著作權法之趨勢，故針對運用 AI 所產生之侵權仍適用現行法令規範。

## 二、 結論

以目前國際趨勢來看，各國皆無針對 AI 相關之著作運用，進行著作權法侵權處罰之相關規範修正或鬆綁。歐盟總體政策仍以保護著作權人之權益為優先，雖搭配有行政罰鍰之制度，但若涉及著作侵權等相關責任仍尊重各會員國國內著作權法所規定之相關罰則。而歐盟各國目前也尚無針對 AI 運用之相關著作權議題有刑罰或處罰上之鬆綁。日本與美國就 AI 策略而言較歐盟更具彈性，但針對權利保護部分，日本雖有對於資料探勘部分有法令面之鬆綁，但若涉及著作權益之侵害，



本報告之智慧財產權歸屬於國發會

仍回歸著作權之侵權責任，並對此部分有所修正或鬆綁。美國則較為特殊，雖有部分州法提出對於特定內容之嚴格保護，但聯邦層級之主管機關著作權局仍尚在蒐集意見階段，雖聯邦政府政策趨於希望開放資料運用而淡化著作權之保護，但目前尚未有明確之法令鬆綁之跡象。故以現國際趨勢而言，並無觀測到對於 AI 相關運用之著作權侵權有刑罰或處罰上之鬆綁規範之發展。

## 肆、 Cookie 之監督管理國際規範研析

### 一、 前言

隨著數位科技及網際網路之快速發展，為追蹤網站使用者之瀏覽活動及偏好資訊，並提升使用者對網站之體驗，於 1994 年開始由網景瀏覽器開發者將此一技術與瀏覽器技術融合，至此成為網路服務蒐集與分析使用者行為之重要資料來源。尤其第三方 cookies 的應用，更是數位廣告得以分析追蹤網路跨網站行為之源頭，然而基於 cookies 追蹤引發過度追蹤使用者行為之隱私問題，Google 曾經一度宣布不再使用第三方 cookies 技術，然而，於 2024 年 7 月[155]與 2025 年 4 月兩度宣布放棄屏除第三方 cookies 之政策，將維持其 Chrome 瀏覽器處理 cookies 之模式，交由瀏覽器使用者自行進行隱私與安全設定，決定是否封鎖第三方 cookies[156]。

從技術層面而言，cookies 是網站儲存在使用者之瀏覽器或特定網路服務中之小段文件資料，用以記錄使用者之登錄資訊、追蹤使用者瀏覽行為、偏好設定等，進而建構使用者資料檔案之工具，並優化使

[155] Reuters, Google scraps plan to remove cookies from Chrome, July 23, 2024, https://www.reuters.com/technology/google-scraps-plan-remove-cookies-chrome-2024-07-22/ , last visited 2025/9/3

[156] 陳曉莉，Google 宣布將保留 Chrome 中的第三方 Cookie，iThome, 2025/04/23, https://www.ithome.com.tw/news/168554, 最後瀏覽日：2025 年 9 月 3 日



本報告之智慧財產權歸屬於國發會

用者體驗。cookies 有不同之類型及用途，基本上可從來源、存續時間及使用目的進行區隔。來源類包括第一方 cookies 及第三方 cookies，前者為使用者直接瀏覽之網頁所置入，後者則非出於使用者直接瀏覽之網站所發出，而係由第三方(廣告或相關分析系統)所發布，網路使用者較難察覺，風險較第一方 cookies 為高。以存續期間來看，分為僅於網站瀏覽時存在，關閉即取消的短暫對話型 cookie，以及持續長期存在於使用者之硬體設備中，須待使用者刪除或超過該 cookies 效期方會刪除，後者之個人資料保護風險亦較高。而按使用目的區隔，基本必要之 cookies 為網站服務所必須，若缺乏該功能即無法行使相關之服務；其餘尚有效能 cookies、功能性 cookies、營銷性 cookies 等非必要性 cookies[157]則分別用於紀錄使用者之行為、進行統計分析、追蹤及與廣告商或第三方分享資訊等。

由於 cookies 主要在紀錄使用者之網路瀏覽等活動，故可輕易地針對特定使用者之行為進行比對分析，了解特定使用者之行為特質，進而加以利用(例如投放目標性廣告)，而當事人未必處於有認知之狀態，從而引發諸多關於個人資料隱私保護之疑慮，亦有相當多的國家或國際組織就 cookies 監管事宜，有相當之討論或規範建構。

國際上針對 cookie 之監管各國規範不一。歐盟及其成員國早期即透過電子隱私指令(ePrivacy Directive, ePD)初步提出對 cookies 規制之看法，近年則搭配 GDPR 之規範，普遍採較為嚴格之監管，然於實務操作層面不乏出現爭議，成員國間之作法與解釋亦不盡相同。美國則無全國統一之個人資料保護法，故係各州自行制定法律規範，對於 cookies 是否直接視為個人資料予以保護亦有不同看法。故本研析將蒐

[157] 郭戎晉，「從個人資料保護立法談 cookie 之定位、應用爭議與規範課題」，東吳法學學報第 32 卷第 1 期，2020/07，頁 72-74。



本報告之智慧財產權歸屬於國發會

集整理重點國家 cookies 之立法模式、規範重點及主管機關等監管模式資訊，供我國政策評估參酌。

## 二、 國際趨勢重點

### (一)主要國家/國際組織規範重點

#### 1. 歐盟

##### (1) 歐盟一般資料保護規則(GDPR)

GDPR 於 2018 年 5 月生效後，已取代原先 95 年資料保護指令(Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data，下簡稱 95 年指令)。部分 95 指令的原則或要件於 GDPR 被保留下來，期中包括以當事人之事前同意為資料處理合法性要件之一(第 6 條第 1 項(a)款)，以及對於同意之定義及概念，必須是當事人基於其意思，透過聲明或明確肯定之行動，所為自主性、具體、知情及明確之表示同意處理個人資料(第 4 條(11)款)，而依據前言第 32 點之說明，單純沉默、預設選項為同意或不為表示，皆不構成 GDPR 認定當事人同意之要件。

然 GDPR 並未認為只要是 cookies 所蒐集之資料當然為個人資料。依據 GDPR 前言第 30 點之說明，「透過設備、應用程式、工具及通訊協定，諸如網際網路協定位址、瀏覽歷程記錄識別碼(cookie identifiers)或其他識別工具，諸如無線射頻識別系統標籤，當事人可被連結到網路上識別碼。此可能留下軌跡，並可被用於對當事人建檔並識別其身分，特別是當該軌跡結合了唯一的識別碼及從服務商



本報告之智慧財產權歸屬於國發會

取得其他資料[158]。」。而依據 GDPR 第 4 條(1) [159]「關於個人資料之定義係指有關識別或可得識別當事人之任何資訊；可得識別係指得以直接或間接地識別該自然人，特別是參考諸如姓名、身分證統一編號、位置資料、網路識別碼(online identifier)或一個或多個該自然人之身體、生理、基因、心理、經濟、文化或社會認同等具體因素之識別工具。」故 GDPR 認為 cookie 是一種可能用以識別特定個人之工具之一，但其所蒐集之資料仍須滿足可識別到特定當事人之程度才屬於個資保護之範疇。若 cookies 軌跡與個人之唯一識別碼進行結合後之資料係可識別當事人身分，則該結合資料也應視為個人資料予以保護。

經上述原則判斷若 cookies 所進行之資料蒐用符合 GDPR 所定義之個人資料，則資料處理上必須符合 GDPR 第 6 條所規範之合法處理要件之一，包括當事人同意、當事人履行契約所必要、資料控管者為遵守法律義務之必要等。實務上，最常被運用之要件為經當事人同意，此處之同意則必須依循上開同意認定之原則。

除了同意外，撤回同意亦係 GDPR 之重要規定。依據 GDPR 第 7 條第 3 項規定當事人有權隨時撤回其同意。同意之撤回並不影響撤回前基於該同意所為處理之合法性。故當事人為同意前，亦應被告知其得隨時撤回該同意，且同意之撤回應與給予同意一樣容易。故當事人即便已同意 cookies 之資料蒐集，依據上開規定，則應可撤回其同意。

---

[158] 歐盟個人資料保護規則前言部分(Recitals) 翻譯，https://www.pdpc.gov.tw/CP/55/，個人資料保護委員會籌備處，最後瀏覽日 2025/9/1。

[159] 歐盟個人資料保護規則本文部分翻譯，https://www.pdpc.gov.tw/CP/55/，個人資料保護委員會籌備處，最後瀏覽日 2025/9/1。



本報告之智慧財產權歸屬於國發會

(2) 電子隱私指令(ePD)

隨著網路時代之興起，歐盟於 2002 年通過歐盟 ePD，期間伴隨數位網路環境高度變動，由其 cookies 逐漸被廣泛應用所引發之個人資料保護疑慮，歷經多次修訂，於 2009 年確立對 cookie 的主要規範原則，即於第 5 條第 3 項[160]要求會員國必須確保只有在已獲得訂閱者或使用者之事前同意，並使其獲得與處理目的相關之清晰、全面之資訊的前提下，才得允許於訂閱者或使用者之終端設備上儲存資料，或近用已儲存之資料[161]。

然而由於並未明確說明可被認定為事先取得同意之作法或型態。部分網路服務提供者，乃透過預選 cookies 之操作或 cookies 牆等手段強迫使用者同意，實際上仍常發生未經使用者同意而置入之 cookies，或使用者被迫「同意」才可使用網站等狀況，並非真正讓使用者自主同意，而造成實務監管上之混亂。故 2017 年歐盟提出電子隱私規則(ePrivacy Regulation, ePR)草案，希望可因應當時之科技發展更新指令內容，並借由調整為「規則」(regulation)之性質，統一會員國國內法之標準。然而由於會員國並未達成一致意見，最終未能通過，並於 2025 年正式撤回[162]。

(3) 關於 ePD 與 GDPR 間之相互作用

2018 年 12 月比利時資料保護主管機關要求歐洲資料保護委員會(European Data Protection Board, EDPB)就 ePD

[160] Directive 2002/58/EC of the European Parliament and of the Council, Directive - 2002/58 - EN - eprivacy directive - EUR-Lex, last visited 2025/9/1.

[161] 同註腳 157，頁 79。

[162] 同註腳 157, 頁 79-81。



本報告之智慧財產權歸屬於國發會

與 GDPR 間之相互作用發表意見。主要問題包括資料保護機關基於職權可處理之事務範圍，包括一事件同時觸發兩法之實質適用範圍等問題，請 EDPB 予以釐清。故 EDPB 於 2019 年 3 月提出「關於電子隱私指令與一般資料保護規範相互作用之意見，特別關於資料保護機關之職權、任務及權力」(Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities[163]，以下簡稱 EDPB 指引)。

EDPB 認為兩者之間為特別法與一般法之關係。GDPR 前言第 173 點明確指出「本規則應適用於所有涉及保護個人資料處理之基本權及自由之事件，且不限於歐洲議會及歐盟理事會之歐盟指令第 2002/58/EC 號為同樣目的所規定之特定義務，包括控管者之義務及當事人之權利。為釐清本規則與歐盟指令第 2002/58/EC 號之關係，該指令應依本規則修訂。一旦通過本規則，歐盟指令第 2002/58/EC 號應受檢討，尤其是為確保與本規則之一致性[164]。」故 ePD 在 GDPR 通過後須進行法令檢視，若涉及個人資料保護之事項則應以符合 GDPR 之基本原則為前提。然而，EDPB 指引於第 29 點指出，有許多實務操作可能同時觸發 ePD 及 GDPR 之適用，cookie 之使用即為事例。GDPR 第 95 條規定「關於其等應遵守歐盟指令第 2002/58/EC 號之事項，本規則不得對自然人或法人施加與在歐盟公共通信網絡中提供公共電子通信服務有關之額

[163] Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, https://www.edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf ,last visited 2025/9/2.

[164] 同註腳 158,頁 112。



本報告之智慧財產權歸屬於國發會

外義務[165]。」即若自然人或法人在歐盟公共通訊網路中提供公開可用之電子通訊服務已適用 ePD 時，則優先適用 ePD 之相關規範。

依據 GDPR 之規定，會員國必須指定一個或多個監管機關。然而現實狀況下，由於 ePD 為早於 GDPR 之規範，故可能已有會員國指定資料主管機關執行 ePD 之監管，或係選擇其他機關例如國家電信監管機關(national telecommunications regulatory authority, NRA)、消費者保護機關、或其他適合之機關作為 ePD 權責機關[166]。例如，德國透過「電信及數位資料保護及隱私權保護法」[167](Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz - TDDDG)落實 ePD，其主管機關依據第 29 及 30 條規定，若為與個人資料保護相關係以德國聯邦資料保護與資訊自由委員會(Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, BfDI)作為監管機關；而若為與電信媒體相關之內容則為聯邦網路局(Bundesnetzagentur)之職權範圍。又如瑞典電子通信法(Swedish Electronic Communications Act[168])第 9 章第 28 條規定放置 Cookies 及非消費者明確請求所必須之類似技術，須事先獲得消費者同意。而 GDPR 並未限制不能指定與執行 ePD 相同之權責機關作為監督機關，故會員國得以指定同一資料保護主管機關同時作為 ePD 及 GDPR 之權責機關。惟若確實如

---

[165] 同註腳 159,頁 185。

[166] 同註腳 163, No.63,頁 19。

[167]Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG), https://www.gesetze-im-internet.de/ttdsg/BJNR198210021.html#BJNR198210021BJNG000100000 , last visited 2025/9/1.

[168]Swedish Electronic Communications Act https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2022482-om-elektronisk-kommunikation_sfs-2022-482/#K10, last visited 2025/9/1.

此，則該機關實際行使職權時必須明確區分係依據哪一個規定的授權，不得僅以 GDPR 之執法依據執行基於 ePD 授予之職權[169]。

2. 英國

(1) 隱私暨電子通訊規則 (Privacy and Electronic Communications Regulations, PECR)

英國原屬於歐盟會員國，故承襲歐盟模式，同樣就 cookie 監管層面，依循 ePD 之規定，將之具體化納入內國法 PECR，並作為特別法若涉及 PECR 已有規範之事項則優先於 UKGDPR 適用，且對應英國 2025 年的資料（利用與近用）法（Data (Use and Access) Act，簡稱 DUAA）修訂，已進行調修，部分條文尚待生效。UK GDPR 及 PECR 之主管機關，皆設定為資訊專員辦公室 (Information Commissioner's Office, ICO)。

依據原 PECR 第 6 條第 4 項規定，關於該條第 1 項禁止任何人存取儲存於訂閱戶或使用者終端設備中資訊，以及必須符合第 2 項提供清晰、全資訊後事先取得當事人同意之要求，不適用於為了執行 ePD 之要求或係訂閱戶或使用者利用該資訊社會服務所必要之資料近用。也就是說，絕對必要之 cookies 例外無須取得當事人之事前同意即可蒐集。

為使 cookies 利用應遵循規範之要求明確化，ICO 於 2019 年發布「cookie 使用及相似技術指引」(Guidance on

[169] 同註腳 163, No.66,頁 20。



本報告之智慧財產權歸屬於國發會

the rules on use of cookies and similar technologies[170])。更明確強調 cookies 蒐集禁止及事前同意之例外，只限於必要 cookies 才可不經當事人事前同意而存取，其判斷原則為必要且不可或缺(essential)之程度，包括網站購物之購物車功能、與銀行往來之安全性活動等。此外，針對 cookies 同意之有效性認定，指引提出必須符合一定要求才可算有效之同意，包括用戶必須明確且積極地表達對非必要 cookie 之同意、網站必須明確說明所使用之 cookies 的功能、若使用第三方 cookies 必須解釋將如何使用所蒐集之資料、若為非必要 cookies 不可使用任何已預設之勾選框等。此外，必須提供用戶對任何非必要 cookies 之控制及拒絕的機會，並確保其拒絕非必要 cookies 後仍得以正常使用網站功能[171]。

(2) 資料使用及存取法(DUAA)

值得注意的是，英國於 2025 年 6 月通過 DUAA，針對 cookies 之同意規則有了變化。就上開資料存取限制之例外，DUAA 新增 5 種另外情形[172]：

A. 通訊例外：僅用於傳輸通訊，例如指紋辨識技術僅用於網路管理目的。

B. 絕對必要例外：為提供訂閱或使用用戶請求之服務所須之絕對必要資料。包括確保終端設備安全、防止或

[170] ICO, Guidance on the use of cookies and similar technologies, guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf, P14, last visited 2025/9/2.

[171] Id, at 11.

[172] ICO, New Guidance on the use of storage and access technologies _ What are the exceptions? https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-on-the-use-of-storage-and-access-technologies/what-are-the-exceptions/, last visited 2025/9/2.



本報告之智慧財產權歸屬於國發會

發現詐欺、防止或檢測技術故障、驗證訂閱戶或使用者、紀錄使用者於線上服務之選擇。

C. 統計目的/分析例外：僅用於蒐集就服務訪問之統計資訊以改善服務。

D. 外觀例外：僅用於改進或調整服務之外觀或功能，使其符合訂閱戶或使用者之偏好。

E. 緊急援助例外：僅用於識別需要緊急援助之訂閱戶或使用者位置。

DUAA 放寬了原 PECR 針對 cookie 限制例外之範圍，從原本嚴格必要之 cookie 新增 4 種例外情形，使得更多類型之 cookie 及技術可以無需經過當事人事前同意即可被使用。此外，DUAA 對於 cookie 之定義不僅涵蓋傳統之 cookie，還包含了指紋技術、串流內容追蹤、社群媒體追蹤等存取技術，顯示英國現階段對於數位存取技術範圍之擴大認定。

3. 美國

(1) 加州

加州與 Cookies 相關之規範係規定於加州消費者隱私法[173](California Consumer Privacy Act 2018, CCPA)中，並以加州隱私保護局( California Privacy Protection Agency, CPPA )為主管機關。CCPA 第 1798.140(v)項規定，CCPA 所規範之個人資料，是能夠識別、關聯、描述特定消費者

[173] California Consumer Privacy Act of 2018 (CCPA) https://cppa.ca.gov/regulations/pdf/ccpa_statute.pdf.



本報告之智慧財產權歸屬於國發會

或家庭，或能夠合理的直接或間接關聯特地消費者或家庭的資料，並於同項(A)款，將唯一識別標誌(unique identifier)列舉為識別標誌（identifier）之事例，屬於 CCPA 所定義之個人資料範圍。同條(aj)項進一步定義何謂「唯一識別標誌」或「唯一個人識別標誌」（unique personal identifier），係指可用以識別消費者、家庭或消費者或連結至消費者或家庭之設備的永久識別碼，該識別碼會隨時間變化橫跨不同服務使用，包括但不限於裝置識別碼、網際網路協定位址（Internet Protocol address）、cookies、信標（beacons）、像素標籤（pixel tags）…等類似技術。綜上 cookies 屬於 CCPA 定義下之唯一識別標誌，屬於該法規範之個人資料範圍。

加州 CCPA 規範下，cookie 作為唯一識別標誌而屬於該法所規範之個人資料範疇，故資料控制者必須以符合 CCPA 對個人資料蒐集與利用相關要求之方式使用 cookies，包含揭露有無使用 cookies 之使用，以及透過 cookies 所蒐集之個人資料類型、特定目的以及是否有進行銷售行為等[174]。CCPA 於 cookies 使用係採事後退出[175](opt-out)機制。資料控制者需給予消費者拒絕利用 cookie 蒐集、分享或銷售其個人資料之權利。依據 CCPA 第 1798.135 條(a)項，為使消費者得事後拒絕其個人資料被利用，資料控制者必須於主網頁提供「不銷售或分享我的個人資料」(Do Not Sell or Share My Personal Information)

[174] *Id,* 1798.100.

[175] *Id,* 1798.120.



本報告之智慧財產權歸屬於國發會

之選項，以利使用者可以選擇退出。此外，必須附上隱私權政策及 cookies 政策之單獨連結[176]。

除資料控制者之義務外，對消費者而言，則有權了解其被蒐集之資料類型、是否有出售其資料之行為，以及拒絕 cookies 之使用、售予第三方或要求刪除等權利[177]。

(2) 維吉尼亞州

維吉尼亞州之消費者資料保護法[178](The Virginia Consumer Data Protection Act, VCDPA)為維吉尼亞州與消費者個人資料保護相關之法規，與加州 CCPA 不同，維吉尼亞州並未設有特定主管機關，而是由總檢察長監督及執法。VCDPA 對個人資料之定義為任何與已識別或可合理識別個人相關或可合理連結至個人之資料。雖其並未如 CCPA 直接於法規中將 cookies 列舉出來，但依據其對個人資料之定義，若所採用之 cookies 能識別或連結至個人，亦屬 VCDPA 所規範之客體。VCDPA 與 CCPA 類似，亦是賦予消費者退出(opt-out)之權利，包括拒絕資料控制者以定向廣告、出售個人資料以及透過分析(profiling)作成重大決策為目的處理其個資之權利等，而 cookies 為可用於前述目的之資料，故資料控制者必須於消費者要求退出時停止利用[179]。此外，VCDPA 要求資料控制者處理個人資料需告知消費者其所蒐集之資料類型以及利用方式[180]，故

[176] *Id,* 1798.135.

[177] *Id,* 1798.115-1798.130.

[178] VCDPA, https://virginia-vcdpa.org/%c2%a7-59-1-577-personal-data-rights-consumers/

[179] *Id,* 59.1-577.

[180] *Id*, 59.1-578.



本報告之智慧財產權歸屬於國發會

使用 cookies 之業者亦須遵守規範將其蒐集之資料及利用方式告知消費者。

維吉尼亞州雖未將 cookies 明定於 VCDPA 中，但因該法對個人資料之定義較為寬鬆，因此 cookies 若能符合 VCDPA 個人資料之定義，如廣告追蹤 cookies 等可識別或合理連結至個人，則會被視為個資，屬於該法所管。VCDPA 中並未要求須取得當事人事前同意，而是賦予資料當事人事後退出之權利，換言之，資料控制者需提供資料當事人得拒絕利用 cookies 的機制或管道。

4. 日本

(1) 個人資料保護法

日本個人資料保護法（個人情報の保護に関する法律，下稱個情法）於 2020 年修法時納入「個人關聯資料」（個人関連情報）之概念，依據個情法第 2 條第 7 項，個人關聯資料係指「有關生存個人之資料，為該當個人資料、假名加工資料及匿名加工資料任何之一者。」依據個情法之主管機關個人情報保護委員會（簡稱 JPIPC）之說明[181]，若 cookie 等終端識別索引（端末識別子）不符合日本個情法定義之個人資料，則通常會被視為個人關聯資料，而若 cookies 等終端識別索引得輕易與其他資料進行比對後得識別個人，則該類 cookies 會屬於個人資料。故，cookies 是否屬於個人資料需視其是否得輕易透過與其他資料比

[181] JPPC, cookie 等の端末識別子は個人関連情報に該当しますか。家族等で情報端末を共用している場合はどうですか, https://www.ppc.go.jp/all_faq_index/faq1-q8-1/.



本報告之智慧財產權歸屬於國發會

對而識別個人，若屬於個人資料則須遵守個情法中對個人資料之規定。

雖個人關聯資料無法識別特定個人而非個情法規範之個人資料，惟其有可能於傳輸至第三方後，由第三方接收者透過與自身內部資料比對、組合後成為得識別特定個人之個人資料。因此，個情法第 31 條規定，「個人關聯資料處理事業，預見受提供之第三人，將個人關聯資料作為個資而取得時，對該第三人提供該資料一事，於未確認得到當事人同意前，不得對該第三人提供該個人關聯資料。」舉例而言，若持有屬關聯資料 cookies 之 A 公司欲將該 cookies 提供予 B 公司，A 公司若可預見 B 公司得以其內部資料與該 cookies 比對後識別特定個人，則必須於提供 cookies 前要求 B 公司取得資料當事人之同意。該條規定僅規範將 cookie 提供予第三方之情形，若企業僅於自身網站設置之 cookies 則非此條所欲規範之對象。

(2) 電氣通信事業法

日本於 2022 年修正，2023 年 6 月生效之《電氣通信事業法》（電気通信事業法）第 27 條之 12 規範電信事業或第三類事業提供電信服務時向用戶電信設備等發送資料傳輸指令傳輸用戶資訊之相關要求，與 cookies 之監管相關，主管機關為總務省。該條主要規範向用戶提供於總務省令所稱對用戶利益有重大影響之電信服務之電信事業或第三類事業經營者[182]。而依據日本《電氣通信事業法施行規則》（電気通信事業法施行規則）第 22 條之 2 之 27

[182] 該條所指第三類事業經營者依第 164 條規定，係指電信不設置電路設施，使用電信設施為他人間通訊中介服務之電信業務。如 IP、資料檢索服務及中介類服務等提供網路服務之業者。



本報告之智慧財產權歸屬於國發會

（第二十二条の二の二十七）[183]規定，總務省令就電氣通信事業法第 27 條之 12 所稱之電信服務定義為透過瀏覽器或其他軟體（限於使用者個人電腦、行動裝置上經作業系統執行之軟體）所提供之電信服務如社群平台、網路搜尋引擎或公開網站等「線上服務」。

前述電信事業或第三類事業向用戶提供電信服務（線上服務）時，若欲進行以用戶之電信設備為傳送目的地之資料傳輸指令（情報送信指令通信）[184]，電信事業或第三類事業有事前揭露之義務，其必須於事前通知使用者或以使用者容易得知之方式公告其所欲傳送之用戶資料內容、資料接收方（即傳送目標設備）以及其他法令規定事項。

該條款設有不須事前通知之例外：

A. 若電信事業或第三類事業是為傳輸總務省令所規定使用線上服務所需之資訊時，

B. 用戶端將發送至其設備之資訊傳送回本公司時，

C. 於資料傳送前已取得當事人同意或，

D. 設有退出(opt-out)機制，使當事人得於事後拒絕外部傳輸，並使當事人了解其權利。

---

[183] 依據電氣通信事業法施行規則(電気通信事業法施行規則)第 27 之 2 之 27 條，總務省令指定之電信服務係指以下之一並透過**瀏覽器或其他軟體**所提供之電信服務，包含: 媒介他人通信之電信服務、接收使用者透過電信傳送之資料並記錄或輸入至傳送裝置，並具備依不特定使用者之要求傳送資料與不特定用戶之功能 (如網站伺服器、電子郵件服務)、依輸入資訊輸出對應資訊之網頁網域名稱(IP)或其他位置資訊之電信設備(如搜尋引擎)以及前述以外具備依不特定使用者請求傳送資訊之功能，並提供不特定使用者瀏覽資訊為目的之電信服務(如公開網站、部落格等)。

[184] 依據《電氣通信事業法》第 27 之 12 條，資料傳輸指令係指「透過發送指令以啟動使用者設備所具備之資訊傳送功能，此功能會將使用者設備中記錄與該使用者相關之資訊傳送至第三方之設備。」



本報告之智慧財產權歸屬於國發會

總結而言，日本「電氣通信事業法」並未強制須有事前同意方得使用第三方 cookies，電信事業得透過事前告知或是設計退出權之方式合法將 cookies 傳輸至第三方。

(二)國際規範分析

1. cookies 是否為個人資料保護法制定義下之個人資料而受個人資料保護法制之監督

(1) 類型一、將 cookies 所存取之資料直接視為個人資料

加州 CCPA 將得識別或輕易連結至消費者或家庭之 cookies 直接列舉為唯一識別標誌之一種，故屬於 CCPA 所規範之個人資料範疇。因此得以識別或輕易連結至消費者或家庭之 cookies 將被直接被認定為個人資料而受到 CCPA 之保護。採用 cookies 之資料控制者，則必須於遵守 CCPA 對個人資料蒐集、利用之相關規範，以保障當事人之權利。維吉尼亞州之 VCDPA 雖未如 CCPA 直接於法規中界定 cookies，但依據其對個人資料之定義，若 cookies 能連結或識別特定當事人，則屬於 VCDPA 所欲規範之個人資料，資料控制者於利用上須遵守 VCDPA 之規定。

此外，不論是加州 CCPA 或維吉尼亞州之 VCDPA，皆採取提供消費者事後退出權(opt-out)之方式以保障當事人權利。資料控制者不須於使用 cookies 前取得當事人之同意，惟須給予消費者選擇退出、不提供第三方銷售、分享或刪除其個人資料上之權利。

(2) 類型二、依據 cookies 所存取資料之性質進行判斷

對於 cookie 所存取之資料是否屬於個人資料，歐盟認為 cookies 雖為線上識別態樣之一，但單獨存在時並不必



本報告之智慧財產權歸屬於國發會

然具備識別性，應視所存取之資料是否得以連結到特定當事人而定。若透過結合取得之其他資料加以結合比對得以識別特定個人者，則應受 GDPR 之規範，同時搭配 ePD 之規範，具體化於電子通訊中之隱私保護問題進行規範。當若有情形同時觸發 GDPR 及 ePD 之法律競合時，以特別法優於一般法原則優先適用 ePD，然而 ePD 必須符合 GDPR 之基本規範。

英國亦有 UK GDPR 及依據 ePD 所訂定之 PECR，規範上基本遵循歐盟模式。惟隨著英國脫歐，就涉及數位法令只規範上，英國開始有與歐盟不同之方向，尤以近期所通過之 DUAA 而言，英國就 cookie 之豁免情形予以放寬，從原本僅有必要性 cookies 得以免除當事人同意，到今年新增 4 項豁免情形。

日本將與 cookies 相關之規定分別規範於個情法以及「電氣通信事業法」。個情法僅將得透過輕易比對後能識別個人之 cookies 視為個人資料，以個人資料相關規範進行保護；而若 cookies 並未能識別當事人或屬於個情法下個人資料之定義，則會屬於個人關聯資料，不以個人資料進行保護。若 cookies 屬於個人資料，則須符合個情法規定不得於未經當事人同意之情形下做目的外利用或將資料傳輸予第三方。就屬關聯資料之 cookies，個情法僅就資料控制者於將 cookies 傳送予第三方時進行規範，並要求於可預見接收方能透過自身資料庫經比對後識別個人之情形下，係由接收方先取得當事人同意後，資料控制者方得傳送 cookies。而於《電氣通信事業法》之規範中，僅要求業者於將 cookie 進行傳輸前須以以下三種方式之一保



本報告之智慧財產權歸屬於國發會

障當事人權利，包含事前通知當事人、取得當事人事前同意或給予當事人退出之權利。

2. 各國 cookies 相關規範之主管機關

由於美國並未有聯邦層級之個人資料保護法或消費者保護法等規範，對於 cookies 之監督，主要落於州法，由各州評估是否予以規制。本次蒐集之加州與維吉尼亞州，基本上將 cookies 與個人資料保護法制連動，無論是直接明文納入規範，或以是否符合相關規範管制之個人資料定義範圍等進行納管。至於主管機關層面，則視各州政府組織結構與分工而有所不同，CCPA 於加州為隱私保護局所主管，故關於與消費者有關而適用 CCPA 之 cookies 問題，即係由隱私保護局處理。然而，維吉尼亞州並未有針對消費者資料保護法設置專責的機關，故而係由其檢察總長監督與執法。

歐盟對於 cookies 則是分別依據 GDPR 與 ePD 進行規範，而兩者皆需要指定監管機關。而依據 GDPR 歐盟會員國必須指定一個或多個監管機關。而由於 ePD 係早於 GDPR 之個人資料保護規範，故可能已有會員國指定資料保護主管機關負責 ePD 之執法，但亦有部分國家係指定其他機關例如國家電信監管機關如德國及瑞典，或其他適合之機關擔任 ePD 之主管機關。而 GDPR 並未限制不能指定與執行 ePD 相同之權責機關作為監督機關，故會員國得以指定同一資料保護主管機關作為 ePD 及 GDPR 之權責機關，然須注意行使職權與執法時所依據之法律依據，不得混淆。英國在 UK GDPR 以及 PECR 訂定期間仍為歐盟會員國，並指定同一機關－ICO 擔任主管機關。



本報告之智慧財產權歸屬於國發會

日本就 cookies 之管制規範包括個情法與電氣通信事業法，兩法之主管機關並不相同。個情法係由 JPIPC 主管，主要針對符合個情法個人資料或個人關聯資料定義之 cookies 對當事人可能造成之個人資料保護問題進行規範。然而若為電信事業使用 cookies，則另以電氣通信事業法管制，其管制規範偏向對該事業採用相關機制技術層面與責任之要求，未必限於對當事人隱私或個人資料保護之層面，而該法之主管機關則為總務省。

## 三、 結論與建議

cookies 之特性可使網路經營者藉由分析 cookie 存取之資料，更能掌握使用者之行為或需求，或取得使用者體驗之資訊，以優化其產品或服務。然 cookies 之使用應如何監管，國際上並無一致之作法。部分國家、國際組織或地區，考量 cookies 追蹤使用者行為之特性，可能涉及可識別個人資料之蒐集或利用，或可能侵害當事人隱私，故係以個人資料保護相關法制進行規制或監督，主管機關則為資料保護之主管機關，例如歐盟、英國、美國加州等。有國家則就管制重點與性質區分不同法律或主管機關進行監督，例如日本就個人資料保護層面，以個情法規制，尤其特別對個人關聯資料予以管理，由 JPIPC 主管監督；然而對產業端的要求，則另行透過電氣通信事業法進行責任要求，並由總務省主管。部分地區如美國維吉尼亞州，則並未特別規定，而係透過 cookies 性質有無識別性等有無符合個人資料保護法制規範範圍，由該州消費者保護與個人資料保護事務主管之檢察總長監督與執法。故若要評估對於 cookies 之國內管制法制應考量所欲管制之重點為何，係著重於對當事人識別資料之蒐集、處理或利用，則以個人資料保護法制為主，若係考量產業管制，則應納入產業主管機關之法令與角色。



本報告之智慧財產權歸屬於國發會

此外，雖然於法令未有明確規制而未納入前面管制趨勢蒐集，但對於產業 cookies 應用可能導致數位市場競爭問題之層面，近年來亦受到關注。例如歐盟以數位市場法（Digital Market Act）指定數位市場守門人（gatekeeper）並要求守門人法律義務之模式，促使數位市場守門人必須強化對消費者知情同意機制之落實、確保資料蒐集、利用與共享之透明度、確保消費者拒絕使用 cookies 仍可保有完整服務之權利等，某程度上對於 cookies 利用之主要平臺產生實質限制的效果，亦多面向的保障數位環境下消費者之權益。

我國現行法中尚未有直接將 cookies 概念納入之相關法令，然而個資法第 2 條對於個人資料之定義，如同歐盟、英國、美國維吉尼亞州及日本等，主要強調所蒐集資料之定性，若符合定義要件即屬於個人資料保護法所保障之個人資料。故雖然沒有直接將 cookies 列舉於定義當中，然而只要所蒐集之 cookies 可以直接或間接識別特定個人，則仍屬於個人資料保護法規範之範疇。基此，事業採用 cookies 機制若可能直接或間接識別當事人，則需遵循個人資料保護法之規定，具備法定蒐集、處理或利用之要件，並尊重當事人之選擇。此部分要探討的反而是個資法目前的規範處理 cookies 議題是否已經足夠，或有需要強化規範的地方，例如基於 cookies 蒐集類型與應用之複雜度，就告知義務履行之清晰、全面或可理解層面加強要求，或增加當事人事後拒絕等控制權之規範等。涉及此類具個人資料性質之 cookies，屬於個人資料保護法執法之範疇，則應對應現行個資法之主管機關分工進行監督，尤其非公務機關業務管制層面應有其目的事業主管機關可予以要求，後續獨立機關個人資料保護委員會成立則按其業務移轉進程逐步由該委員會監督之。

至於個人資料保護法層面，如何更有效的針對 cookies 引發的資料保護議題強化管理，或喚醒個人與利用 cookies 之資料蒐集、處理或利用者的保護意識，甚至進一步指導或要求應採行之作法或措施部分，



本報告之智慧財產權歸屬於國發會

可考慮參考歐盟或英國之作法，由個人資料保護法之主管機關發布指引，協助進行法律遵循之判斷，並提供作法建議，強化國內各界對於cookies 與個人資料保護法制間關聯的理解，並具體落實於實務操作。

除符合個人資料保護層面之cookies管制外，對於產業應用cookies進行與個人資料保護無關之商業分析、競爭或目標廣告投放等問題，若已涉及限制競爭或不公平競爭問題，本可由公平交易委員會介入執法。然而，若係目標廣告投放或藉由使用者資料分析限制使用者可取得或瀏覽之資訊等事宜，實際涉及到消費者選擇權的保障，現階段尚未有直接之法令規範進行處理。此部分則是要考慮是否有必要對於特定事業或組織更進一步於法律規範，或參考歐盟針對高度利用 cookies之大型數位平臺進行責任要求，主管機關層面可考量所涉事業之主管機關，或從消費者保護執法層面思考，可再評估。



本報告之智慧財產權歸屬於國發會

## 項次 2. 工作會議

### 壹、 第一次工作會議

一、 會議日期：114 年 4 月 30 日(星期三)下午 2 時 30 分

二、 會議地點：國發會法制協調處 605 會議室

三、 出席人員：

(一)國發會：許科長、陳專員、謝專員

(二)資策會：陳主任、邱資深協理、陳專案經理、劉副研究員

四、 會議結論：

(一)焦點議題一報告初稿修正

1. 請研究團隊參考標註意見進行修正，另請補充並確認：

(1) 關於國際趨勢之經濟合作暨發展組織(OECD)文件名稱，請確認並調整。另此文件四項支柱第 1 項第 1 段前面提及之「政府應建立更具適應性且更為動態、靈活之機制並縮短法制政策評估之週期…」，請確認是否有適當實際執行之實例可補充說明。

(2) 關於日本灰色地帶消除制度，請協助確認該機制之執行流程、執行模式以及執行時程等資訊，並確認日本數位廳或其他相關機關是否有此機制之實例。

(3) 針對我國立法現況，建議補充立法程序之流程圖以利對照，並就流程當中是否有可以簡化或加速之處，再提供補充意見。

2. 請研究團隊於 5 月 14 日前提交修正報告。



本報告之智慧財產權歸屬於國發會

(二)第 6 次數位政策法制協調專案會議議程及幕僚意見之協助

1. 案由四「資料治理規劃藍圖」之簡報資料尚未取得，待取得相關資料後請研究團隊儘速協助提供幕僚建議。

2. 案由五「外送平臺及網路交友服務治理機關歸屬管理事宜」擬整理相關會議資料。

3. 討論事項「臺灣主權 AI 訓練語料庫推動規劃」由數發部主責，該部尚未提供會議資料；該部僅初步對於各部會可釋出之資料庫、配合方式及資料共享之方式提出建議意見。待數發部提供資料後，再請研究團隊提供幕僚意見。



本報告之智慧財產權歸屬於國發會

## 貳、 第二次工作會議

一、 會議日期：114 年 8 月 13 日(星期三)上午 10 時

二、 會議地點：國發會法制協調處 605 會議室

三、 出席人員：

(一)國發會：温專門委員、鄭科長、許科長、陳專員、謝專員

(二)資策會：陳主任、邱資深協理、陳專案經理、劉副研究員

四、 會議結論：

(一)研討會主題：建議改以促進 AI 發展與創新之上位大方向訂定主題。

(二)議題規劃

1. 關於前言，請研究團隊以國發會之角度，融合行政院研擬「AI 新十大建設(草案)」之政策方向，修正文字。

2. 關於研討會議題，考量本次研討會係以 AI 著作權及 AI 監理沙盒機制為主題，議程規劃暫不納入資料開放、資料創新、資料治理及個人資料保護等議題。規劃方向如下：

(1) 主題一 AI 與著作權議題，可整併第一版之主題一、二。議題重點在於，發展 AI 需要使用大量資料，涉及著作權資料之合法取得與利用之問題，包括如何促進著作權人將資料釋出、產業界希望達成什麼樣的法制環境，以平衡技術創新之需求與對著作權人之保障，希望聽取不同角度意見。



本報告之智慧財產權歸屬於國發會

(2) 項下分為兩個子議題，子議題一著重於修法與否之必要性、子議題二聚焦配套措施：

①子議題一：針對因應 AI 發展之訓練資料需求，涉及著作權等議題，包括：透過現行法令解釋「合理使用」之界限、對於修法採行「資料探勘例外」或「強制授權」等法制模式之看法、民刑事責任之衡平性是否得相應調適(例如：於特定情形酌減刑罰、提高民事賠償額度或納入懲罰性賠償、或其他可能之規範模式)等。

②子議題二：除上開修法與否之討論，有哪些可能之配套措施，得以促進資料釋出？(例如：強制授權機制下之利用人透明性義務、建立權利人之退出權、或其他可能增加著作權人授權或釋出資料之誘因的相關機制等。)

3. 主題二 AI 監理沙盒機制

因應新興科技，許多國家設有沙盒機制，歐盟 AIA 亦有類似規定。我國在特定領域雖已有沙盒機制，然而實務案例及效果呈現上似相對有限，爰期透過本次研討會，邀請產官學代表針對我國實施沙盒機制之經驗進行交流討論，以瞭解過往實務應用上所可能遭遇之困境，或對於我國「AI 沙盒機制」應如何建構提出建議等，以提供未來主管機關推動之參考。

(三)專家人選與進行方式

1. 採取主持人及與談人交流討論之模式，針對主題表述意見。又為能使對議題討論更豐富活絡，宜由主持人帶領議題，並自產官學界等不同領域，每個領域邀請 1-2 位邀請專家針對相關議題進行討論對話。且須考慮主持人應有一定身分或經驗，俾有效引導議題討論。



本報告之智慧財產權歸屬於國發會

2. 有關目前提出之建議名單，請依據修正後議題，再行調整適當邀請人選；公協會倘有適當人選，並請納入建議名單。官方代表原則不指定特定人，而由各機關指派適合參與議題之人選，由國發會邀請。

3. 考量推動主權 AI 之 TAIDE 團隊瞭解 AI 訓練資料取用因境，建議將其列為主題一之與談人選。

(四)執行事項

請研究團隊修正研討會議程規劃及建議名單，將於第 3 次工作會議討論修正後之議程及邀請人選。



本報告之智慧財產權歸屬於國發會

## 參、 第三次工作會議

一、 會議日期：114 年 8 月 25 日(星期一)上午 10 時

二、 會議地點：國發會法制協調處 605 會議室

三、 出席人員：

(一)國發會：温專門委員、許科長、陳專員、謝專員

(二)資策會：陳主任、陳專案經理、劉副研究員

四、 會議結論：

(一)議題規劃調整

1. 目前主題一「生成式 AI 的著作權挑戰」規劃討論 AI 訓練階段之著作權法制議題，請研究團隊修改題目，限縮於生成式 AI 訓練資料之著作權法制議題。

2. 主題一之講題(一)：生成式 AI 訓練資料之合理使用界限與突破

   (1) 本項議題包括法定授權及強制授權之討論，不僅針對合理使用之界限，請研究團隊配合修正標題。

   (2) 建議於與談議題 2 之「法定強制授權或強制授權」前，加上緩衝，如「符合一定要件下」，避免使著作權人感到權益受損。

   (3) 與談議題 3 原列「資料探勘例外」，目的在於瞭解 AI 之訓練資料合理使用的可能規範依據，可修改為討論 AI 訓練資料之特定合理使用規範。

3. 主題一之講題(二)：友善生成式 AI 發展之法制配套初探



本報告之智慧財產權歸屬於國發會

(1) 本主題之配套以法制為主軸，倘法制不及調整，或可採取哪些配套機制為輔助，例如合理利益分配等；本次之討論，擬不涉及促進資料創新利用發展條例草案。

(2) 與談議題 1 建議修正為「…，必要採行之配套措施為何（例如：課予利用者透明性義務、賦予權利人退出權）？若法制上尚無法解決時，有何配套措施可搭配調整？」邀請現場與談人員發想。

(3) 與談議題 3 依研究團隊所提供之文字修正為「是否就現行實務狀態與資料運用情形之需要等，評估現行民、刑事規範之合理性及有效性，例如評估行為輕重規範不同刑度，或進行民刑責任之搭配或調整等？」。

(二)議程與講者規劃調整

1. 為使主題一之 AI 著作權議題討論具連貫性，將主題二「AI 監理沙盒機制與創新治理」與主題一「生成式 AI 的著作權挑戰」順序對調。

2. 請整合主題一兩項講題之與談名單，依討論修改(例如加邀李姿儀老師等)，排列名單依序邀請。至官方代表部分，主題一兩項講題請均列經濟部智慧局代表，主題二官方代表可不列環境部。

3. 主題二 AI 監理沙盒機制與創新治理因議程順序調整，國發會代表長官致詞後可能接續主持本場次，故主持人改為國發會代表。

4. 因場地配置限制，每場次之主持人及與談人之人數上限為 7 人。



本報告之智慧財產權歸屬於國發會

(三)行政事項

1. 午膳以環保餐盒供餐，至下午茶點方案及修正後第一場次之主持人選，將俟委託機關確認後提供執行單位。

2. 請執行團隊於 8/27(三)前提交本次討論議程之修正版。



本報告之智慧財產權歸屬於國發會

## 肆、 第四次工作會議

一、 會議日期：114 年 9 月 24 日(星期三)下午 2 時

二、 會議地點：國發會法制協調處 605 會議室

三、 出席人員：

(一)國發會：溫專門委員、鄭科長、許科長、陳專員、蔡科員

(二)資策會：陳主任、陳專案經理、劉副研究員

四、 會議結論：

(三)議程規劃調整

1. 關於流程總體規劃：

(1) 流程增加合照環節：開幕致詞調整為 3 至 5 分鐘，致詞結束後安排第一場次與談人與副主委合照；下午兩場次於交流討論結束後安排合照。

(2) 主持與串場：第二場次及第三場次主持人開場調整為 5 分鐘，串場時間調整為 1 至 2 分鐘。

(3) 發言時間：規劃每位與談人發言時間原則為 10 分鐘，將視會前會與談人之意見調整時間，並由工作人員舉牌提醒與談人回答時間(「1 分鐘」及「時間到」)。

(4) 提問及預備問題：每場次之交流時間先開放觀眾提問，若現場無提問，由主持人提出預備問題。會前會告知與談人預備問題，讓與談人能有所準備，但不須分配問題，依其意願自由回答。

2. 各場次之流程規劃：



本報告之智慧財產權歸屬於國發會

(1) 第一場次：

A. 本主題重點係透過國際觀察引導出後續問題，後兩題為重點，故可安排較多人於第 2 題及第 3 題分享。

B. 有關雷主任優先回答問題順序，待會前會確認，國發會將引導其回答第 2 題。

C. 主持人之預備問題，第 2 題改為「…依據，如何能於現行法制下創造有彈性的做法？」。

(2) 第二場次：第 1 題尚未有與談人選擇為第 1 或第 2 序位回應題，國發會將於會前會再向與談人詢問意願。

(3) 第三場次：

A. 徐總經理尚未回復答題意願，國發會將於會前會引導其回答第 2 題。

B. 賴律師回復皆可回答，且無特別標示優先順序，故第 3 題預擬新增賴律師，國發會將於會前會與其確認。

3. 其他會前會注意事項：

(1) 由國發會主導會前會流程，並依據每場次流程，提醒與會專家報到時間為最晚抵達時間，以及向與談人說明會議手冊相關事宜。

(2) 請資策會於會前會結束後，將模板提供給與談人填寫，內容包含照片(註明解析度)、職稱、簡歷(敘述性 100-150 字)，若有會議分享資料，一併於 10/9 前提供研究團隊。

(四)行政事項



本報告之智慧財產權歸屬於國發會

1. 報名：國發會預計 10 月初將報名資訊發函通知各部會、新創相關公協會，請研究團隊先行提供報名連結及 DM，並於 10/9 前確認報名狀況。另有關老師建議邀學生參加，將於會前電郵併同提供報名連結，以利邀請。

2. 手冊：與談人照片頁請以彩色頁呈現，並附上簡介。

3. 座位：請依與談題目答題次序安排座位，桌牌放在與談人座位旁的小桌子上；請預留第 1 排座位給欲出席其他場次的與談人。

4. 司儀：請司儀參加會前會，以瞭解研討會流程，並建議於研討會前演練或預擬司儀稿。

5. 餐盒回收：為確實回收環保餐盒，請司儀提醒或適當標示等方式提醒出席人員。



本報告之智慧財產權歸屬於國發會

# 附錄一：114 年度國際趨勢觀測重點法案清單

## 一、AI 著作權

| 法案(中文) | 法案(英文) | 法案連結 |
|---|---|---|
| 人工智慧網路透明度及責任法案(美國) | Transparency and responsibility for Artificial Intelligence Networks Act | https://www.govinfo.gov/app/details/BILLS-118s5379is/ |
| 著作權與 AI 報告第二部分：可受著作權保護(美國) | Copyright and Artificial Intelligence Part 2: Copyrightability | https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-2-Copyrightability-Report.pdf |
| 著作權與 AI 報告第三部分：生成式 AI 之訓練報告(美國) | Copyright and Artificial Intelligence Part 3: Generative AI Training pre-publication version | https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-3-Generative-AI-Training-Report-Pre-Publication-Version.pdf |
| 通用人工智慧實踐準則(歐盟) | The General-Purpose AI Code of Practice | https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai |
| 著作權及人工智慧：諮詢(英國) | Copyright and AI: Consultation | https://www.gov.uk/government/consultations/copyright-and-artificial-intelligence?utm_medium=email&utm_campaign=govuk-notifications-topic&utm_source=bda528c5-6cac-46ce-a9a2- |



本報告之智慧財產權歸屬於國發會

| 法案(中文) | 法案(英文) | 法案連結 |
| --- | --- | --- |
| | | 488d2820322c&utm_content=immediately |
| 資料(利用與近用)法(英國) | Data Use and Access Act | https://www.legislation.gov.uk/ukpga/2025/18/contents |
| 防止仿冒商品流通的綜合對策(韓國) | 위조상품 유통방지 종합대책 | https://reurl.cc/VW8WZ6 |
| 人工智慧生成合成內容標示辦法(中國大陸) | 人工智能生成合成内容标识办法 | https://www.gov.cn/zhengce/zhengceku/202503/content_7014286.htm |

**二、AI 消費者/使用者保護**

| 法案(中文) | 法案(英文) | 法案連結 |
| --- | --- | --- |
| 俄勒岡州企業 AI 指引(美國) | Guidance on AI for Oregon Businesses | https://www.doj.state.or.us/media-home/news-media-releases/ag-rosenblum-issues-guidance-on-ai-for-oregon-businesses/ |
| AI 與消費者傷害風險政策方向建議(美國聯邦貿易委員會) | AI and the Risk of Consumer Harm | https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2025/01/ai-risk-consumer-harm |
| 關於加州現行法適用於 AI 之法律諮詢(美國加州) | Legal Advisory on the Application of Existing California Laws to Artificial Intelligence | https://www.skadden.com/-/media/files/publications/2025/03/state-attorneys-general-may-fill/legal-advisory--application-of-existing-ca-laws-to-artificial- |



本報告之智慧財產權歸屬於國發會

| 法案(中文) | 法案(英文) | 法案連結 |
| --- | --- | --- |
| | | intelligence.pdf?rev=1ddc130e80f041e491cfedf097be8431&hash=63283A39FBC4922139C806C780F67E2A |
| 關於與AI系統互動之消費者保護法案(美國科羅拉多州) | Concerning Consumer Protections in Interactions with Artificial Intelligence Systems Act | https://leg.colorado.gov/sites/default/files/images/report_and_recommendations_0.pdf |
| 關於 AI 法案(美國夏威夷) | Relating to Artificial Intelligence Act | https://legiscan.com/HI/text/HB639/2025 |
| 要求聊天機器人通知消費者法案(美國麻薩諸塞州) | Requiring consumer notification for chatbot systems | https://legiscan.com/MA/text/S243/2025 |
| 消費者保護：當消費者誤信為與人互動時，使用電腦與消費者互動，為不法商業行為法案(美國阿拉巴馬州) | Consumer protection, use of a computer to interact with a consumer when consumer believes the interaction is with a human is an unlawful trade practice | https://legiscan.com/AL/text/HB516/2025 |



本報告之智慧財產權歸屬於國發會

| 法案(中文) | 法案(英文) | 法案連結 |
| --- | --- | --- |
| 消費者詐欺與欺騙性商業行為法修正案(美國伊利諾州) | Amends the Consumer Fraud and Deceptive Business Practices Act | https://legiscan.com/IL/text/HB3021/2025 |
| 確保涉及 AI 消費者交易透明度法案(美國緬因州) | An Act to Ensure Transparency in Consumer Transactions Involving Artificial Intelligence | https://legislature.maine.gov/legis/bills/getPDF.asp?paper=HP1154&item=1&snum=132 |
| AI 消費者保護修正案(美國猶他州) | Artificial Intelligence Consumer Protection Amendments | https://legiscan.com/UT/text/SB0226/id/3174279 |
| AI 修正案(美國猶他州) | Artificial Intelligence Amendments | https://legiscan.com/UT/text/HB0452/id/3170911 |
| 德州負責任地人工智慧治理法案(美國德州) | The Texas Responsible AI Governance Act, HB 149 | https://legiscan.com/TX/text/HB149/2025 |
| 關於瑕疵產品之責任與廢除委員會指令，新產品責任指令(歐盟) | EU 2024/2853 on liability for defective products and repealing Council Directive，The new Product Liability Directive | https://single-market-economy.ec.europa.eu/single-market/goods/free-movement-sectors/liability-defective-products_en#software-and-ai-systems |

**三、AI 勞工權益**



本報告之智慧財產權歸屬於國發會

| 法案(中文) | 法案(英文) | 法案連結 |
| --- | --- | --- |
| 消費者金融保護通函2024-06(美國) | Consumer Financial Protection Circular 2024-06 | https://www.consumerfinance.gov/compliance/circulars/consumer-financial-protection-circular-2024-06-background-dossiers-and-algorithmic-scores-for-hiring-promotion-and-other-employment-decisions/ |
| 《工作場所中之可穿戴設備：依聯邦就業歧視法使用可穿戴技術》情況說明書(美國) | Wearables in the Workplace：Using Wearable Technologies Under Federal Employment Discrimination Laws | https://www.eeoc.gov/sites/default/files/2024-12/Wearables_Fact_Sheet_V10_%28002%29_508FINAL.pdf |
| 美國德州負責任地人工智慧治理法案 | the Texas Responsible AI Governance Act, HB 1709 | https://capitol.texas.gov/BillLookup/History.aspx?LegSess=89R&Bill=HB1709 |
| 演算法歧視指引(美國紐澤西州) | Guidance on Algorithmic Discrimination | https://www.njoag.gov/attorney-general-platkin-and-division-on-civil-rights-announce-new-guidance-on-algorithmic-discrimination-creation-of-civil-rights-innovation-lab/ |



本報告之智慧財產權歸屬於國發會

| 法案(中文) | 法案(英文) | 法案連結 |
| --- | --- | --- |
| 第二次修改關於自動決策系統之擬議就業法規(美國加州) | Second Round to Initial Text of Proposed Modifications to Employment Regulations Regarding Automated-Decision Systems | https://www.callaborlaw.com/_images/blog_files/Second_Modifications_to_Proposed_Modifications_to_Employment_Regulations_Regarding_Automated-Decision_Systems.pdf |
| 自動決策安全法案(美國加州) | Automated Decisions Safety Act | https://legiscan.com/CA/text/AB1018/2025 |

**四、AI 個人資料保護及監管**

| 法案(中文) | 法案(英文) | 法案連結 |
| --- | --- | --- |
| 美國加州消費者隱私法更新(美國加州) | The California Consumer Privacy Act (CPPA) | https://cppa.ca.gov/regulations/ccpa_updates.html |
| 聯邦兒童線上隱私權保護法(美國) | Children's Online Privacy Protection Act | https://www.federalregister.gov/documents/2025/04/22/2025-05904/childrens-online-privacy-protection-rule |
| 刪除法(美國) | Take it Down Act | https://www.congress.gov/bill/119th-congress/senate-bill/146 |
| 第 28/2024 號關於 AI 模型中處理個人資料保護意見(歐盟) | Opinion 28/2024 on certain data protection aspects related to the | https://www.edpb.europa.eu/news/news/2024/edpb-opinion- |



本報告之智慧財產權歸屬於國發會

| 法案(中文) | 法案(英文) | 法案連結 |
| --- | --- | --- |
| | processing of personal data in the context of AI models | ai-models-gdpr-principles-support-responsible-ai_en |
| 自動化決策最佳實務指引(2025)(澳洲) | Automated Decision-making: Better Practice Guide | https://architecture.digital.gov.au/design/automated-decision-making-better-practice-guide |
| 隱私及使用市售人工智慧產品指引(澳洲) | Guidance on privacy and the use of commercially available AI products | https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-the-use-of-commercially-available-ai-products#section-top-five-takeaways |
| 生成式 AI 處理指引(韓國) | 생성형 인공지능(AI) 개발·활용 위한 개인정보 처리 기준 제시한다 | https://pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId= 11410#LINK |
| 新全球 AI 信任沙盒(新加坡) | the new Global AI Assurance Sandbox | https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2025/singapore-launches-new-tools-to-help-businesses-protect-data-and- |



本報告之智慧財產權歸屬於國發會

| 法案(中文) | 法案(英文) | 法案連結 |
| --- | --- | --- |
| | | deploy-ai-in-a-trusted-ecosystem |
| 新 PETs 採用指引(新加坡) | a new PETs adoption guide | https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2025/singapore-launches-new-tools-to-help-businesses-protect-data-and-deploy-ai-in-a-trusted-ecosystem |
| 新加坡資料保護標準(新加坡) | Singapore Standard for Data Protection | https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2025/singapore-launches-new-tools-to-help-businesses-protect-data-and-deploy-ai-in-a-trusted-ecosystem |
| 雇員使用生成式人工智慧指引清單(香港) | | https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/guidelines_ai_employees.pdf |

**五、其他重要趨勢**



本報告之智慧財產權歸屬於國發會

| 法案(中文) | 法案(英文) | 法案連結 |
| --- | --- | --- |
| 關於消除聯邦機構 AI 使用及採購障礙之情況說明書(美國) | Fact Sheet: Eliminating Barriers for Federal Artificial Intelligence Use and Procurement | https://www.whitehouse.gov/fact-sheets/2025/04/fact-sheet-eliminating-barriers-for-federal-artificial-intelligence-use-and-procurement/ |
| 人工智慧行動計畫(美國) | America's AI Action Plan | https://www.ai.gov/action-plan |
| 人工智慧系統定義指引(歐盟) | Guidelines on the definition of an artificial intelligence system | https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application |
| AIA 定義之 AI 禁止行為指引(歐盟) | Guidelines on prohibited artificial intelligence practices established by AI Act | https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act |
| 人工智慧治理及風險管理意見書(歐盟) | Opinion on Artificial Intelligence Governance and Risk Management | https://www.eiopa.europa.eu/eiopa-publishes-opinion-ai-governance-and-risk-management-2025-08-06_en |



本報告之智慧財產權歸屬於國發會

| 法案(中文) | 法案(英文) | 法案連結 |
| --- | --- | --- |
| 人工智慧法(歐盟)第73 條—事件通報指引草案(歐盟) | Draft Guidance Article 73 AI Act – Incident Reporting | https://digital-strategy.ec.europa.eu/en/consultations/ai-act-commission-issues-draft-guidance-and-reporting-template-serious-ai-incidents-and-seeks |
| 預防傷害，增進信任：我們的人工智慧與生物辨識策略(英國) | Preventing harm, promoting trust：our AI and biometrics strategy | https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/artificial-intelligence-and-biometrics-strategy/ |
| 人工智慧司法行動計畫(英國) | AI action plan for justice | https://www.gov.uk/government/publications/ai-action-plan-for-justice/ai-action-plan-for-justice |
| AI 採用指引(澳洲) | Guidance for AI Adoption | https://www.industry.gov.au/publications/guidance-for-ai-adoption/guidance-ai-adoption-foundations\| Department of Industry Science and Resources |
| AI 政策指導範本(澳洲) | AI Policy: Guide and Template | https://www.industry.gov.au/sites/default/files/2025- |



本報告之智慧財產權歸屬於國發會

| 法案(中文) | 法案(英文) | 法案連結 |
| --- | --- | --- |
| | | 10/ai_policy_guide_and_template.pdf |
| 關於生成式人工智慧報告 1.0(日本) | About the Report Regarding Generative AI, Version. 1.0 | https://www.jftc.go.jp/en/pressreleases/yearly-2025/June/250606.html |
| 人工智慧相關技術研究開發及應用推動法(日本) | 人工知能関連技術の研究開発及び活用の推進に関する法律 | https://laws.e-gov.go.jp/law/507AC0000000053?tab=cited#Mp-Ch_2 |
| 關於人工智慧發展及建立信任基礎之基本法案(韓國) | 인공지능 발전과 신뢰 기반 조성 등에 관한 기본법안, AI 기본법 | https://www.msit.go.kr/bbs/view.do?sCode=user&mId=307&mPid=208&bbsSeqNo=94&nttSeqNo=3185321 |



本報告之智慧財產權歸屬於國發會

## 附錄二：期中審查意見回應說明

| 委員 | 編號 | 建議 | 研究團隊回應 |
|---|---|---|---|
| 郭麗珍教授 | 1. | 報告項次 1 之國際觀測，整體而言 4 項主題國家別不太平均，AI 與著作權以及個資保護所選之國別較為全面，但 AI 與消費者保護部分僅有美國聯邦、各州以及歐盟《關於瑕疵產品之責任指令》,而該指令是將產品類型增加軟體及智慧型裝置；建議評估下半年可增加歐盟 AIA 涉及消費者保護之相關討論(如聊天機器人部分)及納入美國、歐盟就演算法涉及勞工部分之討論或法案。此外,國際觀測是否就 4 項議題,對應我國相關修法之建議等，請研究團隊予以說明。 | 1. 感謝委員建議。<br>2. 因國際觀測為觀測今年度之法案，消費者保護以及勞工相關議題上今年度之更新多為美國之法案。<br>3. 本案為延續案,113 年已就四項議題提出過我國相關修法建議，故本年度延續追蹤觀測議題動態。 |
| | 2. | 報告項次 2 之焦點議題「加速法規調適或鬆綁研析」,於我國法制現況部分問題列出 5 個重點，其中第 4 個重點建議強化跨部門監督合作部分，因為進行跨部會整合很重要，如何強化各部會橫向間之合作及啟動、行政院協調平台及分組專案會議之機制是否足夠解決跨部會法規調適問題等，期許研究團隊於報告中有相關建議。 | 1. 感謝委員建議。<br>2. 已於報告焦點議題我國作法建議第 2 點補充納入相關補充建議。 |



本報告之智慧財產權歸屬於國發會

| | | | |
|---|---|---|---|
| | 3. | 建議報告內文用語轉化為我國慣用翻譯，讓讀者較容易理解，例如期中報告第 60 頁「經濟營運商」(economic operators)於我國慣用翻譯為「企業經營者」；倘無法完全對應或確定我國法律用語時，建議補充原文。 | 1. 感謝委員建議。<br>2. 已修正為企業經營者。 |
| 陳匡正教授 | 1. | 著作權包含著作人格權、製版權等相關規定，主流意見建議不以修法，而以監理沙盒等方式予以調適。期中報告大部分著重於著作財產權，美國大部分之案例多是在討論合理使用，較無 AI 相關之著作人格權層面的探討；然而法規衝突如何調適？例如 AI 倘非著作權人，則應如何適用製版權或強制授權等問題，後續建議再予以關注。期中報告第 2 分項提及國際趨勢上，並未淡化減少對著作權之保護，但建議對著作人格權之保護，有所分析。 | 1. 感謝委員建議。<br>2. 以現行狀態下，國際上針對著作法制討論仍以著作財產權較多，觀測較少對於著作人格權之法令討論，後續研究將持續關注。 |
| | 2. | 有關跨部會數位法制協調機制之作法，是否需要制定特別法或以現行法制進行？報告中提及之專案會議，其角色為何？是透過跨部會協調會議或單一部會主持？應避免多頭馬車問題。 | 1. 感謝委員建議。<br>2. 相關疑問已於報告焦點議題我國作法建議第 2 點補充論述。 |



本報告之智慧財產權歸屬於國發會

| | | | |
|---|---|---|---|
| 章忠信兼任助理教授 | 1. | 建議期中報告翻譯用語，應轉化為我國用詞或概念，例如第 1 頁「美國法典(U.S. Code.) 第 17 編第 5 章」即為著作權法，宜翻譯為美國著作權法,以利讀者理解。建議全盤檢視,讓用語更為精確,例如涉及著作權法之用語，著作權所保護者為「著作」而非「作品」、是「著作權人」而非「著作權利人」、是「重製」而非「複製」等，第 19 頁「權利人經濟及人格權(economic and moral right)，而由權利人控制其作品如何被利用」建議翻譯為「著作權人之著作財產權及著作人格權，而由著作權人控制其著作如何被利用」等。另美國著作權報告中之 AI 生成的「著作」,不一定相關成果能符合「著作」之定義，建議文字上再為修正。 | 1. 感謝委員建議。<br>2. 已依建議修正。 |
| | 2. | 報告之建議需有更高層次的視野。各國數位政策有其發展背景,例如美國政策、法規較開放，讓著作權自由發展;歐盟則較保守,保護公眾或既有利益。我國並非一定要選擇某一國家之作法，現有的規定也非牢不可破。各國政策立法有其各自立場，相較之下我國之利益為何及需要採何種立 | 1. 感謝委員建議。<br>2. 本案為延續案,113 年已就四項議題提出過我國相關修法建議，故本年度延續追蹤觀測議題動態。 |



本報告之智慧財產權歸屬於國發會

| | | | |
|---|---|---|---|
| | | 場？期許研究團隊在期末報告中建議我國需要採取何種立場，而非僅介紹各國政策。 | |
| | 3. | AI 的訓練不一定要複製(copy)，可能用「看」的即可訓練。現行著作權法，雖然是否給人「看」不是著作權人的權利，但未經許可破解密碼後進去看，會違反著作權法。未來若是機器透過「看」即能學習，過程中沒有複製，系統也沒有儲存相關內容，權利人是否可主張相關權利？這將是立法者必須面對的問題。或許考慮是否給予權利人新的權利，例如 AI 訓練權，使 AI 開發者與著作人進行利益分配，不但不會阻礙技術之發展，反而可能促使資料活用。關於 AI 訓練利用到他人著作，部分觀點認為可以合理使用解決，但合理使用將會導致不需對權利人進行利益分配，對權利人未必公平。 | 1. 感謝委員建議。<br>2. 針對資料探勘國際上仍有爭議尚無法定論，後續研究上將持續關注。 |
| | 4. | 「透明度」為各國都很重視之議題，當前問題是 AI 開發者使用當事人個資、著作等資料，但當事人並不知情，亦無法得知權利受到侵害，建議可在報告中強調透明度之重要性。 | 1. 感謝委員建議。<br>2. 已於國際觀測總結中補充。 |



本報告之智慧財產權歸屬於國發會

| | | | |
|---|---|---|---|
| | 5. | 期中報告內之「法規鬆綁」建議改為「法規調整」，畢竟法規之研擬，均有其背景及嚴謹的立法程序，其實各國法規似未有太大改變，不見得皆有鬆綁之必要性，應視既有法規是否在因應新興科技上遇到困難。例如歐盟 AIA 表明應尊重著作權法，而非修法，也就是請 AI 開發者訓練資料取得授權。各部會協調實屬必要，但應尊重各主管機關的專業，例如我國智慧財產局職責即是保護著作權，並非科技發展之絆腳石；建議參考美國著作權局，其認為訓練 AI 所需之著作時，仍應要與著作權人談授權，以保護著作人之權利。 | 1. 感謝委員建議。<br>2. 已依委員建議調整。部分內容為行政院之法規鬆綁政策，故維持原用語。 |
| | 6. | 以美國與我國著作權要件之不同，例如自盜版網站下載資料去訓練 AI 是否合法？很難想像 Open AI 開發者被抓去關，回到期中報告第 2 分項幕僚意見提到針對著作權刑罰之檢討，各國都未有修法，但我國刑罰似有過重問題。以國際法令來看，針對著作侵害之責任，有些國家甚至無刑事責任。我國是否應重新檢視著作權侵權之刑事罰則，期待研究團隊於期末報告中提供建言。 | 1. 感謝委員建議。<br>2. 著作權法侵權刑罰之規範透過研討會進行意見蒐集及討論。納於期末報告之研討會會議報告。 |



本報告之智慧財產權歸屬於國發會

| | | | |
|---|---|---|---|
| 經濟部<br>智慧財產局 | 1. | 有關國際趨勢觀測，日本與韓國於 2025 年也有發布生成式 AI 著作權相關指引或報告，建議研究團隊於下半年觀測中納入鄰近國家之觀測；另關於美國近期的兩個判決，對於合理使用的部分有相關論述，建議納入報告。 | 1. 感謝委員建議。<br>2. 本計畫為延續計畫，日本之指引已納於去年之報告中，目前未看到更新。韓國之指引以及美國案例已更新於期末報告。 |
| | 2. | 期中報告部分用詞建議再予釐清，例如：第 8 頁提到美國第 107 條合理使用之「非排他因素」是否有特殊意義、第 23 頁英國規範所指「商業資料」之內涵為何。第 245 頁提到日本著作權修法已將合理使用納入，年份應是 2018 年，報告誤植為 2019 年，且日本著作權法第 30 條之 4 為合理使用之規定，是對著作權行使之限制，報告中用語「合法授權」，建議再予斟酌。另，報告第 246 頁「出台」用字建議調整為我國慣用翻譯及用字。 | 1. 感謝委員建議。<br>2. 美國第 107 條合理使用之「非排他因素」為原文「non-exclusive factors」之翻譯，指判斷合理使用之要素。已將原文於文內補充。<br>3. 英國規範之「商業資料」已於註解補充其內涵。<br>4. 日本著作權法部分，已修正為 2018 年，並將「合法授權」修正為放寬 AI 資料運用限制。<br>5. 依建議修正「出台」為「發布」。 |



本報告之智慧財產權歸屬於國發會

| | | | |
|---|---|---|---|
| | 3. | 期中報告第 244 頁有關著作權刑罰，於歐盟 AIA 的標題提到有高額行政罰鍰；考量歐盟 AIA 之規定，就 AI 業者違反揭露義務，屬違反行政上義務，故處以罰鍰，但未必構成著作權侵害；違反著作權法規定，主要仍以民、刑事責任為主。故對 AI 產業的監管及對著作權的處罰建議再確認與區隔，否則容易讓讀者誤解著作侵害有行政罰之問題。第 245 頁美國部分，標題說明美國的著作權報告顯示其管制有趨於嚴格，但結論又指美國沒有要調整法規，結論和標題似不太一致，建議可再評估用語。 | 1. 感謝委員建議。<br>2. 美國著作權報告內容有趨於嚴格管制之趨勢，惟該報告僅屬建議性質，著作權局並未實際修法。已調整內文敘述。<br>3. 針對歐盟 AIA 相關敘述已於報告中更正。 |



本報告之智慧財產權歸屬於國發會

## 附錄三：期末審查意見回應說明

| 委員 | 編號 | 建議 | 研究團隊回應 |
|---|---|---|---|
| 郭麗珍教授 | 1. | 人工智慧(AI)應用的消費者及使用者保護、演算法對勞工權益等議題，篇幅較少，建議增加篇幅；例如國際觀測中針對 AI 消保議題，美國的資料較完整，另第 88 頁提到歐盟「關於瑕疵產品責任法令」針對 AI 軟體產品及其更新、資料毀損等，皆為數位時代下新的規範，歐盟各國應將指令轉換成國內法，建議再關注成員國後續之發展。 | 1. 感謝委員建議。<br>2. 針對歐盟各成員國於 AI 相關應用之規範，後續研究上將持續關注。 |
| | 2. | 報告第 89 頁提到在歐盟數位服務法(Digital Service Act)的特定條件下，即使只是中介平臺，仍需與經銷商承擔相同義務，建議補充所敘特定條件為何；報告 79 頁提及美國紐約州 5 月頒布的 AI 伴侶新法，請補充說明該法所謂「伴侶」之概念。 | 1. 感謝委員建議。<br>2. 已依據委員建議，將歐盟數位服務法之規定以註解補充於第 93 頁。<br>3. 已依據委員建議，將美國紐約州之 AI 伴侶之原文及定義補充於第 87 頁以下。 |
| | 3. | 報告第 333 頁以下針對我國國內作法的建議，建議補充我國哪些法令需要調修，例如報告第 338 頁提到電子支付機構管理條例之法規調適，其他議題上亦可提出 | 1. 感謝委員建議。<br>2. 有關法制建議，補充於第 266 頁以下。未置於原我國國內作法建議部分，因該部分 |



本報告之智慧財產權歸屬於國發會

| | | | |
|---|---|---|---|
| | | 我國修法建議，以作為後續推動法規調適之參考。 | 屬敏捷法制整備的專題，未涉特定法令議題。 |
| 陳匡正教授 | 1. | 著作權之案例，除報告中提及2025年6月美國加州北區聯邦地方法院之判決外，在此判決之前與之後美國還有相關判決，例如2 月德拉瓦州之判決，認為訓練不構成合理使用，建議補充於報告。 | 1. 感謝委員建議。<br>2. 已依照委員建議補充2 月份德拉瓦州之判決於第5 頁。 |
| | 2. | 報告提及目前以函釋因應實務變化及需求，現行函釋是否能做到較彈性之調適機制？若法制需要彈性，是否會與「充分溝通」產生衝突？ | 1. 感謝委員建議。<br>2. 函釋具有通案解釋法令適用原則之效果，亦能針對個案提出主管機關看法，相較法令增修而言，是較彈性與及時之調適機制。但其作成仍應進行充分的意見蒐集，以評估函釋意見的妥適性，故並不會與「充分溝通」產生絕對的衝突。 |
| | 3. | 關於智慧機器人幕僚建議，請問美國聯邦法規與州法之間的關係，為相輔相成，還是需要溝通協調？ | 1. 感謝委員建議。<br>2. 聯邦法屬較上位之規範，州法則是實際落實之細部規範，為相輔相成之關係。 |



本報告之智慧財產權歸屬於國發會

| | | | |
|---|---|---|---|
| | 4. | 關於跨域資料的幕僚建議，其中「日本的資料信託功能認定指引3.0」，主要是安全醫療保健之個人資料(個資)，請問安全醫療保健之外的個資是否也適用此信託指引？ | 1. 感謝委員建議。<br>2. 安全醫療保健之個資於 3.0 版之前即已屬指引範圍，3.0 版係將健康及醫療個資納入規範。 |
| | 5. | 研討會有關「友善 AI 發展法制配套初探」問題 2：若需使用他人著作權內容，如何給予合理報酬以兼顧公益及私益。我認為不應以是否營利作為區分判斷，例如美國著重對社會及文化是否產生重要意義為判斷依據。另有關應選擇交易成本降至最低之方式（含違法成本），報酬是否有可能造成遵守法律的成本大於違法之成本，導致利用人選擇違法之方式？ | 1. 感謝委員建議。<br>2. 研討會紀錄係專家之意見呈現。與會專家學者提醒將來法制面解決方式，須評估交易成本與違法成本的落差，避免造成遵守法律的成本大於違法之成本，導致利用人選擇違法之方式。 |
| 章忠信兼任助理教授 | 1. | AI 是一種工具，對於設計、提供、訓練或使用 AI 的人會獲得好處，但若造成壞處且由廣大民眾承擔時，政府對於這類工具可能需有所規範，例如透明性義務，讓從中獲得利益之人承擔相應之責任，以保護公共利益。 | 1. 感謝委員建議。<br>2. 未來相關研究報告執行團隊將參考委員建議。 |
| | 2. | 有關國際判決之引述，似缺少研究團隊是否同意或比較我國法制部分。例如美國法院判決認為著 | 1. 感謝委員建議。<br>2. 本計畫之任務，有關國際法制觀測，主要 |



本報告之智慧財產權歸屬於國發會

| | | | |
|---|---|---|---|
| | | 作權法合理使用之標的必須為「合法資料」,對應我國著作權法第 52 條,合理使用之標的並未要求為合法資料，那是因為美國法制有衡平法(equity)之概念，也就是「法律不保護不乾淨之手」,但我國法制無此概念，兩國法制不同，美國法院的判決不能直接適用於我國。又對於侵權責任上，我國除了民事責任外還有刑事責任，與國外法規主要以民事責任賠償不同，建議在介紹國外法律或判決時，可比較我國法規是否相同，並做出相應評論。 | 在於法令動態的引述，而非特定議題的研究分析。若後續委託機關有為特定議題研析需求，將納入提出進一步的相應評論。 |
| | 3. | 關於著作權國際觀測，歐盟執委會、智慧局及歐洲議會皆有提出相關報告，歐盟執委會及智慧局報告中認為應作利益分配；歐洲議會於今年 7 月的報告則質疑 AIA 關於資料探勘的規定，認為把 AI 訓練比照資料探勘是錯誤的法律連結(legal mismatch)。另今年 11 月，德國法院認為 OpenAI 使用音樂訓練 AI 構成侵害 GEMA 所管理音樂著作之著作權，法院認為非合理使用，都值得我們關注，建議將相關報告及判決納入報告中。 | 1. 感謝委員建議。<br>2. 已依據委員建議修正補充歐洲議會之報告於第 29 頁，以及德國法院之判決補充於第 41 頁。 |



本報告之智慧財產權歸屬於國發會

| | | | |
|---|---|---|---|
| | 4. | 報告第 333 頁對國內之建議，偏抽象性規範，希望研究團隊進一步針對各國趨勢觀測與我國的差距，以及我國應如何因應，提供具體規範或建議作法。 | 1. 感謝委員建議。<br>2. 有關法制建議，補充於第 266 頁以下。未置於原我國國內作法建議部分，因該部分屬敏捷法制整備的專題，無關特定法令議題。 |
| 經濟部智慧財產局 | 1. | 有關美國 AI 著作權相關議題部分，報告第 14 頁至第 16 頁僅就 2025 年 6 月美國加州北區聯邦地方法院 Bartz 控告 Anthropic PBC 案之合理使用裁決進行說明，而同年月同法院於 Richard Kadrey 等 13 人控告 Meta 公司案亦有相關裁定，建議於報告補充上述 Meta 案之法院見解。 | 1. 感謝委員建議。<br>2. 已依據委員建議補充 Meta 案之判決於第 18 頁。 |
| | 2. | 歐洲議會 2025 年 7 月之委託內部政策部門進行研究之報告，探討生成式 AI 對歐盟著作權法的影響，並提出確保公平、透明與法律明確性的政策選項供未來改革參考,建議研究團隊予以補充。 | 1. 感謝委員建議。<br>2. 已依據委員建議補充歐洲議會報告於第 29 頁。 |
| | 3. | 就著作合理使用規範是否納入資料探勘,目前國際上權利人與 AI 產業仍意見分歧，例如澳洲於今年 10 月明確提到不會訂定資料探勘之合理使用，其他國家尚無 | 1. 感謝委員建議。<br>2. 針對國際上資料探勘與著作權之相關發展，後續研究上將持續關注。 |



本報告之智慧財產權歸屬於國發會

| | | | |
|---|---|---|---|
| | | 具體修法之意見。目前國際間雖有多起訴訟案例，但主動授權的案例也相當多，因此該議題於國際間仍在發展中，須持續觀察。 | |
| | 4. | 就著作權罰則部分，歐盟行政罰應為透明義務之違反，著作權侵害仍須回到各國著作權相關規定。國際間就是否針對 AI 運用著作權減輕刑事責任，屬於重大經貿議題，各國均遵守 WTO TRIPS 規定，目前尚無相關修正之法例。 | 1. 感謝委員建議。<br>2. 此建議與本報告撰擬方向一致。 |
| | 5. | 報告第 25 頁：「(2)自網路爬取資料時，僅得重製及擷取依法可獲著作權保護之內容」，語意不明，建議釐清。報告第 34 頁：「(二)2025 年 6 月英國議會通過資料使用及近用法新增 AI 商業資料透明度相關規範」一節，該法案主要係新增生成式 AI 業者之透明度要求，並未修正其著作權法合理使用等相關規定，建議予以補充。 | 1. 感謝委員建議。<br>2. 已依據委員建議調整語意。 |
| | 6. | 報告第 447 頁至第 448 頁：「(三)美國：部分州提出…而著作權局近期報告則有趨於嚴格管制之趨勢」一節，從美國著作權局第 3 份報告來看，雖尚無修正現行著 | 1. 感謝委員建議。<br>2. 已依據委員建議調整內容。 |



本報告之智慧財產權歸屬於國發會

| | | | |
|---|---|---|---|
| | | 作權法之趨勢，但亦似無趨向嚴格管制之建議，建議確認釐清。 | |



本報告之智慧財產權歸屬於國發會

前瞻數位科技法制政策變革趨勢研析/陳益智計畫主持.
-- 初版. -- 臺北市 : 國發會, 民114.12
面: 表，公分
編號:(114)012.0901（平裝）
委託單位：國家發展委員會
受託單位：財團法人資訊工業策進會
工業法制
555.4

題名：前瞻數位科技法制政策變革趨勢研析
委託單位：國家發展委員會
受託單位：財團法人資訊工業策進會
計畫主持人：陳益智
出版機關：國家發展委員會
電話：02-23165300
地址：臺北市寶慶路3號
網址：http://www.ndc.gov.tw/
出版年月：中華民國114年12月
版次：初版
刷次：第1刷
編號：(114)012.0901(平裝)



本報告之智慧財產權歸屬於國發會