編號：(113) 020.0902

前瞻數位科技法制政策變革趨勢研析

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 113 年 12 月

編號：(113) 020.0902

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：邱映曦

計畫期程：中華民國 113 年 4 月至 113 年 12 月

國家發展委員會

中華民國 113 年 12 月

目錄

摘要..... i

Abstract..... ii

國內數位法制調適與變革之評估.....1

項次 1. 焦點議題 1：AI 著作權相關議題國際趨勢.....1

壹、 背景說明.....1

貳、 近期國際發展趨勢重點.....2

一、 AI 著作權之立法發展 2

二、 現階段國際著作相關議題發展重點.....4

三、 趨勢發展重點歸納.....35

參、 我國法制概況.....37

肆、 小結.....40

項次 2. 焦點議題 2：AI 應用之消費者/使用者保護議題國際趨勢....48

壹、 背景說明.....48

貳、 近期國際發展趨勢重點.....51

一、 美國.....51

二、 歐盟.....67

三、 英國.....73

本報告之智慧財產權歸屬於國發會

四、 日本.....76
五、 趨勢發展重點歸納.....80
參、 我國法制概況.....85
肆、 小結.....89
項次 3. 焦點議題 3：AI 或演算法運用與勞工權益相關議題.....96
壹、 背景說明.....96
貳、 近期國際發展趨勢重點.....99
一、 美國.....99
二、 歐盟平臺工作指令（Platform Work Directive）.....108
三、 新加坡平臺工作者法（Platform Workers Act 2024）.....119
四、 趨勢發展重點歸納.....122
參、 我國法制概況.....127
肆、 小結.....133
項次 4. 焦點議題 4：AI 與個人資料保護及監管相關議題.....137
壹、 背景說明.....137
貳、 近期國際發展趨勢重點.....138
一、 歐盟.....138
二、 澳洲.....145
三、 日本.....148

本報告之智慧財產權歸屬於國發會

四、 韓國.....152
五、 新加坡.....160
六、 美國加州.....163
七、 OECD.....164
八、 趨勢發展重點歸納.....168
參、 我國法制概況.....174
肆、 小結.....178
項次 5. 法制政策綜整建議.....182
國際法制政策趨勢觀測雙月報.....199
項次 1. 四月雙月報.....199
壹、 資料治理.....199
一、 歐盟.....199
二、 英國.....205
三、 美國.....208
四、 聯合國.....209
貳、 AI 法制政策.....211
一、 歐盟.....211
二、 英國.....215
三、 美國.....217

本報告之智慧財產權歸屬於國發會

四、 新加坡.....224
五、 聯合國.....225
參、 數位監管.....230
一、 歐盟.....230
二、 英國.....238
三、 日本.....245
肆、 數位身分.....246
一、 歐盟.....246
二、 英國.....248
三、 澳洲.....250
伍、 資訊隱私.....251
一、 美國.....251
項次 2. 六月雙月報.....255
壹、 資料治理.....255
一、 歐盟.....255
二、 英國.....259
三、 美國.....262
四、 新加坡.....264
五、 中國大陸.....266

本報告之智慧財產權歸屬於國發會

六、 西班牙.....268

貳、 AI 法制政策.....270

一、 歐盟.....270

二、 英國.....272

三、 美國.....280

四、 日本.....306

五、 新加坡.....311

六、 德國.....313

七、 法國.....315

八、 經濟合作暨發展組織(OECD).....317

參、 數位監管.....322

一、 美國.....322

二、 法國.....327

肆、 數位身分.....329

一、 歐盟.....329

二、 英國.....330

三、 瑞士.....333

伍、 資訊隱私.....334

一、 歐盟.....334

本報告之智慧財產權歸屬於國發會

二、 英國.....336

陸、 競爭法制.....338

一、 義大利.....338

項次 3. 八月雙月報.....342

壹、 AI 法制政策.....342

一、 美國.....342

二、 英國.....353

三、 加拿大.....355

四、 韓國.....356

五、 OECD.....358

六、 中國大陸.....359

七、 歐盟.....363

八、 國際合作或會議.....367

貳、 數位身分.....369

一、 美國.....369

二、 中國大陸.....371

參、 數位政策.....372

一、 日本.....372

二、 歐盟.....377

本報告之智慧財產權歸屬於國發會

三、 美國.....379
四、 國際合作或會議.....380
肆、 資訊隱私.....382
一、 歐盟.....382
伍、 網路/資訊安全與韌性.....385
一、 比利時.....385
二、 日本.....387
三、 美國.....389
項次 4. 十月雙月報.....392
壹、 資料治理.....392
一、 日本.....392
二、 韓國.....393
貳、 AI 法制政策.....395
一、 美國.....395
二、 英國.....424
三、 日本.....427
四、 韓國.....429
五、 澳洲.....439
六、 中國大陸.....441

本報告之智慧財產權歸屬於國發會

參、 數位政策.....445

一、 美國.....445

二、 歐盟.....449

三、 英國.....451

四、 日本.....455

五、 韓國.....457

肆、 數位身分.....460

一、 美國.....460

二、 歐盟.....462

三、 日本.....464

伍、 資訊隱私.....465

一、 美國.....465

二、 歐盟.....476

三、 荷蘭.....480

四、 韓國.....482

五、 澳洲.....483

陸、 競爭法制.....489

一、 國際合作.....489

柒、 網路/資訊安全與韌性.....492

本報告之智慧財產權歸屬於國發會

一、 美國.....492
二、 韓國.....494
三、 聯合國.....498
捌、 智慧財產.....500
一、 韓國.....500
項次 5. 十二月雙月報.....502
壹、 資料治理.....502
一、 英國.....502
二、 韓國.....503
三、 中國大陸.....505
貳、 AI 法制政策.....508
一、 美國.....508
二、 歐盟.....527
三、 英國.....531
四、 韓國.....536
五、 新加坡.....537
六、 澳洲.....542
七、 中國大陸.....544
八、 國際合作.....547

本報告之智慧財產權歸屬於國發會

九、 經濟合作暨發展組織.....549

參、 數位政策.....552

一、 歐盟.....552

二、 英國.....553

三、 韓國.....555

肆、 數位身分.....559

一、 歐盟.....559

二、 日本.....561

伍、 數位監管.....562

一、 歐盟.....562

二、 韓國.....564

陸、 數位服務.....567

一、 日本.....567

柒、 競爭法制.....569

一、 國際會議.....569

捌、 網路/資訊安全與韌性.....572

一、 歐盟.....572

二、 中國大陸.....578

國內法規環境建構幕僚協助與新興議題之因應事宜.....583

本報告之智慧財產權歸屬於國發會

項次 1. 法制幕僚意見詢問.....583

壹、 歐盟人工智慧法案之重點與產業影響（2024 年 5 月 24 日）583

一、 背景.....583

二、 研析建議.....583

貳、 數位國家法制政策藍圖思考.....601

項次 2. 工作會議討論.....606

壹、 第一次工作會議.....606

貳、 第二次工作會議.....608

參、 第三次工作會議.....612

肆、 第四次工作會議.....613

伍、 第五次工作會議.....615

附錄一：國際趨勢觀測重點法案清單.....616

附錄二：期中審查會議記錄及意見回應說明.....625

附錄三：期末審查會議記錄及意見回應說明.....632

本報告之智慧財產權歸屬於國發會

摘要

本計畫主要係基於數位科技發展日新月異，觸發多元、跨領域與虛實整合之產業環境，帶動人與科技之緊密互動，亦促使法制環境需因應新興科技帶來之影響進行適當之調適。而近年來國際組織或主要國家均積極擘劃數位/智慧國家或區域之整體發展策略，包括配套之法制政策。考量數位科技創新應用持續衝擊國家整體法制架構，而國家發展委員會立於就國家整體發展政策之整合、協調、規劃與推動的角色，宜掌握國際法制政策脈動，以因應國內實務走向或需求，思考國內法制政策應投入之發展。

本年度計畫大致分為三個部分，「國際法制政策趨勢觀測雙月報」、「國內數位法制調適與變革之評估」、「國內法規環境建構幕僚協助與新興議題之因應」。基於閱讀便利性之考量，結案報告順序將優先置放「國內數位法制調適與變革之評估」為第一部分，再置放各期雙月報供參酌，最後為幕僚意見與會議相關資料。

於年度趨勢觀測部分，本年度國際 AI 法制政策發展，大致涵蓋 AI 監管規範、安全與個資保障、內容產製議題、消保與演算法歧視、國家安全與勞工權益等重要議題。其他數位法制政策層面，則涵蓋資料治理、數位身分、數位監管、資訊隱私等議題。至於國內法制調適部分，則擇定 4 項焦點議題，包括 AI 與著作權、AI 與消費者/使用者保護、AI/演算法與勞工權益及 AI 與個資保護及監管等議題，並就整體趨勢觀察，提出法制政策綜整建議。

本報告之智慧財產權歸屬於國發會

Abstract

Digital technology is developing at rapid pace and triggering a diversified, interdisciplinary, and integrated virtual-physical industrial environment. It also allows closer interaction between humans and technology, and requires the legal policies to be appropriated adjusted in response to the impact of emerging technologies. In recent years, international organizations or major countries have actively planned and proposed development strategies for digital and smart countries or regions, including the introduction of many supporting legal policies. Considering that the innovation and application of digital technology will continue to impact the country's overall legal framework, and the National Development Council（NDC）has the role of integrating, coordinating, planning and promoting the country's overall development policies, it is necessary to understand the development trends of international legal policies in order to respond to domestic practical needs and consider the development that domestic legal policies should focus on.

This project is divided into three parts：“Bimonthly report on international legal policy trends”, “Evaluation and analysis of the necessity of adjusting domestic digital regulations”, and “Assistance in analyzing the domestic regulatory environment in response to emerging issues.” Considering the convenience of reading, this final report will place anaylsis documents of “Evaluation and analysis of the necessity of adjusting domestic digital regulations” in the first part, followed by the bimonthly reports for reference, and finally the opinions on emerging topics and meetings records.

Based on the bimonthly report, the development of international AI laws and policies this year generally covers important issues such as AI regulatory standards, security and personal information protection, content

本報告之智慧財產權歸屬於國發會

production issues, consumer protection and algorithmic discrimination, national security and labor rights. Other aspects of digital legal policy development are including data governance, digital identity, digital supervision, and information privacy. As for the focus issues of domestic legal system adjustment, four issues have been selected, including “AI and copyright”, “AI and consumer/user protection”, “AI/algorithms and labor rights”, and “AI and personal information protection and supervision”. At the end, we observe the overall trend and put forward comprehensive legal policy recommendations.

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」委託研究計畫

國內數位法制調適與變革之評估

中華民國 113 年 12 月

國內數位法制調適與變革之評估

本分項研析，主要是透過本計畫對國際數位法制趨勢觀測，尤其本年度重點領域 AI 相關法制政策變化之觀察，搭配國內現階段數位法制政策發展著重之議題走向，與委託機關討論擇定年度 4 項焦點議題，進行年度國際重點發展趨勢之整理，並對應國內現行法制狀態進行分析，提出對於各焦點議題相關法制政策初步建議。並就整體年度國際趨勢觀測重點，及整體計畫研析過程之實務討論及觀察，提出對於我國法制政策推動方向之綜整建議。本年度擇定之焦點議題為 AI 與著作權、AI 與消費者/使用者保護、AI/演算法與勞工權益及 AI 與個資保護及監管，以下依序就各議題分析說明與就該議題之建議，最後則提出法制政策綜整建議。

項次 1. 焦點議題 1：AI 著作權相關議題國際趨勢

壹、 背景說明

人工智慧（AI）科技迎來契機，其生成內容隨著科技發展日新月異，時常可以看見民眾在網路上分享 AI 技術生成的圖像和影音。經濟部智慧財產局(下稱智慧局)近日陸續收到民眾詢問，是否能將 AI 生成的圖案用在馬克杯或衣服販售，或是將 Chat GPT 內容當作補習班教材，但發展訓練 AI 的資料與運用 AI 的產出，卻也衍生出智慧財產權爭議。2023 年即有媒體報導[1]指出--智慧局表示，目前已著手討論生成式 AI 的著作和專利權疑慮，以及 AI 訓練資料合理使用範圍，未來規劃建立指引，提醒民眾應注意侵權問題。

報導指出智慧局表示，AI 技術仍處萌芽階段，因無法確定訓練資料是否來自別人的作品，也無法判定 AI 公司是否獲得授權，或是可以轉授權給消費者商用，建議民眾將 AI 生成內容僅作為娛樂或自家使

[1] 使用生成式 AI 圖片販售？智慧局將研擬指引防侵權爭議 www.cna.com.tw/news/afe/202307160024.aspx , last visited 2024/07/10。

本報告之智慧財產權歸屬於國發會

用，以免衍生不必要的法律糾紛。至於 AI 演算法發展及成果的權利歸屬問題，現行的著作權法保障的主體為自然人或法人，若是單純由 AI 生成的圖像和文字，原則上並不受著作權法保護。

近年來國際上不乏 AI 著作權的政策、指引、立法例之討論及研議，並有相關爭議的訴訟發生，例如知名的圖庫平臺 Getty Images 提告 AI 科技公司非法使用其所屬圖片[2]，以及藝術家控訴畫作[3]或聲音遭侵權的案例。在 AI 開發、提供、使用過程，可能產生那些有關著作權之議題，例如被用以訓練 AI 之訓練資料的相關權利人，其並無法獲得任何該 AI 工具的收益，但所屬資料卻已被利用，有權益受損之虞，此處資料之利用是否符合合理使用範圍、如何界定、利益又應如何合理分配？若創作者將 AI 當成輔助工具，創作中有來自人類實際的思想和心力貢獻，應該到如何程度始可主張受法律保障？於各國政策、法令或指引中，近年來有相當之討論與發展，可作為我國後續法制政策評估之參考。

貳、 近期國際發展趨勢重點

一、 AI 著作權之立法發展

著作權法的立法目的，除「保護著作權」外，最終係希望透過權利的賦予，促進內容的創造，以造福人類社會。因此，著作權法制政策的思考面向，並非僅是對權利保護，而是兼顧權利保障及「公平、順利地使用著作權作品」間之平衡，從而為文化的發展做出貢獻。AI 與著作權的關係也需要基於上述平衡及法制建構之目的來考慮。故在 AI 發展之過程，首須處理的即是既有著作供 AI 訓練的合法使用問題，

[2] 控 AI 公司圖像工具侵權 Getty Images 擬開告，https://www.rti.org.tw/news/view/id/2156695 , last visited 2024/07/10。

[3] AI 與畫家智財訴訟案例系列 1：美國畫家控告 Stability 生成式 AI 工具著作侵權之程序判決出爐，https://iknow.stpi.narl.org.tw/post/Read.aspx?PostID=20448 , last visited 2024/07/10。

本報告之智慧財產權歸屬於國發會

此議題即明顯涉及如何在保障著作權人權益之基礎下，同時讓著作得以適切被利用以賦予科技發展合理之空間。例如知名的圖庫平臺 Getty Images 提告 AI 科技公司非法使用圖片，與藝術家、歌手控訴畫作和聲音遭侵權的案例，雖目前尚未定論[4]，但持續受到各界關注。

然而，目前各國或由於技術持續發展、或涉及諸多利害關係人、或對於推動 AI 發展或社會應用之共識仍在形成中，尚未有如何建構適切之著作權法制的共通原則。即便是已於著作權法賦予 AI 訓練資料合法空間的日本，其文化廳於 2024 年 3 月 15 日提出「關於 AI 和著作權的思考」[5]，便認為生成式 AI 涉之利害關係人眾多，以生成式 AI 而言，即包含、提供 AI 訓練內容之著作權人、AI 服務商、運用 AI 創作之權利人，故對相關利害關係人的溝通是重要的[6]。而除了日本文化廳點出之利害關係人外，於不同社會環節利用到最終生成內容之利用者，亦可能因為前面開發訓練或前手 AI 應用情形或合法性而受到影響，需要有相當之法制政策保障其利益。

本計畫觀測初步蒐集近年來之聯合國、歐盟、世界智慧財產權組織，以及美日等主要國家之倡議、法令、政策、指引資料，大致可以看出目前對於 AI 的著作權議題已進行實際立法之案例仍為少數。包括日本、新加坡等，目前多數國家或國際組織仍係以指引、政策來促進 AI 使用者等相關利害關係人之間建立溝通共識，但確實已有部分從可信賴 AI 之角度出，著手要求 AI 服務提供者應對 AI 生成內容進行標識、揭露，甚至登錄之立法案例。

---

[4] 同前 2。

[5] 文化廳發布「關於人工智慧和著作權的思考」，https://current.ndl.go.jp/car/218811 , last visited 2024/07/10。

[6] 日本文化廳「關於人工智慧和著作權的思考」(概要版)，頁 18，https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/pdf/94057901_01.pdf , last visited 2024/07/10。

本報告之智慧財產權歸屬於國發會

二、 現階段國際著作相關議題發展重點

就本次初步蒐集近年來之聯合國、歐盟、世界智慧財產權組織，以及美日等主要國家之倡議、法令、政策、指引資料，整理其所揭示、提出或關切之著作權保護、訓練資料利用或與 AI 生成內容相關的例如信賴保護揭露等議題之措施、政策或法令機制。說明如下：

(一)聯合國：AI 生成應有「可信任的內容與來源認證機制」，透過浮水印或標籤，讓使用者能識別、確認資料來源，並提供受影響補救方案

第 78 屆聯合國大會於 2024 年 3 月 21 日通過第一個與 AI 相關的決議，就推動「安全且值得信任的 AI（safe, secure and trustworthy artificial intelligence）」達成共識 [7]。此決議係由美國提出，並於聯合國大會得到澳洲、日本、新加坡、義大利及中國大陸等 120 多個聯合國會員國的支持。

該決議鼓勵會員國透過 17 項作法，促進安全且值得信任的 AI 系統，例如：制定及實施 AI 系統監管暨治理框架，以支持負責任的 AI 創新與永續發展；促進創新，鼓勵在設計、研發階段、部署及使用 AI 系統前，採取有效措施，例如：國際可互通的識別、分類、評估、測試、預防及抵減 AI 的風險；鼓勵納入問題回報機制，允許使用者與第三方於研發、測試及部署 AI 系統時，可透過數據為證據基礎加上資料之利用以支持採取循證決策方式回報 AI 的技術漏洞等問題；推行「制定並實施風險監控及管理、資料保護機制」，包括個人資料保護與隱私權政策、AI 影響評估；促進制定及實施有效、具國際互通性的「培訓及測試 AI 系統」框架、作法及標準，用以強化決策並減少演算法歧視。

---

[7] 第 78 屆聯合國大會決議，「安全且值得信任的人工智慧（safe, secure and trustworthy artificial intelligence）」共識, 2024 年 3 月 21 日, https://news.un.org/en/story/2024/03/1147831 , last visited 2024/07/10。

本報告之智慧財產權歸屬於國發會

其中並提及，對足以影響使用者最終決策的 AI 系統，在該 AI 系統的生命週期內，提供通知及解釋，並強化監管，以促進資料透明度、可預測性、可信度及可理解性，例如審查自動化決策及其過程，或提供「受自動化決策不利影響的人員」之替代或補救方案。而且針對內容生成部分，特別提及鼓勵研發及部署有效、易使用、國際可互通的技術工具、標準或作法，包括「可信任的內容與來源認證機制」，透過浮水印或標籤，讓使用者能識別、確認資料來源。將其獨立列出為 17 項重點之一。

(二)歐盟：通過首部人工智慧法案，未對於著作權議題有直接規範，但開發者必須尊重退出意願；經 AI 深偽技術處理的圖片、聲音、影片內容，則須明確標記

歐洲議會與歐盟理事會先前於 2023 年 12 月對人工智慧法草案內容達成暫時協議，歐盟理事會接續於 2024 年 5 月 21 日批准人工智慧法（Artificial Intelligence Act, AIA）並於 6 月 13 日正式頒佈，預計於 2026 年起實施。該法旨在促進私人和公共行為者在歐盟單一市場上開發及採用安全、值得信賴的 AI 系統，確保尊重歐盟公民的基本權利，刺激歐洲 AI 的投資及創新。同時為 AI 監管奠定全球的典範，採用以風險基礎之監理原則進行立法，即 AI 對社會造成危險的風險越高，受到管制就越趨嚴格[8]。

AIA 立法包含依風險分類 AI 系統，屬一般風險類別的 AI 系統只需履行較輕的透明度義務，而高風險類別的 AI 系統則必須獲得授權，且滿足法令要求及義務方能進入歐盟市場。例如，操縱認知行為和社交評分等目的之 AI 系統，由於其風險被歸類為不可接受，故將被禁止進入歐盟市場。至於不構成系統性風險的通用型 AI 模型將受到有限

[8] Council of the EU, Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI, 2024.05.21, https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/, last visited 2024/07/10。

本報告之智慧財產權歸屬於國發會

的限制，例如透明度的要求，但存在系統性風險的 AI 模型則必須遵守更嚴格的限制公司違反 AI 法之規定將受到裁罰－全球年營業額的一定百分比或者預定金額，而中小型企業和新創企業將按比例被處以行政罰鍰。

AIA 法案並未明文對於著作權議題有直接規範，但就透明度和基本權利之保護，則強力要求提供公共服務的組織於部署高風險 AI 系統之前，需要評估系統對基本權利之影響，其於前言第 49 點所列舉之基本權，即包括智慧財產權。除了前述規範，AIA 要求開發者必須遵守歐盟《數位單一市場著作權指令》，如果著作權人主動表示要「退出」（opt-outs），不想讓自己的創作被利用，事業就必須尊重其意願；而對於通用型 AI 系統及其模型須滿足透明度的義務要求，包含符合歐盟著作權法及發布其訓練資料的詳細摘要；如風險更高的一般用途型 AI 模型需另執行風險評估、風險回報機制。此外，經 AI 深偽（deepfakes）技術處理的圖片、聲音、影片內容，則須明確標記（label）[9]。

(三)WIPO：《生成式 AI：智慧財產權指引》建議透過內部管理制度的建立與契約權利義務分配，緩解包括 AI 著作侵權與歸屬爭議的潛在責任風險

世界智慧財產權組織(World Intellectual Property Organization，WIPO)於 2024 年 2 月 28 日公告《生成式 AI：智慧財產權指引》(Generative AI: Navigating Intellectual Property)[10]。該指引指出開發生成式 AI 的成本可能極高，大多數企業和組織都選擇採用第三方生成式 AI 工具或使用自己的資料對此類模型進行微調。由於目前已知確定運用案例，可看出生成式 AI 可以執行許多任務，但最佳運用案例仍在不斷發展，且因企業和組織的不同而有不同之發展與應用。開發人員授

[9] TaylorWessing, AI, the Artificial Intelligence Act & Copyright，https://www.taylorwessing.com/zh-hant/insights-and-events/insights/2024/05/ai-act-und-copyright , last visited 2024/07/10。

[10] WIPO, Generative AI: Navigating Intellectual Property, https://www.wipo.int/export/sites/www/about-ip/en/frontier_technologies/pdf/generative-ai-factsheet.pdf , last visited 2024/07/10。

本報告之智慧財產權歸屬於國發會

權其 AI 工具的條款包括商業機密和其他機密資訊的處理方式、產出的權利歸屬、賠償的取得可能性以及使用者透過實施對員工之監督及培訓以降低風險的責任等，皆可能存在很大差異，商業契約條款的最佳實踐及規範仍在發展中[11]。

該指引並盤點現行生成式 AI 在訓練及輸出過程，可能產生的機密資料保護、開源義務之違反、深偽應用之肖像權及聲音權、生成結果的權利保護風險等議題。其指出於智慧財產權而言，生成式 AI 應用衝擊最廣的莫過於著作權保護。對於訓練資料層面，由於一些生成式 AI 工具是使用從網路上抓取的資料進行訓練，其中可能包括著作權作品、個人資料、生物識別資料、商業資料或甚至抓取到有害、錯誤或非法之內容。故其訓練過程之資料抓取、下載和處理、經過訓練的 AI 模型及其輸出是否涉及侵權、智慧財產權所有者和 AI 開發者之間利益平衡的爭論仍在繼續[12]。

大多數國家的智慧財產權法是在 AI 出現之前制定的，對於利用生成式 AI 之產出是否享有智慧財產權、以及對於其應用是否應進行監管等依舊存在不確定性，僅部分國家有司法判決提供參考標準。因此指引建議產業應考量使用未侵權之智慧財產權標的進行訓練，或以契約約定侵權賠償之範圍，保留模型訓練記錄，減少出現第三方公司名稱、商標及著作。而 AI 產出之智慧財產權及所有權，目前亦尚無生成式 AI 所生成之內容是否受到智慧財產權保護之相關立法或修法，然即使 AI 輸出不受智慧財產權保護，亦可以透過契約明定所有權，並盡可能在未侵害智慧財產權的前提下使用生成式 AI 產出內容[13]。

[11] Id, Overview of issues, Differences in contractual terms.
[12] Id, Overview of issues, Training data issues.
[13] Id,IP rights in and ownership of AI outputs. Reuters, 2023.10.20.

本報告之智慧財產權歸屬於國發會

(四)美國：部分州法與聯邦法案提出 AI 生成內容的被訓練知情揭露、識別標示、通報登錄、公示閱覽、退出訓練權等義務，生成肖像、圖像、聲音須取得授權

1. 民主黨眾議員提出《生成式 AI 著作權揭露法案》（Generative AI Copyright Disclosure Act of 2024）

美國於積極投入生成式 AI 技術研發的同時，在與智慧財產領域的交互應用過程已衍生出許多關於著作權侵害之爭議，衝擊影視、音樂、創作、傳媒市場，牽動各產業諸多詞曲創作人、編劇、畫家、小說家、劇作家、出版商及新聞媒體從業人員的權益。例如新創公司 Anthropic 在開發自家 AI 模型時，即有未經原著作權人授權而擅自將音樂著作非法重製及散布等違法情事，遭到多家音樂唱片公司訴請損害賠償[14]；再如美國現有 8 家報社及媒體已向 OpenAI、Microsoft 提起訴訟[15]，主張其未獲明示授權或支付合理報酬，而直接利用數百萬篇受著作權保護的新聞文章作為 ChatGPTAI 聊天機器人之語言模型訓練。惟這類 AI 技術公司多以「合理使用原則」(Fair Use)作為抗辯事由，且聲稱係自可公開取得的網站摘錄內容乃受美國的著作權法相關規範之保障，並表明這些有價值的原始資料僅是被用於訓練模型而非作為內容的重製或改作。此外其亦主動釋出善意，願與新聞媒體業者達成內容配送及廣告的量身訂製協議。

為協助 AI 訓練以推動技術革新之需求，並兼顧著作權人的權益保障，使其得以知悉個人產製內容可用於推動 AI 技術

[14] Blake Brittain, Music publishers sue AI company Anthropic over song lyrics, https://www.reuters.com/legal/music-publishers-sue-ai-company-anthropic-over-song-lyrics-2023-10-18/ , last visited 2024/07/13.

[15] Jordan Novet, Eight newspaper publishers sue Microsoft and OpenAI over copyright infringement, CNBC, 2024.04.30, https://www.cnbc.com/2024/04/30/eight-newspaper-publishers-sue-openai-over-copyright-infringement.html , last visited 2024/07/13.

本報告之智慧財產權歸屬於國發會

成長，以尋求產業創新與創作保護兩者之平衡，美國民主黨眾議員 Adam Schiff 於 2024 年 4 月 9 日提出《生成式 AI 著作權揭露法案》（Generative AI Copyright Disclosure Act of 2024）[16]，主張應確保開發者能公平且負責任地使用 AI 技術，同時維護著作權人在邁入 AI 創造力時代之研究貢獻、著作權與知情同意權；並要求蒐集受著作權保護之內容進行模型訓練的 AI 技術公司必須履行向美國著作權局局長（Register of Copyrights）通報之事前程序，草案內容重點如下所述：

(1) 訓練資料來源公開透明化：建立訓練資料集或對該資料集進行任何重大變更的相關 AI 開發事業，應於正式推出提供公開使用的全新生成式 AI 工具系統前，向美國著作權局呈遞通知。提前揭露該模型訓練資料集中受著作權保護著作的完整清單列表，包含用來訓練或建置該系統所使用的任何受著作權保障內容等資料之管理概況，以及其所使用可公開存取資料的網址。此外該草案並規定對於過去任何已可公開存取的 AI 系統均具有溯及效力，倘現有既存 AI 模型的訓練資料集發生重大改變之情形時，亦必須及時向著作權局闡明使用著作物至訓練過程的受保護程度是否與過去採用相同標準。

(2) 問責機制之建立：對於違反上述事前資訊揭露聲明之透明化義務者，主管機關可根據個案違背情節與事業規模等因素綜合考量，處予罰鍰。

[16] US Congress, A bill of "Generative AI Copyright Disclosure Act of 2024", H.R.7913, https://www.congress.gov/bill/118th-congress/house-bill/7913/text , 2024.04.09, last visited 2024/07/10.

本報告之智慧財產權歸屬於國發會

(3) 建置公共資料庫：將建立一個由各事業向著作權局提交的通知聲明、著作物清單等證明文件所匯集而成的線上公共資料庫，可供公眾隨時進入瀏覽檢視。

2. 眾議院議員和 AI 工作小組提出《保護消費者免受人工智慧欺騙法草案》（Protecting Consumers from Deceptive AI Act）

考量現今深偽已造成眾多社會問題，包括對消費者之欺騙、國家安全之威脅、市場秩序混亂、對未成年人之傷害等社會問題及威脅，因此，美國眾議院議員和 AI 工作小組於 2024 年 3 月 21 日提出《保護消費者免受人工智慧欺騙法草案》（Protecting Consumers from Deceptive AI Act[17]），擬藉由制定識別及標記標準，並要求 AI 生成軟體開發商及平臺揭露 AI 所生成的內容，以解決上述社會問題。

該法案除要求由美國國家標準與技術研究院（National Institute of Standards and Technology, NIST）推動制定識別及標記 AI 生成內容的標準，包括透過針對出處之詮釋資料（metadata）、浮水印（watermarking）和數位指紋（digital fingerprinting）等技術措施外，並要求生成式 AI 開發者確保由此類應用程式創建或實質修改的音訊或視訊內容包含（以人類獨立感官可能或可能無法感知的方式）應用程式名稱和版本、創建或修改此類內容相關的日期和時間。另應制定並實施合理措施，以防止上開揭露資訊被刪除或以其他方式竄改。並要求該法涵蓋之線上平臺的提供者合作，協助此類提供者識別及存取揭露資訊，確保程式使用者能夠在詮釋資料中納入有關資訊。同時進一步，要求數位平臺就提供使用者

[17] US Congress, A bill of "Protecting Consumers from Deceptive AI Act", H. R. 7766, 2024.03.11, https://www.congress.gov/bill/118th-congress/house-bill/7766/text , last visited 2024/7/10.

本報告之智慧財產權歸屬於國發會

存取的音訊或視訊內容，應清楚且明顯地揭露該法要求應揭露之資訊，且不得刪除此類揭露資訊內之任何訊息[18]。

3. 田納西州：《確保肖像、聲音和圖像安全法案》要求第三方若利用生成工具重製肖像、聲音或圖像應得本人之事前同意

2024 年 3 月 21 日田納西州州長 Bill Lee 簽署《確保相似聲音和圖像安全 (ELVIS) 法案》(Ensuring Likeness Voice and Image Security (ELVIS) Act)，這是該州首次立法保護詞曲作者、表演者和音樂行業專業人士的聲音免受 AI 濫用的影響。雖然田納西州現有的法律保護姓名、圖像和肖像，但它並沒有具體解決新的個人化生成式 AI 模仿人類之問題，導致用戶以他人的圖像和聲音製作未經授權的偽造作品，不但誤導作品之接觸者，也導致藝術家和音樂家面臨剝削，侵害其作品的完整性，甚至導致其身分、性格特色、喜好等相關資訊被不當的竊取。《ELVIS 法案》成為首部保護音樂家或藝術家免受 AI 生成或實質修正之內容影響的法律[19]。

此處之 ELVIS 法案為美國首部禁止他人未經授權使用或重製權利人的聲音以供訓練 AI 模型或生成深偽內容所制定之州法[20]，本法修訂田納西州現行的 1984 年《個人權利保護法》（Personal Rights Protection Act, PPRA），該法原先之制定及通過部分是為在貓王 1977 年去世後擴大他的公開權，然而保護並未延伸至對個人聲音的使用。本次修訂將個人的實際或模擬「聲音」添加到已受 PPRA 保護的個人特徵清單中。同時進一步規定，明知該聲音或肖像的使用未經該個人授權，

[18] Id, SEC. 3. (b)(1)、(2).

[19] TN Governor's Office, PHOTOS: Gov. Lee Signs ELVIS Act Into Law, https://www.tn.gov/governor/news/2024/3/21/photos--gov--lee-signs-elvis-act-into-law.html , last visited 2024/07/10.

[20] 此處田納西州之 ELVIS Act 已於 2024 年 7 月 1 日生效實施，https://digitalpolicyalert.org/change/8698-the-ensuring-likeness-voice-and-image-security-act-of-2024-hb-2091-in-tennessee , last visited 2024/07/10。

本報告之智慧財產權歸屬於國發會

而有以下情況者，表演人、唱片公司可以提起訴訟尋求補救措施，法院並可對行為人判處監禁或處以罰款；不過基於憲法第一修正案之保護範圍，對個人姓名、照片、聲音或肖像的使用，於符合著作權法之要件下，仍被視為根據著作權權法的合理使用[21]，包括，所使用之內容為新聞、公共事務資訊、體育廣播資訊；或為用於評論、批評、學術研究或模仿目的；或屬於視聽作品中之個人表現，除非該聲音作品創作之目的即在意圖形成該作品係聲音所屬本人實際參與錄音之錯誤印象；或該創作僅為短暫或偶然的；或係用於廣告應用等。此外，本次修訂亦針對二種類型之行為，被認為是違法行為而需負擔民刑事責任：

(1) 出版、表演、發行、傳播或以其他方式向公眾提供個人的聲音或肖像，但明知該聲音或肖像之使用未經所涉個人之授權者。然而若該聲音或肖像屬於未成年人或死亡者，則應係指未經具適當權利之人授權。

(2) 發行、傳輸或以其他方式提供演算法、軟體、工具或其他技術、服務或設備，其主要目的或功能是製作特定的、可識別的個人的照片、聲音或肖像。且行為人明知該發行、傳輸或以其他方式製作照片、聲音或肖像之行為，並未經過個人授權，或若為未成年人或死亡者，則未經具適當權利之人授權。

4. 美國著作權局(US Copyright Office)

[21] Holland & Knight LLP, First-of-Its-Kind AI Law Addresses Deep Fakes and Voice Clones, https://www.jdsupra.com/legalnews/first-of-its-kind-ai-law-addresses-deep-9596588/ , last visited 2024/07/10.

本報告之智慧財產權歸屬於國發會

(1) 發布包含 AI 生成資料的著作權登記指引[22]，重申 AI 生成著作可登記與否重要的是人類的創意控制程度，申請人應披露 AI 生成內容的包含情況，並提供人類作者對該作品貢獻的簡要說明。

美國著作權局，為澄清其審查和登記包含使用 AI 技術生成內容的作品的做法，於 2023 年 5 月發布「著作權註冊指引：含有 AI 生成內容之作品(Copyright Registration Guidance:Works Containing Material Generatedby Artificial Intelligence)」。

由於 AI 技術透過對大量現有的人類創作作品進行「訓練」，並利用這些訓練來生成新內容，美國著作權局提及在 2018 年即已收到了一份表明該作品是由運行在機器上演算法自主創建的登記申請，因該作品沒有任何人類創作，因此拒絕申請。而近期又出現包含人類創作元素與 AI 生成圖像結合的作品的登記申請案例，這些申請將 AI 技術列為作品的作者或共同作者，或在作者創建或致著作權局說明部分中包含聲明，表明該作品是由 AI 製作或協助製作的。其他申請人則未披露包含 AI 生成內容，但在作品標題或存檔的「致謝」部分提及了 AI 技術的名稱。因此針對 AI 所產生的內容是否受到著作權保護的問題，以及包含人類創作和 AI 生成內容的作品是否可以登記與應提供的登記資訊問題。

美國著作權局於該指引表明，一部由人類創作文字與 AI 服務 Midjourney 生成圖像組合而成的圖畫小說構成了可著作權保護的作品，但單獨的圖像本身則不能受到著作

[22] US Copyright Office, Copyright Registration Guidance:Works Containing Material Generated by Artificial Intelligence,37 CFR Part 202, https://www.govinfo.gov/content/pkg/FR-2023-03-16/pdf/2023-05321.pdf, , last visited 2024/10/17.

本報告之智慧財產權歸屬於國發會

權保護。該局一直要求作品必須是人類作者的產物，它不會登記在沒有人類作者的任何創造性輸入或干預的情況下由機器或純粹的機械過程隨機或自動運行產生的作品。任何登記申請案，先會被確認「作品」是否基本上是人類創作的，電腦（或其他設備）僅僅是輔助工具，還是作品中的傳統創作元素（文學、藝術或音樂表達或選擇、排列等元素）實際上是由機器而非人類構思和執行的？在涉及 AI 生成內容的作品中，著作權局將考慮 AI 的貢獻是否屬於「機械複製(mechanical reproduction)」，還是作者有自身「原創的心智概念(original mental conception)，並賦予其可見形態」。答案將取決於具體情況，特別是 AI 工具如何運作以及如何用於創作最終作品。當一項 AI 技術僅接收來自人類的提示並生成複雜的書面、視覺或音樂作品，例如指示 AI 文字生成技術「寫一首關於著作權法的詩，以威廉·莎士比亞的風格」，可以期待系統生成可識別為詩的文字，提到著作權並且類似莎士比亞的風格，但 AI 技術決定押韻模式、每行中的單詞以及文字結構，而不是由人類使用者決定。使用者並不對這些系統如何解釋提示和生成內容擁有最終的創意控制，這些提示更像是委託藝術家的指示—它們確定使用者希望描繪的內容，但機器決定如何在其輸出中實現這些指示。

當由 AI 技術確定其輸出的表達元素時，生成的內容就不是人類創作的產物，必須在登記申請中聲明放棄。不過，美國著作權局仍於指引中提醒在其他情況下，包含 AI 生成的作品也可能包含足夠的人類創作，以支持著作權主張。例如，人類可能以足夠具創意的方式選擇或排列 AI 生成內容，使得整體結果構成一部原創著作。或者，一位藝術家可能修改原本由 AI 生成的內容，使得這些修改符合著作權保護標準。

本報告之智慧財產權歸屬於國發會

美國著作權局認為作者長期以來一直使用創作工具來創作作品，或重新塑造、轉化或改編他們的表達性著作。例如，視覺藝術家使用 Adobe Photoshop 編輯圖像、音樂藝術家在創作錄音時可能會使用吉他效果器等效果。在每種情況下，重要的是人類對作品表達的創意控制程度，以及「實際形成」創作元素的程度。

該指引要求申請人在提交登記的作品中有責任披露 AI 生成內容的包含情況，並提供人類作者對該作品貢獻的簡要說明。使用標準申請表，在其中識別作者並在「作者創建」欄位中提供簡要說明，描述人類所做出的著作貢獻。例如，將 AI 生成文字納入更大文字作品中的申請人應該聲明文字作品中人類創作的部分。而創意地排列人類和非人類內容的申請人應在「作者創建」欄位中填寫：「由作者創建的『描述人類創作內容』的選擇、協調和排列，以及由 AI 生成的『描述 AI 內容』」。申請人不應僅因為在創作過程中使用某項 AI 技術而將其列為作者或共同作者。

前述申請應明確排除並非微不足道的 AI 生成內容，於申請表的「其他」欄位中說明排除的 AI 生成內容的簡要描述。而已處理並導致登記的申請，申請人應透過提交補充登記來更正記錄。申請人應在「作者創建」欄位描述人類作者所貢獻的原始內容，在「排除內容/其他」欄位聲明放棄 AI 生成內容，並完成「新增內容/其他」欄位。只要有足夠的人類著作權，著作權局將發出新的補充登記證書，其中包含針對 AI 生成內容的聲明放棄。未補充的申請人，如果被美國著作權局發現對其評估可登記性至關重要的資訊「完全被遺漏或存在疑問」，則可能採取措施取消該登記。如果法院認為申請人有提供不準確資訊的故意行為，則可能會根據《著作權法》第 411(b)條忽略該登記。

本報告之智慧財產權歸屬於國發會

(2) 美國著作權局對 AI 系統引發的著作權法和政策問題進行研究、徵詢

2023 年 8 月著作權局為幫助評估該 AI 著作領域的立法或監管措施是否必要，發布「著作權與人工智慧議題徵詢通知 (Copyright Office Issues Notice of Inquiry on Copyright and Artificial Intelligence)」[23]。對外尋求對包括涉及使用受著作權保護的作品來訓練 AI 模型的問題、適當的透明度和披露水平受著作權保護的作品的使用以及 AI 生成的輸出的法律地位等問題的意見。其提出的問題主要包括一般問題、訓練資料來源、構成合理使用的情況、揭露與通知的義務、既有權利的保護、AI 侵權的舉證、AI 生成的識別區分等等。例如：

I. 關於立法政策

對立法政策而言，法律保護對促進生成式 AI 技術和系統發展是否必要？現有針對運行生成式 AI 系統程式碼的著作權保護是否提供足夠激勵措施？

II. 關於 AI 訓練資料

用於訓練 AI 模型的著作權保護內容有哪些類型？這些內容是如何收集和策劃的？ AI 模型開發者如何獲取其模型訓練所需的內容或數據集？訓練內容在多大程度上是由第三方實體（如學術研究人員或私營公司）首先收集的？AI 模型開發者在訓練完成後是否保留某些或所有訓練內容？保留這些內容是出於什麼目的？在訓練 AI 模型時如何使用和/或複製訓練內容？

[23] US Copyright Office, Copyright Office Issues Notice of Inquiry on Copyright and Artificial Intelligence, https://www.copyright.gov/newsnet/2023/1017.html , last visited 2024/10/17.

本報告之智慧財產權歸屬於國發會

從訓練過程中獲得的推論是如何存儲或在 AI 模型中表示的？

AI 模型是否能夠「忘記(unlearn)」從特定訓練內容中獲得的推論？如果可以，這在經濟上是否可行？除了重新訓練模型外，還有其他方式可以「忘記」來自訓練的推論嗎？在無法訪問基礎數據集的情況下，是否能夠確定某個 AI 模型是否是在特定訓練內容上進行過訓練？

III. 關於訓練 AI 的合理使用

如何評估使用受著作權保護作品來訓練 AI 模型的「目的和性質」？需要分析的相關用途是什麼？不同的訓練階段，例如預訓練和微調，是否在合理使用有不同的考量？

在訓練數據集中或用於訓練生成式 AI 模型時使用受著作權保護的內容可能是出於非商業或研究目的。如果 AI 模型或數據集後來被調整為商業用途，合理使用分析應如何適用？如果這些非商業或研究用途的資金來自營利的 AI 系統開發者，這是否會有所不同？

生成式 AI 模型的開發者在訓練中使用多少量的訓練內容？用於訓練 AI 模型的內容量是否會影響合理使用分析？如果會，具體如何影響？如何衡量用於訓練 AI 模型的受著作權保護作品對潛在市場或價值的影響？

IV. 關於被訓練資料的衡平

著作權擁有者是否應該明確同意（選擇加入）其作品用於訓練內容，或者應該提供他們反對（選擇退出）

本報告之智慧財產權歸屬於國發會

的方式？著作權擁有者是否應該對所有使用受著作權作品來訓練 AI 模型的情況要求同意，還是僅限於商業用途？如果採取「選擇退出」的方式，對於反對其作品用於訓練的著作權擁有者，這一過程將如何運作？是否存在技術工具可以促進此過程？考慮到用於訓練的作品數量，提前獲得著作權擁有者的同意是否可行？如果反對意見未被尊重，應提供哪些救濟措施？在人類創作者不擁有著作權的情況下—例如因為他們已經轉讓或因為該作品是為雇主創作—他們是否應該有權反對 AI 模型基於其作品進行訓練？如果是，這樣的系統將如何運作？

自願集體授權方案是一種可行或理想的方法嗎？是否存在適合提供這些許可的集體管理組織，以及是否存在法律或其他障礙阻止這些組織履行此角色？應否考慮法定或其他變更，例如反壟斷例外，以促進集體許可的談判？是否應考慮建立強制性授權制度？如果是，這樣的制度應該是什麼樣子？許可應涵蓋哪些活動、哪些作品將受到許可，以及著作權擁有者是否能夠選擇退出？如何設定、分配、報告和分配版稅率和條款？

為讓著作權擁有者確定其作品是否被使用，AI 模型開發者是否應被要求收集、保留並披露有關用於訓練其模型內容的記錄？培訓數據集創建者是否也應有類似義務？應要求什麼程度的具體性？對於整合第三方模型的 AI 系統開發者，有哪些義務（如果有）？對於 AI 模型或系統開發者、創作者、消費者或其他相關人而言，此類記錄保存系統將帶來什麼成本或其他影

本報告之智慧財產權歸屬於國發會

響？是否應該通知著作權擁有者其作品已被用於訓練 AI 模型？

V. 生成結果的記錄、區別與保護

在什麼情況下，人類使用生成式 AI 系統時應被視為該系統所產生內容的「作者」？是否需要對《著作權法》進行修訂，以澄清人類著作要求或提供額外標準，以決定包括 AI 生成內容在內的內容何時受到著作權保護？如果保護是可取的，那麼它應該是形式上的著作權還是單獨的新型權利？如果是後者，那麼對於 AI 生成內容而言，其保護與著作權相比應在哪些方面有所不同？

是否存在或者應當設立防止 AI 系統產生模仿人類創作者藝術風格輸出的保護（例如，一個 AI 系統生產「以某位特定藝術家的風格」創作視覺作品）？誰應符合此類保護資格？應採取何種形式？

AI 生成輸出能否涉及現存受著作權保護作品專屬權利，例如重製權或衍生作品權利？如果可以，在什麼情況下會如此？實質相似性測試能否充分解決基於生成式 AI 系統輸出的侵權索賠問題，或者需要其他標準嗎？如果開發者未維持或提供其所用培訓內容記錄，那麼著作權擁有者如何證明抄襲要素（例如通過證明接觸過受著作權保護作品）？如果發現 AI 生成內容侵犯受著作權保護作品，那麼誰應承擔直接責任或間接責任(Secondary Liability)—生成式 AI 模型開發者、整合該模型系統開發者、系統最終用戶還是其他方？

法律是否應要求將 AI 生成內容標籤化或以其他方式公開識別為 AI 生成？如果是，那麼這一要求應適用

本報告之智慧財產權歸屬於國發會

在哪種情境下，以及它應如何運作?誰應負責將某項作品識別為 AI 生成？是否存在標籤化或識別要求方面的技術或實際障礙？不標示特定作品或移除標籤將面臨什麼後果？現在有哪些工具存在或者正在開發，用以識別 AI 生成內容，包括由標準制定機構提供? 這些工具準確度如何？有哪些限制？

(3) 美國著作權局對 AI 系統引發的著作權法和政策問題發表研析以數位複製為主題的第一部分報告

美國著作權局在分析 AI 引發的版權法和政策問題的意見徵詢結果後，於 2024 年 7 月 31 日，以數位複製物(digital replicas)主題，發布「著作權與人工智慧分析人工智慧引發的著作權法和政策議題」(Copyright and Artificial Intelligence analyzes copyright law and policy issues raised by artificial intelligence)報告的第 1 部分[24]。該報告針對以數位方式創建或操縱，錯誤的描繪特定個人的真實影像、圖像或音訊的數位複製物[25]激增，產生的實際或潛在危害，包括人們對表演者等藝術家將失去工作或收入的擔憂，認為現有法律的保護存有差距，建議國會頒布新的聯邦法律，保護所有個人免遭未經授權數位複製品的故意散佈。

美國著作權局認為雖然著作權保護原創的著作，包括賦予著作權人重製和衍生的權利，然而著作權並不保護個人的身分。透過擷取有著作權作品或對其進行修改（例如將某人的臉疊加到視聽作品上，或模擬其聲音唱出音樂作品的歌詞），所產生的數位複製品，除非被描繪的個人是

[24] US Copyright Office, Copyright Office Releases Part 1 of Artificial Intelligence Report, Recommends Federal Digital Replica Law , https://www.copyright.gov/newsnet/2024/1048.html, last visited 2024/10/17.
[25] Id, at 2.

本報告之智慧財產權歸屬於國發會

著作權作品的擁有者，可能提出侵害著作權的主張，否則僅是他們的形象或聲音的複製並不構成著作權侵權[26]。

但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。某些州目前並未提供公眾形象權和隱私權，有些州則僅保護特定類別的個人、多個州要求證明個人的身份獨特且知名具有商業價值，而那些提供保護的州可能將保護範圍限制於聲音而非數位複製物。這些法律並未解決非商業用途造成的損害，包括在網路環境中特別普遍的深偽色情。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居住地或未經授權使用發生地[27]，因此應該於聯邦層級建立法律規範。

而此法律規範可以借鑑著作權法中的間接責任(Secondary Liability)原則，如果被告「在知曉侵權活動的情況下，誘導、導致或實質性促成他人的侵權行為」，則可以課予其助長侵權行為的共同侵權責任。如果被告「直接從侵權中獲利，並有權利和能力監督直接侵權者」，則可能會被認定為間接責任。此外，如果被告「散佈一種設備，目的是促進其用於侵權著作權的行為，並且有明確的表達或其他積極措施來促進侵權」，則可能會對誘導侵權負責。這部分大多有關於傳輸、儲存、託管或連接用戶內容的線上服務提供者，且在許多情況下其最能防止這些複製品造成持續的傷害。例如，散佈者可能是匿名或無法聯繫的，這使得無法對他們採取直接行動，無論是非正式的還是透過法院訴訟[28]。

[26] Id, at 17.
[27] Id, at 23.
[28] Id, at 36.

本報告之智慧財產權歸屬於國發會

美國著作權局認為一旦線上服務提供者(online service provider, OSP)知道這些複製品是未經授權的，應該鼓勵其協助移除這些複製品，並在這樣做時免於承擔責任。同時該局也認為結合適當的安全港的通知與移除系統，類似於《數位千禧年著作權法》(DMCA)鼓勵著作權擁有者和 OSP 合作「檢測和處理著作權侵權」，為通過為符合條件的 OSP 提供對其用戶所犯侵權行為的責任豁免，可能是一種有效的方法[29]。

(4) 美國著作權局對藝術風格的保護看法

AI 系統引發的著作權法和政策問題發表研析以數位複製為主題的第一部分報告中，美國著作權局也提到藝術風格的保護。報告提及作家公會在 2024 年國會聽證會上表示，「藝術家和創作者花了一生時間磨練和精煉技能，如今卻可以被生成式 AI 模型瞬間複製其辛勤工作的複製品。」。美國著作權局認為，考慮到 AI 生成作品的正確歸屬和利用問題，對於藝術風格的保護需求日益增加，應該為這類損害提供適當的救濟。但亦表示著作權法在這一領域的適用性有限，因為它不保護藝術風格作為作品的獨立元素。對風格的著作權保護將與美國著作權法第 102(b)條的思想/表達二分法不一致。此外，在大多數情況下，藝術家風格的元素無法輕易地與特定的基礎作品分開劃分和定義[30]。

不過，由於美國《著作權法》可能在「以某藝術家風格」請求的輸出中提供救濟，如果該輸出不僅複製藝術家的風格，還複製特定作品中可保護的元素，或者存在使用

[29] Id, at 38.
[30] Id, at 53-54.

本報告之智慧財產權歸屬於國發會

藝術家自身作品訓練 AI 系統以生成模仿其風格材料的情況，可能支持侵權主張。另外，在其他法律框架中可能找到對風格模仿的有意義保護，例如美國聯邦貿易委員會（FTC）在其評論中表示：「模仿創作者的寫作風格……也可能構成不公平競爭的方法或不公平或欺騙性的行為，特別是當著作權違規欺騙消費者、利用創作者的聲譽或降低其現有或未來作品的價值、揭露私人資訊或以其他方式對消費者造成重大損害時。」，因此在不將類似財產權利擴展至風格本身的政策原因考量下，目前美國著作權局並不建議在其提議的聯邦數位複製物法下，將風格納入受保護主題，除非現有保護措施被證明不足[31]。

(五)日本：賦予 AI 資料訓練合法授權，但仍不得「不正當損害著作權人利益」

為提高機器學習的資料取得與利用之便利性，日本於 2019 年即修正其著作權法，於第 30 條之 4 規定，在下列情況下，如果目的不是為了自己或他人感受作品中表達的想法或感情，在根據作品的種類、目的和使用方式，不會不當損害著作權人利益的情況下，可以在必要的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（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 。此外，日本為推動 AI 發展並因應相關著作權疑義，於近年接續提出相關研析、政策與指引。說明如下：

1. 日本文化廳：文化審議會著作權分科會法制度小組會議提出「關於人工智慧和著作權的思考」 指出，創造性的 AI 生成

[31] Id, at 55-56.

本報告之智慧財產權歸屬於國發會

結果仍受保護，訓練 AI 無須授權的訓練但仍不得「不正當損害著作權人利益」，且提供者負有防止生成結果侵權之義務。

日本的著作權法力求在「保護著作權及其他權利」與「公平、順利地使用著作權作品」之間取得平衡，從而為文化的發展做出貢獻。AI 與著作權的關係也需要基於上述平衡和目的來考慮[32]。日本區別「人工智慧開發/學習階段」和「生成/利用階段」來討論著作權議題，認為使用著作權素材的行為不同，相關著作權法的規定也不同。分別包括：蒐集並複製受著作權保護的作品作為訓練數據，以創建訓練數據集、使用該數據集進行學習開發 AI（訓練模型）；而生成/利用階段則包括：利用 AI 生成圖像等、上傳並公開生成的圖像等、生成的圖像等的複製品（插圖集等）銷售。另外，需要單獨考慮 AI 產品（AI 生成的內容）是否屬於「著作權作品」[33]。

(1) 資訊分析非感受目的的行為可以在未經著作權人同意的情況下實施

關於利用著作權作品創造 AI（訓練模型），文化廳認為對於非感受目的的行為，即使這種行為可以在未經著作權人同意的情況下實施，但一般認為這不會損害著作權人的經濟利益，因此依日本著作權法第 30 條之 4 屬「非感受目的」的運用，原則上無需著作權所有者的許可即可進行此操作，情況包括：(1) 用於測試與錄音、錄影或其他作品使用相關的技術的開發或應用；(2) 資訊分析（從大量作品和其他大量資訊、構成資訊的語言和聲音），提取

[32] 文化審議会 著作権分科会 法制度小委員会「AI と著作権に関する考え方について【概要】」, https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/pdf/94057901_01.pdf , last visited 2024/07/10。

[33] 同前註，頁 3。

本報告之智慧財產權歸屬於國發會

與影像和其他要素有關的資訊，並進行比較、分類和其他分析。

(2) 無須授權的訓練行為仍然不得「不正當損害著作權人利益」

所謂「不正當損害著作權人利益」的情況，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等。但有無「不正當損害他人利益」的情況是創作者及其他權利人、從事 AI 開發的企業、AI 使用者等的擔憂。在生成式 AI 的基礎模型的額外學習（微調）中，故意「過度擬合」，以產生與著作權作品相似的作品（具有共同的創意表達），或蒐集資料（受著作權保護的作品），用於輸入生成 AI，用於某些搜尋增強生成（Retrieval-Augmented Generation, RAG），或針對特定創作者的 AI 學習，應被認定為非屬「非感受目的」。

(3) 著作權人作品之使用是否與市場產生衝突是判斷有無「不正當損害著作權人利益」的重要因素

第 30 條之 4 但書之適用，應視著作權人之作品之使用是否與市場產生衝突，著作權人未來的著作權需要從「是否阻礙產品的潛在銷售管道」的角度，綜合考慮「技術的進步」和「著作權素材用途的變化」等各種情況。如果網路上的資料（資料庫作品）以可用於資訊分析的形式有償提供，則該資料庫作品（其創意表達得到認可的某種資訊集合）可能屬於無需付費即可使用的情況。於某些情況，例如已採取技術措施（網站上的「robots.txt」文件和 ID 中的說明、限制措施爬蟲訪問網站，透過密碼認證進行 AI 學習複製以防止複製 AI 學習著作權作品等），因此需要「對某個網站（AI 學習等）上的數據進行資訊分析」，

本報告之智慧財產權歸屬於國發會

其中若受著作權保護的作品已被組織成可用於各種目的的形式，並計劃在未來出售，則規避上述技術措施而複製用於 AI 學習的資料庫的著作權作品的行為應屬使著作權人利益受到不當損害之情形[34]。

(4) 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，應負侵權責任

如果 AI 開發者或 AI 服務提供者在明知該網站包含盜版或其他侵權之作品複本的情況下仍從該網站蒐集學習數據，由此產生的 AI 即可能造成對著作權的侵權，相關企業將面臨被追究法律責任的可能性。權利人將向企業提供哪些網站發布侵權複本等資訊，將使得企業能夠識別盜版網站並改進學習數據的蒐集。嚴禁明知網站發布盜版或其他侵權內容而蒐集學習資料。若開發 AI 的企業明知學習數據是盜版等而蒐集學習數據，則可能會因產生的 AI 而承擔著作權侵權責任。

(5) 生成式 AI 於開發/學習階段有使用受著作權保護的作品，則 AI 使用者應被認定為有運用到既有作品

即使不清楚學習資料是否包含與產品相似的現有作品，權利人也應該知道 AI 開發者與服務使用者是否有機會能夠存取其現有作品或產品，而可以推定其存在與現有作品間之依存關係（即接觸可能性）。此外，如果現有的受著作權保護的作品是在生成式 AI 的開發/學習階段提供學習，即使 AI 使用者不知道現有的受著作權保護的作品，通常也會被認為存在依存關係[35]。

[34] 同前註，頁 9。
[35] 同前註，頁 12。

本報告之智慧財產權歸屬於國發會

(6) AI 開發者應負有移除侵權作品、限制侵權指令等以技術手段降低侵權風險之義務

當 AI 開發者作為行為人而應對產品的創作和使用所造成的著作權侵權負責時，其可能需要從用於開發生成侵權作品之訓練資料集中，提取被侵權的之著作權作品，使之可以被請求移除（處置）。於創造侵權素材的 AI，後續可能會導致進一步創造侵權作品的情況下，可以要求 AI 開發者或 AI 服務提供者採取必要的措施，例如，對 AI 進行技術限制，包括（1）不產生回應特定提示輸入的資料等措施，或（2）不產生特定作品的類似作品等措施。開發者必須考量如何加入相關措施，以防止產生或技術產生 AI 引起的著作權侵權[36]。

(7) 構成超越簡單勞動的「創造性貢獻」係是否 AI 生成結果可受著作權保護的重要因素

一個人是否可以說使用 AI 作為「工具」進行創作，取決於這個人是否具有「創造性意圖」以及其是否做出可以被認可為具備「創造性貢獻」的行為。AI 產品是否可以取得著作權，係根據每個 AI 產品的具體情況來決定。因此，「作為 AI 產品」本身，並不能一概認定其是否具「符合著作權作品的資格」。此須綜合考慮 AI 使用者的行為介入與累積到何種程度，可以構成超越簡單勞動的「創造性貢獻」來做出判斷。因此「具體表明什麼可以稱為創造性表達的詳細指令」可增加被評估為「創造性貢獻」的可能性，但大量嘗試本身並不會影響創意貢獻的判斷[37]。

[36] 同前註，頁 13-14。
[37] 同前註，頁 16。

本報告之智慧財產權歸屬於國發會

2. 執政黨自民黨公布 2024 年 AI 白皮書，擬實現成為全球 AI 最友善的國家、促進 AI 的合理利用、通力建構 AI 所需資料

2024 年 4 月 11 日由日本自民黨制定並發佈 2024 年 AI 白皮書（AI ホワイトペーパー 2024）[38] ，宣誓日本將進入 AI 發展之第二階段：成為「世界上對 AI 最友善的國家」。

該白皮書指出，考量 AI 從資料中學習和進化，資料策略益顯重要。當有助於解決商業和社會問題的資料，可在全球範圍內自由傳播，同時確保個人資料保護、安全、智慧財產權等方面的信任時，AI 將可實現其健康的發展。此外，由於 AI 應用於各個領域，因此與新創公司、半導體、機器人等各個領域的策略和政策合作並有效利用措施亦同為重要因素。基於上述因素考量，白皮書建議推動實現成為全球 AI 最友善的國家，即全球對 AI 最了解、最容易研究、開發和實施 AI 的國家。公營部門應共同努力，最大限度地提高 AI 的收益，同時最大限度地降低公眾面臨的風險，繼續在安全可靠的 AI 國際規則制定中發揮領導作用[39]。

根據公眾意見徵詢結果，關於 AI 開發、提供和使用的 AI 商業指南（AI 事業者ガイドライン）1.0 版計劃很快制定發布。未來，重要的是各個領域傳播 AI 業務指南，並以此為基礎進行各行業的應對。日本 AI 發展策略的基礎是企業等根據 AI 商業指南等自願、持續地評估和降低風險。另一方面，為推動指引等風險降低措施的社會落實，需要政府和企業經營者密切溝通、共同努力，並落實有效措施[40]。

[38] 日本自由民主黨，AI ホワイトペーパー 2024 ステージⅡにおける新戦略，ttps://storage.jimin.jp/pdf/news/policy/208287_12.pdf , last visited 2024/07/10。
[39] 同前註，頁 4。
[40] 同前註，頁 13。

本報告之智慧財產權歸屬於國發會

此外，要努力明確使用新一代 AI 生成及發佈圖像、影片時，能夠明示其為 AI 生成的產品。為了加快刪除非法（侵權）訊息，包括應對使用生成的 AI 生成的惡搞影片，並使平臺運營商的運營狀況更加透明，政府將採取必要的系統開發工作[41]。

就 AI 與著作權的關係，將在短時間內積極、公開地進行，提供基於法律法規的明確解釋，在維持現有的法律體系下，繼續與多方利益相關者交換意見。透過結合法律、技術和合約措施，快速實現一個平衡生成式 AI 技術的進步和適當保護智慧財產權的生態系統，結合技術進步，創造 AI 可以適當使用的環境[42]。

3. 經濟產業省和總務省共同公佈 AI 運營事業指引，提醒開發者應確保導入之資料在整個 AI 生命週期內皆應遵循法律

2024 年 4 月 19 日由經濟產業省（METI）和總務省（MIC）共同公佈 AI 運營事業指引（AI 事業者ガイドライン）[43]，該指引整合了總務省主導之 AI 發展指引（AI 開発ガイドライン）、AI 利用指引（AI 利活用ガイドライン）以及由經濟產業省所提出之實踐 AI 原則之治理指引。提出針對 AI 所應面對之社會及各適用主體應適用的相關共通規範，並分成「A. 基本理念」、「B.原則」、「C.共同指引」及「D.先進 AI 系統相關企業的共同指引」及「E. AI 治理」五大部分。除要求應確保透明度，減少 AI 使用帶來的社會風險，確保安全性和公平性等價值外，對 AI 開發者提出應注意於資料處理和訓練時，

[41] 同前註，頁 14-15。
[42] 同前註，頁 17。
[43] 日本総務省及経済産業省，AI 事業者ガイドライン，https://www.meti.go.jp/press/2024/04/20240419004/20240419004-1.pdf , last visited 2024/07/10。

本報告之智慧財產權歸屬於國發會

確保導入之資料在整個 AI 生命週期內皆應遵循法律之提醒[44]。

指引亦提及，有必要根據業務的地理發展狀況、使用開發之 AI 模型的 AI 提供者/AI 使用者的位置、執行學習的伺服器的位置等來遵守各項適用的法律。在遵守日本國內法律的情況下處理資料，即使法律沒有規定，也存在因利害關係人之間的契約關係而禁止使用資料的情況[45]。該指引反映了這幾年來日本對 AI 技術之進展和國內外 AI 社會實施之討論，以鼓勵事業實踐 AI 的社會實施與治理，以非具約束力之軟法提供指導原則，其制定不是由政府單方主導，而是由教育和研究機構、公民社會包括一般消費者以及民間企業等多方利害相關者進行討論，以確保實際效率性和正當性。

(六)韓國：發布「生成式人工智慧著作權指引」幫助著作權產業和創作理解，關注國內外立法趨勢並等待國內共識形成

雖然隨著 AI 技術的迅速發展，在各個領域的應用為經濟和社會利益產生許多助益，但也出現一個無法預測的環境，影響到著作權產業和創作活動的各個層面；有人將生成式 AI 作為創作工具，同時也有人擔心生成式 AI 可能帶來的經濟損失和就業威脅等問題。

因此，韓國文化體育觀光部的著作權委員會於 2023 年 2 月成立，由學界、法界和技術界專家以及利害關係人組成的「AI 著作權制度改善工作小組」，以審酌生成式 AI 引發的著作權問題並尋找應對方法，並於 2024 年 1 月 16 日發布「生成式人工智慧著作權指引 (생성형 AI 저작권안내서)」[46]。從實現生成式 AI 而建立基礎模型開始，到 AI 產出

[44] 同前註，頁 26。
[45] 同前註，頁 12。
[46] 「生成型人工智慧著作權指引 (생성형 AI 저작권안내서)」，https://www.copyright.or.kr/information-materials/publication/research-report/view.do?brdctsno=52591# , last visited 2024/07/10。

本報告之智慧財產權歸屬於國發會

物的生成，聚焦於可能引發法律爭議之數據學習和 AI 產出物生成部分，從現行著作權法的角度說明 AI 業者、著作權人和 AI 使用者需要了解的內容。同時為幫助理解，亦納入介紹目前提供的生成式 AI 案例以及相關的國內外立法趨勢。

該指引重點提及 AI 經營者宜採取防範措施以區別 AI 產出物與人類創作物，例如 AI 業務經營者在提供相關服務時，確保不會產生與現有作品相同或相似的 AI 輸出[47]。對著作權所有人，該指引特別建議如果著作權人不希望其作品用於 AI 學習，可以透過適當方式表達反對，以防止作品被用於 AI 學習；即使著作權人後來得知自己的作品被用於 AI 學習，亦可適當地採取技術手段來防止，以避免放任使用產生默許的問題[48]。

對 AI 使用者則提醒其注意，即使是用 AI 學習歌手聲音而重新創作或產生現有歌手的歌曲，也會涉及重製或輸入侵權資料的疑慮。同時，對學術研究或投稿，該指引特別建議在論文等中引用生成 AI 撰寫的文章之前檢查其來源，並標註特定段落是以什麼 AI 工具與指令所生成[49]。至於生成內容的保護，該指引認為在人類以創意方式進行修改、增加等「額外附加工作」的情況下，該額外工作的部分可被認定為具有著作權屬性，可以進行著作權登記。但是，著作權註冊的效果僅限於附加的部分[50]。

此外，在法令發展上，韓國文化體育觀光部近年來持續研議著作權法的全盤修正，2021 年 1 月韓國國會的都鍾煥 (도종환) 等 13 位議員曾提出最新草案版本，以日本、新加坡立法例為主要參考對象，增訂第 43 條為資料探勘著作權限制及例外規定，為生成追加性的資訊或價值，而非感受著作所表現的思想或感情之目的，透過利用電腦的自

[47] 同前註，頁 15。
[48] 同前註，頁 15。
[49] 同前註，頁 29。
[50] 同前註，頁 41。

本報告之智慧財產權歸屬於國發會

動化分析技術，對多數著作的大量資訊進行分析，於得合法接觸著作的前提下，可在必要之限度內重製、傳送[51]。但該修法受到各界的討論，是否應立即推動通過修法存有爭議[52]，雖陸續有國會議員提出類似修正案，目前尚無相關著作權法案修正通過[53]。而對於隨著生成式 AI 創作的內容輸出迅速發展，產生的深度造假、假新聞、侵犯著作權等各種問題，國會文化體育觀光委員會委員長李相憲表示，AI 技術的快速發展正在為所有創意活動創造出不可預測的環境，已提出《內容產業促進法》的修正案，要求對 AI 使用進行標記，將蒐集音樂、網路漫畫和媒體等各個領域創作者的意見[54]。

為因應生成式 AI 諸多著作權相關議題，前述提出指引的工作小組計畫持續研析 AI 時代著作權制度的完善途徑。例如：AI 企業需要產業支援措施，例如根據著作權法建立文字和資料探勘（Text and Data Mining, TDM），但考慮到自動化系統使用大量受著作權保護的作品來發展 AI 的現實，可能很難獲得使用所有受著作權保護的作品的事先許可，AI 學習使用著作權作品需要製定適當的補償方案。集中於透過信託管理組織管理的作品，例如新聞、音樂或文學作品，以及學術界或 AI 領域的權利持有者與 AI 營運商之間的談判，是目前該工作小組納入考量的方向。另外，如何引導申請人在登記著作權時詳細填寫 AI 輸出成果以及有人類創意貢獻的部分、以及如何揭露 AI 學習數據、單

---

[51] 提案編號 2107440，提案日期 2021 年 1 月 15 日。詳見류시원, 저작권법상 텍스트·데이터 마이닝(TDM) 면책규정 도입 방향의 검토, https://www.moj.go.kr/bbs/moj/166/450511/download.do, 頁 371~372, last visited 2024/07/10。

[52] 류시원, 저작권법상 텍스트·데이터 마이닝(TDM) 면책규정 도입 방향의 검토, https://www.moj.go.kr/bbs/moj/166/450511/download.do , last visited 2024/07/10。

[53] 主要均為提供訓練 AI 的資料合法授權，但差異在於有提供係限制教育研究等非商業目的、特定對象如大學研究機構或被指定的其他機構或組織進行。例如 2023-09-25 案號 2124685 之提案，條文詳見 https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_X2C3N0P1T2B0B0S9Z3V2O5V2W3K2N0 , last visited 2024/07/10。

[54] 한음저협, 'Made by AI' 표기 의무화 공청회 개최...AI 커버곡 저작권 문제, https://www.mk.co.kr/news/musics/10921956 , last visited 2024/07/10。

本報告之智慧財產權歸屬於國發會

純 AI 產品是否與如何受到法律保護，均是韓國仍在研析討論中的議題[55]。

(七)新加坡：提出「生成式人工智慧治理架構草案」，認為各利害關係人承擔應有的責任，應使用可信賴的「數據集(dataset)」，協助用戶辨識內容來源及生成方式，以維護隱私、著作權與社會大眾權益

為因應數位科技發展，新加坡於 2021 年 9 月 13 日通過著作權法修正，其中第 244 條[56]規定，允許涉及他人著作利用的資料探勘之重製或傳播(Copying or communicating for computational data analysis)，不限適用主體與是否非商業利用，任何人皆可為之。但不包括將該重製物用於任何其他目的或向他人提供該重製物（除了為驗證資料分析結果或者進行與資料分析目的相關的研究），亦不能規避付費機制去接觸取得原始重製物或違反資料庫使用者條款，或使用明顯是侵權的原始重製物（除非無法合理的知悉）。而且依同法第 187 條第 1 項規定，權利人不得以契約（使用者）條款排除本條合理使用規定的適用。

此外，新加坡資訊通訊媒體發展局（Infocomm Media Development Authority, IMDA）及「人工智慧驗證基金會(AI Verify Foundation)」於 2024 年 1 月 16 日聯合發布「生成式人工智慧治理架構」草案並於 5 月正式頒布[57]。該 AI 治理架構草案，內容涵蓋究責、數據、開發與運用、通報、測試、安全、內容來源、研究及公共利益等 9 大面向。上述治理架構草案認為，需要檢視現有的治理框架，以培育更廣泛的可信賴生態系統。在保護用戶和推動創新之間取得謹慎的平衡。問責制、

---

55 韓國文化觀光體育部新聞稿, 인공지능 시대 저작권 제도 정비의 실마리를 찾아보다게시일, 2024.06.28, https://www.mcst.go.kr/kor/s_notice/press/pressView.jsp?pSeq=21201 , last visited 2024/07/10。

56 Singapore Copyright Act 2021, https://sso.agc.gov.sg/Act/CA2021 , last visited 2024/07/10.

57 IMDA& AI verify foundation, Model AI Governance Framework fir Generative AI, 2024.05.30, https://aiverifyfoundation.sg/wp-content/uploads/2024/05/Model-AI-Governance-Framework-for-Generative-AI-May-2024-1-1.pdf , last visited 2024/07/10.

本報告之智慧財產權歸屬於國發會

著作權和錯誤訊息等相關議題是相互關聯，需要以務實、全面的態度來看待，任何單一干預措施都不是特效藥[58]。

在資料(DATA)議題上，該草案提出輸入模型的內容很重要，並且需要確保資料質量，例如透過使用可信任的資料來源。如果使用個人資料和著作權資料進行模型訓練存在爭議，應以務實的方式提供清晰、公平的對待[59]。如何衡平利益目前各國尚無一致做法，但考慮到所涉及的各種利益，草案認為政策制定者應促進所有相關利益相關者之間的公開對話，以了解快速發展的生成式 AI 技術的影響，並確保潛在的解決方案是平衡的並符合市場現實[60]。

AI 產生的內容由於創建起來很容易，可能會加劇錯誤訊息之傳遞及應用。如何使最終用戶能夠以確定知情的方式消費內容，存在著運用數位浮水印及來源加密等技術解決透明度的議題[61]。對於生成式 AI 的開發及運用，可借鏡食品的「營養標籤(Food Labels)」機制，針對不同之 AI「模型(models)」貼上標籤，明確列出開發過程中使用的數據及測試等重要資訊。標準化揭露可能包括：

a) 使用的資料：培訓資料來源類型以及培訓前如何處理資料的概述。

b) 訓練基礎設施：所用訓練基礎設施的概述，並在可能的情況下估計環境影響。

c) 結果評估：已完成評估之情形與關鍵結果之概述。

d) 緩解措施和安全措施：實施的安全措施（例如偏差校正技術和保護敏感資料的洩漏）。

[58] Id, at 3.
[59] Id, at 4.
[60] Id, at 11.
[61] Id, at 4.

本報告之智慧財產權歸屬於國發會

e) 風險和限制：模型的已知風險以及解決這些風險的措施。

f) 預期用途：明確說明模型預期用途的範圍。

g) 使用者資料保護：概述如何使用和保護使用者資料[62]。

而為防止生成式 AI 被用於傳播虛假訊息，並應探討使用「數位浮水印」及「來源加密」等兩種標記科技，標示可信賴或原創內容，以協助用戶辨識內容來源及生成方式[63]。

三、 趨勢發展重點歸納

各國目前在 AI 著作權議題之走向，在關注焦點上各有不同，但本文認為仍可歸納出以下幾個較為共通之思考點：

(一)促進 AI 生成的技術創新、保護既有著作權益、確保內容可信賴、是各國共通的基本政策取向，差異處僅在於當其彼此間相衝突時，孰為優先的價值擇取不同

觀諸聯合國將鼓勵保護智慧財產權並促進創新的措施之採用，獨立列為 17 項重點之一，且不論是聯合國、WIPO 甚至歐盟 AIA 法案，雖然觀注 AI 可能產生的風險，但均採取鼓勵 AI 研發運用，並認為發展同時應兼顧既有權益包括著作權的保護，各國立場幾無二致。但熟為優先的價值擇取不同，例如：AI 發展領先的美國，更著力於確保 AI 發展優勢，在 AI 訓練資料是否應取得授權的議題上保持戰略模糊，而從 AI 信賴角度提出應該讓訓練資料透明的立法提案，亦尚無確定通過的聯邦法案。至於日本為加速、強化 AI 發展，直接積極的立法賦予 AI 訓練合法空間，其執政黨並直接表明將成為 AI 發展友善國家，擬推動公私資料的互通利用、促進確保 AI 安全國際合作，AI 但亦認為應尊重(僅在必要範圍內合理的限制)著作權，AI 並要求應促進「可信

[62] Id, at 10-11.
[63] Id, at 24.

本報告之智慧財產權歸屬於國發會

任的內容與來源」，讓使用者能識別、確認 AI 生成與其來源。而在資訊技術相對是屬輸入者的歐盟，則不同於著重 AI 發展之美國及日本，於 AIA 法案中，則係特別重視 AI 風險管理，採取優先確保 AI 可信賴的處理態度。

(二)AI 訓練資料應在合理必要範圍內給予合法使用空間，但具體條件、框架、補償等配套尚欠一致的立法趨勢

即便政策上明示積極發展 AI，且已於著作權法上有對應規範的日本，亦非完全無限制的允許 AI 於無須取得同意下，即可自由使用受著作權保護之著作進行訓練。其仍須在必要且無不合理損害著作權人權益的限制範圍內，方能予以應用。日本文化廳之研究報告特別指出，如果從出售的資料庫複製著作權作品、旨在產生與著作權作品相似的作品、針對特定創作者的 AI 學習、破解規避有防止複製 AI 學習技術之著作權作品或資料庫，仍屬不合法的行為。雖各國立法條件不一，但日本與新加坡已有相近的立法例，而韓國亦已考慮到使用大量受著作權保護的作品來發展 AI 很難獲得使用所有受著作權保護的作品的事先許可，並擬進一步研究 AI 學習使用著作權作品需要製定適當的補償方案。

(三)存有人類的「創造性貢獻」是 AI 生成結果是否受著作權法保護、可受著作權保護的條件，但單純未有人為介入之 AI 創作亦非無保護可能 AI

目前各國著作權主管機關，對於非「人」之「AI 創作」，均對於其保護著作是否含有「人類」創意表達之原則有所保留。但無論如何，單純機械性的 AI 自動生成，基本上欠缺「人的創造性」，非著作權保護對象，已是主流看法。惟並未排除人類以 AI 為工具所產生的內容，所具有的保護可能性，因其過程仍有人的創作行為。美國與韓國均未排除 AI 著作登記之可能性，反而是提出應確認那些部分為人的創作的登記指引。而日本文化廳前揭報告，則更明確的指出構成「超越簡

本報告之智慧財產權歸屬於國發會

單勞動」是 AI 生成結果能否受著作權保護的重要因素。因此，「作為 AI 產品」並不能絕對否定其「符合著作權作品的資格」。而且日本與韓國也均進一步提及應評估單純 AI 產品是否與如何受到法律保護。

(四)標示、揭露、主動避免是 AI 服務提供與使用者被期待及要求的義務

基於 AI 發展應透明可信賴的基本態度，在減少 AI 使用帶來的社會風險，確保安全性和公平性等價值考量下，各國無論於對使用者或開發者的指引或相關政策層面，多出現及強調應確保整個 AI 生命週期應遵循法律的提醒。在美國目前呈現出之立法趨勢，更直接要求登記、公開被用以訓練的資料；韓國亦有修法草案同時提出要求附加辨識內容來源及生成方式之標記，以協助用戶辨識及選擇之規範。歐盟則要求一般用途型 AI 模型需另外執行風險評估及風險回報機制，經 AI 深偽技術處理的圖片、聲音、影片內容，則須明確標記。日本文化廳報告更進一步認為，在明知有侵權可能的情況下，提供者應採取積極的技術手段，例如不回應特定指令的方式，降低侵權問題的風險。

參、 我國法制概況

一、 自然人所為的創作，方可能受到著作權的保護

著作權法第 3 條第 1 項第 2 款所謂作為「著作人」之「創作著作之人」，同法第 11 條及第 12 條規定，於職務著作或出資聘人完成著作之情形，例外得以契約約定，以具雇用人或出資人身分之法人為著作人，是故我國著作權法雖無明文須為自然人之創作，但已明顯呈現受保護的著作須含有「人類」創意表達之原則。

本報告之智慧財產權歸屬於國發會

依經濟部智慧財產局 111 年 10 月 31 日電子郵件 1111031 令函要旨[64]亦謂：「一、依我國著作權法第 3 條第 2 款及第 10 條規定，著作人指創作著作之人，著作人於著作完成時享有著作權。換言之，著作必須係以自然人或法人為權利義務主體的情形下，由自然人所為的創作，方可能受到著作權的保護。」。又該局 112 年 3 月 17 日電子郵件 1120317 令函要旨並進一步指出：「有關藝術生成工具在學習後產出『相同風格』之圖片，由於其僅係利用 AI 技術產生之成果，無人類精神之創作，並不受著作權所保護。不論係 AI 程式之擁有者或利用該 AI 技術之人，均無法主張係該自動生成圖片之著作權人。」

二、 有人類創意投入的 AI 創作仍受著作權保護

然我國著作權法並非絕對排除利用工具進行創作，該創作受著作權保護的可能性，過往已有司法判決肯定工具運用的受保護著作，如智慧財產法院 100 年民著訴字第 55 號判決即認為：「現代科技進步，電腦已被廣泛作為繪圖及文字書寫之工具，一般繪圖者利用電腦繪圖系統程式，藉光筆或滑鼠等工具操作運用完成描繪、著色及書寫之行為，仍需仰賴操作者之經驗、思考及靈感，非電腦可代為判斷，此即為思想或感情之表達，尚不能因使用電腦即認非創作行為，換言之，應用電腦輸入工具及電腦軟體程式之操作繪製美術圖案者，倘若該美術圖案之設計、構形及繪製並非僅是電腦單純機械性操作的結果，或稍作比例、顏色等變更，而是灌注有操作者之精神、思想及情感，表現其個性之獨立創作，自得為著作權法保護之美術著作。」因此，只要有人類的創作參與，可認定為「以 AI 為工具」的創作，其產出之內容有「仰賴操作者之經驗、思考及靈感」，則仍是我國著作權法所保護的標的。

前揭經濟部智慧財產局函釋，亦指出：「以 AI 為工具的創作」，也就是人類有實際的創意投入，只是把 AI 當作如繪圖軟體般的輔助工

[64] https://topic.tipo.gov.tw/copyright-tw/cp-407-914789-dec09-301.html, last visited 2024/07/10.

本報告之智慧財產權歸屬於國發會

具來使用，在這種情形依輔助工具投入創作者的創意而完成的創作成果仍可以受著作權保護，著作權則由該投入創意的自然人享有，除非有著作權法第 11 條及第 12 條之情形。」。但是該函亦表明，「AI 獨立創作」也就是人類並無實際的創意投入，完全是由 AI 的演算功能獨立進行完成創作，此時由於 AI 並非自然人，沒有人類精神文明的投入，其創作完成成果自然不屬於著作權法保護的著作，原則上無法享有著作權。

三、 除符合著作權法第 44 條至第 65 條合理使用之情形外，AI 訓練資料須取得授權

受著作權保護並非意味對該作品的所有使用，均須取得授權。著作權法第 1 條揭示該法立法意旨：「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」，故基於社會公共利益與促進國家文化發展，在著作權法仍然存有法定授權、合理使用之規定，可據以提供 AI 訓練資料無須取得著作權人授權的空間。但我國著作權法目前尚無類如日本、新加坡的資料分析、探勘、非感受內容目的等，涉及 AI 訓練行為特性的專屬著作合法利用明文，只能依賴第 65 條之概括合理使用規範，以抽象的考量利用之目的及性質、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要件，進行個案判斷。均須個別判斷的狀況，自然會對利用巨量訓練資料的 AI 開發來說，產生個別損害小、整體風險高、整體處理成本過大的阻礙，顯非我國 AI 推動發展政策所樂見。

四、 標示、識別等可信賴配套義務尚待立法

至於在美國目前呈現出之要求登記、公開被用以訓練的資料，或歐盟要求一般用途型 AI 模型需另執行風險評估、風險回報機制，經 AI 深偽技術處理的圖片、聲音、影片內容，則須明確標記；日本認為在明知有侵權可能的情況下，提供者應採取積極的技術手段例如不回應特定指令的方式；韓國已有國會議員提出標記 AI 生成內容之修法

本報告之智慧財產權歸屬於國發會

顯降低侵權問題風險等應有配套措施，顯係國際上正在推動的立法趨勢，然於我國著作權法或其他法令上，均待進一步研究，尚無之法令配套。

肆、 小結

一、 對訓練 AI 資料合法使用訂定明確的條件

對於訓練 AI 所需資料的取得（重製），觀諸日本、新加坡已有明確的立法例，針對如果目的不是為了自己或他人感受作品中表達的想法或感情，在根據作品的種類、目的和使用方式，不會不當損害著作權人利益的情況下，可以在必要的範圍內以任何方法利用該作品，例如用於測試與錄音、錄影或其他著作權作品使用相關的技術的開發，或資訊分析（從大量作品等大量資訊中提取構成訊息的語言、聲音、圖像等要素的資訊，並進行比較、分類等分析。韓國文化廳 AI 著作權工作小組亦指出韓國的 AI 企業需要產業支援措施，例如根據著作權法建立文字和資料探勘依據，以提升其於 AI 發展的競爭優勢。

我國著作權法目前尚無類如日本、新加坡的資料分析、探勘、非感受內容目的等，涉及 AI 訓練行為特性的專屬著作合法利用明文規範，只能依賴第 65 條之概括合理使用規範，以抽象的考量利用之目的及性質、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要件，進行個案判斷。但面對使用大量受著作權保護的作品來發展 AI，獲得使用所有受著作權保護的作品的事先許可顯不現實的情況，維持目前著作權法的個別判斷規範，明顯會對利用鉅量訓練資料的 AI 開發來說，產生個別損害小、整體風險高、處理成本過大的阻礙，顯非我國 AI 推動發展政策所樂見。

本報告之智慧財產權歸屬於國發會

任何賦予著作權行使限制之修法,須有社會公益與文化發展考量。就賦予無成本的免費取得訓練 AI 所需資料而言，雖有其必要但亦非全然合理，如果 AI 的學習就如同人類讀書，那麼人的學習須買書來讀，為何 AI 的學習資料因為鉅量即可以無須付出成本。但 AI 的發展已經是全球熱潮如同新資訊時代的來臨，將全面影響我們的生活，限制與禁止並無法改變趨勢,是故本文認為應先於規範面建立明確的 AI 訓練資料取得的合法空間，同時採取降低權益影響的合理兼顧限制。

具體而言，建議可以評估以日本、新加坡立法例為參考對象，透過立法增訂或以函釋方式，建立資料探勘分析的著作權免責與例外規定，積極於著作權法第 65 條一般性的合理使用外，明確的降低 AI 開發過程的侵權風險：

(一) 非感受著作目的的使用：為生成追加性的資訊或價值,而非感受著作所表現的思想或感情之目的。

(二) 以資訊設備或方法：透過利用電腦的自動化分析技術。

(三) 進行大量資料處理：對多數著作的大量資訊進行分析。

(四) 於非感受著作目的內合法：得在必要之限度內重製、傳輸。

二、 限制 AI 訓練免責範圍以衡平著作權人合理權益保障

國科會 AI 基本法草案第 3 條規定，政府推動 AI 之研發與應用，應在兼顧社會公益與數位平權之前提下，發展良善治理與基礎建設，並遵循永續發展與福祉及問責等原則。依該條立法說明，我國發展 AI 應衡平創新發展與可能風險，以回應國內人文及社會所需。因此，在賦予明確的訓練 AI 資料合法使用條件的同時，應確保未不合理影響著作權人既有權益，以及賦予開發者承擔相應之責任。即便賦予取得訓練資料免責之日本、新加坡，其無須授權的訓練行為仍然不得不當損害著作權人利益。

本報告之智慧財產權歸屬於國發會

日本文化廳於前揭指引中亦指出，如有下述情況係屬不當損害著作權人的權利，包括：從販售的資訊分析資料庫中複製著作權作品；在生成式 AI 的基礎模型的額外學習（微調）中，故意「過度擬合」以產生與著作權作品相似的作品（具有共同的創意表達）；蒐集資料（受著作權保護的作品），用於輸入生成 AI 以增強生成（Retrieval-Augmented Generation, RAG）；針對特定創作者的 AI 學習；規避上述技術措施而複製用於 AI 學習的資料庫；明知或可得而知蒐集包含盜版或其他侵權之作品。而新加坡著作權法賦予的免責範圍，亦不包括規避付費機制去接觸取得原始重製物或違反資料庫使用者條款，或使用明顯是侵權的原始重製物，除非無法合理的知悉。而美國為協助 AI 訓練以推動技術革新之需求，並兼顧著作權人的權益保障，其眾議員係從透明角度切入，提出法案要求訓練資料來源應公開透明化，於推出提供公開使用的全新生成式 AI 工具系統前，向美國著作權局呈遞通知，揭露該模型訓練資料的完整清單列表，包含所使用可公開存取資料的網址，並對於違反處予罰鍰。

考量促進 AI 發展、保護既有著作權益、確保內容可信賴、是各國共通的基本政策取向，本文認為除建立資料探勘分析的著作權限制規定外，亦應從保護著作權人合理權益之角度，透過修法或函釋對該著作權限制有例外不適用之配套規範，例如：

(一) 規避付費機制，從販售的資料庫中非法複製著作權作品。

(二) AI 學習目的係過度擬合，以產生與著作權作品相似的作品（具有共同的創意表達）或針對特定創作者的 AI 學習。

(三) 明知或可得而知來源為盜版或侵權作品。

(四) 著作權人已限制存取措施，如爬蟲訪問網站，透過密碼認證防止複製。

本報告之智慧財產權歸屬於國發會

(五) 著作權人明示反對或已採取、運用可供取得授權的管道、機制。

(六) 未適當揭露 AI 訓練資料的來源。

三、 使用 AI（提供、生成、使用）

(一) 提供 AI 提供者防制侵權的免責條件

無論是人機協作或是單純 AI 的機械性生成結果，須有可創造侵權素材的 AI，後續始可能會導致進一步創造侵權作品，若 AI 提供者可採取一定防阻措施，係為最經濟、快速的有效作法，因此其對於著作權保護扮演重要的關鍵角色。就此，日本與韓國均不約而同的要求 AI 開發者或 AI 服務提供者採取必要的措施，例如日本文化廳於前揭指引中，要求 AI 提供者必須考量如何加入相關措施，以防止產生或技術產生 AI 引起的著作權侵權例如對於特定指令給予可能侵權的警示，甚至不對特定提示輸入產生回應。韓國直接於前揭指引表示 AI 業務經營者在提供相關服務時，應確保不會產生與現有作品相同或相似的 AI 輸出。

若基於有社會公益與文化發展考量，就賦予無成本的免費取得訓練 AI 所需資料，則本文認為同樣應基於社會秩序維護的考量，賦予 AI 提供者於當前技術水準可行下，採取降低權益影響的合理避免措施。AI 提供者應制定明確的著作權歸屬政策，確保 AI 的內容生成，符合當時通常應有的水準。不過，此部分涉及服務商品的消費者保護，包括 AI 工具的開發者、用戶及服務提供者之間的權利義務的歸屬，以及記錄、留存、提供查詢生成歷程等問責要求，建議宜由主管機關頒布「AI 服務使用條款應記載及不得記載事項」或是「AI 服務使用條款應注意事項」。

不過，美國著作權局於前述有關數位複製的報告中提及，有關 AI 複製侵權，多有關傳輸、儲存、託管或連接用戶內容的線上服務提供

本報告之智慧財產權歸屬於國發會

者(OSP)，且在許多情況下其最能防止這些複製品造成持續的傷害。美國著作權局認為 OSP 應該被鼓勵協助移除這些複製品，並在這樣做時免於承擔責任。適當的安全港的通知與移除系統，類似於《數位千禧年著作權法》(DMCA)鼓勵著作權擁有者和 OSP 合作「檢測和處理著作權侵權」，為通過為符合條件的 OSP 提供對其用戶所犯侵權行為的責任豁免，可能是一種有效的方法。因此，若明文賦予對 AI 提供者賦予無成本的免費取得訓練 AI 所需資料的權利，又 AI 產出必然含有 AI 生成部分(不論是人機協作或是單純 AI 機械性生成)，必有可一起創造侵權素材的 AI，後續始會在人的指令下生成侵權結果，則本文認為同樣應基於社會秩序維護的考量，鼓勵 AI 提供者協助防止 AI 造成的負面影響，溯及自內容生成階段即應鼓勵 AI 提供者防止。惟我國著作權法第 6 章之 1 已有網路服務提供者之民事免責事由，依同法第 3 條第 1 項第 19 款的網路服務提供者定義觀之，其範圍連線、快速存取、資訊搜尋、儲存這四種服務，並不包括 AI 線上服務，建議宜於著作權法上配套新增可供其主張免責的對應的侵權防阻條件，至少應提供問責管道、協助辨識內容來源、提供生成歷程、揭示生成的規範。

(二) 強化或建立 AI 訓練資料與生成結果使用收益分配機制

考慮到 AI 使用大量受著作權保護的作品來發展 AI 的現實，可能很難獲得使用所有受著作權保護的作品的事先授權的現實，因此有日本與新加坡給予 AI 學習使用著作權作品合法空間，但日本於前揭指引中仍限制排除已經以收費方式提供的資料庫、已採取限制 AI 學習資料收集技術的作品措施，及以原樣輸出作為學習資料的著作權作品的學習方法，不適用於收集盜版等侵害著作權上傳的資料。無論有無賦予 AI 訓練免責空間，AI 訓練資料如何簡便、經濟、明確有效的取得授權，均是發展 AI 必須處理的議題。

從國際立法例上，尚未見有法制面的明顯事例，即便迫切於促進 AI 發展但對於是否有必要賦予 AI 訓練免責立法尚在爭議中的韓國，其文化廳亦仍在研究是否應集中於透過信託管理組織管理的作品，例

本報告之智慧財產權歸屬於國發會

如新聞、音樂或文學作品，以及學術界或 AI 領域的權利持有者與 AI 營運商之間的談判等可能方向。本文認為推動以技術或機制，建立完善的授權收費、分配做法，降低 AI 訓練資料取得的授權的困難，增加讓原著作人也可以因為被 AI 使用而獲得合理的報酬，像演唱會的音樂著作權一樣有類似分潤的概念，仍是優先研析與推動的選項，如此始能鼓勵創作、保護著作權益，同時兼顧發展 AI 社會公益，達成雙贏的局面。

於實際商業授權操作上，例如 Open AI 跟媒體、出版社合作授權，獲得可信賴之資料，以解決生成式 AI 資料不即時、不具正確性的問題。另如 Adobe 提出新的商務模型約定權利人將資料放上作品利用平臺即為同意，而使用者使用該平臺資料則不會造成侵權，且權利人可分紅，自是政府可鼓勵的方向。若從法令機制面思考，則如果將來立法政策上已採取仿效日本賦予免責空間的同時，限制排除已經以收費方式提供、已採取限制收集技術、以原樣輸出作為學習資料的著作權作品的模式，那麼基於給予勤勉於維護自身權利的著作權人，以及努力合法取得授權的使用人，均應給予相應保護的思考，建議可思考情境類似的數位串流音樂授權機制。類如美國音樂現代化法案(MLC)的模式，由認證適格的民間單位建立完整性與即時性之著作資料庫，提供 AI 訓練資料重製的概括授權，並開放讓一般民眾得以使用，可以增加著作財產權人運用該機制獲得權利金收入，也減少 AI 提供與使用者的授權取得成本，緩解其巨量資料授權的現實困難。若能同時賦予據以取得授權者免受侵權追訴的法律效力，此機制將能更具誘因而可長期持續而且無須政府資源投入於建立與維護著作資訊系統。

(三) 明確認定 AI 生成結果的抄襲(接觸可能性)

現有受著作權保護的作品被生成式 AI 於開發/學習階段，在權利人、使用者，甚至開發者亦不能具體確知的情況下，即使使用者不清楚學習資料是否包含與產品相似的現有作品，應否被認定為有接觸既有作品？而權利人又如何能舉證或可無須舉證，這對而能否認定有接

本報告之智慧財產權歸屬於國發會

觸可能而應負侵權責任的結果存在重大影響。如果可證明 AI 有機會可存取現有作品或產品，將有被認為有接觸他人作品，而有被認定抄襲的風險，此邏輯與結論或許正確，在 AI 來自巨量學習資料，法令未要求提供者適度揭露，使用者不知亦無法可得而知學習資料是否包含與產品相似的現有作品情況下，將對於創作者而言可能產生擔憂責任歸屬的寒蟬效應。因此，在使用 AI 著作侵權責任認定上，建議透過函釋或指引等軟性的規範，一定程度明確化 AI 使用者的責任，例如：

1. AI 使用者將現有的著作物本身輸入生成 AI（如 Image to Image）。

2. AI 使用者輸入了現有著作物的題名（標題）或其他特定的固有名詞。

3. AI 使用者有接觸現有著作物的可能性（例如該現有著作物已發行並可獲得，或該現有著作物具有知名度或廣為人知）。

4. AI 生成物與現有著作物高度類似，受到 AI 的示警且未標示為 AI 生成。

整體而言，關於 AI 生成的著作權尚有其他例如 AI 產出淡化特定創作人的獨特風格、是否強制標示 AI 生成、單純 AI 自主生成是否保護等議題。惟考量風格本即屬不受著作權法保護範圍，保護特定風格或影響創作自由度特定風格，而風險亦有可能因原創性極高、已化為具體表達而為著作權法保護，亦尚可以透過契約、公平交易法等措施來保護創作者的風格，尚無於著作權法處理的急迫性。至於強制標示 AI 生成，於著作權角度觀之，其並非單純的 AI 信賴考量，應與前述免責議題併同處理。

AI 發展的著作權議題，涉及個人法益與社會公益的取捨，而且從國家發展角度須考量其對於未來國力的影響，因此國際上對於其相關法令的制訂，多處於持續研究而只有少數立法例的情況，反而是透過

指引、行政指令提出原則性的方向，希望能蒐集、形成各界意見共識，包括其中爭議最大的訓練 AI 合法性及其界限，因此本文僅從其等現有的政策與原則方向中，提供將來法令機制的思考方向，在 AI 持續發展情況下，於將來法令規範形成前，主管機關採取發布指引或報告以建立共識，或亦為各國不得不採取的的 AI 法制發展因應策略。

本報告之智慧財產權歸屬於國發會

項次 2. 焦點議題 2：AI 應用之消費者/使用者保護議題國際趨勢

壹、 背景說明

近年來人工智慧（AI）之發展與應用，已擴張至各行各業，並進入人民之一般生活。2023 年著名生成式 AI（Generative Artificial Intelligence）－Open AI 的 Chat GPT 服務推出 2 個月，即達到 1 億之月活躍使用者[65]。一個符合民眾生活所需之 AI 應用，已經可以迅速獲取高量之使用率，亦代表民眾對於 AI 之利用，已有相當之接受度。

然而 AI 技術類型及運用眾多，部分技術已應用於人們日常之生活、工作、社交、理財、娛樂、創作、知識獲取等各項領域，也因技術與應用領域之差異，亦產生不同之法制面議題。部分 AI 之應用，對於其直接或間接使用者或接觸者而言，會產生某程度上之風險或侵害，而有必要思考是否應透過法制政策面之規劃或建構以進行合理之把關，或降低其發生之可能性。

歐盟於 2024 年 5 月通過之人工智慧法（Artificial intelligence Act, AIA）即是從 AI 產品或服務可能產生之風險作為分類基礎，區隔不同風險 AI 開發必須遵循之要求與法制面義務，同時將對權利影響最大而不可接受之高風險 AI 技術明列禁止，僅於為保護人類公共利益之特殊情況下方得予以開放。足見 AI 發展及運用於產品或服務，對人類權益之影響有其法制政策思考之重要性。

常見之 AI 日常運用，包括以人類活動相關資料分析為核心之服務，如智慧金融、精準醫療、電子商務消費者行為分析或行銷等相關應用，以及用以生成各類內容之 AI 應用，包括影像、聲音、文字生成相關技術之運用，2023 年初開始備受關注之 Chat GPT 等大語言模型

[65] Ericsson Consumer Lab, 10 Hot Consumer Trends: The AI-Powered Future－A tension between AI hopeful and AI fearful, https://www.ericsson.com/en/reports-and-papers/consumerlab/reports/10-hot-consumer-trends-unveiling-the-ai-powered-future , last visited 2024/07/01.

本報告之智慧財產權歸屬於國發會

生成式 AI 即為其中一個事例。生成式 AI 被廣泛用於不同領域，包括各類內容創作、數據或資料分析、教育、商業服務等。當然也有其他類型 AI 應用於不同之產業領域，例如鑑別式 AI（Discriminative AI，又稱分辨式 AI），則是另一種運用資料標籤之機制，協助進行特定模式、關係、類型等等之分析，常用於須對資料進行辨識、判斷、推薦或決策之應用等。自動車與外界之互動等輔助駕駛技術、電子商務之廣告推薦、理財機器人等各項運用，相較近兩年生成式 AI 之發展，為更早進入實務應用之 AI 類型。

然而，不同 AI 技術，可以用於人類生活之正向應用，亦可能被用於較為負面而具高風險之應用。例如將影像或聲音生成之 AI，用於竄改既有影像或聲音而致利用或閱聽人產生錯誤之深偽技術；或利用精準演算法分析，對於不同之交易對象或使用者，作成具備選擇性、歧視性之決定或建議等，皆可能對於 AI 應用相關之使用者、消費者或利害關係人產生損害，如此則有必要考慮是否透過法制政策之規劃或調適，提升對於相關人員之保障。

前些年對於 AI 技術之實務應用之法制面探討，主要針對相關應用若對消費者、使用者或第三人造成損害，應如何界定責任之問題。此議題尤其於自駕車部分有相當之討論。是故歐洲議會曾經於 2020 年 10 月依據《歐盟運作條約》（Treaty on the Functioniing of the European Union，TFEU）之規定通過一項對於 AI 民事責任之立法倡議，要求歐盟指委會應針對 AI 引發之民事責任問題提出立法對策。而歐盟指委會並於 2022 年 9 月 28 日提出《人工智慧責任指令》（Proposal for an Artificial Intelligence Liability Directive）作為回應，並由歐洲議會及理事會於 2023 年 12 月初步同意該提案文本，期望引入新的 AI 責任體制。若此一指令通過，將可補充歐盟 AIA 之規定，強化法的確定性並提升消費者對 AI 的信任。2024 年 9 月歐洲議會之研究服務單位（the European Parliamentary Research Service, EPRS）就此指令發布一份研究意見，建議須調整 AI 責任指令適用之範圍，使之得以包括通用、其

本報告之智慧財產權歸屬於國發會

他高影響力之 AI 系統（high-impact AI systems）及軟體，然截至本計畫結案報告收尾之時點現在（2024 年 11 月），尚未有進一步之內容提出。產品責任部分對於 AI 法制面向確有其重要性，將持續觀測此指令之發展，但基於專案時程及相關內容尚未公布，故不列入本次研析範圍。

另於本年度專案期程之觀察，除了歐盟 AIA 對產品與服務風險監管之法制建構外，美國部分州別亦對於 AI 衍生之消費者保護議題，陸續有相當之法制通過；英國雖未針對 AI 之消費者或使用者保護議題進行規範，今年通過之《數位市場、競爭及消費者法》（Digital Markets, Competition and Consumers Act 2024, DMCC）亦未將 AI 議題直接納入，然透過強化英國競爭與市場管理局（Competition and Markets Authority, CMA）之調查權限，亦有助於 CMA 後續得以深入調查演算法可能產生之影響，而其 4 月份更新之 AI 戰略（CMA AI strategic update）亦進一步分析了 AI 對消費者帶來之風險；此外，鄰近之日本，雖然亦未對於 AI 涉及之消費者或使用者保護問題提出對應之法制，但於今年 5 月由消費者廳就生成式 AI 之運用，出版一版「AI 活用手冊－生成式 AI 篇」（AI 利活用ハンドブック～生成 AI 編～[66]），對消費者提出軟性的指引，而就一般消費者以外之使用者部分，日本則有 2020 年通過之《特定數位平臺之透明性及公正性提升法》，從平臺使用者之角度，促進演算法之透明度與公平性，降低演算法對平臺使用者(商業使用者)之負面影響，亦為涉及演算法運用之於使用者之法制事例。惟基於研究討論之貫穿與篇幅之限制，本文就 AI 影響消費者/使用者層面之趨勢探討，將先排除涉及商業使用者之規範，而以本年度各國針對一般消費者/使用者之法制政策為摘整與討論之核心。

[66] 日本消費者廳，AI 利活用ハンドブック～生成 AI 編～，https://www.caa.go.jp/policies/policy/consumer_policy/information/ai_handbook，最後瀏覽日：2024/11/05。

本報告之智慧財產權歸屬於國發會

本年度觀察相關法制政策之發展，可以看出國際上已逐步重視 AI 進入到市場應用層面，尤其涉及數位服務面向，對於消費者或使用者可能產生之風險與問題，而逐步形成因應策略，值得觀察並作為我國面對 AI 相關消費者或使用者保護法制政策規劃之參考。趨勢分析與討論之前，需先說明各國就 AI 影響消費者層面，於法制面所稱之消費者未必與我國消費者保護法第 2 條定義之消費者範圍相當，而可能包括非基於消費目的之 AI 商品或服務的使用者，合先敘明。

貳、 近期國際發展趨勢重點

一、 美國

(一)猶他州《人工智慧政策法》（Utah Artificial Intelligence Policy Act, UAIPA ）

猶他州於 2024 年通過對 AI 監管之修正法案，稱為《人工智慧政策法》，於 5 月 1 日正式生效。基於該法規定，該州設置了人工智慧政策辦公室（Office of Artificial Intelligence Policy），將監督並推動 AI 學習實驗室（Learning Laboratory）及相關學習實驗計畫，同時與該州事業及其他利害關係人就可能之 AI 監管或規範建議進行諮詢商談。AI 學習實驗計畫相關之程序、要求、費用及申請之規劃及處理，包括邀請、接受、拒絕或排除參與之規則建構，以及參與者資料使用限制與網路安全標準之要求等。

本法案針對生成式 AI 之應用，可能違反消費者保護法相關責任及影響層面有相當之著墨。首先對生成式 AI 加以定義，認為其應符合下列要件：1、以資料進行訓練；2、使用文字、聲音或影像與人進行溝通或互動；3、於有限或無人監督之情況下，能夠產製類似於人類精神創作之成果。

本報告之智慧財產權歸屬於國發會

而本法對於採用、提示或以其他方式促使生成式 AI 與人產生互動之相關事業或部門，則要求需具備一定之揭露義務，讓與生成式 AI 互動之使用者清楚、明顯知曉，其所互動之對象為 AI 而非人類[67]。而「受管制職業」（Regulated occupations），也就是依該法定義，係依據商業部門要求，必須取得特定執照才可以從事之職業[68]，必須於其提供服務時，於顯著之處向使用者/消費者揭露其係於何時與生成式 AI 進行互動。且從事受監管職業者，不得於不符合監管規範要求之情況下，透過生成式 AI 提供涉及受監管職業內涵之相關服務[69]。前述受管制職業者之揭露義務執行時機，為開始進行口語對話或溝通之前，或於後續進行書面文件交換前，以電子訊息進行揭露[70]。

針對違反上述揭露義務者，猶他州之消費者保護部（Utah Division of Consumer Protection, UDCP）對此一規定有執法權限，對於違反上述揭露義務者，得處以最高 2,500 美元之罰款，並有權向法院提起訴訟以落實對本節規定之執行[71]。法院於收到 UDCP 之起訴後，得進一步聲明特定行為已違反本節規定，並就該違法行為發出禁制令。若行為人因該違法行為有收取相關款項，可命其交出，或該違法行為有造成他人受到損害，亦得向行為人追繳相關款項；此外，可對行為人每次之違法行為，裁定處以最高 2,500 美元之罰款，或施以法院認為其他合理且必要之其他救濟要求[72]。

故猶他州本次 AI 政策法之修訂，著重在服務提供者對使用者/消費者提供採用生成式 AI 相關服務時之揭露義務，以及對應之處罰規範，以確保使用者係於清楚明確認知之狀態下，接受非人類直接提供而與生成式 AI 互動之服務。

---

67 Id, Utah Code Section 1, Section 13-2-12(3).
68 Id, Section 13-2-12 (1) (c).
69 Id, Section 13-2-12 (4).
70 Id, Section 13-2-12 (5).
71 Id, Section 13-2-12 (6)、(7).
72 Id, Section 13-2-12 (8).

本報告之智慧財產權歸屬於國發會

(二)科羅拉多州《人工智慧消費者保護法》(An Act Concerning Consumer Protections in Interactions with Artificial Intelligence Systems[73])

科羅拉多州於 2024 年 4 月提出《人工智慧消費者保護法》，並已於 5 月由州長正式簽署，成為本年度美國 AI 立法重要發展之一，該法案預計將於 2026 年 2 月 1 日生效。

本法關注之重點在於如何確保消費者參與或應用有 AI 介入之系統或服務時，能夠避免演算法造成的歧視。為達成規範之目的，首先定義了何謂演算法歧視，以及哪些情形不屬於演算法歧視之範疇。故該法第 1 條即揭示，本法所稱的演算法歧視係指肇因於演算系統而導致基於實際或想像之年齡、膚色、殘疾、種族、遺傳、語言能力、國籍、宗教、生殖健康、性別或其他受到本州或聯邦法律所保護之分類等差異，而對個人或群體進行不法之差別待遇或影響[74]。

以下情形則不涵蓋於演算法歧視探討之範圍，包括開發者或部署者係為兩種目的而提供、授權或使用高風險之 AI 系統，其一、為開發者或部署者進行自我測試時，用以識別、減輕、防止歧視或以其他方式確保對州法或聯邦法之遵循者；其二、則係為擴大申請人、消費者或參加者群體之參與，以提高參與者之多樣性或糾正基於歷史而產生之歧視等作為。或依據聯邦 1964 年民權法案規定，屬於不向公眾開放之私人俱樂部或其他機構之作為或不作為，皆不屬於本法所欲保障避免演算法歧視之範圍[75]。

此外，對於如何避免或降低演算法歧視之發生，本法並針對開發者(developers)或部署者(deployer)於何種情形下可被認為已採取合

---

[73] State of Colorado, In Colorado Revised Statutes, add part 17 to article 1 of title 6 as Artificial Intelligence, https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf, last visited 2024/7/10.
[74] Id, part 17 Article 6-1-4701, Definitions (1)(a).
[75] Id, part 17 Article 6-1-4701, Definitions (1)(b).

本報告之智慧財產權歸屬於國發會

理之謹慎措施，以避免消費者受到因高風險系統之預期或契約之用途而產生任何已知或可合理預見之演算法歧視風險。主要措施大致如下：

1. AI 開發者於本法生效後，應向高風險 AI 部署者或其他開發者提供或揭露以下相關資訊或文件[76]：

   (1) 說明高風險 AI 系統合理可預見之使用方式，以及已知有害或不當使用方式的文件。

   (2) 提供具備以下資訊之揭露文件：

      I. 該高風險 AI 系統使用之訓練資料/數據類型之高階摘要（High-Level summaries）；

      II. 該高風險 AI 系統已知或合理可預期之限制，包括來自其預期用途之已知或合理可預期之演算法歧視風險；

      III. 該高風險 AI 系統設置之目的；

      IV. 該高風險 AI 系統預期可帶來之利益及用途；以及

      V. 其他可使部署者得以遵循本法 6-1-1703 要求義務之其他必要資訊。

   (3) 提供描述以下資訊之相關文件：

      I. 於該高風險 AI 系統提供、出售、出租、授權、贈與或以其他方式提供部署者利用前，是如何評估該系統之性能以及進行可能之演算法歧視的緩解；

[76] Id, part 17 Article 6-1-4702 (2).

本報告之智慧財產權歸屬於國發會

II. 用以處理涵蓋訓練資料之資料治理措施，及評估資料來源之妥適性、可能之偏見並予以適當緩解之相關措施；

III. 該高風險 AI 系統預期之產出；

IV. 開發者為了減輕該高風險 AI 系統因合理可預見之部署，而可能產生之已知或合理可預見之演算法歧視，而採取的措施；以及

V. 當該高風險 AI 系統被用於作成結果性決策（Consequential Decision），或為作成該決策之重要因素時，該系統應如何被使用、或不應被使用或如何得以由個人加以監控。

(4) 其他得以協助部署者了解該高風險 AI 系統之產出並監控該系統之演算法歧視風險所必需的其他任何文件。

本法施行後，向部署者或其他開發者提供、出售、出租、授權、贈與或以其他方式提供高風險 AI 系統的開發者，於可行範圍內，需透過提供模型卡（Model Cards）、資料集卡（Dataset Cards）[77]或其他影響評估等方式，向部署者或與部署者簽訂契約之第三方提供必要之文件與資訊，以完成本法要求之影響評估。以上之義務主要針對開發者與部署者不同一之情形，若開發者與部署者同一，則開發者即無建置並提供上述文件之必要[78]。

[77] AI 模型卡（Model Card）為說明機器學習（ML）模型如何運作的檔案，係用以檢視 ML 透明度的工具。資料集卡（Data Card）則是記載關於 ML 採用資料集之結構化摘要說明，用以解釋資料形成的過程與原理、資料訓練及模型之形成。兩者皆為創建負責任之 AI 並確保 AI 透明度之工具。

[78] Id, part 17 Article 6-1-4702 (3)

本報告之智慧財產權歸屬於國發會

同時，本法施行後，開發者也有義務於開發人員網頁或可公開使用之案例清單，說明其所開發或有意進行實質修改而可提供部署者或其他開發者使用之高風險 AI 系統，以及開發者如何管理所開發或實質修改之高風險 AI 系統可能產生的已知或合理可預見之演算法歧視風險。前項說明並須依據實際情況適時更新，以確保聲明之正確性，該更新聲明不得遲於所描述之 AI 系統實質修改後 90 天[79]。除此之外，本法對於高風險 AI 系統開發者，並有配合司法調查提供資料之義務[80]，但同時也言明並無要求開發者必須揭露營業秘密或依據州或聯邦法律禁止揭露之資訊或可能帶給開發者安全疑慮風險之資訊等[81]。

2. 高風險 AI 部署者有義務採取避免演算法歧視之風險管理政策及計畫[82]

此部分主要針對高風險 AI 系統之部署者，要求其必須採取合理而謹慎之措施，避免消費者受到任何已知或可合理預見之演算法歧視風險。故於本法生效後，高風險 AI 系統之部署者必須制定並實施適切之風險管理政策及計畫，尤其必須於計畫中納入部署者可以用於識別、紀錄或減輕已知或可合理預見之演算法歧視風險的原則、流程及人員配置。該風險管理政策或計畫必須係依循 AI 之生命週期規劃與實施，並定期、有系統的審查與更新。依據本法要求之風險管理政策並須有合理性，並考量到以下要件[83]：

(1) 受認可或指定之風險管理框架標準：

[79] Id, part 17 Article 6-1-4702 (4).
[80] Id, part 17 Article 6-1-4702 (5)、(7).
[81] Id, part 17 Article 6-1-4702 (6).
[82] Id, part 17 Article 6-1-4703.
[83] Id, part 17 Article 6-1-4703 (2) (a).

本報告之智慧財產權歸屬於國發會

I. 美國國家標準與技術研究院（National Institute of Standards and Technology, NIST）發布之最新版人工智慧風險管理框架（Artificial Intelligence Risk Management Framework）規範之指引及標準，以及國際標準組織之 ISO/IEC 42001 標準或其他受到國家或國際認可之 AI 系統風險管理框架，若各該標準實際較本法規定更加嚴格。

II. 州總檢察長指定適切之風險管理標準。

(2) 部署者之規模以及複雜度；

(3) 部署者部署的高風險 AI 系統的性質和範圍，包括高風險 AI 系統的預期用途；以及

(4) 部署者於部署高風險 AI 系統時，處理之數據的敏感性與數量。

除前述高風險管理政策及計畫外，本法中亦列舉諸多部署者於本法通過後應採取之措施，包括風險層面之評估與監督，以及對消費者權益保障相關之措施[84]：

(1) 完成高風險系統的影響評估，包括對於高風險 AI 系統進行有意圖之重大修改後之影響評估。且須提出相關聲明，揭示該高風險之 AI 系統經修改後，於使用上與開發者預期之使用方式是否一致，或不一致之情形。

(2) 每年對部署者所部署之所有高風險系統情況進行稽核，以確保各該高風險系統不致造成演算法之歧視。

[84] Colorado General Assembly, Consumer Protections for Artificial Intelligence, SB24-205, Bill Summary, https://leg.colorado.gov/bills/sb24-205 , last visited 2024/7/11.

本報告之智慧財產權歸屬於國發會

(3) 若高風險 AI 系統會作出影響消費者的結果性決策，或可能對該結果性決策產生重要之作用，需以平易近人方式描述該高風險 AI 系統，並通知消費者。

(4) 提供消費者關於其是否有選擇退出其個人資料處理之資訊，並提供消費者於高風險系統於可能作出結果性決策時，有機會更正不正確之個人資料。

(5) 於技術可行之前提下，為消費者提供得透過人工審查對高風險系統產生對消費者不利之決定時申訴的機會。

(6) 發表公開聲明，說明部署者當前部署之高風險系統的類型、部署者控管其部署之高風險系統之已知或合理可預見之演算法歧視風險的作法。

(7) 部署者發現演算法歧視風險的 90 天內，向總檢察長揭露高風險系統所造成或可能導致之演算法歧視風險。

對消費者之揭露義務，不僅是前述針對高風險系統層面，AI 之開發者與部署者皆需要確保消費者知曉其正與 AI 系統互動，除非與 AI 系統互動的狀態對消費者而言是顯而易見的[85]。

綜上，科羅拉多州本次人工智慧消費者保護法之規範，整體著重於 AI 應用對消費者產生演算法歧視風險的降低，更完整的從開發者、部署者之角度進行風險層面之控管，同時強調消費者對 AI 互動之揭露與認知。

[85] Supra note 73, part 17 Article 6-1-4704.

本報告之智慧財產權歸屬於國發會

(三) 賓州眾議院提出《不公平貿易行為及消費者保護法》（Unfair Trade Practices and Consumer Protection Law[86]）修正案

賓州眾議院認為人民有權利知悉其接收之內容是否為 AI 所創造，並認為 AI 技術日益複雜，難以驗證內容之創作素材與作者，其內容真實性並無法確保，可能導致不實訊息之傳播或受到利用，造成使用者受到 AI 所誤導或欺騙。故眾議員於 2024 年 4 月提出對《不公平貿易行為和消費者保護法》之修正案[87]，期望透過提高揭露及透明度，以保護消費者，該法案目前已進入該州參議院審議。主要重點摘述如下：

1. AI 之定義[88]：本法案對於 AI 之定義，係指運用演算法創建新內容之技術或工具，包括音訊、程式碼、圖像、文字、模擬或影像。

2. 於「不公平競爭方法」（Unfair methods of competition）與「不公平或欺詐行為或實踐」事例（unfair or deceptive acts or practices)，新增運用 AI 生成資訊之態樣[89]：包括故意或未顧及後果的創造、散布或發布任何運用 AI 生成之內容，且並未清晰及顯著揭露資訊者，包括書寫之文字、圖像、音訊、影像內容以及其他形式之媒體等。此處之資訊揭露，其聲明必須包括說明該內容係由 AI 生成，且必須於內容呈現給消費者時率先顯示，同時必須得以合理理解且易於被注意到之方式呈現，且須顯示於與該內容相同之媒體。

---

[86] State of Pennsylvania, Amendment of PENNSYLVANIA UNFAIR TRADE PRACTICESAND CONSUMER PROTECTION LAW, 73 P.S. §§201-1 - 201-9.2, https://www.legis.state.pa.us/cfdocs/billInfo/billInfo.cfm?sYear=2023&sInd=0&body=H&type=B&bn=1598 , last visited 2024/7/10.

[87] The General Assembly of Pennsylvania, Hose Bill No.1598.

[88] Id, Section 2. Definitions (14).

[89] Id, Section 2. Definitions (4)(xxii).

本報告之智慧財產權歸屬於國發會

3. 定義「清晰及顯著」(Clear and conspicuous)之要件：針對需明顯或顯著揭露或聲明之義務，如何達到明顯或顯著，則必須符合本法規定之要件[90]：

(1) 該聲明或揭露必須採取易於被注意到、可讀、可理解以及可被聽取之適切大小、顏色、對比、位置、持續期間以及清晰度的方式。

(2) 聲明或揭露之資訊不得相互矛盾，且不得與該聲明或揭露內容提供之其他資訊不一致。

(3) 若該聲明或揭露資訊已被修改，則需同步解釋、釐清該聲明或揭露呈現之其他資訊。且前述資訊必須以易於注意、可讀、可理解之方式，呈現於被修改資訊之附近，且不得模糊。

(4) 若聲明或揭露係以音訊方式為之，則必須採取足以讓消費者聽到並理解其內容之音量與節奏來傳達。

(5) 若聲明或揭露係以影像方式為之，則必須採取具備一定大小及色彩，並持續呈現於螢幕達到足夠讓消費者閱讀及理解該聲明或揭露資訊之時間。

(6) 若聲明或揭露係以印刷廣告或推廣資料，包括直接向消費者於銷售點展示或簡介之資料等，則該聲明或揭露資訊所採取的字體大小以及置放之位置，必須係足以讓消費者閱讀及理解之印刷位置，並與該資訊放置之背景形成對比。

以上為本次修正涉及消費者權保障層面之規範，主要亦係著重於對消費者之揭露義務，強調揭露必須清晰及顯著，俾使消費者明確知

[90] Id, Section 2. Definitions (15)(i~vi).

本報告之智慧財產權歸屬於國發會

道所看到之內容資訊為 AI 所產出，並對於何謂清晰及顯著建立明確之要件，以避免消費者沒有注意到而被誤導。

(四)聯邦眾議院及人工智慧工作小組提出《保護消費者免受人工智慧欺騙法案》（Protecting Consumers from Deceptive AI Act[91]）

聯邦眾議院及其 AI 工作小組，針對 AI 消費者保護議題，於 2024 年 3 月提出《保護消費者免受人工智慧欺騙法案》，主要係考量目前生成式 AI，尤其是深偽技術之運用，已造成社會多面向之問題。對於消費者亦然，難以辨識所看到之資訊內容是否為真實，或係經由深偽技術所變造等，人們可以透過 Deepfake 技術創造虛假的影片，欺騙消費者，包括假冒名人代言之廣告等[92]，故提出本法案。本法案目前尚未出眾議院，截至 2024 年 11 月仍於眾議員能源及商業委員會下之創新、資料及商業委員會審議中。

本法案主要前言開宗明義說明，法案期望要求美國國家標準與技術研究院(NIST)成立工作小組，以促進、報告並制定針對生成式 AI 所創造之內容之識別技術與相關標準或指引，確保由生成式 AI 創造或為實質修改之音訊或影音內容，可以涵蓋適切之揭露資訊，確認該內容來源是生成式 AI，並用於其他之目的[93]。其規範主要重點摘述如下：

1. 建立協助辨識生成式 AI 生成內容之指引

法案要求 NIST 必須於法案生效 90 天之內成立一專案小組以完成指定目標[94]：

(1) 協助訂定技術標準與指引，用以提供針對出處之詮釋資料（content provenance metadata）、浮水印（watermarking）

[91] US Congress, A bill of "Protecting Consumers from Deceptive AI Act", H. R. 7766, 2024.03.21, https://www.congress.gov/bill/118th-congress/house-bill/7766/text , last visited 2024/7/10.
[92] Id.
[93] Id.
[94] Id, Sec.3 (a)(1).

本報告之智慧財產權歸屬於國發會

及音訊或影像檔之數位指紋（digital fingerprinting）與其他專案小組認為重要之技術措施。並於技術可行之範圍內，專案小組並得努力促使詮釋資料之可驗證性，並讓浮水印難以被移除或模糊化。

(2) 協助訂定標準或指引，以助益線上應用程式或內容提供者或經營者得以識別（identifying）及標記（labeling）由生成式 AI 創作或實質修改之音訊或影像內容。包括尋求得以支持社群媒體或其他線上平臺可互通之標準，使之得以相互識別、維護、翻譯及顯示浮水印、數位指紋及保護與音訊或影音資訊相關聯之詮釋資料。同時評估可能規避之技術及如何執行。

(3) 協助訂定標準或指引，以識別及標記由生成式 AI 創作或實質修改之以文字為基礎的內容（text-based content）。此部分之支援，可以包括制定創作此類內容時得以嵌入詮釋資料、浮水印、數位指紋或其他技術措施之相關標準。

前述相關標準或指引之制定，皆可獨立成立專案小組，就其需要邀請相關之聯邦組織、生成式 AI 科技的開發者、與開發內容檢測標準或技術（包括認證或可追溯性等）相關之組織、社群網站或網路即時通訊服務提供者、網路搜尋引擎服務提供者、網路瀏覽器或行動作業系統之開發者、相關學術機構/民間團體/研究團體或其他尤其涉及內容檢測標準或技術之相關組織、隱私倡議者及專家、人權律師或倡議者（尤其對於科技專業知識並有國際影響力者）、媒體（包括新聞發布者及影像提供者）、創作協會或組織（以代表著作權利人）、AI 測試專家（例如於 AI 紅隊演練[95]具備隱私專業知識者）、數位

[95] 紅隊演練（red-teaming），紅隊任務主要是模擬駭客或潛在之危險人物，透過模擬實際情境之方式試圖找到系統之漏洞。過往主要用於測試安全性弱點之系統化對抗性攻擊，目前 AI（尤其

本報告之智慧財產權歸屬於國發會

證據/密碼學或數位內容傳輸內容之相關技術專家及其他 NIST 執行長認為適當之專家參與[96]。

而各專案小組成立後，1 年至 5 年內，有義務每年對法案指定之委員會提交報告[97]。而就隱私層面，並建議專案小組應為線上服務、應用程式提供者或經營者發相關指引，使其得以透過保護隱私之方式儲存或顯示內容詮釋資料。包括清楚指導此類服務提供者或經營者於其使用者共享含有來源或詮釋資料之相關內容時，如何提醒使用者其所分享之資料具備來源或詮釋資料，而得以提供使用者可限制涵蓋隱私影響資訊之相關資料分享的選擇[98]。

2. 告知消費者內容是由 AI 所生成

本法案除前述對於生成式 AI 應用識別技術標準或指引之研議推動外，亦對消費者是否得以正確認知所看到之內容是否來自生成式 AI，針對不同對象課與相當之告知義務。

(1) 生成式 AI 應用之提供者

本法案要求向使用者提供生成式 AI 應用之服務提供者，具備以下義務：

I. 確保經由此類應用程式創作或為實質修改之音訊或影音內容，必須具備以下之揭露資訊—該資訊需機器可讀、且確認內容包括來自生成式 AI 之來源。

大型語言模型 LLM）開發者（如微軟等）有採用此一概念進行開發系統量測或降低風險之探查及測試，以識別可能發生之危害及驗證風險降低之有效性。

[96] Supra note 91, Sec.3 (a)(3).

[97] Id, Sec,3 (a)(4)(B).

[98] Id, Sec.3 (a)(5).

本報告之智慧財產權歸屬於國發會

II. 建構並採行合理之措施，避免前述應揭露資訊被刪除或以其他方式竄改。

III. 與涵蓋之線上平臺服務提供者合作，協助其識別及存取前述揭露資訊。

IV. 確保此類應用程式使用者得以於運用此類應用程式創作或修改之內容的詮釋資料中，置入該內容涵蓋生成式 AI 來源之相關資訊，以及預防資訊被竄改之相關訊息。包括該應用程式之名稱、該用於創作或修改內容之生成式 AI 模型的名稱及版本、與運用此類應用程式創作或修改內容相關之日期及時間、以及透過此類應用程式進行內容創作或修改之部分等資訊。

(2) 涵蓋之線上平臺服務提供者（covered online platform）

本法案所稱涵蓋之線上平臺服務提供者，係指提供給美國使用者之網站、網路應用程式或行動應用程式，包括社群網站、影音分享服務、搜尋引擎或內容整合服務，而符合年營收至少達到 5 千萬美元或於過去 12 個月當中至少有 3 個月擁有 2 千 5 百萬之月活躍使用者[99]。

本法案要求涵蓋之線上平臺服務提供者，具備以下義務：

I. 需對於利用其平臺存取具備前述應揭露資訊之音訊或影音內容的使用者，清晰及顯著的提供該揭露資訊。

[99] Id, Sec.3 (c)(4).

本報告之智慧財產權歸屬於國發會

II. 對於利用其平臺存取具備前述應揭露資訊之音訊或影音內容的使用者，不得刪除依本法案前述規定應包含於揭露內容之任何資訊。

綜上，可以看出美國聯邦眾議院於本法案對消費者保護主要著重點仍是保障消費者於正確充分之認知下接觸使用生成式 AI 創作或修改之資訊。也就是讓使用者或消費者得以透過適切而標準化之科技措施，以及生成式 AI 應用服務提供者與涵蓋之線上平臺服務提供者負擔之揭露義務，獲得充分的認知。此一法案從標準及指引研議之專案小組組成等相關討論，亦可充分顯示對於如何透過科技措施揭露有生成式 AI 介入之內容，可能涉及之利害關係人及專業領域的各個面向，故其雖尚在討論階段，仍有助於我國後續若要評估相關法制政策可諮詢或協調對象之參考。

(五)麻薩諸塞州總檢察長發布人工智慧適用州消費保護及其他相關法令之諮詢意見

除前述直接透過立/修法方式對消費者權益之保障外，部分州別雖未進行立法，仍對於 AI 應用之消費者保護議題加以關注。麻薩諸塞州總檢察長即於 2024 年 4 月發布諮詢意見，針對日益廣泛應用之 AI 及以演算法決策系統，及該應用隱藏之黑箱作業等問題，提醒 AI 之開發者、供應商與企業必須於符合現有相關法令之規定，包括州消費者保護法 (Massachusetts Consumer Protection Act)、反歧視法 (Anti-Discrimination Law)、相關個人資料保護標準 (Commonwealth's Standards for the Protection of Personal Information of Residents of the Commonwealth)等[100]。

[100] Mess.gov, AG Campbell Issues Advisory Providing Guidance On How State Consumer Protection And Other Laws Apply To Artificial Intelligence, 2024/4/16, https://www.mass.gov/news/ag-campbell-issues-advisory-providing-guidance-on-how-state-consumer-protection-and-other-laws-apply-to-artificial-intelligence , last visited 2024/7/12.

本報告之智慧財產權歸屬於國發會

1. 該諮詢意見列出依據麻薩諸塞州消費者保護法之規定，可能被視為違反平等互惠或構成欺騙性行為之舉例，諸如：

(1) 虛假宣傳 AI 系統之品質、價值及可用性。

(2) 為廣告目的，提供有瑕疵、無法使用或不切實際(impractical)之 AI 系統。

(3) 扭曲 AI 系統之安全、功能、安全性以及其實際狀況。

(4) 將一個違反保證(breach of warranty)之 AI 系統提供出售或使用，尤其當該系統無法適用於其通常使用之用途，或不符合銷售者所知可能用於特定用途之目的需求者。

(5) 扭曲特定個人之音訊或影音內容，以欺騙他人從事商業交易或向可信賴之第三人提供個人資料，例如用於詐欺的深度偽造、AI 擬聲(voice cloning)或聊天機器人。

(6) 違反麻薩諸塞州法規中，與保護公共健康、安全、福利相關之規範等。

2. 此外，對於避免對使用者/消費者歧視之議題，該諮詢意見並強調 AI 之開發者、提供者與使用者必須注意該州反歧視法之相關規定，尤其該法第 4 條[101]禁止開發者、供應商及使用者部署歧視居民的 AI 系統，包含仰賴或使用歧視性輸入並產生歧視性結果之演算法決策，例如使用具有不利於或使個人處於不利地位效果之個人特徵，可能構成詐欺行為及平等互惠原則之違反[102]。

[101] Commonwealth's Anti-Discrimination Law, G.L c. 151B, § 4.

[102] Mess.gov , Attorney General Advisory on the Application of the Commonwealth's Consumer Protection, Civil Rights, and Data Privacy Laws to Artificial Intelligence, https://www.mass.gov/doc/ago-ai-advisory-41624/download , last visited 2024/7/12.

本報告之智慧財產權歸屬於國發會

3. 州總檢察長也提醒關於聯邦相關法令之適用，以及關於個人資料保護法令之遵循，提醒 AI 開發人員、供應商、使用者必須採取必要和適當之措施保護 AI 系統使用之個人資料，並遵守資料洩漏時之通知程序[103]。

是以透過現行法令解釋之安排或呼籲，亦係於評估相關法令修正前，面對 AI 影響消費者權益議題之方式。

二、 歐盟

歐盟理事會(Council of the European Union)於 2024 年 5 月 21 日正式批准人工智慧法(Artificial Intelligence Act, AIA)[104]，並於 6 月 13 日頒布，預計於 2026 年起實施。統一歐盟會員國間對於 AI 監管之法制概念，可謂全球現階段首創以 AI 產品及服務風險與監管為核心之專法。其規範涵蓋之面向廣泛，主要以 AI 產品或服務開發及使用層面之風險分級進行監管，其所關注之歧視或權益保障面向亦較消費者保護層面為廣，然其針對歧視等問題所採行之邏輯與部分作法，與上開美國部分州法有相當之呼應，故就可相應處予以簡單摘述。

(一)關於 AI 技術利用或介入操控之內容產製的揭露

於 AIA 前言第 132 點指出，某些旨在與自然人互動或生成內容之 AI 系統，可能會帶來特定之冒充或欺騙的風險，無論該技術是否屬於高風險，因此必須遵守透明度義務。第 134 點亦提及，AI 之部署者可能使用 AI 系統以產製圖像、音訊或影音內容，此類內容可能與目前實際存在之人物、物體、地點、組織或事件相類似，且可能會錯誤的出現在人們面前而被誤認為確有其事或為真實，也就是所謂的深偽。此

103 Id.

104 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689 , last visited 2024/7/12.

本報告之智慧財產權歸屬於國發會

類情形應該透過相對應之標記，以揭示其來源，並以清晰可區別(clearly and distinguishably)之方式，揭露該內容係來自 AI 產製或操縱。此處之透明度義務，係以不妨礙對作品之展示或欣賞（包括對作品之正常開發與利用）之適當方式進行。並於前言第 135 點闡明歐盟執行委員會（European Commission, 執委會）將鼓勵建構歐盟層級之行為準則，以強化對 AI 生成內容之檢測與標記，使檢測機制易於使用，並促進價值鏈中參與者間之合作。同時於第 136 點揭示，AI 系統之提供者及部署者，有義務偵測及揭露相關系統之內容輸出，是人為生成或被操縱，以使法令規範得以有效落實；尤其超大型線上平臺或超大型搜尋引擎提供者，有義務識別及減輕因傳播人為生成或操縱之內容而產生之系統性風險，尤其是因為虛假資訊可能造成之實際或可預見之負面影響的風險，包括對民主進程、公民揭露以及選舉進程之風險[105]。

因此 AIA 第 4 章即針對 AI 之提供者與部署者之透明性義務進一步規範，要求 AI 之提供者，應確保於設計或開發與自然人直接互動之 AI 系統時，應能使自然人知悉其正與 AI 互動，除非該互動是顯而易見的[106]。若為產生合成音訊、影像、影音或文字內容之 AI 系統（包括通用 AI 系統）之提供者，則應確保該系統輸出內容須為機器可讀的形式，並可被偵測為 AI 生成或操縱，提供者並須確保該技術方案為有效、具互通性、穩定且可靠[107]。此外，若為產生或操縱構成深偽影像、音訊或影音內容之部署者，有義務揭露該內容為人工生成或操縱，但用於法律授權之偵查、預防、或刑事犯罪調查，則不適用。但若該內容構成明顯之藝術、創意、諷刺、虛構或類似作品或節目之一部分時，此一揭露義務僅限於不妨礙該作品之展示或欣賞之適當方式為之。同樣的，用以產生或操控向公眾通知公共利益相關事務文字之 AI 系統的部署者，亦須揭露該文字內容係經過 AI 生成或操控[108]。

---

[105] Id.
[106] Id. Chapter IV, Article 50, 1.
[107] Id. Article 50, 2.
[108] Id. Article 50, 4.

本報告之智慧財產權歸屬於國發會

上開應揭露之資訊，最遲應於相關自然人與 AI 系統首次互動或接觸時，以清晰且可識別之方式提供之，並須確保該資訊之接觸可能性(accessibility)[109]。對此，AIA 並要求人工智慧辦公室(AI Office)應鼓勵並促進歐盟層級行為準則(code of practice)之建構，以使相關檢測與標記經 AI 生成或操縱內容之義務，得以有效之落實。若執委會後續認為相關行為準則仍有不足，亦得再通過相關執行法案(implementing acts)，以建立共通之規則[110]。

(二)關於避免 AI 對人民產生之歧視

AIA 當中對於 AI 產品或服務可能產生之風險層面，AI 運用對於個人可能產生之不當分類或歧視亦為重要之環節。於前言第 27 點即聲明，雖然本規範是基於風險方法建構一套適當之且有效之監督規則，但仍需考量執委會曾經於 2019 年頒布之值得信賴 AI 的道德準則(Ethics guidelines for trustworthy AI[111])，包括七項基本原則，其中即包括多元化、非歧視性及公平。而多元化、非歧視及公平，代表 AI 從開發及應用，皆應涵蓋不同之參與者，同時亦須避免歐盟及國家法律已禁止之歧視性影響及不公平之偏見，上述原則於可行的情況下應轉變成 AI 模型設計與使用之基礎。

前言第 29 點則明文闡述，由 AI 所操縱的技術，可能被用來說服個人從事其所不欲作出之行為，或對個人進行欺騙，使之於違反自主意願情況下作出決定。而為產生對人類行為實質扭曲之目的或效果，而將此類 AI 系統投入市場，即可能對相關人員造成損害或危險，包括身體、心理健康或經濟利益等之不利影響，故需要予以禁止。此一規範同時補充歐盟 2005 年之電子商務指令[112]，尤其是針對可能對消費

[109] Id. Article 50, 5.
[110] Id. Article 50, 7.
[111] EU, Ethics guidelines for trustworthy AI, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai , last visited 2024/11/5.
[112] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and

本報告之智慧財產權歸屬於國發會

者造成經濟或財務損害之不公平商業行為，皆應被禁止。故 AIA 於此部分規範如前所述，探討的是更廣之歧視，而非僅是就消費者保護觀點切入之演算法歧視問題，但亦於前言當中明確指出其亦是呼應及補充電子商務指令當中保障消費者免於受到不公平商業行為損害之意旨。故其所採取之作法，亦可為處理消費者角度之歧視問題於法制面評估之參考。

此外就人權保障層面，AIA 前言第 49 點特別指出，若被歸類為高風險之 AI 系統時，可能對於歐盟《基本權利憲章》(Charter of Fundamental Rights)所保障之基本權導致負面之影響，須予以評估其可能產生損害之嚴重程度，並於歐盟層級之政策中施以高標準之環境以保護各該基本權利。而憲章所保障之相關基本權，則包括人性尊嚴、對私人及家庭生活之尊重、對個人資料之保護、言論及資訊自由、集會及結社自由、不受歧視之權利、受教育之權利、消費者保護權、勞工權利、身心障礙者權益、性別平等權、智慧財產權、獲得有效救濟及公平審判之權利、受辯護及無罪推定的權利、良好行政管理之權利等。同時亦須包括憲章及聯合兒童權利公約(United Nations Convention on the Rights of the Child)保障之兒童具體權利。故對於 AI 產品服務之監管，消費者權益保護亦為不可被忽視之面向。

而對於如何使得 AI 系統得以落實免歧視之目標，AIA 大致有以下作法：

1. 訓練開發階段資料之慎選與治理

AIA 從 AI 模型訓練階段之開發層面，即考量到訓練資料之來源可能造成的影響，故對於用以訓練、驗證與測試高風險 AI 之資料集，設定必須符合其所規範之要件，以及遵循適切之資料治理與管理。其中即要求必須評估資料集之可用性、

of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (OJ L 149, 11.6.2005, p. 22).

本報告之智慧財產權歸屬於國發會

數量與適用性，尤其考慮到高風險 AI 可能影響人員健康與安全、對基本權利產生負面影響、或產生歐盟法律規範所禁止之歧視或可能之偏見，必須採取適當措施以發現、預防與減輕可預見的偏見[113]。

2. 偏差檢測與修正技術或程序之必要性

為確保前述 AI 系統開發過程得以降低高風險 AI 系統可能導致之歧視，必須建立適當之偏差檢測(bias detection)機制及修正(correction)機制，為開發此類系統，提供者得例外處理歐盟規範規制之特種個人資料(special categories)[114]，並滿足以下條件[115]：

(1) 該偏差檢測或修正機制無法透過處理特種資料以外其他類型資料以有效實踐。

(2) 該特種資料受到個人資料再利用之技術限制，並施以最先進之安全及隱私保護措施（包括假名化措施）之拘束。

(3) 確保該特種資料受到妥適之處理及適當之安全保障，並嚴格控制其檔案之存取，以避免資料被濫用，並確保僅有被授權之人有權存取此些具備適當保密義務之資料。

(4) 該特種資料不得被第三方傳輸、移轉或以其他方式存取。

(5) 一旦系統之偏見已被處理或修正，或該資料已經達到保存之期限，該特種資料即應被刪除。

---

[113] Id. Article 10, 2. (e)、(f)、(g).

[114] 此處之歐盟規範，包括歐盟一般資料保護規則（Regulation (EU) 2016/679, GDPR）、歐盟政府機關資料保護規則（Regulation (EU) 2018/1725 ）及歐盟執法機關資料保護指令（Directive (EU) 2016/680）。

[115] Supra note 112, Article 10, 5.

本報告之智慧財產權歸屬於國發會

(6) 以此規定進行特種資料之處理，其記錄當中必須記錄為何必須處理此類特種資料之原因，亦即為何此類檢測無法透過處理其他資料來實現。

此外，高風險 AI 系統若已投入市場或提供使用，而該系統之提供者認為其有不符合 AIA 規定之情況，亦須立即採取必要措施，依其實際情況撤銷、停用或召回該系統或相關產品[116]。

3. 對系統運作之持續監督，對偏差或錯誤之出現適時施以緩解

AIA 要求高風險 AI 系統之提供應儘可能對應系統內或系統運作環境可能產生之錯誤、故障或不一致，尤其是針對與自然人互動所產生者，採取適當之技術或組織面措施，包括適切之備份或故障安全排除方案。且應考量已進入市場或應用後繼續學習之高風險 AI 系統該如何開發，方能減少或消除可能之偏差與未來回饋循環風險，採取適當之因應措施（包括採取適切之預防、偵測、回應、解決或控制攻擊等相關措施）。

4. 對個人決策 AI 系統之解釋權利與機制

針對高風險 AI 系統所作成之決定，若對特定對象產生某些法律效力或影響，諸如被認為對該對象之健康、安全或其他基本權利等造成負面影響，則受影響之人有權自該 AI 部署者，針對該 AI 系統於決定過程當中扮演之角色以及納入該決定評估之相關因素等資訊，獲取清楚且有意義之解釋[117]。

綜上，歐盟 AIA 雖然並非全然針對消費者保護所訂定之規範，而係以風險等級為基礎所建構的整體面 AI 產品或服務的監理架構，然

[116] Id, Article 20.
[117] Id. Article 86.

本報告之智慧財產權歸屬於國發會

其規範建構之背景，從人權角度而言，亦包括對於消費者保護權益之層面，其所採取之 AI 介入之揭露要求及降低 AI 開發與應用對人之歧視等部分作為，亦可作為評估對使用者或消費者權益保障之參考。

三、 英國

(一)CMA 人工智慧戰略更新（CMA AI strategic update）

英國 CMA 於 2024 年 4 月 29 日發布更新之人工智慧戰略，針對 CMA 如何應對 AI 發展帶來之消費者與競爭的問題進行策略面之調整，其中對於 AI 可能對消費者帶來之風險進行分析。戰略中提及，AI 驅動的服務，可能藉由得以提供消費者更高品質、更低價格及更個人化之產品或服務，而讓消費者獲得利益。然而，AI 之應用亦有很大的可能性，可能促成對消費者不公平之作為及風險。例如[118]：

1. 消費者可能會接觸到大量之虛假或具備誤導性之資訊，而此類資訊可能是 AI 系統所生成之錯誤訊息或稱為 AI 的幻覺(hallucinations)，抑或是以 AI 為基礎之技術，使得不良之行為人更容易以更低的成本創造出虛假或具備誤導性之資訊，且可能進一步擴大影響的規模，或加深對消費者欺詐之有效性。而事業可能透過已採行對消費者不公平之措施（如：訂閱陷阱、隱藏廣告或虛假評論等）故意利用 AI 進行不公平之作為，或另外開發對消費者不公平之新興商業模式。

2. AI 的運用可以支持個人化的發展，而個人化之定價或優惠等資訊，很難被察覺，故若事業運用 AI 採取對弱勢消費者不公平之作為，或產生不公平之分配效益，則對消費者而言亦將造成損傷。

[118] CMA, CMA AI strategic update, https://www.gov.uk/government/publications/cma-ai-strategic-update/cma-ai-strategic-update#alt-text , last visited 2024/11/5.

本報告之智慧財產權歸屬於國發會

CMA 指出，現階段對於消費者會如何理解 AI 之輸出以及限制，並未有足夠的研究分析，一些消費者對於 AI 理解之不確定性，可能會加劇上開風險之影響，此處所謂之不確定性因素包括[119]：

1. AI 生成與人工生成內容之區分不易：消費者可能難以區分 AI 產生之內容以及人類生成之內容。而對於 AI 生成的內容，亦可能識別其是否公允(faithful)或是否真實(factual)。

2. 消費者與 AI 互動之揭露不清：實務上對於消費者何時係與 AI 互動，及消費者如何被告知其係與 AI 互動等資訊，並不十分清晰。而浮水印(Watermark)並不是針對標記 AI 生成內容所開發之技術，故其使用上仍有相當之侷限性而不易克服，其中可能包括技術開發層面之問題，以及不良之行為人對浮水印之偽造或濫用，而對消費者產生誤導。

3. 明知 AI 應用之侷限性仍過度依賴或不願意依賴（依賴不足）導致損害：即使消費者已充分被告知 AI 之應用可能的侷限性，其仍然可能對 AI 過度之依賴或因而不願意依賴而對其帶來損害。前者，例如消費者依賴不可靠、不準確或誤導之描述進行商品或服務之購買；後者則相反，消費者可能因為對於 AI 產品無法信任或失去信心而不願意利用，以致其無法享受 AI 產品或服務可能帶來之利益。

CMA 指出，AI 價值鏈中之透明度不足以及責任之不明確，皆可能妨礙 AI 部署者與消費者了解 AI 或 AI 所支援之服務有如何之風險或侷限性。尤其演算法相關系統之開發、部署及運用，通常橫跨整體供應鏈之複數參與者。不同參與者若以不同之方式生產、部署與應用 AI，則其商品或服務若最終對消費者產生損害，責任之分配與認定將

[119] Id.

本報告之智慧財產權歸屬於國發會

有不確定性。故上游開發者必須提供與 AI 模型有關之足夠資訊，方能使下游之部署者進行有效之評估，並進一步提供消費者正確之資訊[120]。

(二)《數位市場、競爭及消費者法案》對演算法調查強化之規範

英國於 2024 年 3 月通過《數位市場、競爭及消費者法案》(DMCC[121])，並於同年 9 月正式生效。規範架構主要涵蓋四個面向，包括對數位市場執法部門(Digital Markets Unit, DMU)之賦權、數位消費者之權利保護框架、數位市場事前管制架構、以及評估限制競爭風險機制。其終於消費者權利保護部分，特別強化企業經營者資訊揭露之義務，並賦予 CMA 更強之調查權限，此一權限得以讓 CMA 為其執法之需要，要求事業提供其認為與數位市場功能有關之資訊(information[122])，而本法所謂之資訊，包括各類文件式資訊（包括草稿或最終文件）、任何其他形式資訊、以及資料、程式碼、演算法、評估、預測、回覆及解釋等[123]。 而對於資訊取得與調查之必要性，CMA 並得要求受調查之事業進行指定之演示或測試[124]，以確認及補強未為提供之資訊，且取得資訊之範圍亦包括事業儲存於英國境內或境外之資訊[125]。此一權限則可讓 CMA 藉由檢視相關資料記錄以及演算法之演示或測試，進一步評估事業演算法之應用對於市場競爭或消費者權益之影響。

此外，DMCC 並賦予 CMA 得以要求事業對其用戶或潛在用戶，就其提供之數位服務提供必要資訊，以確保其服務提供之透明度。相關資訊必須讓其使用者或潛在使用者得以了解事業透過相關數位活動所提供的服務或數位內容，其中亦包括提供相關服務或數位內容對應之條件或條款，以利使用者或潛在使用者得以就其是否要透過相關數

120 Id.
121 UK, Digital Markets, Competition and Consumers Act 2024, https://www.legislation.gov.uk/ukpga/2024/13/enacted#part-1-chapter-6 , last visited 2024/11/7.
122 Id. 69 Power to reauire information.
123 Id. 118 General interpretation.
124 Id. 69 Power to reauire information (5).
125 Id. 71 Power of access (6)；74 Power to enter business premises without a warrant (8).

本報告之智慧財產權歸屬於國發會

位活動與該事業互動，作出適當之決定[126]。條文規範上雖未直接提及AI 或演算法，但亦可應用於涉及 AI 之服務提供，透過揭露事業透過AI 與使用者互動，以提供數位服務之相關資訊，讓使用者或潛在使用者得以有效評估是否繼續使用各該服務，或如何使用等。

DMCC 是著眼整體數位市場之競爭與消保議題所訂定之規範，其並非直接針對 AI 之立法，然而，各類 AI 應用實廣泛進入數位市場之商品或服務之提供，故其對數位市場之調查或對數位服務可為之處置，於涉及 AI 或演算法之商品或服務提供時，亦可透過 CMA 之調查與要求，強化對消費者之保護以及對 AI 或演算法用於商業活動之了解，其規範概念可為參考。

四、 日本

日本並未直接針對 AI 對消費者之影響進行法制面之調整，而係以較為軟性之指導提醒消費者對於 AI 利用應注意之事項。其消費者廳於 2020 年 7 月就已經對消費者出版了「AI 活用手冊－如何明智的使用 AI」(AI 利活用ハンドブック～AI をかしこく使いこなすために～)；於 2024 年 5 月則進一步以生成式 AI 為核心，出版了「AI 活用手冊－生成式 AI 篇」(AI 利活用ハンドブック～生成 AI 編～[127])。基於本研究關注之趨勢範圍以本年度發展趨勢為主，故簡要摘要 2024 年針對生成式 AI 部分之手冊重點，供參酌。

2024 年之「AI 活用手冊－生成式 AI 篇」，主要包括生成式 AI 之定義、生成式 AI 之注意事項、生成式 AI 於社會上之利用情境及利用檢核表、兩類應用實例（圖像生成服務及聊天機器人服務）、以及消費者之救濟[128]：

[126] Id.19 Power to impose conduct requirements (8).
[127] 日本消費者廳，AI 利活用ハンドブック～生成 AI 編～，https://www.caa.go.jp/policies/policy/consumer_policy/information/ai_handbook/assets/consumer_policy_cms102_240718_002.pdf，最後瀏覽日：2024/11/05.
[128] Id.

本報告之智慧財產權歸屬於國發會

(一)生成式 AI 之定義

手冊開始對於生成式 AI，定義為 AI 之一種，可以根據輸入之指令（文字等）建立文字、圖像、影片或程式等內容。而生成式 AI 可以透過自然對話創建句子或圖像，如同與人類之交談。

生成式 AI 之運作原理，係依據其大量學習之資料（例如文句或圖像）概率進行內容的建立，並非透過真實之理解所創建的內容。例如可以生成文句的 AI，會透過分析選擇最有可能跟隨某個單字之字彙以創建文句。例如，鍵入詢問日本的首都，則 AI 會選擇連結前面問題文句機率最大之詞彙，也就是東京。

對於生成式 AI 之運用必須注意，生成式 AI 不一定會輸出準確的答案，且若來源資訊不正確或有偏見，其回應之內容則可能包括錯誤之資訊。此外，由於其反應是基於機率而生，故也可能出現幻覺現象，也就是出現與現實不同之資訊。

手冊並提示生成式 AI 適用及不適用之用途：適合之用途，主要是可以用於專業層面，包括協助總結、解釋、翻譯或產生想法。不適合之用途，則是需要最新且高度精確資訊之情形。

(二)生成式 AI 於社會上之利用情境及利用檢核表

手冊對於生程式 AI 於社會上之利用，就使用者端，可能是使用者自己運用生成式 AI 創建內容，或使用者利用運用了生成式 AI 之企業服務，或是使用者接觸由第三人透過生成式 AI 製作之內容等三種基本型態。而利用生成式 AI 有正反面之運用事例，就企業服務部分，例如聊天機器人（生成文章之運用事例）或虛擬服裝試穿（圖像生成是 AI 運用事例）等；反面之運用事例，則包括利用生成內容進行詐騙，包括自然生成之詐欺郵件，或生成式 AI 採用與特定人相似之聲音或偽裝熟人進行詐騙。另一反面運用，例如運用生成式 AI 形成假圖像、

本報告之智慧財產權歸屬於國發會

影音或文字，影響輿論或使人誤以為係特定政治人物之假影音等可能造成評論之誤導或引起社會混亂。

因此，對於生成式 AI 之應用，手冊另提供一份利用檢核表，就開始利用前應注意之事項，以及利用時應注意之事項，對應不同之生成式 AI（如聊天或圖像生成）給予查檢之事項之提醒。例如於聊天視窗不要輸入個人資料或不能透漏予他人之資訊、必須注意 AI 回應之內容未必正確、若 AI 建議購買商品或服務須謹慎評估需要等。而對於圖像生成之 AI，則必須注意生成之內容是否與現存具備著作權之內容近似，以及不得製作及散布假圖像等。

(三)實務應用案例

本手冊共提供兩則 AI 應用之實務案例說明：

1. 圖像生成服務

說明所謂圖像生成服務，係利用生成式 AI 技術，依據用戶指定之內容製作圖像之服務。部分服務可以指定圖像生成之風格，例如漫畫風格或插圖風格；部分服務得以透過圖像之輸入而非文字進行圖像製作。

手冊當中以今昔對比讓消費者可以了解，過往要製作圖像時，需要評估是自己動手或是委託製作。而圖像生成服務，則是可以將需求對 AI 進行描述，例如對 AI 下達「用漫畫形式，畫一張開車的狗」之指令，AI 則從指令說明當中選取須生成內容之要素或特徵，生成符合說明之圖像提供使用者參考。

手冊並提醒使用者於利用圖像生成服務時應注意之事項，包括於使用服務前，必須確定服務之利用是否有相關限制，例如年齡限制或生成圖像用途之限制。而使用者是否可以將 AI 生成之圖像用於投稿部分，則是說明利用圖像生成服務所

本報告之智慧財產權歸屬於國發會

製作之畫作，若被認為與現有受到著作權保護之人類著作類似，則創建該圖片之使用者若利用開圖片，可能需要承擔侵害著作權之風險。而依據該服務之使用條款，若要利用 AI 服務生成之圖像，亦可能需要註記其為透過生成式 AI 所作成。同時，需要注意圖像生成服務未必可以準確繪製出使用者期待之內容，甚至可能出現具有奇怪形狀或位置關係之影像。

2. 聊天機器人服務

此事例向消費者說明，聊天機器人(Chatbot，チャットボット)是「chat（聊天）」加上「bot」（機器人） 之組合詞，為一種系統自動回答之服務。透過生成式 AI，系統可以回應各種問題，就如同人類之回答。此類服務不但可以用於回覆使用者之問題，也可以用於線上英文會話服務講師，或 AI 好友服務等。手冊並圖示說明生成式 AI 用於英文會話服務及 AI 好友服務之情境，其工具結構主要係用戶可以透過文字或語音輸入問題，再由生成式 AI 透過資料援引、學習手冊或會話資料等背景資訊，為使用者所輸入之問題生成答案以回應使用者。

手冊並提醒使用者利用聊天機器人時應注意之事項，包括聊天機器人之回答之正確性必須要再行自我判斷，因為生成式 AI 是依據所學習之文件資訊及概率生成回答之內容，若學習之內容錯誤、偏頗或有幻覺，可能產生看似合理但錯誤之答案。此外，聊天機器人也可能會暗示使用者購買商品或服務，需要謹慎確認必要性後再決定是否購買，並保存聊天紀錄。此問題出現之原因，主要在於使用者與聊天機器人係進行自然之對話，於提問中獲得解答，故很容易讓使用者與機器人間產生信任關係，而企業經營者可能會調整 AI 之運作，使 AI 傾向給予使用者該企業經營者期待之答案，甚至出現鼓勵購買之風險。

本報告之智慧財產權歸屬於國發會

(四)消費者之救濟

此部分主要在提供消費者若利用生成式 AI 遇到問題，可以解決的方法或救濟的管道。包括提醒消費者若對於生成式 AI 之使用方法不確定時，應該查閱服務頁面、使用者指引、廠商提供之問答後，再諮詢提供各該 AI 服務之事業。若有糾紛則可撥打政府消費者 188 熱線，至於非生成式 AI 利用之疑問，則參考 2020 年之「AI 活用手冊－如何明智的使用 AI」。

五、 趨勢發展重點歸納

綜合上半年之觀察，以美國、歐盟、英國及日本之法制政策發展而言，針對 AI 使用者/消費者保護層次之法制政策重點大致有以下層次：

(一)確保 AI 應用之透明度，即強化並落實揭露義務

1. 要求必須於使用者/消費者互動前告知其互動對象為 AI

此部分強調向使用者/消費者揭露資訊之時間點，著重使用者/消費者係在已知之前提下，進行技術或服務之運用。例如猶他州《人工智慧政策法》要求揭露之時機為開始進行口語對話或溝通之前，或於後續進行書面文件交換前，以電子訊息進行揭露。賓州眾議院提出之《不公平貿易行為及消費者保護法》修正案，則是要求必須於內容呈現給消費者時率先顯示。歐盟 AIA 認為應最遲於相關自然人與 AI 系統首次互動或接觸時提供之。英國雖未明確對 AI 之告知義務進行規範，然主管機關亦可要求事業向其商品或服務之使用者或潛在使用者說明其透過數位活動所提供之商品或服務的必要資訊，以利使用者或潛在使用者對是否繼續透過該數位活動與事業互動作出明智決定，而該數位活動即可包括運用 AI 對使用者之互動。

本報告之智慧財產權歸屬於國發會

2. 針對 AI 介入產製或實質修訂內容之揭露資訊必須「清晰及顯著」

此部分著重在揭露義務執行之方式,必須是清晰及顯著,方能收切實讓使用者/消費者知悉功效。美國各州規範於此粗細不一,其中最仔細者,為賓州眾議院提出之《不公平貿易行為及消費者保護法》修正案,臚列六項達到清晰及顯著之要件,包括其顯現形式、內容一致性、可讀可理解,以及基於不同 AI 之特性,音訊、文字或影像等之揭露模式等皆有相當之要件揭示。聯邦眾議院及 AI 工作小組提出之《保護消費者免受人工智慧欺騙法案》則特別要求該法涵蓋之線上平臺服務提供者,必須協助清晰及揭露相關資訊。歐盟 AIA 則強調對於 AI 內容來源之揭示,應採取「清晰可區別」之方式,讓使用者知悉該內容來自 AI 產製或操縱,並以適切之方式進行。

3. 標記制度建立及標準化研議

此部分在於建立可標記之技術、機制甚至標準,以利包括經營者或大眾得以識別相關內容係屬於 AI 所為或實質介入/修改/操縱之內容,以利揭露義務之實踐。此部分較屬整體監管架構之思維,諸如美國聯邦或歐盟整體層次之角度。包括美國聯邦眾議院及 AI 工作小組提出《保護消費者免受人工智慧欺騙法案》,當中即認為應該由 NIST 召集各方專家組成專家小組,訂定相關之標準或指引,以使各方進行標記有可採行之共通技術、標準與規則。歐盟 AIA 亦認為必須建立相對應之標記機制,以揭示 AI 產製或操控之內容與來源,且若涉及相關藝術創作等,其標記揭示尚不能影響該作品之展示或欣賞的正常運用;同時 AIA 並認為,尚須搭配檢測機制以強化揭露之落實,並建立歐盟層級之行為準則。

4. 顯而易見之互動的豁免

本報告之智慧財產權歸屬於國發會

此議題主在平衡提供者/部署者之揭露義務與消費者知的權益，也就是說，於個別情境下消費者得以明顯知道其係與AI互動，則可豁免提供者/部署者此部分之揭露義務。此規定主要出現在科羅拉多州《人工智慧消費者保護法》，提及AI開發者與部署者，皆需要確保消費者知曉其正與AI系統互動，除非與AI系統互動的狀態對消費者而言是顯而易見的。歐盟AIA亦採取同樣的態度，認為AI之提供者，應確保於設計或開發與自然人直接互動之AI系統時，應能使自然人知悉其正與AI互動，除非該互動是顯而易見的。

5. 需擔負揭露義務之義務人的確立

就本次觀察而言，揭露義務主要落在AI服務之提供者，可能涵蓋開發者及部署者。然而，部分AI係於線上平臺應用，故亦有美國聯邦眾議院，特別將具備特定條件（大型）之線上平臺服務提供者，列為必須落實揭露義務之對像，可為參酌。

(二)確保、降低及排除AI運用可能導致歧視之機制

1. 定義何謂演算法歧視

此部分主要是科羅拉多州《人工智慧消費者保護法》對於該法所認定之演算法歧視進行定義，並排除該法認為不屬於演算法歧視之範圍。故其所認定之演算法歧視，係指肇因於演算系統而導致基於實際或想像之年齡、膚色、殘疾、種族、遺傳、語言能力、國籍、宗教、生殖健康、性別或其他受到該州或聯邦法律所保護之分類等差異，而對個人或群體進行不法之差別待遇或影響。

2. 避免AI演算法歧視之揭露義務

本報告之智慧財產權歸屬於國發會

此議題主要關注如何讓使用者/消費者知道所參與或使用之演算法可能造成之歧視。就科羅拉多州《人工智慧消費者保護法》而言，其所採行之方式是提供相當之說明文件，讓使用者/消費者知道，哪些是所提供或部署之 AI 合理可預見之使用方式，與可能有害或可預見不當之使用方式。同時提供相關文件予部署者，揭露該 AI 之訓練背景資訊與可能之歧視風險，以及可能如何緩解與採取之措施等訊息。

3. 採行得以降低或排除 AI 演算法歧視之措施

(1) 風險評估機制之提供

開發者之層次，著重在讓 AI 之部署者能夠對於所部署之 AI 技術或應用有更為清楚之認知，包括其訓練開發之重要背景及其於不同應用層面可能出現之歧視風險等（如前述科羅拉多州規範對部署者之揭露義務）。於科羅拉多州《人工智慧消費者保護法》並要求該 AI 之開發者必須向部署者或其他開發者於可行範圍內提供相關資料、機制或影響評估之方式，以利其後手得以有效評估及控制歧視風險。

(2) 採取適切之內部管理機制

此部分著重在開發及部署 AI 者，必須有相當之內部管理機制，以避免所開發或部署之 AI 產生對使用者/消費者之歧視結果。美國科羅拉多州《人工智慧消費者保護法》主要係要部署者採取合理而謹慎之措施避免歧視之風險，包括建立計畫並採取可以識別、紀錄並減輕已知或合理可預見之風險的原則、流程與人員配置。歐盟 AIA 層面，主要從訓練開發階段之資料選擇與治理開始進行要求，必須避免採用可能形成偏見之資料進行訓練，同時於開發中以及上市後，皆須持續進行偏差之檢測與修正，降低歧視之

本報告之智慧財產權歸屬於國發會

發生；最後對於產生法律效果者，並應給予受影響之人取得明確解釋之機會。

(三)擴大主管機關調查權限，強化對 AI 實務影響之了解與因應

英國 DMCC 之規定並非僅係針對 AI 之規範，其主要著眼於數位市場環境有涉及新興數位技術堆疊應用，有相當之複雜性，加上大型數位平臺基於其市場支配地位，對於數位市場之有效競爭及消費者之權益都有相當之影響。基此，競爭與消費者保護主管機關，應有充足之法律支持，並有足夠之權限對於數位市場相關服務進行調查分析，切實發現對市場及消費者權益有害之事業作為，適時予以介入。

而此一調查權限之擴張，極為重要的部分即是對於數位服務相關資訊廣泛取得與調查之權限。其並將程式碼、演算法等涉及技術堆疊與交互應用之重要資料明列為可要求事業提供之資訊，並包括儲存於海外之資訊。這使得執法機關不但可透過文件調查資料之取得，進行涉及數位技術之商業活動的調查與了解，亦可透過對文件資料無法說明之情境，要求事業就演算法或程式碼等進行演示或測試，從實作當中更深入了解各該技術之影響，對於後續進一步評估及考量相關政策或執法措施將有所助益。

(四)透過對消費者之軟性指導，提高消費者認知以降低應用風險

除了新興法制之建構外，日本就 AI 應用之法制政策層面，主要採取對應不同之情境、對象或應用需求，提供軟性指導（軟法）之方式，降低 AI 對社會可能產生之影響。2024 年就 AI 對消費者影響部分，公布之「AI 活用手冊－生成式 AI 篇」，明顯與其他國家強調權利義務之法制作為有所不同，而係站在消費者之角度，用簡單與常見應用之方式，使其了解生成式 AI 的運作及風險，並給予檢視工具或建議，引導消費者於面對生成式 AI 實務應用時，得以作出審慎之判斷。

本報告之智慧財產權歸屬於國發會

參、 我國法制概況

一、 AI 基本法草案揭示政府應重視 AI 對國民權益之影響

我國現階段尚未有直接針對 AI 應用對消費者產生影響之作用法規範。而就國家科學技術委員會（國科會）2024 年 7 月預告之《人工智慧基本法（草案)》，於第 9 條第 1 則宣示，政府應避免 AI 之應用造成國民生命、身體、自由或財產安全、社會秩序、生態環境之損害，或出現利益衝突、偏差、歧視、 廣告不實、資訊誤導或造假等問題 而違反相關法規之情事。此一基本法草案，揭示了未來政府對於 AI 應用對國民權益影響層面，需考量之重點，當然亦包括 AI 之消費者與使用者的層面，然具體法制政策應如何應對，尚待後續各目的事業主管機關配套法制政策之規劃。

二、 消費者保護法尚未對應修法，部分規範可為解釋應用

目前我國針對消費者保護之規範主要為《消費者保護法》(簡稱消保法)，最新修訂於 104 年 6 月，本法所定義之消費者，依據消保法第 2 條第 1 項第 1 款之定義，係指以消費為目的而為交易、使用商品或接受服務者。本法對於消費者權益保障大致分為「健康與安全保障」、「定型化契約」、「特種交易」、「消費資訊規範」四大面向。除特種交易部分，係針對通訊交易或訪問交易特性之特別規定外，其餘主要係對於一般性之商品或服務提供所為之通用性規範，原則上若特定商品或服務沒有其他法律之特別規定，其對消費者之權益保障則適用消保法，消保法未規定者，則回歸民法之適用。

故商品或服務提供予終端消費者層面，若為消保法消費關係，則對消費者之保障應適用消保法之規定。若有適用上不充足或有疑義之層面，方有必要評估法制面之補充修訂或強化解釋。故按照消保法第 7 條第 1 項之規定，應確保該商品或服務，符合當時科技或專業水準可合理期待之安全性，並於同條第 2 項規定商品或服務具有危害消費者生命、身體、健康、財產之可能者，應於明顯處為警告標示及緊急

本報告之智慧財產權歸屬於國發會

處理危險之方法。基此，商品或服務若有採用到 AI 技術，若其可能有安全性之風險或對消費者產生危害，則企業經營者須適用前開規定確定其產品以符合可合理期待之安全性，或仍有危害可能時，進行明顯處之警告標示並說明對緊急危險之因應。故本年度國際上相關法制提及應提醒消費者其互動對象為 AI，或告知其利用相關服務可能產生之歧視（包括可能與其他消費者不同之差別待遇）或負面影響等風險，若不予以告知將可能對消費者之生命、身體、健康、財產產生損害，應可直接透過第 7 條規定予以要求。惟具體應如何告知、如何警示、告知之原則或必要之內容等，並無法從通用性之規範看出。

於定型化契約層面，企業經營者提供涉及 AI 技術之商品或服務予消費者，會依其個別商品或服務之情況，建構適用之契約條款或規約，相關條款基本應適用消保法關於定型化契約之規範，亦即必須符合第 11 條之平等互惠原則、利於消費者之解釋原則及第 12 條之誠信原則，同時亦須依據第 13 條向消費者明示或公告。然而，上述原則規定如何具體落實於 AI 商品或服務之提供，尚未有更細緻之說明或解釋，尚須有具體情境或事例對應，方能歸納出可作為判斷之參考原則。而由於 AI 種類與應用情境廣泛，若要進一步依據第 17 條訂定定型化契約應記載及不得記載事項，必須先評估要擇定哪類型之商品或服務，方得循求對應之中央主管機關，擬定定型化契約應記載或不得記載事項，將應有之權利義務關係詳加要求。

至於消費資訊提供層面，按消保法於第 22 條第 1 項開宗明義強調企業經營者應確保廣告內容之真實，其對消費者所負之義務不得低於廣告之內容。並於第 23 條要求刊登廣告之媒體經營者明知或可得而知廣告內容與事實不符者，就消費者因信賴該廣告所受之損害與企業經營者負連帶責任。故若事業利用 AI 生成商品或服務相關資訊、圖像或動畫，用以吸引消費者購買或訂閱服務，則該內容應屬於廣告，而需適用上開廣告之規定。惟對於廣告部分，並未與揭露義務對應，僅於第 24 條鏈結商品標示法，要求須依商品標示法進行標示，及中文

本報告之智慧財產權歸屬於國發會

書說明書等規定，而廣告為 AI 生成並非商品標示法要求須為商品標示之範疇。

而廣告內容為 AI 生成而非真實之自然人或事物，並不代表即為不實之廣告，例如 AI 生成人體模特兒提供線上試穿展示、或透過 AI 生成商品 3D 圖像等，若無上開第 7 條商品安全性問題，則僅能回歸消保法第 4 條規定，將上述相關資訊之提供，解釋為向消費者說明商品或服務之使用方法，維護交易之公平，提供消費者充分與正確之資訊，及實施其他必要之消費者保護措施。雖有《詐欺犯罪危害防制條例》第 31 條規定（詳後）要求平臺業者揭露內容為生成之訊息，但其揭露義務範圍亦有限，而 AI 生成資訊亦非商品標示法要求須予標示之事項，故是否有必要強化規範，有討論空間。

此外，若消費者係因透過線上與 AI 互動獲得相關建議或由 AI 協助其作成交易決定而受到損害，是否可以認為該服務之提供，不具當時科技專業水準合理期待之安全性，恐有疑義。蓋 AI 技術或服務應用所導致之損害，如何定義，有其爭執之空間，故仍有必要加以解釋，或透過適切之規範或指引加以明確化。至於更進一步對於 AI 開發者或部署者義務具體要求，則尚非目前消保法所能因應。

三、 打詐相關法令修正，部分強化 AI 技術應用犯罪之規範與防詐措施

有鑑於國內詐欺活動猖獗，行政院於 2022 年即頒定「新世代打擊詐欺策略行動綱領」，並於 2023 年修正提出「新世代打擊詐欺策略行動綱領 1.5 版」。法制面則分別於 2023 年 5 月增修打詐五法，於 2024 年 5 月再提出打詐新四法。

2023 年之打詐四法中，對於運用 AI 所為之欺詐行為，主要顯現於 5 月修訂通過之《刑法》第 339 條之 4 針對犯第 339 條詐欺罪而得加重其刑之加重詐欺罪，新增第 1 項第 4 款「以電腦合成或其他科技方法製作關於他人不實影像、聲音或電磁紀錄之方法犯之」之要件，

本報告之智慧財產權歸屬於國發會

究其立法理由，主要是著眼於網路資訊及 AI 技術之運用快速發展，以電腦合成或其他科技方法製作關於他人不實影像、聲音或電磁紀錄，可能真假難辨，易於流傳。詐騙集團之犯罪手法亦推陳出新，為取信被害人而以上開方法施以詐欺行為，易使被害人陷於錯誤，且可能造成廣大民眾受騙，其侵害社會法益程度及影響層面均較普通詐欺行為嚴重，有加重處罰之必要。此部分修法乃為針對 AI 深偽技術應用於對民眾之欺詐，因真假難辨而影響甚鉅，透過加重刑法期望遏阻此類行為。

2024 年打詐五法部分，則係於《詐欺犯罪危害防制條例》第 31 條第 1 項第 4 款就網路廣告平臺業者刊登或推播廣告部分，要求應於廣告中揭露廣告使用深度偽造技術或 AI 生成之個人影像。並於同條第 4 款定義深度偽造，為以電腦合成或其他科技方法製作本人不實之言行，並足使他人誤信為真之技術表現形式。此一規定主要係促進大型廣告平臺業者之資訊透明度，要求平台業者必須標記所提供之廣告內容為 AI 生成，避免利用生成式 AI 技術偽冒生存特定自然人之身分而進行詐騙，協助公眾對網路廣告真偽之判斷。然此部分僅是就數位平臺業者之廣告刊登要求標記，尚無法涵蓋平臺廣告投放以外之其他觸及消費者或使用者之 AI 內容。

四、 因應生成式 AI 相關機關構已逐步建立使用者層面之參考指引

就涉及 AI 使用者之軟性指導部分，目前國內尚未有如同日本消費者廳提供予一般消費者之指導文件，惟基於生成式 AI 於 2023 年迅速廣泛受到關注及應用，行政院於 2023 年 8 月則公布行政院及所屬機關（構）使用生成式 AI 參考指引[129]，提供行政院及所屬機關構人員使用生成式 AI 之參考，包括提醒對生成式 AI 產出資訊必須要再進行客觀且專業之最終判斷、不得完全信任生成式 AI 產出之資訊或以未

[129] 行政院及所屬機關（構）使用生成式 AI 參考指引，https://www.nstc.gov.tw/folksonomy/list/c79bf57b-dc94-4aff-8d14-3262b5559cfc?l=ch，最後瀏覽日：2024/11/07。

本報告之智慧財產權歸屬於國發會

經確認之產出內容直接作成行政行為或公務決策之唯一依據，或採用生成式 AI 為輔助工具應適當揭露及其他涉及資安、個資保護、著作權及其他資訊使用規定應注意之管控等。此外，於教育層面，教育部臺灣學術倫理中心則有訂定教師因應生成式 AI 之教學指引，各級學校亦有個別訂定之生成式 AI 學習應用、教學等相關參考指引等可為參考。

肆、 小結

國際上對於 AI 產品或服務風險控管之專法，如前所述，目前主要係歐盟於 2024 年通過並公布第一部就 AI 相關產品或服務，以風險等級為基本規制架構之監管專法。絕大多數國家目前尚未有對於 AI 產品及服務較為全面之監管專法制定，僅有美國部分州（如科羅拉多州）有跟進部分規範。而歐盟 AIA 之公布，是否將因布魯塞爾效應而促使各國開始提出 AI 監管專法尚需觀察，但已更進一步帶動國際社會對於 AI 監管法制政策更具體之討論。然而，各國於 AI 之技術開發或應用，其程度、進程及發展之優勢或劣勢皆有相當差異，對於該如何進行 AI 相關之監管作為，是否應建立國際共通之監管原則等問題，近年來亦有國家透過國際會議尋求共識。例如 7 大工業國組織（G7）2023 年就廣島 AI 進程達成之協議，以及以英國為首於 2023 年與 2024 年舉辦之 AI 高峰會，所提出之布萊切利(Bletchley)宣言以及首爾(Seoul)宣言等，目的即在逐步建立對 AI 發展之國際監管共識。然而，要建構完整之 AI 監管機制並達到國際共識，仍非一蹴可及之事，各國尚需仔細評估其應有之 AI 政策走向與需要，搭配其發展進程，進行符合國情之適切考量。故我國目前主要先以 AI 基本法之研議，逐步匯集各界對於國內發展 AI 之政策共識，再進一步評估所需搭配之相關措施，諸如法律、政策、產業措施、技術發展措施、權利保障措施等不同面向之配套作為。

本報告之智慧財產權歸屬於國發會

若要評估我國對 AI 相關研發、部署及應用涉及一般（終端）使用者/消費者層面之法制政策需求，需先了解國內之終端使用者/消費者現階段或短期內主要於何種情境可能接觸到 AI，而可能影響其權益，進而評估及思考國內現行規範是否有補強之必要，及是否應有其他法制政策配套。本次研析就電子商務產業 AI 運用情形之訪談，可以了解現階段國內產業於面對使用者或消費者端主要的 AI 應用，仍係以行銷目的為主。可能用於客戶的分析經營、提高使用者/消費者對網站的體驗，促進與優化個人化行銷（精準行銷）以及促進人機協作及資料歸納。也就是主要用於更有效率提供得以影響使用者/消費者決策之資訊，並鼓勵使用者/消費者之主動參與，透過積極有效率之互動提高服務之目標性與品質。以此應用層面觀之，如何讓使用者/消費者得知其參與之數位活動有 AI 之涉入，如何涉入及對其有何影響，可能是最直接需要評估之法制政策面向。使用者/消費者必須確實知曉其係與 AI 進行互動及其運作，方能進一步發掘其參與 AI 相關活動權益面有無受到不利之影響，而得以提出主張，或對法制政策提出需求。除此之外，則是就利用 AI 從事違法詐騙行為導致使用者/消費者侵害層面，提供法制面之防治或救濟。

而現階段國內涉及一般消費者或使用者保障層面，已完成之相關法制或配套作為因應，依據前開整理，主要係配合打詐政策所為之各項規範修訂，包括《刑法》對於 AI 生成不實內容之詐欺行為列入加重詐欺罪之範圍，以及《詐欺危害制條例》要求廣告平臺刊登或推播廣告涉及使用深偽技術生成個人影像之揭露義務等規定，屬於詐騙侵害面之防治規範。至於法規範以外之配套指導措施部分，主要則係針對生成式 AI 使用面，包括政府機關/構人員之使用，以及學校、教育體系之使用等建立相關指引，雖與部分國際規範方向近似，然相關法制政策打擊範圍仍然有限。故就我國後續針對一般使用者/消費者之法制政策，建議可為以下思考：

一、 透過軟性指導，提升企業經營者及消費者對於 AI 應用之意識

本報告之智慧財產權歸屬於國發會

目前對於國內 AI 應用情形之調查尚未有很完整之資料，國人對於參與日常相關活動是否有 AI 介入及其如何運作，除近兩年因生成式 AI 運用之相關資訊獲得較多關注外，未必有明確之認知。因此如何讓消費者就其可能常為接觸之 AI 應用有適當之認知，使之具備基礎知識或資訊得以避免不必要之損害，可建立適當之指導文件進行說明或宣導。日本消費者廳透過舉例方式說明 AI 生活應用之事例及應注意之事項，以圖文方式給予消費者淺顯易懂之資訊及工具，可為參考。而若要使效果強化，建議還須搭配對企業行為之指導，包括建議應以清晰簡單方式讓消費者知道其正與 AI 進行互動，何時告知之建議，建議告知之事項以及建議提供之客戶服務等資訊，供產業界得以參考落實，以使消費者得以取得產業端更直接之資訊，保障其權利。

二、 以函釋或指引補充現行法相關規範於涉及 AI 情境之適用

(一) 消保法商品服務須具備合理期待安全性與揭露義務相關規範

於國內目前對於 AI 產業應用對使用者/消費者影響程度尚未有較為細緻之調查資料前，建議可先就已知之重要問題於現行法規範加強解釋，或建立指引，強化相關商品服務於消保法層面之適用。例如對於事業經營者依據消保法第 7 條第 1 項規定對於所提供之商品或服務進入市場，應確保該商品或服務，符合當時科技或專業水準可合理期待之安全性。並於第 2 項要求商品或服務具有危害消費者生命、身體、健康、財產之可能者，應於明顯處為警告標示及緊急處理危險之方法等規定，若於企業經營者以 AI 提供商品服務情境，應如何適用進行解釋。

例如，若有採用 AI 技術對消費者於平臺或系統之相關活動進行資料蒐集及分析，並提供目標廣告、或消費建議之作為，若其作為有可能誘引消費者作成某種對其不利之決定，或產生誤導，甚至出現不合理之差別待遇，是否即不符合此處合理期待之安全性？或若因而會使消費者交付財物，或購買可能損及其健康之商品或服務，是否可用

本報告之智慧財產權歸屬於國發會

同條第 2 項規定要求必須進行警告標示或提供緊急處理危險方法？以此來處理目前我國消保法並未如同歐盟 AIA 或美國部分州法（如猶他州《人工智慧政策法》、賓州眾議院提出之《不公平貿易行為及消費者保護法修正草案》等）所要求之揭露義務問題，並於相關函釋或指引說明告知、警示以及須對可能誘導消費者之人工智慧生成內容進行標記之問題，與標記之方式等（歐盟 AIA、美國聯邦眾議院《保護消費者免受人工智慧欺騙法案》等），而對企業經營者進行必要之要求。

此外，目前許多數位平臺常運用演算法之資料分析，自動對不同之使用者或消費者提供不同之資訊或廣告。表面上也許是嘉惠供給與需求方之服務提升，使企業經營者可以將資訊提供給適切之消費者，同時便利消費者可以很快取得所關注或喜愛商品或服務類型之更新資訊，實質卻已對消費者進行分類，控制消費者可取得之資訊範圍。而此情形，消費者通常無法察覺，或就算察覺亦無法確實知道有哪些資訊已被演算法或 AI 自動篩除，此時是否仍可適用上開關於合理期待安全性之規定？或若可被認為是通訊交易之類型，是否可依據消保法第 18 條第 1 項第 6 款規定，由中央主管機關公告應揭露事項之方式，要求企業經營者需揭露上述 AI 或演算法篩選機制之應用，或若有提供消費者選擇不被分析之機制應予告知等事宜。

(二) 不實廣告相關規範之適用

目前我國並未有針對廣告之單一法律規範，就對消費者為不實廣告部分，主要涉及之規範有消保法及公平交易法（公平法）之適用。前者係於第 22 條第 1 項要求企業經營者必須確保廣告內容之真實性，對消費者所負之義務不得低於廣告之內容，並於第 23 條第 1 項要求刊登或報導廣告之媒體經營者明知或可得而知廣告內容與事實不符者，就消費者因信賴該廣告所受之損害與企業經營者負連帶責任。後者則是於同法第 21 條第 1 項規定，事業不得於廣告上或以其他使公眾得知之方法，對於與商品相關而足以影響交易決定之事項，為虛偽不實或引人錯誤之表示或表徵，於第 2 項例示何謂足以影響交易決定

本報告之智慧財產權歸屬於國發會

之事項，並於第 5 項規定廣告媒體業、廣告媒體業與廣告主對不實廣告之連帶損害賠償責任。此外，晚近則有《詐欺犯罪危害防制條例》為避免 AI 偽冒廣告使消費者難以辨識而要求平臺須對刊登之 AI 生成廣告予以標記之要求。

然而 AI 於廣告層面之運用如何為不實而得以適用上述不實廣告之規定，可能需要進一步探究。例如由 AI 自動生成模擬人像為模特兒，提供網路商城廣告利用，例如服裝、配飾之模擬試穿，或模擬真人動畫、圖像或聲音進行產品宣傳，若相關資訊酷似特定專家或個人之特徵而導致消費者混淆誤認，或導致消費者對於產品或服務產生某種信賴，是否即可適用明知與事實不符之要件？或若企業經營者有告知為 AI 模擬圖像，是否即可證明其 AI 模擬廣告內容並非刻意引人錯誤？亦非虛偽不實？若並非實際出現廣告文案或圖像，而是透過前述之消費者行為分析自動提供各種商品、服務之消費建議，刻意引導或操弄消費者之認知或選擇，此行為是否亦可屬於明知而故意引人錯誤之不實廣告而適用相關規範，恐有必要說明釐清。

(三) 評估建立 AI 相關商品服務之定型化契約之參考原則或指引

AI 於不同商業模式之運用可能對消費者有不同之影響，而現行消保法第 17 條定型化契約應記載不得記載事項之擬定，必須針對特定行業由中央主管機關訂定報行政院核定後公告。故若是就企業經營者提供商品或服務採用 AI 技術層面，要對消費者權益保障訂定定型化契約應記載或不得記載事項，基於 AI 類型眾多且應用情境之廣泛，以及現階段國內並無 AI 應用之單一主管機關，將很難訂立定型化契約應記載及不得記載事項。然而，事務上部分 AI 對消費者之應用型態，尚有共通性規則可予建構，故得考慮由行政院消保處評估是否以行政院角度訂定對於 AI 商品或服務定型化契約共通注意事項之參考原則或指引，提供各目的事業主管機關就所轄行業事務應用 AI 而產生對消費者特定之影響時，得有相關參考原則供其研議或調整其管轄行業之定型化契約應記載及不得記載事項。

本報告之智慧財產權歸屬於國發會

三、 進行 AI 實務應用對消費者影響之調查及探討，進一步盤點法規調適之需求

AI 實務應用範圍日益廣大且形態多元，消費者保護相關法制主管機關，若要有效評估適合我國國情及實務需求之法制政策，宜投入對企業應用 AI 於消費者商品服務提供層面之情形，所應用 AI 之類型或消費者實際之認知或感受情形等，以利進行整體面之評估。英國 DMCC 規定主要增強了具備消保與市場競爭監管與執法權限之 CMA 於數位市場監督權限，與我國消保與公平交易執法分流之情形有所不同。其考量之事前管制結構，亦與現階段我國法制政策有所不同。然而其規範強化 CMA 對數位市場調查權限層面，尤其加強其可對儲存於境內及境外各類樹為服務提供者所擁有之資訊、程式碼、演算法等資訊，並可要求其演示或測試等權限，即得以讓執法機關對於實務層面堆疊之程式、演算之運作與應用有更進一步之認識，以利有效之執法。

於我國消保、市場競爭分管，以及數位服務相關產業推動主管機關多元且難以單一擇定之情況下，建立如同 DMCC 事前管制並強化執法之單一法制，恐有其難度。在此之前，建議消費者保護相關主管機關可透過會議或其他委託調查方式，對於國內應處理之議題，或實務發展現況進行調與整理，作為法制政策規劃之基礎。

四、 長期 AI 商品服務法制規劃仍需予以評估

於探討 AI 與演算法之消保議題過程中，可以發現 AI 之開發、部署與應用其實是廣泛之議題。於 AI 不同生命週期之作為，都可能對於商品或服務之使用者或消費者產生直接或間接之影響，且相關影響亦可能是環環相扣的。例如從開發訓練階段若以經採用不公允、錯誤或具備歧視性之資料訓練 AI，則將該 AI 服務或產品進行後續部署或應用，實難期待其不會對使用者或消費者產生分析判斷之偏頗，或因而給予錯誤之訊息，誤導消費者而造成損害。就如同 AI 基本法的結構，

本報告之智慧財產權歸屬於國發會

即可看出 AI 之議題並非以現行單一法律規範調整之問題，甚至可以是未來須以整體數位服務商業與社會應用發展綜合評估之問題。故雖然現階段可考慮就現有法律加強解釋或提出指導，並強化調查或研究進一步了解 AI 對一般使用者或消費者帶來之影響。然而，長遠而言，仍需考量我國對於 AI 或演算法實務發展是否有必要有較為整合且全面之法制規範或藍圖，無論是從數位服務整體角度，抑或 AI 開發至應用論理、風險與權益保障之角度，皆為可持續評估之模式。

本報告之智慧財產權歸屬於國發會

項次 3. 焦點議題 3：AI 或演算法運用與勞工權益相關議題

壹、 背景說明

數位科技尤其是人工智慧（AI）的發展對勞工權益的影響，從開始有 AI 機器人應用議題時，即已有所討論。例如由 AI 機器人之應用可能導致之失業議題，進而提出機器人稅之探討，及針對利用 AI 取代勞工之企業徵收一定比例之稅收等，亦有於工作場域透過 AI 進行員工定位、監視、休假監督、工作評估等作為，是否對員工產生不利之影響等，屬於基本勞資關係當中之 AI 運用，導致現有勞工權益受到影響之議題。

此外，近年基於數位平臺演算法以及 5G 高速無線網路之高度發展與應用，加上疫情的影響，使得以數位平臺作為媒介，商品/服務提供者、勞力提供者以及商品/服務需求者之新型態商業模式高度發展，諸如立基於共享經濟而出現之 Uber 載客服務、因應 Uber 載客而修法興起之多元計程車服務平臺（例如台灣大車隊之 55688、Uber 多元計程車、LINE TAXI 平臺等）、美食外送平臺服務（如 Uber Eats 或 Foodpanda）等服務發展，使得依賴數位平臺獲得工作機會之勞動者（Platform Workers, 平臺工作者）增加，讓部分事業可以透過平臺機制將原先需要個別聘僱之勞動需求外部化，平臺也可充分開發與應用演算法精進工作指派之效率，進行勞動情形之監督或對工作效能進行評估等。此類商業模式打破直接之雇主與勞工關係，而形成以平臺為中心之多方服務提供型態，使得平臺服務多方參與者之間的關係變得複雜。尤其透過平臺派工之平臺工作者與平臺間之關係，平臺以演算法對平臺工作者進行監督、評估與調節工作指派之相關運作等操作，引發平臺勞動性質與相關勞動法制適用之疑問。

國際勞動組織(Internaitonal Labour Organization, ILO)於 2023 年即對於生成式 AI 可能職業或就業的影響，以國際行業標準分類作為基

本報告之智慧財產權歸屬於國發會

準進行調查[130]，並於 2024 年 9 月於網站公布將調查圖表等分析結果[131]。調查結果將行業受生成式 AI 應用之影響分為四個類型，分別為具有自動化潛力(Automation Potential)、得以增強潛力(Augmentation potential)、有很大未知數(Big unknown)以及不受影響(Not affected)等四類之行業。第一類具自動化潛力者，即是其業務最有可能以生成式 AI 進行自動化取代的工作。第二類，得以增強潛力者，則是該工作仍有極大部分需要人為完成，而生成式 AI 可以強化該工作執行的速度及效能。而第三類具很大未知數者，則是影響尚未明朗，其工作任務也許可以透過生成式 AI 強化，也可能之後完全被生成式 AI 之自動化取代，而時間之推移或技術的進步可能改變生成式 AI 對該行業之影響。由圖表分布大致可以看出，具備高度未知數之行業類型分布廣泛，足見 AI 對於職業影響層面仍有必要持續觀察。此外較為偏向文職之支援工作，落於基準線 0.5 分以後較可能因生成式 AI 走向自動化層面之機率極高，而較屬於需要體力之職業，則受生成式 AI 影響較低，此為生成式 AI 本身特性所致，故於不同 AI 類型之實務應用，其對不同產業別之影響亦應有別，尚無法一概而論。而 ILO 同時亦調查生成式 AI 對就業之影響，此部分則是以不同收入階層國家進行估計，可以發現高收入階層國家所面臨之就業影響較高，反映其經濟及勞動市場更加多元，而低受入國家則受影響較低，因為大多數人從事不會接觸 AI 之職業，例如農業、運輸或食品銷售等領域[132]。

AI 技術、產品或服務之應用，於對社會整體勞動關係之影響，由 ILO 調查可知，其影響可能因為產業類型、事務類型以及技術發展情形而變化，並非單一國家政策或法制面向之問題。而是否需要進行法制面之修訂以因應數位環境，尤其 AI 或演算法運用引發之重要勞動

[130] ILO, Generative AI and Jobs：A global analysis of potential effects on job quantity and quality, https://www.ilo.org/publications/generative-ai-and-jobs-global-analysis-potential-effects-job-quantity-and , last visited 2024/12/18.
[131] ILO, How might generative Ai impact different occupations, https://www.ilo.org/resource/article/how-might-generative-ai-impact-different-occupations , last visited 2024/12/18.
[132] Id.

本報告之智慧財產權歸屬於國發會

議題，國內外有不同的意見跟探討。本次趨勢說明主要以本計畫期間所觀測近期涉及 AI 勞動法制政策之趨勢發展，基於隱私議題將為另一焦點主題，故本主題之趨勢說明將不包括 AI 隱私相關法制趨勢之討論，而著重於 2024 年 3 月至 9 月間，涉及數位平臺、演算法與 AI 運用於工作場域或勞工法制政策內涵。包括歐洲議會及歐盟理事會對於數位平臺工作指令達成之臨時協議及歐洲議會接續通過之《平臺工作指令》(Platform Work Directive)，以及美國勞工部(United States Department of Labor, USDOL)發布《於公平勞動標準法及其他聯邦勞工標準下之 AI 及自動化系統對工作場所影響之指導意見》(簡稱「AI 勞動工作場所指引」)，並以 USDOL 5 月就 AI 及工作者福祉所發布之開發人員與雇主原則(Artificial Intelligence and Worker Well-being: Principles for Developers and Employers)等文件，以及從 2023 年討論至今，甫於 2024 年 9 月 10 日通過之新加坡《平臺工作者法》(Platform Workers Act 2024)等重點內容為核心，說明 AI、演算法及平臺勞動所涉數位勞動議題近期國際發展之重點，作為我國後續法制政策評估之參考。至於美國公平就業機會委員會(U.S. Equal Emoloyment Opportunity Commission, EEOC)，從 2021 年始，即經常對於 AI 與演算法可對就業影響之問題提出意見，亦曾於 2023 年底發布對於 AI 雇主之技術指引－評估 1964 年民權法案第 7 章之就業選擇程序使用軟體、演算法及人工智慧之不利影響(Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964[133])，於 2024 年並對 EEOC 與 AI 之關聯公布一份簡短的聲明[134]，基於本次研析範圍係以本計畫執行期程之發展為主，故不列入 2023 年之技術指引，其 EEOC 角色聲明部分，則僅簡單說明何種雇傭活動與 AI 及

[133] USEEOC, Select Issues: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964, https://www.eeoc.gov/laws/guidance/select-issues-assessing-adverse-impact-software-algorithms-and-artificial , last visted 2024/12/25.

[134] USEEOC, What is the EEOC's role in AI? , https://www.eeoc.gov/sites/default/files/2024-04/20240429_What%20is%20the%20EEOCs%20role%20in%20AI.pdf, last visited 2024/12/25.

本報告之智慧財產權歸屬於國發會

自動化技術相關，以及 AI 如何之使用可能導致雇傭之歧視，並未有更進一步之分析或指導，其內涵與本次 USDOL 探討之方向相同，故亦不特別納入趨勢摘要。

貳、 近期國際發展趨勢重點

一、 美國

(一)公平勞動標準法及其他聯邦勞工標準下之人工智慧及自動化系統對工作場所影響之指導意見（Artificial Intelligence and Automated Systems in the Workplace under the Fair Labor Standards Act and Other Federal Labor Standards[135]）

USDOL 之工資與工時局(Wage and Hour Division, WHD)著眼於愈來愈多雇主於工作場所或工作中，使用 AI 或其他自動化系統，而 AI 或自動化系統雖可簡化雇主之管理，提高工作場所效率及安全，並強化員工問責，惟若無適切之人為介入監督，此類運用可能會對於聯邦標準產生潛在的法遵疑慮。故於 2024 年 4 月 29 日針對雇主於工作場所使用 AI 或其他自動化系統時，如何適用聯邦勞工相關規範，諸如《公平勞動標準法》(Fair Labor Standard Act, FLSA)及其他聯邦法律如《家庭與醫療假法》(Family and Medical Leave Act, FMLA)、《職場母親集乳保護法》(Providing Urgent Maternal Protections for Nursing Mothers Act, PUMP Act)等公布指導意見。相關法規重點在提醒雇主於應用 AI 於工作場所時，必須符合相關法律規定，並為非法行為承擔應有之責任，且不得以該系統為軟體開發商所設計而主張免責。

[135] USDOL, Artificial Intelligence and Automated Systems in the Workplaceunder the Fair Labor Standards Act and Other Federal Labor Standards , FIELD ASSISTANCE BULLETIN No. 2024-1, https://www.dol.gov/sites/dolgov/files/WHD/fab/fab2024_1.pdf, last visited 2024/08/26.

本報告之智慧財產權歸屬於國發會

本指導意見所指涉之 AI，其定義係依據美國聯邦 AI 倡議[136]之定義，係指一種以機器為基礎之系統，可以透過一組由人類定義之目標，作出能夠影響現實或虛擬環境之預測、建議或決策。而 AI 系統係使用機器以及以人類為基礎之輸入，以感知真實或虛擬之環境、透過自動化之機制將相關感知抽象化並形成模型，以及使用模型推理以形塑資訊或行動之選項。至於所謂的自動化系統，則係指以電腦或軟體為基礎之工具，通常用來代替人類執行工作場所之管理任務，而演算法則係一組用於工作場所或其週邊蒐集特定資料之規則，再於工作場所運算作成決策[137]。

不同的 AI 系統對於雇主而言，可以扮演不同的功能，包括工時追蹤、績效追蹤分析、任務分配等，按個別情境有別。而 AI 可能用於遠端工作、混合之工作或現場之工作場所，故此「AI 勞動工作場所指引」並不限於涉及遠端工作之 AI 應用，而應涵蓋所有涉及 AI 運用之就業，無論工作者於何處進行工作[138]。

運用 AI 於工作場域與聯邦相關勞工標準或規範適用之指導重點大致如下：

1. AI 與《公平勞動標準法》

FLSA 規範之基本原則，係員工之每小時工作薪資必須達到聯邦之最低工資，且每週工時若超過 40 小時，超過的工時薪資必須至少為正常工資之 1.5 倍。且無論員工生產力或績效如何，只要有做到多少工時，就應該要給付多少報酬，且不以積極勞動之時間為限，尚包括等待之時間或短暫休息的時

[136] 15 U.S.C. § 9401(3) The term "artificial intelligence" means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to-
(A) perceive real and virtual environments;
(B) abstract such perceptions into models through analysis in an automated manner; and
(C) use model inference to formulate options for information or action.

[137] Supra note 135, A.

[138] Id.

本報告之智慧財產權歸屬於國發會

間等。而雇主也有義務必須以合理的努力，以了解員工之工作時間，並保存精確之工時紀錄。所謂合理的努力，美國勞工部認為需視具體個案而定。例如一般來說，雇主可能會提供工作時間紀錄工具或報告程序，以清楚記錄員工之工時；然而，於涉及遠距工作之情況時，可能會有在非預定時間(non-scheduled time)工作的情況，則需要提供員工非預定時間工作之報告流程，以利雇主正確計算工時。然而若實際運作上雇主有阻止或不鼓勵員工準確回報工時之情況，則即使雇主有提供非預定時間工作回報流程，亦不能認為已盡合理之努力[139]。

因此對於 FLSA 之適用而言，雇主所應該注意的，係如何確保運用 AI 進行員工工時之追蹤、監督或計算之精確性與完整度，不至於因為 AI 運算沒有人為監督，或漏未將休息時間或必要之等待時間納入計算，或因員工係於多重區域工作或離開固定工作區域，而影響以位置追蹤之工時計算 AI 運作等，導致雇主未完全計算員工工時而未為合法之公司給付，而違反 FLSA 規定[140]。

2. AI 與《家庭與醫療假法》

FMLA 主要是對符合一定要件之雇主，必須給予符合一定家庭或醫療原因之員工適切之工作保護與休假。同時要求給予員工與未選擇休假之相同條件下，繼續享有團體健康之福利。同時，因前述原因休假離開工作崗位之員工，銷假回歸時，必須恢復到相同或幾乎相同之職位[141]。

---

[139] USDOL, Employers' obligation to exercise reasonable diligence in trackingteleworking employees' hours of work, FIELD ASSISTANCE BULLETIN No. 2020-5, https://www.dol.gov/sites/dolgov/files/WHD/legacy/files/fab_2020_5.pdf, last visited 2024/11/4.
[140] Supra note 135. B.
[141] Id. C.

本報告之智慧財產權歸屬於國發會

AI 於工作場域之運用可能用以處理同仁休假之請求、追蹤休假情形以及整合出缺勤天數等功能，若無負責任之人工監督，而完全仰賴自動化之系統以處理相關要求，包括確認提出申請員工是否具備請假之資格等，有可能導致潛在之法遵風險，使員工依據 FMLA 休假之權利遭到剝奪。例如時間控管之系統可能如同前述關於 FLSA 之討論，錯誤的計算與決定員工是否有依據 FMLA 出休假申請之資格。計算錯誤而違反 FMLA，即使是人工計算亦時有發生，然而若為 AI 或自動化系統本身之設置或計算錯誤，則可能會導致對整體員工廣泛性之違法行為[142]。

此外，對於員工為申請 FMLA 等事宜須提供之資料的取得或審核，例如提供醫療相關證明以確定是否確實有具備嚴重健康狀況之家庭成員需要照護，或員工自己有嚴重需健康照護情況或有服役需要等，相關資料的提供皆有必要予以審閱確認，此部分若由 AI 處置而無人工適切監督，亦可能有錯誤判斷之疑慮，甚而導致蒐集過多關於申請者不必要之資料。而相關資料蒐集系統，亦可能被用於對申請者進行追蹤與分析，雇主必須確保該分析不得對於休假之員工進行報復、阻止員工申請 FMLA 規定之休假、或利用此系統作為是否聘用、晉升、處分或計算負面之出缺勤分數等。故雇主若有採用 AI 或自動化技術，必須監督各該系統或技術之使用，避免出現廣泛侵害員工主張 FMLA 權利之風險，並須確保相關系統之設置與運作符合 FMLA 之規範。

3. AI 與《職場母親集乳保護法》

PUMP Act 係對於 FLSA 之修正，主要在確保絕大多數需要進行哺乳之員工，擁有權利於合理的時間與空間進行集乳。

[142] Id. C. i.

本報告之智慧財產權歸屬於國發會

雇主所提供之空間不得是浴室(bathroom)，且必須遮擋視線使集乳不受到干擾。此一權利將一直持續至小孩出生後 1 年內皆有效力，且除非聯邦或州法另有要求，此一法案基本上不會要求員工須將集乳花費之時間補入工時。基於個別員工集乳需求有別，故集乳時間應符合個別員工之需求，雇主與員工可依據需求約定，但不得要求員工同意確定一個不符合其集乳需求之固定時段，約定亦須依據實際需求情況允為調整。

雇主對於 AI 之應用若係用於追蹤及確定員工工時及任務分配、管理休息時間及生產力評估等，則必須考量需集乳員工之需要，不得因為其依法進行集乳未達生產標準或監控之工時，則對其進行不利之評價或判斷，亦不得因此而要求員工必須補足工時，而違反 FLSA 之規定[143]。

4. AI 與《員工測謊儀保護法》(Employee Polygraph Protection Act, EPPA)

EPPA 主要禁止雇主對於員工採用測謊儀器，或對個人進行就業前之監督篩選。而依據 EPPA，所謂測謊儀器包括測謊儀、欺騙記錄儀、聲音壓力分析儀、心理壓力評估儀或其他類似之設備，用以就個人之誠實與否提出儀器診斷意見[144]。

而按照 EPPA，雇主非但不能要求或建議對現有員工或未來員工(pre-employment)進行任何測謊儀測試，並且不能使用、接受或參考任何對於現有或未來員工進行測謊儀測試之結果；亦不得依據相關結果對員工進行解雇、紀律處分、歧視、拒絕僱用、決定晉升或對其加以威脅。亦不得影響員工對於

[143] Id. D.
[144] Id. E.；29 U.S.C § 2001(3).

本報告之智慧財產權歸屬於國發會

雇主依據測謊結果之作為提出申訴、於訴訟程序中作證，或主張其於 EPPA 規範下保障之任何權利。

部分有限之行業可能於特定規定或條件下，可以透過合格之檢驗人員對現有員工或未來員工進行測謊，但必須對相關人員發出書面通知，解釋其權利及限制，並採用嚴格之標準。

部分 AI 技術若可透過眼睛測量、聲音分析、微表情分析或其他動作分析以暗示特定對象正在撒謊，則此類 AI 亦會被認定於此處禁止使用之測謊儀範圍[145]。

5. AI 與禁止報復(Prohibited Retaliation)

FLSA 規定任何人皆不能因為員工依據 FLSA 提出申訴或提出訴訟等原因，對員工以解雇或其他方式進行報復或歧視[146]。而只要雇主利用 AI 或其他技術對受保護之員工採取不利之行動，皆可能構成非法之報復，而所謂不利之行動包括阻止或妨礙員工提出可能違規行為之申訴或影響員工對 WHD 調查之配合，例如透過 AI 機制之運作對員工施以懲罰或紀律之評估；或利用 AI 監控員工受到保護之相關活動以採取不利之措施，例如偵測或監控被懷疑已向 WHD 提出投訴員工，或透過系統進行員工調查或資料分析，以預測員工成立工會之可能性並進行干擾等。綜合而言，使用 AI 或自動化系統於工作場所之雇主，應注意避免將此類技術用於報復依法主張權利之員工。雇主有義務遵守 WHD 關於禁止報復行為之相關規範。

[145] Id.
[146] Id. F.; 29 U.S.C. § 215(a)(3).

本報告之智慧財產權歸屬於國發會

最後本指導意見指出，AI 之應用可能有助於雇主遵循法律規範，但若沒有適當之人為監督，則相關科技的應用，有可能含有對員工潛在之風險，也可能違反 FLSA 以及 WHD 所主管之相關規範。且 AI 之應用於組織當中，因為係演算機制之重複運作，可能導致系統性之違法行為。而無論雇主採用哪類型之AI或自動化系統，只要其違反WHD所執行之規範，雇主皆必須承擔其責任，並確保其 AI 運用符合 WHD 執行之規範。

(二)人工智慧及工作者（勞工）福祉：開發人員與雇主原則

USDOL 於 2024 年 5 月 16 日以 AI 對工作者福祉為概念，考量 AI 之應用不但刺激創新並增加機會外，也改變許多工作以及行業的本質，故需將工作者可能因工作場所採用 AI 有產生相當之風險或損害，並使工作者得以受到使用 AI 之利益。基此，回應美國總統拜登 2023 年之行政命令，而訂定人工智慧及工作者（勞工）福祉：開發人員與雇主原則 (Artificial Intelligence and Worker Well-being:Principles for Developers and Employers[147])，作為全國 AI 開發人員與雇主共同遵行之指導方針。

本次公布之原則適用於在工作場所之 AI 系統開發以及部署，且所臚列之原則，必須於 AI 整體生命週期（包括設計、開發、測試、訓練、部署、使用、監督與稽核等階段）皆須納入考量。USDOL 指出，此處臚列之原則適用於所有事業或組織，個別原則彼此相輔相成，然並非所有原則皆須適用於所有行業或場所，仍需個別評估。此處原則僅作為提供企業之指導，僅為例示並未窮盡，AI 開發者與雇主仍須依據本身所處之情況以及與員工間之意見溝通，建立適合其組織之最佳化實踐。

[147] USDOL, Artificial Intelligence and Worker Well-being: Principles for Developers and Employers, https://www.dol.gov/general/AI-Principles , last visited 2024/08/26.

本報告之智慧財產權歸屬於國發會

本次原則摘要如下：

1. **以工作者賦權為核心**：工作者及其代理人，尤其那些來自資源較不充足之社區或社群的工作者或其代理人，必須被充分告知並實際參與針對使用於其工作場所之 AI 系統的設計、開發、測試、訓練、使用與監督等過程。

2. **以符合倫理之方式開發 AI**：AI 系統必須以能夠保障工作者的方式進行設計、開發以及訓練。

3. **建立 AI 治理以及人員監督機制(Human Oversight)**：採用 AI 之組織必須針對使用於工作場所之 AI，具備清楚的治理制度、程序、人員監督機制以及評估流程。

4. **確保 AI 利用之透明性**：雇主應該向工作者或求職者公開其於工作場所使用之 AI 系統。

5. **保障勞工與就業權利(Labor and Employment Rights)**：AI 系統之運用不能侵害或減損工作者之相關權利，包括組織權利、健康/安全的權利、薪資與工時的權利、反歧視及反報復之保護等。

6. **使用 AI 賦能工作者(Enable Workers)**：AI 系統必須能夠協助、補強及賦能工作者，並提升工作品質。

7. **對於受 AI 影響之工作者給予支持**：雇主應於 AI 相關工作轉換期間，為相關工作者提供支援或提高其技能。

8. **確保負責任的使用工作者資料(Worker Data)**：AI 系統蒐集、利用或創造工作者之資料，必須限定於特定範圍或地點，亦僅能應用於支持組織之合法業務目標，並受到負責任之保護與處理。

(三)《人工智慧與包容性招聘框架》

本報告之智慧財產權歸屬於國發會

USDOL 於 2024 年 9 月 24 日發布新聞稿，說明由「就業與無障礙技術合作夥伴」（Partnership on Employment & Accessible Technology, PEAT）所發布之《AI 與包容性招聘框架》(AI & Inclusive Hiring Framework)，該框架目的在透過提升透明度，以協助事業應用 AI 工具進行招聘時，減少 AI 無意中造成的行為或決策歧視(unintentional forms of discrimination)，促進身心障礙求職者的就業機會。由 USDOL 下的職業健康與身心障礙政策辦公室(ODEP)資助 PEAT 研發此 AI 框架。

當組織評估、收購或部署 AI 招聘技術時，每個區域都包含有關員工及求職者利益最大化與管理風險之資訊。依據美國國家標準與技術研究院(NIST)的 AI 風險管理框架，《AI 與包容性招聘框架》提出 10 個重點領域包括：

1. 確認就業與身心障礙、隱私法之要求。
2. 考慮組織需要的員工角色，建立員工的職責、培訓員工。
3. 將透過 AI 供應商蒐集有關組織計劃部署 AI 招聘技術之相關資訊，例如與 AI 技術的預期用途、預期優勢、輔助功能一致性狀態、可用性報告、風險分類、部署狀態與範圍的資訊，加入至 AI 系統清單並進行盤點與分類。
4. 制定與第三方合作、控管第三方風險等政策，與負責任的 AI 供應商合作。
5. 評估 AI 招聘可能帶來的積極與消極影響。
6. 為身心障礙者提供便利的求職申請流程。
7. 從 AI 供應商處蒐集可解釋的 AI 的說明及文件，並以明確的文字通知使用者，向使用者描述該 AI 的目的與應用方式。
8. 制定有效的人為監控之政策與流程，並決定組織內部之關鍵監管人員。
9. 定義並管理 AI 申訴事件，與內部人員、外部使用者溝通、持續追蹤事件，留存相關紀錄。

本報告之智慧財產權歸屬於國發會

10. 定期監控 AI 效能，評估 AI 可信度，決定 AI 技術的配置、維修、逐步汰換及停用。

此框架結合政府、業界及身心障礙倡導者的意見，協助事業在 AI 時代下，採取公平的招聘流程。事業不需要一次施行 AI 和包容性招聘框架的所有內容，可隨組織的 AI 營運發展來逐步推行此框架。

二、 歐盟平臺工作指令

2021 年歐盟執委會針對日益成長的數位勞動力平臺及利用數位勞動力平臺取得勞動機會之龐大人口，包括叫車服務、送餐服務、線上資料編碼或翻譯服務等各類服務提供，所引發之法律適用及保障等議題，提出平臺工作指令（Platform Work Directive[148]）草案。該指令於 2024 年 3 月由歐盟理事會與歐洲議會宣布，主要內涵係針對改善數位平臺工作者之勞動條件並規範數位勞工平臺對於演算法之使用。而理事會主席與歐洲議會 27 個會員國談判代表於 2024 年 2 月 8 日達成臨時協議，期待未來通過之指令，可以使人力資源管理中之演算法運用更加透明，並確保相關自動化系統由合格之人員監控，工作者有對自動化決策提出異議的權利，並有助於確定平臺工作者之就業情形，使其享有應有之勞動權利[149]。其後，平臺工作指令隨即於同年 4 月 24 日由歐洲議會完成一讀，於 10 月 23 日經歐洲議會與歐盟理事會主席簽署並於 11 月 11 日正式公告於歐盟官方公報。

2024 年 3 月份宣布之臨時協議，揭示了法制建構將主要關注於兩個層面，其一為處理平臺工作模式的假性自僱(false self-employment[150])議題；其二則是規範於工作環境中的演算法管理監督之問題。

[148]European Commission, DIRECTIVE(EU) 2024/2831 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2024 on improving working conditions in platform work, https://eur-lex.europa.eu/eli/dir/2024/2831/oj , last visited 2024/12/17.

[149] Council of the EU, Platform workers: Council confirms agreement on new rules to improve their working conditions, 11 Mar. 2024, last visited 2024/9/4

[150] 假性自僱(false self-employment)，於我國學界實務常指涉「假承攬，真雇傭」之情形。

本報告之智慧財產權歸屬於國發會

第一部分關於平臺工作之假性自僱現象，臨時協議著重於在尊重各國勞工制度之基礎下，平衡並確保歐盟之數位勞動平臺上超過 2800 萬名工作者之基本保護。各會員國共識主要針對法律推定(legal presumption)的層面，協助確認平臺工作者實際的受雇情形。協議並指出，對於新措施之實施，會員國將對數位平臺及主管機關提供指引。臨時協議於解決假性自雇問題部分，大致有以下 4 個重點[151]：

1. 會員國將於法律體系中建立勞雇關係的法律推定(legal presumption of employment)，當發現有實際指導或控制事實時，則會適用此一推定。

2. 相關事實判準將依據國法律及集體協議來確定，亦須考慮歐盟判例法。

3. 透過數位平臺工作之人員，其代表(representative)或國家主管機關可引用此一法律推定，主張他們被錯誤分類。

4. 必須由數位平臺自行證明勞雇關係不存在。

就第二部分演算法管理監督層面，此次協議著重於確保平臺工作者能夠充分了解(duly informed)自動監督或決策系統於涉及聘用、工作條件以收入等之應用情形。禁止平臺運用自動監控或決策系統對於平臺工作者特定之個人資料進行處理，例如涉及生物識別之資料或關於其情緒或心理狀態等。此外，於自動決策之運用層面，亦須確保人為之監督與評估，工作者並有權請求對平臺相關決策之說明與檢視[152]。

指令前言第 4 點提出訂定此一指令之背景，主要係數位化發展改變了工作的環境，可以提高生產力並增加工作的靈活性，但也會對就業或工作條件帶來風險。以演算法為基礎之科技，包括自動化監督或決策系統，帶動數位勞動平臺的出現，若其能夠被適切的監督，可以

[151] Supra note149.
[152] Id.

本報告之智慧財產權歸屬於國發會

為傳統社會環境下無法獲得體面及高品質工作之人，拓展或創造與不同工作接觸的機會。但若沒有適切的監督或規制，此類勞動模式也可能造成技術監控，導致權力失衡或決策上之不透明，也為勞工之工作條件、健康、安全、平等以及隱私帶來風險[153]。

本指令所定義之「平臺工作」(platform work)，依據草案第 2 條，係指任何透過數位勞動平臺進行組織，且由個人於歐盟境內基於其與勞動平臺或中介服務提供者之契約關係，於歐盟境內所執行之任何工作，至於契約關係是否存在於該個人或中介服務提供者與服務接受者間，則非所問[154]。「執行平臺工作之人」(person performing platform work)係指任何執行平臺工作之個人，無論其契約關係之性質或係由哪一方參與者指定[155]。至於「平臺工作者」(platform worker)，則係任何執行平臺工作者當中具有僱傭契約或依會員國法律、集體協議、慣例或法院判例，被視為具有勞雇關係之人[156]。而此處所謂的「數位勞動平臺」(digital labour platform)則係指提供滿足符合指令第 2 條第 1 項(1)款項下要求之服務的任何自然人或法人。該款之要求為[157]：

1. 所提供之服務至少部分為透過遠端電子方式所提供，例如透過網站或行動應用程式。

2. 其服務之提供係基於服務接受者之請求。

3. 此類服務必要條件，必須係規劃由個人提供之工作需有報酬作為對價，而無論該工作係於線上或特定地點執行。

4. 該服務涉及自動化監控或決策系統之採用。

---

[153] Council of the European Union, Proposal for the DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on improving working conditions in platform work-Analysis of the final compromise text with a view to agreement, Brussel, 8 Mar. 2024, https://data.consilium.europa.eu/doc/document/ST-7212-2024-ADD-1/en/pdf , last visited 2024/9/4.
[154] Id. Article 2. 1 (b).
[155] Id. Article 2. 1 (c).
[156] Id. Article 2. 1 (d).
[157] Id. Article 2. 1 (a).

本報告之智慧財產權歸屬於國發會

本指令對於平臺工作之規範原則，係以確立勞雇關係或地位，以及對於演算法之管理，為規範之重點。此外，另就平臺工作之透明性與救濟、執法提出必要之要求，大致說明如下：

1. 勞雇關係之定位(Employment Status)

平臺工作對於勞工之保障，最重要之前提在於確定勞雇關係，指令提醒會員國應具備適當且有效的程序，以查證並確認從事平臺工作之人員正確的勞雇狀態，以確定是否存在符合會員國法律、集體協議或慣例所認定之勞雇關係，以及對法院判例與本指令第 5 條法律推定之情形[158]。對於勞雇關係是否存在的判斷，必須以實際執行工作之相關事實綜合判斷，包括是否採用自動化監控或決策系統進行工作之規劃等，而不論該工作關係於參與平臺工作之各方於契約當中如何分類[159]。一旦認定勞雇關係存在，雇主必須依據會員國法律規定，明確承擔應有之責任。

至於臨時協議所強調之法律推定，指令第 5 條指出，若依據會員國之法律、集體協議或慣例，平臺對於執行平臺工作之人具備控制與指導(control and direction)時，該數位勞動平臺與執行平臺工作之人間的契約關係，應於法律上被推定為勞雇關係(employment relationship)[160]。若數位勞動平臺想要推翻此一法律推定，則必須自行負擔舉證責任，證明該契約關係並非會員國法律、集體協議、慣例或依循法院判例所認定的勞雇關係[161]，以平衡平臺與執行平臺工作者之間於勞雇關係間權力上的不平衡[162]。

158 Id. Article 4. 1.
159 Id. Article 4. 2.
160 Id. Article 5. 1.
161 Id.
162 Id. preface (32).

本報告之智慧財產權歸屬於國發會

為使此一法律推定發揮效能，會員國應以平臺工作者之利益為基礎，提供便利之程序，以建構有效且可被推翻之法律推定機制。且會員國必須確保此處之法律推定，不會對平臺工作者或其代表增加需要確定其勞雇情形之額外負擔[163]。若確定從事平臺工作者勞雇關係是否存在於個案上有其必要性，則此一法律推定之要件將一體適用於所有相關之行政或司法程序[164]。

2. 演算法之管理

於演算法的管理層面，指令主要係從運用自動化監督或決策系統進行個人資料處理之限制、資料保護影響評估、自動化監督或決策系統之透明性、對自動化系統之人為監督、人工審核、安全與健康、知情與協商、工作者資訊、平臺工作者代表等面向進行規範。

其中關於限制採用自動化監督或決策系統進行個人資料處理的情形，可以看出本指令認為哪些行為之演算法操作，對於個人相關資料之保護影響較大。指令第 7 條第 1 項臚列禁止數位勞動平臺利用自動化監督或決策系統進行之行為包括：

(1) 處理與執行平臺工作之人員之情緒或心理狀態相關的個人資料；

(2) 處理任何與私人對話相關之個人資料，包括與其他執行平臺工作之人員或其代表之交流等。

[163] Id. Article 5. 2.
[164] Id.

本報告之智慧財產權歸屬於國發會

(3) 於執行平臺工作之人員未提供或執行平臺工作時，蒐集其個人資料。

(4) 透過個人資料之處理以預測平臺工作者之基本權利行使，包括基於歐盟基本權利憲章(Charter)所保障之結社權(right of association)、集體談判及行動權(right of collective bargaining and action)、與知情權及諮詢權(right to information and consultation)等。

(5) 處理可以推斷種族、血統來源、移民身分、政治立場、宗教或哲學信仰、殘疾、健康狀況(包括慢性病或愛滋病等)、情緒或心理狀態、商會會員身分、個人性生活或性取向等資訊。

(6) 依據 GDPR 第 4 條第(14)之定義，處理執行平臺工作之人員的任何生物辨識資料，並透過該資料與資料庫中個人生物識別資料進行比對，以進行身分核對。

運用自動化監督或決策系統進行個人資料之處理，應屬於 GDPR 第 35 條第 1 項可能對當事人之人權或自由造成高風險的處理態樣[165]，故指令第 8 條特別提醒，若採行此一作為，數位勞動平臺作為資料控制者，必須進行資料保護風險影響評估，並將評估提供勞工之代表人[166]。除了 GDPR 之要求外，數位勞動平臺所運用之自動化監控系統或用以協助作成影響執行平臺工作者決策的自動化系統，例如作成關於其工作條件的決策，像是取得工作任務指派的機會、收入、安全與健康、時間、晉升或契約狀態等相關之決定，須遵守及落實相關之資訊透明義務[167]。此部分之義務體現於指令第 9 條，

[165] Id. preface (44).
[166] Id. Article 8.
[167] Id. preface (45).

本報告之智慧財產權歸屬於國發會

規定會員國應要求數位勞動平臺向執行平臺工作者及平臺工作者之代表以及依據國家主管機關之要求，告知其使用自動監控或決策系統之情形[168]。該告知可以透過書面或電子形式提供，但必須採用清晰、簡單易懂之語言，並以透明、易懂且易於取得的方式呈現[169]。應告知之事項，應涵蓋由自動化決策系統所支援或採行之所有類型的決策，即使系統支持或採行之決策對於執行平臺工作者並不會產生重大影響[170]。指令並指出針對自動化監控系統或自動化決策系統應告知之事項，摘錄如下：

(1) 自動化監控系統應告知之事項

I. 此類系統被使用或正要導入之事實；

II. 該系統所監控、監督或評價之資料或行為類型；

III. 該系統進行監督之目的，以及如何達成該目的；

IV. 取得該系統所處理之個人資料之接受者或接受者之類型，以及任何該資料可能被傳輸或移轉之對象，包括企業集團。

(2) 自動化決策系統應告知之事項

I. 此類系統被使用或正要導入之事實；

II. 此類系統所作成或協助作成之決定類型；

[168] Id. Article 9. 1.
[169] Id. Article 9. 2.
[170] Id. Article 9. 1 (a).

本報告之智慧財產權歸屬於國發會

III. 此系統所考慮之資料類型、主要參數及其於自動化決策過程當中之相對重要性，包括個人資料或行為影響決策之方式等；

IV. 作成限制、暫停或終止平臺工作者帳戶、拒絕對平臺工作者所完成之工作支付酬金、以及作成關於契約地位之決定或其他同等或有負面影響之決定等之理由。

數位勞動平臺就自動化監控或決策系統之運用，可能延伸至對於平臺工作者整體面之管理，諸如對於工作的分配、薪資計算、安全健康的監控、工時監督、訓練機會的安排甚至涉及工作者之晉升或地位之相關決策，對於執行平臺工作之人員權益影響甚鉅，故有必要定期（每 2 年）對於系統所作出之決定進行影響評估，並邀請工作者之代表參與評估之過程[171]。平臺必須確保足夠的人力資源執行前述之評估，且確保相關人員具備可以推翻自動化決策結果之權利及能力，並保護其不致因推翻自動化決策結果，而受到解雇、處分或不利益之待遇。

數位勞動平臺有義務處理所採行之自動化決策系統的系統性缺陷，例如確保演算法運作結果不致於對執行平臺工作人員產生高風險結果（如產生歧視），若發現該系統會導致對執行平臺工作人員之歧視或侵害，則必須採取適當措施導正、修改甚至終止系統之利用[172]。此一原則主要體現於指令第 10 條之規定，該條文並要求對系統監督評估之相關資訊必須提供予執行平臺工作者之代表，或基於國家主管機關或平臺工作者之要求提供之[173]。同時強調，任何涉及、暫停或終止平臺

[171] Id. preface (48).
[172] Id.
[173] Id. Article 10. 4.

本報告之智慧財產權歸屬於國發會

工作者之合約關係或帳戶的決定或具備同等損害影響之決定，皆必須由「人」作成[174]。

相對的，平臺工作者也有權要求數位勞動平臺對於自動化決策系統所作成或協助作成之決定提出說明，且該說明採用清晰白話的用語，以透明易懂的方式提供[175]，且不得無故拖延。為保障平臺工作者此一取得解釋之權利，指令並要求會員國必須確保平臺指定具備適切之能力、訓練以及授權之聯絡人，讓平臺工作者得以與之討論或釐清造成該決定之事實、情況及原因[176]。

此外，指令對於其他歐盟勞動保障相關指令於涉及演算法自動監督或決策應用層面之要求並予以提醒及補充。例如對於運用演算法監督勞工安全與健康層面，要求數位勞動平臺必須對所採取之自動化監督或決策系統進行風險評估，尤其是對於可能發生與工作相關之事故、對社會心理(psychosocial)或人體工學(ergonomic)層面的風險[177]；同時必須評估此類系統之安全措施於特定工作環境之特性下識別風險之適合性，並採取適當之預防或保護措施[178]。指令並提醒會員國必須保障平臺工作者獲得歐盟關於勞工資訊及諮詢權、協商權以及知情權之保障[179]。勞工並得請專家協助審查資訊及協商事項並提供專家意見，若該平臺於相關會員國擁有超過250名員工，數位勞動平臺應承擔適當比例之專家費用[180]。

3. 平臺工作透明性要求

---

174 Id. Article 10. 5.
175 Id. Article 11. 1.
176 Id.
177 Id. Article 12.
178 Id.
179 Id. Article 13, 14.
180 Id. Article 13. 3.

本報告之智慧財產權歸屬於國發會

本指令為使平臺工作具備一定程度之透明度，規定會員國必須要求數位勞動平臺依據會員國之規定與程序，於平臺工作所在會員國之主管機關申報平臺工作者所從事之工作[181]。同時基於對勞工權益之保障，會員國並須確保數位勞動平臺向主管機關以及平臺工作者之代表提供以下資訊[182]：

(1) 透過相關數位勞動平臺從事平臺工作之人數，並依據其工作之程度、契約或受雇狀態等進行分類；

(2) 由數位勞動所確認並適用於此類契約關係之一般條款及條件；

(3) 透過相關數位勞動平臺定期執行平臺工作人員之平均工作時間、每人平均每週工作時數以及平均工作收入；

(4) 與該數位勞動平臺契約關係有關之中介機構。

指令要求成員國必須確保數位勞動平臺向國家主管機關提供有關平臺工作者之工作及其受僱狀態之相關資訊，並至少每 6 個月更新資訊一次。主管機關並有權要求數位勞動平臺補充說明相關詳細資訊，包括涉及受僱契約之相關資訊，數位勞動平臺並有義務立即回應並提供經過證實之答覆。但對於微型、小型或中小企業經營之數位勞動力平臺，會員國可減少資訊更新週期至每年 1 次[183]。

4. 救濟與執法

指令對於平臺工作者權益保障與執法層面，主要包括要求會員國須確保對平臺工作者，包括其他受雇或其他契約關

[181] Id. Article 16. 1.
[182] Id. Article 17. 1.
[183] Id. Article 17. 2-5.

本報告之智慧財產權歸屬於國發會

係已結束之人員，提供及時、有效及公正之爭端解決機制[184]。會員國亦必須確保有相當程序可以讓平臺工作者之代表或依據各會員國法律或慣例對協助執行平臺工作者主張權益具備合法權益的實體，可以捍衛平臺工作者之權利，並可參與任何司法或行政程序以執行基於本指令所形成之任何權利或義務，且若平臺工作者權益受到損害，亦可代表或支持一到多名平臺工作者進行權益主張[185]。

基於平臺工作者通常透過數位平臺遠端機制進行派工，缺乏共通之工作場所，無法讓平臺工作者彼此了解及相互交流，亦無法與平臺工作者之代表相互交流，為保障平臺工作者之權益，應該為其建立與工作組織之通訊管道，讓平臺工作者得私下、安全的相互交流並與其代表聯繫，數位勞動平臺有義務協助建立前述通訊管道，並尊重個人資料與隱私，避免存取或監控相關聯繫與通訊[186]。此外，為保障平臺工作者之訴訟權益，指令規定，會員國應保障國家法院或主管機關有權於訴訟程序中，要求數位勞動平臺必須提供其所擁有之相關證據，法院並有權命令平臺揭露其認為與訴訟相關聯之證據，包括機密資訊，但須確保法院可採取有效措施保護此類資訊[187]。

除訴訟證據之取得外，指令亦要求會員國必須採取必要措施保護執行平臺工作之人員或其代表不會受到任何對其不利益之待遇或負面之結果，包括平臺工作者或其代表對數位平臺進行投訴或啟動指令所保障之權利而可能受到任何不利之後果[188]。同樣的，會員國也必須採取必要措施防止平臺工作

[184] Id. Article 18.
[185] Id. Article 19.
[186] Id. preface (61)；Article 20.
[187] Id. Article 21.
[188] Id. Article 22.

本報告之智慧財產權歸屬於國發會

者因主張本指令所賦予之權利而遭到解僱、終止契約或類似之待遇。若確實發生被解僱、終止契約等類似情況，亦需確保平臺工作者有權向數位勞動平臺請求作成此類不利決定充分之理由，平臺須以書面提供相關理由[189]。

於執法層面，原則上各會員國主管機關於其管轄範圍內執行本指令之要求，主管機關間有權進行資料交換，及於透過相關資訊或最佳實務作法以進行合作。有鑑於平臺工作跨域的特性，草案指令亦特別規定若發生平臺工作者係於不同會員國執行工作，則會員國間可進行資料之交換以執行本指令之要求。會員國應規範具相當效力與韌性之處罰規定以有效落實本指令相關規範，尤其對於平臺工作者之侵權，必須制定對應之處罰措施，其中可包括經濟層面之處罰[190]。

三、 新加坡平臺工作者法

新加坡於 2024 年提出平臺工作者法(Platform Workers Act 2024[191])（草案），於 8 月 6 日進入議會審議，其人力部(Ministry of Manpower)對於本草案並於 9 月 9 日就法案發布官方聲明，議會隨即於 9 月 10 日審議通過。不同於歐盟之平臺工作指令對於演算法的關注，新加坡之平臺工作者法著重於對於平臺工作者生活層面的保障。雖並非 AI 或演算法之法案，然亦可顯示出不同國家對於平臺工作所關注之法制政策方向差異，故以新加坡人力部對法案之說明為基礎，摘述法案重點如下：

平臺工作者所提供的服務已成為新加坡人日常生活不可或缺之部分，然而此類工作者面臨收入不穩定、交通事故以及用於住房及退休

189 Id. Article 23.1,2.
190 Id. Article 24.
191 Singapore, PLATFORM WORKERS Bill 2024, Bill No. 26/2024, First reading, 2024-08-06, https://sso.agc.gov.sg/Bills-Supp/26-2024/Published/20240806?DocDate=20240806 , last visited 2024/9/11

本報告之智慧財產權歸屬於國發會

需求之公積金儲蓄有限等等的生活風險，且其受到平臺經營者一定程度管理及控制，與自營工作者也有所不同，無法完全控制其就業條環境與條件，因此需加強對從事平臺工作之人員的保障。因此期望透過本次立法，建構三個面向的保護，包括由平臺業者與工作者共同繳納中央公積金(Central Provident Fund, CPF)制度，以保障住房及退休條件的充足性、工作受傷之經濟補償制度、以及工作者代表之法律架構。

1. 平臺經營者與平臺工作者之關係定位

涉及到平臺工作，即有必要對於平臺以及平臺工作者間之關係進行定位。新加坡本次法案於此部分之認定與歐盟指令以及我國實務就是否為勞雇契約關係之討論有很大的不同。其直接認定平臺經營者與平臺工作者間既不是僱傭關係亦非自營工作者(freelancer)，而創設第三種工作關係，將平臺工作者獨立區隔為一類工作群體，並以本法保護其權利。

本法案所認定之平臺營運商(platform operator)，於 2024 年 8 月 6 日議會一讀審議之草案第 4 條規範，係指與一個或多個使用者以契約或其他協議進行平臺服務之提供，且對於平臺工作者提供平臺服務行使之管理及控制權者[192]。人力部 9 月 9 日新聞稿，則限縮於與用戶達成協議向其提供叫車或送貨服務，並利用資料決定與平臺工作者相關之決策，諸如工作任務之分配以及每項任務可支付之報酬，且對平臺工作者施以規則、要求或禁止限制者[193]。其範圍相較於一讀草案更加限縮，但進一步強調平臺採用自動化決策與監督之特性。

[192] Id.

[193] Singapore Ministry of Manpower（SGMOM）, New Platform Workers Bill to Strengthen Protections for Platform Workers, press release, 2024-09-09, https://www.mom.gov.sg/newsroom/press-releases/2024/0909-new-platform-workers-bill-to-strengthen-protections-for-platform-workers, last visited 2024/9/11.

本報告之智慧財產權歸屬於國發會

法案所欲保障之平臺工作者(platform worker)，於一讀審議之草案第 5 條規定，係指具備與平臺營運商之協議（無論是書面、口頭、明示或默示），於新加坡為平臺向使用者提供平臺服務者，其服務之提供受到平臺營運商之管理控制，並基於其服務之提供自平臺獲取報酬或利益，且服務提供時在新加坡[194]。人力部之新聞稿同樣將所提供之服務限縮於叫車或送貨服務，並再度強調其受到平臺營運商之監督控制，諸如任務之分配以及報酬之給付等。而平臺工作者會獲得一份收入單(earnings slip)以確定其平臺工作者之地位[195]。

2. 住房與退休公積金制度

本法要求平臺工作者與平臺經營者共同繳納公積金，其繳款比率將於 5 年內逐步提高，以期達與員工及雇主關係相當之比率。此公積金將按月存入平臺工作者之一般帳戶、特別帳戶以及醫療儲蓄帳戶，以協助其獲得與收入相當之受雇員工相同水準的住房及退休適足性，也同時提高平臺工作者之整體收入[196]。

強制增加公積金繳納之對象，主要為 1995 年 1 月 1 日以後出生之工作者，年輕工作者對於公積金之需求較高，因為其有住房需要，且有更長的人生得以累積，可自複利中獲得更多的收益。年長之平臺工作者則可按其意願自由選擇是否加入繳納公積金，因為其可能已經有相當之計畫滿足住房與退休的需求[197]。預計於 2024 年 11 月起，平臺工作者即可透過 CPF 網站選擇加入公積金繳納，此加入並不得撤回

194 Platform Workers Bill, supra note 191.
195 SGMOM, supra note 193.
196 Id.
197 Id.

本報告之智慧財產權歸屬於國發會

(irreversible)。年長之工作者，若選擇不加入包含住房的 CPF，仍會被要求繳納醫療儲蓄之公積金[198]。

3. 工傷補償機制

平臺工作者於工作時須承擔極大的風險，包括工傷的風險。因此為了讓平臺工作者於工傷期間可以獲得補償，本法要求平臺營運商必須為平臺工作者依據工傷賠償法(Work Injury Compensation Act, WICA)規定提供與受雇員工同等級之工傷賠償保險；平臺工作者與平臺經營者也皆有義務預防工作安全事故之發生[199]。

4. 平臺工作者代表法律架構

由於平臺工作者與一般受雇勞工不同，無法依照現有法律架構透過工會與雇主進行談判，因此必須為其建立適切之法律架構，並得以組織平臺工作者，使其可透過代表主張與爭取利益。因此本法創設了平臺工作協會(Platform Work Associations, PWAs)機制，其運作模式將比照受雇勞工之工會代表，且必須向 PWA 註冊處進行註冊，並由人力部指派註冊員(Registrars)進行監督。已註冊之 PWA 若已受到平臺營運商之認定，或透過其成員投票獲得授權，則可代表平臺工作者進行談判[200]。

四、 趨勢發展重點歸納

綜合前述包括美國、歐盟、新加坡對於數位勞動層面，尤其 AI 與演算法運用部分之法制政策發展趨勢，可以歸納出以下幾個關注面向（新加坡部分因其立法方向不以 AI 與演算法運用為重點，而是放在

198 Id.
199 Id.
200 Id.

本報告之智慧財產權歸屬於國發會

平臺工作者定性與權益保障層面，故以下歸納將僅以對應歐盟之平臺工作者定性納入歸納，合先敘明）：

(一)數位勞動平臺與平臺工作者法律關係定性之明確化

數位勞動平臺與平臺工作者之服務型態，在目前觀察之法制政策，包括歐盟或新加坡，可以發現其並非從同樣的角度切入規範，也未必與 AI 的應用正相關。例如，歐盟於平臺工作指令，十分著重與演算法應用之影響，但新加坡的平臺工作者法，則幾乎沒有考量演算法之問題，而著重於為平臺工作者確立基本的生活層面保障，切入點並不相同。然而其共通之處在於，必須將數位勞動平臺與平臺工作者之間，有別於一般勞雇關係之狀態，於法律面予以定性，以確立應適用之規範，或於必要時修正或創設新的規範。

目前觀察之兩種立法例，其一為推定僱傭關係之方式，如歐盟；其二則是創設新形態之工作關係，如新加坡。前者採行推定的做法，主要考量平臺工作模式可能多元，於符合相當條件即予以推定，使平臺工作者得以適用勞動保障相關之法令規範，對於平臺工作者之保障較為直接且有效率。而新加坡創設新形態工作關係之作法，則需要透過新興法制之建構，就平臺工作之屬性，將所欲對於平臺工作者提供保障之範圍明確於法律中訂定，好處是可針對平臺工作特性擇定必要之保障事項或給予特別規定，相對的，也可能遺漏應保障之項目，而損及平臺工作者權益。

(二)工作場域採用自動化監督或決策系統對勞工權益影響之因應

就工作場域 AI 運用層面，觀測趨勢主要呈現於 AI 介入進行自動化監督或決策之情境，對勞工權益可能產生哪些影響，以及法制政策層面須要如何因應。此部分為 AI 勞動議題層面進其較受關注之重點。其主要之規範大致有以下幾個面向：

本報告之智慧財產權歸屬於國發會

1. 採行 AI 進行自動化監督，必須確保採行相對之人工檢視或配套比對機制，避免因錯誤或過度評價影響員工/工作者權益。

例如 USDOL 提出之指導意見，即十分重視雇主運用 AI 監督須有適切之人為介入事宜，其指導主要提醒雇主，勞工於現行規範下擁有哪些權利，可能因為 AI 自動化的判斷而受到影響，甚至可能因為沒有人為介入之檢視，使得 AI 自動化決策之結果導致雇主產生違法之風險。例如用 AI 監督工作時間，不當扣除員工短暫休息之時間，或漏未將必要之等待時間納入工時評估等，或錯誤計算休假申請資格或蒐集過多之員工資料等等各種因 AI 錯誤評價而未有人工介入檢視可能產生的損害。USDOL 之開發人員與雇主原則，亦揭示組織必須建立 AI 治理與人員監督機制；於包容性招聘框架則提醒必須制定有效之人為監控政策與流程，並決定組織內部之關鍵監管人員。

此外，歐盟之平臺工作指令於演算法管理層面，強調必須對自動化監控或決策系統所作成之決定進行評估，平臺需要設置適切且有相當能力之人員對自動化決策機制加以審視，以避免受評估對象遭受不當而不利益之待遇，並有權予以調整。其更進一步要求必須對於負責介入演算法決策並調整之人員，給予工作上的保障，使其不致因為調整演算法結果而被解雇或為不利益之對待。

2. 使用自動化監督或決策機制，必須確保對個資相關法令之遵循，避免過度蒐集資料，並注意法令禁止應用之情境。

AI 監督或決策系統之運作必須蒐集、利用工作者資料，甚至分析及產生與工作者相關之進一步資料，故對工作者之個人資料與隱私保護必須更為慎重。USDOL 之開發人員與雇主原則，特別提醒必須確保負責任的使用工作者之資料，尤

本報告之智慧財產權歸屬於國發會

其必須限定於特定範圍或地點、應用於支持組織之合法業務目標、且受到負責任之保護與處理。歐盟平臺工作指令並提醒採用自動化監督或決策系統必須落實 GDPR 之相關要求，並做好資料保護之影響評估，同時臚列禁止數位勞動平臺利用自動化監督或決策系統進行的行為，諸如對工作者情緒或心理狀態之分析、監督私人對話或工作者與其代表間之交流、於非工作狀態時蒐集個人資料、預測工作者之基本權利行使取向、推斷對工作之者可能產生歧視之分類（如種族、血統、政治立場等）、進行生物辨識資料之比對等。

3. 須避免採用自動化監督或決策系統於可能對工作者產生歧視、錯誤分類或影響其基本權主張等之用途

USDOL 提出之指導意見明確提醒雇主必須遵守 EPPA 之規定，不得對員工採用測謊儀，或雖沒有使用測謊儀，但是透過 AI 技術達成與採用測謊儀類似效果之應用，例如透過眼睛測量、聲音分析、微表情分析或其他動作分析以暗示特定對象正在撒謊等，以避免因採行此類應用而對員工形成不利的決定，包括產生歧視、紀律處分、決定是否雇用或晉升等。其開發人員與雇主原則同樣也提醒，AI 系統之開發應用必須保障勞工與就業權利，確保 AI 運用不致產生歧視，並避免工作者受到報復。歐盟工作者指令則將可能產生歧視、錯誤分類與影響基本權利行使之應用列為禁止利用自動化監督或決策系統之範圍。

4. 工作者賦權與告知義務之落實

AI 應用於工作場所之監督，必須讓實際被監督之工作者及其代理人有充分的認知。歐盟平臺工作指令，即特別臚列自動化監控系統與自動化決策系統分別之應告知事項，除讓工作者知曉於其工作場域有採行相關之系統外，最重要的是

本報告之智慧財產權歸屬於國發會

要讓其了解這些系統在何時以及如何會對其監督或對其作成決策，而此監督或決策系統可能蒐集或採用之資料或參數為何，將可能對其產生怎樣的影響等資訊。相關告知必須採用清晰、簡單易懂的語言，並以透明、易懂且易於取得之方式呈現。USDOL 之開發人員與雇主原則除要求充分之告知義務外，更認為應該要讓工作者或其代理人實際參與將使用於其工作場所之 AI 系統的設計、開發、測試、訓練、使用與監督的過程。

(三)救濟程序或管道之確保

此部分主要保障勞工對於雇主於工作場域應用 AI，而對其造成損害或有疑義時，可以有適切之救濟管道，且雇主必須確保員工可以沒有顧慮的利用該救濟程序，而不會受到報復。相對的雇主也不可基於 AI 監視分析，發現特定員工可能會提出相關權益主張，而事前予以干預或阻止。例如 USDOL 提醒雇主必須遵守 FLSA，讓員工可以提出申訴或訴訟，不得利用 AI 分析阻止員工可能對違規行為的申訴或對員工施以懲罰、紀律評估或特別監控可能提出投訴的員工等。歐盟平臺工作指令，則要求會員國必須確保對平臺工作者可以獲得及時、有效及公正之爭議解決機制，以及讓平臺工作者及其代表可以爭取權利正當合理程序。

(四)保障勞工/平臺工作者可由自己或透過其代表爭取權益之機會

AI 進入工作場域之應用，無論是實體之場域，或是遠端之場域，對於場域之勞工/工作者而言，多數是較難察覺、理解或判斷的狀態，或相對於雇主或平臺，沒有足夠的知識及能力對於因 AI 運用對其產生的錯誤判斷、歧視與不合理待遇提出申訴。且若是遠端場域，包括平臺工作模式，工作者本身更難彼此交流而發現 AI 運用是否已產生傷害。且部分工作模式，於所處國家也未必會被認為屬於勞雇關係而

本報告之智慧財產權歸屬於國發會

能夠透過工作組織（如工會）主張權利。故有必要確保勞工或平臺工作者有表達意見或透過其代理者代表爭取權益的機會。

歐盟平臺工作指令即提醒會員國必須確保有相當程序可以讓平臺工作者之代表或依據各會員國法律或慣例對協助執行平臺工作者主張權益具備合法權益的實體，可以捍衛平臺工作者之權利；且要求數位勞動平臺必須建立平臺工作者與工作組織之通訊管道，讓平臺工作者得私下、安全的相互交流並與其代表聯繫，並須尊重個人隱私，並保障平臺工作者或代表不會因而受到不利的待遇。新加坡平臺工作者法雖然將平臺工作者獨立於一般勞工之外，然而亦強調必須保障平臺工作者能夠擁有能夠代表其主張權益的機制，並為此建構平臺工作者代表之法律架構，以及平臺工作協會機制。

參、 我國法制概況

一、 勞動部過往主要對實體場域機器人運用提出相關指導

我國勞動部過往對於 AI 運用對勞動場域之影響，主要是針對實體機器人運用的層面，曾針對工業用機器人以及協同作業機器人之運用，依據職業安全衛生法訂定工業用機器人危害預防標準，以及協同作業機器人作業安全評估要點。

二、 數位平臺與平臺工作者關係之定性已有相當討論與實務運作

對於近年來數位經濟發展下數位勞動平臺、AI 與演算法運用之相關勞動議題，我國現階段尚未有直接之修立法或配套規範。然而近年來因疫情促進外送平臺之發展，引發許多關於平臺外送員與平臺間關係應如何定性，是否存在從屬性而構成勞動契約，或僅為承攬契約等議題，勞動部、學界及法院實務皆有相當之討論。勞動部並有針對平

本報告之智慧財產權歸屬於國發會

臺勞動之從屬性議題作成專區，提供可參考之相關函釋，以及針對勞動契約之認定提出指導原則與檢核表供產業應用[201]。

(一)勞動部現階段可用於平臺勞動關係之相關規範、函釋或指導原則：

1. 勞動基準法勞動契約定義，納入之從屬性概念。

108 年勞動基準法修法對於第 2 條第 6 款勞動契約定義部分，從原來之「約定勞雇關係之契約」修正為「約定勞雇關係而具有從屬性之契約」。此次修法雖並非針對平臺勞動議題所為之修法，卻也為當時立法者綜整行政機關及司法機關實務上對於勞動契約採行人格、經濟及組織從屬性之認定特徵，所為之修訂。對不斷發展變化之平臺勞動關係之認定，有相當之助益。

2. 援引勞動部 104 年對勞動派遣與勞務承攬函釋，強調指揮監督是否存在對從屬性判斷之重要性。

對於勞務派遣與勞務承攬之判斷則參考勞動部 104 年 4 月勞動關 2 字第 1040125914 號函對於勞動派遣與勞務承攬之解釋，強調勞動派遣：指要派單位（機關）與派遣事業單位約定，由派遣事業單位指派所僱用之勞工至要派單位（機關）提供勞務，並接受要派單位（機關）指揮監督管理之契約。而勞務承攬，則係指定作人（機關）與承攬人約定，由承攬人為定作人(機關)完成一定之工作，定作人（機關）俟工作完成，給付報酬予承攬人之契約。如承攬人依約須指派所僱用之勞工至定作人（機關）工作場所完成工作者，定作人（機關）對承攬人所派駐人員，

[201] 勞動部，平臺業者與外送員法律關係（專區），https://www.mol.gov.tw/1607/28162/28652/28922/28925/ ，最後瀏覽日：2024 年 09 月 11 日。

本報告之智慧財產權歸屬於國發會

並無指揮監督之權，僅得檢驗工作成果，並依據該成果給付價金。由兩者之差異可以看出，指揮監督是否存在，對於判斷是否具備從屬性有直接的關聯。

3. 以勞動契約認定指導原則強調勞動契約應以個案事實及契約整體內容為從屬性認定，不以契約名稱為斷。

勞動部公布之勞動契約認定指導原則，於第 2 點即說明事業單位與勞務提供者雖得本於契約自由原則，約定勞務契約類型，但其法律關係是否為勞動契約，應就個案事實及整體契約內容，依從屬性之高低實質認定，不受契約之形式或名稱拘束。該原則並從人格從屬性、經濟從屬性、組織從屬性三個層面提供可資參考的判斷條件，以利評估從屬性與勞動契約存在。

(二)法院判決實務就個案面亦係以從屬性評估勞雇關係之存在

最高行政法院 110 年度上字第 488 號判決亦援引釋字第 740 號，認為必須考量勞務給付的性質，以個案客觀事實探求各勞務契約之特徵，諸如人的從屬性、親自履行、經濟上從屬性以及組織上從屬性等。而勞務契約之提供勞務者，若所從事職務上非如同委任契約之受任人或承攬契約之承攬人一般享有獨立性，而對於所屬事業已顯相當之勞雇關係特徵者，雖未具足從屬性之全部內涵，仍應定性雙方間之契約關係為勞動契約，依勞動基準法予以規範，俾能落實憲法保護勞工權益之意旨。

最高法院上開判決亦指出，基於上訴人對外送員之管家合作手冊內容觀之，外送平臺（上訴人）對所屬外送員不但訂有權利義務、管理工作紀律，同時針對其如何取餐、送餐、運送方式、消費者服務之提供都訂有明確的標準作業流程及違規者之罰則，外送員必須接受上訴人之平臺系統教學、職業安全、食品衛生及交通安全的教育訓練後，始具備工作資格；且訂明外送員可獲取之報酬，原則上按上訴人向消

本報告之智慧財產權歸屬於國發會

費者收取費用之85%計算，但因店家未營業或消費者取消訂單致未完成交易者，仍可領取空跑費，如店家延誤提供餐點達一定時間，外送員可領取等待費，即使因此退還消費者服務費，亦由上訴人與店家全額負擔、吸收，外送員無須分擔風險。又店家及消費者係分別與上訴人成立服務契約，外送員並非契約主體，外送員係與上訴人成立契約關係，由外送員依約履行取餐及送餐工作之義務（包括為上訴人向店家索取以上訴人統一編號製作之發票，並向消費者解說發票開立情形）等情況，足見外送工作應受平臺之指揮監督，具備人格及組織上從屬性。且所提供的勞務是為平臺營業所提供而非其自己之營業目的，故也具備經濟上的從屬性。因而認定平臺與外送員具備勞動契約之關係，平臺應依據勞工退休金條例規定申報勞工退休金。

(三)國內見解雖未達到直接推定，但與歐盟平臺工作指令之認定於個案上可能形成相同的結果，新加坡雖定性略有不同但保障平臺工作者之精神一致

勞動部與最高行政法院之看法，並未採取直接推定雇傭關係的作法，而係以從屬性評估為基礎，然最終於個案上之認定，可能與歐盟平臺工作指令採用之推定，產生同樣的結果。而歐盟指令要求會員國應該建立數位勞動平臺與平臺工作者間勞雇關係法律關係間推定之明文化，站在勞工保障的角度，除非平臺有反面事實舉證再進行爭執，法律面之推定對勞工之保障可能較有效率。

新加坡的平臺工作者法，看似跳脫勞雇契約之判斷，而透過新興立法賦予此類關係不同的法律定位，然究其規範之內容可以看出，其亦期待可以將平臺經營者與平臺工作者關係，提升與僱傭關係相當之等級，以對平臺工作者有充足之保護。我國部分地方政府亦有透過自治條例方式，確保外送員具備特定保障之事例，例如《臺北市外送平台業者管理自治條例》第4條、《高雄市外送平台業者管理自治條例》第4條及第5條《桃園市外送平台業者管理自治條例》第5條等，即要求外送平臺業者必須替外送員投保意外險，並確保該保險於外送員

本報告之智慧財產權歸屬於國發會

提供外送服務契約之存續期間之效力。此外對於外送員面對政府機關天災宣布停止上班上課應停止外送，並要求須受到足夠時數之職業安全、食品安全及交通安全訓練等並有明確之要求。此作法雖未直接定性外送員與平臺間之法律關係，但與新加坡平臺工作者法特別規定權益保障之精神一致。

三、 AI 基本法草案提示政府須因應人工智慧發展保障勞工權益

2024 年國科會提出之 AI 基本法草案，針對 AI 各面向應關注之重測重點進行揭示，於第 12 條就勞工權益層面，提出政府為因應 AI 發展，應避免技能落差，並確保勞動者之職業安全衛生、勞資關係、職場友善環境及相關勞動權益。並揭示政府應就 AI 利用所致之失業者，依其工作能力予以輔導就業。此一條文僅是政策層面宣示 AI 對勞動權益可能產生負面影響且需要政府政策面予以重視，然而，亦僅是大方向之宣示，仍需勞動相關法令之評估與配套，方能有其功效。

四、 除平臺工作者之法律定位外，對於平臺或其他勞動環境之 AI 運用，尚未見直接之法制規劃

我國目前對於 AI 與演算法應用對勞工影響之層面，除前述平臺與平臺工作者關係定性外，其他部分包括運用 AI 或演算法對於勞工業務執行之監督、判斷、績效評估、決策、權益保障與限制等相關層面，則尚未有直接對應之修立法或配套政策措施提出。

以現行法而言，《就業服務法》第 5 條第 1 項已有明定雇主對於求職人或所雇用之員工，不得以種族、階級、語言、思想、宗教、黨派、籍貫、出生地、性別、性傾向、年齡、婚姻、容貌、五官、身心障礙、星座、血型或以往工會會員身分為由，予以歧視。此部分規範範圍包括就業前之求職階段及就業後雇用階段，皆不得對勞工有所歧視。然而 AI 演算法之訓練及運用，若招募過程已進行履歷篩選，其演算法採用之分析參數及其運作是否已導致歧視，例如該演算法訓練係將於特定類型公司表現優異之員工資料納入訓練等，即可能篩選後履歷已出

本報告之智慧財產權歸屬於國發會

現歧視結果，即使公司於面試過程中確保不歧視，亦為時已晚。且若履歷配對篩選來自第三方人才招募平臺，則利用第三方平臺獲取履歷之公司是否能夠評估或確保履歷篩選之公平性，亦為問題。

此外，雇主於招募或雇用階段若有採用 AI 進行求職者情緒或表情分析等機制，亦可能涉及勞工資料取得適切性的問題。現行法有《就業服務法》第 5 條第 2 項第 2 款規定雇主不得違反求職人或員工之意思，要求提供非屬就業所需之隱私資料。而 AI 情緒、表情分析等監督機制，是否會過度蒐集求職者或受雇者面部特徵、表情或情緒資訊，導致對求職者或受雇者不當之隱私分析，或導致歧視性之分析結果與決策，上開《就業服務法》之規定尚無法處理此一情形。而《就業服務法施行細則》第 1 條之 1 第 1 項第 2 款所稱心理資訊，包括心理測驗、誠實測試或測謊等資料，是否包括前述特徵、表情或情緒分析資訊，亦未有定論。

此外，就平臺工作議題之討論，將平臺、AI 與演算法納入業務經營之情狀並非僅有外送平臺之類型。國內實務亦有其他於業務或職場運用 AI 之情境，例如國內著名計程車叫車平臺 55688，即採 AI 進行所屬計程車安全管理與智慧派遣[202];部分事業亦開始開發或應用 AI 進行人力資源之招募評估、監督、工作指派或進行各類分析（情緒分析、發展分析、工作效率分析等）[203]。相關運用可能會使事業獲得一定程度之便利性，甚至可能對員工之評價產生更客觀的評估資訊，然而，若 AI 採用參數之不適切、運用觀念不得當、或未有人工適切介入校準或檢視等，都可能對於受監督之工作者/員工產生錯誤或偏頗的評估，而若被監督分析之工作者/員工根本不知有 AI 監督之情事，或組織並未建構適切之更正、申訴等救濟管道，則對於勞工權益將有極為不利

[202] 臺灣大車隊，55688 平臺攜手新創 AI 展開智慧城市交通新貌，https://www.taiwantaxi.com.tw/Article?fid=70&sid=10892&tid=10919 ，最後瀏覽日；2024/09/11。
[203] 周尚勤，從同事變身績效主管》AI 打考績的人性考驗，能力雜誌，2018/12/24，https://mymkc.com/article/content/23075 ，最後瀏覽日；2024/09/11。

本報告之智慧財產權歸屬於國發會

之影響。因此對於在工作環境運用 AI 或演算法之相關情境，對勞工權益之影響以及法制政策面的評估，仍待更進一步思量。

肆、 小結

AI 運用於工作場域之態樣日益多元，部分用於生產創造，包括作為員工工作之輔助，提升工作效率；或用於管理生產或服務提供過程，提升產能或服務品質；或用於觀測掌握市場情報，提升事業市場分析效能等；當然也可能被用於人員招募、面試、績效管理、業務分派、場域或工作監視及其他視事業組織業務型態與需求的各項應用，為事業帶來招募效率、組織管理、業務推行與策略規劃之各種便利。然而，特定 AI 之功能、用途與分析/決策的結果，可能導致與其運用相關之勞工/工作者在不知情或無法控制的情況下，受到程度不等之不利影響或損害，有必要從法制政策層面予以思考。

一、 平臺與平臺工作者之關係與定位，雖非 AI 或演算法直接議題，但為數位平臺工作權利義務關係之根本，仍應審慎考量

本研析整理 2024 年度之觀測發展，可以發現 AI 若是被用於工作場域之自動監督或決策，無論是實體、遠端或透過平臺之工作型態，對於勞工/工作者權益之影響實有關注的必要。而若為平臺工作型態，則更需要在源頭確立數位勞動平臺與平臺工作者間的關係與定性，方能進一步探討對平臺工作者權益之保障，以及若平臺有透過 AI 或演算法對工作者進行監督或決策，應如何保障其權益或確保工作評價之公平性。故數位勞動平臺與平臺工作者關係，雖非與 AI 或演算法運用直接相關之法制議題，其亦為此類勞動型態工作者取得權益之根本，就整體數位勞動環境之法制政策評估上仍有其重要性。觀乎我國目前法制體系主要依據勞動基準法當中勞動契約之從屬性進行個案判斷，勞動部並透過函釋與指導原則之訂定協助進行勞動契約從屬性之認定。然而現階段國內法制實務以個案發生，方對是否符合從屬性予以認定，

本報告之智慧財產權歸屬於國發會

並就是否屬於勞動契約關係進行爭執。此一法制現況，使得日益蓬勃發展之平臺工作模式，及平臺工作者與平臺間關係無法於勞工投入及簽定相關工作契約之前，有更明確之認定，似不利平臺工作者之權益保障。

歐盟平臺工作指令及新加坡平臺工作者法，雖然對於平臺工作者之法律定位採取不同的認定，但其作為至少顯示一個共通的走向，就是應將運用數位平臺取得工作機會及執行平臺派定任務之工作者於法律上給予清楚明確的定位。此一作法可使此類非典型之工作型態，能夠有共通之法律定位，降低平臺與工作者間就法律關係、應適用之法律及雇主與工作者間對於工作權利保障之爭執。於數位經濟發展下，結合數位平臺之延伸商業模式將更加多元而複雜，而仰賴平臺取得工作機會之工作者，型態亦將不僅是外送員，地方政府對於外送平臺管理之自治條例僅能處理外送員職安、保險等層面之保障，無法協助於事前定性其契約關係，亦無法及於其他類型之平臺工作。故為讓平臺工作者與平臺間勞動關係之定性得以明確化,保障平臺工作者之權益,使法律關係穩定並降低爭議，宜考慮具備對於需要保障之平臺工作特性與權益加以定義及法制化，包括但不限於對於特定類型勞動關係之保險權益等,並評估是否給予推定之勞動契約關係或第三類勞動關係,因應平臺工作模式之發展。

二、 AI 及演算法應用對國內勞動環境之影響應予調查了解，以規劃適切之法制政策

目前國內勞動環境有哪些與勞工相關之 AI 應用，並未有明確之調查，討論多來自於國內外相關新聞資料以及法制已有討論關於招募與人力資源相關之就業篩選/歧視，或是勞工隱私的問題。然而，究竟在國內，除已受到關注之外送平臺外，AI 或演算法是否用於其他類型之平臺服務？於平臺派工或對工作者之評價或考核是如何運作？國內除平臺外有哪些產業有透過 AI 進行勞工監控或評核？對勞工權益有無不利之影響？於就業前端，事業有無/如何利用 AI 之演算分析進行

本報告之智慧財產權歸屬於國發會

履歷篩選，所採行之模式與技術為何？國內或跨國性人力平臺或專業人力資源社群網站之 AI 運用是否涉及不當之履歷篩選？以及不同類型 AI 之運用，對於勞工就業之機會或能力養成之需求影響為何？有關 AI 於勞動環境實際應用狀況與影響資訊等於國內皆不清楚，僅透過短暫有限之訪談，與實際狀況恐有相當之落差，建議勞動主管機關應加強對國內產業 AI 不同層面應用之調查，以利法制政策適切之評估與規劃。

三、 可先就現行法層面，就已知之 AI 或演算法之應用，及影響或運用型態，提供法律適用、遵循或應注意事項之指導原則

由 USDOL 之作法來看，其並未因 AI 於勞動場域之應用而立即進行法制面之調整，而主要係持續提出對於法制適用或 AI 應用開發之指導意見，將現行勞動相關法制規範於 AI 或自動化系統介入之情況下如何適用，以及雇主或開發人員，在開發或部署 AI 技術於工作場域時有哪些應注意之原則予以明確說明，並持續提醒於工作場域之 AI 運用必須有人為介入監控，且需要定期檢測評估以避免 AI 長期運作是否產生系統化之潛在風險等，同時也需給予受影響之勞工或工作者，有申訴或救濟的管道。USDOL 於公平勞動標準法等規範之指導意見部分，更是直接說明相關聯邦法律規範，於其所定義之 AI 及自動化決策技術範圍內如何適用，且強調該指導意見並不僅適用於遠端工作之 AI 應用，亦包括所有勞動場域之 AI 運用，且不論工作者於何處進行工作。基此，其係暫先跳過對於特定工作型態之定性（如平臺工作），而係就認為勞工權益有較大影響之 AI 或自動化決策系統之應用，進行法制適用及事業應注意事項之明確說明。

USDOL 此一做法也許是現階段國內勞動主管機關，於尚未能夠確切掌握國內實務 AI 於勞動場域運用情形，但已知可能有相關應用存在時，透過軟性指導原則之情事，將必要關注之法遵事宜，明確的向產業說明。無論國內產業是否皆已將國際討論之技術應用於組織相關之招募、監督或績效評估等面向，若已利用但因不清楚相關法令切

本報告之智慧財產權歸屬於國發會

實應如何適用而有違反規範之情況者，得儘速進行調整或排除影響；若尚未利用而已在評估利用者，亦可參考指導原則進行 AI 或演算法之開發或部署，建立適切的機制以避免違反法律或影響勞工權益。例如對雇主開發或採用人才履歷篩選或對員工之 AI 評估，應如何具體適用就業服務法第 5 條避免歧視、不得要求提供非就業所需隱私資料等相關規定，以及 AI 情緒、面部表情、特徵等分析技術之應用，是否屬於心理資訊及如何適用就業服務法相關規定等提出具體說明。

四、 長遠而言對於 AI 或演算法於勞動環境之應用，仍須考量更直接明確之法制規範

AI 或演算法應用於勞動環境已為不可擋之趨勢，現行勞動法規之思維並非數位經濟環境之思維，對於不斷變動商業模式及新興模式與勞工之關係，實難以有效應對，將出現許多複雜而需要透過一再解釋之事件或問題。2024 年趨勢所看到的，歐盟、新加坡是針對平臺工作先行走向法制化，雖歐盟層面是指令之性質，對於各國是否納入內國規範並無法強制，然而亦呈現了歐盟國家對於相關議題的共識，其中也包括了對於平臺運用演算法管理之規範。相關規範所重視的，並非只是平臺工作需要重視的議題，甚至是可以推導至所有 AI 應用於工作場域之情形。需要關注與要求的事項將因實務運用之增加而更加複雜，故即使不另立新法，亦建議未來得於現行勞動規範就 AI 或演算法決策須重視與避免之問題，進行補充規範。於我國 AI 基本法目前政策走向觀之，國內對於 AI 議題法制化未必可能如歐盟訂定風險控管之專法，故對於個別領域之法制面向仍應做具體考量，尤其 AI 應用對勞工權益之影響與因應，應係必要處理的議題，主管機關宜考慮具體之法制政策調適。

本報告之智慧財產權歸屬於國發會

項次 4. 焦點議題 4：AI 與個人資料保護及監管相關議題

壹、 背景說明

近年來人工智慧（AI）技術已被廣泛運用在各不同領域中，企業乃至於政府單位皆可能開發或使用 AI 系統協助處理事務或提供服務以增加效率。AI 技術開發與訓練需要利用大量不同類型之資料，其中不乏得以識別個人之相關資料；此外，部分 AI 之應用，亦可能於應用過程中取得或利用大量資料，例如生成式 AI 應用過程之資料輸出與輸入等，這些資料之蒐集、處理及利用對個人資料保護形成隱憂。且在 AI 技術的快速發展下，資料蒐集以及分析效率相較過往大幅提高，透過大量資料之快速運算、比對與分析，亦可能使得過去技術分析無法產生之個人識別結果被打破，故須在技術創新以及個人資料隱私風險間取得平衡。

自一般資料保護規則(General Data Protection Regulation, GDPR)在歐洲實施以來，透過資料戰略之推動陸續通過關於數位環境監理相關規範，其中多有強調資料之運用仍須以符合 GDPR 規定為基礎。而歐洲資料保護委員會(European Data Protection Board, EDPB)於 2024 年 7 月並發布聲明[204]，主張歐盟 AI 法(Artificial Intelligence Act, AIA)通過後，為解決歐盟各會員國依據 AIA 指定市場監管機關與個資保護業務可能產生之監督或協調問題，建議各會員國可指定因 GDPR 或其他相關指令（如歐盟針對刑事追訴之資訊保護指令[205]）指定之個人資料保護主管機關，擔任高風險 AI 系統之市場監管機關(market surveillance authority, MSA)。而對於公、私部門 AI 應用之個資保護層面，歐盟、澳洲、日本、韓國、新加坡等皆陸續有相關政策框架或指導文件提出，

[204] European Data Protection Board, Statement 3/2024 on data protection authorities 'role in the Artificial Intelligence Act framework, https://www.edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf , (last visited 2024/9/24).

[205] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

本報告之智慧財產權歸屬於國發會

揭示各組織/國家對於 AI 與個資保護監理或法遵之看法。故雖未有法令層面直接之修法，亦可作為我國評估後續法制政策走向之參考。

貳、 近期國際發展趨勢重點

一、 歐盟

(一)「生成式 AI 與 EUDPR－第一份關於使用生成式 AI 以確保資料保護合規」參考文件

歐盟資料保護監管機關(European Data Protection Supervisor, EDPS)於 2024 年 6 月發布「生成式 AI 與 EUDPR－第一份關於使用生成式 AI 以確保資料保護合規」[206](Generative AI and the EUDPR－First EDPS Orientations for ensuring data protection compliance when using Generative AI systems)之參考文件（下稱歐盟參考文件）。此文件旨在提供歐盟機關（構）、辦事處等單位或組織(the EU institutions, bodies, offices and agencies, EUIs)在使用生成式 AI 系統處理個人資料之實務建議，以確保其符合歐盟政府機關資料保護相關法規，尤其是歐盟政府機關資料保護規則[207](Regulation (EU) 2018/1725，簡稱 EUDPR)之規定。

1. 生成式 AI 之定義

歐盟參考文件對生成式 AI 的定義為：「使用特定機器學習模型以製造廣泛通用且多樣輸出的 AI 子集。」該子集能處理一系列任務以及應用，如文字、聲音以及影像。生成式 AI

[206] European Data Protection Supervision, First EDPS Orientations for EUIs using Generative AI, (2024), https://www.edps.europa.eu/system/files/2024-06/24-06-03_genai_orientations_en.pdf (last visited 2024/9/25).

[207] Regulation (EU) 2018/1725 of the European Parliament and of The Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, 2018 O.J. (L295/39).

本報告之智慧財產權歸屬於國發會

依賴基礎模型(Foundation models)之使用，不同之生成式 AI 系統會以基礎模型為基準進行微調。大型語言模型(Large langue models)是其中一種基礎模型，其係透過大量文字資料訓練，並透過廣泛的文字輸入以及圖像關係生成自然語言回應，其訓練的資料來源可能為網路、書籍及其他可得之來源等。部分已於實務上應用之服務諸如虛擬助理、內容創造工具、語言翻譯引擎、自動語音辨識或醫療診斷系統等皆為此類基礎模型的應用[208]。

生成式 AI 的應用相當多元，包含一般面向消費者的應用程式如 Chat-GPT 等，以及應用於特定業務場合之預先訓練模型，或基於基礎模型再根據特定活動領域需要調整之預先訓練模型等[209]。

2. EUIs 使用生成式 AI 之注意義務

由於歐盟未限制 EUIs 使用生成式 AI，在符合現有規範並尊重個人基本權利與自由之前提下，EUIs 可自由運用新興科技提供服務。基於任何歐盟境內公務機關所進行與個人資料有關之活動皆應適用 EUDPR，故歐盟 EUIs 在使用生成式 AI 時若有涉及個人資料之處理，應遵循 EUDPR 所規範之義務，並且注意需明確識別各類生成式 AI 模型形成供應鏈中之各參與者責任義務，以符合問責原則(principle of accountability)[210]。EUIs 亦可自行開發或部署生成式 AI，但須清楚界定各參與者於相關資料處理運作層面之角色(控管者、處理者、共同控管者)以及確保其遵守於 EUDPR 規範下之義務與責任。

[208] Supra note 206, at 4.
[209] *Id.* at 4-5.
[210] *Id.* at 6.

本報告之智慧財產權歸屬於國發會

3. 生成式 AI 處理個人資料之階段

根據歐盟參考文件，於任何利用生成式 AI 之環節（AI 系統之生命週期）皆可能會涉及個人資料處理，無論該處理是否顯而易見。於 AI 系統生命週期可能之個資處理包含建立訓練資料庫、訓練階段本身之資料蒐集與利用、模型創建並開始使用後分析推測出全新或額外之訊息，或是系統開始運行後之輸入與輸出[211]等。因此，當生成式 AI 系統之開發者或提供者聲稱其系統並未處理任何個人資料時，EUIs 必須進一步詢問相關資訊，以了解開發者或提供者是以何種方式確保其 AI 系統不會處理到任何個人資料。

警告不要使用網路抓取技術(web-scraping techniques)蒐集個人資料，因為透過此一技術，若於當事人不知情之情況下蒐集利用個人資料，可能與當事人預期之利用有違，並超過原始蒐集之目的，導致當事人失去對個人資料利用之控制，有違歐盟資料保護相關規則。因沒有對資料來源進行可靠性評估，亦有違個人資料蒐集最小化及準確性原則[212]。

4. 資料保護專員於開發或部署生成式 AI 系統過程之角色

EUDPR 於第 45 條規定，資料保護專員（Data Protection Officer, DPO）之功能在於就資料保護相關義務提供資訊及建議、協助資料控管者監控內部法遵情形、提供資料保護影響評估（DPIA）之建議並擔任當事人與歐盟資料保護監督機關（EDPS）間之窗口[213]。EUIs 在使用生成式 AI 處理個人資料時應確保資料保護專員在其職權內可獨立針對 EUDPR 的適用給予組織內部建議及協助。同時，資料保護專員應完整理

[211] *Id*. at 7.
[212] *Id.* at 7.
[213] *Id*. at 8

本報告之智慧財產權歸屬於國發會

解 EUIs 正考慮採購、設計或執行之生成式 AI 的生命週期及其運作方式，並應參與審閱與模型提供者簽署的資料分享協議當中相關法遵事宜。歐盟參考文件強調，確保於符合 EUDPR 規定基礎下使用生成式 AI 並非僅是資料保護專員之義務，參與 AI 生命週期之所有利害關係人皆應持續保持對話。因此，控管者應該促進組織內涉及 AI 系統生命週期之各相關部門間的聯繫，並確保 EUIs 能在使用生成式 AI 系統時確實遵守 EUDPR 之規範

5. 開發、採用生成式 AI 時之資料保護影響評估

若 EUIs 欲自行開發或使用生成式 AI 系統，須注意將資料保護納入設計(data protection by design)，並且按照 EUDPR 規定在處理可能造成個人基本權利及自由造成高風險之資料前須進行資料保護影響評估（Data Protection Impact Assessment, DPIA）。須注意的是，識別以及評估資料保護風險必須在生成式AI系統之完整生命週期中進行[214]。進行DPIA時，控管者應尋求資料保護專員的建議，並考慮相關責任及背景下採取適當的技術以減緩已知之資料隱私風險[215]。AI 模型的運作除可能加劇原已知之風險外，也可能在運作過程中產生新的隱私風險，因此控管者除了要確保 DPIA 之確實執行外，亦須定期對資料隱私風險進行審查及評估，且所有 DPIA 的參與者須確實記錄所有審查以及所採行之相關作為[216]。

6. AI 系統合法性之確保

[214] *Id*. at 9.
[215] *Id*. at 9.
[216] *Id*. at 9.

本報告之智慧財產權歸屬於國發會

在設計、開發以及驗證 AI 系統的過程中必須確保資料之處理符合 EUDPR 以及其他歐盟內部相關規範，並且必須準確援引所應適用之法律。一旦相關法律之依據嚴重影響資料保護與隱私等基本權利時，則需進一步訂定更為清楚及明確之具體保障規範及措施[217]。EUDPR 第 5 條規定，獲得當事人之同意為處理個人資料的法律基礎之一。若 AI 使用以同意作為個人資料處理之法律基礎，則須確保於系統生命週期整體過程皆遵守 EUDPR 規範之同意合法要件，包括該同意必須出於當事人自願、清楚及知情之情況方為合法。關於同意的撤銷，參考文件中敘明，若在同意撤銷前業經同意之資料已合法進入相關使用程序，則該使用部分仍為合法有效，但應立即停止繼續執行與該資料有關之業務，並若沒有其他法律依據應將該相關資料刪除[218]。另外，由於 EUDPR 之規範對象為歐盟內部機構，規範企業或是個人與資料有關活動之法規為 GDPR，因此若 EUIs 在使用由 AI 系統供應商所提供之 AI 服務時，負有確認相關事業在個人資料之使用上有符合 GDPR 個人資料處理之相關規定[219]。

在資料傳輸部分，在開發或使用 AI 系統的任何階段若需進行資料傳輸必須符合 EUDPR 之規定，尤其若是要將資料傳輸至歐盟以外之國家或組織，則須注意符合 EUDPR 第五章之相關規定[220]。

7. 資料最小化及通知義務

AI 的開發使用至生產各階段皆須注意個人資料最小化原則[221]，將所涉個人資料之處理限於與處理目的充分相關之資

[217] *Id*. at 11.
[218] *Id*. at 11-12.
[219] *Id*. at 12.
[220] *Id*. at 12.
[221] Supra note 205, Article Chapter II, 4.1 (c).

本報告之智慧財產權歸屬於國發會

料範圍，且不得於處理目的以外之業務任意使用個人資料[222]。EUIs 在處理個人資料時也須注意資料使用的透明化，必須告知用戶其使用個人資料之相關資訊如使用目的及時間等[223]。

8. 自動化決策

若生成式 AI 系統有涉及運用個人資料而由系統進行自動化決策者，須遵守 EUDPR 相關規定，設置個人資料之安全保護措施。控管者需能適時進行人為干預並確保人為干預措施之適當落實[224]。

9. 資料更新及當事人權利

生成式 AI 在其系統生命週期整體大量處理各類資料，包含個人資料。EUDPR 第 4 條之資料正確性原則(principle of data accuracy)要求資料必須準確且保持最新，並要求資料控管者須更新或刪除不正確之資料，故資料控管者應於生成式 AI 的完整生命週期中，透過整合之資料保護規劃，採取必要措施以確保資料於所有階段皆具備準確性。

EUDPR 第 3 章保障個人對資料有存取、更正及刪除等權利，而生成式 AI 係透過大量資料進行系統訓練，主要係透過詞嵌入(word embedding)過程形成數值向量，而非直接儲存特定文字字串，如貓或狗。故要對儲存於模型中之資料進行存取、更正與刪除，將會非常困難，且可能會對模型運作之效能產生影響。故應對於資料集進行適當之管理以促進資料之存取，但若該訓練資料取自於公開來源且為無監督之訓練，則管理仍有其困難。

---

[222] Supra note 204, at 14.
[223] *Id*. at 17.
[224] *Id*. at 18.

本報告之智慧財產權歸屬於國發會

基此，參考文件建議控管者應保留可追溯之紀錄並以可追溯其使用之方式管理資料集[225]，較有助於支持當事人之權利行使。而資料最小化技術，亦可幫助減輕因無法確保當事人得以依據 EUDPR 適當行使其權利之風險。

(二)EDPB 針對資料保護機關於 AIA 上角色之聲明

2024 年 7 月 16 日，歐洲資料保護委員會（EDPB）針對資料保護機關在 AIA 上之角色發佈聲明(Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework[226]，以下簡稱 EDPB 聲明)，主張歐盟於 2024 年 7 月頒布之 AIA 旨以風險為考量，建立統整性規範以因應 AI 技術於市場上之服務及使用，並促進以人為本且值得信賴之 AI 服務環境之發展。就個人資料保護之議題上，AIA 法與 GDPR 之規範可謂相輔相成，皆以保障人類之基本權利，且就技術層面上 AI 之訓練亦無法避免個人資料之議題。依據 AIA 之施行進程，成員國應於 2025 年 8 月 2 日之前任命國家級特別市場監督機構(in particular market surveillance authority/authorities，以下簡稱 MSA)，以監督 AIA 之適用與實施。為協助各國確立 MSA，EDPB 通過此份聲明，認為個人資料保護機關(the Data Protection Authorities, DPAs)適合擔任 MSA，具體建議如下：

1. DPA 應被指定為用於執法、邊境管理、司法及民主進程之高風險 AI 系統之 MSA。

2. 建議成員國考慮指定DPA為其他高風險AI系統之管理機構，尤其可能影響自然人之權利及自由之個人資料處理相關之高風險 AI 系統。

[225] *Id*. at 22.
[226] Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework. https://www.edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf (最後瀏覽日:2024/11/20)

本報告之智慧財產權歸屬於國發會

3. DPA 在被指定為 MSA 的情況下，應被指定為公眾以及成員國及歐盟層級對應部門的單一聯絡點。

4. 應建立明確的程序，以便 MSA 與負責監管 AI 系統的其他監管機構（包括 DPA）之間的合作，以防止事務生態系中不同監督機構所為決策之不一致。此外，歐盟 AI 辦公室和 DPA/EDPB 之間應建立適當的合作。

二、 澳洲

澳洲財政部(Department of Finance)於 2024 年 6 月發布《確保 AI 於政府原則之國家框架》(National framework for the assurance of artificial intelligence in government，下稱澳洲 AI 框架[227])，基於 2019 年澳洲產業、科學暨資源部(Department of Industry, Science, Energy and Resources，下稱資源部)所發布之《AI 倫理原則》(Australia's AI Ethics Principles)，澳洲 AI 框架之目標在促進政府安全且負責任的使用 AI。該框架屬聯邦層級，主要提供原則性規範，各州及領地政府將再依據各該司法管轄範圍之政策執行背景及法律訂定具體規範。

2019 年澳洲資源部所發布之 AI 倫理原則中包含八大原則，而本次澳洲 AI 框架即是此八大原則之實踐，目的在為安全且負責地使用 AI 奠定基礎，協助政府實現更安全、可靠與公平之 AI 服務，並以高道德標準設計、開發及使用 AI，減少因運用 AI 可能產生之負面影響[228]。八大原則包括：人類、社會及環境福祉(Human, societal and environmental wellbeing)、人本價值(Human-centred values)、公平性(Fairness)、隱私保護及安全(Privacy protection and security)、可靠性及

[227] Department of Finance, National framework for the assurance of artificial intelligence in government (2024).https://www.finance.gov.au/sites/default/files/2024-06/National-framework-for-the-assurance-of-AI-in-government.pdf (Last Visited:2024/9/24).
[228] *Id*. at 6.

本報告之智慧財產權歸屬於國發會

安全性(Reliability and safety)、透明度性及可解釋性(Transparency and explainability)、可爭論性(Contestability)及問責(Accountability)。

除此之外，澳洲 AI 框架中亦說明，為有效實踐上開倫理原則，政府應同時考慮五項基本保障：

1. 治理(Governance)，AI 治理應包含組織架構、政策、流程、監管、角色、責任以及風險管理架構，確保未來也能安全且負責地使用 AI[229]；

2. 資料治理(Data Governance)，創建、蒐集、管理、使用及維護經過驗證、可靠且精確的資料集並維持合法穩健的資料治理[230]；

3. 風險基礎方法(risk-based approach)，政府應考慮在高風險狀況下建立監管機制，包含但不限於外部或內部審查機構，諮詢機構或是 AI 風險委員會以提供專家建議[231]；

4. 標準(Standard)，政府應建立一致的程序及規範標準，以達成安全且負責任地使用 AI 的目的[232]；

5. 採購(Procurement)，政府在採購過程中必須考慮到可能產生的風險，例如在隱私保障部分，必須注意契約內容是否包含對隱私安全的保障[233]。

而上開 AI 倫理八大原則當中，「隱私保護及安全」為其中涉及個人資料保護之重要原則，而本次 AI 框架對此之實踐，則落實於三個部分：

---

[229] *Id*. at 6
[230] *Id*. at 7.
[231] *Id*. at 8
[232] *Id*. at 9.
[233] *Id*. at 10.

本報告之智慧財產權歸屬於國發會

1. 遵循隱私法制政策之義務

政府須確保對 AI 系統之使用，符合有關個人資料之同意、蒐集、儲存、使用、揭露以及保有之法律規範，包括當 AI 系統進行個人資料蒐集或個人資料被用於其他目的時（如用於訓 AI 系統訓練）需告知當事人[234]。

此外，「隱私始於設計」(privacy by deign)原則與「隱私影響評估」(privacy impact assessments)，有助於識別、評估與降低隱私風險，故政府應予以採用，並於必要時諮詢相關專家之建議[235]。

2. 資料運用最小化並保護個人資料

政府須評估每一使用 AI 之事例，於蒐集、利用及揭露個人資料時皆具備必要性及合理性，並須符合比例原則。政府應考慮透過合成資料、資料匿名化及去識別化、加密、安全聚合(secure aggregation)等隱私強化技術以減少個人資料保護風險，同時須特別注意特種資料之管理[236]。

3. 保護系統及資料

政府應確保每一 AI 使用之事例，都符合資料安全及資料保護法規，並確保對於系統、應用程式以及資料庫之使用，限於依職權所需並經授權之人員，若有必要，並須尋求領域相關專家之建議[237]。

對於安全層面之措施，則應將過往澳洲政府曾經訂定之相關安全指導集策略或指引納入考量，包括 2023 年公布之

[234] *Id*. at 18.
[235] *Id*. at 18.
[236] *Id*.
[237] *Id*. at 19.

本報告之智慧財產權歸屬於國發會

「2023-2030 澳洲網路安全戰略」(2023-2030 Australian Cyber Security Strategy)、內政部公布之「託管認證架構」(Hosting Certification Framework)、澳洲信號局(Australian Signals Directorate, ASD)2024 年公布之「參與 AI 指引」(Engaging with Artificial Intelligence)以及「部署 AI 系統之安全報告」(Deploying AI Systems Securely)、與 2023 年總檢察長部(Attorney-General's Department)公布之「應對內部威脅：澳洲政府指引」等。

三、 日本

2024 年 4 月日本總務省(MIC)及經濟產業省(METI)共同發布《AI 運營事業指引》(AI 事業者ガイドライン（第 1.0 版），下稱日本指引[238]）為 AI 營運相關事業提供建議及注意事項。其中 AI 營運事業者係指在各種商業活動中開發、提供、利用 AI 之事業，中央與地方政府以及公家機關亦包含在內。除對所有 AI 事業之一致性原則建議，該指引亦將 AI 事業根據其業務性質分為 AI 開發者(AI Developer)、AI 提供者(AI Provider)以及 AI 使用者(AI Business User)三類並分別針對各事業業務特性給予建議。

日本指引架構第一部分為 AI 相關定義；第二部分為透過 AI 欲實現之社會目標，並評估 AI 對社會可能帶來之風險，以及應採行與實踐之共通原則。而第二部分為後續其他指引內容之核心基礎，故亦為相關事業必須注意的重點；第三至第五部分則是給予三類事業之個別建議。指引之內容涵蓋廣泛，以下僅就內容涉及本研析之個人資料或隱私保護層面之討論進行摘整。

1. 共通原則（基本理念）

[238] AI 事業者ガイドライン（第 1.0 版），令和 6 年 4 月 19 日，https://www.meti.go.jp/press/2024/04/20240419004/20240419004-1.pdf (最後瀏覽日:2024/9/16)。

本報告之智慧財產權歸屬於國發會

日本政府於 2019 年 3 月發布「以人為中心的 AI 社會原則」政策，期望 AI 能為 Society 5.0[239]作出貢獻，其提出之基本理念有三：尊重人性尊嚴的社會(dignity)、擁有多元背景之人皆可追求多元與包容之社會(diversity and inclusion)以及永續的社會(sustainability)[240]。為實現以上基本理念，三類 AI 事業須共同配合之基本原則為：以人為中心、安全性及公平性、隱私保護、安全保護、透明性以及問責。

在隱私保護部分，指引提醒所有事業應遵循個人資料保護之相關法律規範，並應在開發、提供、利用 AI 系統及服務時尊重隱私並遵守相關法令。在使用 AI 時須注意勿過度依賴自動化決策，且須適時進行人為干預，以避免造成個人權利侵害[241]。各事業應根據個人情報保護法及相關法律，考慮到社會背景以及利害關係人之隱私保護，參考國際個人資料保護原則後研擬、公告其內部隱私政策[242]。

於透明性確保之層面，指引提醒 AI 事業者必須於開發、提供或利用 AI 系統或服務時，考量相關社會背景，確保 AI 系統與服務之可驗證性，並於技術可行的範圍內提供利害關係人必要且合理之資訊。所需提供之資訊，則須包括 AI 使用之事實、程度及範圍、資料蒐集與標示的方式、學習及評估之方式、AI 基礎模型之資訊、AI 系統與服務之功能、限制以及適當或不適當之使用方式，以及 AI 系統及服務使用者所在國家、區域以及適用之相關法律等。上述向利害關係人提供之資訊，必須基於對隱私及商業機密之尊重，並依據所採用技術之特性及預定用途，以社會上認為合理的方式進行[243]。

---

[239] 提倡以人為中心，透過整合網路與實體空間以平衡經濟發展以及社會問題。
[240] 同註 238，頁 10。
[241] 同註 238，頁 13-15。
[242] 同註 238，頁 15-16。
[243] 同註 238，頁 17。

本報告之智慧財產權歸屬於國發會

於問責層面，AI 事業者於開發、提供或利用 AI 系統及服務時，必須確保可追溯性以及共通原則之遵循。其中於可追溯性層面，必須要確保資料的來源以及於 AI 系統開發；提供及利用過程之決策，於合理之技術可能性範圍內，具備可追溯性。於共通原則之遵循層面，尤其在隱私保護相關之問責確保，則要求必須定期對利害關係人說明，AI 系統或服務可能對個人或利害關係人產生的隱私危害風險與對策，以及若發生隱私侵害時預計將採取之措施。此部分也需反映於對利害關係人之具體回應層面，要求須制定及公布 AI 治理政策以及隱私政策，以管理利用 AI 系統服務之相關風險並確保其安全性[244]。

2. AI 開發者

AI 開發者在資料學習階段應注意採行隱私始於設計之相關方法，確保適當蒐集系統學習時所需資料，若當中包含第三人個人資料或智慧財產權，必須根據所適用法律進行適當之處理。同時也需要採取適當之保護與管理措施，例如採用資料管理或限制相關功能，以管控訓練研究過程之資料存取[245]。

在 AI 系統開發後，應即時向利害關係人提供 AI 模型學習之資料蒐集政策、學習方法及實施機制等相關資訊，以確保符合公平性、隱私保護與安全性[246]。

而於廣島進程中針對高階 AI 系統開發組織之國際行為準則[247]，則進一步敘明，若要採取適當措施進行資料品質之管

[244] 同註 238，頁 18-19。
[245] 同註 238，頁 26。
[246] 同註 238，頁 28。
[247] 七大工業國集團（G7）領袖於 2023 年 5 月 20 日的廣島峰會上達成共識，為了發展值得信賴的人工智慧（AI），各國應開發並施行一套符合 G7 價值觀的國際技術、監管標準，以規範 AI 的應用，並由指派各國高級官員，建立「廣島 AI 進程」（Hiroshima AI process），以討論人工智

本報告之智慧財產權歸屬於國發會

理，則應包括機器學習之透明度及隱私保護，以及針對敏感資料外洩之測試與調整。同時須採取適當保護措施，以尊重隱私並保護智慧財產權[248]。

3. AI 提供者

於 AI 系統導入時，需採取相關隱私保護措施，例如運用相關技術對個人資料之存取進行管理及限制[249]。此外，於 AI 系統服務提供後，一旦發現系統服務中之隱私侵害事件，應在發生侵害時採取適當行動並研議防止再發生之方法[250]，並提醒使用者須避免將個人資料不當輸入至所提供之 AI 及服務當中。同時應鼓勵 AI 使用者適當地利用 AI，並向其提供以下注意資訊[251]：

(1) 提醒使用者須注意個人資料之利用，保持資料之正確性，並於必要時保持其為最新狀態。

(2) 警示特定情境學習可能導致不當之 AI 模型學習的情況。

(3) 個人資料輸入應注意之事項。

4. AI 使用者

指引再次提醒 AI 使用者於利用 AI 系統或服務時，應注意不要不當輸入個人資料。而事業並應對不當登錄個人資料

慧相關事務，並於 2024 年 5 月於巴黎舉辦部長理事會時宣布啟動，落實《開發先進 AI 系統組織國際指導原則》及《開發先進 AI 系統國際行為準則》，由 49 個國家與地區共同參與，以因應生成式 AI 風險與促進國際合作。

[248] 同註 238，頁 30。

[249] 同註 238，頁 32。

[250] 同註 238，頁 32。

[251] 同註 238，頁 33。

本報告之智慧財產權歸屬於國發會

以及隱私侵害設有相關對應機制，適當蒐集涉及隱私侵害之相關事件，並研議防止發生及預防之方法[252]。

四、 韓國

南韓個人資料保護委員會(Personal Information Protection Commission, PIPC)於 2023 年下半年至 2024 年，對於 AI 隱私之議題積極參與國際會議，並於 2023 年成立 AI 小組對於 AI 涉及之技術發展、個資與隱私處理之相關問題進行研議，陸續發布相關政策及指引文件，並進行民間及國際組織交流。

(一)AI 時代個人資料安全使用政策方向

2023 年 8 月，PIPC 發布《AI 時代個人資料安全使用政策方向》（Policy Direction for Safe Usage of Personal Data in the Age of A.I.[253]，下稱韓國政策方向），此為 PIPC 首個針對 AI 使用提出政策指引。鑒於 AI 技術被各領域廣泛運用對個人資料隱私保護帶來之挑戰，此政策方向著重於 AI 之監管，解釋如何在 AI 運用中實踐法律規範，以協助降低 AI 利用於隱私及資料保護之潛在風險，同時促進資料的安全使用[254]。該政策方向共有 4 個重點及相應的行動計畫：

1. 減輕法律及監管不確定性的新方法

因應 AI 技術需大量使用資料且具有高度複雜性，PIPC 採取基於原則(principle-based)而非基於規範(rule-based)之監管方法。PIPC 將建立 AI 隱私團隊(AI Privacy Team)，負責處理

252 同註 238，頁 34。

253 《AI 時代個人資料安全使用政策方向》(Policy Direction for Safe Usage of Personal Data in the Age of AI.)， https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=2275#none (最後瀏覽日:2024/9/24)。

254 同前註，頁 1。

本報告之智慧財產權歸屬於國發會

與 AI 隱私有關之事務。AI 隱私團隊之作用在於透過以下三項職能降低 AI 服務開發者及部署的法律不確定性：

(1) 提供資料保護法規之釋義以釐清合法並安全處理個人資料之要求。

(2) 檢視企業是否符合申請監管沙盒之資格。

(3) 進行「充分的事先評估」(prior assessment of adequacy)（暫名）。PIPC 將與企業合作制定相關保障措施之計畫以符合 PIPC 要求，並對企業實際實施狀況進行審查。

2. 對 AI 服務以及產品開發與部署不同階段之具體安全措施

此政策方向根據 AI 系統在不同階段所適用之資料保護原則及標準：

(1) 設計及規劃階段，透過隱私始於設計原則以大幅降低資料隱私風險。

(2) 資料蒐集階段，根據不同種類資料訂定具體資料隱私保護要求。

(3) 模型建構與訓練階段，採取適當的資料保護措施如資料去識別化及隱私加強技術。

(4) AI 服務提供階段，維持透明度並確保當事人之權利。

3. 規劃針對具體需求發布進一步指引

此政策方針敘明 AI 處理個資之治理原則及標準，未來將以此為基與各方利害關係人合作，訂立各領域的具體措施。為此將於 2024 年 10 月成立「AI 隱私權政策諮詢理事會」

本報告之智慧財產權歸屬於國發會

(Policy Advisory Council for AI Privacy)（暫名）[255]，由各領域之專家提供包括資料處理標準、風險評估及確保透明度之相關建議，PIPC 將採納理事會建議並制定包含非結構化資料假名化標準、生物識別資料規範、公開資料使用規範、使用從行動影像處理設備擷取之視覺影像資料規範、AI 透明度標準及綜合資料使用規範等事項之相關指引。

4. 國際協調與合作

PIPC 將積極參與全球制定 AI 相關資料隱私保護之相關討論，強調跨境合作之重要性，將與各國資料隱私單位及國際組織合作以建立一致之國際規範。

(二)個人資料保護施行令之修正

2024 年 3 月 6 日，PIPC 宣布對個人資料保護法施行令進行修訂(Enforcement Decree of the Personal Information Protection Act, PIPA Enforcement Decree)，並於同年 3 月 15 日生效。本次修訂主要對應 2023 年個人資料保護法(PIPA)修訂之落實，著眼於 AI 時代個人資料安全措施之落實，包括關於自動化決策之資料當事人權利，及對隱私長（Chief Privacy Officer, CPO）專業能力之要求。

1. 規範 AI 等自動化決策所涉之當事人權利

此部分修正主要是針對 PIPA 於 2023 年 3 月增訂第 37 條之 2 自動化決策規定之落實，明定當事人可對自動化決策所產生之不正確或不當結果採取措施。當事人有權要求對完全之自動化決策進行解釋或審查，且若該自動化決策對當事人之權利義務造成重大影響，當事人有權拒絕自動化決策處理

[255] 截至專案結案之 2024 年 12 月止，暫未見相關成立資訊。

本報告之智慧財產權歸屬於國發會

其個人資料。此次修法亦要求資料控管者之揭露義務，資料控管者必須解釋其決策依據以及進行決策之方法[256]。

2. 強化隱私長之專業性與獨立性

對於處理大量個資或敏感個資之企業或公共機構的隱私長有更嚴格之要求，例如超過一定規模之個人資料控制者，其指定之隱私長必須為具有至少有 4 年個人資料保護、資訊保護或資料科技經驗（需有 2 年個人資料保護經驗）之人員，以確保其具備專業能力及可獨立履行職責之能力。

除前述兩個與 AI 相關之重點規範調整外，本次修訂尚包括對公部門個人資料保護水準評估規定之修正、調整對當事人負擔損害賠償責任之義務人範圍及門檻以及對未來 PIPC 定期檢查頻率之調整等，因與本議題無關，故不予摘述。

(三)AI 開發與服務處理開放資料指引

PIPC 著眼於網路上公開之資料為 AI 開發與訓練重要的資源，於 2024 年 7 月發布《AI 開發與服務處理開放個人資料指引[257]》Guideline on Processing Publicly Available Data for AI Development and Services, 下稱韓國指引），以指導 AI 開發及服務提供者合法且安全的使用網路上公開可用之資料（包括可能涵蓋之個人資料），建立適切之個人資料處理準繩。現行南韓《個人資料保護法》(Personal Information Protection Act, PIPA)當中對於使用公開個人資料之規範尚不足夠且明確。網路上

[256] South Korea: PIPC announces upcoming PIPA Enforcement Decree amendments，https://www.dataguidance.com/news/south-korea-pipc-announces-upcoming-pipa-enforcement (last visited: 2024/9/24).

[257] PIPC，《AI 開發與服務處理公開資料指引》（PIPC Offers Guideline on Processing Publicly Available Data for AI Development and Services）(인공지능(AI) 개발·서비스를 위한 공개된 개인정보 처리 안내서)，https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=10362#LINK （韓文）； https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=2591 （英文）(最後瀏覽日:2024/9/24)。

本報告之智慧財產權歸屬於國發會

之公開資料可能包含地址、唯一可識別資訊(unique identifiable information, UII)、信用卡卡號或其他個人資料。而網路上公開資料為任何人皆可讀取，此為開發生成式 AI 模型（如 Chat GPT）關鍵之資料來源，而公開可用資料的大量使用，將使用戶隱私暴露於高度風險之中。除此之外，網路上公開資料來源眾多，若想於現行法框架下逐一向用戶取得同意或簽訂契約並不切實際，AI 的開發與訓練為現行法關於個人資料法制之規定及解釋帶來挑戰[258]。

此指引為 PIPC 於 2023 年 8 月發布前開 AI 個人資料安全使用政策方向後，透過與 30 名專家（涵蓋學術界、法律界、產業界及民間團體代表）與三個小組委員會（分別負責資料處理標準、風險評估與透明度議題）共同研議所提出，其中考量國際（歐、美、英）近期相繼形成對 AI 與資料處理之個人保護監管機制，故此一指引之目標則設定於建立國際可互動之標準。指引內容包含使用合法利益內容、建議可行保護措施及保護當事人權利方法，以及促進 AI 事業在開發使用 AI 時注意可信任度三部分，簡述如下：

1. 合法利益概念之適用

指引闡明南韓《個人資料保護法》（PIPA）第 15 條關於合法利益之規定，即蒐集、利用資料必須屬於合法利益且明顯優於當事人權利時，可利用公開資料進行 AI 培訓及 AI 服務之開發。AI 系統開發以及服務提供者要適用並符合合法利益之概念，必須達成目的正當性、資料處理必要性以及對個人資料處理者與當事人間風險評估之三項要件。

目的正當性係指資料處理者須確保其有合法事由處理個人資料，透過明確之 AI 預期開發目的，以確立是否確有合法

[258] 同前註，頁 1。

本報告之智慧財產權歸屬於國發會

利益之存在，例如為支援醫療診斷開發、進行信用評等或生成/分類或翻譯等各類模型開發目的。

資料處理必要性指應確保公開資料之蒐集為其目的所必要、充分且適當的，例如於開發醫療診斷之 AI 模型時，已排除涉及個人收入或財產等與模型開發目的不相關之資料。

個人資料處理者與當事人間之風險評估，目的在確保個人資料處理者之利益明顯高於當事人之權利，以符合前開 PIPA 第 15 條第 6 款[259]以合法利益所必須作為可蒐集利用個人資料之法律基礎[260]。

2. 可行保護措施及保護當事人權利方法建議

指引提供 AI 事業在根據合法利益使用公開可用個人資料時，應建立技術及組織的安全措施以保障當事人之權利之建議，分為技術安全保障、行政與組織保障、以及尊重當事人權利三個部分：

(1) 在技術安全保障部分，應檢查訓練資料之來源、採取措施防止個人資料外洩（如刪除或去識別化）措施、安全儲存及管理個人資料、運用額外之安全措施、採用提示及輸出過濾機制、於訓練中移除目標性之訓練資料（機器遺忘，Machine Unlearning）等。

(2) 行政與組織保障則包含，建立資料蒐集、利用及訓練之處理標準並納入隱私權政策、考慮執行隱私影響評估、組織

[259] 南韓現行 PIPA（2024 年 3 月施行）第 15 條就個人資料及與利用之合法條件，於第 6 款規定，為實現個人資料控制者之合法利益所需且該利益明確優先於資料處理權利，為合法要件之一。而此類情況僅限於個人資料控制者之合法利益重大、且不超出合理範圍之情形。

[260] 同註 257，頁 2。

本報告之智慧財產權歸屬於國發會

AI 隱私紅隊、及實施專屬 AI 模型開發及部署 AI 服務之保障措施。

(3) 於尊重當事人部分則應確保將公開資料蒐集情形以及主要資料來源納入隱私政策文件、維護當事人權利，包含在訓練及部署 AI 模型時建立相關措施，使當事人得以行使其資料外洩之刪除權及停止利用之權利[261]。

(4) 由於 AI 技術發展迅速，指引亦給予 AI 事業根據其技術發展、條件及業務內容建立合適之安全保障措施之彈性[262]。

3. 促進 AI 事業在開發使用可信賴之 AI 時之角色

指引強化 AI 事業之隱私長於 AI 模型開發及資料處理之重要性。建議事業應設立專門處理 AI 隱私之團隊，透過隱私長之培養以達成指引中對隱私保護之基本要求[263]。企業應隨時監控技術上風險因素，例如技術之重大改變或資料外洩可能造成之風險，並應制定補救及救濟措施[264]。

(四)自動化決策當事人權利指引

於 2024 年 9 月 26 日 PIPC 針對事業利用自動化決策系統影響當事人權利部分，發布《自動化決策當事人權利指引》(자동화된 결정에 대한 정보주체의 권리 안내서[265]，簡稱韓國自動化決策指引)，要求特定領域之自動化決策系統運用，必須遵守個人資料控制者之相關措施標準。而此指引所稱之自動化決策依據 PIPA 第 37 條之 2 規定，係指透過完全自動化之系統(包括應用 AI 技術之系統)處理個人資料

261 同註 257，頁 3。
262 同註 257，頁 3-4。
263 同註 257，頁 4-5。
264 同註 257，頁 4-5。
265 PIPC，自動化決策當事人權利指引(자동화된 결정에 대한 정보주체의 권리 안내서), https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=10611#LINK , (last visited 2024/9/29)

本報告之智慧財產權歸屬於國發會

以進行決策。而依據該條規定，個人資料控管者進行自動化決策時，當事人可以對決策要求提出說明，也必須公開自動化決策之標準、程序及個人資料處理之方式，以利當事人確認。當事人若認為自動化決策對其影響重大，亦得拒絕，此時事業除非有正當理由，則不能再採用自動決策及依據該自動決策採行相關措施。

本次指引主要係繼前述 3 月之個人資料保護法施行令修正後，進一步說明事業應如何踐行個資法及施行令修正於自動化決策規範之要求。指引當中特別提醒，並非所有自動化系統所為之決策皆屬於自動化決策，就個案當中必須檢視其是否符合自動化決策之定義。若於系統完成最終決定之前，已經有人為判斷程序之介入，即可能不被認定為自動化決策，指引當中並提供判斷之原則與「自動化決策自我診斷表」供事業運用[266]。

此外，於進行自動化決策之情況下，事業或組織必須依照當事人依法行使權利之請求，採取以下措施：

1. 當事人要求提出解釋之說明時，必須選擇並提供對當事人有幫助及有意義之資訊。若當事人對關於其之自動化決策提出意見，則必須對於該自動化決策進行審查與評估該意見，並告知其結果。尤其必須注意，涉及演算法或機器學習之過程，必須向當事人提供簡潔且有意義之資訊，而非提供對個人資料處理複雜的數學說明。也就是說，必須考慮人類基本上難以理解 AI 模型如何得出結果之演算過程，故需以人類可理解之形式進行解釋[267]。

2. 自動化決策對當事人權利或義務產生重大影響，而當事人依法拒絕該決策時，事業或組織必須暫停利用該決策，並將處理結果告知當事人。過程當中亦可讓人為介入重新處

[266] 同前註，指引本文頁 4-5。
[267] 同註 268，頁 2。

本報告之智慧財產權歸屬於國發會

理相關資訊，並將處理結果通知當事人。惟若該自動化決策應用係經過當事人同意，或已透過契約方式事先告知當事人，或法律有明確規定者，則當事人不得拒絕，僅可要求說明及審核。至於此類情況如何判斷是否屬於對當事人有重大影響，則必須綜合考量當事人之權利或義務是否涉及生命、與人身安全，以及是否會持續及有無恢復之可能性等[268]。

3. 事業或組織進行自動化決策時，必須事先於網站上公開其標準及程序，以利當事人查閱。同時必須訂定並揭露具體之權利行使方式，以使當事人易於理解[269]。

五、 新加坡

新加坡個人資料委員會(Personal Data Protection Commission, PDPC)於 2024 年 3 月發布《於 AI 建議及決策系統使用個人資料建議指引》（Advisory Guidelines On Use Of Personal Data In AI Recommendation And Decision Systems[270]，下稱新加坡指引）提供機構[271]使用個人資料開發及部署嵌入式機器學習模型（AI 系統）之明確時機，使之符合現行新加坡個人資料保護法(Personal Data Protection Act, PDPA)及其相關法規，並且給予用戶保障，確保其個人資料在 AI 系統中之安全。

新加坡指引中所指之 AI 系統為建議、決策系統以及機器學習模型，此類系統是在透過自動化決策協助人類決策者提供建議及預測[272]。指引除前兩部分之執行摘要以及法律效力範圍外，根據 AI 系統開發

[268] 同註 265，頁 2-3。
[269] 同註 265，頁 3-4。
[270] Advisory Guidelines On Use Of Personal Data In AI Recommendation And Decision Systems, PDPC,advisory-guidelines-on-the-use-of-personal-data-in-ai-recommendation-and-decision-systems.pdf (pdpc.gov.sg) .(last visited 2024/9/25)
[271] 根據新加坡個資法（PDPA）第 2 條第 1 項，機構包含任何個人、公司、機構或社團不論使否根據新加坡法律成立，亦不論是否居住或於新加坡擁有辦公室或商業處。
[272] Supra note 270. at 3.

本報告之智慧財產權歸屬於國發會

階段分為：利用個人資料於 AI 系統開發、測試及監控、部署—AI 系統中的個人資料蒐集及利用(deployment – collection and use of personal data in ai systems)、AI 系統採購—服務提供者如何支援機構實施 AI 系統之最佳實踐三個部分(procurement of ai systems – best practices for how service providers may support organisations implementing ai systems)。

1. 利用個人資料於 AI 系統開發、測試以及監控

根據 PDPA，除此法所規定例外情況外，機構在獲得當事人同意後始得利用其個人資料。新加坡指引中所提及例外為商業改善目的例外及研究目的例外，企業為加強現有商品及服務而開發 AI 系統時，享有商業改善目的之例外，開發具公共利益之 AI 系統則屬於研究目的例外[273]。在符合以上兩類例外之前提下，企業得於未經當事人之同意下利用其依據 PDPA 所蒐集之個人資料進行 AI 系統之開發。

機構應於開發 AI 系統時實踐資料最小化原則，僅使用訓練 AI 系統時必要之資料，並且應設置資訊保護措施[274]。新加坡指引提醒組織在設計、測試以及監控 AI 系統對個人資料之利用時，應有適當的技術流程或/及法規控制措施，並且鼓勵對用於基本控制目的之個人資料進行去識別化[275]。

2. 部署－於 AI 系統蒐集、利用個人資料

此部分主要針對組織於其產品或服務當中部署 AI 系統，並蒐集與利用個人資料以提供新功能或強化產品特性時，應如何遵守 PDPA。主要強調對當事人之同意、通知義務及問責。對於當事人同意以及通知義務層面，提醒必須依循 PDPA 第

[273] Supra note 270. at 5-6.
[274] Supra note 270. at 10.
[275] Supra note 270. at 11-12

本報告之智慧財產權歸屬於國發會

13 條（同意）及第 20 條（通知）規定，在蒐集個人資料時應告知用戶蒐集個人資料的目的以及其預期用途[276]。此外，依據 PDPA，機構有義務建立內部政策及實踐，確保機構能負責任的利用個人資料。機構應提高透明度，提供用戶資料保護及安全措施之相關資料以利其了解相關風險並同意企業利用其個人資料[277]。

除此之外，新加坡指引亦建議機構進行資料保護影響評估(data protection impact assessments)，協助機構在 AI 系統中識別及減輕資料外洩之風險[278]。

3. AI 系統採購—服務提供者如何支援機構實施 AI 系統之最佳實踐

AI 服務提供者以開發或客製化 AI 系統為其客戶處理個人資料，則係扮演資料中介者之角色，並須遵守 PDPA 之規定，此類服務提供者應在處理資料前使用如資料標記等技術以追蹤被用於訓練之資料，並保留資料訓練紀錄以識別資料來源及追蹤資料之轉換方式[279]。

指引提供兩步驟建議 AI 服務提供者如何向機構提供服務：

步驟一：根據客戶需求及對使用者的影響以了解客戶所需資料。AI 服務提供者應參考前段部署階段之規範以達成其客戶於同意、通知及問責之義務[280]。

[276] Supra note 270. at 13-16.
[277] Supra note 270. at 16.
[278] Supra note 270. at 19.
[279] Supra note 270at 19.
[280] Supra note 270. at 20

本報告之智慧財產權歸屬於國發會

步驟二：確保系統設計可獲得相關資料。指引鼓勵服務提供者在設計客製化 AI 系統時建立相關程序作為隱私始於設計之一部分，以達成 PDPA 之義務。其內容包含，提供用戶機構內部使用之資料並以用戶可理解之語言轉譯 AI 之操作方式、以及向用戶機構提供適當之支援，使其得以充分了解其購買之 AI 系統，如給予用戶機構適當訓練及指導，以確保其能正確理解並使用 AI 系統[281]。

指引強調，雖受託之 AI 服務提供者可協助機構在同意、通知以及問責上之義務，但委託機構仍須承擔主要責任以確保其所使用之 AI 系統能符合 PDPA 規範。

六、 美國加州

2024 年 8 月，加州議會通過 AB1008 法案，修改加州消費者個人隱私法案(California Consumer Privacy Act of 2018, CCPA[282])。依據 CCPA，消費者有權要求企業刪除其個人資料，以及修正不正確之個人資料。消費者對其個人資料有知情權及退出權，知情權是指消費者得要求企業揭露其所欲蒐集個人資料之種類以及使用目的；退出權則是指消費者可隨時要求企業不得出售或分享其個人資訊予第三方。CCPA 所規範之對象為在加州年收入超過 2500 萬美元以上之企業、每年單獨或共同購買、銷售或分享超過 10 萬個人或家戶資料之企業以及百分之五十之年營收是透過銷售或分享個人資料之企業[283]。

本次法案對個人資料(personal information)定義進行增修，增加的部分主要為個人資料之存在形式，包含但不限於實體形式(Physical formats)，如紙本文件、印刷資料、黑膠唱片或錄影帶；或數位形式(Digital formats)，包括簡訊、圖片、聲音或影像檔案。亦包括抽象之數

281 Supra note 270. at 21.
282 California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199 (2018).
283 *Id.* California Consumer Privacy Act of 2018, §1798.140 (d)

本報告之智慧財產權歸屬於國發會

位形式(Abstract digital format))，包含壓縮或加密檔案、元資料或「能夠輸出個人資料的 AI 系統」[284]。因此修正後，CCPA 規範下之企業在使用 AI 系統進行與消費者個人資料相關之分析，若該系統得以分析輸出個人資料，則屬於 CCPA 定義之個人資料範疇，須符合 CCPA 之規範。而消費者根據 CCPA 則有權要求企業將其個人資料自 AI 模型中刪除或修改。

七、 OECD

OECD 於 2024 年 6 月發布《AI 資料治理及隱私：綜效與國際合作領域》報告（AI, data governance, and privacy: Synergies and areas of international co-operation，下稱 OECD 報告），旨在透過倡導國際合作建立一更具包容性及協調性之政策框架，確保 AI 系統發展之同時，能尊重且保護隱私。

依據 OECD 報告之執行大綱， 各國於 AI 監管政策及隱私保護政策仍是針對相關議題各自規範，兩者並未互相協調、合作，導致各管轄區域或法律體系對相同問題之應對方式產生差異，增加監管及執法上之困難[285]。該報告強調仍應協調差異並相互合作、配合。OECD 作為 AI 及隱私保護於國際領域法制政策溝通之重要平臺，過去針對 AI 以及隱私保護皆有發布過相關文件指引，包含 2013 年修訂之《OECD 隱私保護及個人資料之國傳輸指導指引[286]》（OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data，下稱 OECD 隱私保護指引）及 2024 年更新之《OECD AI 原則[287]》（AI Principles，下稱 OECD AI 原則），同年亦成立 AI、資料及隱私聯合專家小組，針

[284] Cal. Assem. Bill No. 1008, § 1798.140 (v) (2023-2024 Reg. Sess.).
[285] AI, data governance, and privacy: Synergies and areas of international co-operation, OECD, at 9, (last visited 2024/12/18).
[286] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en(last visited 2024/12/18).
[287] OECD AI Principles, https://www.oecd.org/en/topics/ai-principles.html#:~:text=The%20OECD%20AI%20Principles%20are%20the%20first%20intergovernmental,AI%20that%20respects%20human%20rights%20and%20democratic%20values.

本報告之智慧財產權歸屬於國發會

對 AI 以及隱私保護政策進行重點議題之探討。OECD 報告將《OECD AI 原則》及《OECD 隱私保護指引》整合，提供 AI 及隱私政策之共同參考框架。此外 OECD 報告亦評估國際上與 AI 及隱私保護相關之倡議並提出得整合之部分，如隱私強化技術(Privacy Enhancing Technologies, PET))等。而 AI、資料及隱私聯合專家小組將更精確說明技術發展及其監管可能方向以確保隱私保護落實[288]。

OECD 報告內容由三個部分組成，第一部分為 AI 以及隱私之調和，說明 AI 以及隱私政策間之背景關係，並強調生成式 AI 之發展更凸顯兩者間之協調必要性；第二部分為比對現有 OECD 隱私原則及 OECD AI 原則之重要政策考量，說明如何於 AI 技術創新政策與隱私政策間取得平衡；第三部分則是國家及區域於 AI 及隱私政策上之發展，說明 OECD 於推動 AI 及隱私政策所扮演之角色。第一部分主要為政策背景說明，故以下僅就報告主要之第二及第三部分內容進行重點摘要。

（一）第二部分－OECD AI 原則與 OECD 隱私保護指引之關鍵考量因素

OECD 報告第二部分比對分析 OECD AI 原則與 OECD 隱私保護指引，透過分析 AI 原則中之五項基本價值原則，識別其應與隱私保護政策協調整合之部分。同時亦針對兩政策原則之用語異同進行比對。以下為五項 AI 原則對應隱私保護政策應考慮之重要因素摘要：

1. 原則 1.1 包容性成長，穩定發展及福祉

此原則重點在平衡 AI 及社會利益間之風險。OECD 報告指出，本原則所涵蓋內容並非隱私資料保護規範之重點關注領域，惟法院及主管機關仍會就社會公益判斷 AI 對隱私權利

[288] AI, data governance, and privacy: Synergies and areas of international co-operation, OECD, at 10, (last visited 2024/12/18).

本報告之智慧財產權歸屬於國發會

影響之比重。因此 AI 政策及隱私保護政策應共同就如何平衡 AI 及社會公益風險（包含隱私權利風險）提供指導[289]。

2. 原則 1.2 尊重法治、人權及民主價值包含公平及隱私

OECD 報告指出，AI 政策群、隱私保護政策群及監管機構都應對該原則所設內容進行密切協調。包含對公平性(Fairness)之解釋及釐清隱私及資料保護之範圍，考量如資料最小化、目的利用限制、資訊及個人權利保護等政策，可以共同制定適切之治理及可行之法遵方案，尤其對於可能面對隱私法遵衝擊之中小企業建立可能實踐之作法。此外，隱私權法制長期運作下來，對於權利衝突及利益權衡有相當之經驗，有助於 AI 法制政策之運用。尤其於人權影響及隱私風險評估層面，可更加緊密結合，兩者互相協調以更有效應對 AI 可能產生之風險，並降低執法層面之歧異與衝突[290]。

3. 原則 1.3 透明度及可解釋性

AI 透明度及可解釋性(Transparency and explainability)為 AI 政策群及隱私保護政策群之共同關注焦點。於 AI 原則當中翻譯為可寫釋性之用語有「explainability」及「interpretability」兩字，惟兩者意涵不盡相同，前者側重於個人權利之主張，也就是當事人要求解釋之權利，屬於法律、政策面之用語（如隱私保護相關規範當中關注確保資料處理之正確性、公平性與當責）；後者則是對於 AI 模型之解釋，屬於資料科學之說明。兩者在 AI 與隱私保護層面皆有相當之討論，部分議題則超出資料保護相關法制討論之範圍，例如當可解釋性用於協助 AI 開發者強化或改善所開發之 AI 模型時，則可能與資料保護無關。然而，在協助 AI 使用者或受影響之

[289] Supra note 285. at 30.
[290] Supra note 285. at 35.

本報告之智慧財產權歸屬於國發會

人識別是否存在 AI 演算法歧視或是幫助當事人理解 AI 運作過程等層面，兩政策群之觀點一致。於透明度及可追溯性(traceability)部分，兩政策群亦具備同樣一致的關注點。透明度強調如何讓複雜之系統可兼顧得由一般人輕易取得、瞭解，並同時維持其完整性，此亦為隱私保護主管機關長期關注的問題。可追溯性則為 AI 及隱私保護政策群共同關注之重點，建議兩者應加強整合，以達成更全面之 AI 風險管理[291]。

4. 原則 1.4 健全性及安全性(Robustness, security and safety)

生成式 AI 資料外洩風險及隱私強化技術為 AI 政策及隱私保護政策共同關注之議題，OECD 報告指出，於此議題上，兩者存在互相影響之關係，故更應加強合作，協助 AI 政策群更深入了解隱私保護相關規範及標準[292]。

5. 原則 1.5 問責性(Accountability)

AI 系統之分類以及問責之規範框架，係以 AI 系統之生命週期為基礎所建構，建議應與隱私管理程序相互結合，以促進方法論之一致性[293]。

（二）第三部分各國/區域於 AI 及隱私之發展

OECD 報告第三部分是盤點 2024 前半年各國/區域於 AI 以及隱私保護之重要政策發展。該報告指出，各國之隱私主管機關正對 AI(包含生成式 AI)之隱私規範進行合作，包含 G7 以及全球隱私會議(Global Privacy Assembly)皆有針對隱私強化措施之國際合作發布聲明[294]。

[291] Supra note 285. at 39.
[292] Supra note 285. at 39-40.
[293] Supra note 285. at 41.
[294] Supra note 285. at 42.

本報告之智慧財產權歸屬於國發會

除了國際聲明外，各國隱私主管機關亦有針對其國內發布於開發、提供及利用 AI 時之隱私保護指引、原則或是框架等政策指引。報告中提及之國家包含加拿大、法國、西班牙、土耳其、英國、美國及新加坡。此外，亦有國家對 AI 或生成式 AI 進行隱私強化技術之執法或採取相關強制措施，相關規範多針對 Open AI 以及 ChatGPT。如義大利於 2023 年 3 月 30 日發布緊急命令限制 Open AI 處理義大利境內人員個資；日本則於同年 1 月，對 Open AI 發布警告，要求其不得未經同意自 ChatGPT 蒐集用戶個資、韓國亦於該年 7 月對 Open AI 之資料外洩處以行政罰鍰；其他如加拿大、英國、美國、巴西及歐盟等亦曾對其採取隱私保護相關之法律措施。OECD 報告指出，各國在 AI 服務提供者如何遵守各國隱私保護相關法規，顯示了各國法規義務之共通性，故強調隱私保護規範國際合作有其重要性[295]。

八、 趨勢發展重點歸納

由前開國際對於 AI 在個人資料保護相關政策來看，目前尚未有國家針對 AI 個人資料保護單獨立法，而是於個別之個人資料保護法訂定相關規定（如關於自動化決策之規定），或以指令或參考文件形式建議或指導開發、部署或利用 AI 之事業、組織或個人如何遵循現行個人資料保護規範，或對現行規範作進一步之補充。換言之，開發提供利用 AI 時蒐集、利用個人資料，以目前國際趨勢觀之，仍以遵守現有個人資料保護法規規定為原則，而前述之指令或參考文件皆是以其國內現行個人資料保護規範為基礎進行解釋或補充，提供事業、組織或政府部門在開發或利用 AI 系統時能不違反現行個人資料保護規範。

(一)AI 個資保護之指引對象分為政府或官方組織及民間事業

前開國際政策趨勢中可將其參考文件/指引建議對象區分為對政府部門以及對民間事業。針對政府部門之指引主要目標係促進政府得以安全且負責任地使用 AI 技術，制定公部門統一適用之原則。而針對

[295] Supra note 285. at 42-45.

本報告之智慧財產權歸屬於國發會

民間事業提供指引則主要係針對 AI 技術開發、部署或利用可能產生之風險提醒事業注意及並給予法遵概念之必要協助與指導。

1. 政府或官方組織之參考原則

上開歐盟發佈之歐盟參考文件，對象係針對歐盟機關（構）、辦事處等單位或組織。由於政府機關通常基於公權力而蒐集、處理及利用個人資料，故認為不論其於使用 AI 模型或自行開發時，皆應負有一定之責任義務，以確保政府機關在使用 AI 技術上得以符合歐盟資料保護相關法規及規則。

歐盟 EDPB 並認為在 AI 議題上認為 DPA 具備充分專業知識處理，不論於風險評估或經驗與獨立性都較適合擔任 MSA。此一作法可以確保不同監管機構之間更好的協調，增強所有利益相關者的法律確定性，並加強 AIA 及 GDPR 之監督和執行，且與 GDPR 之單一窗口同一就機制運作上亦更有效率。

澳洲 AI 框架係以聯邦層級訂立隱私保護之原則性規範，即必須遵循澳洲隱私保護法令相關要求、透過技術手段蒐集、適用及揭露最小化之個人資料、並確保政府使用 AI 時其所管轄之個人資料安全等原則，各州及領地政府將根據該原則再各自制定其內部規範。

2. 民間事業之指引

日本、韓國及新加坡 2024 年皆以指引之方式，提供私人事業於 AI 事業在開發、提供或使用 AI 時之合規性建議。

日本 AI 事業指引針對 AI 生命週期不同階段，提出相關之建議，例如認為 AI 開發者能夠直接設計與修改 AI 模型，其所輸出之資料對於社會影響力很大，故要求其在數據訓練時應採取隱私始於設計原則，而提供者則係在提供附加價值

本報告之智慧財產權歸屬於國發會

服務時應引入隱私機制保護及措施、在使用階段則需注意不當之個人資料輸入和侵犯隱私之應對策略。

韓國指引是針對 AI 使用網路上開放資料給予建議，網路上之開放資料為訓練生成式 AI 之重要元素之一，然現行韓國法規並未有對其之明確規範。此指引確立法律基礎即開放資料可依 PIPA 中合法利益規範使用於 AI 之訓練以及開發，並給予 AI 開發以及服務提供者安全政策之建議以保障當事人之權利。韓國指引亦建議於企業內部設立隱私專門團隊以及隱私長，以專責處理與 AI 相關個人資料隱私問題。至於韓國自動化決策指引，則是搭配其個資法及施行令增訂對於當事人進行自動化決策之權利規範，提供進一步之法遵指導，包括如何判斷是否屬於法令規範之自動化決策之檢核原則及表單工具，以及若確屬自動化決策時，如何依法保障當事人之權利，包括提供對當事人可理解有意義之解釋、拒絕權之確保、如何判斷對當事人權利有重大影響、以及資訊公開之義務等。

新加坡指引則是根據 AI 系統在不同階段可能須注意之個人資料相關風險問題給予建議，除此之外，在 AI 系統開發時將商業改善目的及研究目的列為例外，在滿足條件下可未經當事人同意即可使用個人資料進行 AI 系統之開發，在部署階段則應取得同意並充分通知個人資料之預期用途。新加坡指引認為受委託進行 AI 服務提供並蒐集、處理個人資料，可被認定為資料中介者，應在處理資料前使用如資料標記等技術以追蹤被用於訓練之資料，並保留資料訓練紀錄以識別資料來源及追蹤資料之轉換方式等。

(二)建立隱私保護內控機制以因應 AI 可能造成之風險

本報告之智慧財產權歸屬於國發會

2018 年歐盟通過 GDPR 以來，關於個人資料隱私保護之相關原則及機制即已逐漸影響各國個資法令之訂定。近幾年 AI 技術之快速發展，個人資料及相關隱私保護議題再次被提起重視，不論政府官方亦或民間事業，導入或建立隱私保護內控機制皆可有效降低 AI 侵害個資之風險。盤點目前趨勢，各國在法令政策或指引上主要規範有以下內控機制：

1. 於 AI 開發階段即應納入隱私始於設計政策

隱私始於設計政策主要針對資料控制者在進行資料處理之過程中，應考慮包含資料處理之性質、範圍、內容以及目的，並對當事人之權利及自由是否產生嚴重風險等因素，並嵌入整個系統之設計中，故在 AI 開發階段即應盡早預測到隱私風險，並在設計何開發階段解決這些潛在風險，預設內建之隱私保護，除開發階段外，還應考慮整個 AI 週期之隱私安全。除此之外，應考量個人資料最小化，注意蒐集、處理及利用之合理性及適當性，不得於處理目的外任意使用個人資料。

歐盟參考文件以及澳洲指引皆建議政府單位在開發 AI 系統時須考慮採取隱私始於設計原則。

日本指引建議 AI 開發者在開發設計 AI 系統時應採行隱私始於設計政策，新加坡指引則是建議 AI 提供者使用此政策以確保其客戶在使用上能符合 PDPA 的義務。

2. 於整個 AI 生命週期內應建立資料保護影響評估制度

GDPR 第 35 條規定，若處理資料之過程可能使個人權利與自由造成高風險者，於該資料處理之前，應進行資料保護影響評估。由於 AI 之處理可能對自然人之個人特質、特定個人資料等進行處理，應屬需進行資料保護影響評估之範疇，故歐盟建議歐盟政府機構在使用或開發 AI 系統處理個人資

本報告之智慧財產權歸屬於國發會

料前須進行資料保護影響評估，澳洲指引亦建議政府在使用AI處理個人資料時須進行隱私影響評估。新加坡指引建議AI機構在部署階段須進行資料保護影響評估以識別並減輕相關風險。

歐盟之資料保護影響評估，係評估之剩餘風險是否可被組織所接受，而評估之過程通常應有資料保護專員參與規劃及給與意見。

3. 透過設立資料保護專員/隱私長於內部協助個人資料隱私保護提供建置建議並進行內部監督

歐盟EUDPR於第45條規範資料保護專員之職責包含提供個資保護建議、協助資料控管者進行內控法遵、提供資料保護影響評估之政策並擔任歐盟資料保護之窗口。參考文件建議政府設立資料保護專員職位，提供資料保護義務相關建議並協助控管者監控內部在資料保護相關部分能符合法律規範，同時亦要求資料保護專員能了解AI運作，以給予控管者適當協助及建議。

雖設有資料保護專員專職管理個人資料風險，歐盟參考文件強調各利害關係人及政府單位仍須維持溝通共同維護個人資料使用之合規。

在私部門部分，韓國指令建議AI事業應於企業內部設立專門處理AI隱私之單位並設立隱私長一職，以達成對資料隱私之相關要求。

(三)擴增資料利用之利益權衡範圍

根據新加坡PDPA修訂之規範，例外情況下可不經當事人同意即可利用個人資料。此處例外情況包含商業改善目的及研究目的之例外。

本報告之智慧財產權歸屬於國發會

商業改善目的例外之適用前提，係該商業改善有合理事由且無法利用不可識別之個人資料達成改善目的之情形下可使用。指引中提供範例包含在社群媒體服務中之推薦引擎，提供更符合其瀏覽紀錄之內容、自動工作分配系統、內部人力資源推薦潛在候選人及提高產品和服務之競爭力等[296]。

研究目的例外適用，前提係必須以個人資料作為提供數據否則無法合理實現研究成果，且該研究有明顯之公益目的，而所做之研究結果並不會做出任何影響個人之決定。另在研究結果公開時必須以不可識別個人身分之形式予以公佈結果[297]。

(四)告知義務

歐盟參考文件以及澳洲指引皆要求政府在利用個人資料時，且同時須告知當事人其個人資料被運用之相關資訊。新加坡指引提及除法定例外情況外，機構在利用個人資料時有取得當事人同意之義務。加州 CCPA 設有消費者知情權，因此消費者有權要求企業在使用 AI 時揭露所欲利用之個人資料以及目的。

(五) AI 及個人資料/資料隱私監管原則及機制之協同運作

國際參考文件基本上都不約而同強調 AI 監督與隱私保護相關原則層面有一定之關聯性，而個人資料相關法制規範與管理制度，對強化 AI 開發與應用等過程中對當事人之資料隱私相關權利之保障，有其重要性。而從 OECD 就 AI 及隱私政策群，個別對兩項法制政策領域所關注原則之比較分析，亦可看出兩監管原則間亦有相當之共通性，或可相輔相成。歐盟 EDPB 亦更進一步發佈聲明，指陳基於 AIA 與 GDPR 為相輔相成之規範，且皆有保障人權之目的，故建議各國可考

[296] *Id*. at 7.
[297] *Id*. at 9.

本報告之智慧財產權歸屬於國發會

慮指定 DPAs 作為高風險 AI 之市場監管機構，足見 AI 及個人資料監管原則或機制間之共通性或相互協同運作之必要性，應予重視。

參、 我國法制概況

一、 我國 AI 基本法（草案）確立隱私保護為該法原則之一

為確立我國推動 AI 技術與應用發展之方向及作用，我國於 2024 年 7 月 15 日制定並公告「AI 發展之基本法」草案（下簡稱 AI 基本法），從基本原則以及政府推動重點等構面提出基本價值、治理原則及政策方針。其中該法第 3 條規定政府推動 AI 之研發與應用，應遵循隱私保護與資料治理之原則，即應妥善保護個人資料隱私，避免資料外洩風險，並採用資料最小化原則，同時促進非敏感資料之開放及再利用。並於第 14 條規定個人資料保護主管機關應協助各目的事業主管機關，於 AI 研發及應用之過程，避免不必要之個人資料蒐集、處理或利用，並應促進個人資料保護納入預設及設計之相關措施或機制，以維護當事人之利益。

我國在 AI 隱私保護之立法性質上，與前述澳洲 AI 框架相似，以國家層面決定各項原則具體之政策方向，在以 AI 隱私保護與資料再利用為核心，由個資保護主管部門依據該原則具體落實保護措施與機制於作用法或規範指引中。

二、 國內採行指引先行法制政策，現階段於相關指引亦部分揭示個人資料或隱私保護之必要性

目前國內對於 AI 法制政策推動，係以指引先行之方式進行，主要由相關部會就所轄業務等，評估建立 AI 相關指引。現階段大致有國科會協助行政院，因應公務機關之生成式 AI 利用，發布《行政院所屬機關（構）使用生成式 AI 參考指引》；以及金管會對於所轄金融機構提出《金融業運用人工智慧(AI)指引》等。相關指引皆不約而同對於個人資料法制之遵守、資料或隱私保護等事項，有相當之著墨，簡述如下：

本報告之智慧財產權歸屬於國發會

(一)《行政院所屬機關（構）使用生成式 AI 參考指引》

鑒於行政院所屬機關利用生成式 AI 執行業務有助提升效率，並為使各所屬機關於使用生成式 AI 有一致之認知及基本原則，行政院於 2023 年發布《行政院所屬機關（構）使用生成式 AI 參考指引》(下稱行政院指引)，提供行政院下各機關視其業務需求，參酌該指引另訂相關規範或措施。除行政院所屬之機關外，公營事業機構、公立學校、行政法人及政府捐助之財團法人若使用生成式 AI 則準用該指引，行政院所屬機關以外之機關亦得參照該指引訂定相關規範。行政院指引第 7 點，要求各機關在使用生成式 AI 時需遵守個人資料保護之規定，同時於第 4 點提醒業務承辦人不得向生成式 AI 提供涉及公務應保密、個人及未經機關(構)同意公開之資訊，亦不得向生成式 AI 詢問可能涉及機密業務或個人資料之問題。惟若係於封閉式地端部署之生成式 AI 模型，則得於確認系統環境安全後，依文書或資訊機密等級分級使用。各機關得再依各自業務性質及生成式 AI 設備訂定使用規範或內控管理措施。

(二)《金融業運用人工智慧(AI)指引》

金管會於 2024 年 6 月發布《金融業運用人工智慧(AI)指引》（下稱金融指引)，旨在鼓勵金融機構於風險可控情形下使用 AI。指引提醒金融機構得就其 AI 系統具體使用情境，選擇適當緩解風險之機制及方法，並建議金融機構運用 AI 系統時，得就個別使用情境所涉相關風險進行評估，分配較多資源於高風險 AI 以有效管控風險，而風險評估所需考量之因素之一為使用個人資料之程度。若 AI 系統使用個人原始資料或機敏資料程度越高，則可能具較高之風險。

金融指引與隱私相關之規定為第三章「保護隱私及客戶權益」，主要概念包括使用 AI 系統之生命週期均應保護客戶隱私、

本報告之智慧財產權歸屬於國發會

採用資料最小化原則，僅蒐集及處理必要之客戶資料，避免蒐集過多或不必要之資料；使用 AI 系統時應告知客戶並尊重客戶選擇使否使用 AI 服務，並依情形提供替代方案。而在隱私保護及資料治理部分，金融指引則依循 AI 生命週期，分為 4 階段說明。

首先，在系統規劃設計階段，金融機構須評估 AI 系統是否符合個人資料保護法之相關規範及其內部資料治理政策、遵循資料最小化蒐集個人資料、並建議金融機構設有相當機制保護個人資料免受未經授權之存取、損壞、損失或洩漏。並應定期進行安全監控審查，確保員工接受適當之保密訓練。其次，在資料蒐集及輸入階段，金融機構應紀記錄資料蒐集之來源，驗證資料之準確性及完整性、確認已取得客戶同意或符合相關法令，並以風險評估判斷是否需進行額外之隱私保護處理。

於模型建立及驗證階段，應確保訓練 AI 模型之資訊及 AI 系統產生之資訊不違反個資法及相關規範，而於系統部署及監控階段，應定期監控 AI 系統之隱私規範遵守情形及安全標準，若有資料外洩或違反個資規範之情事，應立即遵循其機制進行通報及處理，並視需要調整 AI 系統。

兩部指引當中，行政院指引基本上係精簡的提醒相關業務承辦人於使用生成式 AI 應注意及遵循之重點規範領域，然並未有該如何遵循或處理之進一步說明。此做法與上開歐盟對於公務機關之參考文件，具體說明關於 AI 系統生命週期處理個資之各階段應注意之原則、資料保護專員之職責任務、應進行之資料保護影響評估、如何確保系統之合法性、如何確保資料處理之最小化及通知/告知資料使用情境、資料有無用於自動化決策、資料如何更新及保護當事人權利等有明確的說明。而金管會對金融業之指引則較符合以風險評估及 AI 生命週期作為基準之指導。

本報告之智慧財產權歸屬於國發會

三、 我國個人資料保護法令尚未將 AI 相關個人資料保護或監督機制入法

目前國際上主要對於 AI 個人資料保護或監管層面大致關注於隱私始於設計、個人資料保護影響評估、組織內部個人資料保護專業人員或監管人員（資料保護專員或隱私長）及自動化決策之當事人權利保障等規範與配套措施。

雖於 AI 基本法草案第 14 條規定個人資料保護主管機關應促進個人資料保護納入預設及設計之相關措施或機制，而目前我國現行個人資料保護法，尚未將隱私始於設計之概念納入規範。對於歐盟及韓國個資法之自動化決策相關規定，現行法亦尚未有所著墨。

另對於國際趨勢上已將資料保護影響評估（DPIA）制度明文納入法令或指引中，以識別於 AI 整個生命週期內之個人資料保護風險，並設定可降低風險之解決措施。該制度於歐盟 GDPR 建置之初即已存在並非新設，而 AI 係為處理資料之工具之一，除歐盟體系外，包含日本、韓國以及新加坡等國皆已納入法律或指引，查我國尚未將該機制納入規範。除此之外，搭配 DPIA 以及隱私始於設計之法制規劃與實施，於組織內部搭配之機制主要為資訊保護專員或隱私長以促進評估機制之落實，負責規劃及監督相關風險控管，並作為與主管機關聯繫溝通之管道，有其重要性。

四、 對於個人資料學研目的外使用未放寬

我國個資法針對目的外使用之例外，無論於特種資料之第 6 條、告知義務之第 9 條、公務機關資料蒐集利用之第 16 條以及非公務機資料蒐集、利用之第 19 條及第 20 條規定，適用範圍主要皆以公務機關及學術研究機構為主體，且以公共利益統計或學術研究（第 6 條為醫療、衛生或犯罪預防目的）有必要為前提要件。適用主體與前提範圍相對較小。

本報告之智慧財產權歸屬於國發會

觀察日本、韓國及新加坡，只要是基於研究目的或科學研究之目的者即可作為蒐集個資與利用之合法事由，而此次新加坡指引則規定出於商業改善目的以及研究目的之個人資料利用，無須經過個資當事人同意下得以直接利用，但必須可以說明其合理使用理由以及該資料應有符合規範之技術處理得以保護資料安全。而目前 AI 之研發未必僅由公務機關或學術研究機構進行，多數 AI 之開發與利用實則係由民間事業進行投入，是否有必要擴大學術研究條款之規範，亦為後續討論之重點。

肆、 小結

綜觀 2024 年所觀測國際對 AI 在個人資料應用之政策，不論是對政府或是企業給予建議，參考文件或指引之內容皆在強調資料使用的正當性及合理性。並且根據其國內現有個人資料保護規範，建議政府或是企業宜採行設有資料保護影響評估措施以及強化資料保護專員之效能，以確保資料隱私之風險受到監控。

一、 指引先行為國際趨勢，然配套法制之前提要件須納入修法評估

本年度觀測主要國家對於 AI 個人資料保護之法制政策，主要係透過建立政策說明或指引之方式進行，而非直接對於現行個資相關法令進行研修或為專法之研議。然而所觀察之政策說明或指引，主要重視與應用之規則，包括隱私始於設計、自動化決策規範及資料保護影響評估機制之應用，於目前我國個資法皆尚未有對應之規範。此外，主要落實涉及 AI 部署或應用之個資保護影響評估的組織內部重要角色－個資保護長（DPO），現階段亦尚未入法，故國際相關參考指引仰賴之基本個資法制規則，於我國則尚無法以現行個資法直接之條文加以指涉。

本報告之智慧財產權歸屬於國發會

然而，數位經濟環境之發展及 AI、演算法等數位科技之應用為不可擋之趨勢，而我國個資法目前尚未對應數位科技可能帶來之經濟社會動態變遷有相當之應對。故於參考國際指引或做法之際，建議仍需回歸探討個資法本身對於數位科技發展所需具備之態度或機制，例如將資料保護影響評估或隱私始於設計適切入法，強化對於公務及非公務機關採行相關技術措施時對資料隱私保護之要求納入規劃，從開端即評估，根本性的提升公務及非公務機關資料隱私保護之觀念及義務。

至於自動化決策對當事人之影響層面，基本上並非單純資料隱私之問題，實際上於不同領域層面皆有 AI 或演算法進行對當事人權益有關之自動化決策，可能對當事人帶來損害之可能性，包括本次專案其他焦點之消費者保護、勞動保護等層面，皆不乏有 AI 應用對當事人自動做成之決定，可能產生歧視或剝奪消費者選擇權等問題。此部分問題若有跨領域整體面之 AI 法制政策，應配合整體考量納入評估。

此外 AI 生命週期之資料蒐集、處理與利用之議題，亦與個人資料保護法制息息相關，尤其涉及技術開發層面之資料蒐集與利用，現階段學術研究條款對組織及利用範圍之限制是否有調整之必要，亦得納入考量。

二、 法制尚未修訂前仍得透過指導原則或函釋之強化，協助機關法遵之落實

基於法律研議過程之冗長，以及我國尚待先行籌設獨立機關－個人資料保護委員會，方能進一步對於個資法實質議題進行修訂。然而 AI 之開發、部署與應用已於社會各層面如火如荼的展開，實無法持續等待法制的具體修正及通過。故個資主管機關仍得於現行法之框架下，對於 AI 不同階段應如何遵循個資相關法律規範，或有須提醒注意之事項，建立指導原則或強化法規適用之解釋，以協助公務及非公務機關落實個資法等相關規範之要求。

本報告之智慧財產權歸屬於國發會

例如參考新加坡之指引，強調資料開發應注意之資料最小化、比例原則及資料之去識別；於部署階段強調如何依據個資法取得當事人之同意、告知義務及問責，並建立適當之安全保護措施。於系統採購層面，則要求系統服務之提供者於開發前段，必須適切進行資料標記與訓練資料之記錄，以利後續應用之追蹤，並說明如何於符合個資法要求之前提下對使用者提供服務等。或如韓國對於 AI 開發或服務提供涉及來自公開來源之資料，如何適用個資法及應注意之層面提供指引，此部分雖然我國目前僅於非公務機關蒐集部分，於個資法第 19 條有一般可得來源之規定，然而關於資料之利用，涉及公益性層面，則主要是公務、非公務機關或特種資料相關之學術研究條款，適用範圍有相當之限制。但仍可對於現行法一般可得來源資料或其他特定情形於 AI 層面之適用性詳加說明。

三、 個資法制規範與執法與 AI 發展運用息息相關，宜善加考量個資主管機關角色，以兼顧 AI 開發與應用對資訊隱私之保障並促進整體社會經濟之發展

歐盟本年度通過之 AIA 後 EDPB 發表聲明指陳 AI 開發與使用將影響人類基本權利，而保護個人資料不被濫用係不容忽視之一環，故建議應指定各成員國之 DPA 擔任市場監管機關較為合適，其不僅具備獨立性，且 GDPR 施行至今也已經累積監管實務經驗與能力，可確保 AI 法制之推動及執行與 GDPR 具備一致性。

由 EDPB 之聲明可以發現其明確的意識到 AI 發展的風險與 AIA 法案之落實與資料保護法制政策有密不可分的，有必要將 GDPR 等資料隱私保護之核心規範與價值，於 AI 生命週期各階段具體落實。尤其於訓練階段即應注意與考量，方有可能有效降低 AI 運作對人民資料隱私可能帶來的風險。而 DPAs 亦須與 AI 相關主管機關或歐盟之委員會形成緊密之關係，針對涉及個人資料處理與利用之 AI 相關議題積極參與，以確保跨部門或組織單位相關 AI 開發、部署等同實符合 AIA 及歐盟相關資料保護規範。

本報告之智慧財產權歸屬於國發會

雖然並非所有國家或國際組織都如同 EDPB 明確認為個資保護獨立機關應擔任 AI 之市場監督機關。且目前國際上主要亦是歐盟有較為明確且具廣泛影響力之 AI 風險規範。然而其認為 DPAs 需正視並積極參與 AI 法遵監督落實之看法仍有相當之參考價值。我國正值獨立機關籌設階段，於法制及整體制度尚待建立之初即納入 EDPB 之邏輯尚嫌過早，因 EDPB 認為 DPAs 可以擔任 MSA 之基礎在於 DPAs 執法經驗已相當充足，然而我國則尚在起步階段，要一步到位恐有困難。然而，個資保護獨立機關仍可於組織任務層面，將新興科技或 AI 應用之影響納入規劃。短期內先行透過對於我國實務發展與應用進行了解，提出對應之指導或作法，累積相關資訊、知識及執法能量，中長期再搭配國內 AI 法制政策整體走向調整法制政策參與之角色，亦不失為可行之作法。

本報告之智慧財產權歸屬於國發會

項次 5. 法制政策綜整建議

一、 國際數位科技相關法制政策已從多面向開展

由本年度計畫自 4 月開始進行之前瞻數位科技法制政策變革趨勢觀察，雖基於計畫期程因應政策需要以 AI 相關之法制政策為主要關注點，然亦觀察到許多於 4 月以來國際上之其他數位科技議題面向，包括資料治理、數位監管、數位身分、資訊隱私、競爭法制、網路/資訊安全與韌性及智慧財產等層面之法制政策發展。

整體而言，可以說數位科技相關之法制政策為多面向之議題，近年來許多議題已有法制面之變化，例如歐盟已經通過之資料治理法、數位服務法、數位市場法等。但仍有許多面向尚在發展中，而陸續於各國有不同的進展，例如資料之流通應用、數位身分、競爭以及安全的議題。而在 AI 層面，尤其是基於這兩年生成式 AI 開發應用對社會經濟帶來快速的衝擊，加上近幾年已逐步受到關注的演算法黑箱以及 AI 分析決策等議題與今年歐盟 AIA 之通過，更是讓 AI 延伸各面向法制政策探討成為關注的重點。

綜整今年度觀察的情形大致可歸納於以下面向：

(一) AI 法制政策層面：

2024 年 AI 法制政策於國際上大致係從監管、安全與個資保障、內容產製或技術應用之影響、消保與演算法歧視、國家安全與勞工權益等面向為發展之重點。而國際會議或國際組織對於 AI 監管之框架、原則以及執法之邏輯亦持續探討中，故除了本年度已擇定之 AI 著作權、消費者/使用者保護、勞工權益及個資保護與監管之趨勢已於前面焦點分析歸納趨勢發展之重點，於此不贅述外，其他 AI 法制政策層面亦有部分之進展，例如：

1. AI 監管規範方向層面：

本報告之智慧財產權歸屬於國發會

本年度國際上最受矚目也最為重要之發展里程，為 5 月份歐盟 AIA 之通過，並於 8 月份正式生效。促使各國（包含我國）皆開始積極探討如何建立 AI 之法制監管規範，範圍及強度等議題。至今僅有美國部分州別採行類似於歐盟 AIA 對於高風險 AI 加強規範之作法，例如美國科羅拉多州 5 月接續通過，預計於 2026 年 2 月生效之《人工智慧消費者保護法》等。其他國際會議如英國主導之 AI 高峰會，於 5 月於首爾舉行之第二屆會議發表「首爾宣言」則強調確保各國 AI 治理框架之互通性有其重要性。新加坡則自成一格，僅先針對生成式 AI 進行治理框架之建構，提出非強制性重點指引，協助事業依據本身之屬性，依循該治理框架建構適合之實踐模式。

2. AI 內容產製影響層面：

除了關於 AI 生命週期之著作權議題之外，應用得以生成或修改內容之 AI，例如深偽技術可能形成不實影音、聲音或圖像等應用，於今年亦受到相當之關注。有從詞曲創作人或表演藝術工作者角度切入，考慮將聲音等個人特質亦納入肖像權保障者或建立保護規範者，例如美國田納西州之《確保肖像、聲音和圖像安全法案》、美國參議院提出之《培育原創、促進藝術與保障娛樂安全法》等；亦有從犯罪與網路安全角度切入者，例如英國修正《網路安全法》將深偽技術製作之不實影像列為刑事犯罪、美國愛荷華州之《散布、播送及陳列不實性影像法案》與《散布、播送及陳列與兒少性剝削有關之性影像法案》將數位性暴力納入刑事立法等。

3. AI 與國家安全層面：

AI 涉及國家安全之議題亦開始受到關注，此部分係以美國政府為主，例如美國國土安全部於 4 月成立 AI 安全顧問委員會，針對能源、公營事業、交通、國防等共 16 項關鍵服務

本報告之智慧財產權歸屬於國發會

領域應用 AI 技術衝擊議題進行對策之研商。並由國會提出《保護美國人免受外國對手應用程式侵害法案》對於可能對國家安全產生威脅之「外國敵對勢力控制的應用程式」於法案生效 6 個月內須拆分於美國之業務或出售持股。以及強化《晶片及科學法》之執法落實，降低美國半導體產業對其他國家之依賴，建立半導體生態系。

(二) 其他數位法制政策層面：

除 AI 外其他數位法制政策層面今年亦有部分之進展，大致從以下幾個面向重點說明：

1. 資料治理層面：

此部分發展係以歐盟為主軸，最重要之進展為《資料法》及《歐洲互通法》之生效，促進公私部門及公部門間之資料互通與合作；針對特定領域部分則有《歐洲健康資料空間規則》之通過，提高歐盟人民對個人健康資料存取之便利性，並促進政府之循政決策。英國創新科技部於 10 月份亦對於公共資料之利用，研議《資料利用與近用法》草案將公共資料共享與應用規定明文化，除簡化部分資料利用程序外並促進特定領域（如金融或能源等）相關資料之共享，並建立數位身分驗證制度。除法制之建構外，相關資料互通之機制亦為發展重點，例如韓國與歐盟即於 10 月召開國際資料合作研討會議，討論資料價值鏈之合作議題，韓國並成立公私資料聯盟。

2. 數位身分層面：

數位身分議題為數位網路環境法制政策一個根本性之問題，為於數位環境下從事法律行為或參與各項活動之基礎，故近年來亦廣為受到重視。以 2024 年度觀測發展來說，歐盟於 3 月通過《歐盟內部市場電子交易之電子身分認證及信賴

本報告之智慧財產權歸屬於國發會

服務規則》為歐盟居民建立數位身分錢包機制，提高數位身分於跨國線上服務之互通無礙，並保障個人資料。瑞士及澳洲則於上半年皆陸續通過數位身分法相關法案，促進數位身分制度之建構及配套規範之完備。日本則於下半年陸續針對電子簽章法認證標準等議題進行討論，以評估未來電子認證議題之配套作為。

3. 數位監管層面：

此議題於前些年主要為歐盟對於數位平臺監督所提出之《數位服務法》（DSA）與《數位市場法》(DMA)。2024 年對此議題主要屬於執行層面之發展，以及對於更早訂定之《特定數位平臺透明度及公正性規則》執行情形之評估。此外歐盟新興法案層面則是針對數位媒體監理架構提出並通過之《歐洲媒體自由法》（EMFA）預計於 2025 年 8 月施行，以確保媒體之獨立性及透明度，並保護媒體免受大型線上平臺無故刪除線上內容。英國則於 2024 年通過《數位市場、競爭及消費者法》（DMCC），強化執法機關英國競爭及市場管理局（CMA）之執法權限，促進數位市場消費者權益保障及維持市場競爭。

4. 網路、資訊安全與韌性層面：

此議題則主要有連動 AI 發展之網路安全議題，以及涉及網路關鍵基礎設施等提升網路韌性之議題，前者諸如加拿大安大略省提出《公部門網路安全強化及信任建立法案》針對運 AI 應用涉及之網路安全問題進行系統面之要求；以及英國科學、創新及技術部就 AI 網路安全提出計畫並進行意見徵集。後者則如美國網路安全暨基礎設施安全局（CISA）發布礎設施韌性規劃架構，提供關鍵基礎設施經營者進行風險評估、發展行動措施、執行與成效評估之指導；以及歐盟於 10

本報告之智慧財產權歸屬於國發會

月通過《網路韌性法》強化項歐盟境內提供之數位產品於網路安全層面之要求，尤其要確保物聯網整體供應鏈之產品生命週期皆符合相關網路安全要求；於同月並發布依據修正之《歐盟高度共通程度之資安措施指令》所訂定，針對關鍵實體（critical entities）及網路安全之實施規則（implement regulation），強化特定數位服務提供者之網路安全風險管理及就重大事件對主管機關之通報義務等。

二、 國內相關法制政策推動情形與綜整建議

(一) 國內目前相關法制政策推動情形

我國目前對於 AI 整體面之法制推動，以現階段行政院數位政策法制協調專案會議之方向，係採取先指引後立法之法制規劃原則，故已有相關行政機關就所轄事務發布與 AI 相關之指引（如行政院及所屬機關（構）使用生成式 AI 參考指引；金融業運用 AI 指引等）。然而就新興立法層面，目前主要為 2024 年國科會提出之 AI 基本法（草案），已提報行政院審議。而對於 AI 應用層面已進行之法規修正，則是以前述 AI 對使用者/消費者保護焦點議題探討時所提及牽涉國內打詐政策之法制修正，包括刑法第 339 條之 4 利用電腦合成技術製作不實影像、聲音或電磁紀錄之加重詐欺罪、及《詐欺犯罪危害防制條例》第 31 條規定要求平臺業者必須標記以 AI 技術生成內容之規範等。其餘議題，包括焦點所探討之著作權、使用者與消費者保護、勞工權益及個資保護與監管部分，則尚未進入到法制研議之階段，而多數仍處於函釋或議題研析之過程。

就目前 AI 基本法之內容觀之，其涵蓋了包括創新合作、人才培育、風險管理、應用責任、權益保障及資料利用層面，後續並須由各部會進行法規調適及業務檢視，進行後續是否須推動相關法制增修之研議。故就 AI 基本法草案之推動邏輯與進度而言，現階段我國 AI 法制政策，應該是進入到宣示法制政策重點方向之階段，而該如何達成

本報告之智慧財產權歸屬於國發會

相關推動方向，則仰賴各部會進一步評估及規劃適切之作法，包括政策措施之提出、軟法或硬法之規範研議或修正等。

除了 AI 之議題外，國際數位法制政策層面關注之議題，於我國現階段部分議題有初步進展，惟多數亦尚未有明顯之進展。其中於資料治理層面，搭配 AI 法制政策以及行政院數位政策法制協調專案會議之推動，目前係由數位發展部（數發部）提出未來將研議《促進資料創新利用發展條例（草案）》，以提升公部門資料加值利用及公益資料之共享，促進產業創新。而數發部於 2023 年則係先行公布《數據公益運作指引》及《隱私強化技術應用指引》，推動自願、無償之公益數據利用，及降低對於涉及隱私之資料利用的風險。而特定資料類型部分，則有衛生福利部(衛福部)提出之《衛生福利資料管理條例（草案）》研議中。除上述法制政策的進度外，現行法層面則尚未有較為全面性之資料治理法制規範存在。另對於相關之個人資料去識化及擴大資料用於科技研發等相關議題，則尚待個人資料保護委員會設置後對法制面之修訂進行評估。

於數位身分部分，電子簽章法雖然於 2024 年 5 月修正通過，然而其並未如同歐盟將數位身分識別納入規範，亦未如同日本，將電子身分認證議題納入法案討論。而國內 2020 年雖曾提出數位身分證之政策，然因當時仍有相當之資安、隱私風險及法令配套尚未完全建構之疑慮，故暫停推行，留待後續進行個資、資安與法制面之整合評估，以求慎重。而數位身分法制政策及配套機制之建置，實為數位經濟及社會環境發展重要之要素，建立適切之法制規範或機制有其必要性，期待未來國內相關主管機關完成法制政策配套討論與評估後，能夠建立符合我國國情與國際趨勢之數位身分規範與機制。此外，歐盟本年度甚至透過修訂數位身分法制框架，進一步建立公民資料之數位錢包制度，除得以促進歐盟成員國對於國家電子身分識別之相互承認外，並建立共通之安全措施、技術框架與標準，提高各國對數位身分認證機制之相互信任與互通。同時也藉此一修法建立了歐盟數位身分錢包，

本報告之智慧財產權歸屬於國發會

便利歐盟人民自主之資料共享與控制，以及改善跨國數位服務對身分資料之存取與安全度，降低身分驗證成本並保護隱私。足見優良之數位身分規範與配套機制，對於政府與民間數位服務於可信賴之環境發展，及個人資料自主權與控制權皆有相當之助益，實有必要加以評估。

於數位監管部分，此為近年來除了近期之 AI 監管外，國際上最受到重視之議題。此議題由早期電子商務議題發展至今，面對數位科技之變化與數位平臺商業模式之高度發展，於近年由歐盟開始進行法制監管層面之變革。歐盟備受關注之《數位市場法》及《數位服務法》也已於去年及今年相繼施行，前者針對一定規模之數位平臺，透過指定為守門人之機制，對其進行事前義務之要求及監管，促進市場之有效競爭；後者則將線上平臺類型化，進行責任與接受監管義務之要求，並必須有指定之人員對應處理歐盟主管機關之要求及協調。英國今年則是透過 DMCC 強化執法機關對數位事業之調查與要求之權限。相關規範對應於我國，國家通訊傳播委員會（NCC）曾於 2022 年參考《數位服務法》之精神，提出過《數位中介服務法》，然因有損害言論自由之相關爭議，未繼續推行。其次則是 2024 年通過之《詐欺犯罪危害防制條例》中對於網路廣告平臺業者等，參考歐盟 DSA 之精神對於在我國境內無營業所、住居所、未設立分公司等事業，要求必須提報法律代表，作為執法機關連絡之對象，並強化其配合執法之義務、管理及連帶賠償責任等。然而，除網路廣告平臺之外，現階段尚未有對於共通性之平臺或數位服務監理議題有直接之法令規範或法制政策規劃，而平臺商務模式引發之目的事業主管機關及監督之議題，仍未有對應之法制政策處置。

最後於網路、資訊安全與韌性層面，現階段國內對於資訊安全議題最主要之規範為《資通安全管理法》相關規範，然而其主要在處理者，惟涉及國家資通安全環境之事務，僅有公務機關，及特定受指定之非公務機關方有其適用。此外，則是於特定領域規範之網路安全或資訊安全規定，例如針對電信事業及電信服務市場顯著地位者互聯，

本報告之智慧財產權歸屬於國發會

於網路介接點安全性評估層面，在《電信事業網路互連管理辦法》及《市場顯著地位者互連管理辦法》規定網路互連是否有損電信網路安全性與可靠性必須納入技術可行性評估；於《金融創科技創新實驗條例》則將資訊系統安全控管列為創新實驗計畫必須定期提出報告之範圍；或各中央目的事業主管機關就個人料檔案安全管理訂定之辦法中之資訊安全要求等。至於普遍性之網路安全層面，或類似歐盟《網路韌性法》對於物連網產品等具備數位元件產品安全度提升之則尚未有相關法制規範。

(二) 綜整建議

綜上，若對比晚近國際趨勢法制政策發展重點及我國現行數位法制政策現況而言，我國尚有相當之發展空間，惟基於各國國情、數位技術及產業發展狀況各有不同，且部分國際組織，如歐盟之法制政策，實為近年來推動數位歐洲整體策略環節之持續發展，有其法制建構之優先順序，及歐盟整體發展之區域背景。故我國法制政策推動仍應以我國國情特性、實務發展情況、法制發展進程及未來可能發展進行考量。依據本年度計畫觀察及研析，提出以下綜整建議方向：

1. 短期建議

(1) 對於國內 AI 實務應用情形及影響應強化調查，作為適切評估法制政策之基礎

國內對於 AI 法制政策之討論，現階段多數在探討國際規範之情況，尤其 2024 年歐盟 AIA 通過，以風險分級邏輯進行 AI 產品與服務之監管，其具體之規範，受到國內各界廣大之關注。然而，國內現階段並未有對於 AI 實務應用層面有較為深入之調查，以致對於 AI 實務應用產生之問題較難精確的界定，於法制政策評估上就會有所疑慮。到底應該採取歐盟界定高風險 AI 並進行高度監理之作為，抑或應先採取軟法讓產業先行發展等，或哪些領域

本報告之智慧財產權歸屬於國發會

已經出現需要立即解決之問題等，國內目前之資料掌握度仍不高。

確實有部分民間之調查針對台灣企業之 AI 整備度等層面，然而相關資料調查目的主要著重於對相關事業利用 AI 或技術佈局之建議，所得資訊較不適宜法制政策面之評估。例如焦點議題當中關於消費者保護或勞工權益層面，提供終端使用者或消費者之商品或服務，有採用哪些類型之 AI 或演算法應用，服務型態為何以及使用者或消費者之感受為何，影響為何等，並未有客觀之資訊可供評估。於勞工權益層面亦然，雖對於 AI 就業評估、篩選、派工、工作評估等議題皆有所討論，然而國內實務應用之情況為何，則同樣未有客觀之調查資訊可供主管機關進行政策規劃評估。故建議法制主管機關，尤其涉及 AI 基本法已揭示議題之法制主管機關，宜先就主管規範所涉 AI 議題規劃適切問題進行調查，以利後續法制政策評估。

於調查層面，可考量先就主管行業當中，近年來資訊化程度較高之事業，調查其於業務或內部管理層面使用 AI 之情形。業務層面應視其主要業務型態進行調查議題之設計，例如是否運用 AI 或演算法對於服務使用者進行資料的蒐集或分析，主要蒐集哪些資料、進行哪些分析，以及用於怎樣的用途或目的；運用哪類/哪些類型之演算法達成上開用途或目的，及其效果如何；對於所蒐集之資料，有無相關管理之作為，有無監督或限制 AI 或演算法蒐集分析之資料；有無避免 AI 過度蒐集資料之機制；利用期間有無發生過怎樣的爭議；有無採取相關機制確認演算法運作是否正常，或有無出現建議或結論之偏差，若有相關機制，則該機制為何。對內部管理部分，例如是否採行任何 AI 或演算法系統於內部管理，例如人員招募、績

本報告之智慧財產權歸屬於國發會

效評估、派工、工作監督、健康監督或其他應用層面；利用之目的或情境為何；自行開發或委託他人開發；若為自行開發，過程中對於員工權益有做怎樣的考量，有無參考可能受影響之員工意見；若委託他人開發，如何選擇開發者；如何確保開發者於保障員工權利之立場進行開發；如何進行確認；以及部署/應用過程中有無監督或人為介入措施；有無給予申訴管道及爭議處理機制如何運作等。

(2) 涉及人民權益保障與法律關係穩定性之議題，宜先強化現行法適用之解釋或指導原則，提升法律適用明確性

美國 AI 法制政策之走向與歐盟有相當之不同，其於聯邦層面並未先制定共通性之監管專法，但國會之 AI 小組及各州，於法制層面之考量則主要偏向於處理人民已經面對的問題，也就是 AI 應用已經進入到涉及民眾權益之層面，先行進行法制面之評估與因應。包括焦點議題探討之著作權之利用、終端使用者與消費者保護層面之議題、勞動權益當中探討之平臺勞動關係及就業歧視之議題以及 AI 應用對個資法適用之議題等，皆為已直接影響人民之議題。

上開議題所對應之現行規範，雖然尚未針對 AI、演算法、平臺等問題進行法規面之調整，然因多數屬於共通規範層面，有機會先行透過對於現行法之解釋，或進一步建構對於特定技術應用之指導原則，將法律關係之定位、法律適用之疑問或可參考作法提供產業及公眾了解或參考。此一作法有助於在進一步法制政策評估前讓法律關係與適用明確化，降低不必要之爭議。可參考前述各焦點議題小結針對函釋、指引或指導原則建立之建議。

本報告之智慧財產權歸屬於國發會

(3) 加速推動 AI 基本框架法制之通過，建立並強化各界對國內整體法制政策推動之共識

歐盟 AIA 從最初提案至最終通過，係從 2021 年由歐盟執委會提出草案，至 2024 年 3 月正式於歐洲議會通過，5 月獲得理事會簽署，共計 3 年的時間。而這僅是歐盟內部共識形成之過程，甚至在法案提出之前，即已透過 2018 年之歐洲 AI 戰略(European AI Strategy)、AI 協調計畫(Coordinated Plan on Artificial Intelligence)等政策研議之過程[298]，尋求聯盟成員對 AI 發展與法制監管架構之共識，整體而言則是 6 年的光景，足見如何評估 AI 法制政策，實相當複雜。2024 年度觀測之英國與韓國 5 月於第二次 AI 高峰會所公布之首爾宣言，亦主張各國 AI 監管框架不但須有共識，且應具備一定程度之互通性。而歐盟於通過 AIA 後於 2024 年 9 月也進一步與包括美國、英國、澳洲、冰島、挪威與以色列等國簽訂人工智慧框架公約(Framework Convention on artificial intelligence and human rights, democracy, and the rule of law299)，繼續為 AI 監管之國際共識而努力。

從國際法制政策的發展可以看出，AI 之法制政策推動，政策方向之明確與共識之形成有其重要性。我國目前已經研議 AI 基本法，雖並非如同 AIA 之作用法性質，但對於法制政策應著重之重點與原則，已形成相當之框架，可作為後續政府各機關落實法制政策建構之基礎。故短期內宜以加速推動基本法通過，並以此為基礎強化配套作用

[298] European Commission, European approach to artificial intelligence, https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence , last visited 2024/12/18.
[299] Council of Europe, Council of Europe opens first ever global treaty on AI for signature, https://www.coe.int/en/web/portal/-/council-of-europe-opens-first-ever-global-treaty-on-ai-for-signature , last visited 2024/12/18.

本報告之智慧財產權歸屬於國發會

法或政策措施之提出，將有助於 AI 法制政策結構之逐步完備。

(4) 建立資料治理及資料應用法制規範及監督體系

資料之取得與利用為數位經濟與技術發展，包括 AI 之開發與利用重要之議題。歐盟對於資料相關法制之建構系依循其整體資料戰略(Data Strategy)所為之建構，其中涵蓋個人資料、公部門資料及公私部門資料共享或互通之層面。而我國現階段除了前述數發部即將研議之《促進資料創新利用發展條例（草案）》並已知可能涉及公部門資料加值利用及公益資料之共享議題之處理外，似乎並未有較為完整之資料治理法制規劃。

然而數位經濟與技術發展所需應用之資料，其類型或權利態樣雖具多元性，然其取得或利用之機制可能具備共通性，也許可以透過單一法令之整體規劃進行推動，而無須由不同主管機關針對個別法令分別進行修訂或研議。例如生成式 AI 之訓練資料，其可能來自於開放網路取得之所有類型或權利之資料，可能為已經開放應用無需另為授權之公共資料，也可能是仍具備著作權或具備特定個人識別性之個人資料等。然而，無論資料為何，皆出自同一之取得方式，實可透過共通性規則之建構（如資料治理或 AI 資料治理相關專法之建構）進行規制，而無須重複於不同法制規範，該共通性規則之內涵可以考慮包括資料權利之取得規範或機制、資料權利人之權能（如可否禁止或退出 AI 資料之利用）、資料權利人行使權利之效果（如主張資料退出或撤回同意對已開發之 AI 模型之效果或向後生效）、資料權利人之保障機制（同意權行使、授權費用費用等）開發者應擔負義務（如需建立、保留資料訓練紀錄或歷程、確保資料來源之可信賴及合法權利、確保開發技

本報告之智慧財產權歸屬於國發會

術不致過度蒐集資料或歧視）、申訴與救濟之規定等。或針對建構 AI 或技術開發訓練資料庫層面，建立共通之規則，同時強調資料取得應具備之合法性要件，以及資料應用須避免之情狀等。歐盟資料治理法及後續資料法之建構即是採取此一邏輯，為我國資料治理法制推動之參考。

2. 中長期建議

(1) AI 開發與應用範圍廣泛，但有相當共通性之議題應為整體原則性之考量，長遠而言需評估建構 AI 共通性之作用法規範

現階段我國部分法制體制係保留產業主管與對應之概念。即便是涉及共通權益之法制規範，例如消保法或個資法等仍有針對特定產業別進行子法要求之體制。然而 AI 之開發到應用，未必有必要進行產業區隔，而是有共通之問題，從開發者、部署者到使用者端必須考量、遵循或注意。例如對於 AI 之開發者，要求必須避免開發會出現歧視結果之 AI，對於部署者要求必須讓參與之使用者知曉或了解其正在利用 AI 或被 AI 分析，AI 可能對他作些哪方面之決定或可能產生甚麼影響，有無申訴的機會。以及要求事業若運用 AI 於業務各層面，必須有適當之人為監控或定期檢測評估等等。皆是於不同領域應用都需要考量之問題。

此外 AI 之運用也可能改變對於既有法規判斷的邏輯，例如關於當事人曾經授權給 AI 進行訓練之資料，可否收回之問題。包括著作權人或個人資料當事人等具備特定權利之訓練資料取得可能皆有同樣的問題。當權利人撤回/撤銷其授權或撤銷其同意，則該資料若已被用以訓練 AI 模型，則其撤回或撤銷之影響或效果為何，則可有共通

本報告之智慧財產權歸屬於國發會

性之原則規範，例如規定於資料授權或同意撤回或撤銷前已訓練之 AI 模型應用不受影響等。

故現階段雖然於基本法之邏輯下係分別由各法令主管機關進行法制面之評估，然而長遠而言，共通性原則之規範建構仍應納入考量。

(2) 確立我國數位經濟發展定位，建立適合之數位監管法制體系及新興數位科技應用發展之法制因應機制

現階段我國對於數位經濟相關之法制政策議題如何處理，基於個別部會傳統之組織分工，對於新興議題如何監管時而出現多頭馬車或無人處理之情況。然而，數位監管議題有許多具備跨領域性質，需要有較為橫向之思考與評估。例如近年來備受關注之數位平臺監督與法制適用之問題，其所橫跨之議題面向因平臺生態系發展而相對複雜。然而多數現行法令規範於建立之初並未考慮如數位平臺此類具中介媒合，雙邊或多邊市場性質之服務類型，使得涉及平臺之商業模式，於法令關係以及法令適用上常難以處理。而相關問題在涉及跨國性平臺之案例層面，將更加複雜，甚至可能因為跨國平臺服務多數並未有傳統規則上落地之概念，使得法律適用及對國人權益保障部分，產生極大之問題。故國際近年來對於平臺監管應採取怎樣之法制結構亦有相當之探討，包括前述歐盟之 DSA、DMA 及 EMFA 以及近年國內外探討之平臺壟斷、競爭與媒體議價之問題等，皆為應對數位平臺發展之法制變革。

我國實務近年來對於數位平臺衍生之問題如何處理亦有相當之爭論，包括數位平臺議題之主管機關、數位平臺與利用平臺之事業或消費者間之法律關係及爭議處理、平臺演算法之黑箱作業、對使用者或消費者之誘導或誤

本報告之智慧財產權歸屬於國發會

導、使用者隱私、平臺與商業使用者間之公平性及平臺責任建構等問題。而對跨國平臺服務執法或消費者權益保障層面，另有無法找到適切對應窗口之問題，而導致執法或爭議處理之困難。對於現階段以各類數位平臺及跨國數位平臺為核心之數位經濟環境，建立適當之監督機制實已十分迫切。然而基於我國法律體系關於目的事業主管機關之建構邏輯，導致相關個案出現首要面臨之問題，為目的事業主管機關之決定，法制建構層面亦然。而數位經濟環境涉及之議題，高度虛實整合及縱橫交錯之數位生態系發展，已非垂直產業切分邏輯可以解決。

然而我國是否可以直接如同歐盟對平臺訂定高度責任要求之規範，或如英國強化對平臺調查及事前責任之要求，或要採取如何之監管強度或作法，或應著重於哪部分之監督強化，實取決於我國產業發展於數位經濟層面之定位。包括產業或技術研發對國際數位平臺經濟依賴之情況，使用者或消費者對相關平臺服務應用之情形等。而對於法制政策層面之規劃與評估，需要有適切之角色進行整合，現階段或可考量透過行政院之數位法制政策協調機制，然而長遠而言，面對不斷變動之數位環境，宜建立常態之運作體制，指定主責機關進行推動，方能有效率的檢視、評估與決定新興商業模式所需之法制對策。

(3) 新興權利之考量與建構應納入法制政策評估

各類 AI 技術之研發及變化，實已逐漸衝擊現有法律規範之權利體系，例如於 AI 著作權議題層面，近年來不斷有 AI 開發者想要挑戰 AI 之產出是否具備著作權或專利權等現有權利之問題。此部分目前國際上多數意見認為純然 AI 產出之結果，並非人類智慧投入創造之成果，不宜被賦予著作權。然而即使非屬著作權，但投入 AI 訓練

本報告之智慧財產權歸屬於國發會

研發使之產出各種作品，是否可以讓相關產出具備某種權利，則為是否應建構新興權利之問題。而晚近另有運用深偽技術模擬出類似特定名人之聲音或影像，而引發名人聲音是否是否有相關權利保障等問題，亦是因為 AI 發展出現之問題，美國部分州別考量將肖像權範圍擴張至聲音，為一種改變既有權利範圍限制之作法，亦不失為可評估之方向。若長遠而言國內可對 AI 共通議題建立規範，則可考量對於 AI 利用涉及之權利問題，評估建構新興權利或規範之可能性，一方面保障可能被影響之權利人，一方便亦能使產出權利明確化，使其具備一定之經濟價值。

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」委託研究計畫

國際法制政策趨勢觀測雙月報

中華民國 113 年 12 月

國際法制政策趨勢觀測雙月報

項次 1. 四月雙月報

壹、 資料治理

一、 歐盟

(一)2024 年 1 月 11 日歐盟資料法（Data Act）生效後對自然人及法人之市場效益

近年來物聯網（IoT）使得數位資料量有著飛快的增幅，然就資料的利用權限尚不明確，生產者也未必同意使用者任意取用該類資料，導致數位資料的近用及互通落差甚大，進而阻礙數位經濟發展與價值創造。為打造資料經濟且推動 2030 年數位轉型工作，並賦予使用者自主控制資料之權利、工具與技能，《歐盟資料法》（Data Act）遂於 2024 年 1 月 11 日生效，而該法成為「歐洲資料策略」（European data strategy）底下的第二項立法措施，不僅制定公平且創新之資料近用原則，明定創造資料價值之主體與條件，更與現行其他多項規範調和，包括一般資料保護規則（GDPR）、數位單一市場著作權指令（Directive on Copyright in the Digital Single Market）、數位服務法（DSA）、資料治理法（DGA）等，共同形塑歐盟資料市場。該法最快將於生效日起 20 個月後開始適用，即 2025 年 9 月 12 日，惟第 3(1)條涉及新產品資料存取簡化之規定係適用於該法生效日起 32 個月後上市之智慧連網產品及其相關服務，亦即 2026 年 9 月 12 日。

資料法旨在規範如何公平取用歐盟各經濟部門所產出之資料，以及納入物聯網（IoT）互連裝置所產生資料的使用規定，塑造具競爭性的資料市場生態，以確保資料經濟的參與者在資料價值分配上的公平性，且聚焦於非個人資訊的數位資料上，除適用於對歐盟提供產品/服務之事業外，亦囊括可於歐盟境內取得資料之相關情況，並同時兼顧投資資料產品及服務之個人與事業的合法利益，其核心理念如下述：

本報告之智慧財產權歸屬於國發會

1. 近用性：使用人易於資料的取得。

2. 互通性：簡化資料處理服務供應商之間的轉換程序，制定一套防免非法傳輸的保護措施以及開發資料再利用的互通性標準。

3. 可攜性：強化個人與事業控制智慧型物件（smart objects）、機器及裝置所產出資料的量能，得以隨時在不同服務裝置之間切換，並自主選擇複製或傳輸資料，以及對連網產品（connected products）所產出資料的後續利用有知情同意權。

4. 開放機會：向以資料為主的新創產業提供發展機會。

5. 競爭性：鼓勵競爭性的資料經濟市場。

6. 公允性：確保在數位市場參與者之間的資料價值分配結果應公正。

基於上述意旨，針對資料共享所訂定之相關規範，可讓資料使用之相關條件與規則明確化，確保數位資料能順利由製造商/服務商流動至第三方（包含產品/服務使用者或售後服務提供者），提供參與資料經濟市場之誘因，創造資料之經濟價值；本法最終展望在降低維修成本並增加互通性、機敏資訊維護、公益用途及補償等願景，維持資料持有者與使用者之間的利益衡平：

1. 增加互通性來降低維修成本並取得維修權（right to repair）：該法允許使用者在不同雲端供應商之間任意轉換，讓使用者有更多資料的自主控制權，故其得向製造商請求提供或存取資料，並要求製造商與第三方共享資料（惟接收資料之第三方不得與守門人共享資料），此舉不但有利其挑選更具經濟且效率的維修及保養供應商（或決定自行維修），亦有助於激發售後服務的創新及優化，進而提供相類服務來與製造商公平競爭，例如在製造業層面，若接收由工業設備產生之資料，為

本報告之智慧財產權歸屬於國發會

製程的改善創造了機會，第三方便可利用資料，再結合 AI 技術分析，從而精進營運週期、生產線及供應鏈。

2. 機敏資訊維護：該法亦充分保障事業營業秘密與智慧財產，以及防範潛在商業間諜行為，倘若資料共享及使用發生適法上爭議，資料法亦提供爭端解決機制，若各會員國之主管機關不只一者時，各國應指定「資料協調員」（data coordinator）負責處理資料法適用爭議之單一窗口，以期維持製造商持續投入研發高品質的資料生成產品及服務。

3. 公益用途及補償：發生洪水、野火等自然災害、流行疾病、恐怖攻擊等緊急情況，若無法透過其他管道輕易取得必要資料時，公部門機構、執委會、歐洲中央銀行及歐盟機構有權逕自私部門取用其持有之資料，以快速做出決策應變並降低事業相關負擔，為此而構成特別犧牲之事業，亦有機會獲得合理補償，價額之核定將由執委會負責制定指引。

資料來源：

1. デジタル庁, 「オープンデータ基本指針」に係る意見募集の結果が公表されました, 2024-07-31, https://www.digital.go.jp/news/be176649-155c-4e12-b3af-a787939f54f6 (last visited 2024/08/14)

2. デジタル庁, 「オープンデータ基本指針」に係る意見募集を行います, 2024-02-13, https://www.digital.go.jp/news/7290df8a-ea84-4332-8cc0-1fe85e69b599 (last visited 2024/08/14)

3. デジタル庁, オープンデータ基本指針（改正案）改正履歴あり, 2024-02-13, https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/7290df8a-ea84-4332-8cc0-1fe85e69b599/fb0415d5/20240213_news_public_comments_draft_01.pdf (last visited 2024/08/14)

本報告之智慧財產權歸屬於國發會

(二)2024 年 3 月 5 日歐盟理事會批准《歐洲互通法》，改善歐盟跨部門的協作和資料交換，簡化公共服務的流程

為了創造歐盟能夠互通的數位公共網路環境，歐盟理事會（European Council）於 2024 年 3 月 5 日批准《歐洲互通法》（Interoperable Europe act），提高歐盟內各公共部門間之互通性水準和促進合作關係，加速歐盟公部門之數位轉型。

《歐洲互通法》旨在為歐盟之公共行政部門建立新的合作框架，確保無縫提供跨境服務及數位資料交換，簡化公民和事業申請服務之流程，推行促進創新、強化技能、知識交流之措施，創建共享且具互通性的生態系統，特別是透過設置「監理沙盒」（regulatory sandboxes），使歐盟公共管理部門之政策制定方向趨於一致。

該互通法案提出具體之措施包含以下重點內容：

1. 由「互通歐洲委員會」指導制定多層次治理框架，作為法制架構之核心。

2. 提倡具共享與重複使用可能的「互通性解決方案」，透過一站式的解決方案及共通合作為驅動，促進各會員國間之創新能力、技術升級與資訊交流。

3. 確保歐盟合作框架的規定，使會員國之公共管理部門共同合作。

4. 互通性評估的主要目標及條件應符合比例原則，避免對國家和地方行政部門產生行政負擔。

資料來源：

1. European Council, Interoperable Europe act: Council adopts new law for more efficient digital public services across the EU, 2024-03-04, https://www.consilium.europa.eu/en/press/press-releases/2024/03/04/interoperable-europe-act-council-adopts-new-

本報告之智慧財產權歸屬於國發會

law-for-more-efficient-digital-public-services-across-the-eu/ (last visited Mar. 22, 2024)

2. Digital Government, EU Council Adopts Interoperable Europe Act, 2024-03-06, https://www.nldigitalgovernment.nl/news/eu-council-adopts-interoperable-europe-act/ (last visited 2024/03/22)

3. EU Debates, News & Opinions, The Interoperable Europe Act will improve online public services for people and businesses, 2023-11-14, https://www.pubaffairsbruxelles.eu/eu-institution-news/the-interoperable-europe-act-will-improve-online-public-services-for-people-and-businesses/ (last visited 2024/03/22)

(三)2024 年 3 月 15 日歐洲議會與歐盟理事會達成關於歐洲健康資料空間之臨時政治協議

歐洲議會（European Parliament）與歐盟理事會達成關於歐洲健康資料空間（European Health Data Space, EHDS）之臨時政治協議。該協議將建立歐洲健康資料空間之框架，以方便民眾跨國存取個人健康資料，並促進資料安全共享之公共利益；讓病患得於歐盟不同的醫療保健系統以電子方式存取其個人醫療資料，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，並對敏感資料的共享方式和目的提供強而有力的隱私保護，以下就該協議之三項主要目標簡述之：

1. 病患得以電子方式存取其個人醫療資料：

病患透過歐洲健康資料空間，即使於歐盟不同的醫療保健系統，仍能存取其個人健康資料，包含病歷摘要、電子處方、醫學影像及實驗室結果，此外，各國將建立國家健康資料存取之服務，制定歐洲電子健康資料共享格式、品質、安全性之互通性規範。

2. 為公共利益目的共享資料之保障：

本報告之智慧財產權歸屬於國發會

EHDS 允許基於公共利益目的共享匿名或化名的健康資料，包括健康記錄、臨床試驗、病原體、基因、健康登記以及有關醫療資源的資訊。此一資料共享限於進行研究、創新、政策制定、教育和病患安全等公益範疇，禁止出於廣告或評估保險目的而共享資料。

3. 強化機敏性資料的保障：

賦予病患對如何使用、近用資料擁有發言權。近用資料時必須通知病患，病患有權利要求更正違誤資訊，且患者有權利拒絕醫療專業人員取得其資料，除非基於保護資料當事人或其他人重要利益之目的，則應使公民能夠自主控制個人健康資料。

資料來源：

1. European Parliament, EU Health Data Space to support patients and research, 2024-03-15,https://www.europarl.europa.eu/news/en/press-room/20240304IPR18765/eu-health-data-space-to-support-patients-and-research (last visited 2024/03/15)

(四)2024 年 3 月 19 日歐盟宣布將資助歐洲共同行動資料空間部署計畫（Deploy EMDS），逐步實現歐洲共同資料空間效益

歐盟依據 2020 年發布「歐洲資料戰略」（European Data Strategy），為達成建立「歐洲共同資料空間」（Common European data space）之目標，於 2023 年 11 月啟動歐洲共同行動資料空間部署計畫（Deploy EMDS），該計畫為期三年，將持續至 2026 年 10 月底。

2024 年 3 月 19 日宣布將投入資源，支持 9 個城市和地區之實施工作，展現資料空間如何用於解決城市問題，及其所發揮之正面效益，該計畫預計至 2026 年 10 月結束。

本報告之智慧財產權歸屬於國發會

Deploy EMDS 計畫有助於發揮資料之潛力，推動永續、高效率之城市交通發展，其目的在實現資料之共享及促進重複利用，故此計畫將部署一個可操作之資料空間同時建構一個一般性的監管架構。2024 年 3 月宣布將以歐盟資金投入，支持 9 個城市及地區發展 20 項涉及交通管理、資料驅動政策制定以及多式聯運（multimodal mobility）之利用案例，以促進創新服務之開發與應用，並可推動改善當地交通之政策，參與之相關城市包含巴塞隆納、米蘭、斯德哥爾摩等。例如，斯德哥爾摩關注於主要道路之空氣品質與其是否合於標準，運用歐洲共同行動資料空間，改善溫室氣體之排放及測量空氣品質，對低排放區域之空氣品質實行數位監控；布達佩斯關注確保行動不便者之無障礙環境，在城市公共交通應用程式彙整各個共享交通營運商之資料，轉型為當前之路線規劃服務。

綜上，每個城市依據所面對之獨特挑戰和困難，皆透過歐洲共同行動資料空間之運用，協助制定並推動解決策略，讓相關問題實際取得改善之效果，彰顯歐洲共同行動資料空間發揮促進轉型之潛力，以及如何滿足城市之需求。

資料來源：

1. European Commission, DeployEMDS, the common European mobility data space starts to become reality, 2024-03-19, https://digital-strategy.ec.europa.eu/en/news/deployemds-common-european-mobility-data-space-starts-become-reality (last visited 2024/03/25)

二、 英國

(一)2024 年 3 月 12 日英國資訊委員辦公室就事業資料戰略（EDS）截止公眾諮詢

本報告之智慧財產權歸屬於國發會

英國資訊委員辦公室（Information Commissioner's Office, ICO）於2024年3月12日就事業資料戰略（Enterprise Data Strategy, EDS）草案截止公眾諮詢，預計將於5月24日正式發布，使ICO成為利用資料進行創新之指標機關，運用資料強化對社會之影響力，並以此戰略指導ICO及適用之事業或組織所有之作為並加速轉型。

ICO預計將於5月24日正式發布「事業資料戰略」，說明將如何利用資料為事業、監管及策略優先事項提供資訊及指導，目的在達成以下3項目標：

1. 為ICO與其客戶創造資料的實際價值。

2. 改善員工對組織資料能力之體驗。

3. 顯著提高資料之成熟度。

為了實現資料目標和願景，本策略草案針對 10 個能力領域提出資料成熟度量表,確定以下5個強化投入之戰略能力及四項治理原則，其中 5 個戰略能力包含 1.資料營運和傳輸模式（Data operating and delivery model）2.資料治理和資料品質（Data Governance and Data Quality）3.資料治理的文化及智識（Data Culture and Literacy）4.資料處理技能和專業技能（Data Skills and Professionals）5.資料、分析和機器學習技術平臺（Data, Analytics and Machine Learning (ML) Technology Platform）。

關於治理之原則涵蓋以下四項，以下簡述四項原則之意義：

1. 民主化（democratise）

   於內部及外部適當地共享資料，提升所有人員之資料素養，創造資料專業人員有價值的職業生涯。

2. 尊重人權（dignify）

本報告之智慧財產權歸屬於國發會

確保機關使用資料不會剝奪人民的資料控制權。同時透過智慧自動化（intelligent automation）之發展，幫助職員進行最有價值的工作，重新塑造提供服務的方式。

3. 規範嚴謹（disciplined）

確保資料的高品質、結構化及可用性，及對資料之風險採取合理的控制措施。

4. 勇於突破（daring）

鼓勵利用資料進行創新活動，突破固有之發展方向。

ICO 將進一步進行關鍵措施之實現規劃，例如，開發資料營運模型，羅列實現願景所需的人員、流程和技術，擴大資料團隊，確保擁有充足之人員和技能推動策略的實施；在精簡的管理框架下，實施並整合清晰、易用的資料政策，保護資料的完整性，確保機關使用資料不會剝奪人民的資料控制權。同時透過智慧自動化（intelligent automation）之發展，幫助職員進行最有價值的工作，重新塑造服務提供的方式。從而在整個組織內提高資料品質並採行有助一致性提升之重要措施。

資料來源：

1. Information Commissioner's Office, ICO consultation on the Enterprise Data Strategy, 2024-03-12, https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-enterprise-data-strategy/ (last visited 2024/03/21)
2. Information Commissioner's Office, ICO Enterprise Data Strategy: Foreword and introduction, 2024-01-30, https://ico.org.uk/about-the-ico/ico-enterprise-data-strategy/ (last visited 2024/03/21)

本報告之智慧財產權歸屬於國發會

三、美國

(一)2024 年 3 月 28 日美國副總統 Harris 女士宣布改良 AI 治理、創新和風險控管的新政策

美國副總統 Harris 女士於 2024 年 3 月 28 日宣布美國行政管理及預算局（Office of Management and Budget, OMB）將根據《AI 權利法案藍圖》（Blueprint for an AI Bill of Rights）與《AI 風險管理框架》（AI Risk Management Framework），並回應 2023 年 10 月美國總統 Biden 先生針對 AI 管理政策之 150 日行政命令，發布首項政府端政策。當中除了提及與各部會積極在 AI 的安全管理與創新之外，亦提及政府各機關部門應對政府所擁有之資料，包含 AI 代碼（code）與模型（model）進行開源、與大眾分享等治理操作。

此政策包含以下幾個關鍵原則：

1. 管理 AI 的使用風險：聯邦機構在使用可能影響美國公民權利或安全的 AI 時，必須實施具體的保障措施，評估、測試和監控 AI 對公眾的影響。

2. 提升 AI 使用透明度：此政策要求聯邦機構提高在使用 AI 時的公眾透明度，例如：

   (1) 公告年度 AI 使用案例清單，包括列舉有危及權利或安全的案例以及風險應對措施。

   (2) 在不對公眾或政府運營造成風險的前提下，發布政府擁有的 AI 代碼、模型和數據。

3. 推動有責的 AI 創新：確立組織實驗 AI 的有責性、需設置適當的安全措施，並協助面對當代的社會危機，例如天災、公共衛生、公共安全等。

4. AI 人才培育：引導組織擴大徵才和培養 AI 專才。

本報告之智慧財產權歸屬於國發會

5. 加強 AI 治理：要求聯邦組織對 AI 使用設置專責單位領導及監督。

資料來源：

1. The White House, FACT SHEET: Vice President Harris Announces OMB Policy to Advance Governance, Innovation, and Risk Management in Federal Agencies' Use of Artificial Intelligence, 2024-03-28, https://www.whitehouse.gov/briefing-room/statements-releases/2024/03/28/fact-sheet-vice-president-harris-announces-omb-policy-to-advance-governance-innovation-and-risk-management-in-federal-agencies-use-of-artificial-intelligence/ (Last visited 2024/04/10)

四、 聯合國

(一)2024 年 3 月 11 日聯合國世界糧食計畫署發布 2024-2026 年全球資料戰略，打造世界級資料生態系統

全球各地正在面對糧食危機、區域衝突、氣候變遷和經濟動盪的巨大挑戰，聯合國世界糧食計畫署（World Food Programme, WFP）必須充分利用資料的力量採取行動，有效管理資料、知識和分析工具，賦予組織更智慧高效的工作流程，確保有限之資源投入於最急迫的需求上，以縮短救援之時間。該組織於 2024 年 3 月 11 日發布 2024-2026 年全球資料戰略（WFP Global Data Strategy 2024-2026），本資料戰略之目的在調整現有規範，促進紀律執行迅速產出成果，提升營運效率與影響力，建立世界一流的資料生態系統，評估資料治理的成熟度，利用資料資產之價值，充分發揮資料的潛力，推動尖端解決方案，消除糧食不安全之困境，加速實現無飢餓世界的願景之核心目標。

本策略由構築一個健全的資料生態系統出發，擬定四大目標於 2026 年達成：

本報告之智慧財產權歸屬於國發會

1. 具備目的與證據之成果交付（Delivering with intent and evidence），促進數位價值鏈最大化。

2. 架構最佳的資料服務（Architecting best of class data services），投資於正確數據與分析之基礎建設。

3. 建構具備效能及效率的資料基礎（Effective and efficient data foundations），透過資料管理及資料治理整體管理糧食計畫署之資料資產。

4. 負責的為人民賦能（Responsibly empowering people），開發以資料為核心之勞動力與文化。

為落實全球資料戰略，WFP 認為應該建立糧食署的資料生態系統，以糧食署之現代資料資產（Modern Data Estate）為核心，將資料生態系統延伸至與糧食署合作之夥伴、聯合國大家庭、獲得糧食署援助之人民、以及其他公眾間之資料及資訊交換。對資料共享開放、並促進資訊系統互通之能力的需求，凸顯了糧食署優先評估與採行資料關措施以建立資現代化資料資產之必要性。

至於 WEP 概念下的現代化資料資產，對於創造資料價值具有高度重要性，主要概念係以資料資產為核心，強化資料基礎（Data foundation）、確保資料來源(Data sources)、發展自動分析能力(Self-service analytics)、優化 AI 資料利用(Artificial Intelligence and Machine Learning layer)。整體而言希望能夠達到「一次構建，多次使用」（build once, use many times）之目標。

此外，WEP 將採用全球資料之軸幅運作模式（Global Data Hub and Spoke model），建立一個全球資料中心之模型，透過資料驅動之人員投入、文化及流程建構以創造價值，從而建立問責機制並促進合作。

於人員能力的部分，須致力於提升人員之資料素養（data skills and knowledge），建構資料素養能力框架（Data Literacy Competency

本報告之智慧財產權歸屬於國發會

Framework），提供培訓課程予 WEP 之工作人員及合作夥伴，使工作人員能夠對資料提出正確的問題，累積知識，推動決策，並與他人交流。

綜上所述，WFP 將開始執行 2024-2026 年全球資料策略，並每年定期進行成效評估，確保組織之資料治理能力日趨成熟，實現零飢餓世界之終極目標。

資料來源：

1. World Food Programme, WFP Global Data Strategy 2024–2026, 2024-03-27, https://www.wfp.org/publications/wfp-global-data-strategy-2024-2026 (last visited 2024/03/14)

貳、AI 法制政策

一、歐盟

(一)2024 年 1 月 24 日歐盟 2024 年上半年將推動《人工智慧公約》，蒐集並公布「事業領頭羊因應人工智慧法的法遵作法」

歐盟將於 2024 年上半年召集有意願的各方討論「如何推動《人工智慧公約（AI Pact）》」，目的為促進事業盡早適應《人工智慧法案》(參下述(二))通過可預見的要求並儘早且自願實施相關作為。歐盟執委會先前已就此一公約，於 2023 年 11 月向願意積極參與人工智慧公約的組織發起意願徵集（call for interest）。

《人工智慧公約》是一個促進事業儘早採取措施以落實人工智慧法案要求之計畫，具體而言係鼓勵歐盟及非歐盟的各領域產業領頭羊自願地承諾（pledge）及分享，各事業為遵循法規，正在實施或預計實施的流程、作法，並確保事業 AI 的設計、研發及使用是可信賴的。

本報告之智慧財產權歸屬於國發會

歐盟執委會將蒐集、公布前述事業所分享的「承諾」，除提高參與事業之知名度與可信賴度外，並可形成產業對《人工智慧法案》因應作法之共識，如制定內部流程、人員培訓或採用 AI 自我審查系統（self-assess AI systems）等，提升 AI 應用的可信度，並建立外界對事業研發 AI 技術的信任。

歐盟執委會將於《人工智慧法案》正式通過後啟動《人工智慧公約》，邀請產業領頭羊做出首份公開承諾。

資料來源：

1. European Commission, AI Pact, 2024-03-06, https://digital-strategy.ec.europa.eu/en/policies/ai-pact?fbclid=IwAR2-xM_Dz3tesiyVduKCdMMd40DC5jL3DUVfVmjMycO8cGrnX0DgRDQYxfQ (last visited 2024/04/19)

(二)2024 年 3 月 13 日歐洲議會通過《人工智慧法》，規範 AI 的風險評估、研發獎勵及資訊透明度

為了促進 AI 創新的同時，也透過對健康、安全、基本權利及環境的高標準保護，防止 AI 系統的負面影響，歐洲議會（European Parliament）於 2024 年 3 月 13 日通過《人工智慧法》（Artificial Intelligence Act）。預計歐盟 27 國將於 2024 年 4 月正式批准《人工智慧法》，預計將於 2024 年 5 月至 6 月於歐盟官方公報（EU Official Journal）公布。人工智慧法將於公布 20 天後生效，除例外規定適用日期者外，其餘條文將於公布 24 個月後全面適用。例外規定適用日期者，如：「違反人工智慧法的處罰規定」將於生效日起算 6 個月後適用；「行為準則（codes of practice）」則將於生效日起算 9 個月後適用；「一般用途型 AI（General-purpose AI, GPAI）」規則及義務，將於生效日起算 12 個月後適用。所謂一般用途型 AI 也可稱為「基礎模型」。

本次通過條文重點諸如：

本報告之智慧財產權歸屬於國發會

1. 禁止將 AI 應用於影響公民權利的行為以及責任豁免的例外

2. 高風險 AI 的範圍及其義務

3. 一般用途型 AI 的透明度要求

4. 對中小事業的支援措施

摘要說明如下：

1. 禁止 AI 應用於影響公民權利的行為

人工智慧法禁止「影響公民權利的 AI 應用」，包括：分析種族、政治立場、宗教信仰或性傾向及以敏感特徵為基礎之生物特徵辨識 AI 系統；從網路或監視器蒐集不特定對象的臉部畫面，用以研發人臉辨識資料庫；在工作場所或學校進行情緒辨識、社會評分；根據個人或生物特徵進行預測性警察行政（predictive policing）。法案也禁止在公共空間進行即時臉部辨識，但執法單位（警方）如果取得司法或行政單位之事前授權，可以於刑事案件中使用生物特徵識別系統（RBI）。

違反同法第 5 條者，依同法第 99 條第 3 項規定，依違反類型、事業規模而定，處以 3,500 萬歐元（約台幣 12 億元），或事業全球年營收 7%的罰鍰，以較高者為準。若為違反同法第 5 條以外規定，依同法第 99 條第 4 項規定，依違反類型、事業規模而定，處以 1500 萬歐元或事業全球年營收 3%的罰鍰，以較高者為準。

2. 高風險 AI 的範圍及其義務

高風險 AI，高風險 AI 用途的例子，包括關鍵基礎設施（如交通）、教育和職業培訓、就業、基本私人和公共服務（如醫療保健、銀行業）、可影響人民基本權之執法（如用以評估證據證明力）、移民及邊境管制（如確認旅行證明文件是否真

本報告之智慧財產權歸屬於國發會

實的系統）、司法和民主進程所使用之系統（例如選舉投票系統）等。如果 AI 工具僅用於協助法官決斷或行政作業時，則非屬於高風險。

由於高風險 AI 對健康、基本權、環境及民主影響重大，高風險 AI 的提供者須針對 AI 執行風險評估，並確保產品符合法規方能將產品上市。

3. 一般用途型 AI 的透明度要求

一般用途型 AI 系統及其模型須滿足透明度的義務要求，包含符合歐盟著作權法及發布其訓練資料的詳細摘要。如風險更高的一般用途型 AI 模型需另執行風險評估、風險回報機制。此外，經 AI 深偽（deepfakes）技術處理的圖片、聲音、影片內容，則須明確標記（label）。

4. 對中小事業的支援措施

應建置國家層級的監理沙盒及現實世界的測試場域，有助於中小事業、新創公司推出創新的 AI 前，透過沙盒研發及訓練 AI。

資料來源：

1. European Parliament, Artificial Intelligence Act: MEPs adopt landmark law, 2024-03-13, https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law (last visited 2024/03/14)

2. European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), Texts adopted - Artificial Intelligence Act - Wednesday, 13 March 2024

本報告之智慧財產權歸屬於國發會

(europa.eu) (last visited 2024/03/14)

3. European Commission, AI Act, 2024-03-06, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (last visited 2024/03/14)

4. CNBC, World's first major act to regulate AI passed by European lawmakers, 2024-03-13, https://www.cnbc.com/2024/03/13/european-lawmakers-endorse-worlds-first-major-act-to-regulate-ai.html (last visited 2024/03/14)

二、英國

(一)2024 年 3 月 18 日英國發布 2024-2030 數位發展戰略，建構以性別平等、區域均衡、數位公共基礎建設為核心之 AI 監管框架

英國外交、聯邦事務暨發展部（Foreign, Commonwealth and Development Office, FCDO）於 2024 年 3 月 18 日發布「2024-2030 數位發展戰略」，旨於實現 4 個核心目標：

1. 數位轉型：透過數位科技促進經濟、政府及社會發展。

2. 數位包容：協助中低所得國家消弭數位落差。

3. 數位責任：建置安全、可靠且具韌性的數位環境。

4. 數位永續：透過數位科技推動氣候變遷與環境目標。

為達上開目標，2024-2030 數位發展戰略強調英國將優先發展 4 領域的數位科技：

1. 最後一哩路

確保偏遠、低收入地區可連接數位科技。2030 年之前，英國預計至少支援 20 個合作國家減少其 50%的數位落差。

本報告之智慧財產權歸屬於國發會

2. 數位公共基礎建設（digital public infrastructure, DPI）

DPI 如數位政府與國家支付系統（national payment system）為推動政府與私部門數位轉型的關鍵。2030 年之前，英國預計透過改善 DPI 角度，至少支援 20 個合作國家由國家層面推動數位服務。

3. 人工智慧

AI 伴隨的機會與風險，AI 對發展中國家的衝擊更高。2030 年之前，英國預計於非洲設立至少 8 個負責任的 AI 實驗室，並協助訂定負責任的 AI 監管框架。

4. 提供性別平權的數位教育

為改善性別數位落差，2030 年之前，英國預計支援至少 5 千萬名婦女及女童安全且有意義地參與數位世界。

資料來源：

1. GOV.UK, Digital development strategy 2024 to 2030, 2024-03-18, https://www.gov.uk/government/publications/digital-development-strategy-2024-to-2030 (last visited 2024/03/20)
2. UK International and development, Digital development strategy 2024 to 2030, 2024-03-24, https://assets.publishing.service.gov.uk/media/65f45adf8112250011579f3f/FCDO-Digital-Development-Strategy-2024-2030.pdf, 6-7 (last visited 2024/03/20)
3. GOV.UK, New UK strategy aims to improve lives through digital technology, 2024-03-18, https://www.gov.uk/government/news/new-uk-strategy-aims-to-improve-lives-through-digital-technology (last visited 2024/03/20)

本報告之智慧財產權歸屬於國發會

三、美國

(一)2024 年 2 月 21 日美國國家電信暨資訊管理局針對 AI 的「雙重用途的基礎模型」(dual-use foundation models)之問題進行公眾諮詢

2023 年 10 月 30 日美國總統拜登提出關於「研發與使用安全、可靠、可信賴的 AI」的行政命令(Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence),要求公私部門推進 AI 發展並管理 AI 風險。因此,隸屬於美國商務部的國家電信暨資訊管理局(National Telecommunications and Information Administration, NTIA)於 2024 年 2 月 21 日就 AI 領域的監管框架,提出「雙重用途的基礎模型(dual-use foundation model)」的一系列問題,公告徵詢意見 30 天。NTIA 將評估所獲取之徵詢意見,與商務部長、州務卿合作,準備一份提交給總統的報告,該報告可能會提供與雙重用途的基礎模型有關的具體政策及監管策略。

所謂「雙重用途的基礎模型」,依上開行政命令之定義,係指 AI 模型可以進行自我監督之學習(self-supervision),其學習過程須至少經過資料庫中數百億個參數,且適用領域廣泛。

關於「雙重用途的基礎模型」之徵詢問題,摘要說明如下:

1. 於思考基礎模型或模型權重時,NTIA 應如何定義「開放(open)」或「廣泛可用性(widely available)」?
2. 如何比較「具廣泛可用性的基礎模型權重」與「非公開模型權重」的風險?
3. 與全封閉模型相比,具有廣泛可用性的基礎模型權重有哪些優點?

本報告之智慧財產權歸屬於國發會

4. 開放基礎模型是否尚有其他之相關元素，若同時廣泛使用，是否可能改變廣泛可用性基礎模型的權重以及可能帶來的風險或效益？

5. 於管理風險以及擴大具備廣泛可用性基礎模型之雙重用途基礎模型之效益時，會涉及那些安全或更廣泛的技術層面問題？

6. 與開放基礎模型相關之法律或產業議題為何？

7. 目前或潛在的自願、美國監管及國際機制管理 AI 風險的作法，以及如何將「具廣泛可用權重的基礎模型」的優勢最大化？何種事業組織（entities）應發揮領導作用以及治理性成果？

8. 面對不斷變化的技術，考慮到不可預見的風險及利益，政府、公司及個人應如何就未來有用的開放基礎模型做出決策或計畫？

9. 於分析具備廣泛可用性基礎模型權重之雙重用途基礎模型的風險及效益時，有無其他需考慮之其他問題、主題或進步的技術？

資料來源：

1. National Telecommunications and Information Administration, Dual Use Foundation Artificial Intelligence Models with Widely Available Model Weights, 2024-02-21, https://www.ntia.doc.gov/federal-register-notice/2024/dual-use-foundation-artificial-intelligence-models-widely-available (last visited 2024/02/29)

本報告之智慧財產權歸屬於國發會

(二)2024 年 3 月 13 日美國猶他州發布《猶他州人工智慧政策法案》（Utah Artificial Intelligence Policy Act, UAIP）

美國猶他州立法機關於 2024 年 3 月 13 日發布《猶他州人工智慧政策法案》（Utah Artificial Intelligence Policy Act, UAIP），將於 2024 年 5 月 1 日生效，該法案對「向客戶使用生成式人工智慧工具的事業組織」課予揭露義務，並限制組織將違反消費者保護義務之言論或行為效果歸責於生成式 AI，以下為 UAIP 之四項重要規範內容：

1. 生成式 AI 之定義

UAIP 僅規範涉及生成式 AI 之管制，其定義為經過資料訓練，使用文字、音訊或影片與人互動，在有限程度甚至無人操控的情況下，能夠產製類似於人類精神創作成果的 AI 系統。

2. 揭露義務

指從事「受管制職業」（regulated occupations）的人民，也就是必須取得許可或國家證書方可從事的職業，必須明顯於任何通訊開始進行時明確向消費者揭露其正在與生成 AI 進行互動。非從事「受管制職業」之人民，但受猶他州消費者保護法所拘束者，若經消費者提出請求，則必須明確揭露生成式 AI 的使用情況。

3. 事業應對生成式 AI 之產出負責

違反猶他州消費者保護法之事業，無法以係 AI 工具所生成的不當言論及不法行為進行抗辯，或以其作為不法量能之積累為由主張責任豁免，事業應對生成式 AI 之產出負責。

4. 罰則

猶他州消費者保護部（Utah Division of Consumer Protection, UDCP）得對每次違法行為處以最高 2,500 美元的

本報告之智慧財產權歸屬於國發會

罰鍰，並且法院有權在由 UDCP 提起的訴訟處以罰鍰，及禁止非法活動並命令返還因違反 UAIP 所生的不法利益。

資料來源：

1. UTAH STATE LEGISLATURE, ARTIFICIAL INTELLIGENCE AMENDMENTS, 2024-03-13, https://le.utah.gov/~2024/bills/static/SB0149.html (last visited 2024/04/11)
2. JDSUPRA, Utah Becomes First State To Enact AI-Centric Consumer Protection Law, 2024-02-27, https://www.jdsupra.com/legalnews/utah-becomes-first-state-to-enact-ai-2635614/ (last visited 2024/04/11)

(三)2024 年 3 月 15 日美國食品及藥物管理局（FDA）發布人工智慧與醫療的政策文件

美國食品及藥物管理局（Food and Drug Administration，FDA）於 2024 年 3 月 15 日發布「AI 與醫療產品：生物製劑評估暨研究中心、藥物評估暨研究中心、醫療裝置與放射衛生中心、複合式產品辦公室合作政策文件（Artificial Intelligence & Medical Products: How CBER, CDER, CDRH, and OCP are Working Together），簡稱「AI 與醫療產品政策文件」)」，旨於回應美國總統 Biden 先生在 2023 年 10 月 30 日簽署首個關於推動「安全且可信任 AI」之第 14110 號行政命令，該行政命令指示美國衛生及公共服務部（U.S. Department of Health and Human Services, HHS）應制定戰略計畫，範圍包括「藥物及醫療器材安全」、「公共衛生」等。

本次 AI 與醫療產品政策文件，概述監管 AI 的 4 面向：

1. 與利害關係人建立合作關係，推動教育倡議

本報告之智慧財產權歸屬於國發會

FDA 將與 AI 研發人員、病患團體、國際監管機構及國際標準組織等利害關係人建立合作夥伴關係，諮詢 AI 之透明度、可解釋性、歧視、資安及品質控管，以制定「病患為本」之 AI 監管模式。同時推動教育倡議（educational initiatives），以使產業相關利害關係人於研發或使用醫療產品時，引導其安全且負責任的使用 AI。

2. 制定監管政策以推動創新

監控及評估趨勢及議題，以即時調整 AI 於醫療產品生命週期之應用。發布研發及使用 AI 相關醫療產品的指引，包括但不限於：

(1) 「關於『異動人工智慧設備的軟體功能控制計畫的上市送件審查建議」最終指引（Final guidance on marketing submission recommendations for predetermined change control plans for AI-enabled device software functions）。

(2) 關於 AI 設備軟體功能「生命週期管理」注意事項及「上市前送件審查建議」指引草案（Draft guidance on life cycle management considerations and premarket submission recommendations for AI-enabled device software functions）。

(3) 應用 AI 以支援藥物及生物製劑的監管決策指引草案（Draft guidance on considerations for the use of AI to support regulatory decision-making for drugs and biological products）。

3. 促進制定統一的標準、規範、作法及工具

FDA 預計以 2021 年 10 月由 FDA、加拿大衛生部、英國藥物及保健產品管理局（Medicines and Healthcare Products Regulatory Agency, MHRA）共同制定之「指導原則（Guiding Principles）」為基礎，進一步完善 AI 生命週期的評估因素，

本報告之智慧財產權歸屬於國發會

比如：資訊安全、確保訓練資料可用，以及研發 AI 工具的品質保證框架。

4. 支持與 AI 功能評估或監控相關研究

研究包括對於應用 AI 之醫療產品安全性及有效性評估等。

資料來源：

1. FDA, Artificial Intelligence & Medical Products: How CBER, CDER, CDRH, and OCP are Working Together, 2024-03, https://www.fda.gov/media/177030/download?attachment (last visited 2024/03/28)
2. FDA Publishes White Paper on Artificial Intelligence & Medical Products, 2024-03-26, https://www.jdsupra.com/legalnews/fda-publishes-white-paper-on-artificial-9869915/?origin=CEG&utm_source=CEG&utm_medium=email&utm_campaign=CustomEmailDigest&utm_term=jds-article&utm_content=article-link (last visited 2024/03/28)

(四)2024 年 3 月 21 日美國眾議院議員和 AI 工作小組提出《保護消費者免受人工智慧欺騙法草案》（Protecting Consumers from Deceptive AI Act）

考量現今 Deepfakes（深偽技術）已造成眾多社會問題，包括對消費者之欺騙、國家安全之威脅、市場秩序混亂、對未成年人之傷害等社會問題及威脅，因此，美國眾議院議員和 AI 工作小組於 2024 年 3 月 21 日提出《保護消費者免受人工智慧欺騙法草案》（Protecting Consumers from Deceptive AI Act），旨在藉由制定識別及標記 AI 生成內容的標準，並要求 AI 生成軟體開發商及平臺揭露 AI 所生成的內容，以解決上述社會問題。

本報告之智慧財產權歸屬於國發會

具體而言，《保護消費者免受人工智慧欺騙法草案》將推動以下四項重點措施，保護人民免於深偽技術等 AI 技術運用形成之欺騙：

1. 指導國家標準與技術研究院（NIST）推動制定識別及標記 AI 生成內容的標準，包括透過針對出處之詮釋資料（metadata）、浮水印（watermarking）和數位指紋（digital fingerprinting）等技術措施。

2. 要求生成式 AI 開發者在其 AI 應用所生成的音訊或影片內容中包含機器可判讀的揭露資訊，並允許使用者得選擇讓前述資訊中包含具備額外資訊的詮釋資料（metadata）。

3. 要求平臺使用揭露資訊以標記 AI 生成的內容。

4. 本規範以多家具領導地位之 AI 公司於去年(2023 年)所作出之承諾以及專家與全球利害關係人所為之努力為基礎。

資料來源：

1. CONGRESS.GOV, H.R.7766 - Protecting Consumers from Deceptive AI Act, 2024-03-21, https://www.congress.gov/bill/118th-congress/house-bill/7766/text/ih?overview=closed&format=txt (last visited 2024/04/11)

2. Congresswoman Anna G. Eshoo, U.S. Congresswoman Anna G. Eshoo (CA-16), Co-Chair of the House AI Caucus, and U.S. Congressman Neal Dunn (FL-2), both members of the bipartisan Task Force on Artificial Intelligence, today introduced the Protecting Consumers from Deceptive AI Act., 2024-02-27, https://www.psnews.co.kr/news/articleView.html?idxno=2048196 (last visited 2024/04/11)

3. eshoo.house.gov, the Protecting Consumers from Deceptive AI Act, 2024-03-21, https://eshoo.house.gov/media/press-releases/rep-eshoo-introduces-bipartisan-bill-label-deepfakes (last visited 2024/04/11)

本報告之智慧財產權歸屬於國發會

四、 新加坡

(一)2024 年 1 月 16 日新加坡政府提出「生成式人工智慧治理架構草案」，內容涵蓋究責、數據、通報等 9 大方面

依據新加坡資訊通信媒體發展局(IMDA)及「人工智慧驗證基金會（AI Verify Foundation）」本（2024）年 1 月 16 日聯合發布的新聞稿指出，新加坡政府預計於 2024 年年中推出「生成式人工智慧（Generative AI）治理架構」，並就草案內容徵求海內外專家意見，致力於打造可信賴的 AI 環境。此次提出之 AI 治理架構草案，乃是以 2019 年新加坡所推出之全球第一個 AI 治理架構為參考之基礎，惟舊版架構並未考量生成式 AI 之發展與應用。

本次治理架構草案，內容涵蓋究責、數據、開發與運用、通報、測試、安全、內容來源、研究及公共利益等 9 大面向，並將著重於建立指導原則及識別重點，為全球第一個針對生成式 AI 的多面向治理架構。

生成式 AI 的開發過程將涉及各類業者，因此須制定明確之問責機制。上述治理架構草案建議，應由模型開發者負責協調，以每個利害關係人於生成式 AI 開發鏈中之控制程度等關聯，進行責任的分配，以確保每項環節參與者或利害關係人承擔應有的責任。此外，資料為促進 AI 模型或應用程式開發之核心元素，驅動生成式 AI 開發之數據對最終成果之品質具有極大影響，業者須使用可信賴的「數據集（dataset)」，以維護個人隱私及著作權。

治理架構草案主張對於生成式 AI 的開發及運用，可借鏡食品的「營養標籤（Food Labels）」機制，針對不同之 AI「模型（models)」貼上標籤，明確列出開發過程中使用的數據及測試等重要資訊。「模型」

本報告之智慧財產權歸屬於國發會

係指 ChatGPT、DALL-E 等不同之生成式 AI 系統。由於任何系統皆可能出現漏洞，該治理架構草案亦提出關於舉報、測試及安全等機制。

為防止生成式 AI 被用於傳播虛假訊息，多國政府正探討使用「數位浮水印」及「密碼溯源」等兩種標記科技，標示可信賴或原創內容，以協助用戶辨識內容來源及生成方式。

資料來源：

1. Infocomm Media Development Authority, Singapore proposes framework to foster trusted Generative AI development, 2024-01-16, https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2024/public-consult-model-ai-governance-framework-genai (last visited 2024/04/18)

五、 聯合國

(一)2024 年 2 月 28 日世界智慧財產權組織（WIPO)公告《生成式 AI：智慧財產權指引》

世界智慧財產權組織(World Intellectual Property Organization，WIPO)於 2 月 28 日公告《生成式 AI：智慧財產權指引》(Generative AI: Navigating Intellectual Property)。該指引旨在幫助產業釐清利用生成式 AI 可能產生之智慧財產權風險，並提出緩解保障措施以降低潛在危害。

盤點現行生成式 AI 對產業之影響，需考量包含 AI 之訓練及輸出在內之各個面向，大致可包含：

1. 機密資訊保護

機密資訊中包含商業機密，為潛在具有經濟價值及競爭優勢之資訊。如使用生成式 AI 訓練很可能會導致商業機敏資訊被無意中洩漏，對於資料存取應盡量考慮存放於私有雲、

本報告之智慧財產權歸屬於國發會

檢測監控 AI 提供者之保護或保證、限制存取權限之管控以及考量新增資安專家審查與監控生成式 AI 訓練狀況。

2. 智慧財產權侵權

目前生成式 AI 所訓練之資料，很多係以受智慧財產權保護之作品進行訓練。現階段主要糾紛集中在著作權及商標權之侵權爭議。但隨著科技發展，亦逐步擴及至工業設計及專利發明等領域。然由於現行各國對生成式 AI 之法令規範仍存在很大之不確定性，故產業應考量使用未侵權之智慧財產權，或以合約約定侵權賠償之範圍，保留模型訓練記錄，減少出現第三方公司名稱、商標及著作。

3. 開源義務

開源軟體向公眾開放並可自由使用，但應注意是否附隨需遵守義務之風險，如資料歸屬、風險收益等隱藏危害。

4. Deep Fakes 之肖像權及聲音權

Deep Fakes 最常運用於肖像及聲音，其權利之保護並非各國都規範於智慧財產權，其可能包含於人權、形象權乃至於憲法基本權，故取得原權利人授權同意使用為產業應注意重點。

5. 人工智慧產出之智慧財產權及所有權

目前尚無生成式 AI 所生成之新內容是否受到智慧財產權保護之相關立法，然即使 AI 輸出不受智慧財產權保護，也可以透過合約明定所有權，盡可能在未侵害智慧財產權利的前提下使用生成式 AI 產出內容，如內部使用、創意生成個人社交媒體文章等。

本報告之智慧財產權歸屬於國發會

於智慧財產權而言，生成式 AI 衝擊最廣的莫過於著作權保護，然對於生成式 AI 是否享有智慧財產權利、是否應進行監管等依舊存在不確定性，僅部分國家有司法判決提供參考標準。WIPO 此次指引，除羅列侵權面向之解決措施外，尚從內部規範、事前存儲安全、偵測工具狀態等生成式 AI 可能影響智慧財產權益之層次，提供產業遵循的指引，以利其在法令尚未明確權利歸屬之情況下，保護自身利用過程的適法性。

資料來源：

1. WIPO, Generative AI: Navigating Intellectual Property, 2024-04-10, https://www.wipo.int/about-ip/en/frontier_technologies/news/2024/news_0002.html (last visited 2024/04/19)

(二)2024 年 3 月 21 日聯合國通過首個與人工智慧相關的決議，多數建議制定人工智慧的監管框架、強調應建立資料管理及風險控管機制

第 78 屆聯合國大會於 2024 年 3 月 21 日通過首個與 AI 相關的決議。為了推動「安全且值得信任的人工智慧（safe, secure and trustworthy artificial intelligence）」達成全球共識。此決議係由美國提出，並於聯合國大會得到澳洲、日本、新加坡、義大利及中國大陸等 120 多個聯合國會員國的支持。

本決議所涉及的 AI 為非軍用的 AI 系統，其生命週期包括設計前置作業、設計、研發、評價、測試、部署、使用、銷售、採購、運作及淘汰（decommissioning）等階段。

本決議鼓勵會員國通過以下 17 點的作法，以促進安全且值得信任的 AI 系統：

1. 依各國政策、優先事項及國際法義務，制定及實施 AI 系統監管暨治理框架，以支持負責任的 AI 創新與永續發展。

2. 為促進創新，鼓勵在設計、研發階段、部署及使用 AI 系統前，採取有效措施，例如：國際可互通的識別、分類、評估、測試、預防及抵減 AI 的風險。

3. 鼓勵納入問題回報機制，允許使用者與第三方於研發、測試及部署 AI 系統時，可透過數據為證據基礎加上資料之利用以支持採取循證決策方式回報 AI 的技術漏洞等問題。

4. 提升民眾對民用 AI 系統的功能、限制等認知。

5. 在 AI 系統的整個生命週期中，推行「制定並實施風險監控及管理、資料保護機制」，包括個人資料保護與隱私權政策、AI 影響評估。

6. 增進「有效保護 AI 措施」的投資，包括實體安全、AI 系統安全及 AI 系統的整個生命週期的風險管理。

7. 鼓勵研發及部署有效、易使用、國際可互通的技術工具、標準或作法，包括「可信任的內容與來源認證機制」，透過浮水印或標籤，讓使用者能識別、確認資料來源。

8. 促進制定及實施有效、具國際互通性的「培訓及測試 AI 系統」框架、作法及標準，用以強化決策並減少演算法歧視。

9. 鼓勵保護智慧財產權並促進創新的措施之採用。

10. 於測試及評估 AI 系統時，保障隱私及個人資料，並遵循國際、國家法規對資料透明度的要求。

11. 對足以影響使用者最終決策的 AI 系統，在該 AI 系統的生命週期內，提供通知及解釋，並強化監管，以促進資料透明度、

本報告之智慧財產權歸屬於國發會

可預測性、可信度及可理解性，例如審查自動化決策及其過程，或提供「受自動化決策不利影響的人員」之替代或補救方案。

12. 增加「有效保護 AI 措施」的投資，包括 AI 系統生命週期內的風險及影響評估。

13. 推行 AI 系統，為保護文化多樣性，應使用多語言的訓練資料，特別是大型語言模型。

14. 在 AI 系統扮演不同角色的各組織（entities），需依協商條款來加強 AI 系統的資料共享，以理解、執行 AI 的政策、循證作法，降低 AI 生命週期的潛在風險。

15. 鼓勵與國際合作，以了解、平衡 AI 系統的數位落差，如開源之 AI 系統。

16. 呼籲會員國採具體措施，減少性別數位落差，關注隱私、資安、加強數位技術（AI）的使用等議題。

17. 鼓勵與發展中國家合作，提供技術、資金等資源以消弭其數位落差。

綜上可得出，由於 AI 系統的重點為使用大量訓練資料，而資料內容及來源難以確認，故多數建議落在制定 AI 的法規框架、強調資料管理及風險控管機制。

資料來源：

1. U.S. Department of State, United Nations General Assembly Adopts by Consensus U.S.-Led Resolution on Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development, 2024-03-21, https://www.state.gov/united-nations-general-assembly-adopts-by-consensus-u-s-led-resolution-on-seizing-the-opportunities-of-safe-

本報告之智慧財產權歸屬於國發會

secure-and-trustworthy-artificial-intelligence-systems-for-sustainable-development/ (last visited 2024/03/27)

2. Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development, draft resolution, https://digitallibrary.un.org/record/4040897?v=pdf (last visited 2024/04/23)

參、 數位監管

一、 歐盟

(一)2024 年 1 月 31 日歐盟執委會依據數位服務法公布新透明度資料庫

為確保網路對所有人的安全與公平，歐盟執行委員會於 2024 年 1 月 31 日依據《數位服務法（Digital Services Act, DSA）》針對 2023 年 9 月上線的線上平台服務提供者透明度資料庫（Transparency Database）提出「新版本的使用者介面」，有助於民眾查詢線上平臺服務提供者依法提交之資訊。

依據 DSA 規定，平臺業者必須依法提交透明度資料，內含其刪除或限制使用者平臺內容存取權限的理由陳述（statements of reason），以提升網路平臺的資訊透明度。從 2023 年 9 月起，該透明度資料庫已有超過 30 億個理由陳述，可供資料庫使用者搜尋、下載。

於資料庫建置時，僅 2023 年 4 月所指定的超大型線上平臺（Very Large Online Platforms, VLOP）有義務依循 DSA 規定提交理由陳述，但從 2024 年 2 月 17 日 DSA 全面適用後，除微型及小型事業（micro and small enterprise）外之所有線上平臺都必須提交有關其平臺內容存取權限的審核決策資料。

本報告之智慧財產權歸屬於國發會

歐盟執委會下一步將讓利害關係人、研究人員、記者及所有有興趣的使用者可以透過新使用者介面的透明度資料庫進而篩選搜索、分析內容。而新透明度資料庫設計，讓資料庫使用者可以透過視覺化的圖表，看到線上平臺業者提供的透明度報告的資訊，包含 A 概述；B 時間軸；C 透明度報告中常被列為違反平臺規則的行為，如超出平臺服務範圍、非法言論、非法產品；D 主要限制之類型；及 E 其他分析等資訊。

資料來源：

1. European Commission, Digital Services Act: Commission launches Transparency Database Update with Dashboard | Shaping Europe's digital future (europa.eu), 2024-01-31, https://digital-strategy.ec.europa.eu/en/news/digital-services-act-commission-launches-transparency-database-update-dashboard (last visited 2024-04-19)
2. European Commission, Welcome to the DSA Transparency Database, 2024-04, https://transparency.dsa.ec.europa.eu/ (last visited 2024-04-19)

(二)2024 年 2 月 8 日歐盟執行委員會發布「選舉公正指引草案」進行公眾諮詢

歐盟執委會於 2024 年 2 月 8 日依據數位服務法第 35 條發布數位服務法（Digital Services Act, DSA）首部「選舉公正指引草案」並進行公眾諮詢，該指引草案之目的在向 VLOP 與超大型線上搜尋引擎（Very Large Online Search Engines, VLOSE）提供可採取之緩和威脅民主選舉正當性與完整性風險的應對措施，解決平臺上可能發生之風險。

近年來，線上平臺和搜尋引擎已成為公共討論與引導民意走向之重要場域，本指引草案，提供指定之 VLOP 及 VLOSE 針對選舉活動、

本報告之智慧財產權歸屬於國發會

生成式 AI 內容風險之預防措施與具體範例，以解決選舉活動進行中所可能發生之風險，例如，深度偽造（Deep Fakes）技術應用之問題等。

指引於未來生效後，VLOP 及 VLOSE 的提供者將依據指引履行其法定義務，透過以下措施之運用，避免使所提供之服務操縱及干預選舉活動之進行，降低選舉活動過程中特定風險的發生：

1. 向使用者提供選舉活動之官方資訊。
2. 採取強化使用者媒體識讀能力之行動。
3. 讓使用者知悉所接收內容和使用者之背景資訊。
4. 標識候選人宣傳之政治宣傳廣告。
5. 控管含有威脅選舉活動之病毒內容，查核事實並註記警告標籤。

資料來源：

1. European Commission, Commission is gathering views on draft DSA guidelines for election integrity, 2024-02-08, https://digital-strategy.ec.europa.eu/en/news/commission-gathering-views-draft-dsa-guidelines-election-integrity (last visited 2024/02/22)

(三)2024 年 3 月 11 日歐盟理事會與歐洲議會就數位平臺工作者之勞動條件如何改善達成臨時協議

透過數位平臺媒合的新商業模式為勞動市場帶來零工經濟風潮，也由於形成新工作型態而使勞動工作條件異化，自去年 6 月起歐盟各會員國勞工部長與歐盟理事會啟動協商，擬就數位平臺工作者權益保障提出一項適用於各會員國之「數位平臺工作者指令」，而歐洲議會和歐盟理事會於 2024 年 3 月 11 日宣佈，歐洲議會議員和歐盟 27 個會員國之代表已就改善數位平臺工作者勞動條件之立法達成臨時協議，

本報告之智慧財產權歸屬於國發會

為涉及勞動權益及演算法管理的規範提供一套暫時性基準，以待將來「數位平臺工作者指令」能順利批准。

數位平臺的複雜性與跨境流動的性質，挑戰了歐盟境內現有市場的慣例與法律規範，為勞動市場帶來了以下重要待解的問題：

1. 勞動權利和社會保障不足：

大多數的數位平臺工作者常以自營工作者承接工作，平臺業者可躲避傳統勞動法中身為僱用人之義務，並將風險（健康安全、職災、交通事故等）責任轉嫁及外部化，最終由工作者和社會共同承擔。

2. 演算法管理的偏見與歧視：

由於 AI 演算法的偏見大多是透過資料庫的參數學習而來，且數據蒐集本身即存在性別種族、年齡或其他類型的歧視與偏見。目前演算法管理平臺缺乏透明化，且難以理解其演算法的決策過程，故數位平臺透過運用演算法管理決定是否給予或剝奪工作機會，對平臺上工作者的工作條件和薪酬產生極大的影響，而恰是由數位平臺掌握演算法管理，形成可任意操弄的結果，偏見與歧視的影響力將藉由演算法被延續和放大，進而影響勞動者工作機會的權益。

3. 缺乏有效的爭端解決機制：

由於工作者與數位平臺之間非典型的僱傭關係，當數位平臺工作者遇到勞資糾紛時，由於其不具受僱人之身分而多半沒有適當的爭端解決機制，尤其當面臨跨境交易時更無法確立其司法管轄權，管轄權的競合衝突將使得爭議變得更加複雜。早前歐盟各會員國針對數位勞動平臺的監管方式仍存在某程度分歧，尤其是數位平臺工作者被錯誤地歸類為自營

本報告之智慧財產權歸屬於國發會

工作者而非雇員的法律事件已在歐盟衍生出許多訴訟爭議，故歐盟認為有必要催生一套數位平臺工作權的改革規範。

按歐盟執委會最初於 2021 年 12 月發布「數位平臺工作者指令」提案，包括僱傭之界定標準、賦予工作者享有同等的勞動權益及社會保障等，指令的內容可歸納為三大重點，以下試分述之：

1. 就數位平臺從業人員之身分定性問題，擬提出數位平臺僱傭關係的認定準則，使數位平臺工作者能享有基本勞動權利和制度性保障，共有五項「從屬性」判定的標準用以確認平臺業者是否具「僱用人」地位：

   (1) 薪資報酬由平臺業者決定；

   (2) 得對工作者的主觀條件限制或工作績效要求；

   (3) 透過電子化的方式監督工作程序；

   (4) 決定工作時間或派發工作項目；

   (5) 具勞務專屬性，得限制工作者為第三方業者提供勞務。

   若平臺業者滿足上述條件中至少兩項標準，在法律上即被視為僱用人，於該平臺的工作者則被視為受僱人，並享有勞工的基本保障，包括最低工資、勞資協商、工作時數與休假天數、職業災害賠償、失業和疾病津貼、養老金等。而平臺業者有權對上述「從屬性」的判斷方式提出異議，但須舉出僱傭關係不存在的反證推翻。

2. 提高數位平臺發展的公平性、透明化及追溯性，以及一套跨境適用的規則，確保平臺工作者具有申訴及解決爭端的管道機制。

3. 要求數位平臺業者對演算法管理的自動化決策應更加透明：

本報告之智慧財產權歸屬於國發會

(1) 平臺業者有義務向工作者揭露將演算法運用於分配工作、計算薪酬，以及評估考核工作者之績效；

(2) 確保人工監控的工作條件；

(3) 賦予當事人對自動化決策提出異議的權利。

資料來源：

1. Platform workers: Council confirms agreement on new rules to improve their working conditions, 2024-03-11, https://www.consilium.europa.eu/en/press/press-releases/2024/03/11/platform-workers-council-confirms-agreement-on-new-rules-to-improve-their-working-conditions/ (last visited 2024/04/10)
2. EU rules on platform work, https://www.consilium.europa.eu/en/policies/platform-work-eu/ (last visited 2024/04/10)
3. Spotlight on digital platform workers in the EU, 2024-04-05, https://www.consilium.europa.eu/en/infographics/digital-platform-workers/ (last visited 2024/04/10)

(四)2024 年 3 月歐洲議會批准《歐洲媒體自由法案》，在數位媒體服務之監理架構下確保新聞自由，保障歐盟媒體獨立性及多元化

為確保歐洲媒體自由與多元，歐盟執委會於 2022 年 9 月提出《歐洲媒體自由法案》(European Media Freedom Act)草案，作為公開諮詢文件之一部分，其係以委員會的法制報告和業經修訂的《視聽媒體服務指令》為法源基礎，該指令之目的在於協調歐盟會員國關於視聽媒體的立法；歐洲議會於 2024 年 3 月正式批准《歐洲媒體自由法案》，保障境內新聞自由與新聞工作者之人身安全，並確保公共媒體穩定資金來源、媒體所有權與廣告資源分配之透明度，解決國家監管機構間

本報告之智慧財產權歸屬於國發會

缺乏橫向聯繫、國家廣告和受眾指標缺乏透明度等情形，以防止任何政治或商業手段監視或干預媒體編輯之獨立性，最終期望得以銜接今年始施行的《數位服務法》(Digital Services Act, DSA)，法案之重點如下：

1. 監管機構之轉換：

歐盟欲透過創立新的獨立機關「歐洲媒體服務委員會」(European Board for Media Services, EBMS)，取代「歐洲視聽媒體服務管制組織」（European Regulators Group for Audiovisual Media Services, ERGA），建立具一致性之歐盟內部市場媒體服務監理機制，以克服跨境媒體監管手段之不足。

2. 保護編輯獨立性：

歐盟會員國必須尊重媒體服務提供者之有效編輯自由，並提升對新聞來源的保護；該法另外還要求「媒體服務提供者」(media service providers)必須公開揭露有關其所有權結構、政府公部門廣告收入及數位廣告收入的詳實資訊，以增強媒體所有權與資金來源的透明度，強化公共服務媒體之獨立性。

3. 不得針對媒體使用間諜軟體：

基於對新聞媒體編輯自由之尊重，不得於媒體服務提供者及其家屬、雇員或雇員之家屬所使用之設備中安裝間諜軟體，僅有在個案情形下，得基於國家安全、重大犯罪偵察等正當理由例外適度開放使用監控軟體。

4. 增加政府廣告透明化：

該法要求各國政府應建立公開公平透明的政府廣告資源分配機制，且政府廣告分配給媒體的方式必須透明且無差別

本報告之智慧財產權歸屬於國發會

待遇；此外與媒體廣告收益連動的閱聽調查系統(audience measurement)，將增強其透明度與客觀性。

5. 強化公共服務媒體之獨立性：

若歐盟會員國有公共服務媒體，應提供其充足且穩定的資金，要求評估媒體市場集中度對媒體多元化和編輯獨立性的影響，並維持各國公共服務媒體（即公共廣電媒體）的獨立運作，以保證編輯之獨立性，且公共服務媒體負責人與董事會成員應以透明、公開和非歧視的方式任命及選任。同時，公共服務媒體提供者也應符合公共服務使命，以公正客觀的方式提供閱聽者多元的資訊與觀點。

6. 媒體內容之保護：

為了能與 DMA 接軌，對於專業媒體內容的無故移除應設有保障措施，只要在不涉及整體風險(systemic risk)之情況下，超大型線上平臺（very large online platform, VLOP）於移除合法媒體內容前，「應採取一切可能的措施」將暫停、屏蔽其內容的原因事由告知「遵守共同監管或自律機制的編輯標準的新聞媒體」，且平臺必須優先處理媒體服務提供者所提出之申訴，並要設法使歐盟會員國的相關新聞媒體機構接受其決定。

7. 建立媒體多元性測試：

歐盟會員國根據媒體市場集中對媒體多元和編輯獨立性的影響性評估，各會員國需有正當理由始得採取對媒體造成影響之立法、監理或行政措施，且手段須符合比例原則。

8. 賦予使用者更新設置的權利：

本報告之智慧財產權歸屬於國發會

製造商與開發商應確保其產品與服務之功能，可讓使用者控制及管理系統之預設(default)，亦即允許使用者在其設備及介面上隨時更改視聽媒體服務的預設，以符合其個人使用偏好。

資料來源：

1. Media Freedom Act: a new bill to protect EU journalists and press freedom, 2024-03-13, https://www.europarl.europa.eu/news/en/press-room/20240308IPR19014/media-freedom-act-a-new-bill-to-protect-eu-journalists-and-press-freedom (last visited 2024/04/10)
2. European Media Freedom Act: Council adopts new rules to protect journalists and media providers, 2024-03-26, https://www.consilium.europa.eu/en/press/press-releases/2024/03/26/european-media-freedom-act-council-adopts-new-rules-to-protect-journalists-and-media-providers/ (last visited 2024/04/10)

二、英國

(一)2024 年 2 月 6 日英國公布制定新措施導入數位標籤（digital labelling）

英國商業與貿易部（Department for Business and Trade）經過和相關業者公開諮詢程序後，於 2024 年 1 月 24 日公布未來將透過新的法制規範，引入「數位標籤」新措施，並就相關產品，如玩具或機械等仍然承認 CE 標誌，降低事業之負擔，並確保製造商產品之安全性符合法律要求，同時藉由脫歐促進數位標籤改革，以使英國之產品監管要求符合現代世界之需要。

此次為英國首次推動進口標籤之數位化，允許事業將重要之監管、檢驗測試及製造資訊公開於網路，取代過去實體列印在產品上之方法，

本報告之智慧財產權歸屬於國發會

從而減省事業之時間及金錢成本，更能促進事業業務規模之擴大和成長。

除無限期持續承認 CE 標誌外，並將實施一系列配套法規，將有利於吸塵器、電視機、玩具、汽車、機械等產業之競爭力，及其售後市場及供應鏈之事業之持續營運，減少不必要的成本及作業程序，確保其製造及維修達到一定標準。但此政策不適用於政府部門主導的醫療器材、建築產品、船舶設備、鐵路產品、可移動壓力設備或無人機系統等面向之相類產品。

英國政府除了將進口之標籤數位化外，同時制定立法政策，使事業得在一系列產品上同時申請歐盟 CE 標記，以及針對消費者的 UKCA 產品安全標準標籤，無須經過反覆多次的驗證程序，以此提高製造商的市場競爭力。

製造玩具、機械產品之事業，於「數位標籤」政策推動後，得選擇在產品上使用 CE 或 UKCA 標誌，將重要之審查評估及製造資訊公開於網路，以證明製造商生產之產品符合本地法規標準。

資料來源：

1. GOV.UK, New laws to introduce digital labelling for businesses and reduce regulation costs, 2024-01-24, https://www.gov.uk/government/news/new-laws-to-introduce-digital-labelling-for-businesses-and-reduce-regulation-costs, (last visited 2024/04/18

(二)2024 年 3 月 26 日英國通過《數位市場、競爭及消費者法案》之提案，以期保障數位消費者之權益及促進數位市場競爭力

英國上議院於 3 月 26 日通過《數位市場、競爭及消費者法案》(Digital Markets, Competition and Consumers Bill, DMCC)，法案預計將於 2024 年秋季生效，擬建構一套監管數位市場競爭的新機制，防杜數

本報告之智慧財產權歸屬於國發會

位平臺濫用市場獨占地位而導致服務品質降低、扼殺創新及偏離交易價格水準，以維護自由市場的自然運作，並確保消費者使用數位服務時之資料控制權及可攜性，綜觀全法案可歸納為四大部分，各領域遂再分別連動至英國競爭及市場管理局(Competition and Markets Authority, CMA)2024~2025 年之年度計畫中，茲分述如下：

1. 機關賦權及擴張執法權限：

(1) 賦予「數位市場部門」(Digital Markets Unit, DMU)法定職權：

CMA 最初成立 DMU 時僅屬非正式部門，惟該部門早已著手處理數位市場案件，並進行市場研究與市場調查，該法案通過目的在於明確其法定地位，明文化其職務權限，除定期進行前瞻性研究與探索數位市場新興技術之趨勢外，並專責審查數位平臺在競爭市場的動向，監管數位平臺與使用平臺服務的第三方事業及終端用戶間之關係。此外，CMA 得在未經司法程序下，於 DMCC 的授權範圍直接行使公權力，強化調查及執法的量能，而關於其執行措施之過程，原提案要求須符合比例原則(proportionate)，但於上議院報告階段程序之修正版本僅要求手段具適當性(appropriate)即可，為其提供決策時之彈性空間；而管轄權之行使係採長臂管轄原則，法案規定 CMA 基於調查權之行使便可調取蒐集境外公司之電磁紀錄及數據資料，此與先前英國上訴法院作成之見解不同。

(2) 與其他單位之協調合作：

為 DMU 創設法定職務權限後，能持續與「數位監管合作論壇」(Digital Regulation Cooperation Forum, DRCF)成員合作與交流，DRCF 屬自願合作論壇，由 CMA 與英國資訊委員辦公室(ICO)、英國通訊傳播管理局(Ofcom)和

本報告之智慧財產權歸屬於國發會

英國金融行為監理局(FCA)聯合成立，DRCF 的決定或交流內容並不影響各成員機構的政策或執行。而 DMU 對 Ofcom、ICO 及 FCA 具諮詢責任(duty to consultation)和協調責任 (duty to cooperate)，使競爭監理單位得以在早期介入相關領域協調，類似金融服務監理機制，與政府各單位橫向聯繫及共享情報資訊。

(3) 權力分立之界限仍有待觀察：

鑒於 DMU 可以直接干涉及管轄 SMS 公司(詳下述 3.)，可能給予 CMA 過於膨脹的權力，故本次通過之法案可發現 CMA 的部分權限有所減縮，如對機關處分與罰款數額的部分有異議，仍回歸法院進行實質審查，再如 CMA 公布的指引(guidance)須由國會批准同意。

2. 數位消費者之權利保護框架：

具高度市場支配地位之大型數位平臺，憑藉數據優勢，透過使用者條款迫使消費者提供更多個人資訊，導致消費者無法控制個人隱私資料之利用。故法案使 CMA 的執法在未經司法審查下能更有效率決定案件對象何時違反消費者保護，或對於被不實產品的使用評論欺詐(如 greenwashing)、訂閱服務陷阱(subscription traps)、強迫推銷、採取水滴定價(drip pricing)策略哄抬價格等不公平商業行為直接採取預防措施。要求提供用戶正確資訊、警示標語及進行重要資料更新，預設提供促進用戶選擇之資訊，以確保用戶決策時取得最佳利益，同時敦促數位平臺必須在免費試用期或低價優惠期即將結束前提醒消費者，讓消費者能直接取消訂閱，避免對用戶應如何利用數位服務施加不當限制。此外，並要求數位平臺需確保第三方技術之相互操作性，強化消費者選擇權(right to choice)、透明度(transparency)與服務設計(service design)以保

本報告之智慧財產權歸屬於國發會

護消費者個人隱私；法案通過後可預期經由競爭所產生的動能，可激勵事業投入資源到用戶安全以及相應服務之優化。

3. 數位市場之事前管制架構：

英國現行競爭法偏向事後管制，為因應目前數位市場巨擘壟斷議題之相關競爭特性，本法案遂創設一套指定「具戰略市場地位」(Strategic Market Status, SMS)的數位公司之概念，意在對商業活動上具有實質(substantial)、固有(entrenched)市場力量，或具戰略地位(strategic position)之公司，皆有可能受 DMU 所指定而需符合事前管制之法律要求，如此便能管轄事業行為，防止其濫用市場壟斷地位。DMU 基於本法案，將可能介入制定關於該公司運營方式的行為準則(code of conduct)，該準則將係由促進競爭目標(objectives)、衍生原則(principles)及 DMU 制訂之指引(guidance)三要素構成，使其符合公平交易、開放選擇、信任及透明性等目標，例如指示該公司向競爭對手的搜尋引擎開放所屬資料或演算法，或是提高對這些公司的應用程式商店或審查系統運作方式的透明度，若公司不遵守為其制定的規則，CMA 將有權對這些公司直接處以高達其全球營業額 10%的罰鍰。然為避免對數位平臺造成不必要負擔，DMU 尚須進一步檢驗數位公司的活動是否該當於干擾市場競爭的「指定活動」(designated activities)，此類指定活動多半具備營收高(全球營業額超過 250 億英鎊或在英國境內營收超過 10 億英鎊)、網路效應強、監管之高必要性等特色。法案正式生效後，首批被認定為 SMS 之公司預計於 2025 年 7 月開始履行相關義務。

DMCC 就事業得主張之豁免範圍起初係採用對價利益豁免原則(countervailing benefits exemption)，此係透過利益權衡之審查方式，被 DMU 認定為 SMS 之公司倘能證明消費者自其從業行為中獲得之利益大於其因違反相關規定而對競爭造

本報告之智慧財產權歸屬於國發會

成的實際上、潛在或推定行為的負面影響，則公司可免受DMU 所制定之行為準則(code of conduct)拘束，然最終仍採納上議院報告階段程序之修正版本，以「消費者之依賴程度」(indispensable)作為得否豁免之判斷，藉由較嚴格之標準來減少大型數位平臺正當化自身限制競爭行為之機會。若交易相對人對該事業體不具有足夠且可預期之脫離可能性時，亦即該事業體具有市場優勢地位，則應認有依賴性存在而無適用豁免條款之餘地。

4. 評估限制競爭之風險：

CMA 可以對可能損害英國消費者及事業用戶之事業結合採取行動，如垂直整合或異業結合，於結合審查程序中，透過市場調查及反競爭行為調查以箝制非法競爭行為；觸發CMA 介入審查的併購門檻乃係併購之任一方掌握英國至少33%的商品銷售或服務供應，且境內總營業額超過 3.5 億英鎊時的事業主體。英國國內現有結合案主要係聚焦在有助於數位市場創新的領域，如行動瀏覽器、雲端遊戲服務的發布、電子商務和數位廣告及行動瀏覽器等潛在的反競爭行為。

另外，法案尚賦予 DMU 實施促進競爭干預(Pro-competitive interventions, PCI)措施的權力，旨在解決數位市場中強大而固有的市場力量，透過有效使用 PCI，鼓勵數位市場採取動態且有益於競爭的變革，創造經濟增長機會，例如在數位平臺和數位廣告商間實施 PCI，促進競爭發展。

綜上所述，再搭配 CMA 2024~2025 年之年度計畫作整體觀察，可歸結出以下趨勢：

1. 創造消費者福祉，避免因缺乏透明度而受不公正的歧視對待，且對其個人資料享有充分的控制權。

本報告之智慧財產權歸屬於國發會

2. 確保數位平臺經營者與競爭對手或商業用戶之間的產品或服務的相容，實現數位創新與發展資料共享。有助於降低進入壁壘，使新的市場參與者能夠進入並與現有之平臺競爭。

3. 藉開放自由的市場推動事業創新及提高生產力，建立多元化的供應鏈來維持數位韌性。

4. 加速英國轉型成零碳經濟國家的目標，在 DMCC 的基礎上對環境永續之商品服務及綠色市場有所行動，開展關於綠色能源及淨能產業之工作。

資料來源：

1. Current version of the Bill, 2024-03-26, https://bills.parliament.uk/bills/3453 (last visited 2024/04/09)

2. Written Evidence submitted at Report Stage in the House of Lords, 2024-03-11, https://bills.parliament.uk/bills/3453/stages/18513 (last visited 2024/04/10)

3. UK Digital Markets, Competition and Consumers Bill: Extraterritorial Regulation Affecting the Tech Investment Climate, 2024-03-04, https://www.csis.org/analysis/uk-digital-markets-competition-and-consumers-bill-extraterritorial-regulation-affecting (last visited 2024/04/07)

4. UK Digital Markets, Competition and Consumers Bill: One step closer to becoming law, 2024-01-17, https://www.ashurst.com/en/insights/uk-digital-markets-competition-and-consumers-bill-one-step-closer-to-becoming-law/ (last visited 2024/04/09)

5. Competition and Markets Authority Annual Plan 2024/25, 2024-03-14, https://www.gov.uk/government/publications/cma-annual-plan-2024-to-2025 (last visited 2024/04/10)

本報告之智慧財產權歸屬於國發會

三、日本

(一)2024 年 2 月日本經濟產業省公布「特定數位平臺透明度及公正性」之評估結果，而數位廣告業者為首次進行評估

日本經濟產業省(METI)依據 2020 年通過《特定數位平臺透明度及公正性提升法案》之授權，分析數位平臺對國民生活及國民影響程度，指定達到日本國內交易金額超過 3,000 億日圓的網路商業平臺與超過 2,000 億日圓的 APP 商店營運商為本法的「特定數位平臺業者」。受指定之納管對象則有義務公開與客戶間的契約條件、理由等資訊，以及事先通知契約變更條件，若經 METI 判斷業者未充分公開資訊時，可進行勸告或命令採取必要措施。目前雅虎、亞馬遜日本、樂天集團、谷歌、蘋果電腦及 iTunes 等 6 家事業皆為法案之適用對象，故這些數位服務公司需向其用戶公開交易條款及營運狀況等資訊，並主動整合爭端處理程序與通報機制，每年尚須提交自我評估報告作為 METI 審查依據。

該法案建構之數位監管架構屬共同監管(Co-Regulation)之模式，乃政府試圖在促進產業自主創新與法令拘束間取得平衡的展現，由政府提供業者廣泛性指導，再將技術性措施留給產業自主執行。政府透過蒐集專家學者意見，結合數位平臺使用事業之建議進行評估，讓「特定數位平臺業者」自主且積極提升數位平臺透明性與公正性，將國家的干預及其他管制的影響降到最低，達到營運改善目的並消弭紛爭。

METI 於 2024 年 2 月 2 日發布「特定數位平臺透明度和公正性」之評估結果，本次評估之數位平臺共分為線上商城(日本 Amazon 公司、樂天公司、Yahoo!購物公司)、應用程式商店(App Store、Google Play 商店)、媒體整合類型之數位廣告(位在 Google 公司旗下的 YouTube 與隸屬 Meta 公司旗下 Instagram 之展示廣告)，以及廣告仲介類型之數位廣告，其中數位廣告為首次進行透明度及公平性評估，指定為「特定數位平臺業者」業者後續則應依該評估結果盡力改善該數位平臺的透明

本報告之智慧財產權歸屬於國發會

性及公正性。惟本法案由政府評估並公布特定數位平臺之營運是否具備透明性及公正性之規定，而該評估主要係以特定數位平臺業者提出之「自我評估」報告(內容應包含其事業概況、資訊公開等規定的遵循狀況)為基礎。

資料來源：

1. Evaluation on Transparency and Fairness of Specified Digital Platforms Compiled, 2024-02-02, https://www.meti.go.jp/english/press/2024/0202_002.html (last visited 2024/04/10)
2. Making the Digital Market Easier to Use: The Act on Improving Transparency and Fairness of Digital Platforms (TFDPA), 2021-04-23, https://www.meti.go.jp/english/mobile/2021/20210423001en.html (last visited 2024/04/10)
3. Act on Improving Transparency and Fairness of Digital Platforms, 2024-02-02, https://www.meti.go.jp/english/policy/mono_info_service/information_economy/digital_platforms/index.html (last visited 2024/04/10)

肆、 數位身分

一、 歐盟

(一)2024 年 3 月 26 日歐盟理事會通過《歐盟內部市場電子交易之電子身分認證及信賴服務規則》（eIDAS 規則）之修訂

歐盟議會於 2024 年 2 月批准《歐盟內部市場電子交易之電子身分認證及信賴服務規則》（electronic IDentification, Authentication and trust Services, eIDAS 規則）之修訂，歐盟理事會（European Council）並於 2024 年 3 月 26 日通過議會所提交之修正草案，歐盟會員國未來將向民眾及事業提供數位身分錢包（digital identity wallets）服務，將

本報告之智慧財產權歸屬於國發會

數位身分與其他個人屬性證明相互連結，使用手機簡易證明身分與共享數位身分錢包中之電子文件，透過數位身分接取線上服務，而數位身分將在歐盟境內受到承認，民眾不需使用私人身分識別方法及共享非必要之資料，可確保使用者僅共享自身所需的資料，以下為重要之修訂內容：

1. 每個會員國至 2026 年前，必須向人民及事業提供數位身分錢包服務，並接受其他會員國之數位身分錢包服務。

2. 使用數位身分錢包服務須係出於人民自主決定，故須制定充足的保障措施，避免對選擇不使用數位身分錢包之人民造成間接歧視。

3. 數位身分錢包之發行、使用、廢止對所有自然人皆以無償為原則。

4. 關於個人屬性證明之驗證，會員國需要提供免費之驗證機制，且僅用於驗證錢包與使用者身分之真實性及有效性。

5. 數位身分錢包的原始碼將是屬於開放原始碼，故會員國擁有立法形成自由，基於合理的原因，除了安裝在使用者裝置設備上的元件外，無需揭露其他特定元件。

6. 錢包作為數位身分的一種形式態樣，應確保與發行數位身分錢包計畫之間的一致性。

歐盟官方公報將於未來幾週公布所修訂之規則條例，並在發布 20 日後生效，預計於 2026 年全面實施。

資料來源：

1. Council of the European Union, European digital identity (eID): Council adopts legal framework on a secure and trustworthy digital wallet for all Europeans, 2024-03-26, https://www.consilium.europa.eu/en/press/press-

本報告之智慧財產權歸屬於國發會

releases/2024/03/26/european-digital-identity-eid-council-adopts-legal-framework-on-a-secure-and-trustworthy-digital-wallet-for-all-europeans/ (last visited 2024/04/11)

2. European Parliament, MEPs back plans for an EU-wide digital wallet, 2024-02-29, https://www.europarl.europa.eu/news/en/press-room/20240223IPR18095/meps-back-plans-for-an-eu-wide-digital-wallet (last visited 2024/04/11)

二、英國

(一)2024 年 3 月英國上議院持續審議《資料保護及數位資訊法草案》

英國政府之科學、創新與技術部（Department for Science, Innovation and Technology）自 2023 年 2 月開始致力推動數位身分（Digital Identities）服務政策，幫助人民安全證明自己的身分，而無需依賴實體證明文件，而為了建立數位身分服務之可信度與統一標準，遂於 2022 年 6 月推出「數位身分信賴框架」（UK digital identity and attributes trust framework），2023 年 3 月著手制定《資料保護與數位資訊法草案》（Data Protection and Digital Information Bill），以支持數位身分信任框架和資料治理，目前該法案已於 2024 年 3 月進入上議院持續審議。本法案主要涉及處理可供識別的個人資訊，使提供數位身分服務者得以利用資料來進行個人資料之驗證服務。

依據「數位身分信賴框架」，規範之範圍含括三類服務提供者，其一為身分服務提供者（Identity service providers），其二為特徵屬性服務提供者（Attribute service providers），「特徵」乃是為描述個人或組織之生物、行為或身分地位資訊，可能和實體或電子文件、行動裝置、學歷、健康狀態或財務狀況相關，其三為編排服務提供者（Orchestration service providers），上述組織需遵循框架之規則提供安全可信之服務。

本報告之智慧財產權歸屬於國發會

服務提供者參與該信賴框架，需符合該框架的規則，證明組織能夠安全管理使用者的數位身分或屬性特徵，自認證機構獲取認證後，則須受到主管機關的監管，例如身分服務提供者於範圍內提供使用者服務，透過軟體完成身分驗證服務，提供使用者（出租人、僱用人等對象）身分驗證服務，協助使用者進行身分資格審查。

英國之數位身分服務提供者 OneID 與 SurePay 公司則建立合作關係增強事業安全性，透過整合數位身分驗證與確認收款人服務，提供強大的電子支付詐騙防制策略，打擊網路詐欺事件，確保安全的數位交易。

資料來源：

1. UK Parliament, Data Protection and Digital Information Bill, https://bills.parliament.uk/bills/3430 (last visited 2024/04/23)
2. UK Parliament, Lords resumes scrutiny of Data Protection and Digital Information Bill, https://www.parliament.uk/business/news/2024/march/data-protection-and-digital-information-bill-subject-to-lords-line-by-line-scrutiny/ (last visited 2024/04/23)
3. GOV.UK, UK digital identity and attributes trust framework beta version (0.3), 2023-07-23, https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version/uk-digital-identity-and-attributes-trust-framework-beta-version#rules-for-all-identity-and-attribute-service-providers (last visited 2024/04/18)
4. globalgovernmentforum, UK Cabinet Office seeks feedback on data sharing legislation to develop digital ID, 2023-01-16, https://www.globalgovernmentforum.com/uk-cabinet-office-seeks-feedback-on-data-sharing-legislation-to-develop-digital-id/ (last visited 2024/04/18)

本報告之智慧財產權歸屬於國發會

三、 澳洲

(一)2024 年 4 月 3 日澳洲參議院通過數位身分法案(Digital ID Bill)

澳洲參議院於2024年4月3日通過數位身分法案(Digital ID Bill)，並將修正法案提交眾議院審議，本法案將為數位身分系統建立法制框架，確保選擇透過經認證的服務提供商使用數位身分的人民享有強而有力的隱私及安全保障，為個人提供安全、便捷的身分驗證方式，用於與政府和私營部門提供之服務，以下為本次參議院所提出之修正項目：

1. 建立執法報告框架以提高透明性：

限制執法部門向數位身分提供商取得由其控制之個人資料的權能，並建立規範要求取得個人資料的執法機關或相關單位必須每年向總檢察長報告，而總檢察長則必須向議會報告。

2. 規劃各階段擴展政府數位身分系統之時程表：

私營事業目前無法加入政府數位身分系統，政府預計將於 2 年內將該系統擴展到私營部門，經認可的私營事業在數位身分法案生效後 2 年內得申請加入政府數位身分證系統。

3. 賦予個人對數位身分之停用或重新啟動具更強之資訊控制權：

確保一旦個人選擇停用數位身分，則未經其明示同意，不得使用或重新啟用該數位身分。

4. 進一步限制資料保留及資料分析：

限制數位身分服務提供者於不再需要個人資料後保留個人資料的權能及限制分析。

本報告之智慧財產權歸屬於國發會

5. 確保無需數位身分亦可使用及接觸服務，並且不會對無數位身分的人民造成不利影響，對可能有不便利性的數位難民給予適切之包容。

6. 為使用政府系統的個人制定救濟管道：

加強救濟管道，並要求在該法案生效後 12 個月內針對詐欺和網路安全事件制定救濟框架，以確保在發生紛爭時為個人提供救濟。

7. 強化生物辨識測試的要求：

增加生物識別測試相關的要求，以降低生物識別系統對任何個人或群體產生不利或歧視的風險。

資料來源：

1. Australia Governments, Department of Finance, 2024-04-03, https://www.finance.gov.au/about-us/news/2024/digital-id-bill-passes-senate (last visited 2024/04/11)
2. Australia Governments, Australia’s Digital ID System, https://www.digitalidentity.gov.au/legislation (last visited 2024/04/11)

伍、 資訊隱私

一、 美國

(一)《美國隱私權法案》(American Privacy Rights Act)將限制科技公司獲取用戶之個人資料

美國參議院兩大政黨協商達成共識，將資訊隱私權作為美國公民的基本權保障，著手制定一部聯邦層級的法律來規範公司應如何蒐集、處理、儲存、傳輸、共享及利用美國公民的個人資料，使個別用戶自

本報告之智慧財產權歸屬於國發會

主控制個人資料之利用，得以決定此類資料的使用時機與場域，以及隨時選擇退出(opt-out)個人資料的演算及目標式廣告投放的權利，並要求公司揭露類此資訊是否曾被轉移至第三方，防止資料遭盜賣或強制刪除。該法案如順利闖關，將會是美國首部針對所有族群並且涵蓋各種資料類型的聯邦層級法律，該法案所創建的指標性意義可與歐盟的《一般資料保護規則》（GDPR）比肩。

兩黨之協議將透過聯邦層級之立法來保障美國公民的資訊隱私權，賦予聯邦貿易委員會（Federal Trade Commission, FTC）及各州檢察總長更擴張的權力，透過一套究責機制監督數位消費者的隱私問題。同時將讓個別用戶具有訴訟實施權，得對違法取用個人資料的事業提起訴訟，請求損害賠償。然該法案並非一概禁止公司藉由定位服務追蹤並獲取用戶位置資訊，亦未限制對用戶投放目標式廣告，如基於預防詐欺等正當化事由仍可為之。惟法案之核心首重透明性，大幅度限縮事業之操作空間，除要求公司將機敏資訊轉移給第三方之前，應向用戶揭露並取得其事前同意，使用戶得以知悉事業如何蒐集資料以投入演算之方法，並給予用戶更大程度的自主性，擁有自由選擇退出的機制，可隨時複製、刪除、更正或轉移個人隱私記錄。此一立法措施隱含著對抗地緣政治中敵對國家的意圖，避免美國公民個資流入與美國正處在競爭關係中的國家。最後，法案試圖阻止事業於運用演算法分析用戶位置、搜尋記錄、財務狀況或生物特徵等識別資訊的過程中產生種族、性別、年齡的歧視性結果，故定期要求對演算法進行年度追蹤審查，確保演算法不會對用戶，特別是對未成年人造成嚴重損害。

以下為法案中的草案主要內容及預期目標：

1. 資料運用最小化（Data Minimization）：公司對個人資料蒐集與處置的範圍限制，不能獲取逾越本於服務範圍所需之資料，僅限於特定業務之產品或服務，如完成交易之目的、證實用戶真實身分之目的、滿足產品保固之目的以及網路安全預防之目的等。

本報告之智慧財產權歸屬於國發會

2. 機敏資訊之保護：除非獲得用戶事前之明示同意，否則不得向第三方移轉其個人資料，且應向用戶揭露資料掮客（data brokers）的資訊與資料移轉第三方的使用期間。

3. 用戶資料使用之透明性：事業應本於善意(bona fide)使用戶明確知悉演算法的投入運用，並公告其隱私權政策及安全措施的效力期間。

4. 用戶對資料之自主控制權：用戶可隨時向事業請求複製、刪除、更正或轉移其個人隱私記錄，而事業應明確告知用戶得行使該項權利。

5. 退出權(opt-out rights)與集中化退出機制（centralized opt-out mechanism）：用戶有選擇退出非敏感性個人資料的移轉及目標式廣告投放的權利，而集中化退出機制應由 FTC 建置，使用戶在未受阻之情況行使退出權利。

6. 對消費者權利之保障：不得因用戶對其個人資料行使各項權利時而拒絕向其提供商品服務或干預用戶行使法案所賦予之權利。

7. 服務提供者與接收個資的第三方：服務提供者應確保個資的安全性及隱密性之保障，且將個資移轉至第三方之前負有盡職調查 (due diligence) 義務，而接收資料的第三方則應確保僅於目的範圍內為授權之使用、移轉或儲存。

8. 資料掮客（data brokers）之預防：根據資料掮客影響之用戶數量來規範其義務，限制其在蒐集用戶資料之過程中剝奪用戶對資料之自主控制權及行使退出權，也禁止其基於騷擾及詐欺之意圖分析用戶的個人資訊。

9. 基本權與演算法間之消長：探討演算法對基本權之侵害，尤側重在種族、性別、年齡之反歧視措施。

本報告之智慧財產權歸屬於國發會

10. FTC 與各州之公權力行使：劃分 FTC 與各州執法機關之權責次序及管轄權限(前者優先)；同時該當不公平商業競爭行為時 FTC 和各州檢察長所能採取的保全措施及訴訟類型；被害者補償基金之建置由 FTC 專責。

資料來源：

1. CNN, US lawmakers unveil a plan to give all Americans a right to online privacy, 2024-04-08, https://edition.cnn.com/2024/04/08/tech/online-privacy-bill/index.html (Last visited 2024/04/15)

2. American Privacy Rights Act discussion draft, American_Privacy_Rights_Act_of_2024_Discussion_Draft_0ec8168a66.pdf (d1dth6e84htgma.cloudfront.net) (Last visited 2024-04-16)

3. section-by-section of the discussion draft, APRA Section by Section (d1dth6e84htgma.cloudfront.net) (Last visited 2024-04-16)

本報告之智慧財產權歸屬於國發會

項次 2. 六月雙月報

壹、 資料治理

一、 歐盟

(一)2024 年 4 月 18 日《歐洲互通法》（Interoperable Europe act）生效，為個人和企業提供更好的互聯公共服務

歐盟執行委員會提出的《歐洲互通法案》（Interoperable Europe act）於 2024 年 4 月 11 日生效，此法案將促進跨境資料交流和公部門的數位轉型。該法案對於歐盟《數位十年》（EU's Digital Decade）的目標至關重要，例如 2030 年實現 100% 關鍵公共服務線上化。互通性是數位單一市場（Digital Single Market）的核心特徵，掌握公共政策的數位化，例如司法、衛生、交通。公民、企業和公部門在使用需要跨境資料交流的數位公共服務時，將受益於此法案。例如共享下列資料：學歷或專業資格、交通安全、社會安全和健康、稅收、海關、公開招標、數位駕照、商業登記等。根據該法案的影響評估報告，預計每年可節省高達 50 億歐元。

法案的主要實施方案如下：

1. 建立一個多層次合作框架，集結會員國的數位政府單位、民間企業、專家、學者和在地行動者；該框架將由歐洲互通委員會（Interoperable Europe Board）指導，並受到歐洲互通共同體（Interoperable Europe Community）的支持。

2. 引入強制互通性評估，以建立「具備可互通性和可重複利用的設計（interoperable-by-design）」的公共服務。有助於公部門機構探索並嘗試解決在新服務或工具設計階段就存在的資訊跨境互通性問題。委員會將提供必要的指導和支援。

本報告之智慧財產權歸屬於國發會

3. 「資料互通的歐洲門戶（Interoperable Europe Portal）」，一個單一入口網站／搜尋引擎，鼓勵公部門之間共享高品質和可靠的資料。

4. 加強創新和政策支持機制，包括培訓、監理沙盒（regulatory sandboxes）、公私合作和政策實施支持專案。

該法規適用於公部門，包括歐盟機構。《歐洲互通法》的實施將通過數位歐洲計畫（Digital Europe Programme）提供資金。根據影響評估，預計該法案每年將節省高達 50 億歐元。大部分規範將在生效之日起 3 個月內（即 2024 年 7 月 11 日）適用，但有兩點值得注意：

1. 自 2025 年 1 月起，歐洲組織單位和政府機關將進行互通性評估

2. 成員國將在法案生效日起 9 個月後，即 2025 年 1 月前指定國家專責機構

資料來源：

1. European Commission, Interoperable Europe Act enters into force for better connected public services for people and businesses, 2024-04-11, https://ec.europa.eu/commission/presscorner/detail/en/IP_24_1970 (last visited 2024/04/22)

2. EUR-Lex, Interoperable Europe Act, 2022-11-18, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022SC0721 (last visited 2024/04/22)

3. 3European Commission, Interoperable Europe Act enters into force today, 2024-04-11, https://commission.europa.eu/news/interoperable-europe-act-enters-force-today-2024-04-11_en (last visited 2024/04/29)

本報告之智慧財產權歸屬於國發會

(二)2024 年 4 月 24 日歐洲議會通過歐洲健康資料空間和人類來源物質規則

歐洲議會於 2024 年 4 月 24 日通過歐洲健康資料空間 (European Health Data Space, EHDS)和人類來源物質規則，提高人類來源物質（Substances of Human Origin, SoHO）之安全性和品質，穩固歐洲衛生聯盟（European Health Union）之發展基石，以保護人民之健康和醫療系統之彈性，以下說明通過之重要規則：

1. 有關「歐洲健康資料空間」之政策

(1) 歐洲健康資料空間政策有兩個目標，其一為，讓人民完全控制自己之健康資料，提升醫療服務之品質，其二為，在嚴格之條件下，將人民之健康資料用於研究和公共衛生目的。

(2) 在歐盟實施歐洲健康資料空間政策後，人民在歐盟境內，無論身處何地，都能立即、簡單地存取自己的數位健康資料，將促進循證決策，減少重複檢驗程序，加強病患的照護，例如，當病患在國外尋求醫療服務時，醫療人員能夠在必要時存取病人所在成員國的醫療資料。

(3) 歐盟還為歐洲健康資料空間建立強大的法律框架，在符合嚴格的歐盟資料安全和存取標準、基本權利和網路安全規則的情況下，將健康資料再次用於研究、創新和公共衛生目的，有助於開發挽救生命的治療方法和藥物，改善歐盟的危機應變能力。

2. 有關「人類來源物質」規則

歐盟執委會先前於2022年7月頒布之新法規係為人類來源物質之監管提供了整體方法。此一新規定主要著重在更好

本報告之智慧財產權歸屬於國發會

的保護人類來源物質之接受者和捐贈者，以及透過醫療輔助人工生殖出生的子女。

(1) 新規則明確涵蓋固體器官之外的所有人類來源物質，例如，糞便、微生物群及母乳。

(2) 註冊所有可能影響人類來源物質安全及品質的活動之實體。

(3) 加強專業知識，以現有技術機構為基礎，特別是歐洲疾病預防暨控制中心（European Centre for Disease Prevention and Control）及歐洲藥品暨保健品質理事會（European Directorate for the Quality of Medicines & HealthCare），以不斷更新技術指引。

(4) 為創新而採用共同程序評估和授權人類來源物質之準備工作，並使工作與風險平衡。

(5) 加強國家之監督措施和對當局的支持措施。

(6) 支持供應連續的新措施，幫助會員國在關鍵人類來源物質的供應受到威脅時及時採取行動。

(7) 將與成員國共同組織協調委員會 (SCB-SoHO Coordination Board)，以支持新法規的實施並提供法律明確性。

(8) 將建立歐盟數位人類來源物質平臺，以蒐集所有必要資訊、簡化報告程序。

下一步將由歐盟理事會正式通過新的歐洲健康資料空間法規，預計將於秋季在官方公報上發佈，根據使用情況和資料類型分階段適用，理事會還將正式通過人類來源物質的規則，以提高人源性物質的安全性和品質，該規則將於 2027 年生效。

本報告之智慧財產權歸屬於國發會

資料來源：

1. European Commission, Commission welcomes European Parliament's adoption of the European Health Data Space and regulation on substances of human origin, 2024-04-24, https://ec.europa.eu/commission/presscorner/detail/en/IP_24_2250, (last visited 2024/05/03)

二、英國

(一)2024 年 4 月 18 日英國商業及貿易部發布 2024-2025 智慧資料藍圖（The Smart Data Roadmap）

英國商業及貿易部（Department for Business and Trade）於 2024 年 4 月 18 日發布 2024-2025 智慧資料藍圖（The Smart Data Roadmap）推動智慧資料經濟計畫，在 2024 至 2025 年間，於銀行、能源、金融、房地產（home buying）、零售（retail）、電信（telecommunications）、交通等 7 個重點產業領域優先實施智慧資料措施。智慧資料政策旨在為企業、個人提供資料，其允許企業於取得消費者之同意之下，可存取其資料以開發創新服務，促進產業投資、生產、競爭及經濟成長。

1. 於銀行領域，聯合監理委員會（Joint Regulatory Oversight Committee）於 2023 年 4 月制定開放銀行之發展藍圖，提出兩年期之分階段執行策略，並確定五項關鍵行動，將於近期發布開放銀行下一階段之發展建議。同時，英國政府承諾建立長期監管框架，消除開放銀行間之給付障礙，確保開放銀行之效益，及創造可持續之經營模式。

2. 於金融領域，英國政府將參酌金融、創新和技術中心（The Centre for Finance, Innovation and Technology）近期提出之報告和建議，進一步制定開放金融戰略（strategy for Open Finance）。

本報告之智慧財產權歸屬於國發會

3. 於能源領域，將在道路燃料價格方面採取措施，制定能源價格之資料開放計畫和法令，加速推動電費價格資料互通性之政策，發起公眾諮詢以蒐集有關消費者同意之意見。

4. 於電信領域，科學、創新與技術部（Department for Science, Innovation and Technology）將審查先前公眾諮詢之回覆，並制定和推動下一步措施，包含探索建立智慧電表資料庫之可行性，發布關於實施安全智慧電力系統建議之資訊。

5. 於交通領域，交通運輸部將以智慧資料為目標推動政策，包含續行探索工作開發智慧資料之交通應用，利用探索成果作為證據，以及提出可能之問題，預計於 2025 年發布有關智慧資料在交通領域發展機會之資訊。

6. 於零售領域，將和零售產業委員會（Retail Sector Council）、零售產業協會（Retail Trade Associations）合作，進一步認識智慧資料於零售領域之發展機會，並完成首輪評估制定推動的計畫。

7. 於房地產領域，將於 2024 年啟動試辦項目，為未來之買賣交易流程數位化及智慧資料計畫之發展提供前置資訊。

資料來源：

1. Gov.uk, The Smart Data Roadmap: action the government is taking in 2024 to 2025, 2024-04-18, https://www.gov.uk/government/publications/the-smart-data-roadmap-action-the-government-is-taking-in-2024-to-2025 (last visited 2024/04/25)

2. Thepaypers, The UK's plans for Smart Data, 2024-04-24, https://thepaypers.com/payments-general/the-uks-plans-for-smart-data--1267830 (last visited 2024/04/25)

本報告之智慧財產權歸屬於國發會

(二)2024 年 4 月英國發布「食品資料透明度夥伴關係：農業食品環境資料」（Food Data Transparency Partnership: agri-food environmental data）文件

英國之社會和衛生關懷部（Department for Health and Social Care）、環境食品和農村事務部（Department for Environment, Food and Rural Affairs）、食品標準局（Food Standards Agency）於 2024 年 4 月 18 日宣布共同組織合作夥伴關係，為了支持全球對資料之需求和因應環境保護之意識，而為農業產品系統提供一致、準確之環境資料蒐集方法，藉由所蒐集之資料更能呈現設定目標之達成狀態，以及直接指出達成目標需要採取之政策，其提出以下重要之資料蒐集措施：

1. 揭示以一致、精確之方法量化和蒐集原始農業環境資料

為了蒐集具有精確性之原始資料，進而使高品質之二手資料易於取得，將透過支持溫室氣體計算工具提供者統一計算方法，鼓勵農場採取行動完成溫室氣體之審計，重新使用現有資料完成審計措施，提升整體農業系統共享資料之數量和品質，建立大規模之資料共享環境，量化供應鏈對環境產生影響之資料。

2. 揭示如何提升二手農業環境資料之價值

二手資料成為越來越重要之資源，必須確保供應鏈之企業能夠取得精確、一致、近用之二手資料，將透過整合農場之原始資料至二級資料集，強化評估資料品質之要求和機制，提升二手農業環境資料之價值。

3. 揭示如何促進資料在供應鏈中之互通性

在供應鏈各組織間無縫進行資料交換，為維護公平競爭之關鍵因素，為了防止資料被特定控制者限制傳輸至其他組

本報告之智慧財產權歸屬於國發會

織，和減輕組織轉換資料之負擔，將透過制定統一之資料交換格式，發展框架和利用 AI 技術減少資料共享之障礙。

綜合以上，食品資料透明度夥伴關係匯集了農業食品系統之參與者，透過一致、精確之農業環境資料蒐集方法，量化和共享生產過程影響環境之資料，加以應對氣候變遷的危機。

資料來源：

1. Gov.uk, Food Data Transparency Partnership: agri-food environmental data, 2024-04-23, https://www.gov.uk/government/publications/food-data-transparency-partnership-agri-food-environmental-data (last visited 2024/04/29)

三、 美國

(一)2024 年 4 月美國疾病管制與預防中心更新公共衛生資料戰略（The Public Health Data Strategy）

美國疾病管制與預防中心（The Centers for Disease Control and Prevention, CDC）於 2024 年 4 月 11 日發布更新之公共衛生資料戰略，旨在為了達成資料現代化，進一步推動相關措施，提高公共衛生系統內資料交換之速度、品質、完整性，以更好應對公共衛生之威脅和問題，藉此實現以下四項目標，包含 A 加強核心的公共健康資料 B 加快蒐集分析和自動化解決方案的存取速度，以支援公共衛生調查和促進公眾健康 C 視覺化和共享資料，為公共衛生政策提供資訊 D 促進公共衛生資料更加開放和提高互通性。

CDC 將依序逐步執行所訂定之計畫項目和採取對應之措施：

1. 加強核心的公共健康資料

本報告之智慧財產權歸屬於國發會

提升醫療機構提供病患電子病歷（eCR）予公共衛生組織、CDC 傳染病實驗室及提供電子檢測報告予州公共衛生實驗室之比率，要求公共衛生實驗室和醫療機構針對檢測項目合作。

2. 加快蒐集分析和自動化解決方案的存取速度

將使更多農村小型醫療機構採用電子病歷系統，並由 CDC 持續建置和改善現代化國家電子疾病監測系統(National Electronics Disease Surveillance System Base System）政策。

3. 視覺化和共享資料

跨大研發、使用視覺化與共享之核心資料範圍，例如國家層級資料、跨個案病例之整合視覺資料、死亡率與就診率，並透過同一平臺提供前述資料給民眾。

4. 促進公共衛生資料更加開放和提高互通性

基於可尋性（Findability）、可存取性（Accessibility）、互通性（Interoperability）、重複使用（Reuse）原則增加所發布之公共衛生資料集數量，以及根據美國互通性核心資料 (USCDI) 和 USCDI+標準，公布公共衛生資料集的資料元素、維護和更新清單的流程。

資料來源：

1. CDC, The Public Health Data Strategy, 2024-04-11, https://www.cdc.gov/ophdst/public-health-data-strategy/index.html?_cid-lbr-lm#milestones-build-2023 (last visited 2024/04/22)
2. Govciomedia, CDC Updates Public Health Data Strategy, 2024-04-12, https://govciomedia.com/cdc-updates-public-health-data-strategy/ (last visited 2024/04/22)

本報告之智慧財產權歸屬於國發會

四、 新加坡

(一)2024 年 4 月新加坡網路安全局（CSA）對先前針對《網路安全法草案》之公開徵詢意見作出回應

2024 年 4 月 2 日，新加坡網路安全局（Cybersecurity Agency of Singapore, CSA）針對其在 2023 年 12 月 15 日至 2024 年 1 月 15 日期間，對《網路安全法草案》（Cybersecurity Bill）之公開徵詢意見發布了回應。本次草案為自 2018 年《網路安全法》（Cybersecurity Law）頒布以來之首次修訂，旨在因應最新之網路威脅與商業環境發展，要求關鍵資料基礎設施（Critical Information Infrastructure, CII）擁有者對更廣泛範圍之事件作通報，包含供應鏈中發生之事件。本次草案亦擴大了監管範圍，涵蓋了更多企業類型，例如基礎數位設施（Foundational Digital Infrastructure, FDI）、必要服務提供者（Providers of Essential Services, PES）、特別網路安全組織（Entities of Special Cybersecurity Interest, ESCI）、臨時網路安全關注系統（Systems of Temporary Cybersecurity Concern, STCC）等網路資訊安全相關組織。目前 CSA 獲得之產業回應重點大致如下：

1. CII 相關修訂：此部分反饋主要集中在三個方面：

   (1) 使用分散式系統架構監管 CII 擁有者（例如商用雲端解決方案）或運算服務供應者，是否會為 CII 擁有者或其供應商產生額外法定義務。

   (2) CII 擁有者和 PES 業者可能面臨更高的管制成本，因為義務增加，例如事件報告及需要獲得具有法律約束力之承諾。

   (3) 修訂後的法案將如何實施，包括 PES 的指定程式以及網路安全專員進行現場檢查之權力範圍。

本報告之智慧財產權歸屬於國發會

2. PES 業者合法協議之獲取

有關於 PES 與其運算服務供應商如何獲取外包 CII 合法使用協議之疑慮，以及如果 PES 無法獲得此類協議，監管機構是否會要求 PES 停止使用外包 CII。於現場查驗之公權力方面，類似於 CII 業者之疑慮，應對專員執行現場勘查時之權力明確規定，以防止權力濫用。

3. FDI 業者之反饋：大致上，FDI 業者支持本次相關修訂，包含認可對外國基礎設施投資者之監管，然對於監管範圍仍有疑慮；哪些團體應被視為 FDI，以及如何確保這些團體的安全。

4. ESCI 與 STCC 業者之反饋：類似 FDI 業者之疑慮，ESCI 與 STCC 業者亦希望能更明確地規定符合該項服務之要件。

針對以上產業反饋，CSA 大致作出以下回應：

1. 針對 CII 相關之修訂，CSA 明確表示，CII 擁有者將繼續對其控制和擁有的系統負責。須對於虛擬電腦運算系統制定其他條款，以釐清 CII 中誰擁有明確之操控權與其他安全管理任務，進一步確認設施之實際擁有者。而關於監管成本，CSA 將努力管理 CII 擁有者的成本負擔，包括發展實用的事件報告操作方法。

2. 關於 FDI 和 ESCI、STCC 的實施：CSA 將進一步澄清如何實施對 FDI 和 ESCI 的規範，並將與行業持續進行諮詢，以確保實施的有效性。

整體而言，各類網路資料安全業者明確地點出了其對於本次草案，包含各類型資料業者之定義是否明確等疑慮，然而 CSA 之回應，除了虛擬電腦運算系統方面將制定新條款，其他方面為較概括式回應，可持續觀察後續是否對本次草案持續修訂。

本報告之智慧財產權歸屬於國發會

資料來源：

1. Singapore Statutes Online, Cybersecurity (Amendment) Bill, 2024-04-03, https://sso.agc.gov.sg/Bills-Supp/15-2024/Published/20240403?DocDate=20240403 (last visited 2024/05/13)

2. Microsoft Start, New bill passed to strengthen SG's digital defenses, 2024-05-08, https://www.msn.com/en-sg/news/other/new-bill-passed-to-strengthen-sgs-digital-defenses/ar-BB1m1tQm#:~:text=The%20bill%20mandates%20stricter%20reporting%20requirements%20for%20owners,Amendment%20Bill.%20%E2%80%9CThis%20bill%20will%20strengthen%20our%20national (last visited 2024/05/13)

3. CSA SINGAPORE, Public Consultation on the Cybersecurity (Amendment) Bill, 2024-04-02, https://www.csa.gov.sg/legislation/consultations/public-consultation-on-the-cybersecurity-(amendment)-bill (last visited 2024/05/13)

4. Privacy World, Singapore Progresses Towards Amended Cybersecurity Law, 2024-04-19, https://www.privacyworld.blog/2024/04/singapore-progresses-towards-amended-cybersecurity-law/ (last visited 2024/05/13)

五、 中國大陸

(一)2024 年 4 月中國大陸信息通訊研究院發布數位政府一體化建設白皮書

為加入數位政府一體化建設落地，中國大陸信息通訊研究院所發布之數位政府一體化建設白皮書（簡稱白皮書）提出「1122」之整體建設框架：以 1 機制為驅動；以 1 執行業務場景為牽引；以政務資料、平臺支持作為 2 大支持；以維護營運、資安為 2 大保障。

本報告之智慧財產權歸屬於國發會

白皮書數位政府強調線上線下服務管道一體化，以電腦端、應用程式一體服務的聯動模式，整合橫向的跨域公共服務資料。白皮書指出中國大陸已有 31 省以建設省級政務服務移動端，並與中國大陸政務服務平臺行動端對接資料。超過 70%的地級市建置政務平臺，將政務資料數位化。

白皮書說明目前在逐步建置政務巨量資料平臺,目標為建設 32 個省級和 n 個國務院有關部門政務資料平臺，推動政務資料整合互通。截至 2023 年 8 月,中國大陸地方政府開放供下載的資料集數量從 2019 年的 15 億成長至 2023 年逾 480 億。比如浙江通過分析公共資料、社會資料，打造安迅應急救援項目，1 分鐘報警、3 分鐘出警、15 分鐘警方到場救援的高速道路及都市道路救援機制。

白皮書指出高品質的政務資料為推動數位政府的關鍵，需透過 3 步：

1. 統一規劃部署制度

   如全國一體化政務大數據體系建設指引等相關政策要求。

2. 編列全國一體化資料資源目錄

   各地政府需加強溝通,持續於目錄更新已有的政務資料。

3. 發展資料源頭治理方案

   建立一致性、可行之資料標準規範體系,明確目錄規範、分類規範、原始資料規範等,發展資料生命週期管理方案,透過涵蓋資料蒐集、儲存、加工、應用、更新之資料生命週期,以及定期評估資料品質，建立資料品質監管機制，提升資料風險之應對能力。

資料來源：

本報告之智慧財產權歸屬於國發會

1. 中國大陸信息通訊研究院，数字政府一体化建设白皮书（2024年），http://www.caict.ac.cn/sytj/202404/t20240401_474827.htm，2024-04-01，（最後瀏覽日：2024/05/03）

六、 西班牙

(一)2024 年 4 月西班牙數位轉型與公共服務部發布「創建示範中心與發展資料空間補助金公告」

西班牙數位轉型與公共服務部（El Ministerio para la Transformación Digital y de la Función Pública）透過數位化與 AI 國務秘書處（La Secretaría de Estado de Digitalización e Inteligencia Artificial）於 2024 年 1 月在西班牙國家官方公報（Boletín Oficial del Estado）上發布「創建示範中心與發展資料空間補助金公告」，鼓勵國內各單位深化和精進資料治理實力。這項計畫的主要目標是透過以補助金作為鼓勵，推動西班牙國家整體數位轉型，並促進資料經濟發展；總預算為 1.5 億歐元，最高補助額為每個項目 500 萬歐元、最低 30 萬歐元。這項補助金計畫的主要目標如下：

1. 促進於策略產業業界建立資料交換系統
2. 消弭資料交換的近用障礙
3. 創建必要的基礎設施並組織資料營運空間
4. 促進基於資料開發之創新商業模式

補助金申請細節如下：

1. 申請時程：申請時程為 2024 年 4 月至 2024 年 5 月 16 日，以獲得申請單位創建或精進數位技術所需的資金。

本報告之智慧財產權歸屬於國發會

2. 申請條件：專案必須在 2025 年 12 月 31 日之前完成；可申請者包括公部門、民間企業、研究機構、通訊單位、學術組織及其他相關實體，但不包括旅遊部門；必要條件是在歐盟內有稅務居所，並在西班牙境內有設立分支機構。

此一補助機制，屬於西班牙「部門資料空間計畫」（El Programa Espacios de Datos Sectoriales）落實之一部分，促進經濟戰略相關部門資料空間之發展。策略上與歐洲資料戰略（Estrategia Europea del Dato）、歐洲資料治理法規（los Reglamentos Europeos de Datos y de Gobernanza de Datos）以及單一資料市場（el Mercado Único del Dato）的目標一致。

資料已成為經濟成長、創造就業機會和社會進步的關鍵，數位化是社會和企業的發展重點。資料分析有助於流程及決策的最佳化、創新以及預測。此全球趨勢在健康、環境、糧食安全、氣候、能源、交通系統，以及智慧城市等各領域都具有巨大潛力。

歐盟執行委員會在 2017 年 1 月發布的《建構歐洲資料經濟的通訊》中將資料經濟描述為由製造商、研究人員和基礎設施提供者等不同類型的市場參與者組成的生態系統，透過合作確保資料是可近用的。這些資料市場參與者可以透過創建各種具有改善人們日常生活潛力的應用程式來從資料中提取價值。

資料來源：

1. Financiado por la Unión Europea / MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA, Lanzada la convocatoria de ayudas para la creación de Espacios de Datos Sectoriales, 2024-04-15, https://espanadigital.gob.es/actualidad/lanzada-la-convocatoria-de-ayudas-para-la-creacion-de-espacios-de-datos-sectoriales (last visited 2024/04/24)
2. MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA, El Ministerio para la Transformación

本報告之智慧財產權歸屬於國發會

Digital y de la Función Pública lanza la convocatoria de ayudas para la creación de Espacios de Datos Sectoriales, 2024-04-15, https://portal.mineco.gob.es/es-es/comunicacion/Paginas/20240415-Ministerio-Transformacion-Digital-Funcion-Publica-lanza-convocatoria-ayudas-creacion-Espacios-Datos-Sectoriales.aspx (last visited 2024/04/24)

貳、AI 法制政策

一、歐盟

(一)2024 年 5 月歐盟理事會通過首部人工智慧法案（Artificial Intelligence Act, AIA）

歐洲議會與歐盟理事會先前於 2023 年 12 月對 AIA 草案內容達成暫時協議，歐盟理事會接續於 2024 年 5 月 21 日批准人工智慧法草案，並將於 2026 年起實施人工智慧法。該法旨在促進私人和公共行為者在歐盟單一市場上開發及採用安全、值得信賴的 AI 系統，確保尊重歐盟公民的基本權利，刺激歐洲 AI 的投資及創新。同時為 AI 監管奠定全球的典範，採用以風險基礎之監理原則進行立法，即 AI 對社會造成危險的風險越高，受到管制就越趨嚴格。人工智慧法依據風險對 AI 進行分類，分為四種類型：不可接受風險（unacceptable risk）、高風險（high risk）、有限風險（limited risk）、最小風險或無風險（minimal or no risk）。此次批准之立法包含以下重要內容：

1. 依風險分類 AI 系統

風險有限的 AI 系統只需履行較輕的透明度義務，而高風險的 AI 系統則必須獲得授權，且滿足法令要求及義務方能進入歐盟市場。例如，操縱認知行為和社交評分等目的之 AI 系統，由於其風險被歸類為不可接受，故將被禁止進入歐盟市場。此外，還禁止將 AI 用於以相貌為基礎之預測性服務，以

本報告之智慧財產權歸屬於國發會

及使用生物辨識系統對自然人根據其種族、宗教或性傾向等特定類別進行分類。

2. 通用型 AI 模型之限制

該法涉及通用型 AI 模型使用之監管，不構成系統性風險的通用型 AI 模型將受到有限的限制，例如透明度的要求，但存在系統性風險的 AI 模型則必須遵守更嚴格的限制。

3. 新的治理架構

為確保適當執法而須設立多個治理機關。例如，在歐盟執委會內設立 AI 辦公室，負責在歐盟範圍內執行相關之共同規則；由獨立專家組成科學小組為執法活動提供支持；由會員國代表組成 AI 委員會，就 AI 執法的一致性及有效實施向歐盟委員會和會員國提供建議和協助。

4. 罰則

若公司違反人工智慧法之規定將受到裁罰，該法案所設定之裁罰基準為違法公司之上一財政年度全球年營業額的一定百分比或者預定金額，並以較高者為準，而中小型企業和新創企業將按比例被處以行政罰鍰。

5. 透明度和基本權利之保護

提供公共服務的組織於部署高風險 AI 系統之前，需要評估系統對基本權利之影響。此外，法案另規定需提高開發和使用高風險 AI 系統的透明度，高風險 AI 系統的使用者將需要在歐盟高風險 AI 系統資料庫中為登記。

6. 支持創新之措施

本報告之智慧財產權歸屬於國發會

該法提供了有利於創新的法律框架，旨在促進循證之監管學習，並且預見 AI 監理沙盒可為創新型 AI 系統的開發、測試和驗證提供受控之環境，允許與真實世界相同之條件下測試創新 AI 系統。

綜合以上，歐盟理事會完成批准人工智慧法，經歐洲議會和歐洲理事會主席簽署後，該法案已於 6 月 13 日頒布，預計 7 月在歐盟官方公報上公告，並於公告 20 天後生效，於生效 2 年後開始適用。

資料來源：

1. Council of the EU, Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI, 2024-05-21, https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/ (last visited 2024/05/23)
2. Council of the EU, Artificial intelligence, https://www.consilium.europa.eu/en/policies/artificial-intelligence/ ,2024-05-21, (last visited 2024/05/23)

二、英國

(一)2024 年 4 月英國司法部提出《網路安全法》修正草案，提案將藉由深偽技術製作不實性影像之行為列為刑事犯罪

伴隨 AI 技術不斷演進，導致近年各式「以假亂真」的深偽影像散見於社群媒體各角落，被害人肖像遭有心人士「移花接木」的現象層出不窮，部分技術現足以完全實現「換臉」的效果，此中往往又以女性被害人居多，促使主管機關祭出相關規定嚴加防範。英國司法部於 2024 年 4 月 15 日提出《網路安全法》（Online Safety Bill, OSB）修正草案，將針對行為人於未經他人同意，無故利用他人肖像，並透過深偽技術等電腦合成或其他科技方法偽造關於他人不實性影像之行為列

本報告之智慧財產權歸屬於國發會

為刑事犯罪，若有散布、播送、交付、公然陳列或以他法供人觀覽其性影像者，最高將被處以監禁之刑罰，且本罪所科罰金未設有上限；另行為人縱然沒有散布或播送以供他人觀覽之意圖，其生成之深偽影像僅須客觀上有足以引起性慾、羞恥或損害他人名譽為目的，即有本罪之適用。

英國早在 2021 年即將行為人以脅迫、恐嚇或其他違反本人意願之方法散布性私密影像的行為刑罰化，但行為人須有滿足性慾或損害他人名譽之意圖始該當本罪；至於涉及深偽影像部分，則在去年英國 OSB 的修正草案遂將任何形式之散布行為入罪，即便無滿足性慾或損害他人名譽之意圖，只要行為人有「未經當事人同意」的情事發生，法院即可對行為人處以最高 6 個月之徒刑，而本次修正乃經由刑事司法法案（Criminal Justice Bill, CJB）之形式提出，擴充既有妨害性隱私樣態的應罰性，主要針對行為人製造合成不實性影像之行為，目前正由國會進行審議，該草案之重點摘述如下：

1. 草案新增之罪行乃針對被害之成年人，只要未經其同意而無故利用深偽技術等科技方法將其肖像合成不實性影像，即能成立本罪，若是以上開技術生成未成年人的性影像則已位列其他相關兒少保護法案中的犯罪行為態樣，故不納入本次修正草案之範疇。

2. 根據草案規定，此類深偽性影像內容涉及裸體影像等色情圖文即足當之，影像中是否有正為性交者在所不問，只須客觀上呈現出足以引起性慾或羞恥之身體隱私部位或行為，以及其他與性相關而客觀上足以引起性慾或羞恥之內容。

3. 起訴被告後，檢方應證明行為人製作不實性影像之行為足以對他人心理狀態或生活造成不利影響，且主觀上係以「強暴脅迫、滿足性慾、貶抑他人名譽、損害他人之名譽人格或造成他人精神上痛苦」為目的，並逾越社會上一般人可以忍受的

本報告之智慧財產權歸屬於國發會

範圍，始能以本罪相繩，且舉證責任之門檻須達「無合理懷疑」（beyond reasonable doubt）之程度。

4. 按舊法規定，散布深偽性私密影像原本最高僅可被處以 2 年之徒刑（註：若有上開所述之意圖為前提要件），若修正草案審議通過，行為人日後倘有違犯前階段的製作生成及後階段的散布行為者，審判時便能同時以兩罪處斷，無法僅從較重之罪論處，故法案修正通過後將加重對行為人製作及散布不實性影像之處罰。

資料來源：

1. GOV.UK, Government cracks down on ‘deepfakes’ creation, 2024-04-16, https://www.gov.uk/government/news/government-cracks-down-on-deepfakes-creation (last visited 2024/05/14)
2. BBC News, Creating sexually explicit deepfakes to become a criminal offence, 2024-04-16, https://www.bbc.com/news/uk-68823042 (last visited 2024/05/14)
3. BABL News, UK Government Introduces Crackdown on ‘Deepfakes’ Creation, 2024-04-23, https://babl.ai/uk-government-introduces-crackdown-on-deepfakes-creation/ (last visited 2024/05/14)

(二)2024 年 4 月英國藥物及保健品監管局發布 AI 監管策略 (AI regulatory strategy)

英國藥物及保健品監管局（Medicines and Healthcare products Regulatory Agency, MHRA）遵循先前於 2023 年發布之 AI 監管的支援創新方法（Pro-innovation approach to the regulation of AI），於 2024 年 4 月 30 日發布 AI 監管策略 (AI regulatory strategy)，考慮 AI 所帶來之機遇和風險，且 AI 已確立為 2030 年之國家優先發展技術，提出監管醫療產業使用 AI 之方法，確保病患之安全與促進產業之創新，其中該

本報告之智慧財產權歸屬於國發會

策略涵蓋之原則包含有安全性（safety）、保障性（security）、穩健性（robustness）；適當的透明度（appropriate transparency）和可解釋性（explainability）；公平性（fairness）；可問責（accountability）和治理（governance）；可競爭性（contestability）及補救措施（redress），以下說明各原則之意涵：

1. 安全性、保障性、穩健性：

   在整個 AI 生命週期中，AI 系統應以穩健、安全和可靠的方式運行，並應不斷識別、評估和管理風險。

2. 適當的透明度和可解釋性：

   AI 系統應具有適當的透明度和可解釋性。

3. 公平性：

   AI 系統不應損害個人或組織的權利，對個人為不公平的歧視，或造成不公平的市場結果。

4. 可治理和問責：

   應制定治理措施，確保對 AI 系統的供應和使用有效監督，並在整個 AI 生命週期建立明確的問責關係。

5. 可競爭性和補救措施：

   在適當情況下，使用者、受影響的合作企業和 AI 生命週期中的參與者應能夠對有損害或造成重大損害風險的 AI 決策或結果提出異議。

此外，MHRA 將從監管醫療器材到作為監管機構如何使用 AI 運作和決策面向改革和推動作為，在監管醫療器材方面，調整現有的醫療器材監管框架，繼續採用基於風險的醫療器材分類系統，提升 AI 產品之分類；特別關注機器學習醫療器材（AIaMD），推動 AIaMD 之監

本報告之智慧財產權歸屬於國發會

管沙盒，發布相關之機器學習開發指導原則；在 MHRA 使用 AI 運作和決策方面，將採取措施利用 AI 的機遇，提高公共服務機構的績效，進而做出影響公眾和病患安全的關鍵決策，例如，使用監督式之機器學習對作為申請上市許可的文件進行初步評估，以減少早期評估階段投入的人力資源；探索生成式 AI 和大型語言模型在醫療監管中可發揮的作用，以及蒐集和分析資料的方法。

資料來源：

1. GOV.UK, MHRA's AI regulatory strategy ensures patient safety and industry innovation into 2030, 2024-04-30, https://www.gov.uk/government/news/mhras-ai-regulatory-strategy-ensures-patient-safety-and-industry-innovation-into-2030 (last visited 2024/05/09)
2. JD Supra, UK MHRA Publishes AI Regulatory Strategy, 2024-05-02, https://www.jdsupra.com/legalnews/uk-mhra-publishes-ai-regulatory-strategy-1540644/ (last visited 2024/05/09)

(三)2024 年 5 月英國 ICO 於 4 月底發布人工智慧治理策略（Regulating AI：the ICO’ s Strategic Approach）

英國資訊委員辦公室（Information Commissioner's Office, ICO）於 2024 年 4 月 30 日發布人工智慧治理策略（Regulating AI：the ICO’ s Strategic Approach），ICO 闡述了過去如何推動 2023 年人工智慧監管白皮書中的原則以及提出未來有關這些原則的實施指導意見。

該策略包含以下重要的內容方針：

1. ICO 有可能成為事實上（de facto）的 AI 監管者

ICO 在此策略中指出，先前之人工智慧監管白皮書提出的許多原則與現有的資料保護原則相一致，例如透明度、公平性和問責制之原則，資料保護法規也適用在技術開發的各

本報告之智慧財產權歸屬於國發會

個環節，因此，ICO 有能力利用隱私保護之原則監督 AI 技術在 AI 生命週期的所帶來的挑戰，從而 ICO 有可能成為事實上的 AI 監管機構。

2. 以務實和注重風險之原則為總體推動方法

在該戰略中，ICO 認為 AI 有巨大的潛在利益，但也指出了具有相關的內在風險，且許多風險源自於業者開發和部署 AI 系統階段之使用資料，又 ICO 在該策略中明確表示，其並不尋求 AI 得以完全遵守英國資料保護法，該組織將是一個務實、注重風險的監管機構，若開發者進行資料隱私影響評估並採取了適當的保障措施，開發者將可以嘗試和開發 AI。

3. 必要時將採取強制之執行活動

ICO 明確表示將採取行動執行資料保護法，並特別提到近期的罰鍰和執法案例，涉及臉部識別技術的使用和兒童資料的保護，雖然支持創新和實用主義，但某些原則不容被忽視。

4. AI 是 ICO 的重點關注領域

AI 是 ICO 於 2024 年至 2025 年的重點關注領域之一，此策略提及 ICO 將確保英國負責任地採用 AI 和遵守資料保護規定，以及加強對該技術的認識而採取的措施，例如，資料使用之審查、監管沙盒計畫。

5. 與其他監管機構的合作關係和公開對話至關重要

ICO 在該策略中強調監管機構之間的積極參與和合作對於全面應對 AI 挑戰至關重要，例如，由 ICO 召集競爭及市場管理局（Competition and Markets Authority, CMA）、通訊管理局（Office of Communication）和金融行為監理局（Financial

本報告之智慧財產權歸屬於國發會

Conduct Authority, FCA）參加論壇，建立一致的監管方法，促進監督和執法的一致性。

而論壇進一步建立的 AI 和數位中心（AI and Digital Hub）加強了合作關係，為創新者提供了平臺使其能夠駕馭多個公部門的監管問題，此外，還成立監管機構與 AI 工作組，促進各監管機構和當局之間對話。

英國政府將對前開策略與其他監管機構提供的戰略一併進行審查，以確定英國是否需要獨立制定或修訂 AI 之立法。

資料來源：

1. JD Supra, The UK ICO Publishes Its Strategy on AI Governance, 2024-05-13, https://www.jdsupra.com/legalnews/the-uk-ico-publishes-its-strategy-on-ai-3228063/ (last visited 2024/05/23)
2. Information Commissioner Office, Regulating AI: the ICO's strategic approach - a response to the DSIT Secretary of State, 2024-04-30, https://ico.org.uk/about-the-ico/consultations/regulating-ai-the-icos-strategic-approach-a-response-to-the-dsit-secretary-of-state/ (last visited 2024/05/23)

(四)2024 年 5 月英國科學、創新及技術部公告徵求 AI 網路安全的意見

英國科學、創新及技術部（Department for Science, Innovation & Technology）於 2024 年 5 月以公告徵求 AI 網路安全的意見，該部門考量目前使用 AI 的組織沒有 AI 的網路安全實踐或程序，故必須確保設計、開發、部署及維護 AI 之安全，而提出 AI 網路安全的計畫，向公眾徵求此計畫之意見。又該計畫係以自願行為準則之形式，為 AI 供應鏈中的相關參與者提供 AI 安全標準，以下說明該計畫之重要內容：

本報告之智慧財產權歸屬於國發會

1. 該計畫係基於自願行為準則和全球標準兩項措施解決 AI 的網路安全風險，並依據自公眾徵集之意見，最終確定自願行為之標準並依此推動全球標準。

2. 該自願行為準則指出利害關係人之範圍及利害關係人負責實施之實踐原則

   (1) 以「開發商」(Developers）為例，其定義指任何部門之企業或組織以及負責創造 AI 模型或系統的個人，例如，向客戶和最終使用者提供 AI 軟體之供應商。

   (2) 自願行為準則制定數項利害關係人間應實施之準則，包含有安全設計（Secure Design）、安全開發（Secure Development）、安全維護（Secure Maintenance）等基礎原則，再個別延伸子原則。

   例如，以安全設計為例，個別延伸之子原則包含提高員工對威脅和風險的認知、設計系統時考慮安全性以及功能和性能、對系統面臨的威脅進行建模等子實施原則。

綜合以上，英國科學、創新及技術部於 2024 年 5 月至 8 月進行意見徵求程序，並鼓勵利益相關者提供與預定實施措施相關的財務和影響資訊。

資料來源：

GOV.UK, Call for views on the Cyber Security of AI, 2024-05-24, https://www.gov.uk/government/calls-for-evidence/call-for-views-on-the-cyber-security-of-ai/call-for-views-on-the-cyber-security-of-ai#how-to-respond-to-the-call-for-views-and-our-next-steps, (last visited 2024/06/06)

本報告之智慧財產權歸屬於國發會

三、美國

(一)2024 年 3 月美國田納西州《確保肖像、聲音和圖像安全法案》要求第三方若利用生成工具重製肖像、聲音或圖像應得本人之事前同意

作為鄉村音樂發源地的美國田納西州，有著蓬勃的音樂產業，匯聚來自各路的表演藝術工作者，因而對相關從業者的個人公開權（Right of Publicity）保障尤為重視，早在 1984 年即制訂《個人權利保護法》（Personal Rights Protection Act），確保該權利不會因權利人死亡而消滅，屬於可由他人繼承之財產權，允許繼承人自由轉讓和授權，包含其姓名（Name）、肖像（Image）、形象（Likeness）之權利主張，但被繼承人之聲音仍不在權利主張的範疇。

惟現今 AI 深偽仿聲技術所生成之音樂亦可能侵害音樂人及藝術家的智慧財產權，因而於 2024 年 3 月 21 日由州長簽署《確保肖像、聲音和圖像安全法案》（Ensuring Likeness Voice and Image Security Act），簡稱貓王法案（ELVIS Act），該法案於 3 月 7 日獲得州議會兩黨一致支持，首度明確將個人公開權得主張之範圍擴及至表演者的聲音（NIL+V），其目的是為了應對 AI 生成音樂的突破性進展，以保護音樂創作人及表演藝術家之權利免受 AI 技術侵害，這是全美首部禁止他人未經授權使用或重製權利人的聲音以供訓練 AI 模型或生成深偽內容所制定的法律（註：加州雖已將聲音作為權利保護客體但非針對 AI 技術之侵害），明確規定第三人在未得本人之同意下，若意圖利用 AI 深偽技術生成經仿製、偽造或變造的圖片、影音、聲音等數位檔案，而後續冒用本人名義進行公開發表或公開演出詞曲創作人及表演藝術工作者之聲音或影像的行為，則須承擔相應的民事侵權行為責任，以及構成歸類在微罪的刑事犯罪，刑期最高可處 11 個月又 29 天的監禁或 2,500 美元以下的罰金，該法案預計於今年 7 月 1 日生效，且僅適用於在田納西州境內的工作者。

本報告之智慧財產權歸屬於國發會

該法案所保護之主體除音樂創作人及表演藝術家外，亦包含動畫配音員及串流媒體盛行下廣播與網路節目的播音員（俗稱播客），以確保這類主要仰賴聲音維生的工作者能免於 AI 仿聲技術而減損其專業價值；另外若有與詞曲創作人或表演藝術工作者締結專屬合約之唱片公司或經紀公司亦為訴訟程序的適格當事人，可代理公司旗下的工作者尋求救濟管道；最後，若利用權利人的姓名（Name）、肖像（Image）、形象（Likeness）或聲音（Voice）屬於法案中列舉的合理使用行為，如基於公益目的、新聞播報、轉化性使用、偶然入鏡或著作之附帶性利用等，則應屬美國憲法第一修正案之保障範圍而非在該法案的規範射程。

除田納西州之外，美國尚有其他 39 個州提出或正在推動相似的法案，但全美目前仍欠缺統一性的立法；聯邦政府仍尚在研擬如何保護表演藝術工作者個人公開權的階段，日前在田納西州政府今年 1 月時提出貓王法案的草案後不久，由美國眾議院議員組成的跨黨派小組曾公佈「禁止 AI 偽造和未經授權的重製法案」(「禁止 AI 詐欺法案」)，旨在推動建立聯邦層級的框架性立法，以確保個人的聲音或肖像權屬美國憲法第一修正案的保障範圍，而該提案據稱是針對美國參議院去年 10 月提出的「鼓勵原創、培育藝術和維繫安全娛樂法案」(「禁止仿冒法案」) 的更新及補充，以維護公共利益，創造具有原創性、正當性及安全性的休閒娛樂環境。

資料來源：

1. JD Supra, First-of-Its-Kind AI Law Addresses Deep Fakes and Voice Clones, 2024-04-02, https://www.jdsupra.com/legalnews/first-of-its-kind-ai-law-addresses-deep-9596588/ (last visited 2024/04/15)
2. Billboard, Tennessee Adopts ELVIS Act, Protecting Artists' Voices From AI Impersonation, 2024-03-21, https://www.billboard.com/business/legal/tennessee-elvis-act-protecting-artists-voices-ai-impersonation-1235637934/ (last visited

本報告之智慧財產權歸屬於國發會

2024/04/15)

3. Music Business Worldwide, ELVIS ACT SIGNED INTO LAW IN TENNESSEE TO PROTECT ARTISTS' VOICE AND LIKENESS FROM THE MISUSE OF AI, 2024-03-21, https://www.musicbusinessworldwide.com/elvis-act-signed-into-law-in-tennessee-to-protect-artists-voice-and-likeness-from-the-misuse-of-ai/ (last visited 2024/04/15)

(二)2024 年 4 月美國賓州眾議院修正《不公平貿易行為和消費者保護法》，增加 AI 內容揭露責任

美國賓州眾議院認為人民有權利知悉其接收之內容是否為 AI 所創造，並認為 AI 技術日益複雜，難以驗證內容之創作素材與作者。且 AI 生成內容之真實性值得懷疑，可能傳播虛偽不實的訊息或內容，使人民受到 AI 所欺騙。故美國賓州眾議院於 2024 年 4 月 11 日透過修正《不公平貿易行為和消費者保護法》（Unfair Trade Practices and Consumer Protection Law），以期促進 AI 之揭露。本次修正要求，當事業使用 AI 協助生成文字、圖像、聲音或影音內容時，應向消費者進行清晰且明顯的揭露。將事業使用生成式 AI 之揭露責任明確化，以防止消費者受到內容誤導，並協助其作出合理決定，例如應標示以 AI 生成的新聞內容。

資料來源：

1. Pennsylvania General Assembly, Regular Session 2023-2024House Bill 1598, 2024-04-11, https://www.legis.state.pa.us/cfdocs/billInfo/billInfo.cfm?sYear=2023&sInd=0&body=H&type=B&bn=1598 (last visited 2024/04/18)

2. Statescoop, Pennsylvania AI disclosure bill advances to state Senate, 2024-04-11, https://statescoop.com/pennsylvania-ai-disclosure-legislation/ (last visited 2024/04/18)

3. Fastcompany, 'Buyer beware,' Pennsylvania bill would require

本報告之智慧財產權歸屬於國發會

consumers to be notified of AI-generated content, https://www.fastcompany.com/91090907/buyer-beware-pennsylvania-bill-would-require-consumers-notified-ai-generated-content, 2024-04-11 (last visited 2024/04/18)

(三)2024 年 4 月美國專利商標局發佈關於在實務中使用基於 AI 的工具的指引

美國專利商標局(USPTO)於 2024 年 4 月 11 日發佈《美國專利商標局關於在實踐中使用基於人工智慧的工具的指引》(Guidance on Use of Artificial Intelligence-Based Tools in Practice Before the United States Patent and Trademark Office)。該指引旨在向從業人員及公眾說明，專利及商標專業人士、發明創新者及事業在利用 AI 向美國專利商標局處理事務時，所必須關注之重要事項：

1. 誠信義務(duty of candor and good faith)：向 USPTO 提交專利申請時負有誠實及善意的義務，其中包括向主管機關揭露個人已知悉關於影響「可專利性」（Patentability）等之重要資訊的義務。對主管機關實施或意圖進行欺詐或因惡意或故意不當行為而致違反申請時的揭露義務，將不予核准通過專利申請。故參與專利申請之相關人員有義務揭露對於「可專利性」中有關實用性、新穎性、可進步性的所有重要資訊，包括發明人、當事人和業者使用 AI 工具的資訊。

2. 資訊保密：業者應盡合理之注意，防止無故或未經授權揭露或未經授權存取與客戶代表有關的資訊。因此，從業人員必須採取措施維護客戶資訊的機密性，包括採取合理措施防止無故和未經授權之揭露。美國專利商標局關於利益衝突的從業行為規範通常禁止從業人員使用與客戶（或前客戶）代表有關的資訊，以損害該客戶的利益。使用 AI 系統進行現有技術檢索、申請之起草等可能會導致通過這些系統的擁有者偶

本報告之智慧財產權歸屬於國發會

然向第三方揭露客戶敏感或機密資訊,從而對客戶造成傷害。故指引旨在提醒業者或法務等相關人員必須注意保護客戶之資訊,並注意使用 AI 系統時有可能涉及敏感及機密客戶資訊。

3. 出口限制：專利從業人員在向國外提交任何專利申請或為準備、提交或可能提交及審理外國申請而出口技術數據之前，必須遵守外國申請許可要求。指引列舉使用 AI 工具可能涉及的國家安全、出口管制和外國申請許可問題，特別是當 AI 工具可能使用位於美國境外的伺服器時，將可能增加數據輸出至美國以外之可能性，違反出口管制或國家安全相關規定。

4. 專業責任：美國專利商標局從業行為規範要求從業人員對客戶負有善良管理人之注意義務。故在使用 AI 時，從業人員須確保其未違反對客戶之義務，例如具備必要的專業知識始能本於代理人之地位為客戶提出申請。

指引自 2024 年 4 月 11 日起適用。它不僅提醒應注意使用 AI 的風險，也提醒如何保護現有 USPTO 之生態系統內，申請或使用上 AI 免受潛在危險。此外，指引還包含了關於如何與 USPTO 的資訊技術系統互動的具體指示。

資料來源：

1. USPTO, Guidance on Use of Artificial Intelligence-Based Tools in Practice Before the United States Patent and Trademark Office, 2024-04-11, https://www.govinfo.gov/content/pkg/FR-2024-04-11/pdf/2024-07629.pdf (last visited 2024/04/25)

(四)2024 年 4 月美國麻薩諸塞州總檢察長發布諮詢意見，要求人工智慧開發商應遵循消費者保護法等法令

本報告之智慧財產權歸屬於國發會

隨著企業越來越廣泛增加對 AI 和演算法決策系統之使用，應用 AI 背後隱藏著黑盒子問題，並對社會和人民造成隱憂，麻薩諸塞州總檢察長辦公室（The Office of the Attorney General）於 2024 年 4 月 16 日發布諮詢意見，為 AI 開發商、供應商、企業提供指導，闡明消費者保護法（Massachusetts Consumer Protection Act）、反歧視法（Anti-Discrimination Law）、個人資料保護標準（Commonwealth’s Standards for the Protection of Personal Information of Residents of the Commonwealth）等現有相關法令之適用範圍，旨在解決和降低 AI 之風險，以下為該諮詢意見彙整相關法令之適用原則：

1. 依據麻薩諸塞州消費者保護法，若有以下行為可能視為違反平等互惠原則或詐欺行為：

   (1) 虛假宣傳 AI 系統之品質、可用性。

   (2) 為廣告目的，提供有瑕疵、無法使用或不切實際（impractical）之 AI 系統。

   (3) 扭曲 AI 系統之安全和可靠性，例如主張屬於全自動化系統。

   (4) 出售或使用 AI 系統之過程，當 AI 系統與其一般使用之用途不相符，或與銷售之特定用途不相符時，將違反維修保固條款及瑕疵擔保責任。

   (5) 歪曲特定個人之影音內容，以欺騙他人從事商業交易或向可信賴之第三人提供個人資料，例如用於詐欺的深度偽造或聊天機器人。

   (6) 違反麻薩諸塞州法中，與保護公共健康、安全、福利相關之法律。

本報告之智慧財產權歸屬於國發會

2. 此外，該諮詢意見亦表示法律禁止 AI 系統開發商、供應商、使用者使用具歧視個人特徵之技術，包含仰賴或使用歧視性輸入並產生歧視性結果之決策，使用具有不利於或使個人處於不利地位效果之個人特徵，可能構成詐欺行為及平等互惠原則之違反。

3. 最後，關於個人資料保護法令之遵循，AI 開發人員、供應商、使用者必須採取必要和適當之措施保護 AI 系統使用之個人資料，並遵守資料洩漏時之通知程序。

資料來源：

1. Mass.gov, AG Campbell Issues Advisory Providing Guidance On How State Consumer Protection And Other Laws Apply To Artificial Intelligence, 2024-04-16, https://www.mass.gov/news/ag-campbell-issues-advisory-providing-guidance-on-how-state-consumer-protection-and-other-laws-apply-to-artificial-intelligence (last visited 2024/04/19)

2. JD Supra, Massachusetts AG Says Consumer Protection, Civil Rights, and Data Privacy Laws Apply to Artificial Intelligence, 2024-04-18, https://www.jdsupra.com/legalnews/massachusetts-ag-says-consumer-7706167/ (last visited 2024/04/19)

(五)2024 年 5 月美國科羅拉多州長正式簽署人工智慧消費者保護法草案（AI Consumer Protection Bill）

科羅拉多州於今年(2024 年)4 月提出《人工智慧消費者保護法》，並已於 5 月由州長正式簽署，成為本年度美國 AI 立法重要發展之一，該法案預計將於 2026 年 2 月 1 日生效。本草案要求高風險之 AI 系統之開發者（developers）、部署者（deployer）採取合理之謹慎措施，以避免高風險系統的演算法歧視，主要措施如下：

本報告之智慧財產權歸屬於國發會

1. 若 AI 工具之開發者遵守以下規範，將被推定為已採取合理之謹慎措施：

   (1) 開發者向高風險系統之部署者揭露有關高風險系統的特定資訊、系統影響評估所需之資訊及文件。

   (2) 開發者發表公開聲明，向部署者說明高風險系統的類型、開發人員如何管理開發中可能出現之已知或合理可預見的演算法歧視風險，以及對相關風險系統進行調整之作法。

   (3) 於發現或收到部署者可信賴之報告後 90 天內，向總檢察長及已知之高風險系統部署者揭露任何關於該高風險系統可能造成或合理預期可能造成演算法歧視風險的資訊。

2. 若 AI 工具之部署者遵守以下規範，將被推定為已採取合理之謹慎措施：

   (1) 實施高風險系統的風險管理政策和計畫。

   (2) 完成高風險系統的影響評估。

   (3) 每年對部署者所部署之所有高風險系統情況進行稽核，以確保各該高風險系統不致造成演算法之歧視。

   (4) 若高風險系統做出影響消費者的決策，需通知消費者該特定項目。

   (5) 提供消費者得以糾正於高風險系統於作出重大決策時，所處理之任何不正確個人資料的機會。

   (6) 於技術可行之前提下，為消費者提供得透過人工審查對高風險系統產生對消費者不利之決定時申訴的機會。

本報告之智慧財產權歸屬於國發會

(7) 發表公開聲明，說明部署者當前部署之高風險系統的類型、部署者控管其部署之高風險系統之已知或合理可預見的演算法歧視風險之作法。

(8) 部署者發現演算法歧視風險的 90 天內，向總檢察長揭露高風險系統所造成或可能導致之演算法歧視風險。

而在通用 AI 模型（general purpose artificial intelligence）部分，其開發者需建立及維護通用模型之相關文件，包含符合聯邦法及州法的通用模型政策及通用模型的內容摘要，並將資料提供給通用模型之部署者，使部署者了解其功能及限制、通用模型之技術要求、訓練參數等。

如果通用 AI 模型涉及生成式內容，則開發者需負下列義務：確保「以機器可讀之方式標示」AI 系統所生成的內容並可被檢測為數位合成內容；確保開發人員的技術解決方案的有效性、互通性、可信賴。此外，本草案要求部署者向消費者揭露 AI 所生成的數位合成內容。

本草案指出擁有執行本草案權力之總檢察長及檢察官應於訴訟前，向涉嫌違反本草案者發出違規通知。如總檢察長或檢察官同意，涉嫌違法者可於 60 天內改善其違規行為。

資料來源：

1. Colorado general assembly, Consumer Protections for Artificial Intelligence, 2024-04-10, https://leg.colorado.gov/bills/sb24-205, (last visited A2024/04/15)
2. JDSUPRA, Colorado Introduces an AI Consumer Protection Bill, 2024-04-12, https://www.jdsupra.com/legalnews/colorado-introduces-an-ai-consumer-8089123/, (last visited 2024/04/15)

本報告之智慧財產權歸屬於國發會

(六)2024 年 4 月科羅拉多州參議院通過《候選人深偽技術揭露法案》，要求競選期間應予揭露 AI 生成與候選人相關之內容

隨著深偽技術不當利用之情形猖獗，且適逢本屆美國總統大選進入白熱化階段，不時有出現透過 AI 深偽仿聲技術仿造候選人言行以干預初選之情形發生，社群中大量充斥著虛實交錯的影像操縱選民如何對選情資訊的判讀與媒體識讀能力，使得短時間內所生成虛假訊息之散布速度往往迅速掩蓋事實真相之釐清過程，衝擊候選人與選民間之互信基礎，因應假訊息到處流竄成為當今選戰的變因之一。於 2024 年 4 月 24 日科羅拉多州參議院遂率先通過 HB24-1147 法案，所稱《候選人深偽技術揭露法案》即規範 AI 技術應用至任何有關競選期間候選人訊息之通訊傳播管道，不論是否來自候選人競選團隊，倘若有使用生成式 AI 產製相關內容即應主動發出揭露聲明，除能避免讓閱聽人陷於錯誤或無法分辨其真實性，並同時賦予因遭冒用而受有損害的候選人具有訴訟上的當事人適格，得提起訴訟請求財產上及非財產上的損害賠償，該法案之主要內容簡述如下：

1. 法案第一節與第二節擴張《公平競選行為法》（Fair Campaign Practices Act）原賦予聽證主持人的現有職權，對違反第三節關於惡意散布內容含有未事前揭露之欺詐成分或虛偽性質的候選人深偽影像，得依其職權處以行政處罰。

2. 針對使用深偽技術之影音創作者的揭露聲明，要求該聲明內容須非難以理解，且須使閱聽人得以明確知悉其正在觀覽深偽影像。而揭露之範圍應包括所生成內容之詮釋資料（metadata）。於技術容許的前提下提供之資料必須是永久性且無法被後續的使用者任意刪除。同時若涉及有線電視或電信網路的公開傳輸，前開揭露聲明亦須滿足由美國聯邦通訊委員會頒布的傳輸規模、存續期間、播送位置等規定。

本報告之智慧財產權歸屬於國發會

3. 該法案亦設有吹哨者條款，明定第三人就其瀏覽之內容足認達到法案第三節所列之違法情節門檻，得向州務卿辦公室進行舉發，州務卿受理檢舉人之告發後則應依法舉行聽證程序，實質調查舉報事項，並給予當事人與利害關係人到場陳述意見及提出證據之機會，程序之聽證主持人於聽取雙方論辯的結果後，再根據法案第一節與第二節賦予之權限作成裁處。

4. 候選人針對因違反揭露聲明而公開播送之深偽影像受有損害，其民事求償權得透過民事訴訟程序聲請禁制令（injunctive relief）等基於衡平法之救濟管道實現。為證明被告深度偽造欺詐或虛假訊息的真實惡意（actual malice），作為原告之候選人所負舉證責任須達證據明確（clear and convincing evidence）之門檻，始能向惡意生成深偽內容之被告請求法定損害賠償及懲罰性損害賠償，而賠償範圍亦及於期間所負擔之訴訟成本與執行法案第三節之程序所生之必要執行費用。

5. 法案第三節亦設有豁免條款，規定第三人若係在明知或因重大過失而不知該候選人的不實資訊或虛偽陳述係透過深偽技術變造之情形，因而導致其自身受有任何損害，則相對人不需額外承擔任何刑事責任。

該法案雖立意良善卻仍有規範射程過窄之批評，該州的民主黨籍州議員即指出為擴大此類操縱或干預選舉的打擊範圍，不能只限於透過生成式 AI 產生之深偽內容，應以「合成媒體」（synthetic media）一詞來含括社群媒體上運用各種技術製造出的虛假消息或錯誤資訊，如影音剪輯功能或平臺演算法的推送機制亦同樣能招致誤導閱聽人的效果發生，其影響程度並不亞於 AI 技術。另外科羅拉多州廣播協會（CBA）認為該法案中的豁免條款則在適用範疇過於狹隘，其指稱在詮釋資料的廣泛應用下，數位媒體及平臺並無足夠資源及龐大量能投入在虛假資訊的審查及深偽內容之辨識上，該法案課予數位媒體及平臺過苛的責任義務，理應將相關責任轉嫁至廣告業者上，要求相關業者嚴格徹

本報告之智慧財產權歸屬於國發會

查購買之付費數位廣告的金流來源是否意圖操控或干涉選舉而達到特定候選人當選之目的；且協會還認為目前給予數位媒體及平臺的免責空間仍不足以擺脫其面臨來自不同群體的濫訴行為，類此訴訟通常僅是競選期間各候選人陣營相互傾軋的手段策略，並無太大的實質意義，如此反倒使數位媒體及平臺暴露於不必要的法律風險中。

資料來源：

1. Colorado General Assembly, Candidate Election Deepfake Disclosures Bill (HB24-1147), 2024-04-24, https://leg.colorado.gov/bills/hb24-1147 (last visited 2024/05/10)
2. Denver Westword, Are Colorado Legislators Doing Enough to Address AI Deepfakes?, 2024-04-05, https://www.westword.com/news/colorado-lawmakers-addressing-ai-deepfakes-in-politics-20299819 (last visited 2024/04/30)

(七)2024 年 4 月美國眾議員擬提《生成式 AI 著作權揭露法案》，要求將受保護之著作物內容用於訓練模型的 AI 技術公司應履行資訊揭露義務

眾多事業組織積極投入生成式 AI 技術研發的同時，在與智慧財產領域的交互應用過程亦衍生著作權侵害之爭議，衝擊影視、音樂、創作、傳媒市場，牽動各產業諸多詞曲創作人、編劇、畫家、小說家、劇作家、出版商及新聞媒體從業人員的權益，此間已引發具體法律糾紛，如新創公司 Anthropic 在開發自家 AI 模型時，即有在未經原著作權人授權而擅自將音樂著作非法重製及散布等盜拷情勢發生，遭到多家音樂唱片公司訴請損害賠償；再如美國現有 8 家報社及媒體已向 OpenAI、Microsoft 提起訴訟，主張其未獲明示授權或支付合理報酬，而直接利用數百萬篇受著作權保護的新聞文章作為 ChatGPTAI 聊天機器人之語言模型訓練，惟這類 AI 技術公司多以「合理使用原則」(Fair Use)作為抗辯事由，且聲稱係自可公開取得的網站摘錄內容乃受

本報告之智慧財產權歸屬於國發會

美國的著作權法規保障，並表明這些有價值的原始資料僅是被用於訓練模型而非作為內容的重製或改作，此外其亦主動釋出善意，願與新聞媒體業者達成內容配送及廣告的量身訂製協議。

類此爭議層出不窮，但現階段仍有賴大量資料協助 AI 訓練以推動技術革新之需求，該如何兼顧著作權人的權益保障，並使其知悉個人產製內容可用於推動 AI 技術成長，以尋求產業創新與創作保護兩者之平衡，美國民主黨眾議員 Adam Schiff 遂於 2024 年 4 月 9 日提出《生成式 AI 著作權揭露法案》（Generative AI Copyright Disclosure Act of 2024），確保開發者能公平且負責任地使用 AI 技術，維護著作權人在邁入 AI 創造力時代之研究貢獻、著作權與知情同意權，如該法案於國會順利通過，即能要求蒐集受著作權保護之內容進行模型訓練的 AI 技術公司必須履行向美國著作權局局長（Register of Copyrights）通報之事前程序，草案內容重點如下所述：

1. 訓練資料來源公開透明化：建立訓練資料集或對該資料集進行任何重大變更的相關 AI 開發業者，應在正式推出可供消費者公開使用的全新生成式 AI 工具系統的 30 日前向美國著作權局呈遞通知。期前揭露該模型訓練資料內集中受著作權保護著作的完整清單列表，包含用來訓練或建置該系統所使用的任何受著作權保障內容等資訊之管理概況，以及其所使用可公開存取資料的網址。此外草案規定對於過去任何已可公開存取的 AI 系統均具有溯及效力，倘現有既存 AI 模型的訓練資料集發生重大改變之情形時，亦必須及時向著作權局闡明使用著作物至訓練過程的受保護程度是否採用相同標準。

2. 問責機制之建立：對於違反上述事前資訊揭露聲明之透明化義務，由主管機關根據個案違背情節與事業規模等因素綜合考量，可處 5,000 美元以上之罰鍰。

本報告之智慧財產權歸屬於國發會

3. 建置公共資料庫：將建立一個由各事業向著作權局提交的通知聲明、著作物清單等證明文件所匯集而成的線上公共資料庫，可供公眾隨時進入瀏覽檢視。

惟該提案尚有力有未逮之處，音樂產業人士特別呼籲法案須進一步賦予著作權人損害賠償的請求權基礎，以及拒絕 AI 技術公司將著作內容持續投入模型訓練之退出權利（opt-out rights），為權利人在資料集建立起適當之退出機制。但法案在受著作權保障之訓練資料來源透明化上所樹立的指標仍普遍獲得來自各產業領域的正面迴響，包括美國作曲家、作家和發行商協會（ASCAP）、美國唱片工業協會（RIAA）、美國演員工會-美國電視和廣播藝人聯合會（SAG-AFTRA）、美國編劇工會（Writers Guild of America）、美國導演工會（Directors Guild of America）、美國職業攝影師協會（Professional Photographers of America）、美西作家協會（Writers Guild of America West）、美東作家協會（Writers Guild of America East）、劇場舞臺員工國際聯盟（IATSE）、人類藝術活動（Human Artistry Campaign）等組織的鼎力支持。

資料來源：

1. Adam Schiff, Rep. Schiff Introduces Groundbreaking Bill to Create AI Transparency Between Creators and Companies, 2024-04-09, https://schiff.house.gov/news/press-releases/rep-schiff-introduces-groundbreaking-bill-to-create-ai-transparency-between-creators-and-companies (last visited 2024/04/26)
2. The Guardian, New bill would force AI companies to reveal use of copyrighted art, 2024-04-09, https://www.theguardian.com/technology/2024/apr/09/artificial-intelligence-bill-copyright-art (last visited 2024/04/26)
3. Billboard, New Federal Bill Could Require Disclosure of Songs Used in AI Training, 2024-04-09, https://www.billboard.com/business/legal/federal-bill-ai-training-require-disclosure-songs-used-1235651089/ (last visited 2024/04/30)

本報告之智慧財產權歸屬於國發會

4. GovInfo, H.R. 7913 (IH) - Generative AI Copyright Disclosure Act of 2024, 2024-04-09, https://www.govinfo.gov/app/details/BILLS-118hr7913ih (last visited 2024/05/03)

5. Associated Press News, Eight US newspapers sue ChatGPT-maker OpenAI and Microsoft for copyright infringement, 2024-05-01, https://apnews.com/article/chatgpt-newspaper-copyright-lawsuit-openai-microsoft-2d5f52d1a720e0a8fa6910dfd59584a9 (last visited 2024/05/06)

(八)2024 年 4 月美國國土安全部成立 AI 安全顧問委員會以因應人工智慧技術對關鍵服務設施之衝擊

美國國土安全部（Department of Homeland Security, DHS）於 2024 年 4 月 26 日宣布成立以 AI 科技之安全及保障為宗旨的顧問委員會，組成的 22 人小組成員中包括政府官員與眾多美國科技巨擘的企業高層，如 OpenAI 執行長阿特曼（Sam Altman）、微軟（Microsoft）執行長納德拉（Satya Nadella）、奧多比（Adobe）執行長納拉延（Shantanu Narayen）、Anthropic 執行長阿莫戴（Dario Amodei）、國際商業機器公司（IBM）執行長克利希納（Arvind Krishna），而谷歌（Google）母公司 Alphabet 執行長皮查伊（Sundar Pichai）、思科系統公司（Cisco Systems Inc.）執行長羅賓斯（Chuck Robbins）、亞馬遜網路服務（AWS）執行長塞利普斯基（Adam Selipsky）也是構成員，另外輝達（NVIDIA）執行長黃仁勳、超微（AMD）執行長蘇姿丰亦在名單之列，此委員會係期望透過事前預警和即時因應境內關鍵服務設施受 AI 干擾之相關情事，防免在國家安全、經濟安全、公共健康及衛生福利等面向之威脅，並與 DHS 共同合作，為運輸部門、管路和電網設備營運商、網路服務供應商提供諮詢建議，委員會預計將於 5 月初首度召開會議，往後計劃每季召開一次例會。

委員會之成立係響應美國總統拜登（Joe Biden）於 2023 年 10 月簽署名為「安全、可靠和值得信賴的人工智慧開發和使用」之行政命

本報告之智慧財產權歸屬於國發會

令，確保在安全、可靠、可驗證及負責任的前提下部署 AI，建立一套全球性的 AI 安全標準，降低 AI 對美國在網路等關鍵基礎設施產生大規模毀滅性的後果，防範 AI 在與智慧財產領域交叉後所衍生的系統性風險。事實上 DHS 早在 2023 年 4 月即成立 AI 特別工作小組，主要任務係研究如何透過 AI 之部署改善貨物通關檢查流程與識別有無進口他國在強迫勞動下所生產的商品，以強化供應鏈韌性與國際貿易的完整性。另一方面 DHS 在 2024 年度的影響評估報告中顯示對美國關鍵基礎設施脆弱性的擔憂，可能隨時面臨潛藏的物理性攻擊、網域入侵、資料竊取或植入惡意程式進行破壞等網站攻擊等事件，並指稱 AI 技術極有可能針對美國民眾賴以維生的線路管道、鐵路軌道和其他美國關鍵基礎設施等目標進行更大規模、更迅速、更高效和具隱匿性的網路攻擊，並特別提及包含中國大陸在內的境外敵對勢力正在研發破壞美國網路防禦的 AI 技術，例如支援勒索軟體攻擊等侵略活動的生成式 AI 程式。

委員會為 DHS 在 2024 年 3 月首度公布之「人工智慧路徑圖」的規劃之一，朝向負責地利用 AI 技術以推進國土安全保護之進程邁進，同時兼顧隱私權、自由權等公民基本權保障，促成全國的 AI 安全防護，並透過與政治盟友凝聚強大的合作夥伴關係，維持美國在 AI 領域的領先地位。為了在以安全為框架之設想下開啟 AI 技術的發展及使用，擬研議一套全面在能源、公營事業、交通、國防、資訊科技、食品、農業、互聯網、金融、保險等橫跨國內 16 項關鍵性服務領域於應對 AI 技術衝擊時之處理方案，該委員會預期以下述運作方式達成上述目標：

1. 非以理論之建構為目的，而係從務實面之實踐進行商討，維繫官方組織與關鍵基礎設施供應群體之協調管道，雖然 AI 的應用大幅改善能源輸送、資訊傳播、金融服務、航空運輸和醫院量能等之效能，但同時須密切關注技術進步下對系統網絡

本報告之智慧財產權歸屬於國發會

產生的安全性隱憂，隨時為其提出可施行的方針以確保 AI 技術使用者得以在安全穩健的環境中利用關鍵基礎設施服務。

2. 為 DHS、關鍵基礎設施供應者、AI 技術領頭羊三方群體創建一個資訊共享的平臺機制，促成三方就 AI 運用所引發的各類風險進行溝通交流及創造定時互換情資的契機。

惟該委員會之成立亦引起質疑聲浪，檢視其組成的成員名單中不乏有壟斷國內數位市場的科技巨頭，外界認為讓其高層接觸國家數位發展之決策核心會有實質上的利益衝突情事，並非有助於作為技術投入下國家安全危機佈防之角色，反倒為其創造出有利將自家產品技術推廣應用的機遇，進而干預國家數位法制政策之走向，故委員會後續能否切實解決 AI 技術背後的潛在風險，抑或僅有為國內科技巨投的科研成果背書之功能，可進一步觀察該委員會後續的運作成效為何。

資料來源：

1. Reuters, US Homeland Security names AI safety, security advisory board, 2024-04-27, https://www.reuters.com/technology/us-homeland-security-names-ai-safety-security-advisory-board-2024-04-26/ (last visited 2024/04/27)

2. Department of Homeland Security, Department of Homeland Security Unveils Artificial Intelligence Roadmap, Announces Pilot Projects to Maximize Benefits of Technology, Advance Homeland Security Mission, 2024-03-18, https://www.dhs.gov/news/2024/03/18/department-homeland-security-unveils-artificial-intelligence-roadmap-announces (last visited 2024/04/27)

3. Department of Homeland Security, Over 20 Technology and Critical Infrastructure Executives, Civil Rights Leaders, Academics, and Policymakers Join New DHS Artificial Intelligence Safety and Security Board to Advance AI's Responsible Development and Deployment, 2024-04-26, https://www.dhs.gov/news/2024/04/26/over-20-technology-and-

本報告之智慧財產權歸屬於國發會

critical-infrastructure-executives-civil-rights-leaders (last visited 2024/04/27)

4. Department of Homeland Security, Department of Homeland Security Homeland Threat Assessment, 2023-09-13, https://www.dhs.gov/publication/homeland-threat-assessment (last visited 2024/05/03)

(九)2024 年 4 月美國康乃狄克州參議院通過《人工智慧監管法案》（SB NO.2）

美國康乃狄克州參議院於 2024 年 4 月 24 日通過《人工智慧監管法案》（SB NO.2），主旨在防止 AI 作出對人民產生偏見之決策避免人民受到傷害，透過制定保障措施以消除演算法之歧視風險，保護消費者和弱勢族群，監管私部門對 AI 之開發和部署，提倡基於風險原則，鼓勵以合乎道德和有價值的方式使用 AI，預計於 2026 年 2 月 1 日生效，以下為該 AI 監管法案之重點內容：

1. 監管之對象

該法案監管之對象為高風險 AI 系統的開發商和部署者，即，AI 系統用於作出教育、就業、金融、貸款、醫療或其他重要生活機會決策之系統，但是，在特定情形下，小型企業之部署者例外不受監管。

2. 開發者和部署者之義務

高風險 AI 系統的開發者和部署者負有合理謹慎的義務避免演算法歧視，並就高風險 AI 系統的使用或銷售發表公開聲明，開發者需要向部署者提供揭露之資訊和文件，資訊包含系統之預計用途、用於訓練系統的資料、風險緩解措施，此外，部署者需制定風險管理政策，對高風險 AI 系統進行影響評估，並確保消費者得向其行使相關權利。

本報告之智慧財產權歸屬於國發會

3. 個人之權利

部署者使用高風險 AI 系統作出相應決策或將其作為作出相應決定的重要因素之前，必須向個人發出通知，若系統作出不利的決定，個人有權要求解釋高風險 AI 系統如何作成決策，包含作成決策使用之個人資料，更正做出決定所使用的個人資料，對決定為上訴再次進行人工審核。

4. 遵守與互惠

法案頒布後，開發者與部署者有兩年時間準備遵守法案之要求，若在其他方面符合美國國家標準與技術研究院的 AI 風險管理框架或其他國內或國際認可的風險管理框架，則可將其作為積極抗辯。

最後，立法機關除了對私部門為規範外，還成立了一個特別工作小組，負責就生成式 AI 和通用型 AI 的監管提出建議，包含有關 AI 生成的未經同意的親密影像、政治競選活動中傳播深度偽造影音、勞動力發展等問題。

資料來源：

1. Future Of Privacy Forum, SETTING THE STAGE: CONNECTICUT SENATE BILL 2 LAYS THE GROUNDWORK FOR RESPONSIBLE AI IN THE STATES, 2024-04-25, https://fpf.org/blog/setting-the-stage-connecticut-senate-bill-2-lays-the-groundwork-for-responsible-ai-in-the-states/ (last visited 2024/05/02)

2. APNews, Connecticut Senate passes wide-ranging bill to regulate AI. But its fate remains uncertain, 2024-04-25, https://apnews.com/article/artificial-intelligence-ai-connecticut-regulation-b004b4477ac20cc365317edff9f7351b (last visited 2024/05/02)

本報告之智慧財產權歸屬於國發會

(十)2024 年 4 月美國愛荷華州參議院一致通過《散布、播送及陳列不實性影像法案》與《散布、播送及陳列與兒少性剝削有關之性影像法案》，將製作及傳輸不實性影像之行為刑罰化

「復仇式色情」（Revenge Porn）或稱為「非同意散布性私密影像」（Nonconsensual pornography）的現象屢見不鮮，近來再透過 AI 發展的深偽技術，進而加劇數位性暴力下「性勒索」（Sextortion）之情事發生，為打擊行為人持有以 AI 技術生成的不實性影像脅迫當事人或故意散布流傳，愛荷華州眾議院日前在 3 月一致通過 HF2240 與 SF2243 兩項法案，將數位性暴力刑事立法，後再經參議院審議通過，並已由州長簽署批准，法案預計於今年 7 月 1 日生效。

愛荷華州參議院 4 月 10 日與 4 月 19 日各自通過的 HF2240 與 SF2243 法案將分別針對不同數位性暴力進行類型化處置，前者係《散布、播送及陳列不實性影像法案》，意在因應行為人「復仇式色情」或「性勒索」之騷擾行為，亦即行為人基於威脅、報復、毀損對方名譽、破壞對方人際關係等目的，未經過當事人同意而故意散布、播送、陳列或以任何方式讓第三人觀覽當事人為性交、裸露性器官等性私密之影像圖片，或者持有性私密影像並以之脅迫當事人行無義務之事，均屬該州加重其刑的輕罪（Aggravated Misdemeanor），最高可處 2 年徒刑，得併科 855 美元以上 8,540 美元以下罰款。

而後者乃《散布、播送及陳列與兒少性剝削有關之性影像法案》，立基在參議院早前通過《兒少性剝削法案》（The Child Exploitation Bill）以防範兒童色情的基礎上，劍指深偽技術等科技方法所合成的兒少性影像，對於利用未成年人肖像製作或變造其為性交或與性相關之圖像畫面，呈現出半部裸露或全部裸露之身體隱私部位，在客觀上足以滿足性慾或暗示其與性行為之描繪產生關聯，而引起社會大眾羞恥或厭惡者，將以重罪論處。且論罪上不論持有的未成年人性影像是否以深偽技術合成，或不實性影像中是否得特定及識別未成年人之真實身分亦在所不問，只要生成之影音內容屬於有害未成年人的身心健全發展

本報告之智慧財產權歸屬於國發會

之類別，於該州初犯本罪之行為人均直接被歸類在 D 級重罪，最高可處 5 年徒刑，得併科最高 10,245 美元的罰金；另外本罪之累犯則被歸屬在 C 級重罪，將被處以最高 10 年之徒刑，得併科最高 13,660 美元的罰金。

資料來源：

1. The Iowa Legislature, House File 2240, 2024-04-19, https://www.legis.iowa.gov/legislation/BillBook?ga=90&ba=HF2240 (last visited 2024/05/20)
2. The Iowa Legislature, Senate File 2243, 2024-04-10, https://www.legis.iowa.gov/legislation/BillBook?ga=90&ba=SF2243 (last visited 2024/05/20)
3. The Gazette, Iowa House lawmakers unanimously pass bills criminalizing 'deepfake' porn, 2024-05-07, https://www.thegazette.com/state-government/iowa-house-lawmakers-unanimously-pass-bills-criminalizing-deepfake-porn/ (last visited 2024/05/20)

(十一) 2024 年 4 月 4 月美國勞工部發布關於人工智慧及其對工作場所影響的新指引

美國勞工部（U.S.A. Department of Labor, USDOL）於 2024 年 4 月 29 日發布「工作場所人工智慧對工資與工時部門執行的聯邦勞動和就業標準的影響」之指導意見，使人民瞭解勞工部如何看待 AI 應用於工作場所，以及其執法重點，此外，DOL 指出僱主可能要為其使用的 AI 系統或工具的非法行為承擔責任，即使這些系統或工具是由合作之軟體開發商所設計，亦即雇主表示不知悉 AI 系統是如何運行的，並不能作為免責的事由。

以下說明此意見對於相關法令之適用提出之重要內容：

本報告之智慧財產權歸屬於國發會

1. 公平勞動標準法（Fair Labor Standards Act）

AI 於工作場所的一些用途包含評估員工的工作效率、追蹤員工的位置、計算員工的工作安排和休息時間等，其可能會減少計算工時，特別是有休息時間或多個地點工作的情形。無論使用何種技術和系統，僱主依法有責任向員工給付其應獲得之報酬，確保給付報酬無違反聯邦報酬標準。

2. 家庭與醫療假法（Family and Medical Leave Act）

無論雇主是否使用 AI 或其他自動化系統追蹤和管理員工之受聯邦保障的休假，皆須遵守該規範，違反該規範的行為包含有干擾、限制或拒絕行使法定的權利，例如未授權或藉由自動化管理工具干擾或限制員工休假之權利等。雇主除遵守規範外，應監督 AI 或自動化技術的使用，避免產生侵害法定權利的風險。

3. 職場母親集乳保護法（Providing Urgent Maternal Protections Act）

無論使用何種技術和系統，雇主都有責任依照法律規定為提供哺乳員工休息時間，以及確保 AI 或其他自動化系統不會因員工在工作中集乳而對其採取不利措施。

4. 受僱者測謊保護法（Employee Polygraph Protection Act, EPPA）

雇主使用 AI 或其他技術衡量真實性須受到 EPPA 的限制。

綜合以上，AI 如果沒有適當的人工監管，這些技術可能會在勞動標準方面給員工帶來潛在之風險，並可能違反相關的法律。此外，在工作場所使用 AI 還有可能造成整個勞動力市場中之系統性違法行為，無論使用何種 AI 或其他自動化系統，當使用這些技術導致違反相關

本報告之智慧財產權歸屬於國發會

的法律時，雇主都應承擔責任，最後，雇主必須負責任地使用 AI，以繼續遵守相關的法律。

資料來源：

1. U.S. DEPARTMENT OF LABOR, Artificial Intelligence and Automated Systems in the Workplace under the Fair Labor Standards Act and Other Federal Labor Standards, 2024-04-29, https://www.dol.gov/agencies/whd/field-assistance-bulletins, (last visited 2024/05/20)
2. Jibble, DOL Releases Guidance on Implementation of AI in the Workplace, 2024-05-10, https://www.jibble.io/news/dol-workplace-ai-artificial-intelligence-guidance-2024 (last visited 2024/05/20)
3. JD Supra, DOL Issues Guidance on Workplace AI, 2024-05-07, https://www.jdsupra.com/legalnews/dol-issues-guidance-on-workplace-ai-9200619/, (last visited 2024/05/20)

(十二) 2024 年 5 月美國參議院發布人工智慧藍圖（Driving U.S. Innovation in Artificial Intelligence: A Roadmap for Artificial Intelligence Policy in the United States Senate）

美國參議院 AI 工作小組於 2024 年 5 月 15 日發布人工智慧藍圖（Driving U.S. Innovation in Artificial Intelligence: A Roadmap for Artificial Intelligence Policy in the United States Senate），針對優先資助事項、新立法的制定以及需要進一步探索的領域提出建議，鼓勵行政部門即時及繼續分享有關其 AI 優先事項的資訊，以及與其他國家簽署的任何 AI 相關備忘錄和相關研究的成果，以為立法活動提供資訊。

以下說明此藍圖中提出的主要資助和立法優先事項，以及工作小組認為值得進一步研究的領域：

1. 與優先資助相關之事項

本報告之智慧財產權歸屬於國發會

為跨政府部門的 AI 研發工作、晶片及科學法案（CHIPS and Science Act）、創造人工智慧法案（CREATE AI Act）等法案和計畫之執行提供資金。

2. 與制定新立法相關之事項

藍圖中提出制定一系列新的立法之建議，包含有鼓勵相關委員會制定立法，利用政府的公私夥伴關係以推動 AI 的進步，並降低 AI 的潛在風險；應對新創企業在 AI 市場競爭中面臨的獨特挑戰，包括考慮是否需要立法，以激勵各州和地方之投資；制定與「培訓和提升私部門勞動技能」有關的立法，使人力成功參與 AI 經濟；AI 工作小組認為現有之法律需要一致、有效的適用於 AI 系統及其開發者、部署者和使用者等立法建議。

3. 與有待進一步研究的領域有關之事項

藍圖為今後的研究提出了各項建議，並支持聯邦政府進一步與其資助的研發中心合作研究 AI，包含探索 AI 對未來長期工作的影響和可能的解決辦法、專業內容創作者和出版商關注 AI 相關問題之影響，防止利用 AI 進行欺詐之各種機制等領域之內容。

資料來源：

1. Klobuchar, Klobuchar Statement on Bipartisan Senate AI Working Group Roadmap, 2024-05-15, https://www.klobuchar.senate.gov/public/index.cfm/news-releases?ID=B2E26559-36D5-46B9-A4D8-137655CF6708 (last visited 2024/05/17)

2. TechPolicy, US Senate AI Working Group Releases Policy Roadmap, 2024-05-15, https://www.techpolicy.press/us-senate-ai-working-group-releases-policy-roadmap/, (last visited 2024/05/17)

本報告之智慧財產權歸屬於國發會

(十三) 2024 年 5 月美國國防部徵求國防應用人工智慧之公眾意見

美國國防部（Department of Defense）於 2024 年 5 月發布公眾意見徵集通知，內容涉及國防部於國防工業基地中應用 AI 得採取之行動，國防部將依據公眾提供之意見制定政策、分配資源以及可信任 AI 國防工業基地藍圖，確保國防工業基地 AI 之整合，包含以下重要項目之意見蒐集：

1. 基礎設施與供應鏈彈性：

   國防部將在國防工業基地中投資，擴大系統中更多 AI 應用；解決供應鏈中的漏洞，以支持 AI 納入國防系統。

2. 人員：

   為承包商、小型企業在設計、開發、測試和部署國防系統之 AI 提供支援；充分培訓國防情報局之人員，以利在 AI 之合作應用。

3. 創新與風險：

   開發 AI 防禦系統面對之相關智慧財產權挑戰；採取措施促進政府機構、承包商和研究機構之間的資訊共享和協作，以增強 AI 防禦系統的能力和創新；評估和減輕 AI 防禦系統利用的風險。

4. 監管環境：

   確定設計、開發、測試和提供 AI 防禦系統的監管或其他政策障礙；AI 轉變為國防應用可支持的計畫、戰略、政策；在未來需要解決之主要障礙，以在國防應用中採用 AI。

本報告之智慧財產權歸屬於國發會

資料來源：

1. Federalregister, Defense Industrial Base Adoption of Artificial Intelligence for Defense Applications; Notice of Availability, 2024-05-22 ,https://www.federalregister.gov/documents/2024/05/22/2024-11195/defense-industrial-base-adoption-of-artificial-intelligence-for-defense-applications-notice-of, (last visited 2024/06/03)

2. JD Supra, DOD Seeks Public Comment to Aid Its Adoption of AI in Defense Applications, 2024-05-28, https://www.jdsupra.com/legalnews/dod-seeks-public-comment-to-aid-its-8772132/, (last visited 2024/06/03)

(十四) 2024 年 5 月美國加州民權理事會發布草案，防止自動化決策系統造成的就業歧視

於 2024 年 5 月美國加州之民權理事會（Civil Rights Council）針對自動化決策系統之法令制定，經過一系列公開討論後，發布「防止因使用 AI、演算法和其他自動化決策系統而導致就業歧視」之擬議法令，該法令明確現有的防止就業歧視的規範將如何適用於新興技術，且民權委員會已啟動擬議法令的公眾評論程序，鼓勵相關各方在 2024 年 7 月 18 日前提交公眾意見。

民權委員會意識到自動化決策系統依賴於演算法或 AI，越來越多地使用於就業環境中，以促進與求職者或員工相關的各種決策，包含了招聘、雇用和升遷方面的決策。雖然 AI 之利用可以帶來無數益處，但也可能加劇現有的偏見以及促成歧視結果，對此問題，擬議之法令提出以下重點措施：

1. 法令明確指出若自動化決策系統使用受保護特徵對申請者或員工造成傷害則違反加州法律。

2. 確保雇主將就業記錄，包括自動化決策資料至少保存四年。

本報告之智慧財產權歸屬於國發會

3. 確保於評估申請者的犯罪紀錄時，僅使用自動化決策系統不得取代個人化之評估需要。

4. 明確禁止第三方助長就業歧視現象，包括透過設計、銷售或使用自動化決策系統之行為。

5. 說明自動化決策系統中使用的測試可能構成非法執行醫療業務或心理監測行為的相關事例。

綜合以上，民權理事會鼓勵所有相關方和公眾參與監管討論，必須在 2024 年 7 月 18 日之前提交書面意見。

資料來源：

1. Civil Rights Departments, Civil Rights Council Releases Proposed Regulations to Protect Against Employment Discrimination in Automated Decision-Making Systems, 2024-05-17, https://calcivilrights.ca.gov/2024/05/17/civil-rights-council-releases-proposed-regulations-to-protect-against-employment-discrimination-in-automated-decision-making-systems/ (last visited 2024/05/27)

四、 日本

(一)2024 年 4 月 11 日日本頒布 2024 年 AI 白皮書（AI ホワイトペーパー 2024）

2024 年 4 月 11 日由日本自民黨制定並發佈 2024 年 AI 白皮書（AI ホワイトペーパー 2024），宣誓日本將進入 AI 發展之第二階段：成為「世界上對人工智慧最友善的國家」。

AI 從資料中學習和進化，因此資料策略很重要。其既有助於解決商業和社會問題的資料在全球範圍內自由傳播，同時確保個人資訊保護、安全、智慧財產權等方面的信任時，AI 將實現健康發展。此外，

本報告之智慧財產權歸屬於國發會

由於 AI 應用於各個領域，因此與新創公司、半導體、機器人等各個領域的策略和政策合作及有效利用措施均為重要因素。故未來 AI 相關政策預計將持續擴大，有必要強化政府的控制塔職能。基於上述因素考量，白皮書建議相關政策如下：

第二階段任務：

1. 實現成為全球 AI 最友善的國家，即全球對 AI 最了解、最容易研究、開發和實施 AI 的國家。

2. 利用 AI 增強日本競爭力的策略：靈活應對環境的快速變化。

3. 將根據機密資訊的處理等制定新的指導方針，以促進政府的進一步利用。針對 AI 風險，將及時制定並發布《AI 商業指引》，以便企業在風險基礎上快速應對環境變化，並廣泛傳播這些訊息，並促進每個組織適當使用 AI。

4. 加強研發能力，擬制定提供政府擁有的資料之相關計畫，分享私人資料的利用實例，並創造對發展有用的新資料，以利維護更新等。對於重要領域公私部門應協力收集、維護、更新資料。

5. 完善基礎設施

   為了確保資料中心等基礎設施成為全球對 AI 最友善的國家，政府將提供財政和其他政策支持，並鼓勵必要的私人投資。將開始「AI 橋接雲（AI Bridging Cloud Infrastructure, ABCI）」的擴展。

6. 安全保障策略

   日本的 AI 治理要求企業根據 AI 商業指引等自願、持續地評估和降低風險作為基礎。對於產生 AI 應對虛假和錯誤訊息之利用應有對策措施，建立日本 AI 安全研究所（AI Safety

本報告之智慧財產權歸屬於國發會

Institute, AISI）與其他如英美等國家建立 AISI 網絡，以促進確保 AI 安全的國際合作。

7. 與著作權等智慧財產權的關係

對於著作權等智慧財產權，政府將尊重這些權利，採取符合 AI 時代的措施，促進 AI 的合理利用。

隨著美國科技巨頭等高性能、大規模、通用基礎設施模式的演進和社會實施的進展，包括日本在內的國家正在尋找多種生存方式，例如小規模、高性能模型和多個模型的組合。日本正在透過新創公司和其他組織開發新模式以及大學和研究機構的先進研究與世界競爭。故此次發佈之 AI 白皮書，旨在定位日本未來於 AI 世界發展之方向，並以成為世界最友善之 AI 國家作為目標。

資料來源：

1. 自民党デジタル社会推進本部，AI ホワイトペーパー2024，https://www.soumu.go.jp/main_content/000944148.pdf，(last visited 2024/5/10)

(二)2024 年 4 月 19 日日本頒布「AI 運營事業指引（AI 事業者ガイドライン）第 1.0 版」

2024 年 4 月 19 日由經濟產業省（METI）和總務省（MIC）共同公佈 AI 運營事業指引（AI 事業者ガイドライン），該指引整合了總務省主導之 AI 發展指引（AI 開発ガイドライン）、AI 利用指引（AI 利活用ガイドライン）以及由經濟產業省所提出之實踐 AI 原則之治理指引 1.1 版(AI 原則実践のためのガバナンスガイドライン Ver1.1)。本指引架構：

本報告之智慧財產權歸屬於國發會

1. 定義：為說明理解本文之義涵，將 AI、AI 系統、先進 AI 系統、AI 模型（ML 模型）、AI 服務、生成 AI 及 AI 治理做了明確定義。

2. 共通規範：提出針對 AI 所應面對之社會及各適用主體應適用的相關共通規範，對象包含於各商業領域進行 AI 開發、提供或利用 AI 之商業實體以及各級政府等公共機構，並分成「A.基本理念」、「B.原則」、「C.共同指引」及「D.先進 AI 系統相關企業的共同指引」及「E. AI 治理」五大部分。

   (1) 基本理念層面，強調應尊重人以人性尊嚴為核心的社會（尊嚴）、具有多元背景的人們可以追求各種幸福的社會（多樣性與包容性）、可持續的社會（可持續性）三個價值，並建構追求這些價值實現之社會。為了實現基本理念。各主體應該促進 AI 系統和服務的開發、提供和使用，同時兼顧人之尊嚴的保護。各主體亦應確保透明度，提高系統或服務之可信度，以實現減少 AI 使用帶來的社會風險，確保安全性和公平性等價值。

   (2) 共同指引之部分詳述包含以人為本、安全性、公平性、隱私保護、資訊安全保障、透明性、責任追究、教育素養、公平競爭保障、創新等 10 項需注意之情況，以此為基礎標準，為建立可信賴之 AI 事業提供實質操作上之指引。針對被定義為先進 AI 系統之開發者，除必須額外遵守廣島進程開發先進 AI 系統組織國際行為準則（Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems）之 11 項標準外，還應遵守本指引中適用於開發先進 AI 系統之要求。

   (3) 為了在整個價值鏈上協同合作，實踐「共同指導方針」，並安全可靠地利用 AI，建立 AI 治理至關重要。在管理 AI

本報告之智慧財產權歸屬於國發會

相關風險，使其處於利益最大化且各利益相關方可接受的水準的同時，也需要建立 AI 治理以應對由此帶來的利益。值得注意的是，在具體研究中，需要考慮 AI 開發、提供和使用所帶來的風險程度和可能性，以及各主體的資源限制。

3. AI 開發者（AI Developer）：AI 開發者應注意於資料處理和訓練時，確保導入之資料在整個 AI 生命週期內皆應遵循法律，注意資料中可能存在之偏見，並於開發後注意最新動態，確認是否有新的攻擊方法產生並不斷完善安全措施。

4. AI 提供者（AI Provider）：AI 提供者之角色係在 AI 開發者之開發商添加附加價值，並將 AI 系統服務提供給 AI 使用者。因此除了要注意 AI 系統服務中包含的 AI 是否適用於該系統服務之外，還要考慮到商業策略或社會環境變化可能改變對 AI 的期望，因此進行適當的變更管理、配置管理和服務維護也至關重要。

5. AI 利用者（AI Business User）：應當接受 AI 提供者提供的安全可靠的 AI 系統服務，並在 AI 提供者意圖的範圍內持續進行適當的使用。利用 AI 系統服務時，應遵守 AI 提供者設定的使用上的注意事項，使用 AI 系統服務時要保持在 AI 提供者在設計中所設想的範圍內，進行資料登錄時，確保準確性和必要時最新性，理解 AI 輸出的精準度及風險程度，並在確認各種風險因素後使用。

該指引反映了這幾年來日本對 AI 技術之進展和國內外 AI 社會實施之討論，以鼓勵事業實踐 AI 的社會實施和治理，以非約束力之軟法提供指導原則，其制定不是由政府單方主導，而是由教育和研究機構、公民社會包括一般消費者以及民間企業等多方利害相關者進行討論，以確保實際效率性和正當性。

本報告之智慧財產權歸屬於國發會

資料來源：

1. G7 Hiroshima process,Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems,100573473.pdf (mofa.go.jp), (last visited 2024/5/10)

2. 日本総務省及経済産業省，AI 事業者ガイドライン，https://www.meti.go.jp/press/2024/04/20240419004/20240419004-1.pdf，(last visited 2024/5/10)

五、 新加坡

(一)2024 年 5 月新加坡發布生成式 AI 模型治理框架

新加坡於 2024 年 1 月 16 日至 3 月 15 日徵求公眾對擬議的生成式 AI 模型治理框架（Generative AI Model Governance Framework, GenAI 框架）進行反饋，並於 2024 年 5 月 30 日由 AI 驗證基金會和資訊通訊媒體發展管理局發布本框架。

本框架旨在針對 AI 應用的下列幾個面向提供指引：

1. 問責制：問責制將促使 AI 開發鏈中的所有參與者對最終用戶負責，可以與當今的雲端技術開發類比。

2. 資料：作為 AI 模型開發的核心元素，從輸入到形成模型的資料品質皆很重要，這些資料應來自可信賴的資料來源。將部分特定的資料用於模型訓練可能引起爭議，例如個人資料及智慧財產權相關資料；以務實的方式界定業務範圍和確保公平對待將至關重要。

3. 可信賴的開發與部署：儘管最終使用者的可見性可能有限，但從模型開發到應用都應制定安全可信賴的揭露標準，例如達到如同食品標籤式（food label）的透明度。

本報告之智慧財產權歸屬於國發會

4. 事件通報：建立監管通知結構及作法有助於促進對任何事件的及時補救，並更廣泛地支援 AI 系統的持續改進。

5. 測試與保證：第三方測試和保證可以發揮互補作用，圍繞 AI 制定通用和一致的標準，並最終展示對最終使用者的信任。由於金融和醫療保健領域已經採用了獨立驗證，即使作為一個新興領域，這些流程也可以在 AI 中類似地採用。圍繞 AI 測試制定通用標準以確保品質和一致性非常重要。

6. 安全性：生成式 AI 引入了針對模型本身的新威脅向量的潛力。這超出了任何軟體堆疊固有的安全風險。雖然這是一個新興領域，但需要調整現有的資訊安全框架，並開發新的測試工具來應對這些風險。

7. 內容來源：內容生成的地點和方式的透明度是必要的，以避免錯誤資訊和詐欺。必須在正確的上下文中考慮使用數位浮水印和加密來源等技術解決方案。

8. 安全與校準研究與開發（R&D）：需要加速研發投資，以提高模型與人類意圖和價值觀的一致性。新加坡希望與 AI 安全研發機構之間的全球合作一起實現這一目標。

9. AI 造福公共利益：使 AI 獲取民主化，提高公共部門的採用率，以及提高員工的技能和可持續地開發系統，將引導 AI 朝著公共利益的方向發展。

GenAI 框架並非強制性監管要求，而是一個治理框架。此框架鼓勵利益相關者「以實用和整體的方式」看待 GenAI 框架中提出的相關問題，並建議企業根據自身的特性、業務性質以及由此產生的相關風險或其他情況，根據此治理框架制定自身的實踐方式。

本報告之智慧財產權歸屬於國發會

此外，對 GenAI 框架的依賴並不能免除公司必須遵守其他適用法律的責任，包括但不限於智慧財產權、資料保護、線上安全、消費者保護、競爭、契約、侵權和行業法規。

資料來源：

1. NATIONAL LAW REVIEW, Singapore Invites International Feedback on Model Governance Framework for Generative AI, 2024-01-19, https://natlawreview.com/article/singapore-invites-international-feedback-model-governance-framework-generative-ai (last visited 2024/06/05)
2. NATIONAL LAW REVIEW, Singapore Publishes Generative AI Model Governance Framework, 2024-05-31, https://natlawreview.com/article/singapore-publishes-generative-ai-model-governance-framework (last visited 2024/06/05)

六、 德國

(一)2024 年 5 月德國資料保護機關（BDFI）於聯邦及各州獨立機關資訊保護監督會議（DSK）發布人工智慧資料保護指引

2024 年 5 月 6 號，德國資料保護機關（Bundes und der Länder, BDFI）於邦及各州獨立機關資訊保護監督會議（Datenschutzkonferenz, DSK）發布了一份人工智慧資料保護指引（Künstliche Intelligenz und Datenschutz），提供公私部門之 AI 部署者如何符合資料保護法之資料之指導原則。該指引側重於 AI 之部署，依據歐盟一般個人資料保護規則（General Data Protection Regulation, GDPR）討論重要標準，解決資料控制者在設計、選擇和使用 AI 部署時所可能遭遇之問題，包含以下重點措施：

1. 部署 AI 以前應注意之事項

本報告之智慧財產權歸屬於國發會

部署 AI 應用程式之前，從資料保護之合規性角度提出應注意之事項，包含有確定 AI 應用部署之目的、評估使用 AI 部署處理個人資料之法律依據、確保遵守透明度要求等事項。

2. 部署 AI 期間應注意之事項

為了確保使用 AI 之部署期間遵守資料保護法之要求，該指引提出之建議包含有明確之權責歸屬、制定 AI 之使用政策、進行資料保護影響評估、人員教育訓練等落實事項。

3. 謹慎使用 AI 之模型

最後，此指引指出根據資料保護法使用 AI 應遵循的共通措施，建議於涉及個人資料時採取嚴謹的方式進行提示和使用 AI 之輸出結果，AI 之輸出結果應受到持續監控和檢查，確保資料完整性並防止資料出現偏見以及歧視。

針對以上重點，此指引亦提示相關事例以利遵循，例如：

1. 一個國家地質辦公室想要利用 AI 應用程式重新評估舊的礦產資源地圖，須評估這些地圖是否不涉及個人資料及住宅區域。

2. 資料保護合法性訓練：LLM 聊天機器人（大型語言模型）利用 AI 運作時，仍須遵守資料保護法規。

3. 一個 AI 應用程式評估所有收到的工作申請並自動發送面試邀請。這違反了 GDPR 第 22 條第 1 款的規定。

4. 透過技術設計之資料保護：為員工使用的帳戶設定功能，以便在啟動帳戶時選擇不使用輸入資料進行 AI 訓練，不會在會話之後保存輸入歷史記錄，亦不會自動公開與帳戶相關的輸出資料等，以保障員工對自己之個人資料的提供有自主決定的權利。

本報告之智慧財產權歸屬於國發會

綜上，本次指引的重點為監督並指導新商業模式中 AI 的應用，並舉出不同應用情況作為事例進行說明。若德國政府與相關事業確實遵循此份指引，應可加強 AI 與資料應用相關的安全性。

資料來源：

1. Decisi 1.Datenschutz, Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 6. Mai 2024, 2024-05-06,https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf, (last visited 2024/05/30)
2. DSK, PRESSEMITTEILUNG der Konferenz der unabhängigen atenschutzaufsichtsbehörden des Bundes und der Länder vom 6. Mai 2024, 2024-05-06, https://datenschutzkonferenz-online.de/media/pm/2024_05_06_DSK_PM_OH_KI_und_Datenschutz.pdf (last visited 2024/05/13)
3. JDSUPRA, AI deployment: German DPAs issue guidance on data protection compliance, 2024-05-08, https://www.jdsupra.com/legalnews/ai-deployment-german-dpas-issue-6371709/ (last visited 2024/05/13)

七、 法國

(一)2024 年 4 月法國資訊自由委員會(CNIL)發布人工智慧開發之建議

法國資訊自由委員會（Commission Nationale de l’ Informatique et des Libertés, CNIL）於經過公眾諮詢後，在 2024 年 4 月 8 日發布了第一份關於 AI 系統開發之建議，調和 AI 之發展與個人資料保護之問題，指導 AI 系統開發者如何遵守 GDPR 等法令規則處理個人資料。

本報告之智慧財產權歸屬於國發會

CNIL 提醒 AI 系統開發者於開發 AI 系統時需注意個人資料之保護，提醒 AI 系統中之參與者需遵守個人資料保護法令，並就 AI 系統之開發應用於 GDPR 之適用問題，提出相關事例加以釐清，大致提出七個應注意之重點：

1. AI 之開發與應用遵守之個人資料保護相關法令。例如若 AI 系統之開發者係依據其所選定之資料進行 AI 之訓練，則應被視為 GDPR 之資料控管者。若開發事業與 AI 服務之提供者共同進行訓練資料庫之設置，則應被視為共同控管者。

2. AI 自開發時即需確定用於開發系統之個人資料處理之特定目的。倘若所開發者為通用 AI 系統，包括大型語言模型或電腦視覺系統等，未來可應用之目的範圍廣泛，故其開發時之特定目的只要符合該開發系統之類型即可預見之功能，則應已達到目的具體明確。

3. 資料之利用須具備有效之法律依據。包括建置資料庫進行 AI 訓練，其資料之取得與利用必須符合法定要件，如同意、具備合法利益、符合公共利益、基於契約關係等。CNIL 並提醒，部分清況下採用同意作為依據有其困難度，可評估是否具備合法利益作為有效之法律依據。

4. 期望重複利用於不同情境下基於不同目的所取得之資料，則須依據個案情境進行檢視，確保目的的符合性，或係重複取用可公開取得之資料（合法之資料庫來源），或來自第三方合法資料共享等，確保資料來源的合法性。

5. 必要時需進行資料保護影響評估（DPIA），了解相關 AI 部署與應用，是否涉及 AI 法或 GDPR 規範下之高風險認定等相關事宜。

本報告之智慧財產權歸屬於國發會

6. 需重視並依循資料最小化及比例原則，尤其設計系統時須避免使用不必要之個人資料。

7. 規劃資料生命週期之各階段實施措施，包括資料之選擇、歸檔與刪除等程序，原則上個人資料不能被無限期保存，不同之利用情境與資料保存期限之規劃亦應有所不同。

此外，CNIL 還公布在諮詢期間由 43 個利害關係人所提出之建議和結構性問題，未來將進一步針對結構性問題加以解決。

資料來源：

1. CNIL, IA : la CNIL publie ses premières recommandations sur le développement des systèmes d'intelligence artificielle, 2024-04-08, https://www.cnil.fr/fr/ia-la-cnil-publie-ses-premieres-recommandations-sur-le-developpement-des-systemes-dintelligence (last visited 2024/04/25)

2. JD Supra, French Data Protection Authority Publishes Recommendations on the Development of AI Systems: Seven Takeaways, 2024-04-24, https://www.jdsupra.com/legalnews/french-data-protection-authority-7334230/ (last visited 2024/04/26)

八、 經濟合作暨發展組織(OECD)

(一)2024 年 5 月經濟合作暨發展組織修訂 OECDAI 原則（OECD Principles on Artificial Intelligence）

2024 年 5 月 3 日，經濟合作暨發展組織（Organization for Economic Cooperation and Development, OECD）之部長理事會會議（Ministerial Council Meeting, MCM）為了應對 AI 技術的最新發展，特別是通用式 AI 和生成式 AI 的出現，通過「OECDAI 原則」之修訂。修訂後之 AI 原則處理了涉及與 AI 相關的隱私、智慧財產權、安全及資訊完整性等

本報告之智慧財產權歸屬於國發會

問題，適用於包括歐盟在內的 47 個會員國，以確保各地的 AI 發展，並因應 AI 可能產生之風險；同時為制定 AI 框架提供藍圖，倡導發展創新、可信賴、維護人權及民主價值觀的 AI。

OECDAI 政策觀察小組審視 2019 年提出 AI 原則後的發展，結果顯示以生成式 AI 進行新創投資之需求增加。同時已有 70 多個國家提出多項 AI 倡議，透過開發及部署 AI 系統提高生產力、加速科學研究、促進環境持續發展、改善醫療保健和教育。而維護人權和民主價值觀的必要性日益增強，但隱私、安全、公平和福祉等方面的風險正在以前所未有的速度和規模增長，甚至造成危害，如偏見和歧視的存在、錯誤資訊的創造和傳播以及對公共論壇和市場的扭曲。

因此本次修訂主要針對該原則之相關性、穩定性和適用性面向，並提出以下重點建議：

1. 應確保系統之安全，在 AI 系統有可能造成傷害時，有健全的機制和保障措施修復或使其安全退役，以及公開系統之透明度與負責任的揭露 AI 系統資訊。

2. 反映在生成式 AI 時代下處理錯誤、虛偽資訊以及保障資料完整性的重要性。

3. 強調整個 AI 生命週期內負責任的作為，包括與 AI 知識和資源供應商、系統使用者和其他利益相關者合作。

4. 釐清 AI 系統之資訊，促進透明度並進行可責之揭露義務。

5. 需進行環境永續性之評估。

6. 強調隨著全球 AI 政策倡議數量的增加，各國需要共同促進 AI 治理和政策環境的互通性。

資料來源：

本報告之智慧財產權歸屬於國發會

1. OECD, OECD updates AI Principles to stay abreast of rapid technological developments, 2024-05-03, https://www.oecd.org/newsroom/oecd-updates-ai-principles-to-stay-abreast-of-rapid-technological-developments.htm (last visited 2024/05/13)

2. OECD, Recommendation of the Council on Artificial Intelligence, 2024-05-03, https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449, (last visited 2024/05/13)

3. OECD, REVISED RECOMMENDATION OF THE COUNCIL ON ARTIFICIAL INTELLIGENCE, 2024-05-03, https://one.oecd.org/document/C/MIN(2024)16/FINAL/en/pdf, (last visited 2024/05/13)

(二)2024 年 5 月日本於 OECD 巴黎部長理事會場邊會議宣布啟動「廣島 AI 進程之友集團」，落實《廣島 AI 進程》以推進開發先進 AI 系統國際指導原則暨行為準則

日本對於 AI 發展之立場係在促進利用和監管之間維持平衡，亦即對 AI 的開發及使用乃在確保安全可控制之前提下採取積極立場；於國際政治上則採取中立性的 AI 政策，以使得日本未來在 AI 領域取得領導地位將更有優勢。適逢日本輪值 2024 年 5 月 2 日於法國巴黎舉行的經濟合作暨發展組織部長級理事會（Organization for Economic Co-operation and Development Ministerial Council Meeting，OECD 部長級理事會）之主席國，日本首相岸田文雄（KISHIDA Fumio）則另於會外，主持生成式 AI 場邊會議（Generative AI side event），以「邁向安全、可靠和值得信賴的 AI：促進 AI 包容性治理」為主題，呼籲全球應立即開展一套具備國際治理、開發安全、可靠和值得信賴的先進 AI 系統。同時宣布《廣島 AI 進程》（Hiroshima AI Process）及啟動「廣島 AI 進程之友集團」（Hiroshima AI Process Friends Group），由 49 個國家及地區(美、加、日、韓、澳、紐、新、泰、印、土、31 個歐洲國

本報告之智慧財產權歸屬於國發會

家及部分南美洲國家)簽署參與，以作為各國支持《廣島 AI 進程》宗旨之自願性框架，並在各國分進合擊之下，將努力落實本進程之《開發先進 AI 系統組織國際指導原則》（Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI System）及《開發先進 AI 系統國際行為準則》（Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI System）以應對生成式 AI 之風險與促進合作，進一步確保全人類均得以受惠於安全、可靠且可信賴的 AI。

針對生成式 AI 潛在與實質之風險及威脅，如真偽難辨之深度偽造內容，或利用 AI 所散播之假訊息，均可能加深歧視偏見與撕裂社會和諧，進而導致犯罪率攀升，甚至衝擊一國之民主和政治穩定。對此日本將建立 AI 全球夥伴（Global Partnership on Artificial Intelligence, GPAI）東京中心，為專家技術示範專案提供強而有力的支援，挹注資源在驗證及識別原創者內容機制之技術發展，慎防未經驗證的資訊流竄。

事實上日本早在 2023 年 5 月於廣島舉行之 G7 高峰會中便積極透過建立新的監管架構引導全球 AI 規則，考量 AI 之國際使用現況及各國實際執行之規範落差，時任主辦國的日本遂提出應對生成式 AI 風險之國際標準規範，並於 2023 年 10 月第 18 屆聯合國網際網路治理論壇（18th Annual Meeting of the Internet Governance Forum）利害關係人會議中討論相關議題；於同年 12 月，為達到「安全、可靠及可信賴的 AI」之目標，順利推出世界上第一個 AI 領域的國際架構—《廣島 AI 進程之綜合政策框架》（Hiroshima AI Process Comprehensive Policy Framework），並在去年底的 G7 數位和技術部長會議通過，該架構包含納入適用於所有 AI 參與者及開發者智慧之國際指導方針原則，即前述之《國際指導原則》以及《國際行為準則》。

《國際指導原則》包含 11 項指導原則，適用於所有於 AI 生命週期中之參與者，包含先進 AI 之設計、開發、部署、供應與使用，旨在

本報告之智慧財產權歸屬於國發會

要求 AI 生命週期之各參與者應對於可信賴及負責任地使用先進 AI 系統作出貢獻。這些原則包括採取適當措施以在 AI 之生命週期中減緩風險、公開報告 AI 系統之能力與使用領域、組織間（含產業、政府、民間及學術界）負責任地分享資訊與通報事故、投資於網路安全設施、優先開發解決氣候危機、全球健康與教育的先進 AI 系統、部署可靠之 AI 生成內容驗證及識別資訊來源機制(如數位浮水印)、實施堅實的安全控制措施（含實體安全、網路安全與內部威脅之保護措施）、揭露 AI 治理與風險管理政策等。

另外，《國際行為準則》則是以上開《國際指導原則》中的 11 項要點為基礎，只針對先進 AI 的開發者提供進一步的詳細指引，然該行為準則係無拘束力的自願性指導方針，其目標係推動安全、可靠、可信賴之 AI 系統並提供最先進 AI 系統（含最先進之基礎模型及生成式 AI 系統）之開發者藉由以風險為基礎之方式採取行動。

資料來源：

1. The Associated Press, Japan's Kishida unveils a framework for global regulation of generative AI, 2024-05-02, https://www.msn.com/en-us/news/world/japans-kishida-unveils-a-framework-for-global-regulation-of-generative-ai/ar-AA1o1L0L?ocid=BingNewsSearch (last visited 2024/05/27)

2. JURIST News, Japan PM unveils international framework for generative AI governance, 2024-05-03, https://www.jurist.org/news/2024/05/japan-pm-unveils-international-framework-for-generative-ai-governance/# (last visited 2024/05/30)

3. The Government of Japan, The Hiroshima AI Process: Leading the Global Challenge to Shape Inclusive Governance for Generative AI, 2024-02-09, https://www.japan.go.jp/kizuna/2024/02/hiroshima_ai_process.html (last visited 2024/05/29)

4. Hiroshima Process International Code of Conduct for Organizations

本報告之智慧財產權歸屬於國發會

Developing Advanced AI Systems, 2023-10-30, https://digital-strategy.ec.europa.eu/en/library/hiroshima-process-international-code-conduct-advanced-ai-systems (last visited 2024/05/28)

5. Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI System, 2023-10-30, https://digital-strategy.ec.europa.eu/en/library/hiroshima-process-international-guiding-principles-advanced-ai-system (last visited 2024/05/28)

參、 數位監管

一、 美國

(一)2024 年 4 月《保護美國人免受外國對手應用程式侵害法案》（Protecting Americans from Foreign Adversary Controlled Applications Act）生效，延長受規範主體出售持股之期限

早在今年(2024 年)3 月 13 日，美國眾議院曾正式表決通過《保護美國人免受外國對手應用程式侵害法案》（Protecting Americans from Foreign Adversary Controlled Applications Act），所有由「外國敵對勢力控制的應用程式」若對國內造成國安威脅，則必須在法案生效後的 6 個月內拆分在美國之業務及出售持股，且收購公司或新成立公司的營運必須完全獨立自主，不得與原事業有任何往來或合作關係，包括演算法或數據分享等。而相關收購案也須經過主管機關審查，確認其出售之後已完全脫離外國敵對勢力的控制，直到分拆業務為止，美國的虛擬主機服務提供者，始得為其架設網站；若超過期限而未出售，其將從應用程式商店和基於網路的託管服務中被關閉，永久被排除在美國的 Google Play、Apple App Store 等軟體商城之外。

攤開美國商務部所列的外國敵對勢力清單，中國大陸和香港、古巴、伊朗、北韓、俄國都在名單之列。然而，擁有 1.7 億美國用戶的短影音平臺 TikTok 在美國極為盛行，且盛傳 TikTok 似將所蒐集的美國

本報告之智慧財產權歸屬於國發會

用戶個人資料提供北京政府，因而成為該法案首當其衝的頭號目標。故法案當中即點名 TikTok，甚至強調其母公司字節跳動（ByteDance）未來推出的應用程式亦在禁止之列，故該法案又俗稱 TikTok 禁令。

該法案為美國迄今針對數位平臺所採取最激進的立法措施，封禁影音平臺在美國境內之營運引來兩黨部分議員的反對，認為這個法案既不能有效保護國家安全，又可能箝制言論自由，立法思維過於狹隘。甚至有議員呼籲不要用專制政權的手段來對付專制政權，應該採取更廣泛的行動措施解決數位平臺的問題，例如讓使用者充分理解風險之後，自行決定是否使用 TikTok；因此該法案在參議院面臨比眾議院更大的阻力。事實上，美國蒙大拿州先前亦曾在 2023 年 5 月公佈相似禁令，預定於 2024 年 1 月施行，但遭 TikTok 以違反美國憲法第一修正案為由提起訴訟，2023 年 11 月美國聯邦地區法院認為蒙大拿州在全州範圍內制訂該禁令已逾越州政府的權力行使範疇，且為審理是否有違反憲法保障之言論自由，遂先作成暫停施行之裁定。

為化解眾議院內部各項關於國家安全法案的分歧，共和黨籍眾議院議長強生（Mike Johnson）試圖拉攏民主黨的支持使法案順利過關，於審議 2024 年度的國安補充撥款法案時遂提出將援外法案裂解成獨立法案的發想，而 TikToK 禁令則屬其他國安需求之類別而包裹在另外一個法案中進行單獨的審議及表決，為兩黨創造更多妥協空間，以便在個別議題上尋求最大公約數。4 月 20 日下午，眾議院以 360 票贊成 58 票反對通過《透過力量實現 21 世紀和平法案》(21st Century Peace through Strength Act)，爾後以四案合一的包裹方式送交參議院審議表決，於當地時間 23 日晚間美國參議院通過該單一修正案，24 日再經美國總統拜登（Joe Biden）簽署後正式生效。該 HR8038 法案包含對以色列、烏克蘭、印太區域安全的 3 項援助法案，至於強制 TikTok 脫離中國大陸母公司字節跳動的措施則位在法案的 D 章節，此部分名為「保護美國人免受外國對手控制應用程序侵害」，實質上乃與眾議院上月通過的法案類同，僅在出售期限上與眾議院上月通過的版本不同，

本報告之智慧財產權歸屬於國發會

其理由在強調該法案首在以「撤資」為核心，故從原先 6 個月之限期展延至 1 年，而此 1 年期限包含法案生效後 270 天內讓受規範者脫售持有股份，如於出售期限屆期之際，倘在任何收購階段已取得進展或近乎完成撤資之目標，總統基於職權可額外授權給予 90 天寬限期以便完成交易程序。從而當前受第一波影響的 TikTok 得暫時在美國市場續命，惟若終局倘未能出售其在美資產及持股而達完全剝離母公司控制之進程，仍舊必須面臨業務全面下架並禁止在美國境內運營的結果。

惟 TikToK 借鑒在蒙大拿州之經驗，表示將同樣基於違反美國憲法第一修正案所保障之言論自由採取法律行動，擬透過司法救濟途徑爭取其在市場上繼續運營的空間。若期間法院未作成任何決定，自法案生效日（2024 年 4 月 24 日）起算 270 天，正值落在下一任總統就職前一天，即 2025 年 1 月 19 日之前，字節跳動公司必須出售 TikTok 在美之業務及資產，屆期未出售則將從 Apple App Store 或 Google Play 等應用程式商店全面下架 TikTok 及其更新版，否則應用程式商店將面臨依用戶數量計算的等比例罰款，另外其他網路服務供應商也將封鎖 TikTok 進行網路存取。

從 HR8038 法案的通過可透析兩個重要訊息：

1. 美方體認到社群媒體強大的認知影響力：此前有關數位平臺演算法如何推薦特定內容的曝光不易由法律監管，任何措施皆須在美國憲法第一修正案的框架下進行，避免任何人對言論自由和獲取資訊施加限制，因而法案改以不公平競爭之角度為外衣，迫使敵國之外國企業出售技術和資產，防免其透過不透明的演算法操縱美國人民的行為判斷。

2. 從法案的性質上綱到國家安全層次觀察：可探知該法案為美中在科技領域角力下之產物，阻止中國大陸將數據資料武器化，由於中國大陸從 2017 年起，陸續通過《國家情報法》、《網絡安全法》和《數據安全法》等國安法規，明文規定如為

本報告之智慧財產權歸屬於國發會

維護國家安全或調查犯罪，有關單位可以調取數據，而握有數據的私人企業或個人只能依法配合，同時北京政府也大力整頓網路科技業者，目的之一就是提高國家對企業收蒐集數據的控制，產生干預美國內政之風險。

此外，HR8038 法案的通過亦有副作用之遺緒產生：

1. 法案有違憲之虞：該法案係以國家安全為由限制言論自由，但須有重大或急迫危險之情事始得為之，如今即使能證明 TikTok 被用來傳播中國大陸的影響力，全面禁用仍可能被認定為手段失衡，此可自美國最高法院 1965 年之判決先例參照(美國郵局限制中國大陸共產黨宣傳共產主義思想)。

2. 由美國科技巨頭出面收購會產生另一市場壟斷的疑慮：在 Microsoft 公司有 LinkedIn、Google 公司有 YouTube 的 Shorts 以及 Meta 有 Reels 等短影音程式的情形下，由前述任何一間科技公司承接其業務或資產均有可能在收購 TikTok 後形成獨占地位。

3. 字節跳動公司能否出售 TikTok 在美之業務及資產存有極大變數：由於字節跳動公司是中國大陸公司，根據中國大陸相關禁止出口技術名單，展開出售案前還得經過中國大陸政府同意，但當前國際局勢幾乎不存在出售 TikToK 美國業務的可能性。

4. 順利與中國大陸脫鉤反而無法取得關鍵演算法：法案雖要求出售後所有業務技術都要與母公司脫鉤，但最重要的是核心演算法是由中國大陸的工程師開發，承接業務的公司勢必得自行投入成本再開發演算法。

5. 禁用前的數據資料仍掌握在母公司手上：即便 TikTok 蒐集這些資料的年份如期停留在 2025 年屆滿日便不再更新，但常人

本報告之智慧財產權歸屬於國發會

可能從未意識到，該政府禁令未明文要求字節跳動公司刪除先前已經轉移到手的資料。

最後，法案設計上存有結構性問題，即便科技公司順利出售業務，但其先前既有的資料仍可能賣給資料掮客轉手洗源頭，最終仍落入敵國競爭對手。因此 TikTok 遭全面下架仍無法阻擋北京政府從資料掮客及其他社群媒體平臺購買美國用戶的數據及個資，美方若擔心資料收集，應透過全面性隱私保護法規之立法，除管制所有社群媒體平臺和科技公司自用戶身上截取到資料外，亦賦予用戶知悉個人數據的收集概況，並讓用戶得隨時取消共享，以及更正或刪除自己的數據，另外還應明確界定針對性別、種族、性向、政治立場等需額外保護的機敏資料類別。

資料來源：

1. CNN, House passes legislation that could ban TikTok in the US amid high-stakes vote on foreign aid, 2024-04-20, https://edition.cnn.com/2024/04/20/tech/house-passes-legislation-that-could-ban-tiktok-in-the-us-amid-high-stakes-vote-on-foreign-aid/index.html (last visited 2024/04/24)

2. Rolling Stone, Foreign Aid Package for Ukraine, Israel… and TikTok Ban Passes House, Frustrating MAGA Republicans, 2024-04-20, https://www.rollingstone.com/politics/politics-news/foreign-aid-package-ukraine-israel-tiktok-ban-passes-house-1235008037/ (last visited 2024/04/24)

3. CNN, Biden Signs TikTok Ban Bill Into Law, Forcing ByteDance to Sell TikTok in Nine Months Or Risk Being Banned, 2024-04-24, https://www.ign.com/articles/biden-signs-tiktok-ban-bill-into-law-forcing-bytedance-to-sell-tiktok-in-nine-months-or-risk-being-banned (last visited 2024/04/24)

4. Associated Press News, A bill that could ban TikTok advances to the Senate. What's next?, 2024-04-21, https://apnews.com/article/tiktok-ban-bytedance-bill-divest-

本報告之智慧財產權歸屬於國發會

5b5a685e8f1e19d22182d62526bf19b8 (last visited 2024/04/24)

5. Library of Congress, H.R.7521 - Protecting Americans from Foreign Adversary Controlled Applications Act, 2024-03-07, https://www.congress.gov/bill/118th-congress/house-bill/7521/text (last visited 2024/04/22)

6. GovTrack, H.R. 8038: 21st Century Peace through Strength Act, 2024-04-17, https://www.govtrack.us/congress/bills/118/hr8038/text (last visited 2024/04/23)

二、 法國

(一)2024 年 5 月法國資訊自由委員會（CNIL）發布對數位空間監管及保護之法案

2024 年 5 月 24 日，法國資訊自由委員會（CNIL）發佈了一份關於 2024 年 5 月 21 日數位空間監管及保護之法案（第 2024-449 號法案，下稱法案）的聲明，旨在保護和監管數位空間。

根據法案內容，數位空間通常指的是網際網路上的虛擬環境，其中包括各種線上服務和平臺，如社交媒體、網路商店、數位媒體和其他形式的線上互動，包含任何透過數位技術進行的通訊和交易活動。該法案認為應積極對數位空間進內容進行管理，包含用戶隱私保護，以及防止未成年人接觸不當內容之相關規範與措施。例如，確保網路成人內容不被未成年人閱覽之系統驗證要求，以及對違反這些規定的網路服務提供者可能面臨的法律後果。這些規定強調了在數位空間中維護法律和道德標準的重要性。該法案的規範內容大致如下：

1. 對未成年人之不當內容限制：該法案要求數位空間及網路服務提供者必須設立妥善措施，以確保色情內容對未成年人無法閱覽。

本報告之智慧財產權歸屬於國發會

2. 限制性內容之技術要求：數位空間及網路服務提供者必須設立一個技術參考框架，使限制性內容接觸之年齡驗證系統得以發揮效用，同時保護數位空間之用戶之隱私。

3. 違反法律之罰則：如果網路服務提供者未能遵守相關規定，CNIL 以及其它主管機關可以發出正式警告，並在必要時施以罰款，罰款金額需考慮違規性質、嚴重性與持續時間，最高可達全球營業額的 4%，或 500,000 歐元。

4. 在數位環境中保護法國國民：包含加強數位教育，以及加強對網路社群霸凌監管等措施。

5. 加強資料經濟之信任與競爭：包含對雲端科技相關服務提供者之監管與規範。

6. 對可貨幣化數位標的與遊戲經濟之監管：監管範圍包含線上博弈、抽獎或可交易之線上遊戲數位內容等，並包含對服務提供者之罰則。

7. 監督法院在行使司法權能時對個人資料之處理：說明應依權力分立原則，以其它部門權力監督司法機關對個人資料之處理。

對以上法案內容，CNIL 發布聲明表示，該法案之實施符合歐盟之數位空間相關規定，包含《資料治理法》（DGA）以及《數位服務法》（DSA），旨在加強網路使用者保護，特別是未成年人之保護。CNIL 將處理資料利他之相關請求，並審理國家資料利他主義組織（OAD）之登記，以促進資料安全以及共享。整體而言，該法案以及 CNIL 的說明強調了數位空間監管的重要性，以創建一個更安全的網路環境，CNIL 將積極準備相關執法。

資料來源：

本報告之智慧財產權歸屬於國發會

1. DataGuidance, France: CNIL publishes statement on law transposing Digital Services Act, 2024-05-28, https://www.dataguidance.com/news/france-cnil-publishes-statement-law-transposing-digital (last visited 2024/06/05)

2. CNIL, La loi visant à sécuriser et réguler l'espace numérique (SREN) renforce la protection des internautes en confiant de nouvelles missions à la CNIL, 2024-05-24, https://www.cnil.fr/fr/sren-loi-securiser-reguler-lespace-numerique-nouvelles-missions-cnil (last visited 2024/06/05)

3. Legifrance, LOI n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, 2024-05-22, https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000047533100/ (last visited 2024/06/05)

4. Legifrance, LOI n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (1), 2024-05-22, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049563368/ (last visited 2024/06/05)

肆、 數位身分

一、 歐盟

(一)2024 年 4 月歐盟與日本合作協力推動數位身分、半導體和人工智慧領域的計畫

於 2024 年 4 月 30 日，歐盟和日本於布魯塞爾舉行第二次數位合作夥伴會議（Digital Partnership Council），由多位歐盟和日本之官員共同主持會議。歐盟和日本再次強調戰略夥伴關係的重要性，以促進推動共同之價值和願景，實現以人為本和尊重基本權利之數位轉型，透過會議評估自第一次數位合作夥伴會議後之計畫進展，商議可交付之成果清單，進一步在 AI、5G、半導體等數位技術領域合作，加強在資

本報告之智慧財產權歸屬於國發會

料、平臺經濟、海底電纜、數位身分識別（eID）和網路安全方面的合作。

有關數位身分之主要成果為歐盟和日本於 2024 年 4 月 30 日簽署數位身分和信任服務的合作備忘錄，建立歐盟和日本之間對數位身分的共識，減少雙方溝通成本並提高合作效率，為電子商務和商業機會創造效益。將在歐盟數位身分和信任服務的基礎上，透過合作和案例應用，促進資料的自由流動和信任。

有關 AI 治理，其主要成果為歐盟 AI 辦公室強化與日本 AI 安全研究所之間的合作，鼓勵日本企業參與由歐盟執委會發起的人工智慧公約（AI Pact），幫助在人工智慧法案（AI Act）生效和適用之前，儘早遵守該法的條款。

有關資料流動，其主要成果為將繼續合作開發歐洲與日本之間的直接連接的海底電纜基礎設施，以促進商業機會、可信賴的跨境資料傳輸。

資料來源：

1. European Commission, EU and Japan advance joint work on digital identity, semiconductors, artificial intelligence, 2024-04-30, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2371 (last visited 2024/05/02)

二、 英國

(一)2024 年 5 月英國發布建立政府身分服務的身分確認原則指引（Identity assurance principles for building identity services in government）

英國政府為了維護個人權利並提高身分確認服務（identity assurance services）的透明度，於 2024 年 5 月 3 日由其隱私與消費者

本報告之智慧財產權歸屬於國發會

諮詢小組（Privacy and Consumer Advisory Group, PCAG）發布一套全面的建立政府身分服務的身分確認原則指引，旨在將控制權交還給使用者，塑造健全之身分管理制度。其採行原則包括使用者控制（user control）、透明度（transparency）、多重性（multiplicity）、資料最小化（data minimization）、資料品質（data quality）、使用者存取和可攜性（service user access and portability），以及認證（certification）、爭議解決（dispute resolution）和例外情況（exceptional circumstances）面向，以下闡述這些原則之意涵：

1. 使用者控制原則：

   個人有權決定對其有影響的身分確認作為，在進行此類作為前，必須取得使用者的同意。使用者並可根據自己的需求使用多種身分識別形式，有權利自主決定保留更新記錄。

2. 透明度原則：

   只有在使用者完全知情的條件下，身分確認服務才能以使用者可理解的方式進行。

3. 多重性原則：

   使用者可以任意使用和選擇不同的識別形式。

4. 資料最小化原則：

   提供之服務僅蒐集所需之最低限度資料。

5. 資料品質原則：

   使用者得自主選擇何時更新記錄。

6. 使用者存取和可攜性原則：

本報告之智慧財產權歸屬於國發會

可以提出申請取得個人之資料，且得隨時移轉或刪除個人資料。

7. 認證原則：

所有服務之參與者都必須根據共同的管理標準進行認證。

8. 爭端解決原則：

若發生爭議，使用者可以向獨立第三方尋求解決。

9. 例外情況：

例外情況必須經過議會批准，並受到獨立之審查。

上述原則滿足個人的需求，重視個人之隱私與個人之控制權，每項原則都同等重要，各有特定之作用，適用之範圍限於身分確認服務中的資料處理，認證程序、與獨立第三方機構合作以及透明的紛爭解決機制是確保這些原則實踐不可或缺的要素；若有偏見或符合例外之情形必須受到審查，以維護公眾的信任。

資料來源：

1. GOV.UK, Identity assurance principles for building identity services in government, 2024-05-03, https://www.gov.uk/government/publications/identity-assurance-principles-for-identity-services-in-government/identity-assurance-principles-for-building-identity-services-in-government (last visited 2024/05/10)
2. BIOMETRIC, New identity assurance principles introduced by UK Government, 2024-05-08, https://www.biometricupdate.com/202405/new-identity-assurance-principles-introduced-by-uk-government (last visited 2024/05/10)

本報告之智慧財產權歸屬於國發會

三、瑞士

(一)2024 年 3 月瑞士下議院通過數位身分法案（e-ID）

瑞士聯邦國會下議院（Swiss National Council）於 2024 年 3 月 14 日以 175 票通過《數位身分憑證暨數位憑證之聯邦法案》（Federal Act on Electronic Identity Credentials and Other Electronic Credentials），強化個人資料之保護，並完成審查使用於開發數位身分系統之預算為 1 億法郎（約新台幣 35.6 億），下一步將由瑞士聯邦國會上議院與國務委員會通過，計劃於 2026 年推出數位身分證，使人民在虛擬世界能夠輕鬆的識別自己之身分，該法案包含以下重點：

1. 自願與無償原則（Free and voluntary）

   數位身分是無償且自願性質，並不會取代目前發行之實體身分證及護照證件，預計在 2023 年至 2028 年期間進行試辦。未來將可以在各類服務中使用數位身分，例如，護照申辦服務、管理居住證明等。

2. 去中心化之資料儲存方式（decentralized data storage）

   使用者透過下載政府提供的應用程式，以相機掃描瑞士發行之身分證，並上傳照片，透過瑞士聯邦警察局（Federal Office of Police）對比檢查資料之真實性，可將商業登記、門票、會員卡等文件以數位憑證存於手機，瑞士聯邦警察局並定期對系統進行安全性稽查。

3. 基礎設施與數位身分之權責組織

   由資訊科技和電信辦公室（Federal Office of Information Technology and Telecommunications）提供數位身分所需之信任基礎設施。由瑞士聯邦警察局負責發行數位身分。

資料來源：

本報告之智慧財產權歸屬於國發會

1. The Federal Assembly — The Swiss Parliament, Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise Loi fédérale sur l'identité électronique et d'autres moyens de preuves électroniques, 2024-03-14, https://www.parlament.ch/en/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=64096#votum20 (last visited 2024/04/18)

2. Werbewoche, New bill on electronic ID goes down well in the National Council, 2024-03-14, https://www.werbewoche.ch/en/digital/2024-03-14/neue-vorlage-zu-elektronischer-id-kommt-im-nationalrat-gut-an/ (last visited 2024/04/18)

3. Biometricupdate, Switzerland presents national digital ID, adoption expected in 2026, 2023-11-24, https://www.biometricupdate.com/202311/switzerland-presents-national-digital-id-adoption-expected-in-2026 (last visited 2024/04/18)

伍、 資訊隱私

一、 歐盟

(一)2024 年 4 月歐洲資料保護委員會發表對「同意或付費」（Consent or Pay）模式的意見

2024 年 4 月 17 日歐洲資料保護委員會（European Data Protection Board, EDPB）針對大型線上平臺採用的「同意或付費」（Consent or Pay）模式提出意見。所謂「同意或付費」模式係指線上平臺在用戶使用服務前提供兩個同意資料蒐集與否之選項，同意線上平臺蒐集用戶個資以投放廣告，或付費以避免提供個資。

本報告之智慧財產權歸屬於國發會

EDPB 主席 Anu Talus 表示：「線上平臺採用『同意或付費』模式時應該為用戶提供合理的選項。許多平臺要求用戶提供個資，否則付費。因此，大多數用戶會同意提供個資以便使用該平臺的服務，但他們不了解這個選擇真正的意涵。」

在意見中，EDPB 認為如果平臺只讓用戶在提供個人資料和付費之間做出選擇，那麼不太可能形成有效的同意，因為平臺很難證明用戶的同意是基於自願性的。EDPB 建議大型線上平臺需要提供一種「等價的替代方案」，該替代方案必須是免費的，並且不涉及蒐集個人資料以執行廣告之行為。任何平臺向用戶收取的費用都不得強迫用戶同意，並且必須避免負面後果，如排除關鍵服務。EDPB 還強調，平臺獲取用戶的資料時仍須遵守 GDPR 原則：

1. 自由意志給予之同意：線上平臺上的個人資料必須是用戶自願提供的，並且在評估是否為自願時，必須充分考慮平臺方是否有對用戶施予任何強制性手段或壓力。

2. 明確的同意：針對一個或多個特定目的，必須證明當事人有明確之真意，且無異議地表示同意。

3. 知情的同意：當事人必須被充分告知其同意的價值、範圍和後果，以便對行為定向廣告的處理過程有完整和清晰的理解。

4. 同意的撤回：當事人應能隨時撤回其同意；其撤回同意之請求應當和准予同意之流程相當。

資料來源：

1. European Data Protection Board, EDPB: ‘Consent or Pay’ models should offer real choice, 2024-04-17, https://www.edpb.europa.eu/news/news/2024/edpb-consent-or-pay-models-should-offer-real-choice_en (last visited 2024/05/09)

2. European Data Protection Board, Opinion 08/2024 on Valid

本報告之智慧財產權歸屬於國發會

Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, 2024-04-17, https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_en (last visited 2024/05/09)

3. European Data Protection Board, EDPB clarifies notion of main establishment and calls on EU legislators to make sure CSAM Regulation respects rights to privacy and data protection, 2024-02-14, https://www.edpb.europa.eu/news/news/2024/edpb-clarifies-notion-main-establishment-and-calls-eu-legislators-make-sure-csam_en (last visited 2024/05/09)

4. European Data Protection Board, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, 2024-04-17, https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf (last visited 2024/05/09)

二、英國

(一)2024 年 4 月英國資訊委員辦公室發布兒童個資隱私政策

英國資訊委員辦公室（Information Commissioner’s Office, ICO）於 2024 年 4 月 3 日發佈其 2024 至 2025 年兒童法規戰略（Children's code strategy），以保護兒童在網路之隱私。該戰略規定了社交媒體和影音共享平臺在未來一年需要優先改進的領域，以及 ICO 將如何執法並確保遵守兒童守則。

該戰略強調了 2024 至 2025 年的下述重點方針：

1. 隱私和地理位置應預設為私密：ICO 指出，兒童的個人資料應預設為機敏資料、其地理位置定位應預設為關閉，以保護兒童的人身安全和心理健康；

本報告之智慧財產權歸屬於國發會

2. 防止目標導向式投放廣告對兒童個人資料進行分析：ICO 建議除非有令人信服的必要理由，否則預設禁止對兒童之個人資料進行廣告投放分析，以保護兒童的自主權並避免經濟損失；

3. 不得在 AI 自動生成系統中使用兒童資訊：在演算法生成的內容中使用兒童個人資訊，可能導致兒童觸及有害身心內容之風險；

4. 使用 13 歲以下兒童的資料：由於 13 歲以下的兒童不具備法律行為能力，無法同意處理其個人資訊，ICO 強調對兒童資料之利用，應獲得父母同意和使用年齡保證技術 來保護年輕使用者。

此外，該戰略指出 ICO 將：

1. 蒐集證據，與家長和兒童個資保護組織等利害關係人合作，加強監督和執法力度，以解決兒童面臨的隱私風險；

2. 對學校教育科技的使用進行審核，以了解維護隱私權會面臨的挑戰，並確保資料保護合法性；

與其他監管機構和國際合作夥伴合作，有效監管網路。

綜上，英國 ICO 此對兒童資料管制的新政策，對於細部實際行為，包含了兒童的人身地理位置、對兒童的廣告投放、以及 AI 對兒童資料的利用進行了限制監管，若落實執行，應可強化兒童在網路上之隱私權益，可持續追蹤英國官方是否有更新的 AI 或資料相關指引與此政策搭配實施。

資料來源：

1. OneTrustDataGuidance, UK: ICO publishes 2024-2025 strategy for protecting children's privacy online, 2024-04-04,

本報告之智慧財產權歸屬於國發會

https://www.dataguidance.com/news/uk-ico-publishes-2024-2025-strategy-protecting (last visited 2024/05/10)

2. ICO, Protecting children's privacy online: Our Children's code strategy, 2024-04-03, https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/04/ico-sets-out-priorities-to-protect-childrens-privacy-online/ (last visited 2024/05/10)

3. ICO, Protecting children's privacy online: Our Children's code strategy, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/protecting-childrens-privacy-online-our-childrens-code-strategy/#achieved (last visited 2024/05/10)

陸、 競爭法制

一、 義大利

(一)2024 年 4 月義大利前總理 Enrico Letta 受歐盟執委會委託，發布歐盟市場研究報告，表示應督促歐洲市場各大產業整合，促進歐洲市場競爭

義大利前總理 Enrico Letta（即現任 Jacques Delors 研究所所長）受歐盟執委會委託進行歐洲市場研究，於 2024 年 4 月提出《不僅限單一市場》（Much More Than a Market）研究報告，報告針對歐洲內部市場各產業，包含金融服務、能源、電信、醫療保健、航太等產業作出分析並建議歐盟各產業應如何創新發展。

該報告提及歐盟市場在全球市場中的處境，當歐洲事業與發展越來越龐大，外國事業間存在顯著的規模差距，尤其與美國及中國大陸等大型競爭對手相比；這在生產力、創新與就業機會等方面已對歐盟造成不利影響，故歐盟應採取手段增強產業競爭力。

本報告之智慧財產權歸屬於國發會

在戰略自主方面，為實現真正的歐洲自主，特別是在國防相關產業上，歐盟須更進一步發展其自屬工業能力，避免重複在過去歐盟多係依賴非歐洲產地原物料之情況。

歐盟單一市場中，各產業面臨碎片化或規模不足等類似問題，考量到歐盟作為單一市場，當中仍存在許多如競爭或服務提供方面的障礙，而財務市場的碎片化亦導致資金與歐盟家庭儲蓄大量流向國外市場(如美國的國外市場)，這凸顯出歐盟在許多經濟資產方面之不足，故 Enrico Letta 強調規模經濟之重要性，並認為應整合歐盟單一市場內之產業，以促進各產業間事業之合作與整合，來保留或吸引更多資源。歐盟應積極與全球各大市場之大型事業進行競爭，以達成經濟發展、創新與戰略自主之目的。報告提出以下促進整合方法：

1. 新增「第 5 自由(多領域自由)」：原本 4 大市場自由為商品、服務、人才與資本的自由流動，此報告提出第 5 自由，為《歐盟運作條約》（Treaty on the functioning of the European Union, TFEU）中所提出之研究、創新、資料、能力、知識及教育等「多領域自由」，強化市場上第 5 自由等元素以強化歐盟市場。

2. 規模經濟之重要性：應支持歐盟大型事業成長，使歐盟大型事業得以在全球舞台上與來自美國、中國大陸與其他國家的大型事業相互競爭。

3. 法律規範之整合：透過最大限度地簡化歐盟的法律規範，並進一步簡化單一市場框架中之協調、互動成本，強化事業間之合作與競爭，來促進經濟發展。

4. 超國界限制之整合：歐盟須朝整個歐洲市場維度發展，以向美國、中國大陸或印度的大型事業抗衡。

本報告之智慧財產權歸屬於國發會

5. 歐洲尺度/標準之整合：透過簡化歐盟法律規範框架，尺度/標準之統一化，來強化事業間之良性合作與結合，尤其在電信、能源產業之標準方面尤其重要。

6. 金融業之整合：創建儲蓄與投資聯盟，充分利用歐盟市場內包含私人儲蓄之各種資金來源，其他相關手段包含透過國家權力支持補助與公共投資，減少市場碎片化情況。

7. 電信產業之整合：歐盟電信產業現已過度碎片化，分布在 27 個不同成員國中，每個成員國中平均每個電信產業僅服務 500 萬個用戶，該數字遠低於中國大陸、美國破億之用戶量，爰建議歐盟從統一電信產業規範標準一事開始整合。

8. 能源產業之整合：烏俄戰爭使能源市場整合更加緊迫，歐盟應優先針對電力、氫氣、碳捕獲與儲存相關部門進行投資。

9. 國防戰略產業之整合：歐盟國防戰略產業同樣面臨市場碎片化問題，加以整合能減少歐盟對外國勢力與大型事業之依賴，強化國家及市場安全。

10. 航太產業之整合：航太產業不僅與創新、大量經濟規模相關，亦在國防科技戰略方面扮演重要角色，歐盟應鼓勵各國相關產業之合作，能促進單一市場中經濟發展，亦能實現歐盟戰略自主之獨立性。

11. 交通產業之整合：進步的交通網絡能減少各地區間物理障礙，故交通產業之整合能直接促進偏遠地區對於市場資源之近用，更可進一步促進各產業部門之整合與競爭。

12. 維護市場公平競爭：強化歐盟產業之整合，減少依賴外國事業，進一步減少受外國事業之控制，能對市場公平競爭帶來更好的效益。

本報告之智慧財產權歸屬於國發會

綜上，在歐盟單一市場中，各產業面臨碎片化、規模不足等問題，故 Enrico Letta 基於歐盟應積極與全球各大市場之大型事業競爭，並強調規模經濟的重要性之論點出發，提出應透過上述方法手段，以促進各產業間事業之合作與整合，以達成經濟發展、創新與戰略自主之目的。

資料來源：

1. consilium.europa , MUCH MORE THAN A MARKET, 2024-04, https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf (last visited 2024/06/05)
2. 2European Commission, Enrico Letta's Report on the Future of the Single Market, 2024-04-10, https://single-market-economy.ec.europa.eu/news/enrico-lettas-report-future-single-market-2024-04-10_en (last visited 2024/06/05)
3. Cencenelec, CEN and CENELEC welcome the vision of Enrico Letta for a strengthened Single Market, 2024-04-19, https://www.cencenelec.eu/news-and-events/news/2024/brief-news/2024-04-19-letta-report/ (last visited 2024/06/05)

本報告之智慧財產權歸屬於國發會

項次 3. 八月雙月報

壹、AI 法制政策

一、美國

(一)2024 年 5 月美國加州參議院通過人工智慧透明度法案（SB942）進入司法委員會審理，二讀修訂後於 8 月 7 日舉行第一次聽證會

於 2024 年 5 月美國加州參議院（California State Senate）通過加州人工智慧透明度法案（California AI Transparency Act），該法案於 2024 年 1 月由參議員 Becker 所提出，將要求被涵蓋之 AI 提供者（Covered provider）建置 AI 檢測工具（AI detection tool）給予使用者識別該 AI 提供者提供之文字、圖像、影片等內容，是否屬於 AI 之修改或為 AI 所創造。法案所指被涵蓋之提供者，係指提供生成式 AI 系統者，其所提供之 AI 系統在過去 12 個月中平均每月訪問量或使用者數量超過 100 萬，並可在加州範圍內公開連結。此外，法案亦要求檢測工具必須能夠在網路上公開取得並保護工具使用者之個人資料，被涵蓋之提供者在 AI 系統生成之圖像、文字等內容中揭露明顯之資訊，最後，被涵蓋之提供者必須實施合理程序以防止未進行揭露而提供下游使用生成式 AI 系統。若被涵蓋之提供者違反法案之規定，每次將被處以 5,000 美元之罰款。

本法案 5 月已經由參議院通過，進入消保及隱私委員會於 6 月通過，再進入參議院司法委員會審理，經 7 月二讀修訂後，已於 8 月 7 日進行第一次聽證會。

資料來源：

1. California Legislative Information, SB-942 California AI Transparency Act, 2024-05-16 , https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB942 ,(last visited 2024/06/14)

本報告之智慧財產權歸屬於國發會

2. HuschBlackwell, California AI Legislation Update: June 5, 2024, 2024-06-05, https://www.bytebacklaw.com/2024/06/california-ai-legislation-update-june-5-2024/, (last visited 2024/06/14)

(二)2024 年 6 月美國財政部公告針對金融服務領域 AI 的使用、機會和風險進行意見徵集

於 2024 年 6 月美國財政部（U.S. Department of the Treasury）公告針對金融服務領域 AI 的使用、機會和風險進行意見徵集。本次意見徵集係以美國財政部近期與其他聯邦機構於 AI 的網路安全與詐欺面向推出或採取各項措施為基礎，就 AI 在金融服務領域的應用以及 AI 在該行業的發展及應用所帶來的機會和風險徵求公眾意見，以了解促進金融機構負責任地使用 AI 之潛在障礙；受到金融機構使用 AI 影響的企業、監管機構、最終使用者或其他實體及其影響程度；以及關於適用於金融服務領域之 AI 立法、監管與框架的建議。

以下概述美國財政部欲深入了解之 AI 使用內容：

1. 提供之產品和服務：

   金融機構如何利用 AI 協助做出與提供金融產品或服務有關的決策，例如是否提供交易帳戶、信貸或保險，以及此類產品的條件，還有金融預測產品和模式識別工具。

2. 風險管理：

   金融機構如何使用 AI 管理各種類型的風險，包括信用風險、市場風險等。

3. 資本市場：

   金融機構如何利用 AI 協助資本市場活動，包括確定投資機會、分配資本、執行交易及提供金融諮詢服務。

本報告之智慧財產權歸屬於國發會

4. 內部營運：

金融機構如何利用 AI 管理內部營運，例如薪資、人力資源職能、培訓、績效管理、通訊、網路安全、軟體發展以及其他內部營運事務。

5. 客戶服務：

金融機構如何在客戶管理中使用 AI，包括投訴之處理、投資者之關係或其他面向的外部功能。

6. 監理合規性：

金融機構如何使用 AI 進行監管，包括資本流動性、監管報告或揭露要求、銀行保密法與防洗錢（BSA/AML）、消費者與投資者保護以及許可證管理。

7. 行銷：

金融機構如何使用 AI 向個人、團體或機構交易對手行銷。

本次意見徵集主要期望針對與金融服務領域相關之利害關係人皆能提供意見，包括提供、促進及接受金融產品或服務之生態系參與者、消費者、小型企業、學者、非營利組織及其他對此領域有興趣者，並鼓勵相關參與者提供具體案例或數據，意見徵集期限為 60 天。

資料來源：

1. U.S. DEPARTMENT OF THE TREASURY, U.S. Department of Treasury Releases Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector, 2024-06-06, https://home.treasury.gov/news/press-releases/jy2393,(last visited 2024/06/27)

本報告之智慧財產權歸屬於國發會

(三)2024 年 7 月美國紐約州金融服務廳發布人工智慧於保險運用之通知

2024 年 7 月美國紐約州金融服務廳發布人工智慧於保險運用之通知（Circular Letter），主要針對保險公司在承保和定價過程中使用人工智慧系統（artificial intelligence systems, AIS）及外部消費者資料與資料來源（external consumer data and information sources, ECDIS）的指導原則，以下是主要重點：

1. 定義和範圍：本通知明確了 AIS 和 ECDIS 的定義，並強調這些技術的使用必須符合相關法律和法規。其中所謂 AIS 係指任何以機器為基礎之系統，用以執行通常與人類智慧活動相關之功能，例如以推理、學習、自我改善功能，整體或部分用以協助或代理傳統之健康、人壽、財產或傷害保險之承保或定價，或識別得以協助申請人之保險或定價評估的生活方式指標，以確定保險之範圍。至於本通知目的下之 ECDIS 範圍，則包括得全部或部分用於補充傳統之醫療、財產或傷害保險或定價之數據或資訊，有助於保險申請人之承保或定價之評估。

2. 公平原則：保險公司依據聯邦法律，不得將 ECDIS 或 AIS 用於處理承保或定價相關程序，除非其可以透過綜合評估，證明所使用的資料和模型不會導致不公平或非法的歧視，該綜合評估最少應該包括三個步驟：

   步驟一、為評估使用 ECDIS 或 AIS 是否會導致對同類或類似情況之被保險人或受保護類別之被保險人的承保或定價決定，產生不合乎比例或不利之影響；

   步驟二、若對於類似情況之被保險人形成差異的判斷，是否具備合理、合法且公平之解釋或理由；

本報告之智慧財產權歸屬於國發會

步驟三、應採取得以符合保險公司法定業務需求之歧視性較小的替代變數或方法進行搜尋或分析，並進行適切之紀錄。

若有對 ECDIS 或 AIS 進行重大更新或更改時，應定期進行不公平或非歧視性測試及分析，並須進行量化及質化指標之評估。

3. 治理和風險管理：保險公司應建立適當的治理框架和風險管理程序，確保高階管理層和董事會對 AIS 和 ECDIS 的使用進行有效監督。包括須建立適切之內部政策、程序及相關文件，明確各項角色、職責與對高階管理層報告之義務，以及必要相關文件之製作、保留與銷毀之流程；同時必須建立風險管理、內部控制程序，以及對第三方供應商之評估程序與合約必要條款。

4. 透明度：由於外部數據來源可信度及準確度之不穩定，保險公司應向消費者揭露其使用 AIS 和 ECDIS 的情況，包括保險公司於承保與定價過程中有使用 AIS、保險公司是否有自外部供應商取得當事人資料、以及告知當事人有權索取影響該成本或定價決定之具體數據等資訊、提供相關資料的查詢和更正機制，且不應以供應商之數據演算法專有為由作出不利承保或定價之決定。

資料來源：

1. Department of Financial Services, Insurance Circular Letter No. 7, 2024-07-11, https://www.dfs.ny.gov/industry-guidance/circular-letters/cl2024-07, (last visited 2024/07/26)

(四)2024 年 7 月美國發布 AI 行政命令進度報告，說明 2023 年 10 月迄今執行情形

本報告之智慧財產權歸屬於國發會

有鑑於生成式 AI 與相關服務日趨成熟，但也衍生政策、法制爭議，例如：AI 訓練資料或生成內容可能侵害智慧財產權、涉及假訊息、色情或暴力等隱憂，對民主與法制構成挑戰。爰美國於 2023 年 10 月發布「開發及使用安全、可靠且可信賴之人工智慧之行政命令（Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence）」，並以可責性（accountability）為核心，兼顧價值、安全與創新。

該行政命令源於自 2023 年 5 月起，白宮陸續邀集 Alphabet、Anthropic、微軟及 Open AI 等重要 AI 服務提供者進行會談。且聯邦政府承諾將持續投資 AI 科技研發，並與業者探討 AI 產品、服務可能衍生之風險及疑慮，遂要求相關企業具體承諾，確保其產品、服務安全、可靠且可資信賴，當時也已取得 Open AI、微軟、Amazon、Google、Meta、Anthropic 以及 Inflection 在內的 15 家企業承諾。

嗣美國白宮於 2024 年 7 月 26 日發布新聞，說明此一 AI 行政命令進度報告。說明在前述 15 家企業承諾的基礎上，目前聯邦政府相關部門執行該命令 270 日後之成果摘要，例如：國家標準與技術研究院（National Institute of Standards and Technology, NIST）於 2024 年 7 月陸續發布管理生成式 AI 風險及安全開發生成式 AI 系統與兩用基礎模型框架（frameworks on managing generative AI risks and securely developing generative AI systems and dual-use foundation models）與其相關文件，如 SP 800-218A ，以供安全開發生成式 AI 系統之參考。

承上，美國 NIST 轄下之人工智慧安全研究所（AI Safety Institute, AISI）前於 2024 年 4 月就四份參考文件對外徵詢意見，包含：1. NIST AI 600-1，AI 風險管理框架:生成式 AI 概況（AI RMF Generative AI Profile）；2. NIST SP 800-218A，生成式 AI 及軍民兩用基礎模型之軟體開發安全實踐（Secure Software Development Practices for Generative AI and Dual-Use Foundation Models ）；3. NIST AI 100-4，減少合成內容之風險（Reducing Risks Posed by Synthetic Content ）；4. NIST AI 100-

本報告之智慧財產權歸屬於國發會

5，AI 標準全球參與計畫（A Plan for Global Engagement on AI Standards）。AISI 並於同年 7 月就 NIST AI 600-1、NIST SP 800-218A 以及 NIST AI 100-5 三份文件發布最終版本，這些參考指引或文件可協助研發人員防止功能日益強大之 AI 系統被濫用，而導致損害個人、公共安全及國家安全，以及協助其提高產品透明度等。

目前 NIST 與所屬單位提供之參考指引或最佳實踐等文件，係依循先前 NIST 發布之 AI 風險管理框架（AI Risk Management Framework, AI RMF）。此一 AI RMF 框架為提供個人、組織及社會各界管理 AI 風險之參考，並已在美國與其他國家被廣泛採用。此外，搭配此一 AI 行政命令進度報告，美國希冀持續透過聯邦政府相關部門採行之措施，持續落實將 AI 人才引入政府、推動負責任之 AI 創新，及提升美國在國際間之影響力等。

資料來源：

1. The White House, FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, 2023-10-30, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/ (last visited 2024/08/07)
2. The White House, FACT SHEET: Biden-Harris Administration Announces New AI Actions and Receives Additional Major Voluntary Commitment on AI, 2024-07-26, https://www.whitehouse.gov/briefing-room/statements-releases/2024/07/26/fact-sheet-biden-harris-administration-announces-new (last visited 2024/08/07)
3. NIST, Secure Software Development Practices for Generative AI and Dual-Use Foundation Models | NIST SP 800-218A, 2024-07-26, https://csrc.nist.gov/news/2024/nist-publishes-sp-800218a (last visited 2024/08/07)
4. NIST, Department of Commerce Announces New Guidance, Tools

本報告之智慧財產權歸屬於國發會

270 Days Following President Biden's Executive Order on AI, 2024-07-26, https://www.nist.gov/news-events/news/2024/07/department-commerce-announces-new-guidance-tools-270-days-following (last visited 2024/08/07)

(五)2024 年 7 月美國聯邦通訊委員會發布監管人工智慧生成之政治廣告擬議規則制定通知

2024 年 7 月美國聯邦通訊委員會（Federal Communications Commission, FCC）發布人工智慧生成之政治廣告擬議規則制定通知（Notice of Proposed Rulemaking, NPRM）徵求公眾意見。由於政治節目為廣播業者服務公眾利益的重要元素，旨在讓人民能獲得正確的選舉資訊，對於實現民主的運作亦至關重要。隨著生成式 AI 工具的發展，政治廣告運用 AI 技術亦為從事政治活動之候選人等帶來相當之益處，例如：可幫助候選人，透過 AI 輔助，針對特定社區訂製廣告投放，讓財務規模較小之競選活動候選人能接觸更多的受眾族群。

惟 AI 技術在政治廣告的使用，可能產生運用生成式 AI 或深偽技術（deepfake）技術等 AI 技術導致所提供之內容並非真實，以產生欺騙性或誤導性訊息，從而造成選民因取得錯誤訊息而混亂。因此，FCC 發布 AI 生成政治廣告 NPRM，透過要求廣播事業及電視廣播事業採取合理措施來解決使用 AI 生成之政治廣告內容可能產生潛在之虛假、誤導性或欺騙性訊息，以使選民能夠獲得正確資訊，從而促進公共利益。此 NPRM 要求廣播事業及電視廣播事業採行以下措施：

1. 須詢問任何購買政治廣告播放時間之人，所提供之廣告是否包含 AI 生成內容。

2. 須於播出前或播出期間使用標準化語言（standardized language）揭露使用 AI 生成內容的政治廣告。若為廣播節目，建議於廣播中透過清楚、明確且速度易於理解之聲音進行口

本報告之智慧財產權歸屬於國發會

頭說明。若為電視廣告，則建議於廣告前或期間，透過清晰、明確且可理解之速度進行口頭說明，或採取視覺上文字等於或大於垂直畫面百分之四之標示顯示該聲明至少 4 秒。

3. 在廣播事業及電視廣播事業之政治廣告檔案中，包含一份使用生成式內容通知之文件，以揭露每次政治廣告購買者運用 AI 之使用情況，同時符合開放政府資料法（OPEN Government Data Act）之要求。

4. 針對揭露要求如何適用於嵌入在網路（embedded in network）或聯賣節目（Syndicated Programming）之政治廣告， FCC 並藉由此次 NPRM 徵詢外界建議。

本次 NPRM 主要係針對廣播業者，但其亦擴張適用至參與節目製作的有線電視運營商、直播衛星（Direct Broadcast Satellite, DBS）提供商和受有數位音訊無線電衛星（Satellite Digital Audio Radio Service, SDARS）授權之事業，以及依據美國電信法第 325 條取得許可授權之事業（取得授權得將節目傳輸回美國之事業）。

本次 FCC 提出 NPRM 時，亦意識到相關規則之建立可能與其他聯邦機構或各州之法規產生衝突，故將其擬議之揭露要求，描述為對各州及聯邦選舉委員會（Federal Election Commission, FEC）已進行對於廣告涉及 AI 監管相關政策措施之補充。惟 FEC 主席 Sean Cooksey 仍以信件對 FCC 主席 Rosenworcel 表達異議，認為此項權力屬於 FEC 之專屬管轄範圍，與現行法律及權責劃分有衝突。且 FCC 監管範圍有限，故此 NPRM 僅能規範到 FCC 監管的對象，對於選民在社交媒體或其他地方看到及聽到之政治廣告，若有使用 AI 者則不適用。

FCC 發布之 AI 生成廣告 NPRM，後續尚須經各界討論，並已引發各方激烈辯論，本次意見徵集時間至 NPRM 發布後 30 日。

資料來源：

本報告之智慧財產權歸屬於國發會

1. FCC Attempts to Regulate Artificial Intelligence in Political Advertising Through New Disclosure Requirements - July 2024, 2024-08-02, https://www.jdsupra.com/legalnews/fcc-attempts-to-regulate-artificial-8059453/ (last visited 2024/08/06)

(六)2024 年 7 月美國著作權局發布人工智慧報告第 1 部分，建議應訂定聯邦數位複製法

美國著作權局（Copyright Office）於 7 月發布關於著作權與 AI 相關的法律與政策問題之報告第 1 部分，其中針對涉及數位複製（digital replica）議題做出回應。報告指出，所謂數位複製泛指透過已授權或未授權使用之任何數位方式創建或操縱看似真實但虛假描繪個人之影片、圖像或音訊記錄。數位複製與深偽技術為可相互替代之用詞。鑑於現階段對於未授權之數位複製的保護規範仍不完善，例如聯邦貿易委員會法（The Federal Trade Commission Act)及蘭哈姆法（Lanham Act，即聯邦商標法)等，雖然提供部分保護，但其保護範圍僅限於與商業相關之情況（commercial circumstances)或具有商業價值之知名人士，並未保護一般個人，故建議應訂定聯邦數位複製法（Federal Digital Replica Law)以強化對於個人之保護。

此報告提出之背景為美國著作權局於 2023 年 3 月提出的一項檢視人工智慧（AI）所產生之著作權法律及政策之倡議（an initiative examining copyright law and policy issues raised by artificial intelligence (AI)），目的在廣泛檢視因 AI 而帶來的著作權問題，包括與生成式 AI，以及數位複製引發之著作權相關的問題。美國著作權局於此項計畫下，同步發布了「著作權登記指引：生成式人工智慧」（Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence)，並持續舉辦公眾聽證會及網路研討會，彙整專家學者及民眾關於生成式 AI 有關之數位複製議題的評論，發現未授權之數位複製並未被囊括於現行法規內。而數位複製之應用，已造成包括隱私

本報告之智慧財產權歸屬於國發會

權、不公平競爭、詐欺等法律問題並與著作權息息相關，引發著作權侵害之相關法律適用疑慮，故提出本次人工智慧報告第 1 部分（Part 1 of Artificial Intelligence Report)之研析。

本次人工智慧報告第 1 部分所探討之數位複製並非僅有負面應用，亦有正面之社會意義，例如透過數位複製技術，可以讓無法再親自表演之藝術家透過此一技術再度進行表演。惟綜觀數位複製相關的歷史、風險、現行法律規範之不足，以及未經授權的數位複製作品或服務之生產與散布規模快速提高，所衍生相關法律問題，已非單一面向之著作權議題，國會應該建立另一項聯邦權利，以使任何人免受數位複製行為的侵害並保障其權利，並使該權利可被授權，與其他智慧財產權（著作權、商標權)一視同仁。可以考慮限制授權時效，例如 5 年或 10 年，避免無限制之完全轉讓，同時應配套知情同意機制，確保個人在授權其權利時，已充分瞭解其擬定用途。美國演員工會-美國電視和廣播藝人聯合會（Screen Actors Guild-American Federation of Television and Radio Artists, SAG-AFTRA)為集體談判協議提供一個範例，其中要求有關數位複製權之契約條款必須「明確且顯著」(clear and conspicuous)。此外，對於權利之侵害，數位複製法應訂立相關補救措施，包括提供損害賠償或禁制令等救濟規範，損害賠償則應包括收入損失、名譽損害或精神賠償；禁制令救濟則用以防止持續未經授權使用個人肖像等個人專屬之特徵，或防止未來的違法行為。而後將陸續發布探討全部或部分由生成式 AI 創建產物之著作權，以及在受著作權保護訓練 AI 模型產物上之法律影響、授權原則，以及任何潛在責任的分配。

資料來源：

1. Copyright Office Releases Part 1 of Artificial Intelligence Report, Recommends Federal Digital Replica Law , 2024-07-31, https://www.copyright.gov/newsnet/2024/1048.html (last visited 2024/08/01)

本報告之智慧財產權歸屬於國發會

2. U.S. Copyright Office , Copyright and Artificial Intelligence , 2024-07-31, https://www.copyright.gov/ai/ (last visited 2024/08/01)

3. Copyright and Artificial Intelligence Part 1: Digital Replicas , 2024-07-31, https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-1-Digital-Replicas-Report.pdf（last visited 2024/08/01）

4. Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence , 2023-03-16 , https://www.federalregister.gov/documents/2023/03/16/2023-05321/copyright-registration-guidance-works-containing-material-generated-by-artificial-intelligence (last visited 2024/08/01)

二、英國

(一)2024 年 5 月英國科學、創新及技術部公告徵求人工智慧網路安全的意見，8 月 9 日完成意見徵集

英國科學、創新及技術部（Department for Science, Innovation & Technology, DSIT）於 2024 年 5 月公告徵求各界對「人工智慧網路安全」之意見，並於 8 月初完成徵集。該部考量目前使用 AI 之組織沒有 AI 的網路安全實踐或程序，因此，必須建立相當之機制，以確保設計、開發、部署及維護 AI 運用之安全，遂提出 AI 網路安全的計畫，向公眾徵求意見。又該計畫主要採取自願行為準則之形式，為 AI 供應鏈中的相關參與者制定 AI 安全標準，計畫之重要內容摘述如下：

1. 此計畫將建立自願行為準則，並將該準則納入國際標準發展之研議，以解決 AI 的網路安全風險。該行為準則將建立對於所有 AI 技術安全之基本要求，並區分 AI 供應鏈當中不同利害關係人應扮演之角色。

2. 本次意見徵集並提供預擬自願行為準則，除明確區隔利害關係人之定義外，並指出各類利害關係人應遵循之行為準則。

本報告之智慧財產權歸屬於國發會

(1) 就利害關係人之區隔，行為準則當中區隔出開發者（Developers）、系統營運者（System Operators）、資料/數據控制者（Data Controllers）以及終端用戶（End-users）。其中所謂之「開發者」係指負責創造 AI 模型或系統之任何類型或跨部門的事業、組織以及個人，此處 AI 開發，包括所有類型之專屬或開源的 AI 技術。而創造 AI 之事業或組織若同時負責於其組織中嵌入或部署該 AI 模型或系統，於此準則將同時定義其為開發者及系統營運者。資料/數據控制者則為控制 AI 模型或系統運行所用資料權限及完整性的事業、組織或個人。由於 AI 系統之運行可能涉及多個資料庫，因此一個 AI 系統可能會有多個資料控制者涉入。

(2) 行為準則中提出 AI 安全必要多項原則，並說明各項細部原則適用於前述哪類利害關係人。例如，安全設計（Secure Design）原則，其中提及之提升員工度威脅與風險認知條款，適用於系統營運者、開發者與資料控制者；確保系統設計於功能及性能之安全性條款，則適用於系統營運者等。另外尚有針對安全開發（Secure Development）、安全維護（Secure Maintenance）及安全運用（Secure Deployment）等之基礎原則，皆明列對應之準則條款及適用之利害關係人。

本次意見徵集已於 8 月 9 日結束，整理相關意見後 DSIT 將據以評估相關主題之未來政策方向，並將於後續發布回應。

資料來源：

1. GOV.UK, Call for views on the Cyber Security of AI, 2024-05-24, https://www.gov.uk/government/calls-for-evidence/call-for-views-on-the-cyber-security-of-ai/call-for-views-on-the-cyber-security-of-ai#how-to-respond-to-the-call-for-views-and-our-next

本報告之智慧財產權歸屬於國發會

三、加拿大

(一)2024 年 5 月加拿大安大略省議會公布 2024 年公共部門網路安全強化及信任建立法案

於 2024 年 5 月加拿大安大略省議會（Legislative Assembly of Ontario）公布 2024 年公共部門網路安全強化及信任建立法草案（Bill 194, Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024），安大略省政府意識到網路安全對於公共部門提供數位服務之信任具有重要性，認為應強化公共部門的網路安全，尤其應規範公共部門內 AI 系統的使用，應採取負責任、透明、和安全的方式，以保護隱私並創造安大略省人民之福祉，草案之重點內容摘述如下：

1. 界定適用行為與範圍

(1) 適用於在某些情況下使用 AI 系統的特定安大略省公共部門，包含安大略省政府部門、醫院和大學等。

(2) AI 系統定義為基於機器的系統，為了實現明確或隱含的目標，從接收到的輸入進行推斷，以產生可以影響物理或虛擬環境的輸出，例如預測、內容、建議或決策之機制。又公共部門使用 AI 系統包括使用公開的 AI 系統以及使用由公共部門自行開發或採購或由第三方代表公共部門開發的系統等情形。

2. 使用 AI 系統之要求

公共部門應負責任、透明和安全地使用 AI 系統，因此，公共部門應向公眾提供有關其使用 AI 系統的資訊、制定並實施 AI 系統所使用的問責機制，包括應製作之文件、系統應具備之效能以及監督管理要求等、採取措施來管理與使用 AI 系

本報告之智慧財產權歸屬於國發會

統相關之風險，例如報告之義務或紀錄之保存、依規定進行AI 系統之利用，以及確立應限制或不得使用 AI 系統之情形、揭露相關行為有使用 AI 系統之資訊，並對之進行監督。

綜上所述，安大略省政府已提出該立法草案，目前正由安大略省議會審查法案及就此蒐集公眾意見。

資料來源：

1. JD Supra, New Ontario Bill 194 to Regulate Public-Sector Use of Artificial Intelligence Systems, 2024-06-06, https://www.jdsupra.com/legalnews/new-ontario-bill-194-to-regulate-public-4764006/ (last visited 2024/06/07)
2. Ontario Human Rights Commission ,Bill 194, Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024 , 2024-06-11, https://www.ohrc.on.ca/en/news_centre/bill-194-strengthening-cyber-security-and-building-trust-public-sector-act-2024 (last visited 2024/07/13)

四、 韓國

(一)2024 年 6 月韓國文化觀光體育部召開完善人工智慧著作權制度之第二次全體審議會，預計本年度將持續召集工作會議，預計於年底公佈完善人工智慧相關著作權制度計畫

韓國文化觀光體育部於 2024 年 6 月 28 日召開完善人工智慧著作權制度審議會第二次全體會議，針對上半年分組工作成果、下半年選題、完備制度之討論，提出進展說明。

文稿中指出，必須將作品提供 AI 學習利用，應有適當之補償計畫提出，而目前學習工作小組正在進行「保障人工智慧訓練學習作品之合法使用措施」(인공지능 학습용 저작물의 적법한 이용 권한 확보 방안)之研究，認為自動化系統使用大量受著作權保護的作品來發

本報告之智慧財產權歸屬於國發會

展 AI 的事實現況 顯然很難獲得所有受保護的作品的事先許可。而在討論如何給予著作權作品使用補償時，認為應將重點關注於透過信託管理組織管理作品之權利持有者與 AI 營運商之間的關係，認為此類狀況可能會更容易進行談判。然而，討論中亦有人認為，AI 企業需要《著作權法》建立文字和資料探勘例外規定，以確保 AI 企業在國際 AI 事業競爭中不會落後。

針對 AI 輸出著作權侵權判定標準、AI 輸出著作權登記、AI 輸出標識制度層面，參與者認為雖然可以根據現有的依賴性、實質相似性，作為判定著作權侵權之判斷因素，但 AI 開發者、服務提供者、使用者是否需要獨立承擔責任則尚不明確。在 AI 輸出成果之著作權登記方面，應引導申請人在登記著作權時詳細填寫 AI 輸出成果以及有人類創意貢獻的部分，並考慮未來科技發展。關於 AI 產品標示制度，許多意見主要來自權利人和法律界，認為有必要在韓國引入該制度，但建議對需要強制引入的領域進行詳細審查、標示方法、技術限制等。

下半年之工作會議，將討論是否以及如何揭露 AI 之學習數據，在權利人不希望其作品投入 AI 學習時，有無將其排除在 AI 學習數據之外的制度或技術措施；證明 AI 學習數據的方法，評估人類對該作品產出的創造性貢獻；還有 AI 產品是否以及如何受到法律保護等議題。

AI 是一個全球性問題，正在迅速、廣泛地滲透到經濟、社會和文化領域。韓國政府期待 AI 可以朝著有利於國家的方向發展，是故其文化觀光體育部亦透過計畫進行「人工智能學習作品適當費用計算研究」以及「人工智能著作權制度完善方法研究」，預計於 2024 年年底公佈完善 AI 相關著作權制度計畫。

資料來源：

1. 韓國文化觀光體育部, 인공지능 시대 저작권 제도 정비의 실마리를 찾아보다게시일，2024-06-28，https://www.mcst.go.kr/kor/s_notice/press/pressView.jsp?pSeq=212

本報告之智慧財產權歸屬於國發會

01 (last visited 2024/07/10)

五、 OECD

(一)2024 年 7 月 OECD 發布新聞稿，說明人工智慧全球合作夥伴關係會議共識，並呼應首爾宣言

OECD 自 2020 年起推動人工智慧全球合作夥伴關係（Global Partnership on Artificial Intelligence, GPAI），結合 OECD 成員國及願意參與 GPAI 之國家，透過每年定期召開會議，藉由跨國合作、交流，以消弭 AI 政策理論與實踐之間的差異，並實現 OECD 對 AI 建議（the OECD Recommendation on AI）內，目前共有 44 個國家參與。目前並透過社群、GPAI 專家支援中心（分別位於法國巴黎、加拿大蒙特婁及日本東京），提供專業知識交流或支援。

GPAI 目前係由印度擔任主席，於 7 月 3 至 4 日於印度新德里舉行 GPAI 第 6 次部長級會議（the 6th meeting of the GPAI Ministerial Council）。2024 至 2025 年將由塞爾維亞擔任主席，預計下半年之峰會將於該國舉行。

於 7 月 3 日會後，由主辦國印度發布新聞，說明 GPAI 成員就 GPAI 未來願景所達成之共識，期望利用 AI 潛力造福人類。聲明中指陳，GPAI 成員已認識到 AI 在型塑人類社會與改變未來經濟的潛力，安全、可靠及值得信賴之 AI 將為加速與推動永續發展帶來機會，但也承認 AI 系統將帶來風險與挑戰，包含安全、潛在惡意使用、錯誤或虛假資訊、歧視與偏見、缺乏透明度與公平性以及對智慧財產權與個人資料保護之風險等。

GPAI 成員將共同致力於透過包容、多方利害關係人參與之方式，依靠強大的科學基礎、開放的解決方案及共同標準，發展值得信賴與以人為本的 AI，並加強政府、學界、研究人員、產業，及私部門等合

本報告之智慧財產權歸屬於國發會

作。此外，考量透過國際合作弭平各國國內或跨國間之數位落差，促進安全、可靠及值得信賴之 AI。同時也將促進 20 國集團（Group of Twenty, G20）與 7 大工業國（G7）等對 AI 不同倡議之協作，如 2024 年 5 月由英國與韓國舉辦之 AI 首爾峰會（AI Seoul Summit）與該峰會後發布之首爾宣言（Seoul Declaration, 의한 서울선언），呼應其安全、創新及包容三大原則。

資料來源：

1. OECD, Global Partnership on Artificial Intelligence, 2024-07-03, https://www.oecd.org/en/about/programmes/global-partnership-on-artificial-intelligence.html (last visited 2024/07/17)
2. OECD, GPAI and OECD unite to advance coordinated international efforts for trustworthy AI, 2024-07-03, https://www.oecd.org/en/about/news/speech-statements/2024/07/GPAI-and-OECD-unite-to-advance-coordinated-international-efforts-for-trustworthy-AI.html (last visited 2024/07/17)
3. Ministry of Electronics & IT, 6th meeting of the GPAI Ministerial Council held on 3rd July 2024 at New Delhi, 2024-07-03, https://pib.gov.in/PressReleasePage.aspx?PRID=2030534 (last visited 2024/07/17)

六、 中國大陸

(一)2024 年 7 月大陸工業和信息化部發布國家人工智能產業綜合標準化體系建設指引（2024 版），說明其 AI 技術標準願景

為推動中國大陸人工智慧（大陸稱為人工智能）產業之發展，工業和信息化部（簡稱工信部）於 7 月 2 日發布工信部、中央網路安全和信息化委員會辦公室、國家發展和改革委員會及國家標準化管理委

本報告之智慧財產權歸屬於國發會

員會等 4 部會關於印發人工智慧產業綜合標準化體系建設指引的通知（关于印发国家人工智能产业综合标准化体系建设指引（2024 版）的通知）。

該通知主要內容為提供中國大陸人工智慧產業綜合標準化體系建設指引（2024 版），以落實其於 2021 年 10 月發布之國家標準化發展綱要，及 2023 年 10 月提出之全球人工智慧治理倡議。並預計至 2026 年將新制定國家標準與行業標準 50 項以上、實施相關標準或推廣之企業超過 1,000 家，及參與制定國際標準 20 項以上，以引導大陸人工智慧產業之發展。

為發展人工智慧標準，此一參考文件提出人工智慧標準體系架構。該架構包含：基礎共性、基礎支撐、關鍵技術、智能產品與服務、賦能新型工業化、行業應用，及安全／治理等 7 部分，以供開發相關標準參考。以基礎共性為例，可研發之標準包含：人工智慧術語、參考架構、測試評估、管理或可持續等內容；而基礎支撐則包含：基礎數據服務、智慧晶片、智慧感測器、電腦設備、算力中心、系統軟體、開發架構、軟硬體共同等（可詳該指引頁 5 之圖 2 及頁 6 以下說明）。

另在此參考文件內，將人工智慧產業分成 4 個部分，包含：基礎層、架構層、模型層及應用層。基礎層主要為算力、演算法及數據。架構層則指用於模型開發之深度學習的架構與工具。而模型層係指大型語言模型（Large Language Model, LLM）等技術與產品。至於應用層為人工智慧技術在各行業或場景內之應用。

延續前述人工智慧標準體系架構，此一參考文件在行業應用部分，已提出智慧城市、科學運算、智慧農業、智慧能源、智慧環保、智慧金融、智慧物流、智慧教育、智慧醫療及智慧交通（可詳該指引頁 4 之圖 1），可供發展人工智慧產業之應用層參考。而此同時，透過開發行業應用之相關標準，可規範人工智慧在各行業之技術要求，並為推動人工智慧發展提供技術保障。

本報告之智慧財產權歸屬於國發會

資料來源：

1. 工业和信息化部, 工业和信息化部 中央网络安全和信息化委员会办公室 国家发展和改革委员会 国家标准化管理委员会关于印发国家人工智能产业综合标准化体系建设指引（2024 版）的通知, 2024-07-02, https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2024/art_e8ebf5600ec24d3db644150873712c5f.html (last visited 2024/07/17)

2. 中国政府网, 国家人工智能产业综合标准化体系建设指引（2024 版）, 2024-07-02, https://www.gov.cn/zhengce/zhengceku/202407/P020240702716282797987.pdf (last visited 2024/07/17)

(二)2024 年 6 月香港個人資料私隱專員公署發布《人工智慧 (AI): 個人資料保障模範框架》

隨著 AI 科技急速發展，AI 的應用日漸普及，為應對 AI 對個人資料隱私帶來的挑戰，體現《全球人工智慧治理倡議》方針，香港個人資料私隱專員公署（私隱專員公署）於 2024 年 6 月發布《人工智慧 (AI): 個人資料保障模範框架》，該框架在草擬及發布的過程中獲得香港政府資訊科技總監辦公室及香港應用科技研究院的支持，並徵詢廣納不同專家及相關人士的意見，以下摘要重要之內容：

1. 該框架建基於一般業務流程，向採購、實施及使用任何種類的 AI 系統的機構，就保障個人資料隱私方面提供有關 AI 管制的建議及最佳行事常規，旨在協助相關機構遵從《私隱條例》的規定，及恪守私隱專員公署在 2021 年出版的《開發及使用人工智慧道德標準指引》中所倡議的三項資料管理價值及七項 AI 道德原則。

2. 該框架涵蓋四個範疇的建議措施，包含制定 AI 策略及管制架構、進行風險評估及人為監督、實行 AI 模型的定製及 AI 系

本報告之智慧財產權歸屬於國發會

統的實施與管理、促進與內部員工、供應商、消費者及監管機構的溝通及交流。摘要如下：

(1) 制定 AI 策略及管制架構。

(2) 制定機構的 AI 策略及考量採購 AI 方案的管理、成立 AI 管制委員會並為員工提供 AI 相關的培訓。

(3) 進行風險評估及人為監督。

(4) 進行全面風險評估，建立一套風險管理機制，採取「風險為本」的管理方式，並根據 AI 的風險高低而採取相應的風險緩減措施。

(5) 實行 AI 模型的定製與 AI 系統的實施及管理。

(6) 為定製及或使用 AI 模型準備及管理所涉資料，包括個人資料、在定製及實施有關 AI 系統的過程中測試及驗證之 AI 模型、確保 AI 的系統安全及資料安全，以及對 AI 系統進行管理及持續監察。

(7) 促進與內部員工、供應商、消費者及監管機構的溝通及交流。

(8) 定期及有效地與利害關係人（尤其是內部員工、 AI 供應商、個別消費者及監管機構）聯絡及交流，以提高透明度及建立信任。

資料來源：

1. 香港個人資料私隱專員公署，私隱專員公署發布《人工智慧(AI)：個人資料保障模範框架》，2024-06-11，https://www.pcpd.org.hk/tc_chi/news_events/media_statements/press_20240611.html(最後瀏覽日 2024/07/11)

本報告之智慧財產權歸屬於國發會

七、 歐盟

(一)2024 年 7 月歐盟人工智慧法已刊登於官方公報，8 月正式生效、並採分階段施行

為因應 AI 所帶來之衝擊與影響，歐洲聯盟執行委員會（European Commission，歐盟執委會）在 2021 年 4 月提出人工智慧法（Artificial Intelligence Act, AIA）草案（2021/0106/COD）。經多次討論，歐洲議會（European Parliament）於 2023 年 6 月通過此一草案；嗣經徵詢各成員國意見，歐盟理事會（European Council）與歐洲議會在同年 12 月達成共識。而在 2024 年 5 月理事會終於批准 AIA，成為全球第一部針對 AI 進行監管的規範，並於 2024 年 7 月刊登於官方公報後，8 月正式生效。

歐盟 AIA（(EU) 2024/1689）計 180 段前言、13 章 113 條文及 13 個附件。依章節與條文重點，摘要如下：

1. 一般規定（§1 至§4）。
2. 禁止使用之 AI（§5）。
3. 高風險之 AI 相關規定，包括：高風險 AI 之類型（§6 至§7）、對高風險 AI 之要求（§8 至§15）、高風險 AI 之相關角色義務（§16 至§27）、通報機關與公告機構（§28 至§39）及標準、合格評定、證書、註冊（§40 至§49）。
4. 特定 AI 之透明度義務（§50）。
5. 通用目的之 AI 模型，包含：分類規範（§51 至§52）、通用 AI 模型提供者之義務（§53 至§54）、具系統性風險之通用 AI 模型提供者義務（§55）及實施守則（§56）。
6. 支援創新措施（§57 至§63）。

本報告之智慧財產權歸屬於國發會

7. 治理，包含：歐洲 AI 委員會等（§64 至§69）與國家級主管機關（§70）。

8. 歐盟高風險 AI 資料庫（§71）。

9. 上市後監督、分享情資等，包含：如上市後監督（§72）、嚴重事件之通報（§73）、執行（§74 至§84）、補救措施（§85 至§87）及通用 AI 模型提供者之監督等（§88 至§94）。

10. 行為準則（§95 至§96）。

11. 授權（§97 至§98）。

12. 罰則（§99 至§101）。

13. 其他規定（§102 至§113），如過渡期規範。

整體觀之，歐盟 AIA 將 AI 區分為禁止、高風險等應用，並對於通用型之 AI 模型設定有不同的要求，同時重視透明性與保護基本權利等。此外，如第 7 章治理規範內，歐盟將成立 AI 辦公室（European AI Office）及科學小組（Scientific panel），分別協助監管與各項作為。且對於違反者，如依第 99 條之規定，將可處以最高 3,500 萬歐元或上一年度全球營業額 7%之罰款。

目前 AI 法已於 2024 年 7 月 12 日刊登於官方公報(Official Journal)，將在刊登後第 20 日生效，並已於 8 月生效。考量該法對實務之影響衝擊，採分階段施行，如依第 113 條規定，該法第 1 章（總則）與第 2 章（禁止使用之 AI，如第 5 條）自 2025 年 2 月 2 日起適用；其他如第 3 章第 4 節（主管機關與其他組織）、第 5 章（通用型 AI 義務）、第 7 章（治理）、第 12 章（罰則）及第 78 條（保密）自 2025 年 8 月 2 日起適用；但第 101 條（針對通用型 AI 提供者之罰則）規定除外；而該法涉及高風險應用相關，如第 6 條第 1 款及相應義務自 2027 年 8 月 2 日起適用。

本報告之智慧財產權歸屬於國發會

資料來源：

1. EU Commission, Official Journal L series daily view, 2024-07-12, https://eur-lex.europa.eu/oj/daily-view/L-series/default.html?&ojDate=12072024 (last visited 2024/07/24)
2. EU Commission, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)Text with EEA relevance, 2024-07-12, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689 (last visited 2024/07/24)

(二)2024 年 7 月歐盟 EDPB 發布聲明，說明 AIA 施行後個人資料保護主管機關與市場監管機關分工之相關建議

歐洲資料保護委員會（European Data Protection Board, EDPB）於 7 月 16 日發布聲明（Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework），說明因應歐盟 AIA 施行後個人資料保護主管機關與市場監管機關之分工事宜。該聲明主要分為二大部分，第一部分說明本聲明之背景與目的，第二部分則說明 EDPB 相關建議。

在第一部分本聲明之背景與目的內，EDPB 先說明因 AIA 將於 2024 年 8 月生效，為保護歐洲聯盟基本權利憲章（the Charter of Fundamental Rights of the European Union）第 7 條及第 8 條規範之隱私權或個人資料等基本權利，且因依 AIA 規定，將透過設立或指定國家主管機關（national competent authorities）處理相關業務。爰透過本聲明，EDPB 希望解決各成員國在個人資料保護業務或相關領域內，指定主管機關可能導致之監督或協調問題。

本報告之智慧財產權歸屬於國發會

如 AIA 第 74 條第 8 項規定之市場監管機關（market surveillance authority/authorities, MSAs），各成員國可指定 GDPR（(EU) 2016/679）或相關指令（(EU) 2016/680）之個人資料保護主管機關（national data protection authorities, DPAs）擔任高風險 AI 系統之市場監管機關。而同項次尚規定，市場監管機關（MSA）不得以任何方式影響司法機關之獨立性，亦不得干擾司法機關之執法行為等。

由於 AIA 對 MSA 有上述相關要求，故 EDPB 於建議當中指出 DPA 應可符合 AIA 之規範，例如 AIA 第 70 條第 3 項之要求，需具備 AI 之知識、對資料運算或個人資料保護等專業，可評估新興技術對基本權利造成之風險等。且 DPA 因具獨立性，亦可符合 AIA 第 70 條第 1 項之要求，可對 AI 系統進行有效之監督。另，EDPB 認為將 DPA 指定為 MSA 有利於 AI 價值鏈中的所有利害關係人，因 DPA 可提供單一聯繫窗口，可促進 AIA 與歐盟個人資料保護業務推動之不同關注方或主管機關間的互動。

此外，由 DPA 擔任 MSA 之角色，其所具備之法律或技術能力，應可勝任 AI 系統監管之任務，然因尚須負責跨國之協調等，會實質增加個人資料保護業務以外之工作，爰建議各成員國亦應提供額外之人力與財政資源。

另，將個人資料做為訓練 AI 之用，特別是通用 AI 模型，因其產出可能會影響個人隱私或資料相關權利，目前 AIA 第 56 條規定 AI 辦公室之權責，如制定行為準則、風險評估或管理內容，與 DPA 或 EDPB 間並無明確之協調機制。基此，EDPB 強調凡通用 AI 模型或其他 AI 系統，涉及個人資料保護時，各成員國之 DPA 與 EDPB 都必須適當參與，以確保基本權利之保障。

資料來源：

1. EDPB, Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework, 2024-07-16,

本報告之智慧財產權歸屬於國發會

https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-32024-data-protection-authorities-role-artificial_en (last visited 2024/07/31)

2. EDPB, Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework, 2024-07-16, https://www.edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf (last visited 2024/07/31)

八、 國際合作或會議

(一)2024 年 7 月國際電信聯盟出版 AI 治理日－從原則到實踐：2024 年報告，俾供了解 AI 生命週期與其風險管理等內容，以各國利規劃政策或其他配套措施

國際電信聯盟（International Telecommunication Union, ITU）於 7 月 17 日發布新聞，因 2024 年 5 月 ITU 前已辦理 AI 造福全球高峰會（AI for Good Global Summit），在此高峰會期間，曾邀集已開發與開發中國家領導人、政策制定者、研究人員及技術專家等共聚一堂，並於 5 月 29 日辦理首屆 AI 治理日－從原則到實踐（AI Governance Day－From Principles to Implementation）活動，討論 AI 治理架構等議題。

該 AI 治理日活動後，ITU 出版 AI 治理日－從原則到實踐：2024 年報告（AI Governance Day－From Principles to Implementation 2024 Report）。在此報告內，除說明當日參與人員、討論過程及會議決議，例如：ITU 之 AI 治理架構是什麼，如何落實等之外，還分享至 2024 年 5 月底主要國家或多邊組織對 AI 之規範或措施，諸如 2023 年 10 月美國白宮發布之 AI 行政命令（Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence）或 2024 年 8 月後將生效之歐盟人工智慧法（(EU) 2024/1689, Artificial

本報告之智慧財產權歸屬於國發會

Intelligence Act），俾供了解 AI 生命週期與其風險管理等內容，以利規劃政策或其他配套措施。

以 ITU AI 治理架構之相關討論為例，因該組織共有 193 個成員，要如何讓多數成員（如超過 85%）能夠遵守目前提出之 AI 治理架構？ITU 秘書長 Doreen Bogdan-Martin 表示，可以透過相關標準之研議來達成。而 AI 相關標準至少應包含：演算法與其透明度、系統安全之保障等要求，且應考量各成員之能力，能夠讓其簡單、有效地執行。目前 ITU 針對 AI 已建立 200 多個標準，刻正陸續發布或制定中。而 AI 應用亦應考量中低度開發國家消費者之需求，且重視永續發展等。

除 2023 年 10 月美國白宮及 2024 年 8 月歐盟對 AI 之規範或措施外，如巴西、中國大陸、愛沙尼亞、法國、日本、新加坡等 10 多國家對於 AI 治理亦有許多相關措施。例如：新加坡資訊通信媒體發展局（Infocomm Media Development Authority, IMDA）補助之 AI 驗證基金會（AI Verify Foundation）於 2024 年 1 月發布生成式 AI 模型治理框架（Model AI Governance Framework for Generative AI）草案，於同年五月發行，包含：問責、資料、事件通報、安全性等內容。而日本經濟產業省於 2024 年 4 月發布 AI 事業者指引第 1.0 版（AI 事業者ガイドライン 第 1.0 版），包含：應考量因素、跨領域案例或國外參考指引等，皆可供參考。

此外，ITU 自 2023 年 7 月開始辦理首屆 AI 造福全球高峰會（AI for Good Global Summit）以來，繼 2024 年 5 月第 2 屆後，明年度（第 3 屆）之 AI 造福全球高峰會預計於 2025 年 7 月 9 日至 11 日在瑞士日內瓦舉辦，屆時亦將討論 AI 治理之議題。

資料來源：

1. ITU, Key findings on the state of global AI Governance, 2024-07-17, https://www.itu.int/hub/2024/07/key-findings-on-the-state-of-global-ai-governance/ (last visited 2024/07/31)

本報告之智慧財產權歸屬於國發會

2. ITU, AI Governance Day – From Principles to Implementation 2024 Report, 2024-07-17, https://s41721.pcdn.co/wp-content/uploads/2021/06/2401225_AI_Governance_Day_2024_Report-E.pdf (last visited 2024/07/31)

3. IMDA, Model AI Governance Framework for Generative AI, 2024-01-16, https://aiverifyfoundation.sg/downloads/Proposed_MGF_Gen_AI_2024.pdf (last visited 2024/07/31)

4. 經濟產業省, AI 事業者ガイドライン（第 1.0 版）, 2024-04-22, https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20240419_report.html (last visited 2024/07/31)

貳、 數位身分

一、 美國

(一)2024 年 6 月美國國家標準與技術研究院宣布啟動數位身分相關合作研究，以呼應 SP 800-63 修正草案

美國國家標準與技術研究院（National Institute of Standards and Technology, NIST）於 6 月 10 日發布新聞，宣布將與喬治城大學的貝克中心（Georgetown University’s Beeck Center）等單位，啟動數位身分相關合作研究。旨在透過數位身分之應用，加強社福管理機構之正當程序與避免系統之潛在偏見，同時還可確保隱私與資料安全，以向符合資格之受益人提供食品、住房及醫療等公益計畫之需求。並透過合作研究與案例累積，持續深化 NIST 之數位身分指引內容。

上開研究源於 COVID-19 疫情期間，需要相關公益計畫資源的民眾增加，也因此導致詐欺與網路安全威脅發生頻率提高，部分公益資源管理機構開始將個人數位帳戶與身分驗證（identity verification，或稱身分證明 identity proofing）整合至申請流程或應用程式。然而，這些方法的採用，例如：依賴臉部辨識或資料辨別，引發隱私、資料安

本報告之智慧財產權歸屬於國發會

全，甚至正當程序等議題。如何有效且合法地運用身分驗證或相關方法，是許多機構期待瞭解的重點。

NIST 出版之數位身分指引（NIST SP 800-63 Digital Identity Guidelines）迄今已逾 20 年，歷經多次修正，目前為第 3 版（NIST SP 800-63-3），旨在對於執行數位身分服務之聯邦政府機關（構）提供技術之參考或建議，例如：定義身分證明、註冊、身分驗證、管理流程。並依不同需求再區分為 A、B、C（NIST SP 800-63A, 63B, 63C），分別就註冊與身分證明（Enrollment and Identity Proofing）、驗證與生命週期管理（Authentication and Lifecycle Management）等，就執行數位身分各項業務提供具體建議。

此一數位身分指引之第 4 版（NIST SP 800-63-4）修正草案曾於 2022 年 12 月至 2023 年 4 月對外徵詢意見（Initial Public Draft），修正重點包含：強化消費者之選擇、防範詐騙與相關威脅，及提供實作參考。其內容除簡介、定義外，還有數位身分模型，如註冊、身分證明、驗證及生命週期管理，及聯合（如共享身分資訊以支援跨系統之身分驗證），以及風險管理之重點，如執行初步影響評估、選擇不同等級、客製化驗證等級等。但因美國各界對第 4 版修正草案尚無共識，截至 2024 年 6 月尚未定稿，後續進展可持續觀察。

資料來源：

1. NIST, NIST Launches Collaborative Research Effort on Digital Identity to Support Secure Delivery of Public Benefits, 2024-06-10, https://www.nist.gov/news-events/news/2024/06/nist-launches-collaborative-research-effort-digital-identity-support-secure (last visited 2024/06/19)
2. NIST, NIST SP 800-63-4 (Initial Public Draft): Digital Identity Guidelines, 2023-12-12, https://csrc.nist.gov/pubs/sp/800/63/4/ipd (last visited 2024/06/19)
3. NIST, Digital Identity Guidelines, n.d., https://pages.nist.gov/800-

本報告之智慧財產權歸屬於國發會

63-3/ (last visited 2024/06/19)

二、 中國大陸

(一)2024 年 7 月中國大陸公安部與國家網際網路資訊辦公室（網信辦）就國家網路身分認證公共服務管理辦法（徵求意見稿）對外徵求意見

中國大陸公安部與國家網際網路資訊辦公室（国家互联网信息办公室，网信办）於 2024 年 7 月 26 日就《國家網絡身分認證公共服務管理辦法（徵求意見稿）》公開徵求意見，徵詢時間至 2024 年 8 月 25 日止。

國家網路（絡）身分認證公共服務管理辦法（徵求意見稿，以下簡稱本辦法草案）共計 16 條，以本辦法草案第 1 條之立法目的，揭示其法源依據為網路安全法、數據安全法、個人資料保護法、反電信網路詐騙法等相關規定，規範內容並涉及透過網際網路進行身分認證，以利民眾使用中國大陸政府提供之公共服務。

參照目前公安部與網信辦對外之說明，本辦法草案內容主要有 4 項重點，包含：1. 明確公共服務與「網號」、「網證」等概念。2. 明確公共服務之使用方式與場景。3. 強調公共服務平臺與網際網路平臺之數據與個人資料保護義務。4. 明確公共服務平臺與網際網路平臺違反數據與個人資料保護義務之法律責任。

所謂「網號」、「網證」依本辦法草案第 2 條第 2 項規定，網號是指與自然人身分資訊對應，由字母與數字組成，不含明文身分資訊之網路身分符號；至於網證是指載有網號及自然人非明文身分資訊之網路身分憑證。而網號與網證可用於網際網路服務，及有關部門、行業管理、服務中非明文登記，核驗自然人真實身分資訊。

本報告之智慧財產權歸屬於國發會

此外，由於本辦法草案明確使用「網號」、「網證」進行網路之身分認證，且對於網號與網證之申領條件、公共服務之使用場景，及身分認證所需證件等都有規範。以本辦法草案第 15 條為例，身分認證所需證件包含中國大陸居民身份證、定居國外之中國大陸公民護照、前往港澳通行證、港澳居民來往內地通行證、臺灣居民來往大陸通行證、港澳居民居住證、臺灣居民居住證、外國人永久居留身份證等。

綜上，中國大陸希望結合相關法定證件，並透過國家網路身分認證公共服務平臺（本辦法草案第 2 條第 1 項參照）與其提供之公共服務，確認使用者之真實身分或進行核驗。且除公共服務之外，參照本辦法草案第 7 條第 1 項，鼓勵網際網路平臺按照自願原則接入公共服務，用以支持用戶使用網號與網證登記、核驗用戶真實身分資訊等。爰除宣示其網路安全法、數據安全法、個人資料保護法等規範，要求業者、用戶恪遵相關法令外，未來應可預見中國大陸網路實名制之擴大實施。

資料來源：

1. 网信办,公安部国家互联网信息办公室关于《国家网络身份认证公共服务管理办法（征求意见稿）》公开征求意见的公告, 2024-07-26, https://www.cac.gov.cn/2024-07/26/c_1723675813897965.htm (last visited 2024/08/07)

參、 數位政策

一、 日本

(一)2024 年 6 月日本內閣已議定本年之《實現數位社會的重點計畫》（デジタル社会の実現に向けた重点計画），包含 8 個重點推動事項

本報告之智慧財產權歸屬於國發會

日本數位廳（デジタル庁）於 6 月 21 日發布新聞，日本內閣已通過（閣議決定）本（2024、令和 6）年之《實現數位社會的重點計畫》（デジタル社会の実現に向けた重点計画）。該計畫係依據 2021 年施行之《數位社會形成基本法》（デジタル社会形成基本法）與相關法令而來，並搭配同年 9 月成立之數位廳，透過相關政策與配套措施，目的在促進日本邁向數位社會。

日本推動數位社會主要有 6 大願景，包含：透過數位化實現成長策略、醫療、教育、防災、兒童等準公共領域之數位化、透過數位化振興區域發展、創造沒有人落後的數位社會、培養並確保數位化人才，及推動以可信數據自由流動（Data Free Flow with Trust, DFFT）為首之國際策略。然目前日本遭遇人口減少與勞動力短缺、產業競爭力下降、自然災難與網路攻擊威脅，以及民間對「數位化」的焦慮與猶豫等問題。本次《實現數位社會的重點計畫》內，主要規劃 8 個欲實施之重點推動事項，以解決前述促進日本邁向數位社會所遭遇之問題。

關於本次《實現數位社會的重點計畫》之 8 個重點推動事項，摘要說明如下：

1. 強化與加速數位公共基礎建設，例如：於公部門持續推動個人編號卡與相關業務之結合，如結合駕照、居留證，並積極推動個人編號卡之普及與利用意願，如推動可用於報稅、可透過智慧型手機於線上申請公共服務等。在對企業部分，建立公共基礎資訊的資料庫，確保資訊之準確度以提高行政效率，並透過 e-Gov、法人與個人事業主數位身分驗證系統（G ビズ ID）及行政業務、補助申請數位化提高企業之便利性。並投入營造具備包容性之數位社會環境，尤其著重強化數位化基礎設施，如擴大 5G 覆蓋範圍、建構任何人皆能取得利用之資通訊基礎設施，完備使用數位產品與服務之無障礙環境。此外，為使數位化成為常態，並需投入數位化人力資源之發展，包括個人數位技能之持續學習與資格證明制度之推動，並強化

本報告之智慧財產權歸屬於國發會

得提供專業教育之課程與教師，強化對數學、資料科學以及AI教育中心聯盟以及大學優秀教育計畫之認證，並加速並支持促進地方政府之數位轉型人力資源儲備。

2. 落實結構性改革之數位化原則，於政策規劃階段即落實「制度、業務、系統」三位一體之規劃，包括持續推動政府之數位轉型，每年確定政府資源於數位化體制改革之重點關注領域，並於政策或制度建立過程；落實對數位原則之檢視，包括相關法律與法規之符合性檢視等；並逐步建構硬性及軟性規則以促進創新科技之發展與運用，以支援並促成《數位生命線全國綜合整備計畫》（デジタルライフライン全国総合整備計画）之落實。

3. 實施行政與金融業務之數位化改革，如運用數位科技優化公共服務，促進專業人才及公共基礎設施之發展，並搭配2024年行政與財政改革總結（デジタル行財政改革取りまとめ2024）之建議措施，大幅運用數位科技以加強公共服務。

4. 加強數位政務，如優化中央與地方公共基礎設施（透過SaaS、政務雲等），協助地方政府資訊系統之統一與標準化等，並推廣安全、順暢之公共服務網路以實現政府與民間之資訊協作。

5. 促進產業數位化相關之現代化措施，如以需求為導向，持續提高安全與韌性，並協助產業擺脫多重分包之架構並提高薪資，以提升整體產業之適應能力、生產力與效率。

6. 運用資料解決問題以加強競爭力，如建立資料共享之標準化機制，促進可信賴之資料自由流動（Data Free Flow with Trust, DFFT）之實現。投入防災數位化平臺之推動，包括建立適切之防災資料協作基礎設施；搭配個人編號卡之利用，確保受災民眾獲得便利之資訊及服務；強化通訊、廣播與電力基礎

本報告之智慧財產權歸屬於國發會

設施之韌性等；並期待後續得以促進未來預測、數位仿生及AI之應用及開發，將日本數位防災科技推廣至海外。

7. 重視安全，包含國家安全與網路安全相關業務，特別是落實2013（平成25）年發布、2022（令和4）年更新之國家安全保障戰略（国家安全保障戦略）與最近一期（2021年、令和3年閣議決定）之網路安全戰略（サイバーセキュリティ戦略）。

8. 投入前瞻技術研發，如AI、Web3.0、量子技術、數位仿生及5G（含6G）等。

資料來源：

1. デジタル庁, デジタル社会の実現に向けた重点計画, 2024-06-21, https://www.digital.go.jp/policies/priority-policy-program (last visited 2024/06/25)

2. e-GOV, デジタル社会形成基本法, 2024-06-07, https://elaws.e-gov.go.jp/document?lawid=503AC0000000035 (last visited 2024/06/25)

(二)2024年7月日本數位廳更新其政府雲使用說明文件（ガバメントクラウドの活用について），以利地方政府規劃或辦理業務參考

按日本數位廳自2022年起，積極推動政府雲（ガバメントクラウド），透過於雲端內建置快速、靈活、安全且經濟高效的共用IT資訊系統，以利中央與地方政府機關使用。目前係由數位廳每年挑選合格廠商，由合格廠商提供所需之功能模組，並兼顧其安全、可用及擴充性，同時又可降低建置成本等。

前述合格廠商以2022年為例，當年10月公告包含Amazon Web Services、Google Cloud、Microsoft Azure及Oracle Cloud Infrastructure

本報告之智慧財產權歸屬於國發會

等 4 家廠商。至 2023 年數位廳於 11 月的公告：新增櫻花雲（さくらのクラウド）1 家；上述廠商皆有資格提供符合政府雲要求之服務。

為了解廠商提供服務之狀況，據數位廳於 2024 年 7 月 5 日發布之政府雲端技術需求使用調查結果（ガバメントクラウドに求める技術要件の利用状況調査結果），截至當年6月25日止之調查結果顯示，目前中央與地方政府機關已有 264 項使用政府雲的實績。

經分析該調查結果，除了基本事項（67 項）外，對雲端服務廠商提供之服務有需求，而廠商亦可提供完全符合機關需求之技術包含：資料庫（29 項）、安全防護（16 項）、Serverless 容器相關（11 項）、加密金鑰管理與資料儲存安全（11 項）、API 相關函數（8 項）、程式碼發布管理（4 項）及機器學習相關功能（1 項）。至於有需求但實際可使用最低者為應用連動功能（アプリケーション連携機能），機關共提出 9 個需求項目，但廠商只提供 4 項供使用。

另為讓各地方政府更加了解政府雲之使用，數位廳亦於本年 7 月 5 日更新《如何使用政府雲》（ガバメントクラウドの活用について）之參考文件，內容包含：政府雲基本概念、在其環境內可以建置之系統為何、如何設定權限、系統管理權責劃分、個資之處理，及相關責任等，以利地方政府規劃或辦理業務之參考。

以系統管理權責劃分，建議劃分數位廳、該政府機關之負責人、實際承辦人或委託之廠商等角色，並設定具體之姓名或職位、人數，及管理或使用權限等（可詳該參考文件頁 15 之表 2）。

此一參考文件除提供上開說明外，亦列出數位廳、雲端服務廠商、使用之地方政府與相關機關間之六種合約簽署方式，以明確權利義務，約定如提供服務之內容、營運管理、安全控制措施及損害賠償等事項（可詳該參考文件頁 5 之圖 2，及頁 11 之表 1）。

資料來源：

本報告之智慧財產權歸屬於國發會

1. デジタル庁, 地方公共団体の基幹業務システムの統一・標準化, 2024-07-05, https://www.digital.go.jp/policies/local_governments#cloud-use (last visited 2024/07/17)

2. デジタル庁, ガバメントクラウド, 2024-07-05, https://www.digital.go.jp/policies/gov_cloud (last visited 2024/07/17)

二、歐盟

(一)2024 年 7 月歐盟執委會發布第 2 份數位十年國家執行報告（Report on the State of the Digital Decade），說明各成員國落實 2030 年設定目標之執行情形

為持續推動歐盟單一市場，歐盟執委會繼 2023 年 9 月發布第 1 份報告後，嗣於 2024 年 7 月 2 日發布第 2 份數位十年執行情形（Report on the State of the Digital Decade），說明依據歐盟數位十年政策計畫（Digital Decade Policy Programme, DDPP），各成員國於達成 2030 年之目標與任務的執行情形。

2024 年報告較 2023 年報告不同的地方，在於檢視各成員國依前述數位十年政策計畫，而規劃之數位十年國家執行路徑圖（National Digital Decade Strategic Roadmaps），如各國在數位技能之培育、採用 AI 與資料分析，促進半導體生產，及新創公司或生態系等措施，能否符合 DDPP 或相關政策。

然依此一報告顯示，目前各成員國執行情形多落後於原設定之目標。舉例而言，依 DDPP 規劃，預計 2030 年歐盟境內之企業採用 AI、雲端或大數據之比例應為 75%，但以 2023 年之資料推估，屆時可能只有 64%企業使用雲端、50%使用大數據，及 17%使用 AI，爰歐盟建議各國應進行額外投資。

本報告之智慧財產權歸屬於國發會

此外，採用或研發創新技術對增加歐洲地區之競爭力至關重要，特別是在目前地緣政治格局下。且因網路安全威脅日益增加，歐盟建議各國應增強韌性及強大的安全措施。為此，歐盟已先成立 3 個歐洲數位基礎設施聯盟（European Digital Infrastructure Consortia），希望整合跨國能量，提供關鍵基礎設施之協助。

DDPP 內還包含提升民眾數位技能與落實公共服務數位轉型之政策目標。首先，在提升民眾數位技能部分，目前歐盟只有 55.6%的人口具備基本數位技能，雖預估至 2030 年歐盟 ICT 專業人員應可達 1,200 萬人，但仍然不足。故為實現相關目標，歐盟建議各成員國應透過多元的方式，鼓勵年輕人、女性等，投入科學、技術、工程及數學（STEM）等領域。

其次，於落實公共服務數位轉型部分，各成員國也在努力實現讓民眾與企業可以在線上存取所有關鍵公共服務與電子健康紀錄，並提供安全的 eID 服務。目前已有 93%的歐盟人口可以使用 eID，搭配歐盟數位錢包（EU Digital Identity Wallet）之推廣，預計到 2030 年應可實現民眾與企業 100%可使用數位公共服務之目標。

綜上，為利持續改善，歐盟規劃各成員國應於 2024 年 12 月前，對各國之執行路徑圖進行審查並調整，以符合數位十年相關政策所設定之目標；且下一份數位十年執行情形（Report on the State of the Digital Decade）將於 2025 年中公布。

資料來源：

1. EU Commission, Second report on the State of the Digital Decade calls for strengthened collective action to propel the EU's digital transformation, 2024-07-02, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3602 (last visited 2024/07/17)

本報告之智慧財產權歸屬於國發會

三、 美國

(一)2024 年 7 月美國發布關鍵與新興技術國家標準戰略之進度報告，說明 2023 年 5 月迄今聯邦政府各部門之執行情形

美國白宮前於 2023 年 5 月發布聯邦政府之關鍵與新興技術國家標準戰略（National Standards Strategy for Critical and Emerging Technology, USG NSSCET），擇定通訊與網路科技、半導體與微電子、AI 等多項關鍵與新興技術領域，並由國家標準與技術研究院（National Institute of Standards and Technology, NIST）主責，協助制定國家標準，且與美國國家標準協會（American National Standards Institute, ANSI）合作，鼓勵私部門透過投資、人才培育等方式參與，以共同鞏固美國在相關技術領域之領導地位與競爭力。

聯邦政府選定之關鍵與新興技術（Critical and Emerging Technology, CET）領域包含：通訊與網路科技（Communication and networking technologies）、半導體與微電子（Semiconductors and microelectronics）、人工智慧與機器學習（Artificial intelligence and machine learning）、生物科技（Biotechnologies）、數位身分基礎設施與分散式帳本技術（Digital identity infrastructure and distributed ledger technologies）、可再生能源發電與儲存（Renewable energy generation and storage）、量子資訊科技（Quantum information technologies）、自動化與聯網基礎設施（Automated and connected infrastructure）、生物資料庫（Biobanking）、自動化與聯網運輸（Automated and connected transportation）、電動車（Electric vehicles, EVs）、關鍵礦物（如稀土）供應鏈（Critical minerals supply chains），以及網路安全與隱私（Cybersecurity and privacy）。

除選定關鍵與新興技術（CET）領域外，也責令聯邦政府相關部門協助推動，嗣於 2024 年 7 月 26 日發布關鍵與新興技術國家標準戰略之進度報告，摘要說明 2023 年 5 月迄今聯邦政府各部門之執行情

本報告之智慧財產權歸屬於國發會

形。例如：NIST 透過公私協力方式，成立卓越標準化中心（Standardization Center of Excellence），推動標準化之前置參與、勞動力能力建設、資訊與資料共享中心，及 CET 試辦協作計畫等措施。

美國國家電信暨資訊管理局（National Telecommunications and Information Administration, NTIA）則持續透過公共無線供應鏈創新基金（Public Wireless Supply Chain Innovation Fund），配合此一戰略推動相關措施。此基金來源係 2022 年晶片及科學法案（CHIPS and Science Act）所資助之 15 億美元，旨在促進開放、可相互操作、基於標準的次世代無線網路技術之研究、開發及採用。

而國家科學基金會（National Science Foundation, NSF）修改其提案與獎勵政策與程序之參考指引（Proposal and Award Policies and Procedures Guide, PAPPG），預計透過相關提案或獎勵，以鼓勵研發人員參與國際或國家標準之制定工作等。

資料來源：

1. The White House, FACT SHEET: Implementing the National Standards Strategy for Critical and Emerging Technology, 2024-07-26, https://www.whitehouse.gov/briefing-room/statements-releases/2024/07/26/fact-sheet-implementing-the-national-standards-strategy-for-critical-and-emerging-technology/ (last visited 2024/08/07)
2. NIST, U.S. Government National Standards Strategy for Critical and Emerging Technology, n.d., https://www.nist.gov/standardsgov/usg-nss (last visited 2024/08/07)

四、 國際合作或會議

(一)2024 年 7 月歐盟與新加坡完成數位貿易協定（Digital Trade Agreement）談判，對數位貿易與跨境資料傳輸已有共識

本報告之智慧財產權歸屬於國發會

歐盟於 7 月 25 日發布新聞，已與新加坡完成數位貿易協定（EU-Singapore Digital Trade Agreement）之談判，雙方就數位貿易與跨境資料傳輸相關事宜已達成共識，以維護競爭、透明及公平之開放數位經濟為共同目標。且此一協定補充雙方於 2019 年簽訂之自由貿易協定（EU-Singapore Free Trade Agreement），就數位貿易事宜予以補強。

此協定是歐盟與其他國家簽署數位貿易相關協定之首例，目前該協定重點包含：促進商品與服務之數位化貿易；確保跨境資料傳輸未產生不合理之數位貿易障礙；增強雙方對數位貿易之信任，如通過對垃圾郵件之嚴格規範等。

雙方並發布聯合聲明，認為此一數位貿易協定有助於協助建立消費者信任、確保企業（特別是中小或微型企業）之可預測性及法律確定性，以及消除與防止不合理之數位貿易障礙。同時也將提供新的經濟發展機會，確保安全之線上環境。

此外，據我國經濟部國際貿易署之觀察，認為此一數位貿易協定將可促進歐盟與新加坡間之數位貿易，包含：1. 開放與安全之跨境資料傳輸：如雙方承諾允許企業在彼此領土無縫傳輸資料，以支持電子商務及其他數位活動之可靠的跨境資料傳輸，並消除數位貿易障礙；2. 點對點之數位貿易：雙方將以電子化格式提供貨物進口、出口及過境所需的貿易文件，並互相接受電子文件；3. 建立互信與安全之數位系統：有鑑於網路安全威脅不斷變化，雙方將合作識別及降低該類威脅，並提升彼此人員之能力。

據歐盟統計，目前與新加坡間有一半以上之服務貿易係透過數位化方式提供。以 2022 年為例，已占歐盟與新加坡服務貿易總額之 55%（約為 430 億歐元）。透過歐盟與新加坡之數位貿易協定，預計可促進數位貿易並持續提高其成長機會。後續歐盟與新加坡都將依各自內部程序，完成此一協定之簽署等事宜。

資料來源：

本報告之智慧財產權歸屬於國發會

1. EC, EU and Singapore conclude negotiations for landmark Digital Trade Agreement, 2024-07-25, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3982 (last visited 2024/08/07)

2. EC, Joint Statement on the conclusion of negotiations for the EU-Singapore Digital Trade Agreement and the second Trade Committee meeting under the EU-Singapore Free Trade Agreement, 2024-07-25, https://ec.europa.eu/commission/presscorner/detail/en/statement_24_3983 (last visited 2024/08/07)

3. 經濟部國際貿易署, 新加坡與歐盟完成「歐盟—新加坡數位貿易協定」（EUSDTA）談判, 2024-07-26, https://www.trade.gov.tw/Pages/Detail.aspx?nodeid=45&pid=787730 (last visited 2024/08/07)

肆、 資訊隱私

一、歐盟

(一)2024 年 6 月歐盟資料保護監管機關發布第一份關於使用生成式 AI 以確保資料保護合規之參考文件

歐盟資料保護監管機關（European Data Protection Supervisor, EDPS）於 6 月 3 日發布生成式 AI 與 EUDPR：第一份關於使用生成式 AI 以確保資料保護合規（Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems）之參考文件。

此文件係提供為歐盟機關（構）、辦公室等（the EU institutions, bodies, offices and agencies, EUIs）參考利用，並非取代歐盟之 AIA（Artificial Intelligence Act），其目的為協助 EUIs 在使用生成式 AI 時，

本報告之智慧財產權歸屬於國發會

能夠落實個人資料（個資）保護，特別是符合歐盟政府機關資料保護規則（(EU) 2018/1725，簡稱 EUDPR）。

此文件採問答方式，以供 EUIs 參考，主要有 13 題，摘要重點如下：

1. 什麼是生成式 AI？除概述生成式 AI 之定義、功能，並簡要說明大型語言模型（large language model, LLM）與其應用。

2. EUIs 可以使用生成式 AI 嗎？答案是可以的，但建議前提符合 EUDPR 與其他法律規定，且權衡 EUIs 之特殊性等。

3. 要如何知道使用生成式 AI 是否涉及個資處理？建議可結合生成式 AI 之生命週期，如訓練階段、創建模型或後續使用，及其輸入、產出等過程，以利判斷。

4. 資料保護專員（Data Protection Officer, DPO）在開發或部署生成式 AI 之作用？建議符合 EUDPR 第 45 條，且透過前述生命週期確保其合規。

5. EUIs 想要開發或使用生成式 AI 時，應於何時進行資料保護影響評估（Data Protection Impact Assessments, DPIA）？建議符合安全預設原則，如符合 EUDPR 第 27 條，並徵詢 DPO 之意見。

6. 在設計、開發及使用過程中，如何確保生成式 AI 處理個資之合規？建議符合 EUDPR 第 5 條第 1 項各款之規定處理。另外，如果涉及國際傳輸（將個資傳輸至第三國或國際組織），則建議遵守 EUDPR 第 46 至 51 條之規定。

7. 使用生成式 AI 時，如何確保資料最小化原則？建議符合 EUDPR 第 4 條第 1 項 c 款，即限於處理目的所需之內容。

本報告之智慧財產權歸屬於國發會

8. 如何確保資料正確性？建議符合 EUDPR 第 4 條第 1 項 d 款，且除正確外，於必要時保持更新等。

9. 使用生成式 AI 時，如何告知當事人有關個資之處理情形？建議符合 EUDPR 第 14 條，落實透明性、提供當事人權利行使管道。

10. EUDPR 第 24 條自動化決策之規範如何因應？ 應考慮如何落實對自動化決策提出建議及異議等方式之人為干預，且同時關切弱勢族群與兒童之權益。

11. 使用生成式 AI 時，如何確保公平及避免偏見？建議對訓練資料進行審核，並定期觀測產出是否有偏差等。

12. 當事人權利如何行使？建議符合 EUDPR 第 3 章之第 14 至 25 條規定，如透明性，提供資訊及個資存取之權限等。

13. 如何確保資料安全？建議符合 EUDPR 第 33 條，如假名化或加密。

最後，如果 EUIs 有其他 AI 問題或需求，可進一步參考 EDPS 網站公布之資訊或文獻，例如：EDPS 與歐洲資料保護委員會（European Data Protection Board, EDPB）於 2021 年 6 月對歐盟 AIA 草案的聯合意見。

資料來源：

1. European Data Protection Supervisor, EDPS Guidelines on generative AI: embracing opportunities, protecting people, 2024-06-03, https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/edps-guidelines-generative-ai-embracing-opportunities-protecting-people_en (last visited 2024/06/12)

2. European Data Protection Supervisor, Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection

本報告之智慧財產權歸屬於國發會

compliance when using Generative AI systems, 2024-06-03, https://www.edps.europa.eu/system/files/2024-06/24-06-03_genai_orientations_en.pdf (last visited 2024/06/12)

3. EUR-Lex, Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.), 2018-11-21, https://eur-lex.europa.eu/eli/reg/2018/1725/oj (last visited 2024/06/12)

4. European Data Protection Board, EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2021-06-18, https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en (last visited 2024/06/12)

伍、 網路/資訊安全與韌性

一、 比利時

(一)2024 年 6 月比利時擔任歐盟理事會輪值主席國，提出關於未來網路安全之結論

比利時為 2024 年歐盟理事會之輪值主席國，在其領導下，理事會做出關於未來網路安全之結論（Council conclusions on the future of cybersecurity），且經理事會於 5 月 21 日批准後於 6 月 5 日發布新聞。該文件含前言除說明當前網路威脅、全球地緣政治發展，如俄烏戰爭等外，指陳本次結論旨在協助擘劃歐盟未來之政策發展與立法方向，強調各成員國之共同執行與保護（implement and protect together），並以深化資安防護，及利用數位身分加強網路安全為核心。

本報告之智慧財產權歸屬於國發會

經檢視該文件，可整理出三項重點：

1. 具體政策建議為建立歐洲網路能力中心（European Cybersecurity Competence Centre, ECCC）相關，例如與歐盟網路安全局（European Union Agency for Cybersecurity, ENISA）密切合作，並落實其事件應變協調、研發及人才培訓等能量，持續鞏固與強化既有的電腦緊急應變團隊（Computer Security Incident Teams Network, CSIRT Network）網絡（且含歐洲網路安全認證小組（European Cybersecurity Certification Group, ECCG）、歐洲網路危機處理組織網絡（European cyber crisis liaison organisation network, EU-CyCLONe）及 ECCC 等組織與工作項目），以呼應共同執行與保護之目標。

2. 涉及立法與執行部分，除呼籲各成員國落實第二版網路及資訊安全指令（Network and Information Security Directive 2, NIS 2）外，針對歐盟於 2023 年提出之網路韌性法（Cyber Resilience Act）與網路團結法（Cyber Solidarity Act）2 項草案，於 2024 年之立法程序內，將規劃與已施行之網路安全法（Cybersecurity Act）進行合併。並責成 ENISA 積極透過與各成員國、歐盟實體（如關鍵基礎設施）及私部門合作，建立優先事項。

3. 關於新興科技應用：該文件也提醒各國應注意 AI、量子、6G 等新興科技為網路安全帶來之機會與威脅，除建議研發後量子密碼學（Post-quantum cryptography, PQC）外，亦應預為因應過渡期間可能遭遇之風險，以保護機密或敏感資訊。該文件尚建議針對自由與開源軟體採取相關措施，以確保安全。

最後，理事會也建議執委會應提出新的網路安全戰略，俾利因應不斷變化與日益增加的威脅。

資料來源：

本報告之智慧財產權歸屬於國發會

1. Centre for Cyber Security Belgium, Council approval of conclusions on the future of cybersecurity, 2024-06-05, https://ccb.belgium.be/en/news/council-approval-conclusions-future-cybersecurity (last visited 2024/06/12)

二、日本

(一)2024 年 7 月日本網路安全戰略本部確認 2023 至 2024 年間與網路安全相關之年度執行報告及次年度計畫內容

日本網路安全戰略本部於 7 月 10 日發布新聞，日本政府已召開網路安全戰略本部第 41 次會議（サイバーセキュリティ戦略本部第 41 回会合），確認 2023 至 2024 年間與網路安全相關之年度執行報告及次年度計畫內容。

該會議資料除說明當前網路安全威脅相關發展，如遭受由敵對國家資助之組織對日本政府與私人企業（主要是關鍵基礎設施營運商）進行攻擊，且一般企業也飽受勒索軟體威脅之外，亦呼應日本 2021 年發布 3 年期之網路安全戰略（サイバーセキュリティ戦略），就先前已規劃之 3 項對策確立 2024 年各部會執行重點包含：

1. 網路安全領域之研究發展與趨勢（サイバーセキュリティ分野の研究開発に関する動向），除發展 5G 相關技術外，如總務省也持續投入量子運算與相關密碼學之研究。

2. IT 或網路安全之人才（IT・サイバーセキュリティ人材），如經濟產業省已透過產學合作，並透過入口網站「學習數位轉型（マナビ DX）」等措施，促進人力資源發展。

3. 國民意識與行動之趨勢（国民の意識・行動に関する動向），由內閣府秘書處主導，與相關部會和機構合作，如經濟產業

本報告之智慧財產權歸屬於國發會

省透過獨立行政法人情報處理推進機構（IPA）提供教育訓練教材，以利提升資訊安全意識。

另於次年度計畫（2024 年度年次計画）內，共有 7 項優先推動事項，重點摘要如下：

1. 強化日本政府網路安全體系,如加強人力資源之利用與培訓。
2. 加強關鍵基礎設施演練，如醫療院所，以提高各別領域之復原能力。
3. 透過強化情報處理推進機構與情報通信研究機構，如 AI、IT 產品安全及人才培育等業務能量，以完備網路安全措施。
4. 基於安全設計（security by design）或安全預設（security by default）原則，促進物聯網設備或軟體產品之網路安全。
5. 促進中小企業網路安全措施，如根據公司規模提供其所需服務或人力資源協助。
6. 與國際網路安全相關組織並加強印太地區之合作，如 G7、FIRST（Forum of Incident Response and Security Teams），並透過演練等方式相互合作。
7. 推動日本警察機構與國內外調查機構、組織合作，如資訊分享，以確保網路空間之安全。

綜上，網路安全戰略本部第 41 次會議之報告，重點在於 2024 年執行摘要，並說明當前網路安全情勢分析，及本年度執行報告及次年度計畫等內容。且依據網路安全基本法（サイバーセキュリティ基本法）第 26 條，日本政府也優先編列網路安全相關預算，以利執行。

資料來源：

1. サイバーセキュリティ戦略本部, サイバーセキュリティ 2024

本報告之智慧財產權歸屬於國發會

（2023 年度年次報告・2024 年度年次計画）, 2024-07-10, https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024.pdf (last visited 2024/07/24)

2. サイバーセキュリティ戦略本部, サイバーセキュリティ関係施策に関する令和７年度予算重点化方針が決定されました, 2024-07-10, https://www.nisc.go.jp/pdf/policy/kihon-s/yosanhosin_r7.pdf (last visited 2024/07/24)

三、 美國

(一)2024 年 7 月美國網路安全暨基礎設施安全局發布基礎設施韌性規劃架構之說明手冊，以利落實該架構之相關步驟與配套措施

美國國土安全部所屬網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）於 7 月 17 日發布基礎設施韌性規劃架構（Infrastructure Resilience Planning Framework, IRPF）之說明手冊（Infrastructure Resilience Planning Framework Playbook），主要供地方政府與各關鍵基礎設施營運者參考，俾利落實 IRPF 建議之步驟與配套措施。

CISA 係美國網路安全與基礎設施安全之主管機關，為提升關鍵基礎設施之安全及韌性，前已於 2024 年 3 月發布基礎設施韌性規劃架構。此一架構由 5 個步驟與配套措施所組成，茲摘要重點如下：

步驟 1、界定基礎（Lay the Foundation）：包含 5 項內容，分別是確定專案範圍、定義與確定執行範圍、蒐集與檢視現有資訊、成立協調工作組，及訂定目的與目標。

步驟 2、識別關鍵基礎設施（Identify Critical Infrastructure）：包含 3 項內容，分別是識別關鍵基礎設施、確定優先投入資源之關鍵基礎設施，及確定關鍵基礎設施之相互依賴性。

本報告之智慧財產權歸屬於國發會

步驟 3、評估風險（Assess Risk）：包含 4 項內容，分別是識別關鍵基礎設施面臨之威脅與危害、評估關鍵基礎設施之漏洞、評估影響，及確定優先處理之關鍵基礎設施風險。

步驟 4、發展行動措施（Develop Actions）：包含 5 項內容，分別是細化目的與目標、識別降低風險之韌性解決方案、識別與評估現有資源與能力、選擇預計執行之韌性解決方案，及發展執行策略。

步驟 5、執行及成效評估（Implement & Evaluate）：包含 3 項內容，分別是搭配現有規劃或機制執行、監控與評估有效性，及更新相關規劃。

7 月發布之說明手冊屬自願性質之參考文件，包含：搭配前述 5 步驟與相關內容，結合輸入、流程及虛擬場景等，以利執行。以步驟 1 之定義與確定執行範圍為例，建議先挑選專案負責人，由其與最高管理階層或各部門領導者進行協調，規劃相關執行範圍、制定時間表，並召開會議、邀請利害關係人參與等。

說明手冊可幫助各關鍵基礎設施營運者或其他對象，有效地執行 IRPF 提及之步驟與配套措施。例如：使用者可透過該 IRPF 說明手冊之虛擬場景，了解輸入、輸出，並規劃相關劇本，以供事件演練之用，俾利落實韌性及快速復原等。

資料來源：

1. CISA, CISA Releases Playbook for Infrastructure Resilience Planning, 2024-07-17,https://www.cisa.gov/news-events/news/cisa-releases-playbook-infrastructure-resilience-planning (last visited 2024/07/31)
2. CISA, Infrastructure Resilience Planning Framework (IRPF), 2024-03-25, https://www.cisa.gov/resources-tools/resources/infrastructure-resilience-planning-framework-irpf (last visited 2024/07/31)

本報告之智慧財產權歸屬於國發會

本報告之智慧財產權歸屬於國發會

項次 4. 十月雙月報

壹、 資料治理

一、 日本

(一)2024 年 7 月日本數位廳公布《資料開放基本指引》修正草案意見徵集結果

日本數位廳於 7 月 31 日發布新聞，說明《資料開放基本指引》（オープンデータ基本指針）修正草案意見徵集之結果。本次指引修正重點摘要說明如下：

1. 在推動資料開放部分，將地方政府資料開放推動指引（地方公共団体オープンデータ推進ガイドライン，最近一次修正為 2023 年 4 月）內容納入，俾供地方政府參考。

2. 增加數位轉型（DX）等描述，以促進對資料開放意涵之理解。

3. 有鑑於生成式 AI 於行政資料層面之應用，鼓勵地方政府應採用政府相關標準使用條款（政府標準利用規約），並擴大推動行政資料之二次利用。

4. 縱使尚未發布之資料未來不一定會成為開放資料，但得於有限度之利用目的或接收者之情境下，鼓勵主動提供未發布之資料。

目前日本政府推動資料開放或資料利用之意涵，主要有 3 項，包含：1. 透過公眾參與或公私協作，以解決各類問題並振興經濟。例如期望透過技術創新，解決日本面臨之嚴峻金融情勢，或快速之老化或少子化現象；2. 促進行政管理細緻化，並提高效率。如透過資料利用所得結果，作為中央或地方政府規劃施政之參考（Evidence Based Policy Making）；以及 3. 提高透明度與信任感。如公開決策所利用之資料，讓民眾對相關政策或公共服務，能作出充分之分析與判斷。

本報告之智慧財產權歸屬於國發會

此一資料開放基本指引修正草案之內容前於 2024 年 2 月對外徵詢，經本次公布成果完成修訂程序後，即已落實 2023 年 6 月內閣會議決議，朝向實現數位社會重點計畫（デジタル社会の実現に向けた重点計画）當中，要求修訂資料開放基本指引之要求。

資料來源:

1. デジタル庁, 「オープンデータ基本指針」に係る意見募集の結果が公表されました, 2024-07-31, https://www.digital.go.jp/news/be176649-155c-4e12-b3af-a787939f54f6 (last visited 2024/08/14)
2. デジタル庁, 「オープンデータ基本指針」に係る意見募集を行います, 2024-02-13, https://www.digital.go.jp/news/7290df8a-ea84-4332-8cc0-1fe85e69b599 (last visited 2024/08/14)
3. デジタル庁, オープンデータ基本指針（改正案）改正履歴あり, 2024-02-13, https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/7290df8a-ea84-4332-8cc0-1fe85e69b599/fb0415d5/20240213_news_public_comments_draft_01.pdf (last visited 2024/08/14)

二、韓國

(一)2024 年 9 月韓國個人資料保護委員會決議針對「於公部門處理大量個資的系統」採取更嚴格之資料保護措施

2024 年 9 月韓國個資保護委員會（Personal Information Protection Commission, PIPC）為加強公部門處理個人資料的安全性、預防資料外洩及個資濫用，於第 15 次全體會議決議要求於公部門處理大量個資的系統，應採取更嚴格的資料保護措施（Higher Data Protection Safeguards）。

本報告之智慧財產權歸屬於國發會

受此一決議影響之公部門，包含：韓國國土交通部、韓國不動產委員會（Korea Real Estate Board）、韓國當地資訊開發研究院（Korea Local Information Research & Development Institute）、韓國教育與研究資訊服務中心（Korea Education and Research Information Service, KERIS）等地方政府及教育辦公室所使用的 28 個系統。

於 3 年計畫（2023~2025 年）施行的第 2 年，PIPC 針對中央與地方行政部門的標準傳遞系統（standards dissemination systems），決議公部門應採取更嚴格的資料保護措施：

1. 公部門推動迄今較有進展的資料保護措施，須持續強化：

   (1) 設置並運行公部門系統之諮詢委員會：公部門採取比例已從 3%增至 94%。

   (2) 建置隱私保護計畫：公部門建置比例已從 25%增至 66%。

   (3) 聘僱個資專責人員：公部門設置個資專責人員比例，已從平均 0.35 人提升至 1.7 人。

2. 公部門現階段仍有待加強之資料保護措施：

   (1) 針對特定系統指定隱私長（system-specific Chief Privacy Officer, CPO）。

   (2) 將人員相關資料（Mapping HR data）對應至各資訊系統，以控管資料密集型系統（data-intensive system）之人員存取權限（包含區隔非公務人員之權限控管）。

   (3) 加強檢查系統之日誌存取紀錄（access logs），並於系統中建置偵測異常活動的功能。

   (4) 擴大系統規模，提升系統的基礎設施及技術能力。

本報告之智慧財產權歸屬於國發會

決議自 2024 年 9 月 15 日生效，開始強制施行前述各項資料保護措施。

資料來源：

1. Personal Information Protection Commission, PIPC Recommends Systems Processing Vast Amounts of Personal Data in the Public Sector Take Higher Data Protection Safeguards, 2024-09-19, https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=2663 (last visited 2024/09/24)

貳、AI 法制政策

一、美國

(一)2024 年 5 月美國勞工部發布《AI 與勞工福祉：開發人員與雇主原則》

2024 年 5 月美國勞工部(United States Department of Labor, USDOL)發布《AI 與勞工福祉：開發人員與雇主原則》(Artificial Intelligence and Worker Well-being：Principles for Developers and Employers)，以回應拜登總統 2023 年 10 月發布關於開發及使用安全、可靠且可信任之 AI 行政命令（Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence，EO14110，下稱 AI 行政命令)。AI 發展擁有非凡的潛力，若於工作場所利用，能提升工作效率，例如：使用 AI 取代自動化重複性任務、或協助日常決策以增強工作能力、或減輕勞工負擔，使其得以更好的履行其職責。惟使用 AI 於工作場所影響的確切範圍及性質仍不確定，決策過程中可能嵌入偏見和歧視，或在沒有透明度、人力監督及審查的情況下做出重要的工作決策，對於勞工會產生失業、個人隱私、就業歧視及員工福祉等風險，USDOL 對此發布此指引，為開發人員和雇主於工作場所使用 AI 制定

本報告之智慧財產權歸屬於國發會

原則，解決工作場所使用 AI 的複雜性，確保勞工從 AI 創造的新機會中受益，並避免遭受潛在的危害，下列為 8 項原則：

1. 以工作者賦權為核心（Centering Worker Empowerment）：工作者或其代理人，尤其那些來自資源匱乏社區之工作者必須被充分告知並實際參與針對使用於其工作場所之 AI 系統的設計、開發、測試、訓練、使用與監督等過程。

2. 以符合倫理方式開發 AI（Ethically Developing AI）：AI 系統應以能夠保護工作者之方式執行 AI 系統的設計、開發及訓練。

3. 建立 AI 治理及人員監督機制（Establishing AI Governance and Human Oversight）：採用 AI 之組織必須針對使用於工作場所之 AI，具備清楚的治理制度、程序、人員監督機制以及評估流程。

4. 確保利用 AI 之透明度（Ensuring Transparency in AI Use）：雇主應該對員工與求職者公開工作場所使用之 AI 系統。

5. 保護勞工及就業權利（Protecting Labor and Employment Rights）：AI 系統之運用不能侵害或減損工作者之相關權利，包括組織權利、健康/安全的權利、薪資與工時的權利、反歧視及反報復之保護等。

6. 使用 AI 賦能工作者（Using AI to Enable Workers）：AI 系統應協助、補強及賦予工作者之能力，並提升工作品質。

7. 支持受 AI 影響之工作者(Supporting Workers Impacted by AI)：雇主應於 AI 相關工作轉換期間，為相關工作者提供支援或提高其技能。

8. 確保負責任地使用工作者資料（Ensuring Responsible Use of Worker Data）：AI 系統蒐集、利用或創造工作者之資料，必須

本報告之智慧財產權歸屬於國發會

限定於特定範圍或地點，亦僅能應用於支持組織之合法業務目標，並受到負責任之保護與處理。

上述之原則適用於工作場所 AI 系統的開發及部署，並需於 AI 之整個生命週期予以考量，從設計到開發、測試、培訓、部署與使用、監督及稽核。該指引之原則，僅為提供事業之指導架構，AI 開發人員及雇主應根據自身情況及員工的意見，審查及客製出最佳之實踐方法。

資料來源：

1. Department of Labor's Artificial Intelligence and Worker Well-being: Principles for Developers and Employers, 2024-05-16, https://www.dol.gov/general/AI-Principles (last visited 2024/09/10)

(二)2024 年 7 月美國參議員正式提出《培育原創、促進藝術與保障娛樂安全法》

2024 年 7 月 31 日美國兩黨參議員組成的小組正式提出《培育原創、促進藝術與保障娛樂安全法》（Nurture Originals, Foster Art, and Keep Entertainment Safe （NO FAKES） Act，下稱《禁止偽造法案》）。相較於 2023 年的《禁止偽造法案》之草案，著重於防止在未經授權之前提下，透過數位技術複製個人之聲音或肖像以創造數位複製品，2024 年提出之《禁止偽造法案》則更強調，防止生成式 AI 於未經授權的情況，以深偽技術利用個人的聲音或肖像創造數位複製品。

《禁止偽造法案》所定義之「數位複製品（Digital Replica）」，係指以數位方式創造易被認為高度相似於真實個人之聲音或影像，實際上卻是偽造特定對象之聲音、影像或影音的作品；或在未經當事人授權的情況，使用、重製該當事人的聲音或影音作品於其他影音作品。該法案指出每個人都擁有「授權他人使用自己的聲音、肖像於數位複製品」的智慧財產權。以下簡介法案重點，稱此權利為「數位複製權」。

本報告之智慧財產權歸屬於國發會

1. 優先適用範圍

除與色情或選舉相關之數位複製品的州法規定外，原則上，《禁止偽造法案》優先於州法適用。

2. 排除適用之安全港條款

《禁止偽造法案》規定之安全港條款可分為 2 類型。第 1 類型係美國憲法第 1 修正案所保障之言論自由，包括：善意（bona fide）新聞、公共事務、體育廣播、作為文獻及歷史之紀錄（documentary and historical uses）、評論、批評、學術、戲謔仿作的數位複製品之創作或使用，以及短暫或可忽略不計的情況；第 2 類型為線上服務提供商於收到數位複製權人的通知後，於其技術與可行情況下，刪除或禁止訪問該未經授權的數位複製品。

3. 數位複製權之有效期限

數位複製權的年限為每個人生前至其死亡後 70 年。

數位複製權人可授權他人數位複製權的期限為 10 年。未成年人可授權他人數位複製權的期限為 5 年。

數位複製權人死亡後，由數位複製權人之法定繼承人取得該權利，該權利繼承人需要證明於數位複製權人死亡後，繼承人仍有持續的商業使用行為，且符合美國著作權局的死亡後權利註冊要求，則繼承人最初可取得之 10 年數位複製權，可按次延長 5 年，年限最多可延長至數位複製權人死亡後 70 年。

4. 法律責任

本報告之智慧財產權歸屬於國發會

數位複製權涉及民事責任，損害賠償的計算方式係將每件作品以 5 千美元至 2 萬 5 千美元計算，與實際所受損害相比，取較高者為計算。

5. 訴訟時效

訴訟時效為權利人發現或於盡職調查後發現侵權行為時起算 3 年。

參議院是否會通過《禁止偽造法案》，仍有待觀察。

資料來源：

1. Congress.gov, Nurture Originals, Foster Art, And Keep Entertainment Safe (No Fakes) Act, 2024-08-01, https://www.congress.gov/congressional-record/congressional-record-index/118th-congress/2nd-session/nurture-originals-foster-art-and-keep-entertainment-safe-no-fakes-act/1920107 (last visited 2024/08/23)
2. Sheppard Mullin, Closer to a Federal Right of Publicity – Senate Introduces NO FAKES Act, 2024-08-14, https://www.ailawandpolicy.com/2024/08/closer-to-a-federal-right-of-publicity-senate-introduces-no-fakes-act/ (last visited 2024/08/23)
3. McDermott Will & Emery, NO FAKES Act Would Create Individual Property Right to Control Digital Replicas, 2024-08-08, https://www.ipupdate.com/2024/08/no-fakes-act-would-create-individual-property-right-to-control-digital-replicas/ (last visited 2024/08/23)

(三)2024 年 8 月美國白宮說明《晶片及科學法》2 週年之施行情形，肯定在美國當地半導體生產之成效

本報告之智慧財產權歸屬於國發會

美國白宮於 8 月 9 日發布新聞，說明《晶片及科學法》(CHIPS and Science Act，簡稱晶片法)2 週年之施行情形，包含半導體製造業回流、為美國當地勞動力創造就業機會、加速區域經濟發展、保護國家安全，以及投資創新。例如：美國事業已對半導體與相關電子產品投資超過 3,950 億美元，並創造超過 11 萬 5,000 個就業機會。

此外，透過該法規範之補助法源，聯邦政府也據此相繼進行投資。如美國國防部已投資 2.8 億美元在 6 項領域，包含：物聯網、電磁戰、5G/6G、量子技術、AI 等科技，用以生產關鍵國防專案（如 F-35 戰鬥機與其他項目）所需之晶片，以及影響所有美國人民日常生活或應用之晶片，如從汽車到安全之 Wi-Fi 等。

《晶片法》源自 2022 年時，有鑑於美國在全球半導體產業的影響力不斷下降，且特別是在相關晶片製造與研究，更由過去佔全球供應量近 40%，下降至當年約 10%左右。不僅美國各界對於其國內半導體產業之競爭力產生憂慮，加上近年中國大陸之威脅與科技領域之競爭，在拜登總統的呼籲下，美國參眾兩院遂於 2022 年 8 月達成共識研議通過，以鼓勵半導體與相關發展。

《晶片法》主要內容係以促進美國半導體研發、製造，以及增加勞動力等措施為主。如由聯邦政府提供 530 億美元補助，並由國家標準與技術研究院（National Institute of Standards and Technology, NIST）結合美國公、私部門共同促進該領域之合作。此外，尚提供半導體及相關基礎設施資本支出之 25%，可作為投資抵減等優惠，旨在推動美國本土半導體產業之發展，與吸引半導體供應鏈相關之產業前往美國設廠。

而《晶片法》訂定之目標與執行重點，在於降低美國半導體產業鏈對他國之依賴、完善其在當地半導體之產業生態系等。依 8 月之新聞稿內容可知，該法施行 2 年後，已逐漸帶動廠商回流美國當地投資、製造，其中商務部已與 15 家事業達成協議，預計提供 390 億美元之補

本報告之智慧財產權歸屬於國發會

助，目前已提供逾 300 億美元。又，美國當地已逐漸具備先進封裝設施、半導體及關鍵供應鏈零組件之生產能力，未來將持續建立一個強大的半導體生態系統。最終希冀能支援汽車與醫療之關鍵產業，或 AI 與航太相關設備之製造等，以保障美國國家安全。

資料來源：

1. The White House, FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China, 2022-08-09, https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/ (last visited 2024/08/21)
2. The White House, FACT SHEET: Two Years after the CHIPS and Science Act, Biden-Harris Administration Celebrates Historic Achievements in Bringing Semiconductor Supply Chains Home, Creating Jobs, Supporting Innovation, and Protecting National Security, 2024-08-09, https://www.whitehouse.gov/briefing-room/statements-releases/2024/08/09/fact-sheet-two-years-after-the-chips-and-science-act-biden-%e2%81%a0harris-administration-celebrates-historic-achievements-in-bringing-semiconductor-supply-chains-home-creating-jobs-supporting-inn/(last visited 2024/08/21)

(四)2024 年 8 月美國聯邦通訊委員會發布關於 AI 生成內容之通話及簡訊之擬議規則制定通知

2024 年 8 月美國聯邦通訊委員會（Federal Communications Commission, FCC）發布擬議規則制定通知（Notice of Proposed Rulemaking, NPRM），指出非法使用 AI 生成之自動語音電話（robocalls）及自動發送之簡訊（robotexts），違反電話消費者保護法（Telephone Consumer Protection Act, TCPA）。因使用深度偽造（deepfake）技術模擬可識別真實人聲或預先錄製之語音，向消費者進行語音電話及發送

本報告之智慧財產權歸屬於國發會

簡訊，或未先行取得消費者同意、提供身分識別及揭露必要資訊，進而傳播錯誤訊息、產品資訊及冒名頂替等相關詐騙案件層出不窮。為保護消費者權益，平衡現行 TCPA 與 AI 技術發展的變化，FCC 發布 NPRM 如下，徵求公眾意見評論：

1. AI 生成內容通訊之定義：使用任何技術或工具產生人工或預先錄製之語音，或使用計算技術（computational technology）或其他機器學習（machine-learning）（包括預測演算法及大型語言模型）方式處理自然語言並產生語音或文字內容，以與受話對象透過聯外電話進行通訊者稱之。

2. AI 生成內容通訊之揭露：規則中要求通訊者，於撥打與發送使用 AI 生成之人工或預先錄製之語音電話與簡訊時，須清楚明顯的揭露該語音通話與簡訊為 AI 技術之利用，並說明若被通訊者同意接收該人工或預先錄製之語音電話或簡訊，亦包括同意接收該 AI 生成內容。

3. 語言或聽力障礙人士利用相關技術之豁免權：NPRM 建議若為有語言或聽力障礙人士使用 AI 技術（例如：文字轉語音或語音產生器）進行的人工或預先錄製人聲語音電話與簡訊，應豁免於 TCPA 相關要求，以確保身障人士能透過 AI 技術擁有透過電話網路溝通之能力。

4. 監管措施使用的成本與效益：FCC 期望可就其所建議之 AI 相關監管措施，可能產生之潛在成本與效益徵詢意見。即採取相關監管措施，是否得以提高消費者（被通訊者）得以識別、管理並受益於使用 AI 生成內容通訊之能力。

5. 法律授權：TCPA 授權 FCC 訂定此 NPRM，若最終此 NPRM 被採納，則使用 AI 生成內容之通訊者，除了遵守現有 TCPA 的規定，亦必須遵守新的擬議規則。

本報告之智慧財產權歸屬於國發會

6. 數位平權及包容：FCC 將持續促進數位平權，故徵求各界對此 NPRM 如何促進或妨礙多樣性、公平性、包容性等議題提出意見。

FCC 本次徵集期限為 NPRM 於聯邦公報上發布後 30 天。

資料來源：

1. NOTICE OF PROPOSED RULEMAKING AND NOTICE OF INQUIRY, 2024-08-08, https://docs.fcc.gov/public/attachments/FCC-24-84A1.pdf (last visited 2024/08/28)
2. Deep-Fake Audio and Video Links Make Robocalls and Scam Texts Harder to Spot, 2024-06-08, https://www.fcc.gov/consumers/guides/deep-fake-audio-and-video-links-make-robocalls-and-scam-texts-harder-spot (last visited 2024/08/28)
3. FCC Proposes New Rules for AI-Generated Content in Calls and Texts , 2024-08-16 , https://www.jdsupra.com/legalnews/fcc-proposes-new-rules-for-ai-generated-4151533/chrome://whats-new (last visited 2024/08/28)

(五)2024 年 8 月美國伊利諾州州長簽署新法案，要求雇主揭露其使用 AI 作成就業決策之情形

美國伊利諾州州長 JB Pritzker 於 2024 年 8 月 9 日簽署 HB 3773 法案，該法案主要係針對伊利諾州人權法（Illinois Human Rights Act）進行修訂，將演算法歧視認定為侵犯人民權利之行為，允許伊利諾州之事業員工就其雇主使用 AI 系統所導致的歧視尋求救濟。並要求伊利諾州之雇主於作出就業決策時，須向員工或求職者揭露使用 AI 技術之情況，以及禁止使用對員工或求職者可能產生歧視行為之 AI，以下簡要敘述本次簽署法案之重點：

本報告之智慧財產權歸屬於國發會

1. 伊利諾州人權法規範雇主從事某些活動將侵害人民權利，例如：雇主不能以特定受保護類別（包括種族、膚色、宗教、性別、國籍、血統、年齡、保護令狀態、婚姻狀況等）為由拒絕僱用或晉升員工。而 HB 3773 法案將採用 AI 技術列為可能造成潛在權利侵害之行為，並禁止於招聘、僱用、晉升、續聘、擇定參訓或學徒、解雇、紀律處分、決定任期或僱傭相關條款、權利或條件等方面使用 AI，使受雇者因而受到歧視；或利用郵遞區號作為本法規定受保護類別之識別代號等。

2. 雇主應評估已採用或計畫採用之 AI 系統，確保其不會產生歧視之影響。並須以清晰、透明之方式，告知員工或求職者有關 AI 系統於就業決策過程之利用。同時，必須依據新的法案，更新既有之政策及程序，確保適當之 AI 利用，並採行影響評估及保護措施，以防止歧視。對於與招募、聘僱、晉升、紀律管理流程等事務執行相關之員工，必須就如何正確使用 AI 進行適當之培訓，包括如何識別及降低 AI 系統偏差之相關資訊。最後必須建立相關機制，對新法之法律遵循進行有效監控，尤其須對 AI 於就業決策之利用進行定期之稽核、審查與評估。

3. 依據該法案，權利受到侵害的員工得向伊利諾州人權部（Illionis Department of Human Right）及人權委員會（Illinois Human Rights Commission）提出申訴，委員會進行初步調查，後續並得提起訴訟。

HB 3773 法案將於 2026 年 1 月 1 日生效，目前伊利諾州成為繼科羅拉多州之後，第二個要求在就業決策中揭露 AI 使用情況的州。

資料來源：

1. Illinois House Bill 3773, 2024-08-09, https://legiscan.com/IL/text/HB3773/id/3002985 (last visited 2024/08/19)

本報告之智慧財產權歸屬於國發會

2. JD Supra, Illinois Civil Rights Protection Goes High-Tech: Illinois Human Rights Act Expanded to Include AI Regulation, 2024-08-15, https://www.jdsupra.com/legalnews/illinois-civil-rights-protection-goes-4853044/ (last visited 2024/08/19)

3. JD Supra, Illinois Passes Bill to Regulate Use of Artificial Intelligence in Employment Settings, 2024-08-22, https://www.jdsupra.com/legalnews/illinois-passes-bill-to-regulate-use-of-7856601/ (last visited 2024/08/27)

4. Employmentlawworldview, Illinois Enacts New AI Legislation, Joining Colorado as the Only States Regulating Algorithmic Discrimination in Private Sector Use of AI Systems (US), 2024-08-19, https://www.employmentlawworldview.com/illinois-enacts-new-ai-legislation-joining-colorado-as-the-only-states-regulating-algorithmic-discrimination-in-private-sector-use-of-ai-systems-us/ (last visited 2024/08/29)

(六)2024 年 8 月加州參議院通過《生成式 AI 訓練資料透明度法案》(AB-2013 法案)，州長已於 9 月簽署生效

2024 年 8 月 27 日加州參議院通過《生成式 AI 訓練資料透明度法案》（AB 2013 法案）（Generative artificial intelligence: training data transparency bill），旨於提升 AI 訓練資料之透明度，要求 AI 開發者於向加州人民提供 AI 系統或服務前，應公開發表透明度聲明。此法案已於 9 月底由加州州長簽署生效。

以下說明 AB 2013 法案重點：

1. 適用對象

生成式 AI 開發者，指設計、編碼、生產或大幅修改（substantially modifies）生成式 AI 系統或服務，提供公眾（即加州人民）使用 AI 之個人、合夥事業、州或地方政府機構或公司。

本報告之智慧財產權歸屬於國發會

2. 此法案對生成式 AI 之定義

生成式 AI 係指模擬 AI 訓練資料的結構與特徵，生成虛擬的內容（generate derived synthetic content），例如文字、圖像、影片及音訊等。

3. 要求 AI 開發者提出透明度聲明之義務

要求在 2022 年 1 月 1 日至 2026 年 1 月 1 日期間，提供加州人民生成式 AI 系統或服務或有實質修改其生成式 AI 系統之開發者，應於其官網公開說明其訓練 AI 之資料，包括但不限於：資料集的來源或所有者；描述資料集如何進一步實現 AI 系統或服務的預期目的；描述一定時間內，動態資料集所包含之資料點的大約數量；描述資料點的標籤類型；資料集是否包含受著作權、商標或專利保護的任何資料，或資料集是否完全屬於公共財；是否購買或取得資料集之授權；是否包含加州消費者隱私權法案（California Consumer Privacy Act, CCPA）第 1798.140 條第 v 項規定之個人資料；是否包含前述同條之整合性消費者資料（aggregate consumer information）；AI 開發者是否對資料集進行任何清理、處理或其他修改，包括為使 AI 系統或服務符合預期目的之行為；蒐集資料集中資料的時間區段；開發過程中首次使用資料集的日期；揭露是否使用或持續性使用「由演算法生成之虛擬資料（synthetic data generation）」作為其 AI 之訓練資料。

當生成式 AI 應用於下列類型，不得要求其公開 AI 系統或服務之訓練資料：生成式 AI 系統或服務，其唯一目的是協助確保安全性與完整性；或其唯一目的用於美國領空飛行；或其係因國安、軍事目的而開發，或僅供聯邦機構使用。

資料來源：

本報告之智慧財產權歸屬於國發會

1. AB-2013 Generative artificial intelligence: training data transparency.(2023-2024), 2024-01-31, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB2013 (last visited 2024/09/10)

2. Husch Blackwell, California Privacy and AI Legislation Update: September 2, 2024, 2024-09-01, https://www.bytebacklaw.com/2024/09/california-privacy-and-ai-legislation-update-september-2-2024/#lxb_mct-form-1 (last visited 2024/09/10)

3. Alston & Bird, California Passes Generative AI "Training Transparency" Bill, 2024-08-30, https://www.alstonprivacy.com/california-passes-generative-ai-training-transparency-bill/?cn-reloaded=1(last visited 2024/09/10)

4. Governor Gavin Newsom, Governor Newsom announces new initiatives to advance safe and responsible AI, protect Californians, 2024-09-29, https://www.gov.ca.gov/2024/09/29/governor-newsom-announces-new-initiatives-to-advance-safe-and-responsible-ai-protect-californians/ (last visited 2024/10/08)

(七)2024 年 8 月美國 AI 安全研究所與 Anthropic 及 OpenAI 2 家公司簽署 AI 安全研究、測試及評估協議

美國國家標準與技術研究院（National Institute of Standards and Technology, NIST）於 8 月 29 日發布新聞，NIST 轄下之 AI 安全研究所（AI Safety Institute）已與 Anthropic 及 OpenAI 2 家公司簽署協議，就 AI 安全之研究、測試及評估等事宜進行合作。

自 2022 年底 OpenAI 公司之 ChatGPT 問世後，生成式 AI 與相關應用蔚為風潮，但因用來供訓練模型之資料或產出結果，可能涉及智慧財產權、個人隱私保護等相關議題，亦讓外界對 AI 之安全、可信任等產生疑義。為此，白宮於 2023 年 7 月邀請 OpenAI 等 7 家公司，研討 AI 安全、保障及信任之內容。更於 2023 年 10 月公布開發及使用

本報告之智慧財產權歸屬於國發會

安全、可靠且可信任之 AI 行政命令，說明拜登政府對於 AI 安全之政策目標，如建立 AI 安全標準、保護美國人民權益、提升研發與競爭力，及強化國際合作，並要求各部會制定並推動相關配套措施。

本次協議，NIST 將分別與各家公司就其 AI 模型，不論於簽署之前或之後所開發，依該 MOU 之內容，對 AI 模型能力與安全風險，及如何減輕相關風險之方法進行合作研究。此類措施除有助於減輕 AI 安全風險外，主要係為落實前述 2023 年 10 月之開發及使用安全、可靠且可信任之 AI 行政命令，並呼應 NIST 之 AI 風險管理框架（AI Risk Management Framework, AI RMF），以持續推動負責任 AI 之研發。

此外，NIST 也將與英國 AI 安全研究所之夥伴密切合作，向 Anthropic 及 OpenAI 2 家公司提供有關渠等 AI 模型潛在安全風險之改進建議。按英國自 2023 年 11 月與美國等國際夥伴發布布萊切利宣言（the Bletchley Declaration）後，積極投入政府資源鼓勵 AI 研發，成立 AI 安全研究所也是配套措施之一。

資料來源：

1. NIST, U.S. AI Safety Institute Signs Agreements Regarding AI Safety Research, Testing and Evaluation With Anthropic and OpenAI, 2024-08-29, https://www.nist.gov/news-events/news/2024/08/us-ai-safety-institute-signs-agreements-regarding-ai-safety-research (last visited 2024/09/11)
2. The White House, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 2023-10-30, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ (last visited 2024/09/11)

本報告之智慧財產權歸屬於國發會

(八)2024 年 8 月美國聯邦交易委員會公布《關於消費者評論與薦證之貿易監管規則》，涉及監管 AI 所生成的虛偽消費者評論

2024 年 8 月 14 日美國聯邦交易委員會(Federal Trade Commission, FTC)公布《關於消費者評論與薦證之貿易監管規則(最終規則)》(Rule on the Use of Consumer Reviews and Testimonials (Final Rule))。FTC 主席認為虛偽評論浪費人民的時間與金錢，並減損市場競爭效能，導致競爭業務自誠實的競爭對手中轉移。以下簡要敘述最終規則之重點：

1. 禁止虛假、偽造的消費者評論、消費者薦證與名人薦證

本此修正之規範涉及由不存在之作者所撰寫之評論及薦證，例如 AI 生成的虛假評論；或不具業務或其產品或服務的實際經驗的人員提供或扭曲提供者體驗之評論等。此最終規則禁止事業建立或銷售此類評論或薦證，亦禁止事業於知悉評論或薦證是虛假情況下購買、獲得或傳播此類評論及薦證。

2. 禁止購買正面或負面評論

此最終規則禁止事業以提供補償或其他激勵措施，促使消費者撰寫表達特定情緒（正面或負面）之評論。

3. 內部人評論與消費者推薦

最終規則禁止由公司內部之人士撰寫無法清楚明顯揭露提供者與事業之實質關係之評論或推薦，包括禁止主管或經理撰寫此類評論。亦禁止事業散布由主管、經理、員工或代理人所提供的薦證。此外，當主管或經理向自己的直系親屬、員工或代理人徵求消費者評論，或主管或經理要求員工或代理人向其親屬徵求評論時，此類要求若導致員工或代理人的直系親屬（immediate relatives）作出評論則應被禁止。

4. 禁止事業扭曲其控制的評論網站

本報告之智慧財產權歸屬於國發會

本此修正之規範禁止事業扭曲其控制的網站提供包含對其自身產品或服務提供獨立的評論或意見。

5. 評論之壓制

此修正之規範禁止事業使用威脅恐嚇來阻止或刪除負面消費者評論。

6. 濫用虛假社交媒體指標

此修正之規範禁止任何人出售或購買社交媒體影響力的虛假指標，例如由機器人或被劫持帳戶生成的追蹤者或評論。

該規則於發布 60 天後生效。

資料來源：

1. Federal Trade Commission, Federal Trade Commission Announces Final Rule Banning Fake Reviews and Testimonials, 2024-08-14, https://www.ftc.gov/news-events/news/press-releases/2024/08/federal-trade-commission-announces-final-rule-banning-fake-reviews-testimonials (last visited 2024/09/07)
2. Federal Trade Commission,16 CFR Part 465: Trade Regulation Rule on the Use of Consumer Reviews and Testimonials (Final Rule) , 2024-08-14, https://www.ftc.gov/legal-library/browse/federal-register-notices/16-cfr-part-465-trade-regulation-rule-use-consumer-reviews-testimonials-final-rule (last visited 2024/09/07)
3. JD Supra, FTC Cracks Down on AI-Generated Fake Reviews – AI: The Washington Report, 2024-08-23, https://www.jdsupra.com/legalnews/ftc-cracks-down-on-ai-generated-fake-8501222/ (last visited 2024/09/07)

本報告之智慧財產權歸屬於國發會

(九)2024 年 9 月加州州長核准 18 個與監管、部署 GenAI 相關法案，其中否決嚴格監管 AI 之《SB 1047 法案》

參照加州州長所發布之新聞稿，加州於 2024 年 9 月期間簽署 18 個與監管、部署生成式 AI(Generative AI, GenAI)相關之法案，其中否決受各界關注之《SB 1047 法案》。本文將 18 個法案分類並簡要說明如下：

1. 與 AI 整體之監管架構相關

(1) 《AB 2885 法案》：在加州法律中建立對 AI 的一致性定義。

(2) 《SB 896 法案》：要求加州科技部（California Department of Technology, CDT）依據 N-12-23 行政命令，向州長提供美國採購與使用生成式 AI 的報告；要求緊急服務辦公室（Office of Emergency Services, OES）針對生成式 AI 對加州關鍵基礎設施的潛在威脅進行風險評估與分析（並向立法機構提供摘要）；要求於州政府於通訊中使用生成式 AI 時，應予以揭露。

2. 與深偽議題相關

(1) 《AB 1836 法案》、《AB 2602 法案》：分別規範禁止 AI 於未取得同意的情況下，生成「表演藝術者」或「已故表演藝術者」之數位複製品（digital replica）。

(2) 《SB 981 法案》：要求社群媒體平臺建立報告（report）機制，並移除使用者標記為深偽的裸露照片。

(3) 《SB 926 法案》：規定使用深偽的裸露照片勒索他人，構成犯罪。

本報告之智慧財產權歸屬於國發會

(4) 《AB 1831 法案》、《SB 1381 法案》：規範擴大現行兒童色情物品法律的適用範圍，將透過 AI 進行數位修改或生成的物品列入其中。

(5) 《AB 2355 法案》：要求創造、發布「含有 AI 生成或實質性修改圖片、音檔或影片」的政治廣告者，應於該廣告中揭露廣告含有 AI 生成內容之聲明。

(6) 《AB 2839 法案》：將禁止委員會或其他實體故意傳送含有 AI 生成或操縱之欺騙性內容的廣告或其他選舉素材之時間範圍自 60 天延長至 120 天，並涉及其他條款。

(7) 《AB 2655 法案》：要求擁有至少一百萬加州使用者的大型網路平臺，於選舉前後的特定期間，若平臺接到通知，應移除與選舉相關之欺騙性與經過數位修改或創造的內容，或應標示該內容。

3. 與資料議題相關

(1) 《AB 1008 法案》：與個人資料相關。闡明加州消費者隱私法（CCPA）所納管的個人資料得以多種格式存在，包括 AI 系統儲存的資訊。

(2) 《AB 2013 法案》：與資料透明度相關。要求 AI 開發者在其網站發布其 AI 系統或服務之訓練資料資訊。

(3) 《SB 942 法案》：與資料來源相關。要求生成式 AI 系統的開發者在其系統生成的原始內容中包含來源揭露，並提供工具以識別生成式 AI 所生成的內容。

4. 與特定產業（醫療）相關

(1) 《AB 3030 法案》：要求特定的醫療提供者應向患者揭露其使用生成式 AI 來生成與臨床資訊相關的內容。

本報告之智慧財產權歸屬於國發會

(2) 《SB 1120 法案》：規定醫療保險與保險公司於應用 AI 進行使用審查（utilization review）或使用管理決策（utilization management decisions）時，必須審酌患者病歷、其他臨床病史及申請醫療保險之提供者（requesting provider）提出之個人臨床情況，且不得以 AI 內容取代醫療照護提供者（health care provider）的決策。

5. 與教育相關

(1) 《AB 2876 法案》：要求教學品質委員會（Instructional Quality Commission, IQC）考慮將 AI 素養納入數學、科學和歷史及社會科學課程框架及教材中。

(2) 《SB 1288 法案》：要求公共教育總監召集一個工作小組，探討 AI 與其他形式的先進技術在教育中的當前應用。

本次州長就法案之決策，除簽署前述通過之法案外，另否決備受各界關注之《安全與創新之前瞻 AI 模型法案》（SB 1047 法案）。加州州長於否決書中表示，其認同《SB 1047 法案》立意良善，然而《SB 1047 法案》僅依據 AI 模型的成本與規模進行規制，而非依其功能進行監管，且沒有考慮是否係於高風險環境中部署 AI 系統、是否涉及關鍵決策或是否使用敏感資料等問題，導致即使僅執行 AI 模型中最基礎的功能，也需要適用於最嚴格的監管標準。綜上，州長不認為《SB 1047 法案》是保護民眾免受 AI 技術所生之威脅的最佳方法，故予以否決。

資料來源：

1. Governor Gavin Newsom, Governor Newsom announces new initiatives to advance safe and responsible AI, protect Californians, 2024-09-29, https://www.gov.ca.gov/2024/09/29/governor-newsom-announces-new-initiatives-to-advance-safe-and-responsible-ai-protect-californians/ (last visited 2024/10/08)

本報告之智慧財產權歸屬於國發會

2. OFFICE OF THE GOVERNOR, https://s3.documentcloud.org/documents/25178071/sb-1047-veto-message.pdf (last visited 2024/10/08)

(十)2024 年 9 月美國加州州長簽署通過 AB2602 法案、AB 1836 法案，禁止 AI 於未取得同意的情況下，生成「表演藝術者」或「已故表演藝術者」之數位複製品

美國加州州長於 2024 年 9 月 17 日簽署通過 AB2602 法案、AB 1836 法案，禁止 AI 於未取得同意的情況下，生成「表演藝術者」或「已故表演藝術者」之數位複製品（digital replica），以保護表演藝術者免受 AI 生成的數位複製品侵害，兩法案將於 2025 年 1 月 1 日生效。

兩法案均將「數位複製品」定義為「電腦生成、高度真實的電子表現，能夠明顯將其識別為某特定個人之聲音或視覺形象，使該形象出現於錄音、影像、影音作品或電視廣播（transmission），而該個人實際上並未參與或出現，或該個人確實參與或出現，但已大幅改變其表演或外觀的基本特徵。」法案並例示說明，經著作權人授權之以下行為，如將音訊或影音作品的樣本轉化運用於另一個作品；對取得授權的音訊或影音作品進行混音、後期處理或數位修復（digital remastering），不屬於兩法案所稱之數位複製品。

以下分別描述兩法案的特點：

1. AB2602 法案

AB2602 法案係於美國勞動法新增第 927 條，該條規定，個人與他人間之契約為 2025 年 1 月 1 日後簽訂或涉及該個人之數位複製品表現，且符合以下所有條件之契約，不可強制執行。條件如下：

本報告之智慧財產權歸屬於國發會

(1) 契約條款允許他方創造並使用個人的數位複製品，取代個人原本將親自執行的工作。

(2) （A）：除了下述（B）款之例外規定外，該契約條款未包含對數位複製品預期用途的合理具體描述（reasonably specific description）。

（B）：如果數位複製品的用途符合個人或專業服務契約的條款，且符合錄製或表演的攝影作品或音軌的基本特徵，則未包含數位複製品用途的合理具體描述，並不會使該條款不可執行。

(3) 該個人沒有以下之談判代表：

（A）：由代表個人談判其數位複製品授權的法律顧問進行談判，且在由個人簽全名（signed）或簽上縮寫名字（initialed）的契約或其他書面文件中明確地陳述商業條款。

（B）：由該個人從業的工會進行談判，且其集體談判協議（collective bargaining agreement）的條款明確涉及使用數位複製品。

2. AB 1836 法案

AB 1836 法案指出數位複製權屬於財產權，可全部或部分轉讓或繼承。此法案採溯及既往模式，並特別點出「已故表演藝術者」的範圍，應包括但不限於西元 1985 年前逝世之自然人。

3. 違反此法案的原則與例外合規之情形如下：

(1) 原則上，於未經該表演藝術者生前同意或其數位複製權繼承人同意授權的情況下，任何人將已故表演藝術者的姓名、

本報告之智慧財產權歸屬於國發會

聲音、簽名、肖像、照片等形象，用於廣告或銷售或招攬購買產品或服務者，須負損害賠償責任，賠償金額以 1 萬美元或實際損害賠償金額兩者中較高者為準。

(2) 例外無須同意授權之使用情況，例示如下

I. 該使用與任何新聞、公共事務或體育廣播或報導有關。

II. 該使用目的為評論、批評、學術研究、諷刺或戲謔仿作。

III. 該使用系將該個人用於紀錄片或歷史或傳記形式的作品中，包括一定程度的虛構，除非該使用旨於創造，並確實創造出該個人真實參與錄製該作品的錯誤印象。

IV. 該使用時間短暫（fleeting）或偶然發生（incidental）。

V. 將前述 I 至 IV 條款的作品用於廣告或商業公告（commercial announcement）。

AB2602 法案及 AB 1836 法案，分別保障「仍在世的表演藝術者」與「已故表演藝術者」之數位複製品（digital replica）權利，強調 AI 創作數位複製品仍應取得同意授權。

資料來源：

1. California Assembly Bill 1836, 2024-09-17, https://legiscan.com/CA/text/AB1836/id/2884620 (last visited 2024/09/25)

2. California Assembly Bill 2602, 2024-09-17, https://legiscan.com/CA/drafts/AB2602/2023 (last visited 2024/09/26)

3. Tribune, California Governor Gavin Newsom signs bills to protect actors from AI-generated digital replicas, https://tribune.com.pk/story/2497165/california-governor-gavin-newsom-signs-bills-to-protect-actors-from-ai-generated-digital-

本報告之智慧財產權歸屬於國發會

replicas (last visited 2024/09/26)

(十一) 2024 年 9 月美國白宮辦理圓桌會議，邀集 Alphabet、Anthropic、OpenAI 等重要 AI 業者討論建置 AI 基礎設施與相關事宜，以鞏固美國在 AI 領域之領導地位

美國白宮於 9 月 12 日發布新聞，除商務部、能源部與相關顧問、官員出席之外，也邀集 AES、Alphabet、AWS、Anthropic、Cpre Weave、EPRI、Exelon、Microsoft、Meta、Nvidia、OpenAI、QTS 等重要 AI 業者代表，辦理圓桌會議，共同討論建置 AI 基礎設施以維持競爭力之策略，俾利鞏固美國在 AI 領域之領導地位。

該圓桌會議後，白宮宣布相關措施措施，例如：建置資料中心與協調機制、鼓勵各部會與地方政府投入資源等，重點摘要如下：

1. 白宮將新成立 AI 資料中心基礎設施之工作小組（Task Force on AI Datacenter Infrastructure），以協調政府各部會或彼此之間相關政策。該工作小組屬跨部門性質，將由白宮副參謀長辦公室、國家經濟委員會及國家安全委員會主導。

2. 由於設置資料中心須取得許可，聯邦政府將擴大對處理此一許可之各單位，包含聯邦各部會、各州或地方政府，提供必要之技術援助。

3. 美國能源部（Department of Energy, DoE）將建立 AI 資料中心之協助團隊（engagement team），並透過計畫資源，如貸款、補助、稅捐抵免等措施，以協助 AI 資料中心之建置。目標是讓相關業者，在建置 AI 資料中心方面，可以取得潔淨、可靠之能源解決方案。

本報告之智慧財產權歸屬於國發會

4. 能源部也將持續與 AI 資料中心開發商共享資源，並規劃重新利用已關閉之煤礦場。這些已關閉煤礦場之土地將可做為 AI 資料中心之建設基地，並重新為其提供能源及運用既有電網等。

5. 美國陸軍工程兵團（United States Army Corps of Engineers, USACE）也將協助前述許可作業，如協助確認並核發全國性之許可證，以協助符合建置條件之 AI 資料中心加快其許可之審核作業。

6. 參與當日圓桌會議之產業代表，承諾將持續進行對話與公私協作，並加強與政策制定者之合作，以進一步探索相關解決方案。

7. 與會重要 AI 業者代表，在當日圓桌會議也重申渠等對實現淨零碳排與購買潔淨能源，為其 AI 相關業務之營運提供動能之承諾。

拜登政府除於 2023 年 10 月公布開發及使用安全、可靠且可信任之 AI 行政命令外，此一圓桌會議亦為其 AI 政策配套措施之一。

資料來源：

1. The White House, Readout of White House Roundtable on U.S. Leadership in AI Infrastructure, 2024-09-12, https://www.whitehouse.gov/briefing-room/statements-releases/2024/09/12/readout-of-white-house-roundtable-on-u-s-leadership-in-ai-infrastructure/ (last visited 2024/09/25)

(十二) 2024 年 9 月美國勞工部發布《AI 與包容性招聘框架》

美國勞工部於 2024 年 9 月 24 日發布新聞稿，說明「就業與無障礙技術合作夥伴」（Partnership on Employment & Accessible Technology,

本報告之智慧財產權歸屬於國發會

PEAT）發布《AI 與包容性招聘框架》（AI & Inclusive Hiring Framework），該框架目的在透過提升透明度，以協助事業應用 AI 工具進行招聘時，減少 AI 無意中造成的行為或決策歧視（unintentional forms of discrimination），促進身心障礙求職者的就業機會。由美國勞工部下的身心障礙政策辦公室（Office of Disability Employment Policy, ODEP）資助 PEAT 研發此 AI 框架。

當組織評估、收購或部署 AI 招聘技術時，每個區域都包含有關員工及求職者利益最大化與管理風險之資訊。依據美國國家標準與技術研究院的 AI 風險管理框架，《AI 與包容性招聘框架》提出 10 個重點領域包括：

1. 確認就業與身心障礙、隱私法之要求。
2. 考慮組織需要的員工角色，建立員工的職責、培訓員工。
3. 將透過 AI 供應商蒐集有關組織計劃部署 AI 招聘技術的相關資訊，例如與 AI 技術的預期用途、預期優勢、輔助功能一致性狀態、可用性報告、風險分類、部署狀態與範圍的資訊，加入至 AI 系統清單並進行盤點與分類。
4. 制定與第三方合作、控管第三方風險等政策，與負責任的 AI 供應商合作。
5. 評估 AI 招聘可能帶來的積極與消極影響。
6. 為身心障礙者提供便利的求職申請流程。
7. 從 AI 供應商處蒐集可解釋的 AI 的說明及文件，並以明確的文字通知使用者，向使用者描述該 AI 的目的與應用方式。
8. 制定有效的人類監控政策與流程，決定組織內部的關鍵監管人員。

本報告之智慧財產權歸屬於國發會

9. 定義並管理 AI 申訴事件，與內部人員、外部使用者溝通、持續追蹤事件，留存相關紀錄。

10. 定期監控 AI 效能，評估 AI 可信度，決定 AI 技術的配置、維修、逐步汰換及停用。

此框架結合政府、業界及身心障礙倡導者的意見，協助事業在 AI 時代下，採取公平的招聘流程。事業不需要一次施行 AI 和包容性招聘框架的所有內容，可隨組織的 AI 營運發展來逐步推行此框架。

資料來源：

1. DOL, US Department of Labor announces framework to help employers promote inclusive hiring as AI-powered recruitment tools' use grows, 2024-09-24, https://www.dol.gov/newsroom/releases/odep/odep20240924 (last visited 2024/10/04)

2. PEAT, Appendix 2: Ten Focus Areas Mapped to NIST AI RMF, 2024-09-24, https://www.peatworks.org/ai-inclusive-hiring-framework/appendices/practices-by-focus-area/ (last visited 2024/10/04)

3. JD Supra, DOL Issues "AI & Inclusive Hiring Framework" Through Non-Governmental Organization, 2024-09-25, https://www.jdsupra.com/legalnews/dol-issues-ai-inclusive-hiring-2293952/ (last visited 2024/10/04)

(十三) 2024 年 9 月美國國務卿發布《全球 AI 研究進程》 與《全球發展中的 AI 手冊》

2024 年 9 月美國國務卿正式公告《全球 AI 研究進程》 （Global AI Research Agenda, GAIRA）與《全球發展的 AI 手冊》（AI in Global Development Playbook）2 份文件，用以指引 AI 的未來研究方向及其

本報告之智慧財產權歸屬於國發會

在推動聯合國可持續發展目標中的應用。此份文件為 AI 行政命令所規定之應交付成果。

以下分述兩份文件的重點：

1. GAIRA

依據 AI 行政命令第 11 條（c）項（ii）款規定，美國國務院、國際開發總署（U.S. Agency for International Development, USAID）應與能源部、美國國家科學基金會（U.S. National Science Foundation, NSF）及勞工部等跨部會制定 GAIRA。GAIRA 內容應包含原則、指引、優先事項（priorities）及最佳作業流程（best practices）。GAIRA 旨在確保 AI 應用符合安全、負責任、有益且永續發展的目標，以及解決在國際背景下，AI 對勞工市場的影響，包括建議的風險管理措施。

實際上，除前述政府單位，GAIRA 亦與產學界合作，研究人員可以利用 GAIRA 來推動創建安全、可靠與值得信賴的 AI 系統，用以支援「從基礎發現到社會應用」之 AI 生態系統，確保以整個社會公平地分享 AI 優勢的方式開發與實施 AI 技術。

GAIRA 包含 5 個主題：

(1) 社會科技研究（Sociotechnical Research）

當前迫切需要研究來加強對 AI 技術與社會間相互作用的了解，並指導設計與部署能夠提升人類福祉的 AI 系統。應將 AI 系統當作社會科技系統，即技術與人類行為、文化及制度間相互產生影響的系統。在真實世界中，應監控與評估 AI 的開發與部署間的影響，該舉對於辨識 AI 應用的實際優點、風險及保障人權與基本自由，具高度重要性。

本報告之智慧財產權歸屬於國發會

(2) 包容性研究基礎設施（Inclusive Research Infrastructure）

推動 AI 研究進展的一個關鍵要素，是為研究人員提供資料、計算能力與研究平臺的使用機會，並採取適當的措施來保護隱私和國際人權，達到促進創新、高品質的研究以及傳播研究成果。多樣化的觀點將推動重要的發現、應用與議題。

(3) 支持應對全球挑戰的 AI 研究

優先考慮以 AI 應用應對全球挑戰，促進環境管理、經濟韌性與社會福祉。此外，協作努力能使 AI 系統、設備與基礎設施增進可持續性，透過應用研究可推動一個更安全、更健康、更繁榮的世界。

(4) 關於 AI 的基礎研究，包括 AI 的安全性、可靠性與可信賴性

AI 仍處於早期發展階段，還需要更多技術上的進步，才能推動其發展，並實現安全、可靠且可信的系統。為支持這些發展，並為國際 AI 治理之討論提供貢獻，研究人員須解決資訊完整性（information integrity）、網路安全以及測量與評估等相關問題。

(5) AI 對全球勞動市場影響的研究

AI 具自動化流程及提升勞工效率方面的潛力，呼籲研究 AI 對勞動市場的影響。此主題說明填補研究缺口（research gaps）的機會，協助了解勞動力市場的改變，並提出因應全球不同的經濟背景的風險管理措施。研究人員應考慮勞動市場的轉變、新型態工作，以及所得分配不均的影響。

本報告之智慧財產權歸屬於國發會

2. 《全球發展的 AI 手冊》

依 AI 行政命令同款規定，《全球發展的 AI 手冊》為美國國務院、USAID 的成果。研擬《全球發展的 AI 手冊》的合作夥伴包含：總統行政辦公室、美國商務部、國家標準與技術研究院、國家電信暨資訊管理局（National Telecommunications and Information Administration）以及美國專利商標局（United States Patent and Trademark Office）、美國能源部、美國衛生及公眾服務部（U.S. Department of Health and Human Services）以及美國勞工部。

《全球發展的 AI 手冊》為 GAIRA 的補充，旨於指導美國境外與 AI 相關之研究與應用，減少潛在的風險與挑戰。

《全球發展的 AI 手冊》包含 8 個重點：

(1) 增進能力，在各領域、各種程度推廣與 AI 相關之技能，並保障勞動力。

(2) 建構可信賴且可持續的數位基礎設施。

(3) 擴大可取得（Access）之資料存儲與計算資源（Compute Resource）。

(4) 建立具代表性、與當地相關之資料集（Locally Relevant Datasets），並保護文化遺產。

(5) 制定策略以履行對於「應用 AI」（AI in Practice）的承諾。

(6) 為發展及使用安全且尊重權利（Rights-Respecting）的 AI 系統，推動良好的治理框架。

(7) 透過開放性、透明度與可解釋性，培養對 AI 的信任。

(8) 可永續部署 AI，並促進氣候行動（Climate Action）。

本報告之智慧財產權歸屬於國發會

資料來源：

1. U.S. Department of State, Global AI Research Agenda, 2024-09-24, https://www.state.gov/global-ai-research-agenda/ (last visited 2024/10/07)
2. Global AI Research Agenda, 2024-09-24, https://www.state.gov/wp-content/uploads/2024/09/Global_AI_Research_Agenda.pdf (last visited 2024/10/07)
3. United States Agency for International Development, AI in Global Development Playbook, https://www.usaid.gov/digital-development/ai-global-development-playbook (last visited 2024/10/07)
4. Federal Register, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 2023-11-01, https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence (last visited 2024/10/07)

二、英國

(一)2024 年 9 月英國簽署《AI 與人權、民主與法治框架公約》

英國大法官 Shabana Mahmood 於 2024 年 9 月 5 日簽署歐洲理事會《AI 與人權、民主與法治框架公約》（Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law，下稱框架公約），進一步保障人權（Human rights）、民主（democracy）及法治（the rule of law），免受 AI 的潛在威脅。又該公約將確保各國對 AI 之監管，並控制相關技術於一定範圍內之發展，要求各國採取行動，打擊超出範圍之相關作為，以解決 AI 的濫用問題。一旦英國批准並生效框架公約，將強化現有法律及措施。以下簡要敘述框架公約之內容：

本報告之智慧財產權歸屬於國發會

1. 協議之三項總體保障措施

(1) 保障人權，確保人民的資料被適當使用、尊重隱私以及 AI 不會產生對人民之歧視。

(2) 維護民主，確保各國採取適切之措施以防止公共機構與程序受到破壞。

(3) 保護法治，簽署國負有監管 AI，防範特定風險之責任，並須保護其人民免受潛在危害，確保其 AI 使用之安全。

2. 締約方應實施之七項共通原則（公約第 3 章）

(1) 人性尊嚴及個人自主權（Human Dignity and Individual Autonomy）

各締約方應採取相關措施，避免於 AI 系統生命週期內之活動侵害人性尊嚴及個人自主權。

(2) 透明度及監督（Transparency and Oversight）

各締約方皆應採取或維持相當措施，以確保針對特定情境及風險之透明度及監督要求得於 AI 生命週期間適當落實，包括識別 AI 系統生成之內容。

(3) 當責（Accountability）與負責（Responsibility）

各締約方應採取或維持措施，確保對 AI 系統生命週期內的活動對人權、民主及法治所造成之不利影響得以負擔責任。

(4) 平等與非歧視（Equality and Non-Discrimination）

各締約方應採取或維持措施，以確保 AI 系統生命週期內的活動遵循國際及國內法規範，包括性別平等及禁止

本報告之智慧財產權歸屬於國發會

歧視之規則；承諾根據其適用的國內及國際人權義務，在 AI 系統生命週期內的活動中採取或維持「旨在克服不平等的現象之措施」，以實現公平、公正及公平。

(5) 隱私及個人資料保護(Privacy and Personal Data Protection）

各締約方應採取或維持措施，確保就 AI 系統生命週期內的活動，個人及其個人資料的隱私權受到保護，包括透過適用之國內及國際法律、標準與框架；根據適用的國內及國際法律義務，為個人提供有效的保障等。

(6) 可靠性（Reliability）

各締約方應視情況採取措施，提升 AI 系統的可靠性及輸出的可信賴性，包括對 AI 系統整個生命週期的品質、安全之相關的要求等。

(7) 安全創新（Safe Innovation）

為了促進創新，且避免對人權、民主及法治產生不利影響，呼籲各締約方於主管機關的監督下，視情況為開發、試驗與測試 AI 系統建立安全環境。

綜合以上，該條約旨在促進 AI 安全國際合作及標準化，設定每個締約方皆需遵守之基準，以確保 AI 系統整個生命週期內的活動充分符合人權、民主及法治。

資料來源：

1. GOV.UK, UK signs first international treaty addressing risks of artificial intelligence , 2024-09-05, https://www.gov.uk/government/news/uk-signs-first-international-treaty-addressing-risks-of-artificial-intelligence (last visited 2024/10/02)
2. JD Supra, UK signs first treaty on AI and human rights, democracy

本報告之智慧財產權歸屬於國發會

and the rule of law , 2024-09-19, https://www.jdsupra.com/legalnews/uk-signs-first-treaty-on-ai-and-human-9293138/ (last visited 2024/10/02)

3. Cleary AI and Technology Insights , 2024-09-19, https://www.clearyiptechinsights.com/2024/09/the-eu-uk-and-us-sign-international-treaty-addressing-risks-of-ai/?__cf_chl_rt_tk=PPNocDsX53U8SKq5.zQ19UW8j3NSVPoxEqhCo.D3PQw-1727265545-0.0.1.1-4991 (last visited 2024/10/02)

三、日本

(一)2024 年 7 月日本文化廳發布《AI 與著作權檢視清單及指引》，有助於減少生成式 AI 產生的著作權風險，並協助著作權人保護及行使權利

日本文化廳為降低生成式 AI 所產生的著作權風險，保護並行使著作權人權利，於 2024 年 7 月以文化廳 3 月發布的《AI 與著作權的思考》、內閣府 5 月發布的《AI 時代智慧財產權研究小組中期報告》，以及總務省及經濟產業省 4 月份發布的《AI 事業指引（1.0 版）》之資料為基礎，發布《AI 著作權檢視清單及指引》(AI と著作権に関するチェックリスト＆ガイダンス)》。

該指引主要分成兩部分，第一部分是「AI 開發、提供及使用檢視清單」，第二部分是「權利持有人指引」。在第一部分中依循總務省及經濟產業省 4 月份發布的《AI 事業指引（1.0 版）》之區分方式，分為「AI 開發者」、「AI 提供者」、「AI(業務)使用者(事業利用人)」與「業務外利用者（一般利用人）」四類利害關係人，依不同之身分別說明如何降低 AI 開發前後之資料處理等智慧財產權侵權風險的相關措施，以及提供與使用 AI 服務時，如何安全、適當地使用 AI 技術。第二部分則針對著作權持有人，以及根據著作權法享有權利之其他權利持有

本報告之智慧財產權歸屬於國發會

人(例如表演人)的權益保護，從權利人的角度，提供如何保護自身權益之指引。

該指引第一部分，主要提及建議開發者應於開發前選擇訓練資料時，應避免所選資料出自盜版資料庫，並須確保學習模型不會直接輸出學習資料中的著作物；開發中須採用可行技術避免智慧財產權之侵權風險；開發後須向 AI 用戶提供關於學習資料內容之資訊、採取防止模型侵權之措施、並廣泛提供關於生成式 AI 機制、技術概要、運作機制等相關資訊。對於 AI 提供者，建議在提供 AI 系統及服務時，訂定適當之使用條款、說明使用什麼樣的訓練資料、學習模式及方法等，以及採取什麼措施來防止生成類似內容。對事業利用人而言，應注意生成結果的正確、安全且無侵權風險、應取得授權的情況、使用前進行近似確認、留存過程中的輸入提供資料、對外適度揭露 AI 的使用等事宜。對一般利用人的提醒，則與業務利用人雷同，惟特別就個人使用部分，提示應確認其使用是否係於可合法使用的權利限制範圍內。

而指引第二部分則定位為權利人應知悉之內容，對於著作權人、表演者等享有著作權法相關權利之權利人，由四個面向切入說明，以協助權利人了解其可採取相關措施保護其權利並獲取適切之補償。包括：應了解的與 AI 使用行為有關的著作權知識、如何應對與自己作品相似的 AI 產出、如何因應自己之作品被用於 AI 學習、以及面對著作權侵害之應對與諮詢窗口之利用。首先著作權知識部分，主要說明生成式 AI 的開發、提供及利用過程會發生哪些著作利用行為；其次，說明近似性之判斷要件、證明、防止與賠償等可主張的法律上請求、可主張侵權之對象、權利主張的限制；於事先或發現後可採取防止 AI 侵權之相關可能措施；最後就侵權因應層面，建議權利人可發出著作權侵權警告、進行訴訟、調解等糾紛解決，並提供可用的法律諮詢窗口資訊。

資料來源：

本報告之智慧財產權歸屬於國發會

1. 文化庁著作権課，AI と著作権に関するチェックリスト＆ガイダンス, 令和 6 年 7 月 31 日, https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/seisaku/r06_02/pdf/94089701_05.pdf (last visited 2024/08/19)

2. 文化庁、「AI と著作権に関するチェックリスト＆ガイダンス」を公開, 2024-08-14, https://jipsti.jst.go.jp/sti_updates/2024/08/15134.html (last visited 2024/08/19)

四、 韓國

(一)2024 年 7 月韓國的數位平臺政府委員會、科學技術情報通訊部及情報化振興院宣布啟動「2024 年基於 AI 之超大規模公共服務開發計畫」

2024 年 7 月 15 日，韓國數位平臺政府委員會（Presidential Committee on the Digital Platform Government, DPG）、科學技術情報通訊部（Ministry of Science and ICT，下稱韓國科技部）及情報化振興院（National Information Society Agency, NIA）宣布啟動「2024 年基於 AI 之超大規模公共服務開發計畫」。此計畫選定 8 個 AI 應用主題，並將 8 個主題分為 3 類型：通用目的公共服務（general purpose public services）；專業服務（specialized services）；以及目的在解決社會問題之服務（services that aim to solve social problems）。以下依 3 類型分別說明 8 個 AI 應用主題及對該 8 個主題有應用需求的 8 個部會、機構。

1. 通用目的公共服務

(1) 以大規模 AI 為基礎，綜整研發支援服務（Hypers cale AI-Based Integrated R&D Support Service）

韓國國家經濟、人文與社會科學研究會（National Research. Council for Economics , Humanities and Social

本報告之智慧財產權歸屬於國發會

Sciences)希望透過 AI 達到擇定研究主題、總結現有研究、管理研究筆記，並提高研究成果的品質。

(2) 智慧消防安全服務

韓國首爾市消防災害本部（Seoul Metropolitan Fire and Disaster Headquarters）希望透過具專業知識的 AI 協助消防員分析建築圖、提高工作效率。

(3) 以生成式 AI 提供國防設施結構的行政支援（Generative AI-Based Administration Support for Defense Facilities Construction）

韓國國防部希望 AI 為國防設施管理者提供從需求機構至授權核准、再至營運及維護的各階段的施工管理與民事請願書（civil petition）資訊。

2. 專業服務

(1) AI 勞動監督支援服務

韓國就業及勞動部（Ministry of Employment and Labor）為確保弱勢勞工權益，希望 AI 透過如自動化準備及分析報告、案例搜尋、24 小時全天勞動法諮詢服務等方式輔助勞動監督官（labor inspectors）。

(2) 青年農民專業服務

韓國農村振興廳（Rural Development Administration, RDA）為透過穩定青年農民返鄉、振興農村，希望透過 AI 為青年農民提供最新的農業技術、個人化的教育建議以及從準備到生長階段的農業設計（farming design）。

本報告之智慧財產權歸屬於國發會

(3) 以超大規模 AI 為基礎的專利審查支援服務（Hyper-scale AI-Based Patent Examination Support Service）

韓國特許廳（Korean Intellectual Property Office）希望透過 AI 強化專利審查準確率、提供相似的專利檢索，並提供摘要意見，以縮短專利審查官的決策時間。

3. 目的在解決社會問題之服務

(1) 以超大規模的多模態基礎模型 AI 支援身心障礙者服務（Hyper-scale AI Multi-Modal Service to Support Communication of the Disabled）

身心障礙者學校等組織希望透過 AI 分析臉部表情、唇形、身體動作及聲音，促進與身心障礙者間的溝通，減少家庭、監護人的照護負擔。

(2) 運用大規模 AI，為學習遲緩者進行早期檢測支援服務（Early Detection Support Service for Slow Learners Using Hyper-scale AI）

韓國全南國立大學兒童醫院希望透過 AI 分析兒童的言語、動作，及早發現輕微智能障礙兒童，減輕公眾的育兒負擔。

韓國科技部部長表示，希望此計畫能積極地將超大規模 AI 模式融入公共部門，並增強韓國應用國產 AI 技術的能力，推動韓國成為全球 AI 前三強國（AI G3）之一。

資料來源：

1. MSIT, Hyper-scale AI Services to be Developed in Eight Key Public Service Areas, 2024-07-16, https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=1015&searchOpt=AL

本報告之智慧財產權歸屬於國發會

L&searchTxt= (last visited 2024/08/30)

(二)2024 年 7 月韓國發布《AI 開發與服務處理開放資料指引》

2024 年 7 月 18 日韓國個資保護委員會（Personal Information Protection Commission, PIPC）發布《AI（AI） 開發與服務處理開放資料指引》（Guideline on Processing Publicly Available Data for AI Development and Services，下稱指引）。由於生成式 AI 可利用 Common Crawl、維基百科等多個公開來源，透過抓取頁面內容之技術，將網頁上之公開資料作為其訓練資料。而這些於開放網路之資料可能包含個資當事人之地址、唯一可識別資訊（unique identifiable information, UII）、信用卡號等個資。然而目前韓國《個人資料保護法》（Personal Information Protection Act，下稱韓國個資法）欠缺處理公開之個人資料的法律依據與法律明確性，故此指引提供 AI 開發人員與服務提供者蒐集、使用公開之個人資料的指導，旨於消除法律不確定性、保護人民隱私，並以推動 AI 時代的創新成長為目標。為從 AI 創新與安全取得平衡，歐美等主要國家的個資主管機關（Data protection authorities）亦正制定處理 AI 等領域之公開資料相關隱私規範及標準，PIPC 欲建立國際可互通之標準。

指引主要可分為三大部分，第一部分為「合法利益概念之適用（Applying the Concept of Legitimate Interests）」；第二部分為「建議的安全措施及保障個資當事人權利之方法（Suggesting Applicable Guardrails and Ways to Safeguard Data Subjects’ Rights）」；及第三部分為「促進開發 AI 產品或服務之事業，得致力於開發、使用具可信任性的 AI（Fostering the Roles of AI Businesses for the Development and Usage of Trustworthy AI）」。

1. 合法利益概念之適用

本報告之智慧財產權歸屬於國發會

指引明確指陳韓國個資法第 15 條關於合法利益之規定。利用、蒐集公開可用資料必須屬於該法中所規範之合法利益，利用公開資料進行 AI 培訓及 AI 服務之開發亦屬該法所訂之合法利益。AI 系統開發以及服務提供者要適用並符合合法利益之概念，必須達成目的正當性、資料處理必要性以及對個人資料處理者與當事人間風險評估之三項要件。

(1) 目的正當性（Legitimacy of the purpose）

依據所指定開發 AI 模型之目的，資料處理者須確保其有合法事由處理個人資料，例如開發大型語言模型（LLMs）或其他 AI 模型的目的為支援醫療診斷而開發、進行信用評級、或進行生成/分類或翻譯等不同目的之模型開發。

(2) 資料處理的必要性

確保所蒐集和利用的公開資料是必要、充分且適當的，例如用於開發支持醫療診斷的 AI 模型，可以排除個人收入、財產等與模型不相關資料。

(3) 個資處理者與個資當事人間的風險評估

確保個人資料處理者之合法利益明顯高於個資當事人的權利以符合前開韓國個資法第 15 條第 6 款，以合法利益所必須作為可蒐集利用個人資料之法律基礎。並為避免侵害個資當事人的權利，採取適當之安全措施。

2. 建議的安全措施及保障個資當事人權利的方法

以下分為「技術防護措施（Technical safeguards）」、「管理與組織防護措施（Administrative and Organizational Safeguards）」及「尊重個資當事人的權利」說明。

本報告之智慧財產權歸屬於國發會

(1) 技術防護措施，包含：檢查訓練資料集來源；採取措施預防個資洩露（例如刪除或去識別化）；安全儲存及管理個資；透過 AI 深度學習的微調（fine-tuning）增加額外保障；應用提示（prompt）及輸出內容過濾（output filtering）功能；從訓練資料中移除該訓練資料點的影響，即機器學習遺忘（Machine Unlearning）。

(2) 管理與組織防護措施，包含：制定蒐集及使用訓練資料的標準，並將其合併至隱私權政策；考慮進行隱私衝擊影響評估（PIA）；組織 AI 隱私紅隊；實施針對 AI 模型量身打造的保障措施，開發及部署 AI 服務（例如開放原始碼、API）。

(3) 尊重個資當事人的權利，包含：將公開資料蒐集情形及主要來源納入隱私政策等文件；保障個資當事人的權利，例如 AI 訓練或部署 AI 服務的過程中，針對資料外洩事件，使當事人可行使其刪除（erasure）及停止利用（suspension）的權利。

韓國個資保護委員會允許 AI 業者不需要實施指引所規定的每項安全措施，而應考量其 AI 的預期功能與影響，例如效能退化（performance degradation）或偏差，以及 AI 技術的成熟度等條件，選擇最合適的安全措施。指引中詳細介紹主要大型語言模型供應商於 2024 年 3 月所採取的技術與管理防護措施，以協助其他事業找到合適的措施組合，並從結果得出建議事業從 AI 訓練資料集刪除 URL。

3. 促進開發 AI 產品或服務的事業，致力於開發、使用具可信任性的 AI

指引建議 AI 驅動的事業自願透過培養首席隱私長的方式，管理專門的 AI 隱私團隊，評估指引的要求。此外，指引

本報告之智慧財產權歸屬於國發會

亦呼籲事業定期監控技術重大變化及資料外洩風險，並建議事業儘速制定及實施補救措施。

為配合韓國個資法修法、AI 技術進步及國際個資主管機關的革新，指引將持續更新。韓國個資保護委員會計劃透過事前適足性審查（Adequacy Review）制、監理沙盒、個資安全區域（Safety Zone）等方式與 AI 驅動的事業持續溝通，以密切關注技術進步及市場情況。參考最佳實踐與經驗，韓國個資保護委員會將順應 AI 時代修訂韓國個資法。

資料來源：

1. Personal Information Protection Commission, PIPC Offers Guideline on Processing Publicly Available Data for AI Development and Services, 2024-07-18, https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=2591 (last visited 2024/09/05)
2. 개인정보보호위원회, 지침(가이드라인), 2024-07-19, https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS217&mCode=G010030000&nttId=10375#LINK (last visited 2024/09/05)

(三)2024 年 9 月韓國政府宣布成立國家 AI 委員會，並宣布 AI 戰略政策方向與執行措施

2024 年 7 月 30 日，韓國科技部部長宣布內閣會議核准「關於建立與營運國家 AI 委員會的總統令提案（下稱總統令）」。韓國科技部依據此總統令於 9 月 26 日發布新聞稿，宣布正式成立國家 AI 委員會(국가 AI 위원회)，並於當日召開第一屆委員會會議。會後由主席尹錫悅

本報告之智慧財產權歸屬於國發會

總統發表國家 AI 戰略政策方向（국가 AI 전략 정책방향），希望成為世界 3 大 AI 強國（AI G3，包含美國、中國大陸及韓國）之一。

韓國將 AI 及半導體領域認定為影響國家將來競爭力遊戲規則的核心之一。委員會欲以公私協力之治理框架，在全球 AI 競賽中爭奪技術主導地位。

依據總統令，委員會之組成大致如下：

1. 委員會之成員結構

委員會由最多 45 名公私部門成員所組成，包括 1 名主席和 1 名副主席。由總統擔任委員會主席，確保全國一致努力。

政府單位之成員，包括：經濟暨財政部長、教育部長、科技部長、外交部長、行政安全部長、文化體育觀光部長、產業通商資源部長、通訊委員會主席、個資保護委員會主席、數位平臺政府委員會主席等。

私部門之成員，為經總統提名之 AI 相關領域（如技術、經濟、人文與社會）具有廣泛專業知識與經驗的個人，將從私部門成員中選出副主席。提名成員的任期為 2 年。

2. 委員會之職能

委員會將審查與協調國家 AI 總體政策，包括：主要的 AI 相關政策；研究、開發及投資策略；擴展資料中心等基礎設施；確認（Identification）並改進（improvement）法規；宣傳（Dissemination）AI 倫理原則；如何因應 AI 發展所帶來的教育、勞工及經濟等領域變動。

3. 委員會活動的支援

本報告之智慧財產權歸屬於國發會

將成立 1 個由私部門專家與相關公務人員組成的支援小組，以協助委員會的活動與運作。

目前韓國透過公私協力推動 4 大 AI 旗艦計畫。具體政策內容包含：

1. 擴大國家 AI 運算基礎設施：如建立國家 AI 運算中心，增加圖形處理器(Graphics Processing Unit, GPU)數量至 15 倍以上，並支持國產 AI 半導體之商業化，甚至創建生態系等。因與世界其他大型科技公司相比，韓國之產業界與學術界，仍然欠缺 AI 運算基礎設施，且相關設施為 AI 競爭力之基礎，故規劃成立國家 AI 運算中心，並推動對 AI 運算基礎設施之持續投資。

2. 拓展民間投入 AI：因與主要國家相比，韓國民間對 AI 投資不足。故擬透過政府投資，引領私人共同投資 AI 領域之技術、人才及運算基礎設施，預計 2024 至 2027 年達 65 兆韓元以上。此外，韓國政府預計在審查相關稅賦時給予優惠，或提供政策融資，甚至設立大規模基金以利投資 AI 相關領域。

3. 實現綜合型國家 AI+X：除了在特定領域內運用 AI 外，韓國政府規劃全面性推動 AI 協助大規模變革，如運用於產業、社會、區域發展或國防領域，以促進國家之 AI 轉型。舉例而言，針對製造業、金融、醫療、生物科技等 8 項產業，將建立並推廣 AI+X 措施，如加強運用 AI 能力於安全、防災。預計到 2030 年實現產業界 70%之 AI 採用率、公共服務 95%之 AI 採用率，並將創造出 310 兆韓元以上之經濟效益。

4. 確保 AI 安全、保障及全球領導力：2024 年 11 月將成立 AI 安全研究所（AI 안전연구소），以因應日益增加之 AI 風險。並

本報告之智慧財產權歸屬於國發會

將於年底提出 AI 基本法（AI 기본법），以實現 AI 技術研發、安全及信任之均衡發展。相關措施將以確保 AI 安全與保障能力，並實現全球 AI 治理為主。

為達成前述 4 項目標，韓國政府預計搭配相關措施，以利該 AI 政策之執行，包含：

1. 新創事業與人才增加，如至 2030 年時培養出 10 家 AI 獨角獸事業，及 20 萬名 AI 人才。
2. 技術與基礎設施創新，如建立 AI 與半導體聯合研究基地，並擴大國際合作。
3. 建立包容、公平之基礎，如訂定數位包容法（디지털포용법），讓所有人都可以享用 AI 帶來的好處。
4. 確保全球領導地位，如確認 AI 責任、權利歸屬等基本原則，並透過國際交流、引領 AI 治理之討論。

資料來源：

1. MSIT, Government and Private Sector Unite to Elevate Nation to AI G3 Status, 2024-07-30, https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=1025&searchOpt=ALL&searchTxt= (last visited 2024/09/06)
2. KOREA.net, President pledges KRW 9.4T investment in AI, chips by 2027, 2024-04-11, https://www.korea.net/NewsFocus/policies/view?articleId=249796 (last visited 2024/09/06)
3. 과기정통부（Ministry of Science and ICT）, 국가인공지능 전략 정책방향, 2024-09-26,

本報告之智慧財產權歸屬於國發會

https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=238&pageIndex=3&bbsSeqNo=94&nttSeqNo=3184952&searchOpt=ALL&searchTxt= (last visited 2024/10/09)

五、 澳洲

(一)2024 年 9 月澳洲《政府負責任地使用 AI 的政策》正式生效

2024 年 9 月 1 日，澳洲《政府負責任地使用 AI 的政策》（Policy for the responsible use of AI in government）正式生效。此政策係由 2016 年成立之澳洲數位轉型局（Digital Transformation Agency, DTA）所提出，旨在透過提升透明度、治理及風險之保障，增強公眾對政府應用 AI 的信任。

《政府負責任地使用 AI 的政策》採用經濟合作暨發展組織（OECD）對 AI 之定義：AI 系統是一種基於機器設備，從系統接收的資訊進而產出預測、建議及決策之內容。

1. 《政府負責任地使用 AI 的政策》之適用範圍

(1) 《政府負責任地使用 AI 的政策》適用於所有「非事業的聯邦實體（non-Corporate Commonwealth entities, NCE）」，非事業的聯邦實體指在法律、財務上為聯邦政府的一部分，須向議會負責。此政策亦鼓勵「事業之聯邦實體」適用此政策。

(2) 此政策不適用於國家情報體系（national intelligence community, NIC）之 AI 運用。而所謂 NIC，主要係依據 2018 年國家情報辦公室法（Office of National Intelligence Act 2018）第 4 條之規定，包括但不限於：國家情報辦公室（Office of National, ONI）、澳洲國防部通訊局（Australian Signals Directorate, ASD）、澳洲安全情報組織（Australian

本報告之智慧財產權歸屬於國發會

Security Intelligence Organisation, AISO）等情報相關單位。但國防部、國家情報體系可以在不損害國家安全保障之能力或利益之情況下，自願採用此政策之內容。

2. 適用《政府負責任地使用 AI 的政策》之機構，須滿足下列 2 要求

(1) 須公布透明度聲明

各機構須在《政府負責任地使用 AI 的政策》生效日起的 6 個月內（即 2025 年 2 月 28 日前）公開發布透明度聲明，概述其應用 AI 之方式。

(2) 須提出權責人員（accountable official）名單

各機構須在政策生效之日起 90 天內（即 2024 年 11 月 30 日前）將權責人員名單提供給數位轉型局。權責人員可由一人擔任或由多人分工，如有人員異動，應通知數位轉型局。

所謂權責人員的職責範圍，主要分為 5 點，包含：

I. 負責在其機構內落實此政策

權責人員應制定政策實施計畫，調整並提升其機構所採取之 AI 治理機制；定期審查、控管政策落實情況，並向數位轉型局回報；促進其機構參與跨政府協作；鼓勵機構為所有員工執行 AI 基礎知識教育訓練，並依業務範圍進行額外培訓，例如：負責採購、開發、訓練及部署 AI 系統的人員。

II. 負責通知數位轉型局，該機構所認定之高風險 AI 應用案例

本報告之智慧財產權歸屬於國發會

政策未要求權責人員負責處理高風險 AI 應用案例，但機構可自行決定是否對權責人員施加額外責任。

當既有 AI 應用案例被評估為高風險時，所提供之資訊應包括：AI 的類型、預期的 AI 應用、該機構得出「高風險」評估的原因，以及其他任何敏感性資訊（any sensitivities）。

III. 成為機構內部協調 AI 的聯絡窗口。

IV. 權責人員應參與或指派代表參與 AI 議題之政策一體性會議（whole-of-government forums）。

V. 了解隨著技術、需求而隨時更動之相關政策，並讓機構內的利害關係人知道政策之影響。

資料來源：

1. Digital Transformation Agency, Responsible choices: a new policy for using AI in the Australian Government, 2024-08-16, https://www.dta.gov.au/blogs/responsible-choices-new-policy-using-ai-australian-government (last visited 2024/08/27)
2. Digital.gov.au, Artificial intelligence in government, 2024-08-16, https:// (last visited 2024/08/27)
3. Australian Government Department of Finance, Non-corporate Commonwealth entity (NCE), 2021-07-16, https://www.finance.gov.au/about-us/glossary/pgpa/term-non-corporate-commonwealth-entity-nce (last visited 2024/08/29)

六、 中國大陸

(一)2024 年 8 月香港金融管理局訂定《應用生成式 AI 的消費者保護指引》

本報告之智慧財產權歸屬於國發會

香港金融管理局（Hong Kong Monetary Authority, HKMA）有鑑於銀行業漸漸擴大其業務中應用 GenAI 技術之範圍，將對消費者保障產生影響，於 2024 年 8 月 20 日公布《生成式 AI 消費者保護指引》。該指引就2019 年 11 月 5 日「認可機構就應用巨量資料分析及 AI（BDAI）的消費者保障」通告中，金融管理局所提出指導原則之四大範疇（管制與問責、公平性、透明度與揭露，以及資料私隱與保障），增定下述原則，旨在確保金融機構在採用會接觸客戶之 GenAI 應用時，應已採取適當的保障措施，以保障消費者的安全，以下簡要敘述增訂保障要求之重點：

1. 管制與問責

認可機構董事局及高級管理層須對所有以 GenAI 推動的決定及程序負責，並在認可機構的管治、監察及問責架構下，通過適當的委員會，全面考慮 GenAI 應用程式對客戶的潛在影響。

(1) 清楚界定面對客戶之 GenAI 應用程式的涵蓋範圍，使 GenAI 不會被應用於非預定之環節。

(2) 以負責任方式使用接觸客戶的 GenAI 應用程式，制定妥善政策與程序以及相關管控措施。

(3) 在使用接觸客戶的 GenAI 應用程式的早期階段，認可機構應適當核實 GenAI 模型，特別是應採用「人在環中」方式，即在決策過程中保留人類控制權，確保模型生成的結果準確可靠，不會有所偏頗。

2. 公平性

認可機構應確保 GenAI 模型能為客戶提供客觀、一致、秉持道德操守及公平的結果。

本報告之智慧財產權歸屬於國發會

(1) 模型產生的結果不會對任何客戶或客戶群組造成不公平的偏見或不利影響，認可機構應考慮在 GenAI 模型中可採用的不同方法，例如把某些類別的資料匿名化、運用能全面及持平地代表相關總體的資料集、在核實及檢視過程中作出調整以消除偏見（例如採用「人在環中」方式）等。

(2) 在使用接觸客戶的 GenAI 應用程式的早期階段，認可機構應向客戶提供退出使用 GenAI 的選項，並在客戶的要求下，盡可能對 GenAI 產生的決定作出人為干預，若基於某些原因無法提供退出使用 GenAI 的選項，認可機構應提供相關管道，讓客戶要求檢視 GenAI 產生的決定，並隨著科技的不斷發展，能夠設計出退出使用 GenAI 的選項。

3. 透明度與揭露

認可機構應以妥善、準確及易於理解的方式向客戶揭露，就 GenAI 應用程式提供予客戶適當的透明度，因此，認可機構應向客戶揭露其 GenAI 的應用，當中包括向客戶說明應用 GenAI 模型的用途與目的，以及有關模型的限制，促進客戶對模型產生的結果的了解。

4. 資料隱私與保障

認可機構應實施有效的客戶資料保障措施，若 GenAI 應用程式涉及蒐集及處理個人資料，認可機構應遵守《個人資料（私隱）條例》及參考個人資料私隱專員公署就 GenAI 發出的相關建議及良好行事方式。

資料來源：

1. 香港金融監理管理局，消費者保障，2024-08-19，https://www.hkma.gov.hk/media/chi/doc/key-information/guidelines-and-circular/2024/20240819c1.pdf （最後瀏覽日：2024/10/14）

本報告之智慧財產權歸屬於國發會

(二)2024 年 9 月中國大陸發布《人工智能安全治理框架》1.0 版

中國大陸全國網路安全標準化技術委員會為了貫徹落實《全球 AI 治理倡議》，於 2024 年 9 月 9 日發布《人工智能安全治理框架》1.0 版，以鼓勵 AI 創新發展，有效防範及化解 AI 之安全風險。其按照風險管理的理念，緊密結合 AI 技術特性，分析 AI 風險來源及表現形式，針對模型演算法之安全、資料安全及系統安全等安全風險與網路領域、現實領域、認知領域、倫理領域等應用安全風險，提出相應技術應對及綜合防治措施。同時提出 AI 安全開發應用指引，相關原則包括：「包容審慎、確保安全」、「風險導向、敏捷治理」、「技管結合、協同應對」、「開放合作、共治共用」等 AI 安全治理的原則，以下簡要敘述治理框架之原則：

1. 包容審慎、確保安全

   鼓勵發展創新，對 AI 研發及應用採取包容態度，嚴守安全底線，對危害國家安全、社會公共利益、人民權利的風險及時採取措施。

2. 風險導向、敏捷治理

   密切關注 AI 研發及應用趨勢，從 AI 技術自身、應用兩方面分析梳理安全風險，提出針對性防範應對措施，關注安全風險發展變化，快速調整治理措施，持續優化治理機制及方式，對所需政府監管事項及時予以回應。

3. 技管結合、協同應對

   面對 AI 研發應用之過程，結合技術、管理的安全治理措施，防範應對不同類型之安全風險，圍繞 AI 研發應用生態系，明確定義模型演算法之研發者、服務提供者、使用者等相關主體的安全責任，有效發揮政府監管、行業自律、社會監督等治理機制之作用。

本報告之智慧財產權歸屬於國發會

4. 開放合作、共治共用

在全球範圍推動 AI 安全治理國際合作，共享實踐經驗，提倡建立開放平臺，透過跨學科、跨領域、跨地區、跨國界的對話及合作，推動形成具有廣泛共識的全球 AI 治理體系。

綜上所述，該框架對促進社會各方積極參與、推進 AI 安全治理具有重要作用，為培育安全、可靠、公平、透明的 AI 技術研發及應用生態，促進 AI 的健康發展，提供基礎性、框架性之技術指引。

資料來源：

1. 全國網路安全標準化技術委員會，《人工智能安全治理框架》1.0 版，2024-09-09，https://www.tc260.org.cn/front/postDetail.html?id=20240909102807（最後瀏覽日：2024/09/21）

參、 數位政策

一、 美國

(一)2024 年 8 月美國白宮發布新聞，說明與新加坡間之第 2 次關鍵與新興技術會談成果，雙方將在 6 項關鍵與新興技術領域持續深化合作

美國與新加坡前於 2023 年 10 月辦理第 1 次關鍵與新興技術會談（U.S.-Singapore Critical and Emerging Technology Dialogue），雙方同意共同合作建立可信賴、開放、方便近用及安全之技術生態系，以促進負責任之創新、具包容性、永續之經濟成長，以及遵守既有規範之國際秩序。

在前述基礎上，美國白宮於 2024 年 8 月 1 日發布新聞，說明第 2 次關鍵與新興技術會談成果。雙方將在 6 項關鍵與新興技術（Critical

本報告之智慧財產權歸屬於國發會

and Emerging Technology, CET）領域持續深化合作，包含 AI、數位經濟與治理等，分別摘要重點說明如後。

1. AI（Artificial Intelligence, AI）

雙方同意擴大美國國家標準與技術研究院（NIST）與新加坡資訊通信媒體發展局（Infocomm Media Development Authority, IMDA）各自於 AI 治理與風險管理架構內，將生成式 AI 納入相關架構之範圍。且將於測試與評估 AI 方面進行合作，如研議紅隊指引等參考文件。

2. 數位經濟與資料治理（Digital Economy and Data Governance）

雙方將持續支援可信任之資料流動（trusted flows of data），例如：促進參與跨境隱私規則（Cross-Border Privacy Rules）與相關活動。且 NIST 與 IMDA 亦將透過技術強化可信任之資料流動，以提高隱私強化技術（privacy-enhancing technologies）之採用、推動標準化及相關成熟度等。

3. 生物科技（Biotechnology）

2024 年 6 月，新加坡科技研究局（Singapore’s Agency for Science, Technology, and Research）與美國能源部轄下之聯合基因研究所（the U.S. Department of Energy’s Joint Genome Institute）已簽署合作備忘錄，雙方同意將進行微生物基因與天然合成物之研究，亦將透過共同舉辦研討會或論壇等方式，持續合作。

4. 關鍵基礎設施與技術供應鏈（Critical Infrastructure and Technology Supply Chains）

雙方將共同參與 5G、開放式無線接取網路（Open Radio Access Network, RAN）及新一代通訊網路等連結技術之合作。

本報告之智慧財產權歸屬於國發會

並將與東協（ASEAN）成員國，共同探討安全、具韌性之海底電纜等議題。

5. 國防創新（Defense Innovation）

雙方之國防部已於 2024 年 5 月簽署合作備忘錄，並將在海上安全、反無人機系統之領域，優先進行相關合作。

6. 量子資訊科技（Quantum Information Science and Technology）

雙方將就量子安全遷移（quantum safe migration）進行合作與交流，例如：後量子密碼學之發展、標準化與遷移相關議題。且就各自之國家級計畫內，擴大量子通訊、運算等產業、研究及人才交流之合作。

美國與新加坡預計於 2025 年進行下一次關鍵與新興技術（CET）會談，將持續討論雙邊、區域或國際之 CET 合作，為雙方人民與印太地區（Indo-Pacific region）創造更繁榮、安全及光明之未來。

資料來源：

1. The White House, JOINT FACT SHEET: Second U.S.-Singapore Critical and Emerging Technology Dialogue, 2024-08-01, https://www.whitehouse.gov/briefing-room/statements-releases/2024/08/01/joint-fact-sheet-second-u-s-singapore-critical-and-emerging-technology-dialogue/ (last visited 2024/08/14)

(二)2024 年 9 月白宮將加強相關措施，保護美國各界免於受關切國家資助「具威脅之車聯網技術」的影響

繼 2024 年 2 月對聯網汽車（connected car）之網路安全進行調查外，美國白宮於 9 月 23 日發布新聞，有鑑於中國大陸汽車製造商正在尋求主導美國與全球之車聯網技術，其已對美國之國家安全產生新的威脅，爰將加強相關措施，保護美國免於受關切國家資助具威脅之車

本報告之智慧財產權歸屬於國發會

聯網技術的影響。以商務部為例，該部將提出擬議規則制定通知（NPRM）。如果該通知經確定，將可禁止銷售或進口採用某些技術之聯網汽車，以及從中國大陸或俄羅斯進口特定零組件。

雖然聯網汽車優點很多，例如：可促進行車安全，或協助駕駛進行導航等。但也帶來新興且日益嚴重的威脅，例如車聯網技術包含可控制汽車運作、蒐集駕駛與乘客之資料，支援自動駕駛以及記錄美國基礎設施詳細資訊之攝影機與感測設備。由於這些車聯網技術能夠獲得地理區域或關鍵基礎設施之資訊，為惡意行為者提供破壞基礎設施或車輛本身運作之機會。且商務部也已確認，中國大陸或俄羅斯之聯網汽車中所使用的某些技術，可監視或破壞美國供應鏈內之關鍵技術，將不利於美國國家安全。

依目前商務部擬議之規則，將禁止進口或銷售由中國大陸或俄羅斯資助之設計、開發、製造或供應之某些車聯網技術。這些技術例如：車輛連接系統（vehicle connectivity systems, VCS）係指連結車輛與網際網路之系統或零組件，像是透過藍牙、衛星網路或 Wi-Fi；或自動駕駛系統（automated driving systems, ADS），允許在無人駕駛情形下運作。該規則將包含限制進口或銷售使用 VCS 或 ADS 軟體之聯網汽車，以及進口 VCS 硬體設備。

承前，相關軟體之限制將對自 2027 年上市之車款開始生效，而硬體之限制將對自 2030 年上市之車款生效。其他若沒有年份之車款，將統一自 2029 年 1 月生效；這些限制有助於解決受關切國家資助之車聯網技術所帶來國家安全之風險。美國政府也鼓勵利害關係人可向商務部提出意見，而國務院也會持續與產業、美國盟友或其他合作夥伴密切協商，以確保相關措施能最大化保護美國國家安全，並最小化其影響或干擾。

資料來源：

1. the White House, FACT SHEET: Protecting America from

本報告之智慧財產權歸屬於國發會

Connected Vehicle Technology from Countries of Concern, 2024-09-23, https://www.whitehouse.gov/briefing-room/statements-releases/2024/09/23/fact-sheet-protecting-america-from-connected-vehicle-technology-from-countries-of-concern/ (last visited 2024/10/02)

二、歐盟

(一)2024 年 7 月歐盟執委會就制定「數位服務法下未成年人網路保護指引」進行證據及意見徵集

2024 年 7 月歐盟執委會（European Commission）針對制定數位服務法下未成年人網路保護指引（guidelines on protection of minors online under the Digital Services Act）進行證據及意見徵集。歐盟執委會先前頒布歐盟數位服務法（Digital Services Act, DSA）旨在確保使用的所有數位服務，即為超大型網路平臺（Very Large Online Platforms）例如：Instagram、YouTube，及超大型網路搜尋引擎（Very Large Online Search Engines）例如：Google，能有效保障使用者的權利、保障其安全、阻止非法或不當內容的散佈及網路霸凌。於未成年使用網路則需更高層級的隱私、安全和保障措施，並確保兒童權利和最大利益，DSA 中設置兒童保護機制，歐盟執委會於 2024 年 2 月發表 DSA 保護 18 歲以下的兒童及青少年上網之措施手冊，說明對於未成年之保護機制，例如：兒童友善資訊之相關條款及條件之撰寫與更新方式，必須讓每個人皆容易理解，尤其了解其同意事項。

為使未成年人之網路世界更加安全，確保更高層級的隱私、安全及保障，歐盟執行委員會呼籲大眾提供證據及意見，蒐集關於未成年人在網路上遇到的風險，以及相關緩解措施之良好作法及建議，並邀請利害關係人參與證據徵集，提供科學報告及研究；評估網路平臺應適用之範圍，除小型事業外，未成年人網路保護指引應適用於所有未成年人可存取的網路平臺，包括不向未成年人開放但仍存在未成年用

本報告之智慧財產權歸屬於國發會

戶的平臺等，以作為制定「數位服務法下未成年人網路保護指引」之參考，證據及意見將持續徵集至 2024 年 9 月 30 日，並計劃在 2025 年夏季前通過此指引。

資料來源：

1. Commission launches call for evidence for guidelines on protection of minors online under the Digital Services Act, 2024-07-31, https://digital-strategy.ec.europa.eu/en/news/commission-launches-call-evidence-guidelines-protection-minors-online-under-digital-services-act (last visited 2024/08/21)
2. The Digital Services Act (DSA) explained - Measures to protect children and young people online , 2024-02-06, https://op.europa.eu/en/publication-detail/-/publication/f3556a65-88ea-11ee-99ba-01aa75ed71a1 (last visited 2024/08/22)

(二)2024 年 10 月歐盟發布「線上消費者保護法制調查報告」，說明相關法制之優點與侷限

歐盟執委會於 2024 年 10 月 3 日發布新聞，說明數位公平適切性調查（Digital Fairness Fitness Check）之結果。該項調查係於 2022 年啟動，主要針對歐盟 3 項線上消費者保護法制，包含：不公平商業行為指令（the Unfair Commercial Practices Directive）、消費者權利指令（the Consumer Rights Directive）以及不公平契約條款指令（the Unfair Contract Terms Directive），以確保相關法制符合數位環境下對消費者權益之保護。

此一調查結果顯示，該 3 項法規對於保護消費者權益與確保歐盟數位單一市場之運作有其助益及必要性。但同時也顯示，消費者在線上與線下之行為有所不同，例如技術之發展讓事業更能追蹤或引導線上消費者之行為；然亦突顯，相關規範要能夠因應網路上之風險與挑戰仍有發展空間。

本報告之智慧財產權歸屬於國發會

調查結果顯示，歐盟該 3 項法規已提供一定之監管功能，並有助於建立消費者之信賴，支援多元化數位市場之發展。惟仍有部分行為，例如：透過線上介面，以不實之緊急聲明帶給消費者不必要之壓力；或設計類似電玩遊戲內之賭博機制，讓使用者上癮或不斷花錢使用該服務；或消費者難以取消訂閱服務等問題，均有賴後續規範之強化。

根據歐盟之調查，上述有害消費者之線上商業行為，每年對歐盟消費者造成至少 79 億歐元之損失。但事業要遵守線上消費者保護相關法制之成本，每年卻不超過 7.37 億歐元。此外，由於部分成員國執法不足、具法律不確定性、成員國國家監管方式破碎化，以及事業缺乏追求最高消費者保護標準之誘因等因素，對於歐盟消費者權益之保障仍有不利影響。

綜此，為創造對消費者公平之數位環境，若解決前述有害消費者之線上商業行為、增加法律確定性、防止分散之監管，及促進公平環境，歐盟執委會後續將針對上開指令及數位服務法（Digital Services Act）等規範，研擬應用與執法之指引手冊。相關參考資料也將透過公眾諮詢，俾利提供符合需求之建議與內容。

資料來源：

1. EC, Commission evaluation shows the benefits and limitations of online consumer protection laws, 2024-10-03, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4901 (last visited 2024/10/09)

三、 英國

(一)2024 年 8 月蘇格蘭政府公布其推廣數位證據共享能力平臺之進度

本報告之智慧財產權歸屬於國發會

蘇格蘭政府於 2024 年 8 月 1 日公布其推廣數位證據共享能力（Digital Evidence Sharing Capability, DESC）平臺之進度。DESC 為蘇格蘭政府、蘇格蘭警局、蘇格蘭皇家辦公室與地方檢察官服務處（Crown Office and Procurator Fiscal Service, COPFS）、蘇格蘭法院及法庭服務局（Scottish Courts and Tribunals Service）、蘇格蘭警方主管機關（Scottish Police Authority）與律師界（defence community）之間的合作專案，旨在改變在整個刑事調查至訴訟過程中管理數位證據的方式。蘇格蘭的警察、檢察官、律師、法官及法院工作人員可以透過使用一個安全、統一的 DESC 平臺，蒐集、儲存、處理及管理數位證據。

在 2023 年 1 月至 2024 年 4 月，蘇格蘭丹狄（Dundee）試行 DESC 平臺期間，該平臺已處理約 19,500 件數位證據，節省警察約 550 小時工時。蘇格蘭司法部部長 Angela Constance 表示「DESC 平臺為蘇格蘭全球首創並具變革性的計劃，有助於司法人員以高效率、安全的方式，蒐集、管理自犯罪現場到法庭階段的數位證據」。目前蘇格蘭已於泰賽德（Tayside）、福斯山谷（Forth Valley）推行 DESC 平臺，並預計於 2025 年秋季完成全國推行。蘇格蘭政府預計 10 年內，會投資 3300 萬英鎊於 DESC 平臺。

DESC 平臺所處理的數位證據類型，包括：閉路電視監視機（CCTV footage）、照片及其他來自電腦或行動裝置的資料，並將擴大資料類型至警詢的文件與錄音。此平臺同時代表著，民眾與事業可以透過電子信件方式向警方提供數位證據。蘇格蘭警察局助理局長（Assistant Chief Constable）Tim Mairs 指出「目前為止，蘇格蘭警方多仍採取將手機內影像、監視器畫面等數位證據儲存於隨身碟、光碟後，再移交至蘇格蘭皇家辦公室與地方檢察官服務處，而 DESC 平臺為實現蒐集、管理、安全儲存數位證據的重要一步」。

蘇格蘭的泰賽德、中央及伐夫（Tayside, Central and Fife）地區的警長 Gillian Wade KC 並補充說明「DESC 平臺有助於更輕鬆地共享數位證據，即有助於提早確定案件的強度（strength of a case），以及有助

本報告之智慧財產權歸屬於國發會

於法官更充分地審理案件。雖然目前 DESC 平臺僅用於簡易案件，但可預見未來會擴大適用範圍」。

資料來源：

1. Police Professional, Digital evidence sharing platform rolled out in Scotland, 2024-08-02, https://policeprofessional.com/news/digital-evidence-sharing-platform-rolled-out-in-scotland/ (last visited 2024/08/16)
2. Scottish Government, National roll-out of digital evidence sharing technology, 2024-08-01, https://www.gov.scot/news/national-roll-out-of-digital-evidence-sharing-technology/ (last visited 2024/08/16)
3. Scottish Government, Digital evidence pilot, 2023-03-07, https://www.gov.scot/news/digital-evidence-pilot/ (last visited 2024/08/20)

(二)2024 年 9 月英國政府宣示將加強打擊《線上安全法》規範之親密影像濫用問題

英國科學、創新與技術部（Department for Science, Innovation and Technology，下稱英國科技部）於 2024 年 9 月 13 日發布新聞，英國政府宣示將加強打擊《線上安全法》（Online Safety Act）內規範關於親密影像之濫用問題。

英國政府制定《線上安全法》係起源於網路色情或私自散布親密影像等情事頻傳，為保護成人、兒童等對象之權益，該法草案前於 2021 年提出後，歷經多次討論、修正，已於 2023 年 10 月生效，並自 2024 年起分階段施行（詳該法第 240 條）。目前該法分為 12 個章節（part）、計 241 條條文，包含刑事與行政責任。且除行為人外，事業無論是否成立於境外，只要提供社群媒體、雲端服務等給英國之消費者（使用者），也都適用該法規定。

本報告之智慧財產權歸屬於國發會

在刑事責任部分，除規範網路霸凌、虛假訊息、報復式色情等內容，且不只分享色情圖片，以造成當事人痛苦或驚恐為目的者，甚至是透過閃光或其他方式，致使癲癇患者產生不適或傷害之行為，亦屬該法規範之網路犯罪類型，違者將有刑事責任。舉例而言，配合《性犯罪法》（Sexual Offences Act 2003）第 66B 條規定之修正，未經同意分享私密影像屬於犯罪行為；此一刑事責任，如該法第 187、188 條之規定，已自 2024 年 1 月施行。

至於行政責任，主要涉及對事業之相關義務要求，主管機關為英國通訊傳播管理局（Office of Communications，下稱英國通傳局）。違反《線上安全法》或英國通傳局要求，最高可處 1,800 萬英鎊或全球營業額 10%之罰款。例如：該法要求提供社群媒體、雲端服務、影音共享、線上論壇、約會服務或線上即時通訊服務之業者，對其網站上之非法或有害兒童之內容，應建立制度或流程，以降低其服務被用於非法活動之可能，並於發現非法內容時，予以刪除。且如依該法第 12 條或第 81 條相關規定，對於非法活動或內容，提供相關服務之業者應予負責；違反者，除如第 82 條將由英國通傳局課予相關義務或應負行政責任外，另依該法第 138 條之規定，最高將可處 2 年以下之有期徒刑。

除英國通傳局於該法生效後，陸續發布參考指引，供民眾或事業了解非法或對兒童不宜之內容與相關保護外，如同英國科技部新聞稿內提及，包含內政部、法務部等部會在內，英國政府預計將未經同意分享私密影像視為優先處理之犯罪行為，也要求社群媒體、雲端服務等業者，保護其用戶免受線上非法內容之侵害。

資料來源：

1. DSIT, Crackdown on intimate image abuse as government strengthens online safety laws, 2024-09-13, https://www.gov.uk/government/news/crackdown-on-intimate-image-abuse-as-government-strengthens-online-safety-laws (last

本報告之智慧財產權歸屬於國發會

visited 2024/09/25)

2. DSIT, Cyberflashing, epilepsy-trolling and fake news to put online abusers behind bars from today, 2024-01-31, https://www.gov.uk/government/news/cyberflashing-epilepsy-trolling-and-fake-news-to-put-online-abusers-behind-bars-from-today (last visited 2024/09/25)

3. legislation.gov.uk, Sexual Offences Act 2003, 2024-01-31, https://www.legislation.gov.uk/ukpga/2003/42/section/66B (last visited 2024/09/25)

4. DSIT, Guidance Online Safety Act: explainer, 2024-05-08, https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer (last visited 2024/09/25)

四、日本

(一)2024 年 9 月日本更新法規審查數位化之參考資料，積極推動政府法律規範現代化

日本數位廳於 9 月 10、12 日陸續發布新聞，更新關於模擬審議法規狀況之統計表（アナログ規制の見直し状況に関するダッシュボード）及地方公共團體審議法規之執行成果（地方公共団体におけるアナログ規制の見直しの取組）等參考資料。

數位廳自 2022 年起推動法規審查機制（アナログ規制），由日本政府對法規內容進行審視，以確認是否符合現代化需求。舉例來說，當今社會已不再使用磁碟片，故應避免在相關法規內仍出現要求提供磁碟片之文字。日本政府將法規之內容分為 8 類，包含：目視、現場檢查、定期檢查、專業人員進駐、書面提出，或向民眾公開等，以確認渠等要求是否合理或符合現代化需求；迄今已審視近 1 萬條法規。

本報告之智慧財產權歸屬於國發會

為協助中央或地方政府之人員進行法規審查，數位廳提供許多原則與參考文件，以協助判斷技術趨勢與可能之因應建議，例如：對河流、水壩或公園等管理人員，規範上應使用目視檢查；但如能透過遠端監控、引進無人機或利用 AI 協助判讀資料，亦可納入相關規範。政府將不斷蒐集意見，持續優化相關參考資料。

前述更新之統計表或地方政府之執行成果，可進一步了解檢視結果與相關建議。例如目前針對車輛之駕駛，相關培訓可透過線上進行，但申請駕照或支付規費，仍以書面形式進行；未來可以搭配個人編號卡等，進行線上申請或支付。至於天氣或災害預告、銀行相關公告事項，目前要求應於告示牌內公告，或張貼於營業處所內之適當處；未來除於告示牌內張貼外，也可以透過網路公告。

由上開數位廳提供參考資料內之相關案例可知，並非所有法規之要求都應採行數位化，或透過線上方式進行。日本政府進行此一法規審查相關措施之目的即在於透過全面審視法規內容，判斷該規範之合理性，而非輕易予以廢止或簡化，以兼顧制定法規之目的，並確實符合現代化需求。

資料來源：

1. デジタル庁, デジタル原則を踏まえた「アナログ規制の見直しに係る工程表」および「アナログ規制（通知・通達等）の見直し方針」のフォローアップ結果, 2024-09-12, https://www.digital.go.jp/policies/digital-extraordinary-administrative-research-committee (last visited 2024/09/18)
2. デジタル庁, 条例等におけるアナログ規制に該当する可能性のある規定を洗い出すためのアナログ規制点検ツールβ版を公開しました, 2024-09-10, https://www.digital.go.jp/policies/digital-extraordinary-administrative-research-committee/local-government (last visited 2024/09/18)

本報告之智慧財產權歸屬於國發會

五、韓國

(一)2024 年 8 月韓國《虛實整合產業促進法》正式施行，規範元宇宙與虛實整合產業相關事宜

韓國《虛實整合產業促進法》(가상융합산업 진흥법) 前於 2024 年 2 月制定，主管機關韓國科技部（Ministry of Science and ICT）於 2024 年 8 月 19 日發布新聞，說明該部已訂定《虛實整合產業促進法施行令》(가상융합산업 진흥법 시행령안)，與該法一同於 8 月 28 日正式施行，將透過相關政策與監管措施，完備虛實整合產業之規範，並促進其發展。

《虛實整合產業促進法》共 7 章 35 條條文，被視為規範元宇宙與虛實整合產業相關事宜之重要法規，為全球首見之元宇宙專法。該法要求韓國政府應考量虛實整合之多元技術、產業特性，希望透過系統化之政策誘因、監管體系等，並結合產業自律，共同促進該產業之有序發展（該法第 3 條參照）。

依據該法與其施行令之規範，未來將透過各項政策促進虛實整合產業，包含但不限於訂定促進虛實整合產業之基本計畫（預計為 2025 至 2027 年，該法第 6 條參照）；進行產業調查，了解相關行業現況與改善監管機制（該法第 8 條參照）；以及培育虛實整合產業（如該法第 12 條），例如：設置區域性虛實整合產業輔導中心（該法第 19 條參照），建立系統化推廣體系或基礎設施。

透過此法，虛實整合業者、服務提供或相關營運商可獲得各項行政或財務支援（該法第 7、15 條參照），而中央或地方政府也可據此提供配套措施，例如：提供資訊與諮詢、提供進駐或育成空間，或協助行銷等，以利培育（該法第 20 條參照）；而中小型廠商，更應優先提供支援。

本報告之智慧財產權歸屬於國發會

較特別的是，中央部會或地方政府在推動虛實整合相關計畫時，依該法應導入虛實整合產業影響評估（가상융합산업영향평가）機制，以了解對一般市場之影響，如侵權之可能性等（該法第 26 條參照）。

最後，為建立安全可靠的環境，以利虛實整合產業相關服務之提供與使用，除業者自律（該法第 27 條參照），該法也規範虛實整合技術與服務之開發，應遵守事前許可、事後監管之原則且由於虛實整合產業需要整合多種技術與產業，可能面臨適用性或適用範圍不明之情形，因此將導入暫行標準（임시기준）機制，用以解釋現有法律法令，俾利彌補監管之不確定性(該法第 28、29 條參照)。

資料來源：

1. 과기정통부（Ministry of Science and ICT）, 가상융합산업 육성을 위한 법령 본격 시행! 2024-08-19, https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=238&pageIndex=&bbsSeqNo=94&nttSeqNo=3184828&searchOpt=ALL&searchTxt= (last visited 2024/08/28)
2. 법제처, 가상융합산업 진흥법, 2024-02-27, https://www.law.go.kr/법령/가상융합산업 진흥법/ (last visited 2024/08/28)

(二)2024 年 8 月韓國制定第 1 期國家戰略科技發展基本計畫(2024 至 2028 年)，涉及 AI、半導體、尖端生技、量子等 12 個領域，用以擘劃科技主權藍圖

韓國科技部於 2024 年 8 月 26 日發布新聞，其政府已制定第 1 期國家戰略科技（或譯技術）發展基本計畫（2024 至 2028 年），主要涉及 12 項領域，例如：AI（artificial intelligence, AI）、半導體、尖端生技、量子科技，用以擘劃科技主權藍圖。

本報告之智慧財產權歸屬於國發會

韓國政府前於 2022 年已選出 12 項國家戰略科技領域與 50 項詳細之關鍵科技內容，包含：半導體與顯示器、充電電池、交通運輸、次世代核能、尖端生物科技、航空航太及航海、氫能、網路安全、AI、次世代通訊、先進機器人與製造，以及量子科技。

該基本計畫將相關國家戰略科技領域分為 1. 維持領先，2. 全力追趕，及 3. 未來挑戰三大類，據此搭配不同措施措施。其中，1. 維持領先類，包含半導體與充電電池領域，重點為鞏固領先地位，故將強化公私研發、穩定供應鏈等；而 2. 全力追趕類，包含 AI、尖端生物科技及次世代核能等領域，將擴大研發與建立生態系，及鼓勵商業化等；至於 3. 未來挑戰類則包含：量子、航空航太及航海、氫能之領域，將透過雙邊或多邊合作研發，並結合外交、安全及碳中和等政策落實創新。

此外，該基本計畫之核心任務有三項，包含：1. 未來成長引擎：透過政策引領科技發展，全力支持 12 項國家戰略科技領域快速產業化。預計以民間需求為主，將於 5 年內投入 30 兆韓元以上鼓勵研發，且將建置研究所、人才培育之教育機構及區域技術創新中心等創新基地，以擴大相關科技之新創事業或規模化。2. 科技安全強國：重視科技安全，提升事件應變能力。將積極參與國際組織，建立穩固之戰略合作夥伴。且針對新興科技、政策法制建立分析預測體系；以及 3. 使命型創新：建立創新推動體系，加強產學研合作，並將讓研發成果看得見，例如商品化或產業化等。

綜上，該 5 年期之基本計畫預計於 5 年內陸續投資 30 兆韓元以上，聚焦在 AI、半導體、尖端生物科技、量子科技等 12 項國家戰略科技領域，除鼓勵公私、產學研合作研發，並透過政策資源，支援商業化與研發相關活動。目標為維持韓國科技在全球之領先地位，或減少與先進國家之差距。

資料來源：

本報告之智慧財產權歸屬於國發會

1. 과기정통부（Ministry of Science and ICT）, 대한민국 과학기술주권 청사진, 제 1 차 국가전략기술 육성 기본계획('24-28) 수립, 2024-08-26, https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=238&pageIndex=3&bbsSeqNo=94&nttSeqNo=3184844&searchOpt=ALL&searchTxt= (last visited 2024/09/04)

肆、 數位身分

一、 美國

(一)2024 年 8 月美國 NIST 第二次就數位身分系列指引（SP 800-63 & 63A, 63B, 63C）修正草案對外徵詢意見

美國國家標準與技術研究院（National Institute of Standards and Technology, NIST）於 8 月 21 日發布新聞，將第二次就數位身分指引（Digital Identity Guidelines）系列之修正草案，含 SP 800-63 及 A、B、C 共 4 份文件，對外徵詢意見，期限至 10 月 7 日止。

此一數位身分系列指引目前為修訂 4 版（Revision 4），包含 SP 800-63-4 數位身分指引 （Digital Identity Guidelines）及 SP 800-63A-4 數位身分指引：身分證明與註冊（Digital Identity Guidelines: Identity Proofing and Enrollment）、SP 800-63B-4 數位身分指引：身分驗證與身分驗證管理（Digital Identity Guidelines: Authentication and Authenticator Management）、SP 800-63C-4 數位身分指引：聯合與確認(Digital Identity Guidelines: Federation and Assertions）。相關修正草案第一次係在 2022 年 12 月發布並對外徵詢意見，經彙整近 4,000 筆建議並參考相關回饋予以修正後，嗣於 2024 年 8 月第二次發布。

2024 年 8 月之修正草案，計有 6 項重點，摘要如下：

1. 更新風險管理相關之文件與背景說明。舉例而言，NIST 修改第一次公開徵詢版本（Initial Public Draft）內之定義與風險管

本報告之智慧財產權歸屬於國發會

理流程，並新增背景說明，例如：背景內描述組織提供之線上服務，與其試圖透過數位身分來保護這些服務。

2. 新增持續評估指標之建議。就第一次公開徵詢版本加入之內容進行擴充，包含新增推薦之指標，可用以評估數位身分解決方案之性能。

3. 擴大防杜詐欺之要求與建議。尤其是針對數位身分之憑證服務提供商等，其程序內涉及防杜詐欺之管理，應包含實施詐欺檢查可能遇到之問題與挑戰。

4. 重新形塑身分驗證之控制措施。例如：根據數位身分驗證措施之不同，對於不同類別之要求重新進行分類與劃分，如至少區分：遠端無人確認、遠端有人確認（如視訊對話）、現場無人確認（如自助式終端設備）、現場有人確認（如面對面）。

5. 整合可同步之身分驗證機制。如 2024 年 4 月 NIST 發布可同步身分驗證機制之建議，相關內容已納入 SP 800-63B-4 之修正草案內。

6. 將使用者控制之數位錢包，納入美國聯邦政府機制。因數位錢包或憑證[規範於 SP 800-63C-4 內之屬性或特性（attribute bundles）]已被廣泛關注與採用。其本質如同聯邦政府提供之數位身分，爰 SP 800-63C-4 內也提供相關內容與具體要求。

由於 NIST 數位身分系列指引前一次修正係在 2017 年，為因應數位環境不斷變化，且線上或現實世界之威脅日增，本次修正希望能落實以風險管理為基礎，進而實現安全、保密、公平且可查閱之身分系統。

資料來源：

1. NIST, NIST Releases Second Public Draft of Digital Identity Guidelines for Final Review, 2024-08-21,

本報告之智慧財產權歸屬於國發會

https://www.nist.gov/news-events/news/2024/08/nist-releases-second-public-draft-digital-identity-guidelines-final-review (last visited 2024/09/04)

二、歐盟

(一)歐盟修正之數位身分架構與相關規範已於 2024 年 5 月正式施行，主要涉及數位身分錢包與其應用

歐盟理事會與歐洲議會前已於 2023 年 11 月就歐盟數位身分架構（European Digital Identity Framework）之修正達成共識，而修正後之規範（(EU) 2024/1183）已於 2024 年 4 月刊登於官方公報，並於同年 5 月正式施行，據以落實歐盟 2030 數位十年（Digital Decade 2030）之政策目標，例如公共服務數位化。

此一歐盟數位身分架構與相關規範（(EU) 2024/1183）除 78 段前言外，共 51 條條文，主要涉及數位身分錢包（European Digital Identity Wallets）與其應用，並修正 2014 年通過、2016 年施行之歐盟內部市場電子交易之電子身分認證及信賴服務規則（(EU) 910/2014 electronic Identification, Authentication and Trust Service, eIDAS），讓歐盟數位身分相關措施能與時俱進，故被部分媒體稱之為 eIDAS 2.0。

舉例來說，修正前之 eIDAS 規則以建立歐盟境內電子身分識別（identities）、認證（authentication）及網站憑證（website certification）跨境使用之法律基礎架構為主。而修正後之 eIDAS 2.0 除持續推動公共服務數位化外（前言第 41 段參照），在私人提供之服務上，結合數位服務法（Digital Services Act）對超大型線上平臺之規範，如 Amazon、Booking.com 或 Facebook，要求相關平臺亦應接受使用者透過歐盟數位身分錢包登入渠等之線上服務（前言第 57 段參照）。

本報告之智慧財產權歸屬於國發會

此外，歐盟各成員國依修正後之 eIDAS 2.0，應於 2026 年前向所有公民或居民，提供 1 個符合歐盟規範之數位身分錢包（第 51 條參照），使其可在歐洲各地由公共或私人提供之線上服務內，識別自己的身分，還要能夠儲存、呈現及共享數位文件，例如：大學文憑或火車車票，且具電子簽章與加密功能等。

為了確保順利推行數位身分錢包，歐盟執委會自 2023 年起已投入 4,600 萬歐元，推動 4 項大規模試點計畫，包含：行動駕駛執照、線上付款及數位教育與專業資格。相關計畫之重點在於確保數位身分錢包於各公共或私人提供之線上服務能互通無礙，且具高度安全性與資料保護之能力，並讓使用者可透過歐盟提供之數位身分錢包應用程式，自願且完全控制其個人資料，俾利 2 年後之全面推行。

資料來源：

1. EC, Commission welcomes final agreement on EU Digital Identity Wallet, 2023-11-08, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5651 (last visited 2024/09/04)
2. EC, The EU Digital Identity Framework Regulation Enters into Force, 2024-05-21, https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/The+Digital+Identity+Regulation+Enters+into+Force (last visited 2024/09/04)
3. EUR-Lex, Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, 2024-04-30, https://eur-lex.europa.eu/eli/reg/2024/1183/oj (last visited 2024/09/04)

本報告之智慧財產權歸屬於國發會

三、日本

(一)2024 年 9 月日本數位廳辦理電子簽章法認證標準相關之第 1 次研究會議，討論實務遭遇之問題，例如與國際標準內涉及風險管理、私鑰加密之差異事宜

日本數位廳於 2024 年 9 月 20 日發布新聞，已辦理電子簽章法認證標準相關之第 1 次研究會議（電子署名法認定基準のモダナイズ検討会（第 1 回））,邀集法律、技術等專家學者，討論該法施行後遭遇之問題，例如：風險管理，及與美國聯邦資訊處理標準（Federal Information Processing Standard, FIPS）140 之差異暨其處理相關事宜。

按日本電子簽章與認證服務法（電子署名及び認証業務に関する法律），簡稱電子簽章法（電子署名法），訂於 2000 年（平成 12 年），歷經多次修正。最近一次修正為 2022 年（令和 4 年），主要放寬電子簽章簽署人身分驗證等，若符合該法之規範即推定其為真正（詳該法第 3 條），預計於 2025 年（令和 7 年）6 月施行。

然而，由於日本電子簽章法施行後，在實務上仍有部分疑義。數位廳彙整 2023 年（令和 5 年）實務遭遇之 6 項議題，作為相關會議討論重點，摘要如下：

1. 欠缺歐洲電信標準協會（European Telecommunications Standards Institute, ETSI）建議之風險管理措施；
2. 該法憑證發行機構之私鑰加密技術與美國國家標準與技術研究院提出之聯邦資訊處理標準（FIPS）140 有所差異；
3. 如何在滿足國際標準下，同時符合雲端服務之需求；
4. 獲認證機房遠端控制與使用公有雲之管理；
5. 自動驗證使用者之真實性；

本報告之智慧財產權歸屬於國發會

6. 地方公共團體資訊系統使用電子簽章等認證業務法（電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律）之憑證管理機構與電子簽章法規定之差異。

此一系列的電子簽章法認證標準相關研究會議，自 2024 年 9 月起將陸續召開 4 次會議、討論前述 6 項議題（詳本次會議簡報第 11 至 13 頁）。本次（9 月 20 日）為第 1 次會議，主要討論第 1、2 項議題。依規劃將分別於 2024 年 11 月上旬、下旬召開第 2、3 次討論其餘 4 項議題；最終預計於 12 月召開第 4 次會議，提出報告說明各議題討論結果。因數位廳規劃之討論內容，對我國精進電子簽章法與相關規範亦有助益，此系列會議之進展值得持續關切。

資料來源：

1. デジタル庁, 電子署名法認定基準のモダナイズ検討会（第 1 回）, 2024-09-20, https://www.digital.go.jp/councils/digitalsign-modernization/08220923-62e0-4171-bee0-68cdb5a05801 (last visited 2024/09/25)
2. e-Gov, 電子署名及び認証業務に関する法律, 2022-06-17, https://laws.e-gov.go.jp/law/412AC0000000102 (last visited 2024/09/25)

伍、 資訊隱私

一、 美國

(一)2024 年 7 月美國紐約州總檢察長辦公室發布網站隱私控制-商業指引，涉及使用網站追蹤技術及隱私控制

2024 年 7 月 30 日美國紐約州總檢察長辦公室（Office of the New York Attorney General, OAG）發布網站隱私控制-商業指引（Business Guide to Website Privacy Controls），現今多數網站使用網站追蹤技術追蹤網站訪客，例如：Cookies 為訪客造訪網站時，由網頁瀏覽器建立的

本報告之智慧財產權歸屬於國發會

一個小文字檔案，可以幫助網站和其他線上服務在訪客從一個網頁點擊到下一個網頁時識別他們，讓訪客在一段時間內保持其帳戶登入狀態，並儲存訪客的偏好，且常用於分析、行銷和詐欺偵測。然而，這些技術也可能侵犯消費者的隱私，為解決此問題，許多網站向訪客提供有關網站的追蹤的資訊及允許訪客管理 Cookies 追蹤的控制項目，惟並非所有網站都採取適當的措施確保其揭露準確並且隱私控制發揮作用，產生網站訪客已停用追蹤技術，卻仍被網站持續追蹤或網站的隱私控制和資訊揭露具有誤導性之情況，故 OAG 發布此指引，幫助事業依步驟識別和預防有問題的 Cookies，以及確保隱私控制和揭露符合紐約法律。

指引中，網站得依下述步驟識別和預防部署追蹤技術問題：

1. 指定：指定專業人員負責實施和管理網站追蹤技術，並進行與網站追蹤技術和政策相關的適當培訓。

2. 調查：在部署或變更現有標籤或工具的使用方式之前，採取適當的步驟來確定蒐集的資料類型及資料的使用和共用方式；於某些情況下，要求標籤或工具的開發者提供未公開提供的資訊。

3. 配置：部署或更改網站標籤或工具的方式時，確保對其進行適當的分類和配置。

4. 測試：進行定期適當的測試，以確保標籤和工具能如預期運行，並在會影響網站訪客的追蹤方式變更時進行測試。確認自動掃描工具可以識別和不能識別的問題類型。

5. 審查：定期進行審查，確認標籤和工具配置正確。審查的範圍取決於網站使用的 tag 和工具，應確認標籤在同意管理工具中正確分類，並且正確同步任何 tag 管理工具。

本報告之智慧財產權歸屬於國發會

向消費者提供的隱私的控制和揭露須遵守紐約的消費者保護法，即事業關於追蹤的陳述，無論明示或暗示須真實且不具誤導性。其建議提供有效的揭露和易於使用的控制來幫助消費者了解，並提出下述注意事項：

1. 為按鈕添加標籤，以明確使用簡單、清晰的語言（避免使用法律或專業術語）。
2. 為按鈕添加標籤，以清楚傳達其功能。
3. 使介面易於存取。例如：訪客能夠使用鍵盤點擊隱私控制。
4. 給予選項同等的權重。例如：如果消費者可以透過點擊同意來追蹤，也可以透過點擊拒絕或提供大小、顏色和強調相同的「接受」和「拒絕」按鈕。
5. 不使用長篇文本，使消費者閱讀時間過長。
6. 不再強調拒絕追蹤的選項。
7. 不要使訪客拒絕追蹤比允許追蹤更困難，例如拒絕追蹤比允許追蹤需要更多步驟。

資料來源：

1. Website Privacy Controls A Guide for Business, 2024-07-30, https://ag.ny.gov/resources/organizations/business-guidance/website-privacy-controls (last visited 2024/08/14)
2. Cookie Cutter: NY AG Announces Cookie Scrutiny with Business Guide to Website Privacy Controls, 2024-08-06, https://www.jdsupra.com/legalnews/cookie-cutter-ny-ag-announces-cookie-6956705/ (last visited 2024/08/14)

本報告之智慧財產權歸屬於國發會

(二)2024 年 7 月美國聯邦交易委員會修訂之健康違反通知規則（Health Breach Notification Rule, HBNR）生效，擴大「對於消費者之『可識別個人健康資料外洩，具通知義務之實體』的適用範圍」

2024 年 7 月美國聯邦交易委員會（Federal Trade Commission, FTC）為促進健康資訊科技的使用，同時加強對健康資訊的隱私和安全保護，鑒於「持有個人健康記錄（Personal Health Record）之供應商與相關實體」不適用《健康保險可攜與責任法》（Health Insurance Portability and Accountability Act, HIPAA），故修訂《健康違反通知規則》（Health Breach Notification Rule, HBNR），要求對健康應用程式及其他類似技術的適用範圍以及擴大所受監管之實體，當個人可識別的健康資料遭違規行為外洩時，須向個人、美國聯邦交易委員會及在某些情況向媒體通報。HBNR 於 2024 年 7 月 29 日正式生效。其修訂內容如下：

1. 闡明適用範圍，明確包括電子健康應用程式開發人員：「未受 HIPAA 涵蓋之個人健康紀錄供應商」適用於 HBNR，即提供或維護個人健康記錄的實體，包括行動健康應用程式的開發人員。

2. 修訂違規行為及受監管實體的關鍵定義：違規行為係指未經授權，而獲得 PHR 可識別健康資訊或透過追蹤技術，例如：cookies 不當外洩可識別資訊。受監管實體為個人健康記錄相關產品及服務的個人健康紀錄供應商（包括其行動健康應用程式）實體，即提供追蹤疾病、健康狀況的機制及線上服務，例如：網站、行動應用程式或網路連接設備，亦或是只有存取或向個人健康紀錄傳送不安全的個人健康記錄可識別健康資訊的實體，只存取或向個人健康紀錄傳送任何資訊的實體，則非屬個人健康記錄相關實體。

3. 闡明個人健康記錄可識別健康資訊:

本報告之智慧財產權歸屬於國發會

(1) 由個人或代表個人提供的資訊。

(2) 與身體或精神健康狀況或向個人提供醫療保健相關的資訊。

(3) 識別個人或合理用於識別個人的資訊。

(4) 由「受監管實體」或其他實體創建或接收的資訊。

4. 修訂規定通知的方式、內容及時間：新增以電子郵件方式及其他電子方式提供清晰有效的違反通知。違反通知之內容須包含由違反安全規定行為獲取不安全的個人健康記錄可識別健康資訊的任何第三方的姓名、身分、網站和聯絡資訊，若提供全名或身分會對個人或提供通知的實體帶來風險則需包含描述，通知亦應包括涉及違規的不安全個人健康記錄可識別健康資訊類型的描述。於涉及 500 人以上的違規行為，受監管實體須在任何情況下不得晚於發現違反安全規定後 60 日通知受影響的個人，並同時通知美國聯邦交易委員會。

資料來源：

1. Health Breach Notification Rule, 2024-05-30, https://www.federalregister.gov/documents/2024/05/30/2024-10855/health-breach-notification-rule (last visited 2024/08/20)

2. The FTC's Revised Health Breach Notification Rule Is Now in Effect, 2024-08-02, https://www.jdsupra.com/legalnews/the-ftc-s-revised-health-breach-9563207/ (last visited 2024/08/20)

3. FTC Finalizes Changes to the Health Breach Notification Rule, 2024-04-26, https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-finalizes-changes-health-breach-notification-rule (last visited 2024/08/20)

4. FTC Announces Final Changes to Health Breach Notification Rule That Broaden the Rule’s Scope and Application, 2024-07-02, https://www.venable.com/insights/publications/2024/07/final-

本報告之智慧財產權歸屬於國發會

changes-to-health-breach-notification (last visited 2024/08/21)

(三)2024 年 8 月美國加州參議院通過修正《2020 年加州消費者隱私法：蒐集 18 歲以下消費者個人資料法案》

2024 年 8 月美國加州參議院通過修正《2020 年加州消費者隱私法：蒐集 18 歲以下消費者個人資料法案》（AB1949 法案）（California Consumer Privacy Act of 2020：collection of personal information of a consumer less than 18 years of age），此修正法案旨在為 18 歲以下未成年人提供更完善的網路保護，要求事業符合比現行加州消費者隱私法（California Consumer Privacy Act, CCPA）更高的身分驗證標準。

現行 CCPA 規定，禁止事業於明知消費者未滿 16 歲的情況下，而蒐集、出售、分享、使用或揭露消費者的個人資料，除非年滿 13 歲未滿 16 歲的消費者，或未滿 13 歲消費者之家長或監護人同意。惟事業多辯稱其實際上不知用戶為未滿 16 歲，忽略未成年人可能使用其網站，而規避現行規定，此情況導致投入識別及保護未成年消費者相關措施或作為之事業處於競爭劣勢，並對身處重要發展階段的未成年人造成負面影響。而不同年齡階段未成年人認知會有顯著差異，故需要不同程度之保護，有必要將保護範圍擴大至 18 歲以下之未成年人。

下列為此法案修正重點：

1. 刪除現行事業明知未滿 16 歲的條件，修正為事業明知消費者未滿 18 歲，不得蒐集、出售、分享、使用或揭露消費者的個人資料，除非年滿 13 歲且未滿 18 歲的消費者，或未滿 13 歲消費者之父母或監護人已明確同意。

2. 增訂事業故意忽略消費者年齡者，應視為明知消費者的年齡。

本報告之智慧財產權歸屬於國發會

3. 增訂事業透過平臺、機制或技術收到訊號，顯示消費者實際上是未成年人，則必須將該消費者視為未成年人。

該修正案於通過前要求公開徵詢意見，加州隱私保護局政策法規部副主任於 5 月曾對此法案提出異議意見：

修正案將年齡擴大至未滿 18 歲，要求事業蒐集、出售、分享、使用或揭露未成年人的個人資料須先獲得年滿 13 歲但未滿 18 歲之未成年人，或未滿 13 歲之未成年家長或監護人同意授權。然而，於某些情況下此修正規定可能導致實務執行之問題，例如：當父母將子女列為受益人或提供子女的個人資料獲得利益時，若子女年滿 13 歲但未滿 18 歲，即使是蒐集子女姓名的行為，事業也需要取得子女的同意，以避免違法。導致此修正案之施行標準雖並非窒礙難行，但非常不實際。

資料來源：

1. Assembly Bill No. 1949 Analysis, 2024-08-29, https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=202320240AB1949 (last visited 2024/09/11)
2. AB-1949 California Consumer Privacy Act of 2020: collection of personal information of a consumer less than 18 years of age, 2024-08-29, https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=202320240AB1949&showamends=false (last visited 2024/09/11)
3. Agenda Item 3—Legislative Update and Authorization of CPPA Position on Pending Legislation. AB 1949 (Wicks): California Consumer Privacy Act of 2020: collection of personal information of a consumer less than 18 years of age, 2024-05-03, https://cppa.ca.gov/meetings/materials/20240510_item3_ab1949_memo.pdf(last visited 2024/09/11)

本報告之智慧財產權歸屬於國發會

(四)2024 年 9 月美國聯邦交易委員會發布《檢視社群媒體及串流服務之資料治理實踐報告》

為了解社群媒體及串流服務平臺如何影響消費者個人資料隱私，2020 年 12 月，美國聯邦交易委員會（Federal Trade Commission, FTC）向亞馬遜（Amazon）、臉書（Facebook）、YouTube、X(前身為 Twitter)、Snap、字節跳動（ByteDance）、Discord、Reddit 及 WhatsApp 等 9 家社群媒體及串流服務公司（Social Media and Video Streaming Services companies, SMVSSs）發布命令，要求針對其如何蒐集、利用消費者個人資料、如何向消費者投放廣告、以及對兒童及青少年個人資料影響等政策提交特別報告。2024 年 9 月，美國聯邦交易委員會審查前述事業及其所提交之報告後，發布《檢視社群媒體及串流服務之資料治理實踐報告》（Examining the Data Practices of Social Media and Video Streaming Services，下稱調查報告）。報告分為五個主題：資料治理、廣告治理、演算法、資料分析或 AI、兒童及青少年、競爭實踐。

該調查報告之主要發現如下：

1. 公司資料蒐集、最小化及保存（retention）之資料保護政策實踐不足，對其使用者及非使用者造成隱私風險。

2. 許多公司仰賴銷售廣告服務予其他業者，且其中多是以消費者資料進行廣告投放。該類技術並非消費者可預見，但對消費者造成顯著的隱私風險。

3. SMVSSs 大量使用演算法、資料分析或 AI 技術於使用者及非使用者之個人資料。包含所有推薦內容及搜尋引擎、廣告及推斷使用者個人資料。但使用者缺乏對個人資料如何運用於 AI 驅動系統之控制。

本報告之智慧財產權歸屬於國發會

4. 多數公司政策未能充分保護兒童及青少年。尤其是不受《兒童線上隱私保護法》（Children's Online Privacy Protection Act , COPPA）保護之青少年。

調查報告最後依據各主題提出建議。

1. 資料治理

調查報告建議國會應制定聯邦隱私保護法律限制、監控並保障消費者隱私權，且 SMVSSs 亦應採取更多措施來保護消費者隱私，包含：減少蒐集個人資料、限制與子公司或公司集團及第三人共享消費者資料、執行具體並可執行之資料最小化及保留政策、刪除不需要之消費者個人資料。此外，SMVSSs 應採取明確、簡單且易理解之隱私保護政策，以利消費者了解平臺政策及其個人權益。

2. 廣告治理

調查報告建議 SMVSSs 應檢查其投放式廣告涉及敏感資料之政策，並應廣義解釋敏感資料，此外，SMVSSs 不應透過侵犯隱私的廣告追蹤技術蒐集使用者之敏感資料。

3. 使用演算法、資料分析及 AI

SMVSSs 應解決自動化系統使用上缺乏存取、選擇、控制、透明度及可解釋性有關之問題，並執行更嚴格的測試及監控標準。報告亦指出，聯邦層級立法將有助於鞏固消費者隱私權利及保障。

4. 兒童及青少年之保護

報告建議 SMVSSs 應將 COPPA 視為最低標準並酌情額外給予兒童安全措施，且應採取更多措施保護青少年使用者。SMVSSs 不應忽視有兒童使用者之事實，對於限制兒童使用

本報告之智慧財產權歸屬於國發會

的 SMVSSs 應設有更加明確之政策，規定若於平臺上發現兒童使用者之應對措施，對於兒童個人資料之管理，SMVSSs 應提供兒童之監護人能簡易管理之方法。此外，由於 COPPA 僅規範兒童，導致社會不認為青少年為成年人，卻無法律保障青少年於數位活動中之隱私安全，因此報告指出國會應訂定聯邦隱私立法以保護青少年網路使用者。

5. 競爭法制

反托拉斯執法者應仔細審查潛在之反競爭收購以及行為，應考慮非法收購對消費者所產生之影響，包含 SMVSSs 應如何對待消費者資料、隱私以及這些做法對競爭之影響。調查報告亦指出，前述對 SMVSSs 在資料隱私等各方面之建議除為消費者帶來利益外，亦能促進優良競爭。

資料來源：

1. Federal Trade Commission, A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services, 2024-9-19, https://www.ftc.gov/reports/look-behind-screens-examining-data-practices-social-media-video-streaming-services (last visited 2024/09/26)

(五)2024 年 9 月美國加州隱私保護局發布關於《「避免黑暗模式：清晰易懂的語言及對稱性的選擇」執行建議》

2024 年 9 月美國加州隱私保護局（The California Privacy Protection Agency, CPPA）發布關於《「避免黑暗模式：清晰易懂的語言及對稱性的選擇」（Avoiding Dark Patterns：Clear and Understandable Language, Symmetry in Choice）執行建議》，CPPA 將「暗黑模式」（Dark Pattern）定義為設計或操縱使用者介面，於使用者介面上使用幾乎相同的語言，並具有「實質上顛覆或損害使用者自主權、決策權或選擇權」的效果。

本報告之智慧財產權歸屬於國發會

依據加州消費者隱私法（CCPA），事業合法蒐集及處理消費者資料取決於自由給予的、具體的、知情及毫不含糊的消費者意願表示，表示同意基於特定目的處理與消費者相關之個人資料，而透過暗黑模式取得消費者同意蒐集及處理其個人資料，並不構成同意，涉及妨礙隱私權。CPPA 發布此執行建議，建議事業須檢視並評估其使用者介面，確保為消費者提供隱私選擇的語言清晰及介面設計清晰並提供對等選擇。

為避免事業創建暗黑模式於消費者須遵守：

1. 於使用者介面使用的語言，須易於閱讀及理解，避免使用技術或法律術語及混淆消費者之語言或互動。

2. 消費者行使隱私權保護程度較高的選擇權的途徑，不得比行使隱私權保護程度較低的選擇權的途徑更長、更難或更費，避免損害及干擾消費者作出對稱（對等）選擇：

   (1) 不對稱或不對等的選擇：「選擇不出售/分享其個人資料的程序所需的步驟」多於「選擇再加入的程序」。選擇加入出售個人資料的程序時，提供「是」和「稍後再問我」兩種選擇。

   (2) 對稱或對等選擇：尋求消費者同意使用消費者個人資料的網站橫幅，提供「全部接受」和「全部拒絕」兩種選擇。選擇加入出售個人資料程序時，可選擇「接受」或「不接受」。

CPPA 建議事業於檢視及評估使用者介面時，應先向自己提問下列問題:

1. 與消費者溝通時使用的語言是否易讀易懂？

2. 使用的語言是否避免使用技術或法律術語？

3. 消費者說「不」的路徑是否比說「是」的路徑更長？

本報告之智慧財產權歸屬於國發會

4. 介面是否讓消費者於要求使用其個人資料，說「不」比「同意」更難？

5. 消費者做出更能保護隱私的選擇是否更花時間？

資料來源：

1. CPPA, CPPA Enforcement Advisory Stresses the Importance of Avoiding Dark Patterns, 2024-09-04, https://cppa.ca.gov/announcements/2024/20240904.html?mkt_tok=MTM4LUVaTS0wNDIAAAGVXRb7lhmWiSPyDC2pBLm9cTgiwy3bbSkK1Z5Q0-eCqP0A8OCauFRrDs5qwFjmR3Ep3c2_gVWCi6e1axE5QTn91aZpZcAIMViEjSlEkut1thkb (last visited 2024/09/30)

2. AVOIDING DARK PATTERNS: CLEAR AND UNDERSTANDABLE LANGUAGE, SYMMETRY IN CHOICE, 2024-09-04, https://cppa.ca.gov/pdf/enfadvisory202402.pdf (last visited 2024/09/30)

3. California Privacy Protection Agency Issues Dark Pattern Enforcement Advisory, 2024-09-11 , https://www.jdsupra.com/legalnews/california-privacy-protection-agency-6385617/ (last visited 2024/09/30)

二、歐盟

(一)2024 年 7 月歐洲資料保護委員會發布《歐盟－美國資料隱私框架》指引文件

2024 年 7 月歐洲資料保護委員會（European Data Protection Board , EDPB）發布針對《歐盟－美國資料隱私框架》（EU-U.S. Data Privacy Framework, DPF）之兩份常見問題指引文件（Frequently Asked Question, FAQ），旨在進一步說明 DPF 之運作。DPF 主要為使歐洲經濟區

本報告之智慧財產權歸屬於國發會

（European Economic Area, EEA）傳輸個人資料至美國之認證公司時，無需採取額外資料傳輸保護措施。

第一份 FAQ 解答，說明 DPF 的整體情況、如何從中受益、如何依 DPF 提出申訴以及處理申訴的方式。下列為 EDPB 對歐洲事業之說明：

1. DPF 適用於「從歐洲經濟區傳輸至美國之任何類型個人資料」，包括為商業或健康目的處理之個人資料，及基於僱傭關係中蒐集之人力資源資料，只要美國端資料接收之事業已依 DPF 進行自行認證（self-certified）可處理此類資料。

2. 當個人資料從歐洲經濟區傳輸至依 DPF 認證之美國事業，DPF 賦予當事人相關權利，使之有權獲知移轉及目的、獲得個人資料存取權限、更正或刪除任何不正確或非法處理的資料，並於發生疑慮時聯絡任何歐洲經濟區國家個人資料保護機關（Data Protection Authority, DPA）。

3. 資料隱私框架清單（Data Privacy Framework List，下稱 DPF 清單）上，受認證公司皆須標示申訴程序及獨立追訴機制的相關資訊，可直接依照所提供表格範本向國家 DPA 提出美國公司應遵守資料隱私框架原則（Data Privacy Framework Principles，下稱 DPF 原則）的申訴。

4. 向歐洲經濟區國家之 DPA 提出申訴時，可能就申訴案件情形，產生以下程序：

   (1) 組成歐盟 DPA 非正式小組

   申訴涉及移轉給美國事業處理之人力資源資料，或美國事業自願選擇歐盟 DPA 作為獨立追訴機制時，會成立數個歐盟 DPA 組成的非正式小組，處理申訴、展開調查，

本報告之智慧財產權歸屬於國發會

期間申訴人與美國事業皆表達意見，於必要解決案件，非正式小組可發出「建議」，對美國事業具有約束力。

(2) 轉介至美國當局

申訴不涉及處理人力資源資料，或選擇不由歐盟 DPA 作為獨立追訴機制時，國家 DPA 將申訴轉介至美國主管機關，例如：美國聯邦交易委員會、交通部航空消費者保護辦公室（Office of Aviation Consumer Protection）或美國商務部（United States Department of Commerce, DoC），亦或由主管歐洲經濟區資料出口商的國家 DPA 直接對資料出口商行使其權力。

第二份 FAQ 說明美國事業加入 DPF 之資格、個人資料傳輸至經 DPF 認證的美國公司前應為之作為，及自何處找尋有關歐洲事業美國子公司之認證指引等。下列為 EDPB 對事業之說明:

1. 為符合 DPF 認證的資格，美國的事業必須受到美國聯邦交易委員會或運輸部（United States Department of Transportation）的調查及執法權力的約束，意即非美國聯邦交易委員會或運輸部管轄範圍內，則無法依 DPF 進行認證，例如：非營利組織、銀行、保險公司及電信服務供應商等。未來將納入其他美國法定機構。

2. 下列為將個人資料移轉前，應

(1) 個人資料移轉至 DPF 認證的美國事業前，歐洲經濟區的資料出口商：

I. 須確定該美國事業具備有效的認證，且認證涵蓋需處理之相關資料。

本報告之智慧財產權歸屬於國發會

II. 檢查該美國事業是否列入美國運輸部網站公布 DPF 清單，已從清單中刪除之公司，只要保留於其具備 DPF 資格時接收之個人資料，須繼續適用 DPF 原則。

III. 將個人資料移轉至未經或不再是 DPF 認證的美國事業，可適用歐盟一般資料保護規則（GDPR）第 5 章的其他移轉理由，例如：「具約束力的公司規則」（Binding Corporate Rules）或「標準契約條款」（Standard Contractual Clauses）。

(2) 個人資料移轉至 DPF 認證事業之美國附屬事業前，歐洲經濟區資料出口商須檢查母事業之認證是否涵蓋相關子事業。

(3) 個人資料移轉給美國的資料控制者前，歐洲經濟區資料出口商須確保移轉符合 GDPR 所有相關規定。

(4) 歐洲經濟區資料控制者將個人資料移轉給在美國的資料處理者時，控制者和處理者有義務依 GDPR 簽訂資料處理協議，不論處理者是否依 DPF 進行認證。

3. 如果歐洲經濟區事業的美國子公司受美國聯邦交易委員會或運輸部的管轄，即可受 DPF 認證，可以於 DPF 官方網站找尋關於資格要求的資訊及自我認證程序指引。

資料來源：

1. EU-U.S. DATA PRIVACY FRAMEWORK F.A.Q. FOR EUROPEAN BUSINESSES, 2024-07-16, https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_en (last visited 2024/09/18)

2. EU-U.S. DATA PRIVACY FRAMEWORK F.A.Q. FOR EUROPEAN INDIVIDUALS, 2024-07-16,

本報告之智慧財產權歸屬於國發會

https://www.edpb.europa.eu/system/files/2024-07/edpb_dpf_faq-for-individuals_en_0.pdf (last visited 2024/09/18)

3. Questions & Answers: EU-US Data Privacy Framework, 2023-07-10, https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752 (last visited 2024/09/18)

4. EU Data Protection Regulators Publish Additional Guidance On The EU-U.S. Data Privacy Framework, 2024-08-21, https://www.jdsupra.com/legalnews/eu-data-protection-regulators-publish-4085589/ (last visited 2024/09/18)

三、荷蘭

(一)2024 年 8 月荷蘭資料保護局發布指引，警告事業注意與使用 AI 驅動之聊天機器人相關的潛在資料保護風險

2024 年 8 月 6 日荷蘭資料保護局（Data Protection Authority , DPA）發布指引，警告事業注意與使用 AI 驅動之聊天機器人相關的潛在資料保護風險。於此指令報告中，DPA 發現工作場所中許多人會使用 AI 驅動的聊天機器人（例如：ChatGPT 和 Copilot）回答客戶問題或彙整文件，可以幫助員工節省時間並提高工作品質及生產力，惟近期卻收到多起因員工使用 AI 的聊天機器人共享個人資料之個人資料外洩通報。

歐盟一般資料保護規則（GDPR）將個人資料外洩定義為未經授權的情況下存取個人資料，而造成個人資料不必要的毀損、遺失、修改或提供。例如：此次通報的一起個人資料外洩事件為一家醫療診所員工違反協議，將病患之醫療資料提供 AI 聊天機器人。醫療資料為高度敏感的資料，應受到法律高度保護，在沒有充分理由的情況下，與科技公司分享這些資料是對相關人員隱私之重大侵害。由於 AI 聊天機器人提供者通常會儲存所有輸入的資料，因此個人資料可能最終會出

本報告之智慧財產權歸屬於國發會

現在科技公司的伺服器上，而輸入個人資料之人通常無法得知此事，亦不知道該公司將如何處理這些個人資料。

為此，DPA 發布指引，強調雇主及員工之間在工作場所使用 AI 聊天機器人須達成明確協議，對於是否允許員工將 AI 聊天機器人用於與工作相關的目的，不應有任何模糊之處，如有員工違反公司政策使用聊天機器人處理個人資料，足以構成個人資料外洩。雇主允許使用 AI 聊天機器人於工作場所，員工應該清楚他們可以輸入的資料範圍，與 AI 聊天機器人提供者的契約中，公司還應包含限制提供者儲存及使用輸入資料的條款。當員工違反協議使用聊天機器人洩露個人資料，GDPR 要求控管者向相關歐盟成員國監管機構（在此指 DPA）通報個人資料外洩事件，並在資料外洩對受害者造成高風險情況下，須將個人資料外洩事件通知受害者。

資料來源：

1. Let op: gebruik AI-chatbot kan leiden tot datalekken, 2024-08-06, https://autoriteitpersoonsgegevens.nl/en/current/caution-use-of-ai-chatbot-may-lead-to-data-breaches (last visited 2024/08/13)
2. What is a data breach?, 2024-08-06, https://autoriteitpersoonsgegevens.nl/en/themes/security/data-breaches/what-is-a-data-breach(last visited 2024/08/13)
3. Reporting or not reporting a data breach, 2024-08-06, https://autoriteitpersoonsgegevens.nl/en/themes/security/data-breaches/reporting-or-not-reporting-a-data-breach(last visited 2024/08/13)
4. Dutch Data Protection Authority Warns that Using AI Chatbots Can Lead to Personal Data Breaches , 2024-08-12 , https://www.jdsupra.com/legalnews/dutch-data-protection-authority-warns-3771700/ (last visited 2024/08/13)

本報告之智慧財產權歸屬於國發會

四、韓國

(一)2024 年 9 月韓國個人資料保護委員會發布《自動化決策資料主體權利指引》

韓國個資保護委員會(Personal Information Protection Commission，下稱 PIPC）於 2024 年 9 月 26 日發布《自動化決策資料主體權利指引》(자동화된 결정에 대한 정보주체의 권리 안내서，下稱指引)，要求事業在 AI 等運用自動化決策之領域須遵守相關措施及標準。自動化決策依據韓國個資法第 37 條之 2 規定，係指透過完全自動化之系統（包括應用 AI 技術之系統）處理個人資料以進行決策。

2024 年 3 月，PIPC 對南韓個人資料保護法施行令（Enforcement Decree of the Personal Information Protection Act, PIPA Enforcement Decree，下稱施行令）進行修訂，本次修訂是為落實 2023 年對韓國個資法之修法，當中包含第 37 條之 2 關於自動化決策之規定。本次指引即是在施行令修正後，進一步說明如何實踐韓國個資法及施行法修訂對自動化決策規範之要求。指引中提醒，並非所有自動化系統所為之決策即為自動化決策，事業仍須就個案檢視其是否符合自動化決策之定義。若在作成最終決策前已有人為判斷介入，則該決策即可能不屬於自動化決策，指引中提供判斷自動化決策時需考量之事項以及「自動化決策自我診斷表」供事業運用。

於進行自動化決策之情況下，事業或組織必須依照當事人依法行使權利採取以下措施：

1. 當當事人要求對自動化決策說明時，事業或組織應選擇並提供當事人有幫助且有意義的資料。此外，當事人若對其自動化決策結果提出意見，事業或機構必須進行審查與評估並將結果告知當事人。在說明涉及演算法或機器學習之過程，事業及組織須向當事人提供簡潔且有意義之資訊，而非複雜的

本報告之智慧財產權歸屬於國發會

數學說明。換言之，必須以人類可以理解之方式解釋 AI 模型之演算過程。

2. 若當事人因自動化決策對其權利或義務產生重大影響且當事人依法拒絕該決策時，事業或組織應立即停止使用該決策，並將處理結果告知當事人。惟若自動化決策已於事前以契約等方式告知當事人或有法律明確規定時，當事人不得拒絕，僅能要求事業或組織進行說明或審核。而在重大影響之判斷上，應考慮是否涉及當事人生命、身體安全相關之權利或義務，以及是否會持續或有無恢復之可能等。

3. 事業或組織在進行自動化決策時，需事先於其網站上公開相關標準以及程序，以利當事人查閱。同時，為使當事人易於瞭解，應揭露具體之權利行使方法以及程序。

韓國個資保護委員會表示，會持續推廣並提供指導以利新政策能順利實踐。

資料來源：

1. 개인정보보호위원회,자동화된 결정에 대한 정보주체의 권리 안내서, 2024-09-26, https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=10611 (last visited 2024-10-07)

五、 澳洲

(一)2024 年 6 月澳洲財務部發布《保證政府 AI 之國家框架》

2024 年 6 月 21 日澳洲財務部（Department of Finance）於資料及數位部長會議（Data and Digital Ministers Meeting , DDMM），經過聯邦、州以及領地政府同意，發布《保證政府 AI 之國家框架》（National framework for the assurance of artificial intelligence in government，下稱

本報告之智慧財產權歸屬於國發會

框架），各州及領地政府(state and territory governments)一致同意在透過 AI 執行政策或提供服務時應優先考慮人民權利、福祉及利益。澳洲產業、科學暨資源部（Department of Industry, Science, Energy and Resources，下稱資源部）部長表示，各形式及規模之政府將需要使用 AI 以提升工作效率，因此確保大眾信任政府所使用之科技極為重要。

基於 2019 年資源部發布之 AI 倫理原則（Australia’s AI Ethics Principles），該框架旨在促進政府安全且負責任的使用 AI。為保障政府如何使用 AI，擴大治理範圍乃為重要一環，該框架僅建立原則，為各司法管轄之特殊需求提供彈性。各司法管轄可以此框架為基礎，根據自身法律、政策及執行背景制定具體政策及指令。各州及領地政府於 AI 保障實踐及改進政策亦將在未來納入該框架中。

該框架共包含人類、社會及環境福祉（Human, societal and environmental wellbeing）、人本價值（Human-centred values）、公平性（Fairness）、隱私保護及安全（Privacy protection and security）、可靠性及安全性（Reliability and safety）、透明度及可解釋性（Transparency and explainability）、可爭論性（Contestability）及當責（Accountability）八個主題，其中第四主題「隱私保護及安全」涉及個人資料保護，該部分內容如下：

1. 遵循隱私法制政策之義務：政府須確保對 AI 系統之使用，符合有關個人資料之同意、蒐集、儲存、使用、揭露以及保有之法律規範，包括當 AI 系統進行個人資料蒐集或個人資料被用於其他目的時（如用於訓 AI 系統訓練）需告知當事人。同時必須採取「隱私始於設計」（privacy by deign）原則並進行「隱私影響評估」（privacy impact assessments）。

2. 資料運用最小化並保護個人資料：政府須評估每一使用 AI 之事例，於蒐集、利用及揭露個人資料時皆具備必要性及合理性，並須符合比例原則。政府應考慮透過合成資料、資料匿名

本報告之智慧財產權歸屬於國發會

化及去識別化、加密、安全聚合（secure aggregation）等隱私強化技術以減少個人資料保護風險，同時須特別注意特種資料之管理。

3. 保護系統及資料：政府應確保每一 AI 使用之事例，都符合資料安全及資料保護法規，並確保對於系統、應用程式以及資料庫之使用，限於依職權所需並經授權之人員，若有必要，並須尋求領域相關專家之建議。對於安全層面之措施，則應將過往澳洲政府曾經訂定之相關安全指導、策略或指引納入考量，包括 2023 年公布之「2023-2030 澳洲網路安全戰略」（2023-2030 Australian Cyber Security Strategy）、內政部公布之「託管認證架構」（Hosting Certification Framework）、澳洲信號局（Australian Signals Directorate, ASD）2024 年公布之「參與 AI 指引」（Engaging with Artificial Intelligence）以及「部署 AI 系統之安全報告」（Deploying AI Systems Securely）、與 2023 年總檢察長部（Attorney-General’s Department）公布之「應對內部威脅：澳洲政府指引」等。

資料來源：

1. National framework for the assurance of artificial intelligence in government, 2024-06-21, https://www.finance.gov.au/sites/default/files/2024-06/National-framework-for-the-assurance-of-AI-in-government.pdf (last visited 2024/09/04)

2. National Framework for Artificial Intelligence in Government Joint Media Release, 2024-06-21, https://ministers.finance.gov.au/financeminister/media-release/2024/06/21/national-framework-artificial-intelligence-government (last visited 2024/09/04)

本報告之智慧財產權歸屬於國發會

(二)2024 年 9 月澳洲政府發布《2024 年隱私權暨其他立法修正案法案》，提交至澳洲議會

2024 年 9 月澳洲政府發布《2024 年隱私權暨其他立法修正案法案》（the Privacy and Other Legislation Amendment Bill 2024），提交至澳洲議會。國會議員 The Hon Mark Dreyfus KC MP 於本法案二讀演講稿表示，數位經濟帶來巨大利益，蒐集與儲存大量個人資料將增加隱私風險。於網路分享資料及監管資料之人，須有足夠靈活及敏捷的法律框架保護與適應科技之變化，現行《1988 年隱私權法》已不足以支撐當前之數位科技，導致數位生態系運作過程之大量資料流通（data flows）可能產生重大之危害，例如：重大資料外洩，洩漏個人敏感資料，使個人面臨身分詐欺與詐騙的風險。為因應當前數位科技時代，澳洲政府發布此修正案，透過此法案，確保個人隱私得到尊重及保護。

此次修正法案分為三部分：

1. 修訂《1988 年隱私權法》，提高其有效性，加強隱私監管機構的執法權力，促進安全的跨國資料流通，制定《兒童網路隱私權法》（Children’s Online Privacy Code），簡化緊急情況及符合條件之資料外洩後的資訊分享（information-sharing），並於組織/實體（entity）使用涉及個人資料之自動化重大決策時，要求提升透明度。

   (1) 監管機構執法權力：

   此法案擴大資訊委員執行法案的監管權力，提供廣泛的執法選項，包括於輕微隱私侵犯行為之民事處罰及侵權通知，以及針對調查複雜之侵害隱私行為，提供資訊專員所須額外之權力，包括搜索及扣押。

本報告之智慧財產權歸屬於國發會

授權法院於確定特定組織/實體（entity）違反民事處罰條款時，可命令該組織/實體賠償個人所受的損失或損害。

本法案擴大監督及評估功能，加強資訊委員能力。新增公共調查權，使資訊委員依據指示或批准調查特定事項，對隱私權威脅進行更密切的監督，包括系統性問題。

(2) 跨國資料流通：

跨國資料流通對於全球國際貿易及服務至關重要，為保護資料的自由流通，此法案草擬與澳洲相似資料隱私法國家之規定，事業及個人能更加確信個人資料的安全，並降低與跨國事業簽訂契約及協議之業務成本。

(3) 兒童隱私：

兒童於網路環境受隱私權侵害風險較成人高，此法案制定《兒童網路隱私權法》，適用於兒童可能存取的社交媒體和其他網路服務，規定須如何遵守與兒童有關的隱私權義務，並與英國等國家之類似法規保持一致，交由澳洲資訊委員辦公室（Office of the Australian Information Commissioner）制定。

(4) 個人資料外洩與緊急情況後的資訊分享聲明：

個人資料外洩使面臨詐欺、身分盜竊及詐騙之風險，本法案將實施技術及組織控制，例如：加密資料與培訓員工進行資料保護，解決資料外洩之風險。新增符合條件的資料外洩聲明，聲明允許於通報資料外洩後分享個人資料，防止或降低對個人造成傷害的風險，例如：於此情況分享個人資料，使銀行等實體能夠迅速採取行動，防止濫用。聲明設有保障措施，確保用於「與防止或降低因資料外洩

本報告之智慧財產權歸屬於國發會

而濫用個人資料，對個人造成傷害風險」相關之目的，並明確分享個人資料類型以及分享對象。

依據本法案發布的緊急聲明，於災難或緊急情況發生後分享個人資料，要求緊急聲明明確分享個人資料的類型、允許分享資料的實體類型以及分享資料的目的，確保個人隱私受到保護。

(5) 自動化決策：

確保自動化決策之安全與負責任的開發及部署，使系統提高決策的效率、準確性及一致性。此法案針對嚴重影響個人利益之自動決策例用個人資料時，要求組織/實體須提高透明度，並告知個人其使用的個人資料類型。此一要求適用於完全或部分之自動化的決策機制，以防止規避。

2. 新增法定侵權行為，為嚴重侵害隱私的行為提供補救措施

本法案將提供「隱私權受到嚴重侵害之個人」法定侵權行為與法定訴訟理由，並將補充《1988 年隱私權法》，確保個人擁有對嚴重侵害其隱私權之個人或組織/實體尋求法律救濟之權利。嚴重侵害隱私權訴訟理由，無論是物理性侵入個人私人空間，或濫用個人資料，原告無需證明其損害係因侵害隱私權造成，其損害為評估侵害嚴重性及授予的補救措施，包括非經濟損失的賠償或要求被告向原告道歉的命令。

於權衡公共利益，原告須證明保護其隱私權之公共利益超過被告提出的任何競爭性公共利益。被告之侵害行為，若為法律規定或授權，或對生命、健康或安全的嚴重威脅而有必要，即有抗辯權。本法案規定侵權責任的豁免，包括新聞業、執法機構及情報機構，為保護新聞自由及確保政府有效進行合法活動。

本報告之智慧財產權歸屬於國發會

3. 修訂《1995 年刑法》(the Criminal Code 1995)，新增「人肉搜索」(doxing）之刑事犯罪

本法案修訂《1995 年刑法》，新增新的刑事犯罪，以威脅或騷擾的方式洩露個人資料之行為，稱為「人肉搜索」，因社群媒體及網路平臺之盛行，增加惡意獲取個人資料並發布於網路的能力，使受害者遭受重大的傷害，對受害者及其家人朋友之生命和安全造成威脅，亦造成重大心理傷害。

資料來源：

1. Privacy and Other Legislation Amendment Bill 2024, 2024-09-12, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7249 (last visited 2024/10/07)
2. Attorney-General's Department, Second reading speech – Privacy and Other Legislation Amendment Bill 2024, 2024-09-12, https://ministers.ag.gov.au/media-centre/speeches/second-reading-speech-privacy-and-other-legislation-amendment-bill-2024-12-09-2024 (last visited 2024/10/07)

陸、 競爭法制

一、 國際合作

(一)2024 年 7 月美國、歐盟和英國的主要競爭執法機構發布生成式 AI 基礎模型及 AI 產品競爭之聯合聲明

2024 年 7 月 23 日美國聯邦交易委員會（FTC）和司法部（Department of Justice, DOJ)、英國競爭及市場管理局（Competition and Markets Authority, CMA）以及歐盟執行委員會的主要競爭執法機構發布生成式 AI 基礎模型及 AI 產品競爭的聯合聲明(Joint Statement on Competition in Generative AI Foundation Models and AI Products)，概述 AI 生態系統中的風險以及保護和促進競爭的共同原則。

本報告之智慧財產權歸屬於國發會

參與聯合聲明之競爭法主管機關表示，基於 AI 變革發展之潛力，以及其發展可能對人民帶來利益，並促進創新與經濟成長，需於各自法律之引導下，努力確保 AI 發展之有效競爭；同時須自數位市場競爭之經驗中汲取教訓，利用各自現有權力適切處理 AI 發展可能之風險，避免造成不可逆轉之損害。聲明當中提出之競爭風險與共同原則摘述如下：

AI 生態系之競爭風險：

1. 集中控制關鍵輸入：專用晶片、算力、大數據及專業技術是開發 AI 基礎模型之關鍵。關鍵要素的控制力，可能會使少數事業有機會利用現有或新興的瓶頸，於 AI 堆疊（the AI stack）中取得優勢，並對相關工具未來之發展產生極大影響。同時也可能限制顛覆性創新之範圍，使事業得以僅為自身利益進行創新，而對公眾利益或市場競爭產生損害。

2. 鞏固或擴大 AI 相關市場的市場力量：大型數位公司已經享有強大的累積之優勢與市場力量，因而有能力防範 AI 驅動之破壞，或利用其特殊優勢，包括控制 AI 或 AI 驅動服務可向個人或事業銷售或提供之管道，以擴大或鞏固其於技術變革過程之地位，並對未來競爭造成損害。

3. 涉及關鍵參與者的安排可能會放大風險：雖然與生成式 AI 相關事業的投資與合作關係非常普遍，於某些情況下不一定會有損害競爭。然而，投資或合作關係可能會被大型事業用以削弱或限制競爭威脅，為自身利益控制市場，以致對公眾利益造成損害。

保護 AI 生態系競爭之原則：

本報告之智慧財產權歸屬於國發會

1. 公平交易（Fair dealing）：擁有市場競爭力之事業若採取排他策略，可能阻礙第三方之投資與創新並破壞競爭。因此愈多事業遵守公平交易原則，對 AI 生態系發展愈有助益。

2. 互通性（Interoperability）：AI 產品和服務及其投入越是能夠互通操作，AI 的競爭和創新越大，故主張需要犧牲隱私和安全性才能達到的互通性，須受到嚴格審查。

3. 選擇(Choice)：多樣化的產品和商業模式將使事業和消費者受益，故應檢視事業是否採用限制事業或個人選擇之鎖定機制（lock-in），而可能會阻止事業或個人尋求其他選擇。亦應檢視現有事業與新進事業間之投資與合作夥伴關係，確保相關協議不會規避事業結合之執法，或以破壞競爭的方式賦予現有事業不當之影響或控制。對內容創作者而言，買家的選擇可能限制賣方獨占力（monopsony power）之行使，並進一步損害思想市場中資訊的自由流通。

資料來源：

1. Joint Statement on Competition in Generative AI Foundation Models and AI Products, 2024-07-23, https://www.ftc.gov/legal-library/browse/joint-statement-competition-generative-ai-foundation-models-ai-products(last visited 2024/08/08)

2. Joint Statement on Competition in Generative AI Foundation Models and AI Products , 2024-07-23 , https://www.ftc.gov/system/files/ftc_gov/pdf/ai-joint-statement.pdf (last visited 2024/08/08)

3. Top Competition Enforcers in the US, EU, and UK Release Joint Statement on AI Competition – AI: The Washington Report, 2024-08-02, https://www.mintz.com/insights-center/viewpoints/2191/2024-08-01-top-competition-enforcers-us-eu-and-uk-release-joint (last visited 2024/08/08)

本報告之智慧財產權歸屬於國發會

柒、 網路/資訊安全與韌性

一、 美國

(一)2024 年 8 月美國紐約州總檢察長辦公室發布《禁止提供兒童成癮性內容法案》及《兒童資料保護法案》的擬議規則制定通知

2024 年 8 月美國紐約州總檢察長辦公室（Office of the Attorney General, OAG）發布《禁止提供兒童成癮性內容法案》（the Stop Addictive Feeds Exploitation (SAFE) for Kids Act）及《兒童資料保護法案》（the Child Data Protection Act, CDPA）的擬議規則制定通知（Advance Notice of Proposed Rulemaking, ANPRM），前者旨在限制使人成癮之社群媒體功能，使未成年人免受其侵害；後者旨在限制使用 18 歲以下之未成年人之個人資料與隱私，為保障未成年人的網路安全及隱私，徵求公眾評論意見。

由於社群媒體成癮造成未成年人心理健康危機。立法機關發現，社群媒體公司透過追蹤使用者在社群媒體留下的數萬或數十萬個資料點，以演算法建立並提供（feed）個人化內容，創造完美的媒體串流。未成年人自我控制能力與成人相比較弱，容易受到使人成癮內容的影響，並增加未成年人罹患憂鬱症、焦慮症、自殺念頭和自我傷害比例。為解決此公共健康危機，OAG 制定《禁止提供兒童成癮性內容法案》，禁止社交媒體平臺向未成年人提供使人成癮的內容，立法機關發布立法的三面向：

1. 以商業上合理及可行之技術方法，測試社群媒體平臺之使用者年齡是否為未成年人。

2. 社群媒體平臺須獲得可驗證之家長同意，才能向未成年人提供使人成癮的資訊。

3. 平臺方需使用紐約常見之多種語言或方言請求家長同意。

本報告之智慧財產權歸屬於國發會

OAG 並針對下列問題，徵求公眾意見評論:

1. 商業上合理及技術上可行的年齡測定方法。

2. 如何驗證家長同意。

3. 使人成癮之社群媒體範圍。

4. 用戶偏好設定,是否存在特定之用戶隱私選項或無障礙設定,或媒體推薦、選擇或優先排序之技術資訊，應被明確排除於 SAFE 法案之成癮內容限制。

5. 平臺方需使用紐約常見之多種語言或方言，請求家長同意。

6. 成癮性資訊對未成年人之危害以及防止危害之保障措施的一般評論。

兒童個人資料保護法之制定目的為確保 18 歲以下之未成年人個人資料隱私與安全，適用於控制個資處理目的和方法的網站、線上服務或應用程式、行動應用程式、連接裝置之經營者，並於業者知悉未成年人的使用者或主要針對未成年人為線上服務之業者時，限制其蒐集處理未成年人的個人資料。惟於《聯邦兒童線上隱私權保護法》（the federal Children’s Online Privacy Protection Act）適用於 13 歲以下或 13 歲至 17 歲之間的未成年人，業者或第三方得於絕對必要之特定目的或獲得使用者知情同意下，處理未成年人之個人資料，例如：於防止惡意、詐欺或非法活動情形。立法機關針對下列問題，徵求公眾意見評論：

1. 未成年人的定義。

2. 個人資料的範圍。

3. 銷售個人資料範圍。

4. 允許處理個人資料之目的。

本報告之智慧財產權歸屬於國發會

5. 知情同意。

6. 家長同意。

評論意見持續徵集至 2024 年 9 月 30 日，《禁止提供兒童成癮性內容法案》於 OAG 發布法規後 180 天生效，《兒童資料保護法案》於 2025 年 6 月 20 日生效。

資料來源：

1. Protecting Children Online, 2024-08-01, https://ag.ny.gov/resources/individuals/consumer-issues/technology/protecting-children-online (last visited 2024/08/26)

2. SAFE for Kids Act, 2024-08-01, https://ag.ny.gov/sites/default/files/2024-08/safe-forkidsact.pdf (last visited 2024/08/26)

3. Child Data Protection Act, 2024-08-01, https://ag.ny.gov/sites/default/files/2024-08/child-data-protection-act.pdf (last visited 2024/08/26)

4. New York AG Seeks Comments on Rulemaking for Minors' Online Protection Laws, 2024-08-12, https://www.alstonprivacy.com/new-york-ag-seeks-comments-on-rulemaking-for-minors-online-protection-laws/?cn-reloaded=1 (last visited 2024/08/26)

二、韓國

(一)2024 年 8 月韓國修正之資訊通訊網路法正式施行，增加侵權事件通報程序等細節及相關罰則

韓國資訊通信網路利用促進及資訊保護法（정보통신망 이용촉진 및 정보보호 등에 관한 법률），簡稱資訊通訊網路法（약칭:정보

本報告之智慧財產權歸屬於國發會

통신망법）。該法於 2024 年 2 月修正之條文，已於同年 8 月正式施行。

此一資訊通訊網路法制定於 1986 年 5 月，並於 1987 年 1 月施行，共 10 章 76 條。其立法目的為促進韓國之資訊通信網路利用，及保護資訊通信網路之使用者，形塑健康、安全之使用環境，為改善人民生活與公共秩序做出貢獻（資訊通訊網路法第 1 條參照）。

該法目前規範重點包含：總則，如資訊通訊網路之定義；促進資訊通信網路利用，如標準化與相關認證；形塑健康、安全之使用環境，如身分驗證；以及保障資訊通信網路之使用者，如青少年保護等。2024 年主要修正第 48 條之 3 與第 48 條之 4 涉及侵權事件之通報細節，如程序、根因分析，及第 73 條、第 76 條之相關罰則。茲摘要說明如下：

1. 第 48 條之 3：本次主要新增該條第 4 項，關於侵權事件之報告時間、方式、程序等事項另行訂定。爰主管機關（科學技術情報通訊部）新增該法施行令（정보통신망 이용촉진 및 정보보호 등에 관한 법률시행령）第 58 條之 2，資訊通訊網路服務提供者通報時，應說明侵權事件發生日期、具體時間、原因及損害情形；該業者對於此一侵權事件之因應情形，包含採取之措施；以及該業者之窗口與聯繫方式等內容。

2. 第 48 條之 4：本條為此次修正核心，除該條第 1 項外，第 2 至 8 項皆有修正。如除資訊通訊網路服務提供者之通報外，韓國科學技術情報通訊部應分析該侵權事件之根因，制定防止損害擴大之措施，進行事件應變、復原，及防止相關事件再度發生，並要求業者採取必要措施（該條第 2 項參照）。此外，科學技術情報通訊部首長尚可就業者改善情形進行檢查，或要求業者保存相關資訊，或於必要時提供資訊，或組成公、私調查小組進入該業者之場所，對侵權事件進行調查等（該條第 3 至 6 項參照）。

本報告之智慧財產權歸屬於國發會

3. 第 73 條：本次為罰則之修正，規範未依第 48 條之 4 第 5 項規定保存相關資訊者，可處兩年以下有期徒刑，或 2,000 萬韓元以下之罰金。

4. 第 76 條：本次為罰則之修正，規範未依第 48 條之 3 第 1 項通報，或未依第 48 條之 4 第 3 項之要求進行改善者，可處 3,000 萬韓元以下之罰金。

資料來源：

1. 과기정통부（Ministry of Science and ICT）, 사이버 침해사고 대응의 실효성을 높이기 위한 「정보통신망법」 개정안 시행, 2024-08-13, https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=238&pageIndex=1&bbsSeqNo=94&nttSeqNo=3184817&searchOpt=ALL&searchTxt= (last visited 2024/08/21)
2. 법제처, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 2024-02-13, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EB%A7%9D%EC%9D%B4%EC%9A%A9%EC%B4%89%EC%A7%84%EB%B0%8F%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%93%B1%EC%97%90%EA%B4%80%ED%95%9C%EB%B2%95%EB%A5%A0 (last visited 2024/08/21)
3. 법제처, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령, 2024-08-13, https://www.law.go.kr/LSW//lsLinkCommonInfo.do?lspttninfSeq=189991&chrClsCd=010202 (last visited 2024/08/21)

(二)2024 年 9 月韓國發布新聞，說明其將主導制定憑證信任技術與虛實整合（元宇宙）相關之 4 項 ITU-T 標準

韓國科技部（Ministry of Science and ICT）於 2024 年 9 月 9 日發布新聞，說明韓國政府將主導制定憑證信任技術與虛實整合（元宇宙）

本報告之智慧財產權歸屬於國發會

相關之 4 項國際電信聯盟電信標準化部門（ITU Telecommunication Standardization Sector, ITU-T）的國際標準。

這 4 項新興技術標準之提案預計在 2025 至 2028 年的 ITU-T 相關會議內討論，包含：1. 去中心化憑證信任技術，可用於數位簽章與相關憑證。2. 虛實整合環境內之個人資料保護技術，可保護使用者之肖像權（如頭像）。3. 基於區塊鏈技術所開發之工業物聯網內，被運用在智慧製造資料之安全需求。以及 4. 運用分散式帳本技術（Distributed ledger Technology, DLT）核發文件之安全需求。

按國際電信聯盟（International Telecommunication Union, ITU）標準之制定流程，需先由相關會議核准新興技術標準之提案，接續開始制定該標準。而該標準通過後經試行，並被 ITU 成員國接受，最後經 ITU 批准，才能成為正式之國際標準。韓國政府前述 4 項提案，係在 2024 年 9 月 2 日至 6 日在瑞士日內瓦舉辦之 ITU-T 資訊安全會議（SG17－Security）內提出，業經來自 54 個 ITU 成員國與近 330 位專家討論後，已獲批准，將進行後續之國際標準研擬與其他程序。

韓國除在 ITU-T 資訊安全會議內提出憑證信任技術與虛實整合（元宇宙）相關標準之 4 項提案外，先前在該會議內也主導例如：汽車邊緣運算之安全需求與指引（ITU-T X.1384, Security requirements and guidelines for vehicular edge computing）、運用於監控線上分析服務之參考資料（ITU-T X.1471, Reference monitor for online analytics services）等 5 項標準，皆獲 ITU 批准，已成為正式之國際標準。

ITU-T 相關進展被韓國政府視為在資訊安全領域內，彰顯國際合作之成果。因為目前網路威脅已無法透過單一國家解決，需要各國相互合作。且憑證信任技術與虛實整合相關標準可實現韓國成為數位強國之目標，韓國政府將盡最大努力確保次世代安全標準之制定，以鞏固該國之領導地位。

資料來源：

本報告之智慧財產權歸屬於國發會

1. 과기정통부（Ministry of Science and ICT）,자격증명신뢰기술, 메타버스 보안 등 정보보호 ITU-T 국제표준 우리나라 주도 개발, 2024-09-09, https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=238&pageIndex=1&bbsSeqNo=94&nttSeqNo=3184901&searchOpt=ALL&searchTxt= (last visited 2024/09/18)
2. ITU, SG17 – Security, 2024-09-02, https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx (last visited 2024/09/18)

三、 聯合國

(一)2024 年 8 月聯合國特設委員會通過打擊網路犯罪公約，並提請聯合國大會批准，建立全球打擊網路犯罪的綜合框架

2024 年 8 月聯合國特設委員會（Ad Hoc Committee）通過打擊網路犯罪公約（Convention Against Cybercrime），並提請聯合國大會（United Nations General Assembly）核可，此公約若經 40 個會員國批准，即將生效。此公約主要係聯合國關注到使用資訊及通訊技術系統對刑事犯罪的規模、速度和範圍產生重大影響，有必要作為優先事項，推行保護社會免遭網路犯罪侵害之全球刑事司法政策，建立全球打擊網路犯罪的綜合框架，通過立法，建立犯罪態樣、司法程序和技術援助和資訊交換，促進國際合作，加強施行措施，有效地預防及打擊網路犯罪，並同時確保基本人權及自由權的尊重、個人隱私不受非法或任意干涉，以及保護個人資料。下列為此公約重點：

1. 網路犯罪態樣：要求各國通過立法將特定網路活動定為刑事犯罪，包含非法存取資訊及通訊技術系統、非法攔截資料、資料干擾、系統干擾、濫用施行網路犯罪之設備。希望各國解決與網路犯罪相關的問題，包含透過資訊和通訊技術系統詐欺、

本報告之智慧財產權歸屬於國發會

偽造身分，及製作、提供、銷售、散布、傳輸、廣播、展示、出版或以其他方式提供有關兒童性虐待或兒童性剝削素材。

2. 制定執法程序：設立、執行和適用條文及保障措施，根據國際人權法保護人權，納入比例原則。調查網路犯罪當資料有遺失或竄改的風險時，採取加速儲存數位資料措施，為方便即時蒐集和截取流量和內容資料，使執法機構能快速、有效從服務提供者處獲取資料，旨在確保執法機構擁有有效的調查和起訴網路犯罪所需的工具。

3. 國際合作：利用國際合作機制於遵守個人資料保護情況下，以數位形式跨境取得及分享證據，建立締約國全天 24 小時聯絡窗口，以便刑事調查單位即時蒐集數位證據，快速保存數位資料，並促進各國之間的資料交換，支援正在進行的調查程序。

4. 技術援助及資訊交流：為增強各國預防、發現和應對網路犯罪的能力，締約國應根據各自的能力或使用現代科技及技術，提供最廣泛的技術援助及能力建設措施打擊網路犯罪，包括制定及規劃預防與打擊網路犯罪之策略政策、實施培訓計畫、交流專業知識以及分享實務經驗。

資料來源：

1. Draft United Nations convention against cybercrime, 2024-08-07, https://documents.un.org/doc/undoc/gen/v24/055/06/pdf/v2405506.pdf (last visited 2024/08/29)

2. Countries Poised to Adopt New Cybersecurity Measures After UN Adopts Major Cybercrime Convention, 2024-08-16 , https://www.jdsupra.com/legalnews/countries-poised-to-adopt-new-6575926/ (last visited 2024/08/29)

本報告之智慧財產權歸屬於國發會

捌、 智慧財產

一、 韓國

(一)2024 年 8 月韓國政府公布大型語言模型等 AI 出現後，衍生之智慧財產權問題因應措施之研究報告

韓國於 2024 年 8 月 20 日發布新聞，有鑑於近期生成式 AI 與其他相關 AI 之應用，對智慧財產權之議題帶來許多討論與影響，如專利、著作權。為此，韓國總統府下之智慧財產權委員會，出版「大型語言模型等 AI 出現後智慧財產權問題因應措施研究（초거대 인공지능 등장에 따른 지식재산 쟁점 대응방안 연구）」報告。

該報告共有 5 章：緒論、大型語言模型與相關 AI 之影響、國內外趨勢、對智慧財產權之挑戰以及結論。說明 2022 年底 ChatGPT 問世後，帶動生成式 AI 與相關應用之風潮，大型語言模型（large language model, LLM）相關技術趨勢，包括文字、影像、聲音及影片創造等生成式 AI 應用現況與發展前景，與對於智慧財產權之管理、公共服務、醫療保健、金融等領域之影響。

該報告同時介紹國內外 AI 相關趨勢，如韓國刻正研擬制定兼顧促進產業與建立秩序之 AI 戰略與政策，另如美國、英國、日本及中國大陸，也都陸續進行相關法律、政策或戰略之研擬，或是積極鼓勵 AI 技術之研發。同時說明由於 AI 之興起，對智慧財產權帶來許多影響與挑戰，例如：訓練生成式 AI 之資料，涉及既有著作權規範，是否需要調整機制等。韓國政府陸續於 2023 年 9 月、2024 年 3 月及同年 4 月，分別針對生成式 AI 產業、對創作與廣播領域、對智慧財產權、AI 治理與法律體系，及對音樂等領域不同利害關係人之意見，並於該報告彙整與分析重點。

韓國於該報告之結論提出，隨著生成式 AI 之發展，如何防止深度偽造技術、網路爬蟲、或連結個人資料，甚至影響相關資訊之公開權、

本報告之智慧財產權歸屬於國發會

或是個人之肖像權等，都是新興的挑戰。且世界各國都在鼓勵 AI 技術與產業發展，故除重申 AI 時代智慧財產權之重要性外，並應與時俱進調整既有智慧財產權規範或相關技術，例如結合修法（例如增修文字與資料探勘（Text and Data Mining, TDM）規範）或提供參考指引；而韓國也預計於 2024 年下半年提出 AI 相關政策，以符需求。

資料來源：

1. 과기정통부（Ministry of Science and ICT）, 초거대 인공지능과 지식재산의 도전 과제, 2024-08-20, https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=238&pageIndex=&bbsSeqNo=94&nttSeqNo=3184832&searchOpt=ALL&searchTxt= (last visited 2024/08/28)
2. 국가지식재산위원회（Presidential Council on Intellectual Property）, 초거대 인공지능 등장에 따른 지식재산 쟁점 대응방안 연구, 2024-08-20, https://www.ipkorea.go.kr/board/articleDetail.do?bbsId=BBSMSTR_000000000009&nttId=20656&pageIndex=1&searchCnd=0&category=POLICY_RESEARCH (last visited 2024/08/28)

本報告之智慧財產權歸屬於國發會

項次 5. 十二月雙月報

壹、 資料治理

一、 英國

(一)2024 年 10 月英國政府向國會提出《資料利用與近用法》草案，預計將促進英國經濟成長並改善公共服務效能

英國創新科技部（Department for Science, Innovation and Technology, DSIT）於 10 月 24 日發布新聞稿，說明已提出《資料利用與近用法》草案（Data Use and Access Bill）提交國會審議。其新聞稿指出，該法案將釋放資料之力量以發展經濟並改善人民生活。此法案若通過，預計將利用資料之力量，促進應國整體經濟成長達 100 億英鎊，並可減少數百萬名英國警察，及國家醫療服務系統（National Health Service, NHS）工作人員之工時。

首先在改善公共服務部分，以英國警察為例，過往需要在警方資料庫內查找犯罪嫌疑人或可疑對象時，需要配合一些行政管理程序，包括手寫紀錄之要求。然而，透過該法案之規範，將可適度放寬行政程序之要求，預計為英國警方節省每年 150 萬小時之工時，讓警察們擁有更多打擊犯罪的時間。

再以 NHS 為例，該法案讓 NHS 醫療機構、診所或救護車等服務機構，可即時存取醫療資訊，如病患之過往病史、預約或檢查狀況。且要求醫療機構之資訊服務業者，應確保其資訊系統可符合跨系統資料存取之標準，以落實資訊共享。此一方式將可為 NHS 工作人員節省每年 14 萬小時之工時，並可讓病患獲得更快速之照護。

而在發展經濟層面，該法案將資料共享明文化，預計可在 10 年內為英國經濟帶來 100 億英鎊之成長。舉例而言，透過該法之規範，將使金融（如開放銀行）或能源（如下水道或能源管線）等領域內可合法進行資料共享，並有機會運用相關資料尋求更佳之交易模式，有助

本報告之智慧財產權歸屬於國發會

減少能源之利用，或降低能源管道事故發生之可能性等。以下水道管線為例，若相關事業可以清楚地知道管線的位置，將有效減少挖斷管線或其他公共安全事故之發生，預計每年可省下約 24 億英鎊的意外損失。

於人民生活層面，該法案將數位驗證服務（digital verification services）法制化，使得提供身分驗證服務之事業得以取得政府認證，獲得信賴標章（trust mark）。此一標章之授予，將有助於民眾選擇可信任之身分驗證工具或服務，也促使英國民眾從出生到死亡之相關登記事務，不再需要進行紙本作業，而皆可透過數位驗證服務進行。

最後該法案並賦予研究人員得以近用網路資料之權利，包括數位平臺持有之數據，使其得以對於網路危害等問題進行研究以有效解決網路危害之相關問題。

資料來源：

1. DSIT, New data laws unveiled to improve public services and boost UK economy by £10 billion, 2024-10-24, https://www.gov.uk/government/news/new-data-laws-unveiled-to-improve-public-services-and-boost-uk-economy-by-10-billion (last visited 2024/11/06)

二、韓國

(一)2024 年 10 月韓國與歐盟召開國際資料合作研討會，討論資料價值鏈合作，韓國並宣布成立公私資料聯盟，促進國內資料互通與應用

韓國科學技術情報通訊部（과기정통부）於 10 月 15 日發布新聞稿，說明該部與韓國情報資訊社會振興院（한국지능정보사회진흥원，

本報告之智慧財產權歸屬於國發會

下稱 NIA）將共同促進韓國與歐盟間之資料合作，並舉辦韓國與歐盟國際資料合作研討會（한-유럽연합 국제 데이터 협력 토론회）。

由於近年生成式 AI 與相關應用之發展，資料之重要性也日益增加，已被視為支持新興產業與國家安全之國家戰略資產。除市場最大之美國外，全球第二大資料市場之歐盟並透過資料戰略（European strategy for data）相關法制與措施之落實，推動資料共享與相關事宜；日本與中國大陸也刻正推動跨產業資料串聯與利用之基礎。

目前韓國科學技術情報通訊部正在尋求與歐盟 Gaia-X 合作，旨在加強韓國資料生態系之能量。本次國際資料合作研討會除安排 Gaia-X 執行長與歐盟相關組織，如德國聯邦經濟與能源部之代表進行分享外，NIA 也分享建立韓國國家資料庫之進展，並於會議中廣泛討論韓國與歐盟在 AI、資料及以網際網路為基礎之資源共享、涉及之資訊與通訊科技領域間之合作、以及國際資料規範與標準化等內容。

研討會後，科學技術情報通訊部宣布成立跨部會之國家資料委員會（聯盟）（국가 데이터 협의체(얼라이언스)）。該委員會（聯盟）由科學技術情報通訊部主導，成員還包含中小企業與教育等相關部會。此外，韓國產業界、學術界及研究界亦有代表共同參與，將討論如何促進資料互通性，並建置各領域資料之線上平臺。

此一聯盟除透過公、私協力促進資料互通與共享外，亦將與歐盟 Gaia-X 合作，期望透過韓國與歐盟透過相關資料生態系之密切合作，為國際資料經濟之發展作出重大之貢獻。

資料來源：

1. 과기정통부（Ministry of Science and ICT）, 「한-유럽연합 국제 데이터 협력 토론회」 개최 / 국제 데이터 가치 사슬 참여를 위한 협력 본격화, 2024-10-15, https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=238&pageIndex=1&bbsSeqNo=94&nttSeqNo=3185005&searchO

本報告之智慧財產權歸屬於國發會

pt=ALL&searchTxt= (last visited 2024/10/23)

三、 中國大陸

(一)2024 年 11 月中國大陸國家網路資訊辦公室發布《全球資料跨境流通合作倡議》

中國大陸主席於 2024 年 11 月 16 日在亞太經合組織第三十一次領導人非正式會議提出，為與各方深化合作，促進高效、便利及安全之資料跨境流通，後續將發布《全球資料跨境流通合作倡議》。同月 20 日中國大陸國家網路資訊辦公室隨即發布《全球資料跨境流通合作倡議》。

該倡議提出，資料跨境流通對於各國電子商務、數位貿易乃至經濟科技文化等諸多方面至關重要，不僅可以有效降低貿易成本，提高企業開展國際貿易的能力，更有助於促進貿易便利化，並加速產業數位轉型，彌合數位鴻溝，實現以資料流為牽引的新型全球化。資料安全為全球議題，國際間正在積極探索以形成全球數位領域之規則與秩序，如：聯合國發布《全球數位契約》（Global Digital Compact）、世界貿易組織之電子商務談判、《跨太平洋夥伴全面進步協定》（CPTPP）以及《數位經濟夥伴協定》（DEPA）等多邊實踐，這些實踐均體現推動全球資料跨境流通合作、促進資料跨境流通已成為各地之共識。

中國大陸政府呼籲各國秉持開放、包容、安全、合作、非歧視的原則，平衡數位科技創新、數位經濟發展、數位社會進步與保護國家安全、公共利益、個人隱私與智慧財產權的關係，於推動資料跨境流通的同時實現各國合法政策目標。期待政府、國際組織、企業、民間機構等各主體堅守共享理念，發揮各自作用，推動全球資料跨境流通合作，共建高效便利安全之資料跨境流通機制，打造共贏的資料領域國際合作架構。

本報告之智慧財產權歸屬於國發會

以下說明倡議之十一點內容：

1. 鼓勵因正常商業與社會活動需求而透過電子方式跨境傳輸資料，以實現全球電子商務與數位貿易為各國經濟成長與永續成長提供新的動力。

2. 尊重不同國家、不同地區間資料跨境流通相關制度之差異性。支持不涉及國家安全、公共利益與個人隱私的資料自由流通。為實現合法公共政策目標，允許監管「資料跨境流通」，前提是相關監管措施不構成任意或不合理的歧視或對貿易構成變相限制，不超出實現目標所要求的限度。

3. 尊重各國依法對涉及國家安全、公共利益的非個人資料採取必要之安全保護措施，並保障相關非個人資料跨境安全、有序流通。

4. 尊重各國為保護個人隱私等個資權益所採取之措施，鼓勵各國在保護個資的前提下，為個資跨境傳輸提供便利途徑，建立健全之個資法與監管框架，鼓勵交流最佳實踐與良好經驗，提升個資保護機制、規則間的相容性，推動相關標準、技術法規及合格評定程序之相互承認。鼓勵企業取得效期 3 年之個資保護認證證書，以彰顯企業在認證範圍內之個資蒐集、儲存、使用、加工、傳輸、提供、公開、刪除及跨境等處理活動符合個資保護標準，並保障個人資訊跨國安全、有序地流通。

5. 鼓勵建立「資料跨境流通管理負面清單」，促進資料跨境高效、便利、安全地流通。

6. 共同建構開放、包容、安全、合作、非歧視之資料流通使用環境，共同維護公平公正的市場秩序，促進數位經濟規範發展。

7. 提高各類資料跨境流通管理措施之透明度、可預見性與非歧視性，以及政策框架之互通性。

本報告之智慧財產權歸屬於國發會

8. 積極進行資料跨境流通領域的國際合作。以建設、技術支援發展中國家有效參與、利用資料跨境流通以促進數位經濟成長。

9. 鼓勵運用數位科技促進資料跨境流通之創新應用，保障資料跨國流通之技術提升，推動資料跨國流通相關之技術與安全保障能力評估標準之國際相互承認，做好智慧財產權保護工作。

10. 於缺乏實證的情況下，不應針對特定國家、特定企業制定特定之資料跨境流通限制性政策，實施歧視性的限制、禁止或其他類似措施。

11. 禁止透過在數位產品與服務設置後門、利用數位科技基礎設施中的漏洞等手段非法取得資料，共同打擊資料領域跨境違法犯罪活動。

中國大陸外交部發言人表示，此倡議為中國大陸繼 2020 年發布之《全球資料安全倡議》後，中國大陸就資料議題發布之另一重要倡議，體現中國大陸欲推動建構網路空間命運共同體之核心目標。

資料來源：

1. 北京市人民政府，習近平在亞太經合組織第三十一次領導人非正式會議上的講話（全文），https://www.beijing.gov.cn/gate/big5/www.beijing.gov.cn/ywdt/dzyjs/202411/t20241117_3942671.html（最後瀏覽日：2024/11/21）

2. 中國大陸國家網路資訊辦公室，《全球資料跨境流通合作倡議》，https://www.cac.gov.cn/2024-11/20/c_1733706018163028.htm（最後瀏覽日：2024/11/21）

3. 新華社，外交部：中方願與各方深化資料跨境流通領域交流合作，http://www.news.cn/world/20241120/1274ea7d20dc49818c175e506a647d2c/c.html（最後瀏覽日：2024/11/21）

本報告之智慧財產權歸屬於國發會

4. 中國網路安全審查認證與市場監管巨量資料中心，5 家企業獲頒首批個人資訊保護認證證書，https://www.isccc.gov.cn/xwdt/tpxw/12/909546.shtml（最後瀏覽日：2024/11/21）

貳、AI 法制政策

一、美國

(一)2024 年 9 月美國司法部修訂《事業法遵計畫評估指引》納入 AI、新興技術之風險評估

美國司法部於 2024 年 9 月宣布修訂《事業法遵計畫評估指引》（Evaluation of Corporate Compliance Programs guidance，下稱《指引》），修訂內容主要涵蓋 AI 與新興技術之風險、法遵計畫監控與資料分析以及保護吹哨者三個領域。

本次指引修訂關注 AI 與資料法遵風險層面，要求檢察官評估事業如何管理 AI 與其他新興技術相關之風險，例如，檢察官將評估該事業之實施政策、程序與控管措施，監控所採用技術之可信度與可靠性，以及是否遵循法律規範或事業內部之行為準則；事業須對員工進行有關使用 AI 等技術之訓練；並監控與測試相關法遵程序之遵守情況等。

建議檢察官依循《指引》之三個基本問題，評估事業法遵計畫之有效性。以下簡述三個基本問題與相關說明：

1. 事業的法遵計畫是否設計完備？

評估計畫的關鍵因素在於該計畫的設計是否足以發揮最大效用，以防止與偵測員工的不當行為，以及事業管理階層是否落實該計畫或是否默許員工從事違法或不當之行為。因此，檢察官應整體審視事業之法遵計畫，是否明確表達無法容忍員工之不當行為，以及政策、程序、責任分配、培訓計畫、

本報告之智慧財產權歸屬於國發會

報告和溝通管道等面向，以確保法遵計畫與事業營運、工作團隊完美融合。

(1) 風險評估

檢察官須自商業角度審視及了解事業之業務經營狀況，方能有效評估事業是否已設計完善之法遵計畫，包含識別、評估及界定其風險之方法；減輕事業風險的具體因素；該計畫用於風險評估之資源。其中於公司是否得以管理新出現之風險及確保應遵守之法律部分，則強調必須能夠識別及管理新出現之內外部風險，包括新科技應用之風險。諸如事業如何評估導入 AI 等新技術對事業法遵能力之潛在影響？AI 或新技術之導入相關風險管理是否已納入事業之風險管理政策？事業於業務計畫或法遵計畫中採用 AI 或新興技術是否有對應之治理方法？如何防止 AI 或新技術應用可能導致之風險或後果？如何於業務推動過程中可能產生對技術應用相關之故意、過失或濫用作為，例如員工濫用新興科技之可能性？事業對於 AI 等新興技術應用是否有相當之控制措施或監控措施以確保其運作之可信度、可靠性或符合事業內部行為準則？是否有適當機制確保 AI 應用之問責？以及如何訓練員工使用 AI 等新興技術等，皆須納入評估。

(2) 政策與程序

檢察官應檢查事業是否制定行為守則，該守則應包括遵守相關聯邦法律的承諾，以及應適用於事業所有員工。據此，檢察官應進一步評估事業是否制定政策、程序，並將法遵文化融入日常營運活動。

(3) 培訓與溝通

本報告之智慧財產權歸屬於國發會

檢察官應評估事業所採取之措施，以確保事業所訂定之政策與程序已融入組織流程，包括對所有董事、員工、代理人及業務夥伴進行定期培訓與認證等。

(4) 秘密舉報架構與調查程序（Confidential Reporting Structure and Investigation Process）

為強化內部秘密舉報之制度，檢察官應對事業如何保護內部舉報者之架構與程序進行評估，例如：檢察官將審視事業內部是否具備適切之投訴處理流程，並使員工不用擔心遭到報復，是否具備提交投訴之適當程序，及保護內部舉報人之相關流程。同時亦須評估事業處理此類投訴或舉報相關作為之適切性，包括投訴或舉報資訊是否被適當的轉達予適當之人員、是否及時且徹底之完成調查以及是否於調查後採取適當之行動或紀律處分等。

(5) 第三方管理（Third Party Management）

檢察官仍應評估事業對第三方合作夥伴資格與合作情形之熟悉程度，與第三方合作之需要與原因，以及第三方合作對象是否為事業帶來風險（如第三方事業之聲譽或與其他國家官方之關聯等）。

(6) 結合與併購（Mergers and Acquisitions，M&A）

法遵計畫應包括對任何收購組織進行全面的盡職調查，以精確評估結合或併購目標之價值，並可就目標組織從事之不當行為及相關之成本納入談判。同時亦須評估事業結合後是否得以將收購之目標組織有效整合至現有的法遵計畫架構與內部控管程序。

2. 事業的法遵計畫是否有充足的資源與權責，以支援有效運作？

本報告之智慧財產權歸屬於國發會

檢察官應評估事業處理風險的方法，了解其是否已設計適當之風險控管措施。此外，檢察官應確定事業是否配置適當數量之員工以審核、記錄及分析事業內部法遵工作之落實。

(1) 中高層管理人員的承諾

組織應於內部各層面培養倫理與法律遵循之文化，而法遵計畫之有效性亦須受到事業領導階層之承諾，由中階至高階管理階層皆能落實法遵文化。故檢察官應審查高級管理人員如何闡明事業之道德標準，有無清晰明確地傳達標準，並以身作則嚴格遵守。同時亦須檢視中階管理人員如何強化該標準之落實，並鼓勵員工遵守。

(2) 自主性與資源（Autonomy and Resources）

檢察官應評估法遵計畫之結構，是否包括適當權限與地位之人員，以及是否具有充分之資源，得以監督法遵計畫落實。同時對於負責法遵監督之管理者是否具備足夠之自主權（獨立性確保），例如得以直接向董事會或董事會之審計委員會報告等。

(3) 薪酬結構與結果管理（Compenssation Strucures and Consequence Management）

事業必須具備清楚的後果管理程序，確保相關程序具體落實於事業各層面，而檢察官必須評估事業如何向員工傳達後果程序之存在，使其了解若採行不適當違法之行為將不被容忍，且無論其職位或頭銜為何皆將迅速面對該有之後果。此外，適當之激勵或薪酬機制，亦有助於組織內部培養法遵文化，而檢察官得以檢視事業是否設計相當之激勵或薪酬機制鼓勵員工落實符合事業價值觀與政策之作為。

本報告之智慧財產權歸屬於國發會

3. 事業的法遵計畫實際上是否有效？

評估事業的法遵計畫實際上是否有效，檢察官應該考慮不當行為是否被發現以及如何被發現，有哪些調查資源可用來調查可疑的不當行為，以及補救工作的性質與落實程度。

(1) 持續改善、定期測試與檢討（Continuous Improvement, Periodic Testing, and Review）

檢察官應審查事業是否已投入適當之努力，以持續檢視並調整其法遵計畫，以確保其有效性。尤其當事業於營運或法遵計畫當中導入 AI 技術時，是否會監控與測試所導入之技術，以確保該技術符合預期並遵循事業之行為準則；以及事業對於導入之 AI 或其他新技術運作不符合事業價值觀時，可於多久時間內發現並予以糾正。

(2) 不當行為調查（Investigation of Misconduct）

事業應建立適當之機制得以對於內部不當行為之投訴或懷疑進行調查，並對事業之作為進行適當之紀錄，包括記錄事業採取之任何紀律處置或補救措施等。檢察官對內部調查制度之評估，應觀察組織如何界定其對不當行為調查之範圍，調查是否獨立、客觀、且適當的記錄下來。

而簡訊傳輸應用程式之利用現今已十分普遍，並作為事業內部溝通之重要工具或平臺，故檢察官於調查事業是否適切識別、報告、調查及補救前在之不當行為或違法行為時，應將事業管理個人裝置、通訊平臺與訊息應用程式使用之政策與程序納入評估。包括各該應用程式之採用是否符合事業之風險狀況與業務需求，且業務相關之電子資料及通訊資訊可被事業存取及保存。檢查官並須了解該事

本報告之智慧財產權歸屬於國發會

業對於上開應用程式利用等之相關政策或措施是否有效傳遞予員工。

(3) 潛在不當行為的分析與補救（Analysis and Remediation of Any Underlying Misconduct）

於評估法遵計畫之有效性，檢察官將審視違法或不當行為之程度與普遍性、涉案事業員工的數量與職級、不當行為之嚴重性、持續時間與頻率、以及事業採取之補救措施。

資料來源：

1. JUSTICE.GOV, Criminal Division's compliance program guidance, 2024-09-05, https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl (last visited 2024/10/15)
2. JD Supra, DOJ Updates Corporate Compliance Program Guidance With a Focus on AI and Emerging Technologies, 2024-10-11, https://www.jdsupra.com/legalnews/doj-updates-corporate-compliance-8002719/ (last visited 2024/10/15)

(二)2024 年 9 月美國預算管理局發布《第 24-18 號備忘錄「促進政府負責任地採購 AI」》

2024 年 9 月美國預算管理局（The Office of Management and Budget，下稱 OMB）發布《第 24-18 號備忘錄「促進政府負責任地採購 AI」》（Memorandum-24-18, Advancing the Responsible Acquisition of Artificial Intelligence in Government，下稱 M-24-18）。該備忘錄要求各政府機關須提升負責任地採購 AI 之能力，利用 AI 之潛力及效用，為各機關帶來現代化營運及改善政府對公眾提供之服務，並保護公眾免受潛在風險或傷害。為實現此目標，政府各部門須認識 AI 會帶來新風險類型，並將 AI 風險管理考量因素整合至機關之採購計畫。

本報告之智慧財產權歸屬於國發會

以下為美國白宮發布 M-24-18 之重點內容：

1. 確保跨職能及跨機構合作（Ensuring Cross-functional and Interagency Collaboration）

為因應管理之新風險及 AI 技術之快速發展，須於各機關建立跨職能團隊，包括具備 AI 專業知識及其他相關領域人員，例如：採購、網路安全、隱私權及公民自由權利等領域，以確保得以適當更新採購管理相關實務政策及程序以因應新興科技，達到有效且負責任之 AI 採購。各機關之跨職能合作，應考量：

(1) 識別最適合於機關使用之 AI，對其進行投資並排定優先順序。

(2) 發展部署（deploy）、採購 AI 之能力。

(3) 發展 AI 採購時，各機關跨職能合作之最佳實踐（best practices）模式。

2. 管理 AI 風險及績效（Manage AI Risks and Performance）

當機關向外部實體（external entities）採購 AI 系統或服務時，因建置、訓練與部署 AI 系統之複雜性將會帶來額外風險，故各機關須確保於規劃 AI 採購時，應優先考量隱私、安全、資料所有權及互通性等要件。M-24-18 提出管理 AI 風險與效能之最佳實踐及具體之要求，其中包括涉及權利影響及安全影響之 AI 相關採購，重點如下：

(1) 要求各機關之隱私相關權責人員，能提早且持續參與 AI 採購流程，以識別及管理隱私風險，並確保遵守法律及政策。

本報告之智慧財產權歸屬於國發會

(2) 要求各機關應與 AI 供應商配合，瞭解何時有必要採購 AI，及何時可能觸發對權利或安全之影響而需採行額外之風險管理。

(3) 推廣使用創新之成果導向型採購（outcomes-based acquisition）技術，以增強各機關有效規劃、管理、持續降低風險及提升績效之能力。

(4) 指示各機關應協商適當之契約要求及評估程序，確保 AI 供應商提供足夠資訊，以供各機關能評估是否須向供應商主張權利、識別及管理風險、進行影響評估，及符合對受影響當事人之通知及提起救濟。

(5) 指示於協商契約條款時，應保護政府資料及智慧財產權，並確保 AI 可能影響涉及公眾之決策時，能安全地使用 AI。

3. 透過創新採購促進 AI 市場之競爭力（Promoting a Competitive AI Market with Innovative Acquisition）

隨著 AI 之發展，各機關須有能力得於多樣化及不斷發展之 AI 技術及供應商中，取得最佳之解決方案，因此本備忘錄呼籲各機關應確保有效競爭之落實，避免過於依賴單一供應商，不但可增加聯邦政府之價值，必可減少對權利及安全之風險，重點包括：

(1) 於契約條款研議時，主動納入降低供應商鎖定之採購原則。

(2) 於市場研究、需求開發及 AI 供應商評估過程，明確考量互通性與透明度。

(3) 利用創新之採購實務，確保 AI 供應商之良好績效及任務成果（mission outcomes）。

本報告之智慧財產權歸屬於國發會

資料來源：

1. The White House, The White House FACT SHEET: OMB Issues Guidance to Advance the Responsible Acquisition of AI in Government, 2024-10-03 , https://www.whitehouse.gov/omb/briefing-room/2024/10/03/fact-sheet-omb-issues-guidance-to-advance-the-responsible-acquisition-of-ai-in-government/ (last visited 2024/10/23)

2. MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES, M-24-18 , 2024-09-24 , https://www.whitehouse.gov/wp-content/uploads/2024/10/M-24-18-AI-Acquisition-Memorandum.pdf (last visited 2024/10/23)

(三)2024 年 10 月美國勞工部發布《AI 與勞工福祉：開發人員與雇主原則及最佳實務指引》

2024 年 10 月美國勞工部（Department of Labor, 下稱 USDOL）發布《AI 與勞工福祉：開發人員與雇主原則及最佳實務指引》（Artificial Intelligence And Worker Well-being：Principles And Best Practices For Developers And Employers），此指引延伸 USDOL 於 5 月所發布之《人工智慧與勞工福祉：開發人員與雇主原則》（Artificial Intelligence and Worker Well-being：Principles for Developers and Employers），新增最佳實踐事例，協助雇主與 AI 開發人員得以具體落實該原則，提高實務執行之成效。本次就 5 月份文件之 8 項補充如下：

1. 以工作者賦權為核心（Centering Worker Empowerment）：

於 AI 之整個生命週期，雇主應納入勞工於採用 AI 之初期至其後之定期得以對於所採用之 AI 提出意見，以使 AI 運用得以有效提升勞工工作品質，達成事業預期之結果。當勞工有工會組織時，雇主應就其在工作場所採用之 AI 或電子監

本報告之智慧財產權歸屬於國發會

控（electronic monitoring）行為，與工會進行善意之協商（bargain in good faith）。

2. 以符合倫理方式開發 AI（Ethically Developing AI）：

(1) 開發人員應建立標準，確保投入於市場之 AI 產品皆能保障勞工之公民權利、降低勞工之安全風險並滿足提升工作效能之要求。

(2) 開發人員應對其投入市場影響，可能對勞工產生影響之 AI 進行影響評估及獨立之審核，並以可讀取之格式將評核結果發布，使雇主了解產品效能及可信賴性。

(3) 開發人員應確保其所開發，用以審查及改進用於訓練 AI 系統（train AI systems）之資料輸入的相關作業，符合基本人權，以及國內及國際之勞工標準。

(4) 開發人員開發會影響勞工之 AI 系統，應使雇主能持續為監控及人工監督，並就 AI 產生之建議或與決策相關之資料進行審查。同時於針對會影響勞工之 AI 系統進行獨立評估時，須為非技術使用者（non-technical users）提供可理解之操作及結果。

3. 建立 AI 治理及人員監督機制（Establishing AI Governance and Human Oversight）：

(1) 雇主應建立可對組織領導階層問責之治理架構，以對組織內部提供指導及協調，確保採用及實施會影響勞工之 AI 系統時，內部組織單位之作為具備一致性，並應將勞工及其代表之意見納入決策過程。

(2) 雇主應為其勞工提供 AI 系統使用之培訓。

本報告之智慧財產權歸屬於國發會

(3) 雇主不得僅依據 AI、自動化系統或電子監視系統蒐集之資料進行重大聘僱決定。

(4) 雇主應識別與記錄 AI 及自動化系統所為之重大聘僱決策類型，若 AI 或演算法之建議為雇主做出重大決策之主要依據，則雇主應向求職者或勞工以清晰易懂之語言提出解釋，說明該 AI 於決策過程之作用及作成決策所依據之資料。

(5) 當全部或部分使用 AI 及自動化系統為重大聘僱決定時，雇主應告知勞工對其不利影響決定之補救措施。

(6) 雇主應確保會影響勞工之 AI 系統定期被獨立審核，並公開報告關於影響勞工權利及安全評估之資訊。

4. 確保利用 AI 之透明度（Ensuring Transparency in AI Use）：

(1) 雇主採用會影響勞工之 AI 系統時，應事先通知勞工及其代表並為適當之揭露，內容應包含對 AI 系統用途之解釋。

(2) 開發人員與雇主應以清晰易懂方式告知勞工及其代表，關於該系統將蒐集、存取之資料範圍以及資料之利用目的。監控勞工時應為明顯之通知，並提前告知監控之活動範圍及目的。

(3) 雇主應於可行之情況下，確保勞工及其代表得對影響重大聘僱決策之個人可識別資料提出更正，並於資料不正確時，提出異議而不受報復。

5. 保護勞工及就業權利（Protecting Labor and Employment Rights）：

本報告之智慧財產權歸屬於國發會

(1) 雇主不得採用會破壞或干擾勞工組織及其他受保護活動之 AI 系統，雇主並須遵守《國家勞工關係法》（the National Labor Relations Act）規定之法律義務。

(2) 雇主應適當減輕採用「會影響勞工之 AI 及自動化系統」，因其可能直接或間接造成勞工健康及安全結果之風險（包括疲勞或受傷率）。雇主並須遵守《職業安全衛生法》（the Occupational Safety and Health Act）及相關標準與法規。

(3) 雇主對會影響勞工之 AI 的採用，不應被用於減少勞工合法應得之薪資、休息時間或福利。且雇主須遵守《公平勞工標準法》（the Fair Labor Standards Act）及其他聯邦勞工標準。

(4) AI 之開發人員與採用 AI 之雇主須遵守反歧視法規之相關要求，審查 AI 系統是否產生不利或違法之影響並公布其結果。

(5) 開發人員與雇主應評估可能影響身心障礙之勞工與求職者之 AI 技術的設計及使用，降低其就業障礙。

(6) 雇主須確保勞工不會因其主張勞動及就業權利或提出對於使用 AI 之疑慮而遭到報復。

6. 使用 AI 賦能工作者（Using AI to Enable Workers）：

(1) 於採購 AI 技術前，雇主應考量 AI 系統如何影響特定之工作任務、所需技能、工作機會及勞工可能面臨之風險。

(2) 雇主應於廣泛地部署「會影響勞工之 AI 系統」前，先進行測試（piloting）。

(3) 雇主應減少電子監控，並確保採用侵入性最小之手段實現合法及明確之商業目的。

本報告之智慧財產權歸屬於國發會

(4) 雇主應採取相關措施，確保使用 AI 確定之工作優先事項或工作安排，有助於實施公平及可預測之排程表。

(5) 使用 AI 系統而獲得生產力提升或利潤增加之雇主，得考量如何分配勞工獎勵。

7. 支持受 AI 影響之工作者(Supporting Workers Impacted by AI)：

(1) 雇主應向勞工提供 AI 系統相關培訓及專業發展。

(2) 於可行情形下，雇主應優先考量，對因採用 AI 而失業之勞工再行培訓，將其重新分配至組織其他工作職位。

(3) 雇主應與州及地方勞動力體系（workforce systems）合作，成立夥伴關係，以支持提升技能之教育與訓練。

8. 確保負責任地使用工作者資料（Ensuring Responsible Use of Worker Data）：

(1) 開發會影響勞工之 AI 時，開發人員應設計及建構具有保障措施之 AI 系統，保障與勞工相關之資料。

(2) 雇主應避免蒐集、保留或以其他方式處理不必要的勞工資料。應設立資料保護人員，以監管勞工資料之蒐集、處理、維護或利用。

(3) 雇主應保障有關勞工的任何資料免受內部及外部威脅，如存取未經勞工授權之資料，應通知勞工及其代表，其受影響之資料、違反之效果及所採取之補救措施，緩解潛在之危害。

(4) 未經勞工同意或法律要求，雇主不得於雇主企業及代理人之外分享勞工資料。

資料來源：

本報告之智慧財產權歸屬於國發會

1. U.S. Department of Labor, Artificial Intelligence And Worker Well-being：Principles And Best Practices For Developers And Employers, 2024-10-16, https://www.dol.gov/general/AI-Principles (last visited 2024/10/28)

2. U.S. Department of Labor, Principles and Best Practices for Developers and Employers, 2024-10-16, https://www.dol.gov/sites/dolgov/files/general/ai/AI-Principles-Best-Practices.pdf (last visited 2024/10/28)

3. JD SUPRA, DOL Issues Guidance on AI and Worker Well-Being Best Practices, 2024-10-21 , https://www.jdsupra.com/legalnews/dol-issues-guidance-on-ai-and-worker-5992908/ (last visited 2024/10/28)

(四)2024 年 10 月美國白宮發布第一份關於 AI 之國家安全備忘錄

2024 年 10 月 24 日美國白宮發布第一份關於 AI 之國家安全備忘錄（National Security Memorandum, NSM）。本 NSM 要求美國政府部門必須實施具體且具影響力之作為，以（1）確保美國得以引領全球，發展安全可靠且值得信賴的 AI；（2）使美國政府得以運用尖端之 AI 技術，實現美國國家安全；以及（3）推動 AI 之國際共識與治理。NSM 雖不具備法律約束力，但內容涉及明確之美國政策方向與原則。以下依 NSM 之三大目標，簡要說明其要點。

1. 確保美國得以引領全球，發展安全可靠且值得信賴的 AI

(1) 由於開發 AI 系統需要大量高階晶片，拜登總統已簽署《晶片法案》（CHIPS Act）以投資高階半導體製造業。NSM 指出應提升晶片供應鏈之安全性與多樣性，以及確保美國得以支援下一世代政府發展超級電腦及其他新興技術時，得以將 AI 納入考量。

本報告之智慧財產權歸屬於國發會

(2) 提醒政府組織，競爭對手將可能透過經濟或技術之間諜活動竊取美國技術，故將競爭對手透過經濟與技術之間諜活動蒐集「美國之 AI 產業行動」列為最高優先等級之情報，並指出與美國政府相關組織應向 AI 開發人員及時提供網路安全及反情報（counterintelligence）資訊，以確保其發明之安全。

(3) 正式指定 AI 安全研究所（AI Safety Institute）作為美國產業與政府之主要聯繫管道。並為 AI 安全研究所與相關國家安全機構（包括情報社群、國防部及能源部）之合作訂定強化及簡化之機制。

(4) 加倍投入國家 AI 研究資源，以確保大學、民間及小型企業之研究人員可進行有意義之 AI 技術研究。

(5) 指示國家經濟委員會（National Economic Council）協調私人組織間於 AI 生態系發展之相對競爭利益，並進行經濟評估。

2. 以保護人權與民主價值為前提，使美國政府運用尖端之 AI 技術，實現國家安全

(1) NSM 指出須以採用符合民主價值的方式為前提，於國家安全任務層面，有效地使用 AI 系統。

(2) 為推動國家安全領域之 AI 治理及風險管理，NSM 會發布另一可定期更新之框架。該框架為實施 NSM 提供更進一步之細節與指導，包括風險管理機制、評估、問責制與透明度，要求各機構監控、評估以及減輕 AI 風險，例如：侵害隱私、偏見與歧視、個人與團體安全以及其他侵害人權行為相關之 AI 風險。

本報告之智慧財產權歸屬於國發會

(3) NSM 並指導各機關提出簡化之採購方法及與非傳統供應商協作之方法。

3. 推動 AI 國際共識與 AI 治理

(1) 美國與七大工業國組織（G7）於 2023 年共同制定第一個《AI 行為準則》。迄今已有 56 個國家簽署《軍事使用 AI 與自主武器的政治宣言》（Political Declaration on the Military Use of AI and Autonomy），該宣言建立軍事 AI 能力之原則。

(2) NSM 指示美國政府與盟國合作，建立穩定、負責任與尊重權利之 AI 治理框架，確保其開發與使用之技術遵循國際法，並兼顧保障人權與自由。

資料來源：

1. The White House, FACT SHEET: Biden-Harris Administration Outlines Coordinated Approach to Harness Power of AI for U.S. National Security, 2024-10-24, https://www.whitehouse.gov/briefing-room/statements-releases/2024/10/24/fact-sheet-biden-harris-administration-outlines-coordinated-approach-to-harness-power-of-ai-for-u-s-national-security/ (last visited 2024/10/28)

(五)2024 年 9 月美國紐約州金融服務部向其監管之組織發布產業信函(Industry Letter)，說明因應 AI 網路安全風險之因應策略

美國紐約州金融服務部（New York State Department of Financial Services）考量 AI 技術的進步對網路安全造成重大影響，將使犯罪者得以更快速地實施大規模的犯罪，然而相反的，AI 技術也將提升組織防禦能力。該部因收到所監管組織對於如何減輕 AI 網路相關風險相

本報告之智慧財產權歸屬於國發會

關之疑問，因此於 2024 年 10 月向其所監管之組織發布產業信函，以回應受監管組織之問題。以下簡述該產業信函重點：

1. AI 技術所造成之風險

應用 AI 存在許多風險，並對網路安全造成威脅，該產業信函強調兩項風險與威脅，其一為威脅行為者使用 AI 帶來的風險，其二為依賴 AI 所造成的風險。

2. AI 驅動之社交工程（AI-Enabled Social Engineering）

AI 支援的社會工程為金融服務業面臨的重大威脅之一。運用 AI 創造逼真的互動式影音與文字創造威脅之行為人（threat actors）日益增加，其可能透過電子郵件、電話、文字、視訊會議以瞄準特定個人標的。此類 AI 攻擊會試圖說服或引導員工洩露自己及雇主之敏感資訊，例如：運用深偽技術導致員工共享憑證時，威脅行為人可能藉此存取包含非公開資訊之資訊系統；或可能導致員工採取未經授權之行為，例如將資金轉入詐騙帳戶等。此外，亦有 AI 模仿個人之外表或聲音，試圖驗證個人身分以規避生物辨識技術。

3. AI 並可能強化網路安全攻擊或導致大量非公開資料之暴露或竊盜

AI 之運作可能協助威脅行為人提高網路攻擊的效能、規模或速度，原因在於 AI 相較於人工，可以更快速掃描及分析各類訊息，掌握可利用之安全漏洞，並可快速存取更多的資訊系統。一旦侵入系統，則可快速完成偵測，佈署惡意軟體並進行快速的存取及滲透。其亦可繞過安全防禦機制而逃避偵測。

此外，利用 AI 產品通常需要蒐集與處理大量資料，包括未公開之資料。擁有大量非公開資料之組織若要開發或佈署

本報告之智慧財產權歸屬於國發會

AI，將需要擴大對其非公開資料的取得與保護，也將使得威脅行為人有更大的動機將此類組織列為攻擊目標，以取得非公開資料而獲取經濟利益或達成其他的惡意目的。

4. 依賴第三方、供應商或其他供應鏈將導致漏洞增加

供應鏈漏洞為 AI 利用另一個須關注之重要問題。基於 AI 驅動之相關工具或應用程式，通常需要仰賴大量之資料蒐集及維護，其過程亦經常需要透過與供應商或第三方服務提供者之合作。供應鏈涉及之環節愈多，則可被威脅行為人利用之潛在安全漏洞就愈多，導致任一供應鏈環節受到網路安全事件侵入，皆可能將整體關聯網絡拉入攻擊範圍。

5. 減輕 AI 相關威脅之控管與措施

網路安全相關規範要求組織必須評估風險並制定網路安全標準，目的在減輕與其業務相關之網路安全與 AI 的風險與威脅。本信函提供監管產業可參考之控制方法或措施，並說明若可一起採用，則即使一種控管措施無效，其他控管措施亦可防止或減輕攻擊的影響，相關建議措施摘述如下：

(1) 應建立網路安全風險評估相關計畫、政策及程序：此部分應該考量個別 AI 應用組織可能面臨的風險，加以識別並採行可實施之防禦措施。於風險評估機制之設計時，應考量組織本身對 AI 之使用、第三方服務提供者與供應商對 AI 之使用以及相關 AI 應用程式可能對組織之潛在風險等。除依網路安全相關法規至少於每年更新一次風險評估外，並於業務調整或改變時，執行新風險之評估及所需採行之應對方案。

(2) 應進行第三方服務提供者及供應商之管理：必須對第三方服務提供者或供應商之選任進行盡職調查。尤其必須將

本報告之智慧財產權歸屬於國發會

AI之採用或相關AI產品或服務可能面臨之威脅納入調查之範圍。

(3) 存取控制

組織應依據其風險評估，決定要採用或實施之存取控管措施。控管措施須限制授權使用者的存取權限，針對較高權限之授權使用者，組織亦須定期檢查其存取權限設定之適切性，以確保每位授權使用者只能存取其執行工作範圍所需之非公開資訊（Nonpublic Information），移除或停用不再需要的存取權限，並於該授權使用者離職後立即終止其權限，並須限制授權使用者遠端存取之裝置及方式。

(4) 網路安全訓練

另一可用於對抗AI相關威脅的重要且必要的網路安全控管措施，係為組織所有人員進行訓練，包括高階主管與管理人員。訓練應確保所有人員都瞭解AI所造成之風險，以及組織所採取相關降低與AI風險之程序，以及如何因應AI強化的社交工程攻擊。

(5) 資料管理

有效的資料管理可限制威脅者存取資訊系統時組織可能暴露的風險。相關組織須執行資料最小化作業，降低未經授權存取或外流的可能性。建議組織應維護並更新資料清單，因為資料清單對於評估潛在風險與確保遵守資料保護法規至關重要。

資料來源：

1. NEW YORK STATE, Industry Letter,2024-10-16, https://www.dfs.ny.gov/industry-guidance/industry-letters/il20241016-cyber-risks-ai-and-strategies-combat-related-

本報告之智慧財產權歸屬於國發會

risks(last visited 2024/11/14)

二、歐盟

(一)2024 年 10 月歐盟聯合研究中心發布《歐盟 AI 法統一標準（Harmonised Standards for the European AI Act）》之政策文件

歐盟執委會聯合研究中心（Joint Research Centre, JRC）回應歐盟執委會之要求，於 2024 年 10 月 24 日發布《AI 法統一標準（Harmonised Standards for the European AI Act）》之政策文件。

歐盟於 2024 年 8 月 1 日生效之《AI 法》（AI Act, AIA），其中於附件 I 之所定之第三方認證合格之產品之嵌入式系統，過渡期為 3 年；附件 III 之所定之其他高風險系統，過渡期為 2 年。即 2026 年 8 月起，高風險 AI 系統必須遵守風險管理、資料品質與治理、電子形式軌跡資料（logging）與可追溯性、技術文件、透明度、人為監管、準確性、穩健性與網路安全相關之要求。所謂高風險 AI，僅限於對個人健康、安全或基本權利產生重大有害影響之 AI 系統，例如：用於人才招募、醫療等領域之 AI。後續將透過建立品質管理系統、要求 AI 投入市場前通過符合性評估（conformity assessment），以確保符合前述之高風險 AI 要求。

本次政策文件主要涵蓋建構 AIA 統一標準應考量之十個重點：

1. 風險管理

應規範使用 AI 之產品與服務的風險管理系統，以識別與減輕對個人健康、安全及基本權利危害之風險。縱使可以借鏡 ISO、IEC 等標準化組織提出來之標準，然該些組織所提標準尚未能體現 AIA 背景下的技術與非技術因素，如：AI 軟體之特性、涉及之基本權利。

本報告之智慧財產權歸屬於國發會

風險管理層面，應要求提供充分證據，以證明已識別並解決所有可預見的風險，且需透過測試與評估加以驗證風險減輕措施之有效性。標準不須為各個 AI 系統制定具體之風險管理措施，但應明確定義 AI 風險管理者需要達成之過程、結果及關鍵標準。

2. 資料治理與品質

為符合 AIA 第 10 條之要求，應定義資料品質指標與治理流程所需之明確標準，並應定義選擇相關指標所依循之資料（define the evidence required to support these choices），以說明採行之標準符合法遵之適當性（suitability）與有效性（effectiveness）。同時應要求組織須採取可對應風險之客制化的資料治理與品質控制措施，並將 AI 系統的生命週期之資料治理等問題，包含 AI 系統資料來源之複雜程度及資料品質等可能對利用 AI 系統產生之風險納入考量。

3. 紀錄保存（Record Keeping）

依據 AIA 第 12 條規定，統一標準應明確定義紀錄保存之要求，包括識別 AI 生命週期間（包含產品上市後的階段）可能導致風險之情況，並記錄所有採行之作為，以監控法遵要求之落實。同時須確保電子形式軌跡資料與紀錄保存等機制規劃，將所有相關事件、觸發因素及資訊因素納入考量。

4. 透明度

為符合 AIA 第 13 條規定及高風險 AI 系統提供者與使用者之相應義務與需求，統一標準應定義相關的透明度資訊。例如協助理解 AI 系統運作方式、特性、能力、優勢、限制與效能的資訊等。特別是與可能導致潛在風險之相關資訊，及支援系統輸出的資訊，以供使用者作成決策，例如：監督 AI

本報告之智慧財產權歸屬於國發會

系統之運作，並在需要時採取改善措施（take corrective action）。

5. 人為監督（Human Oversight）

依據 AIA 第 14 條，為確保高風險 AI 系統在預期的範圍內運作，並使自然人能在必要時控管高風險 AI 系統之產出（outputs），可能需要採取多種監管措施，例如：提升系統決策理解之技術手段、 增進操作人員之監控介面、各種培訓措施等。統一標準應明確定義人為監管措施之要求以及措施之實施與測試方式，以讓高風險 AI 系統之提供者能依據標準的要求，考量其 AI 系統之預期用途與風險，將要求轉為具體之監管措施。

6. 準確性（Accuracy）

依據 AIA 第 15 條，統一標準應定義準確性之指標與門檻（thresholds）。此外，為適切的測試準確性，統一標準應明確定義測試準確性所需採取之流程、方法與技術，以及在選擇各種指標、門檻時的考量，並於適當的細節記錄必要之證據，依照最佳實踐進行報告。目前仍在開發針對自然語言處理或電腦視覺等 AI 系統之多項準確性標準，這些標準將為某些領域之 AI 應用提供具體要求與指導。然而，統一標準建構之主要目標為定義一普遍適用之要求，以確保高風險 AI 系統提供者所選擇之準確性指標與門檻符合法遵之適當性與有效性。

7. 穩健性

依據 AIA 第 15 條，統一標準應定義部署高風險 AI 系統時的韌性相關要求，包括涉及 AI 系統之運作環境錯誤、故障或不一致等問題之要求。AI 系統提供者可以採用多種技術與

本報告之智慧財產權歸屬於國發會

組織措施以支持 AI 系統之穩健性，並防止有害或不良行為。目前某些類型之 AI 系統之穩健性技術已納入 ISO/IEC 標準，統一標準亦可參考這些 ISO/IEC 標準進行研訂。

8. 網路安全

應定義適合 AI 系統風險之技術與組織措施，並可參考既有之 ISO/IEC 27000 系列標準，以保障支援 AI 系統之 ICT 基礎設施安全。為符合 AIA 第 15 條之要求，統一標準應具體涵蓋資料中毒、模型中毒、模型規避（model evasion）、機密性攻擊等 AI 特有的資安挑戰。新的標準化工作應集中於對高風險 AI 系統制定安全風險評估與風險減輕計畫之基本要求，並從系統面定義具體之安全目標及其驗證方法。此外，網路安全標準化應與資料品質、穩健性等其他要求相互參考。

9. 品質管理

應明確規定高風險 AI 系統提供者如何建立與維護有效之品質管理系統，以確保符合法規要求，並支援法遵評估，包括透過進入市場後之監控系統。可以參考現有產品之品質管理系統標準，但須考慮 AI 產品的特殊性，如：AI 嵌入實體產品或 AI 軟體服務。新的品質管理標準應針對 AIA 之具體風險，以產品為中心，涵蓋 AI 產品生命週期及法規第 17 條所規定之法遵要求，例如：計畫、資源、產品要求、AI 系統設計、開發與風險管理技術等。雖然現有的國際標準（如：ISO/IEC 42001 AI 管理系統標準）與 AIA 的目標與方法不完全一致，但統一標準的品質管理標準仍可適當地參考 ISO/IEC 42001 於技術、組織層面之相關條款，同時應確保其重點仍為 AIA 關注之特定風險與目標。

10. 符合性評估（conformity assessment）

本報告之智慧財產權歸屬於國發會

應定義高風險 AI 系統於上市前或投入使用前之法遵評估程序與流程，無論是由 AI 系統提供者內部或由第三方組織進行評估，應明確負責法遵評估執行人員之能力標準。

由於此標準可以適當地運用既有的國際標準，如：ISO 的合格評定委員會（CASCO）所制定之一系列 CASCO 工具箱，提供法遵評估之一般原則與指導。

法遵評估標準與各種高風險 AI 系統要求間的協調至關重要，例如：品質管理系統之評估，在 AIA 之法遵評估中扮演關鍵角色。

標準化組織 JTC21（Joint Technical Committee (JTC) 21 of CEN-CENELEC）已發布 37 個與 AI 相關之國際或歐洲本地標準，這些標準對於解決 AI 可信賴性至關重要。由於清晰且可操作的要求，有助於減少法遵之不確定性，技術專家間的共識亦十分重要，特別是針對開發創新 AI 解決方案之中小型企業。故歐洲執委會將透過 AI 辦公室與聯合研究中心繼續支持此一統一標準建構之進行。

資料來源：

1. European Commission, Harmonised Standards for the European AI Act, 2024-10-25, https://ai-watch.ec.europa.eu/news/harmonised-standards-european-ai-act-2024-10-25_en (last visited 2024/11/04)
2. JRC Publications Repository, Harmonised Standards for the European AI Act, 2024-10-24, https://publications.jrc.ec.europa.eu/repository/handle/JRC139430 (last visited 2024/11/04)

三、 英國

(一)2024 年 10 月英國政府鼓勵外國廠商至當地設立資料中心，並將持續投資 AI 相關計畫，以促進英國經濟發展與 AI 創新

本報告之智慧財產權歸屬於國發會

英國創新科技部（Department for Science, Innovation and Technology, DSIT）於 2024 年 10 月 14、15 日陸續發布新聞，說明英國政府鼓勵外國廠商至當地設立資料中心，並將運用計畫資源持續投資 AI，以促進其經濟發展與 AI 創新。

首先，英國政府歡迎美國 CyrusOne、ServiceNow、Cloud HQ 及 CoreWeave 4 家事業在英國當地設立資料中心。據該國統計，全世界在英國資料中心之投資，如基礎設施，其價值已達 63 億英鎊。以來自美國華盛頓特區之 Cloud HQ 事業的投資為例，該事業在英國牛津郡（Oxfordshire）投資 19 億英鎊建立新的資料中心園區，建設期間將可創造 1,500 個就業機會，而開始運行後至少可以增加 100 個以上的全職工作。

相關資料中心對英國之助益包含提供更多之運算能力與資料存儲空間，且讓英國各界可利用這些基礎設施來訓練與部署次世代 AI 技術，如研發複雜之機器學習模型與演算法，並可促進醫療保健或其他領域之 AI 應用，進而使民眾享受更健康的生活。

其次，DSIT 宣布將透過政府投資，加強對深偽（deepfakes）、不實資訊及相關網路攻擊之研究。因為這些攻擊將造成較高的社會風險，且透過相關研究可提高 AI 安全。為此，英國工程與物理科學研究委員會（Engineering and Physical Sciences Research Council, EPSRC）與研究創新局（Research and Innovation）轄下之 Innovate UK 合作，將自 10 月 15 日起提供計畫資源，以保護英國社會免受 AI 潛在風險之影響。

此外，相關投資還將支援研究因應 AI 系統失敗之威脅。英國政府除了針對特定領域或 AI 應用訂定規範或進行監管外，由於 AI 系統之安全重視 AI 在不同領域部署相關系統與基礎設施，如醫療保健、能源或金融領域，但因 AI 應用可能產生潛在之風險，為降低或解決風險，需要有解決之工具或解決方案。

本報告之智慧財產權歸屬於國發會

目前此一計畫資源預計提供給 20 個專案、每個專案最多可獲得 20 萬英鎊之補助，總金額為 400 萬英鎊。

資料來源：

1. DSIT, Tech Secretary welcomes foreign investment in UK data centres which will spur economic growth and AI innovation in Britain, 2024-10-14, https://www.gov.uk/government/news/tech-secretary-welcomes-foreign-investment-in-uk-data-centres-which-will-spur-economic-growth-and-ai-innovation-in-britain (last visited 2024/10/23)
2. DSIT, Research programme to ensure UK economy uses AI to grow safely, 2024-10-15, https://www.gov.uk/government/news/research-programme-to-ensure-uk-economy-uses-ai-to-grow-safely (last visited 2024/10/23)

(二)2024 年 11 月英國資訊委員辦公室提出將 AI 應用於招聘員工時，應考量之 6 個關鍵問題

英國資訊委員辦公室（Information Commissioner's Office, ICO）於 2024 年 11 月提出將 AI 應用於招聘員工時，應考量之 6 個關鍵問題。

許多從事招聘業務之人員(recruiters)可能希望透過採購 AI 工具，以提升招聘流程之效率，幫助尋找潛在之求職者（candidates）、總結履歷及評估應徵者（score applicant）。然而，若違法使用 AI 工具，可能導致求職者履歷被不公平地排除在外或使其隱私受到侵害。為此，ICO 保障部門處長（ICO Director of Assurance）Ian Hulme 表示：「AI 為招聘可以帶來好處，但如果無法公平、合法地使用 AI，可能對求職者造成損害。考慮採購 AI 工具以協助招聘流程之組織，須向 AI 提供商提出關鍵之個資保護問題，並尋求 AI 提供商明確保證其工具或服務之合法性。」

本報告之智慧財產權歸屬於國發會

ICO 近期稽核幾家開發或提供招聘用途 AI 工具之廠商，發現許多的改進空間，例如：無法證明可確保個人資料受到公平地處理，且符合資料最小化，以及清楚地向求職者解釋個人資料將如何被 AI 工具使用等。據此，ICO 已向相關廠商提出多項改善其對個資保護法之法遵情況之建議，廠商皆已接受。

而對於事業於採購「用於招聘之 AI 工具」前，須考量之 6 個關鍵問題，ICO 建議如下：

1. 組織是否完成資料保護影響評估（DPIA）？

   採購過程為採行或開發 AI 工具前之重要階段，招聘人員可以於此階段透過向 AI 工具提供商提出正確問題，以了解、減輕或解決對個人之潛在隱私風險或傷害。故建議可於採購階段即進行 DPIA，並於其後相關程序不斷更新評估，以符合個資保護法制規範遵循之問責義務。

2. 組織處理個資之法規依據？

   組織處理個人資料，須確定符合之法規依據，例如：是否取得當事人之同意或符合正當利益（legitimate interest）。若招聘人員規劃於招募過程處理敏感個資，例如：人種、種族來源或健康資料，則須滿足法規之特定條件。

3. 組織是否須負擔記錄責任，並應設置明確之處理指示？

   招聘人員與 AI 提供商都對個資保護合規性負有責任。組織須確定誰是個資之控管者與處理者，須清楚記錄於組織與 AI 提供商簽訂的契約並仔細審查。若 AI 提供商是個資處理者，則必須為 AI 提供商提供明確且全面之書面說明，以供其遵循，並可以設置績效衡量指標，例如：統計準確性與偏差目標。

本報告之智慧財產權歸屬於國發會

4. 組織是否檢查過 AI 提供商是否致力於降低歧視的發生？

稽核報告顯示某些 AI 工具未能公平地處理個資，例如：允許招聘人員過濾掉具有某些特徵的求職者。組織須透過監控 AI 工具及其輸出內容之潛在或實際公平性、準確性或有無歧視之問題，進而確保公平地處理個資。組織應與提供商討論前述問題，以便適當地解決問題。組織應向 AI 提供商尋求明確保證，確認 AI 提供商已致力於降低歧視之發生，並要求查看任何相關文件。

5. AI 工具之使用是否透明？

組織須告知求職者，AI 工具處理求職者個資之方式。組織應以清晰之資料解釋該 AI 工具使用的方式、原因以及作出預測或生成可能影響個人之結果的邏輯。組織應告知求職者如何挑戰 AI 工具所做出之任何自動化決策。

6. 組織將如何限制 AI 工具將個資用於不相關之目的？

報告顯示，某些 AI 工具蒐集遠超過需要之大量個資，並無限期保留這類個資，以便在未經求職者知情之情況下，建立潛在求職者之大型資料庫。組織須確保該 AI 工具僅蒐集達成其目的所需之最小化個資，並應確保該個資不被用於其他不相關之目的。

資料來源：

1. ICO, Thinking of using AI to assist recruitment? Our key data protection considerations，2024-11-06，https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/11/thinking-of-using-ai-to-assist-recruitment-our-key-data-protection-considerations/ (last visited 2024/11/11)

本報告之智慧財產權歸屬於國發會

四、 韓國

(一)2024 年 10 月韓國政府宣布三年期之網路基礎設施計畫，並於 11 月成立 AI 安全研究院（인공지능안전연구소）

韓國科學技術情報通訊部（과기정통부）於 2024 年 10 月 18 日發布新聞，宣布於 11 月 27 日成立 AI 安全研究院（인공지능안전연구소），以落實今年 5 月 AI 首爾高峰會（AI Summit Seoul 2024）之決議，並引領該國 AI 研究之發展。

韓國政府前已於今年 9 月公布數位戰略(대한민국디지털전략)，預計於公布後 2 年，由 26 個相關部會，執行共 200 多個措施。由於 AI 被視為該國重點發展項目，韓國政府已於同月發布國家 AI 戰略政策方向（국가 AI 전략 정책방향），希望成為世界 3 大 AI 強國之一。有鑑於 AI 的發展趨勢，國際網路資源共享（雲端）已成為 AI 研發的重要基礎。故於國際趨勢與韓國國內政策的推動下，網路資源共享（雲端）市場不斷成長，但其國內實際利用率仍不算高，顯示 AI 時代所需之技術、競爭力及國際化策略有所不足。韓國政府希望透過前述計畫資源，投入 1. 推動廣泛運用以網路為基礎之資訊分享，如：透過雲端服務分享教材；2. 提升網路資訊分享之競爭力，如：建立半導體與 AI 運算中心，提供產業所需服務；3. 振興網路資源共享（雲端）生態，如：由國家提供基礎設施，引領民間投資 AI 相關創新，並提供 AI 時代所需之客製化人才培訓等。

此外，成立 AI 安全研究院除參考英國、美國及日本之作法外，該研究院之 3 大使命為促進對 AI 安全之認識、研擬 AI 安全政策，及完善韓國 AI 安全體系。並預計設置 AI 安全政策、評估、科技研發 3 個實驗室，初步規劃為 30 人左右，配合 3 大使命，執行 4 項業務，包含：1. 界定 AI 風險，評估 AI 安全性；2. 研究 AI 安全政策；3. 促進 AI 安全之國內外合作；4. 推動研發以確保 AI 安全。

本報告之智慧財產權歸屬於國發會

資料來源：

1. 과기정통부（Ministry of Science and ICT）, 인공지능 안전에 대한 국제 연대를 주도할 ‘인공지능 안전연구소’ 11 월 출범 인공지능 시대를 여는 새로운 인터넷 기반 자원 공유(클라우드) 전략 제시, 2024-10-18, https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=238&pageIndex=2&bbsSeqNo=94&nttSeqNo=3185018&searchOpt=ALL&searchTxt= (last visited 2024/10/30)
2. 과학기술정보통신부, 한국 AI 안전연구소’ 출범…AI 위협에 체계적·전문적 대응, 2024-11-27, https://www.korea.kr/news/policyNewsView.do?newsId=148936794&pWise=main&pWiseSub=L1 (last visited 2024/11/27)

五、 新加坡

(一)2024 年 10 月新加坡網路安全局發布《AI 系統安全指引》與《配套指引》，協助事業以安全的方式應用 AI

新加坡網路安全局（Cyber Security Agency of Singapore, CSA）於 2024 年 7 月 31 日至 2024 年 9 月 15 日進行公眾諮詢，並已依據所收到之 AI/科技事業、網路安全事業與專業協會（professional associations）之 28 份意見書，調整並提升指引，使之與國際標準一致。 10 月 14 日 CSA 舉辦第 9 屆「新加坡國際資安週」（Singapore International Cyber Week，SICW）並發布《AI 系統安全指引》（Guidelines on Securing AI Systems，下稱安全指引）與《AI 系統安全配套指引》（Companion Guide on Securing AI Systems，下稱配套指引），協助事業於 AI 生命週期中可透過安全的方式應用 AI。

為制定《安全指引》與《配套指引》，參考既有之國際產業指引與標準，包括：由英國國家網路安全中心（National Cyber Security Centre, NCSC）與美國國土安全部所屬網路安全暨基礎設施安全局

本報告之智慧財產權歸屬於國發會

（Cybersecurity and Infrastructure Security Agency, CISA）共同制定之安全 AI 系統開發指引（Guidelines for secure AI system development）、美國國家標準與技術研究院（National Institute of Standards and Technology, NIST）推出之 AI 風險管理框架等。

為支援系統所有者（system owners），CSA 與 AI 暨資安業者（AI and cybersecurity practitioners）合作，以研議《配套指引》，其內容涵蓋產學界之實用措施、安全控管與最佳實踐。

CSA 建議系統所有者於 AI 之生命週期，以整體觀點（holistic perspective）識別與減少安全風險。並於《安全指引》提出，於 AI 生命週期的五個關鍵階段，須留意之重點：

1. 規劃與設計階段

(1) 提升安全風險意識與能力：組織應了解 AI 潛在風險，並向所有人員（包括 AI 開發人員、系統所有者及高階主管）提供充分之 AI 安全風險培訓與指導。

(2) 進行安全風險評估：以安全風險評估為基礎，制定風險管理策略。依據相關產業標準或最佳實踐之整體流程，建構 AI 之威脅與風險模型（model threats and risks to an AI system）。

2. 開發階段

(1) 確保供應鏈安全

AI 供應鏈包括但不限於訓練資料、模型、API 與軟體庫。應評估、監控 AI 供應鏈生命週期之潛在安全風險。確保供應商遵守安全政策與國際標準，或以其他方式適當地管理風險。可考慮評估供應鏈元件，例如：透過軟體材料清單、檢查原始碼或漏洞資料庫。

本報告之智慧財產權歸屬於國發會

(2) 選擇 AI 模型時，應考量安全性優點並作出取捨

由於機器學習、深度學習、生成式 AI 等不同的 AI 模型皆具有其特徵與風險，例如：大型語言模型可能容易受到輸入操作攻擊（input manipulation attacks），因此需要不同的安全措施。在為系統開發或選擇合適的 AI 模型時，需考慮可能影響其安全性的因素，例如：複雜性、可解釋性、可理解性及訓練資料的敏感性。

(3) 識別、追蹤及保護「與 AI 相關之資產」

隨業務營運越來越頻繁應用 AI 系統，AI 系統將成為組織策略資產之一部分，亦應對其採取相應之保護措施。為避免敏感資料、智慧財產權及組織資產面臨潛在威脅與外洩之風險，需了解 AI 相關資產之價值，包括模型、資料、指令（prompts）、電子形式軌跡資料（Log）與評估（assessments）。建立一個涵蓋追蹤、身分驗證、版本控管與保護資產之流程。

(4) 保護 AI 開發環境

AI 模型開發需要取得大量訓練資料，而不安全的 AI 開發環境可能導致相關風險之發生，例如：個人識別資訊或機密商業資訊等資料外洩之風險；AI 模型受到中毒等攻擊之風險，導致模型行為異常，或面臨竊取、未經授權而複製或濫用 AI 模型及其他智慧財產權之風險。應採用基礎設施安全之作為，例如：實施適當之接觸控管與電子形式軌跡資料/監控、環境隔離以及預設安全設定。

3. 部署階段

(1) 保護 AI 系統之部署基礎設施與環境

本報告之智慧財產權歸屬於國發會

應用標準基礎設施安全原則，例如：接觸控管、電子形式軌跡資料紀錄/監控、環境隔離、預設安全設定與防火牆。

(2) 建立事件管理程序

鑑於 AI 應用之多樣性及行為預測之困難，AI 涉及之事件範圍可能涵蓋從聊天機器人故障等小問題到關鍵基礎設施運行中斷等關鍵事件。系統所有者應制定適當的事件回應、升級（escalation）與補救計畫（remediation plans）。

(3) 負責任地發布 AI 系統

濫用、資料外洩等 AI 系統風險之發生，將影響使用者之信任與組織聲譽。故組織應先對模型、應用程式或系統進行合適且有效之安全檢查與評估後再發布 AI 系統。

4. 營運與維護階段（Operations and Maintenance）

(1) 監控 AI 系統輸入

基於第三方可能出於隱私原因而未採取監控措施，AI 系統所有者可能希望監控並紀錄 AI 系統的輸入內容，例如：查詢、指令與需求。電子形式軌跡資料之留存，應符合法遵、審計、調查與提供適當之救濟措施。

(2) 監控 AI 系統輸出與行為

AI 系統可能在生產階段出現故障或效能下降，監控 AI 可確保其運作順利，並提醒 AI 系統所有者潛在問題。營運商需監控可能表示入侵系統、資料外洩或資料飄移（data drift）之異常行為。

本報告之智慧財產權歸屬於國發會

(3) 採取以安全始於設計（secure by design）之原則，持續更新 AI 並使之持續學習

更動資料與模型可能影響 AI 行為之變化，系統所有者應確保已考慮並適當管理與模型，並更新相關之風險。

(4) 建立漏洞揭露流程

除監控機制，亦應建立一回饋流程，以供使用者回饋意見，可能藉此發現系統之潛在漏洞。

5. AI 生命週期結束階段（End of Life）

(1) 確保正確之資料與 AI 模型處理（disposal）

由於仰賴大量訓練資料（包含潛在的機密資訊）以訓練 AI 模型，處理不當可能導致資料外洩等事件，應依據相關產業標準或法規，對訓練資料與 AI 模型進行適當、安全的處置或銷毀。

CSA 建議組織領導者、事業、AI 暨資安業者參考 CSA 之指引，以安全地實施 AI 系統，確保 AI 系統係以安全為設計，並建立使用者信心，相信 AI 將依原定計畫執行，並產生創新、安全與有效之結果。

資料來源：

1. CSA, Launch of Guidelines and Companion Guide on Securing Artificial Intelligence Systems, 2024-10-15, https://www.csa.gov.sg/News-Events/Press-Releases/2024/launch-of-guidelines-and-companion-guide-on-securing-artificial-intelligence-systems (last visited 2024/10/22)
2. CSA, Guidelines and Companion Guide on Securing AI Systems, 2024-10-15, https://www.csa.gov.sg/Tips-Resource/publications/2024/guidelines-on-securing-ai (last visited 2024/10/22)

本報告之智慧財產權歸屬於國發會

3. Digital Watch, Singapore launches comprehensive guidelines to secure AI systems, 2024-10-16, https://dig.watch/updates/singapore-launches-comprehensive-guidelines-to-secure-ai-systems (last visited 2024/10/22)

六、 澳洲

(一)2024 年 10 月澳洲資訊委員辦公室發布《隱私、開發及訓練生成式 AI 模型之指引》

澳洲資訊委員辦公室（Office of the Australian Information Commissioner, OAIC）於 10 月 21 日發布《隱私、開發及訓練生成式 AI（AI）模型之指引》（Guidance on privacy and developing and training generative AI models，下稱《指引》）。當 AI 開發人員使用大量資料作為生成式 AI 之訓練資料，其應考量訓練資料是否包含個人資料（下稱個資）。倘使用大量個資作為 AI 訓練資料，將使開發 AI 模型成為具有高隱私風險之活動。

《指引》非以全面概述開發 AI 模型之所有隱私風險為其目的，而側重於 1988 年《隱私法》、澳洲隱私原則（Australian Privacy Principles, APPs）第 1、3、5、6 及 10 條內容所涉及關於規劃、設計生成式 AI 以及編輯（compiling）資料集，用以訓練或微調生成式 AI 模型之相關注意事項。

以下簡要說明《指引》提出針對訓練 AI 模型之隱私考量因素的五大重點：

1. 開發人員應採取合理措施，以確保生成式 AI 模型之準確性及降低 AI 生成內容可能增加之風險，包括使用高品質的資料集，並進行適當的測試。使用免責聲明，以表示針對特定之高隱私風險用途 AI 模型，需要採取適當、額外之保護措施。

本報告之智慧財產權歸屬於國發會

2. 公開資料或得以其他方式取得之資料，不代表該資料可作為AI之合法訓練資料。AI開發人員應審酌其蒐集或預計使用之資料，是否涵蓋個資，並遵守隱私保護之義務。開發人員可能需要採取額外的措施，例如：刪除資訊，以確保其符合隱私保護義務。

3. 開發人員應特別留意是否敏感個資之取得或利用，此類資訊多以取得同意作為蒐集之要件。例如：照片、音檔（涵蓋AI生成之照片、音檔）等，皆可能包含敏感個資。於未取得同意前，可能無法從網路抓取或從第三方資料集蒐集上開敏感資料。

4. 倘開發人員欲將已持有（already hold）之個資用於訓練AI模型，該利用若非屬於原先蒐集個資之目的，開發人員應仔細評估其應負擔之隱私保護義務。倘當事人未同意將其個資用於與AI相關之次要目的，開發人員應能確保當事人可合理預期個資之二次利用，並應特別考量蒐集個資或敏感個資之主要、直接相關目的。

5. 為減少監管風險，當開發人員無法明確提出合理且與主要目的相關之「AI相關之二次利用」之理由時，應徵求當事人對於其個資之新利用目的之知情同意或提供當事人選擇退出（opt-out）的權利。

資料來源：

1. OAIC, Guidance on privacy and developing and training generative AI models, 2024-10-21, https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-developing-and-training-generative-ai-models (last visited 2024/10/24)

本報告之智慧財產權歸屬於國發會

七、 中國大陸

(一)2024 年 11 月中國大陸中央網路安全與資訊化委員會辦公室發布針對 AI 生成內容標示之相關辦法及配套措施，並對外徵求意見

中國大陸中央網路安全與資訊化委員會辦公室於 2024 年 9 月 14 日發布《AI 生成合成內容標示辦法（徵求意見稿）》（下稱《AI 生成內容標示辦法》）及其配套標準《網路安全技術 AI 生成合成內容標示方法（徵求意見稿）》（下稱《AI 生成內容標示方法》）進行對外意見徵詢。《AI 生成內容標示辦法》於 10 月 14 日截止徵求意見。《AI 生成內容標示方法》於 11 月 13 日截止徵求意見。

以下說明《AI 生成內容標示辦法》（共 14 條）、《AI 生成內容標示標準》（共 6 點）之重點。

1. 法理依據

依據《AI 生成內容標示辦法》第 1 條規定，其法源依據為《網路安全法》、《網路資訊服務演算法推薦管理規定》、《網路資訊服務深度合成管理規定》、《生成式 AI 服務管理暫行辦法》等法律、行政法規與機關規定。

《AI 生成內容標示方法》則係依據《AI 生成內容標示辦法》第 11 條要求服務提供者應依據強制性國家標準之要求進行標示之規定，所訂定之配套措施。

2. 適用對象

《AI 生成內容標示辦法》第 2 條規定，適用於中國大陸境內透過演算法推薦技術、深度合成技術或生成式 AI 技術之網路資訊服務提供者（下稱服務提供者）；並排除適用於「研發、應用 AI 生成合成技術，且未提供中國大陸境內民眾服務

本報告之智慧財產權歸屬於國發會

之產業組織、事業、教育與研究機構、公部門、相關專業機構等」。

3. AI 生成合成內容與標示之定義

(1) 《AI 生成內容標示辦法》第 3 條規定，AI 生成合成內容係指利用 AI 技術製作、生成、合成之文字、圖片、音檔、影片等資訊。

(2) AI 生成合成內容之標示包括顯性、隱性標示。

顯性標示，依前述條文規定，係指於生成合成內容或其交互畫面，以文字、聲音、圖片等方式加上可被使用者明顯感知之標示。

隱性標示，依據《AI 生成內容標示方法》第 3 點之規定，係指於生成合成文件資料，加上不能被使用者直接感知，但能透過技術手段獲取之標示。

4. 服務提供者之標示、提醒義務

(1) 依《AI 生成內容標示辦法》第 4 條、第 5 條規定，服務提供者對於不同型態之 AI 生成合成內容，須負顯性或隱性標示之義務。《AI 生成內容標示方法》第 5 點、第 6 點進一步提供顯性或隱性標示之方法說明。

關於顯性標示，以文字型態之生成合成內容為例，應於文章開頭、中間或文章結尾以文字或上標文字（如次方符號）（1）標示 AI 因素：如「人工智能」或「AI」、；（2）標示「生成和/或合成」；（3）使用清楚可識別之字型、顏色。

本報告之智慧財產權歸屬於國發會

關於隱性標示，包括但不限於在加入「生成合成內容之相關資訊、服務提供者名稱」等，並鼓勵服務提供者在生成合成內容添加「浮水印」。

《AI 生成內容標示方法》並進一步指出隱性標示為「詮釋資料（metadata）之隱性標示」，即「以特定原始碼格式嵌入文件之描述性資訊，用以記錄文件來源、類型、用途及著作權等資訊」。隱性標示應包括之因素如下：（1）生成合成內容之標籤因素：將 AI 生成合成內容依類型標籤，包括「確定、可能、疑似」；（2）生成合成服務提供者之名稱或原始碼；（3）生成合成服務提供者對該內容的唯一編號；（4）內容傳播服務提供者的名稱或原始碼；（5）內容傳播服務提供者對於該內容的唯一編號。

《AI 生成內容標示方法》之附件 E、F 提供詮釋資料之隱性標示應符合之具體格式及範例。附件 E 指出，「確定」為 AI 生成合成內容，標記為 1；「可能」為生成合成內容，標記為 2；「疑似」為 AI 生成合成內容，標記為 3。附件 F 提供範例，生成合成服務提供者出於安全防護，對詮釋資料之資訊以雜湊值作為數位簽章。

(2) 依《AI 生成內容標示辦法》第 8 條規定，服務提供者應於使用者服務契約明確說明 AI 生成內容之標示相關規定，並提醒使用者仔細閱讀並理解相關內容。

5. 平臺之審核、提醒及標示義務

依《AI 生成內容標示辦法》第 6 條規定，針對「提供網路資訊之內容傳播平臺」，應負審核文件詮釋資料是否含有隱性標示之義務，對於 AI 生成合成內容含有隱性標示者，平臺負有「增加標示，以提醒使用者該內容屬於生成合成內容之義務」，以及於平臺提供必要之標示功能。

本報告之智慧財產權歸屬於國發會

依《AI 生成內容標示辦法》第 7 條規定，針對「網路應用程式平臺」於應用程式上架前，應審核服務提供者是否依規定標示 AI 生成合成內容。

6. 使用者之標示義務

依《AI 生成內容標示辦法》第 10 條規定，使用者向提供網路資訊內容傳播平臺服務之服務提供者上傳 AI 生成合成內容時，應主動聲明並使用平臺提供之標示功能。

《AI 生成內容標示方法》之項目進度分為起草、徵求意見、審查、核准及發布，預計於發布後 6 個月實施。

資料來源：

1. 人民網，網路安全與資訊化委員會辦公室關於《AI 生成合成內容標示辦法（徵求意見稿）》公開徵求意見之通知，2024-09-14，http：//finance.people.com.cn/BIG5/n1/2024/0914/c1004-40320629.html（最後瀏覽日：2024/11/07）。

2. 《網路安全技術 AI 生成合成內容標示方法（徵求意見稿）》，2024-09-01，https://www.tc260.org.cn/upload/2024-09-14/1726290836419027596.pdf（最後瀏覽日：2024/11/07）。

3. 國家標準《網路安全技術 AI 生成合成內容標示方法（徵求意見稿）》編制說明，2024-09-13，https://www.tc260.org.cn/upload/2024-09-14/1726280659951007638.pdf（最後瀏覽日：2024/11/08）。

八、 國際合作

(一)2024 年 11 月英國與新加坡簽署 AI 安全合作之合作備忘錄，強化於網路安全、公共數位服務等領域之合作

本報告之智慧財產權歸屬於國發會

英國創新科技部（Department for Science, Innovation and Technology, DSIT）於 11 月 6 日發布新聞，說明英國與新加坡已簽署 AI 安全合作之合作備忘錄（The Memorandum of Cooperation (MoC) on Collaboration on the Safety of Artificial Intelligence），雙方同意強化 AI 安全與治理，以提高 AI 科技在研發與使用過程之安全性與可靠性，進而提高公眾對於 AI 應用之信任。

此一合作備忘錄係源於英國與新加坡雙方政府自 2022 年開始，陸續簽署數位經濟協議（UK-Singapore Digital Economy Agreement, UKSDEA）及數位政府服務備忘錄（an MoU on Digital Government Services）等，雙方同意在網路安全、公共數位服務及相關領域持續合作。

前述合作備忘錄之重點，在於確保 AI 系統之可信度，即讓 AI 能按照預期規劃執行作業，並確保 AI 運作之公平、透明及保護隱私，進而提升公眾對於該 AI 系統或相關應用之信任。據統計，目前英國 AI 相關領域有 524 家事業，已僱用 12,000 位員工，每年創造近 10 億英鎊之產值。上開合作備忘錄簽署後，英國政府認為確保 AI 系統可信度之市場在未來 10 年內將可成長 6 倍，且因英國各界亦將利用 AI 促進發展，預估可創造近 65 億英鎊的相關收入。

為確保 AI 應用之安全性與可靠性，英國政府已建立一個 AI 保障平臺（AI assurance platform），透過一站式服務，使英國事業獲取相關資訊，以利識別或減輕 AI 帶來之潛在風險與危害。該平臺並提供相關指引與實用資源，如：列出明確步驟，協助企業進行影響評估，以及審查 AI 系統中使用之資料是否存有偏見，確保人們對於日常使用 AI 之信任。該平臺亦針對中小企業，提供自我評估工具，以落實負責任之 AI 管理，並在研發與使用 AI 系統時，可做出更佳決策。這些資料目前正對外徵求意見，徵求意見之截止日期為 2025 年 1 月 29 日。

本報告之智慧財產權歸屬於國發會

英國政府並將透過推動保障平臺相關服務，與業界共同研商訂定AI科技發展路線圖（roadmap），有助於引領AI保障國際標準之發展。

資料來源：

1. DSIT, Ensuring trust in AI to unlock £6.5 billion over next decade, 2024-11-06, https://www.gov.uk/government/news/ensuring-trust-in-ai-to-unlock-65-billion-over-next-decade (last visited 2024/11/20)
2. MDDI, New Singapore UK Agreement to Strengthen Global AI Safety and Governance, 2024-11-06, https://www.mddi.gov.sg/new-singapore-uk-agreement-to-strengthen-global-ai-safety-and-governance/ (last visited 2024/11/20)

九、 經濟合作暨發展組織

(一)2024年11月OECD發布《評估AI之未來潛在風險、優勢與重要政策》報告

鑒於AI技術之快速發展，政策制定者應考量並因應AI驅動之變革。經濟合作暨發展組織（Organization for Economic Cooperation and Development, OECD）因而成立AI未來專家小組（Expert Group on AI Futures）以預測AI發展與其潛在影響。該小組於2024年11月14日發布《評估AI之未來潛在風險、優勢與重要政策》報告（Assessing Potential Future Artificial Intelligence Risks, Benefits and Policy Imperatives）。

以下說明《評估AI之未來潛在風險、優勢與重要政策》報告之風險、優勢與政策要點：

1. 十個應優先評估之風險，例如：日益複雜之惡意網路犯罪；操縱（manipulation）、虛假資訊、詐欺以及因此而導致對民主與社會向心力之損害；由於對AI的安全性與可信度缺乏足夠的

本報告之智慧財產權歸屬於國發會

投入，致使開發與部署 AI 系統的競賽造成危害；以不適合的方式（inadequate methods）將 AI 系統之目標結合人類利害關係人的偏好與價值觀，可能導致意外損害；權力集中於少數事業或國家；於關鍵系統中發生輕微至嚴重的 AI 事故；侵入式監控與侵犯隱私；治理機制與機構無法跟上 AI 的發展；AI 系統欠缺足夠的可解釋性，削弱問責制；加大不平等與國與國間之貧富差距。

2. 十項 AI 帶來之優勢，例如：加速科學進步；經濟成長、生產力及生活水準提升；減少不平等與貧窮；有助於解決急迫且複雜的議題，包括減緩氣候變遷與推動其他永續發展目標；有助於決策、判斷與預測；改善資訊生產與分發；提升醫療與教育服務；提升工作品質；公民、社會及社會夥伴賦權；改善機構透明度與治理，促進監控與評估。

3. 十項 AI 未來之政策要點

(1) 制定更明確的規則，包括針對 AI 造成損害之責任歸屬。定義 AI 之事故與危害，包括：損害個人或群體的健康；破壞關鍵基礎設施之營運與管理；依據保護勞工、智慧財產權之相關法律，產生人權之侵害或違反法定義務；對財產、社區（communities）或環境造成損害等。

(2) 考慮「限制或預防 AI 使用特定紅線（red line）」之方法。為推動值得信賴的 AI，專家團體提倡針對可能不尊重人權或隱私權之 AI 開發或應用設定紅線，例如：大規模監控、監控公共場所、利用 AI 進行惡意網路活動、致命性自主武器系統等。

(3) 要求或促進「揭露部分類型之 AI 系統之關鍵資訊」。揭露之範圍可能為 AI 模型卡，其涵蓋標準化資訊與訓練資料

本報告之智慧財產權歸屬於國發會

特徵之 AI 模型說明書等。所謂之資料特徵例如：目的、成分、預期用途與潛在偏見。

(4) 確保可能帶來高風險之 AI 系統之生命週期全程遵循風險管理程序。

(5) 減緩激烈地開發與部署 AI 之競賽，透過國際合作可促進公平競爭。

(6) 投資 AI 安全與可信度方法之研究，包括：AI 對齊（AI alignment），（指引導 AI 系統的發展方向符合設計者的利益與預期目標）；能力評估；人類能夠理解的可解釋性（interpretability）；可解釋性（explainability）以及透明度。

(7) 促進教育、再培訓及重塑技能（reskilling）之機會，以因應勞動力市場對 AI 技能之需求逐步增長。OECD 預估，開發、適用與使用 AI 所需的技能將越來越重要，而許多國家既有的公共政策仍不足。AI 技能需要結合學校教育與在職學習。此外，由於 AI 促進自動化工作的範圍，其中部分工作需要進一步關注教育與再培訓工作，以因應潛在風險。

(8) 賦予利害關係人與社會權力，以協助建立信任與強化民主。

(9) 緩解過度集權。專家考量可透過制定或修訂法規、強力的監管執法、監督與追蹤高運算能力之 AI 系統、利益分配（如促進分散 AI 所有權與國際技術標準）等方式解決權力過度集中的問題。

(10) 採取標靶行動（targeted actions）推動具體之 AI 未來優勢。專家建議政府關注並投資於 AI 可實現之優先收益。

資料來源：

本報告之智慧財產權歸屬於國發會

1. OECD, Assessing potential future artificial intelligence risks, benefits and policy imperatives, 2024-11-16, https://www.oecd.org/en/publications/assessing-potential-future-artificial-intelligence-risks-benefits-and-policy-imperatives_3f4e3dfb-en.html (last visited 2024/11/21)

參、 數位政策

一、 歐盟

(一)2024 年 10 月歐盟創新理事會發布 2025 年計畫要項，預計投資 14 億歐元以提升研發創新能量與促進戰略科技之發展

歐盟創新理事會（European Innovation Council, EIC）於 10 月 29 日發布新聞，宣布將於 2025 年投資 14 億歐元，以深度技術研究（deep tech research）及高潛力新創事業（high-potential start-ups）為主；此一計畫金額較 2024 年增加 2 億歐元。另外，創新理事會之戰略科技平台（EIC Strategic Technologies for Europe Platform, STEP）也將規劃擴大計畫範圍，並鼓勵股權融資等。

EIC 係於 2021 年成立，屬於《展望歐洲（Horizon Europe）》框架計畫項目之一。其於 2025 年之補助計畫主要包含 3 項：1. EIC 尋路者（EIC Pathfinder），預計投資 2.62 億歐元，鼓勵跨領域之研發團隊，進行早期科技之研發，以利技術突破；此一計畫最高可獲得 400 萬歐元之補助。2. EIC 轉型計畫（EIC Transition），預計投資 0.98 億歐元，鼓勵將研發成果進行概念驗證或其他創新；此一計畫最高可獲得 250 萬歐元之補助。3. EIC 加速器（EIC Accelerator），預計投資 6.34 億歐元，主要補助新創事業或中小型企業對擴大市場或顛覆市場之創新進行研發、商品化。

此外上開計畫除投資金額較 2024 年增加外，於 2025 年亦將有不少推動亮點。以 EIC STEP 為例，2025 年將投資 3 億元（2025 至 2027

本報告之智慧財產權歸屬於國發會

年共將投資 9 億元），預計讓導入歐盟戰略科技之事業，每家可獲得 EIC 基金投資 1,000 萬至 3,000 萬不等之金額，並吸引私部門共同參與投資，希望總額達到 5,000 萬至 1.5 億歐元。另外，EIC STEP 規劃擴大計畫範圍，將有助於解決深度技術研究資金之缺口，例如淨零或生物科技等。

除此之外，EIC 尚預計投資 1.2 億歐元在新興科技上，包含；自主機器人、能適應氣候變遷之作物，及將廢棄物轉換新材料。另也將投資 2.5 億歐元給運用早期科技之事業，包含：生成式 AI、太空、農業科技，以及未來行動科技解決方案。而且，對於來自研究與創新績效較低的國家之新興事業，歐盟也將優先提供服務，讓這些事業可以獲得更多機會。

資料來源：

1. EC, European Innovation Council to invest €1.4 billion in deep tech and scale up of strategic technologies in 2025, 2024-10-29, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5386 (last visited 2024/11/06)

二、英國

(一)2024 年 10 月英國政府宣布將成立新的創新監管辦公室，以加速民眾享受新興科技之機會

英國創新科技部（Department for Science, Innovation and Technology, DSIT）於 10 月 8 日發布新聞，英國政府將成立新的創新監管辦公室（Regulatory Innovation Office, RIO），以減少過往之複雜審查程序，加速民眾享受新興科技之機會。

英國政府認為，科技創新有利於推動經濟成長。基此，成立新的 RIO 以減少相關程序或負擔為主，讓創新之商品或服務可快速運用於

本報告之智慧財產權歸屬於國發會

商業或其他用途。舉例而言，讓外科醫生熟悉 AI 相關軟體，可提供病患更精準之治療或手術。而無人機可以提高既有業務之效率，將貨物運送至偏遠地區。

目前 RIO 將優先支援 4 項發展快速之領域，以符合英國產業之需求，其包含：

1. 生物工程學（Engineering biology）：此一領域主要運用合成生物學（synthetic biology）及生物科技，以創造新的商品或服務。如透過創新之疫苗或療法，用以改善健康；創造更潔淨之燃料、抗蟲作物或養殖肉類，協助糧食生產或促進永續發展。RIO 將確保相關商品或服務之安全，並節省審查時程讓其可快速投入市場。

2. 航太（Space）：隨著航太產業相關科技之創新，如手機 GPS 或通訊系統，有利於改善天氣預報或災難應變系統。為維持此一領域之發展，監管部分需要提高彈性與明確規範，以協助並促進競爭、鼓勵投資及開放市場進入。

3. 運用於醫療保健之 AI 與數位化（Artificial Intelligence and digital in healthcare）：由於英國國家醫療服務系統（National Health Service, NHS）面臨之壓力逐年增加，AI 將可改變醫療相關服務，讓醫生能夠更快速診斷疾病並改善病患後續護理。且 AI 亦可協助提升醫院經營效率，並減少醫務人員管理負擔及病患等待時間等。甚至未來還可能協助實現客製化藥物，為個人量身訂做其醫療方式。RIO 將支援醫療相關部門安全地部署 AI 之創新，與提高 NHS 效率及病患之健康。

4. 聯網與自動化科技（Connected and autonomous technology）：無人機或其他自動駕駛車輛可快速且有效地向偏遠地區運送緊急物資，爰批准此一領域之科技應用，有助於支援緊急事件發生時之因應。

本報告之智慧財產權歸屬於國發會

然而，由於部分科技創新應用涉及跨領域，分屬不同部會，無法適用於現行監管架構，因此勢必造成審查時間過長，或有障礙等。此一創新監管辦公室（RIO）除負責監管外，也將加快審查程序，並擔任協調角色，讓不同監管機關或機構之間可以順利合作。該辦公室亦將向 DSIT 或其他部會通報影響創新之障礙，將解決相關議題列為優先目標，並支援各不同監管機關或機構，使英國各機關（構）具備滿足解決方案或促進經濟成長之能力。

資料來源：

1. DSIT, Game-changing tech to reach the public faster as dedicated new unit launched to curb red tape, 2024-10-08, https://www.gov.uk/government/news/game-changing-tech-to-reach-the-public-faster-as-dedicated-new-unit-launched-to-curb-red-tape (last visited 2024/10/16)

三、 韓國

(一)2024 年 11 月韓國量子科技與量子產業促進法(양자과학기술 및 양자산업 육성에 관한 법）已正式施行

韓國科學技術情報通訊部(과기정통부)於 10 月 31 日發布新聞，2024 年 11 月韓國量子科技與量子產業促進法（양자과학기술 및 양자산업 육성에 관한 법）正式施行。該法前於 2023 年 10 月通過，計 33 條，主要內容包含：訂定量子中長期發展計畫，成立跨部會委員會，將指定研究中心以利技術研發，建立產業生態系，及支持國際合作等內容。

據科學技術情報通訊部之說明，該法重點主要包含：

本報告之智慧財產權歸屬於國發會

1. 建立完善發展體系，如建置量子科技（如涉及通訊、IoT、運算）研究基地，並透過系統化方式發展量子產業。（該法第 1 條，如立法目標、第 2 條名詞定義及第 3 條國家責任等。

2. 集中政府資源，發展量子科技與量子產業。規範重點如成立跨部會委員會（第 7 條），由國務總理擔任主席，成員最多 20 人，包含公、私部門代表，並訂定 5 年期發展計畫（第 5、6 條），及政府應考量對國防、高科技產業之影響，且評估量子科技對加密技術之影響與因應措施，如可能衝擊公共服務及金融領域（第 10 條）。

3. 建立產學研合作基地或產學合作機制，匯集量子相關產學研能量，以培育量子科技與量子產業。規範重點包含指定量子科技研究中心（第 18 條），以投入中央與地方政府資源；且除訂定 5 年期發展計畫與其細節外，尚規劃建立產學合作機制，及主管機關之權責，如指定、變更或取消等內容（第 24 至 28 條）。

4. 打造量子生態系，特別是透過教育機構協助培育人才，並吸引與運用優秀人才。規範重點包含鼓勵大學校院培育人才，以引領量子科技與量子產業生態系（含技術研發、資源及人才培育）之發展或提供相關支援（第 21 至 23 條）。

5. 促進量子科技研發成果商業化，並推動量子產業之發展，形成良性循環。規範重點包含支援新創企業發展，並促進研發成果商業化（第 14、16 條）。且為積極推動產業化，規定專屬授權應附加於 3 年內要求實施之條件（第 13 條）。

6. 推動國際合作，並維持韓國領先地位。規範重點包含促進國際合作研發、海外培訓及人才交流，以及支持私部門參與及標準化（第 29 條）；並希望吸引優秀之國外研究中心至韓國設置（第 30 條）。

本報告之智慧財產權歸屬於國發會

資料來源：

1. 과기정통부（Ministry of Science and ICT）,「양자과학기술 및 양자산업 육성에 관한 법」시행!, 2024-10-31, https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=238&pageIndex=3&bbsSeqNo=94&nttSeqNo=3185059&searchOpt=ALL&searchTxt= (last visited 2024/11/13)
2. 국가법령정보센터에서, 양자과학기술 및 양자산업 육성에 관한 법률, 2023-10-31, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%96%91%EC%9E%90%EA%B3%BC%ED%95%99%EA%B8%B0%EC%88%A0%EB%B0%8F%EC%96%91%EC%9E%90%EC%82%B0%EC%97%85%EC%9C%A1%EC%84%B1%EC%97%90%EA%B4%80%ED%95%9C%EB%B2%95%EB%A5%A0/(19784,20231031) (last visited 2024/11/13)

(二)2024 年 11 月韓國政府將採行提升處罰強度與強化網路平臺問責等 4 大領域措施，打擊深度偽造與性犯罪

韓國科學技術情報通訊部（과기정통부）於 11 月 6 日發布新聞，為打擊深度偽造（deepfake）與性犯罪，政府將採行提升處罰強度、強化網路平臺問責、及時保護受害者，及客製化預防教育計 4 大領域之 10 項措施，由政府政策協調辦公室（該辦公室於 2024 年 8 月成立，成員包含教育部、司法部、國防部及科學技術情報通訊部等）負責協調，並由各主管機關，如教育部、司法部或韓國警察廳協助推動。關於各領域與執行重點，分別摘要如下：

1. 提升處罰力度，包含擴大調查執法，與加強國際司法合作 2 項措施。主要重點為加強對深偽影片之處罰，例如：2024 年 9 月已修正性暴力預防法，除處罰拍攝、散布者外，對於擁有、購買或儲存相關影片者，最高可處 3 年有期徒刑，或 3,000 萬

本報告之智慧財產權歸屬於國發會

韓元以下之罰金。至於國際合作部分，將透過網路犯罪公約（Cyber-crime Convention）之規範，及結合國際合作網路，如美國 FBI、國際刑警組織進行調查或蒐集資訊。

2. 強化網路平臺問責，包含加強平臺之義務，與國內外業者建立合作體系等 2 項措施。主要重點為強化平臺經營者之義務，如：通報主管機關，或指定當地之代理人，並履行防止非法視訊等義務。國內外業者如 Naver、Kakao、SKT、MS 韓國、Google 韓國等也建立合作體系，以提供諮詢管道，或視法院、調查機關等需求，提供必要之協助。

3. 即時保護受害者，包含強化刪除相關資料之支援、由支援中心提供一站式服務、影像視訊深偽之預防，及檢測技術之研發等 4 項措施。主要重點為即時刪除相關資料，若收到相關請求時，較難判斷是否屬於性犯罪資料，可以先屏蔽該資料，並向主管機關請求協助審查後再予刪除。且依修正之性暴力預防法，已成立一站式服務之支援中心，受理受害者之檢舉或相關事宜等。

4. 客製化預防教育，包含對不同對象提供客製化教育，與提高公眾意識 2 項措施。主要重點為區分大學、國高中、小學，甚至是家長、老師等不同對象，進行預防教育，提供手冊或資訊，以提升意識。教育部與相關部會亦邀請名人代言，共同製作宣導短片，並在 YouTube 或機關官網上播放宣導短片。

資料來源：

1. 과기정통부（Ministry of Science and ICT）, 정부, 이미지 영상 조작(딥페이크) 성범죄 대응 위한 , 4 대 분야 10 개 과제 추진, 2024-11-06, https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=238&pageIndex=3&bbsSeqNo=94&nttSeqNo=3185085&searchOpt=ALL&searchTxt= (last visited 2024/11/20)

本報告之智慧財產權歸屬於國發會

2. 과기정통부（Ministry of Science and ICT）, 딥페이크 성범죄 대응 방안, 2024-11-06, https://doc.msit.go.kr/SynapDocViewServer/viewer/doc.html?key=ef0add67326d405f8faa0e0cb5bf4013&convType=html&convLocale=ko_KR&contextPath=/SynapDocViewServer/ (last visited 2024/11/20)

肆、 數位身分

一、 歐盟

(一)2024 年 10 月歐盟宣布將開發數位旅行應用程式，內含數位護照與數位身分證，預計 2030 年推出

歐盟執委會（European Commission, EC）於 10 月 8 日發布新聞，其已通過 2 項提案，包含 1. 提出一項數位旅行憑證（Digital travel credentials）之架構，以利使用數位護照與數位身分證，及 2. 將開發數位旅行應用程式（EU Digital Travel application），支援數位護照與數位身分證之應用。這些提案之目標，係透過規範架構及提供儲存相關證件資料數位版本之應用程式，以實現更輕鬆、安全之旅行。

目前歐盟與非歐盟公民在跨越歐盟邊境時，都需要經過系統性檢視。依 2023 年統計，有近 6 億人次之邊境進出紀錄，基此，應加快邊境管制並確保旅行或往來更加順暢，保持高水準之安全，且確保每位旅客都受到檢查。

目前規劃之數位旅行應用程式將由歐盟所資助之 eu-LISA 進行開發，預計 2030 年推出。且相關資料將在數位旅行憑證之架構下，包含原護照與身分證內晶片所含之資訊，如證件所有者之臉部影像，但不包含指紋。而數位旅行憑證之資料可存於手機內，且由旅客自願性安裝並使用該數位版本之文件。

本報告之智慧財產權歸屬於國發會

依執委會預估，使用數位旅行憑證與數位旅行應用程式將有助於達成以下事項：

1. 讓旅客往來更順利、過境更快速：歐盟與非歐盟公民往返需經過歐盟邊境時，可於出發前提交數位護照或數位身分證，以便提前進行邊境檢查。

2. 促進歐盟公民行動自由並減輕行政負擔：成員國可允許歐盟公民使用數位身分證進行登記與身分識別。舉例來說，A 國公民可使用數位身分證在B國居住時，向B國政府進行登記，或說明其係有計畫地來 B 國旅行。

3. 提高邊境管制效率：藉由數位旅行憑證實現提前檢查之外，還可讓各邊境管理單位能集中時間與資源，以偵查跨境不法分子或偷渡者。

4. 提高申根區（Schengen area）之安全：因為數位旅行憑證讓各成員國更易驗證相關證件之真實性與完整性，進而讓不法分子難以使用虛假證件，或在未被發現之情形下通過歐盟邊境。

此 2 項提案將有助於落實 2021 年通過之申根政策（Schengen strategy），其希冀促進歐盟境內人員可自由流動，並採數位化之方式。且該提案亦與歐盟數位身分錢包（European Digital Identity Wallets）有關，數位護照及數位身分證可與數位駕照或相關醫療紀錄一同儲存。目前相關提案由執委會提出，後續將由歐盟理事會與歐洲議會達成共識。一旦通過，尚將按照程序訂定數位旅行應用程式與其必要之技術標準。

資料來源：

1. EC, Commission proposes an EU Digital Travel application for easier and safer travel, 2024-10-08, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5047 (last visited 2024/10/16)

本報告之智慧財產權歸屬於國發會

二、日本

(一)2024 年 11 月日本數位廳繼續辦理電子簽章法認證標準現代化相關之第 2 次研究會議，討論如何兼顧雲端或遠端存取等管理與合規之議題

日本數位廳於 11 月 1 日發布新聞，繼 2024 年 9 月已辦理電子簽章法現代化第 1 次研究會議（電子署名法認定基準のモダナイズ検討会（第 1 回））後，續於 11 月 1 日邀集法律與技術相關專家學者，第 2 次討論該法施行後遭遇之問題。

由於修正後之電子簽章與認證服務法（電子署名及び認証業務に関する法律），簡稱電子簽章法（電子署名法），預計於 2025 年（令和 7 年）6 月施行。因先前在實務上仍有部分疑義，數位廳彙整 2023 年（令和 5 年）實務遭遇之 6 項議題，作為相關會議討論重點。9 月第 1 次會議已討論 2 項，包含：1. 欠缺歐洲電信標準協會（European Telecommunications Standards Institute, ETSI）建議之風險管理措施；及 2. 該法憑證發行機構之私鑰加密技術與美國國家標準與技術研究院（National Institute of Standards and Technology, NIST）提出之聯邦資訊處理標準（FIPS）140-3（目前應可符合 FIPS 140-2）有所差異。

2024 年 11 月 1 日辦理之第 2 次會議，繼續討論其他 4 項議題，重點包含：3. 如何在滿足國際標準下，同時符合雲端服務之需求，例如：使用雲端有何好處，但該如何符合硬體密碼模組（Hardware Security Module, HSM）或相關標準，及其審查方法為何；4. 獲認證機房遠端控制與使用公有雲之管理，如認證機構設備需求，或遠端存取（VPN）管理等，及其審查方法為何；5. 自動驗證使用者之真實性，如討論使用個人號碼卡被拒絕之案例；6. 依關於地方公共團體資訊系統使用電子簽章等認證業務法（電子署名等に係る地方公共団体情報システム

本報告之智慧財產權歸屬於國發會

機構の認証業務に関する法律）內之憑證管理機構與電子簽章法規定之差異，以及需要調整的作法建議為何等。

依目前數位廳提供之會議資料，除前述討論題綱外，4 項議題之主軸皆以認證標準現代化之推動為主，具體內容則可視正式發布之討論紀錄或報告。此外，此系列之第 3 次研究會議預計於 11 月 26 日辦理，至於最後之報告彙整與討論會議將於 12 月上旬辦理。

資料來源：

1. デジタル庁, 電子署名法認定基準のモダナイズ検討会（第 2 回）, 2024-11-01, https://www.digital.go.jp/councils/digitalsign-modernization/f93133d6-8f4d-467a-aa0d-c6302d1a3b58 (last visited 2024/11/13)
2. e-Gov, 電子署名及び認証業務に関する法律, 2022-06-17, https://laws.e-gov.go.jp/law/412AC0000000102 (last visited 2024/11/13)

伍、 數位監管

一、 歐盟

(一)2024 年 11 月歐盟執委會通過《線上平臺提供者之透明度報告義務之實施規則》，規定透明度報告之格式、內容與透明度報告之發布期限

2024 年 11 月歐盟執委會通過《線上平臺提供者之透明度報告義務之實施規則》（Implementing Regulation - laying down templates concerning the transparency reporting obligations of providers of online platforms，下稱《平臺透明度報告規則》），該規則概述《數位服務法》（Digital Services Act, DSA）之線上平臺服務提供者透明度報告的格式、內容與透明度報告之發布期限。

本報告之智慧財產權歸屬於國發會

1. 《平臺透明度報告規則》之適用對象

依據 DSA 規定，中介服務提供者（intermediary service）有義務發布透明度報告，詳細說明其內容之審核作法。

依《平臺透明度報告規則》第 2 條規定，超大型線上平臺（Very Large Online Platforms, VLOPs）與超大型線上搜尋引擎（Very Large Online Search Engines, VLOSEs）每半年至少發布 1 次透明度報告，其他的中介服務提供者每年須發布 1 次透明度報告。

2. 透明度報告之內容

透明度報告必須包含之特定類別資訊，取決於供應商的類型，例如：移除的內容數量、自動內容審核系統的準確性、帳戶終止以及有關其內容審核團隊的資訊。

3. 發布透明度報告之格式與期限

由於各平臺在資料分類與格式之解釋上存在巨大差異，且 VLOPs 與 VLOSEs 之透明度報告發布週期也不一致。為此，歐盟執委會發布統一的報告模板與週期，於網站提供《平臺透明度報告規則》、透明度報告模板的 Excel 格式，以便線上平臺服務提供者下載、填寫模板，遵循規則之要求。

依《平臺透明度報告規則》規定，線上平臺服務提供者需從 2025 年 7 月 1 日起，依據新規定蒐集資料，預計 2026 年初提交第一批標準化之透明度報告。

4. 透明度報告之保存期限

依《平臺透明度報告規則》第 3 條規定，為確保民眾能夠取得所有版本之透明度報告，線上平臺服務提供者於發布

本報告之智慧財產權歸屬於國發會

透明度報告後，至少應設定 5 年之透明度報告保留期限（retention period）。

5. 透明度報告應標示版本

依《平臺透明度報告規則》規定，應明確標示透明度報告的版本，以便於識別透明度報告之版本、日期。

《平臺透明度報告規則》將於歐盟官方公報上發布後的第 20 天生效，並直接適用於所有歐盟會員國。

資料來源：

1. European Commission, Commission harmonises transparency reporting rules under the Digital Services Act, 2024-11-04, https://digital-strategy.ec.europa.eu/en/news/commission-harmonises-transparency-reporting-rules-under-digital-services-act (last visited 2024/11/15)
2. European Commission, Implementing Regulation laying down templates concerning the transparency reporting obligations of providers of online platforms, 2024-11-04, https://digital-strategy.ec.europa.eu/en/library/implementing-regulation-laying-down-templates-concerning-transparency-reporting-obligations (last visited 2024/11/15)

二、韓國

(一)2024 年 10 月 23 日韓國個資保護委員會宣布「『加強打擊個資外洩與非法散布之措施』之計畫」，防止因個資外洩而導致之二次傷害行為

2024 年 10 月韓國個資保護委員會（Personal Information Protection Commission, PIPC）宣布「『加強打擊個資外洩與非法散布之措施』之計畫」（Plan to Strengthen Measures against Personal Data Exposure and

本報告之智慧財產權歸屬於國發會

Illegal Distribution），旨於（1）積極地防止惡意攻擊者利用當事人之個資外洩，進行盜用身分（identity theft）、寄送垃圾郵件、釣魚詐騙等非法行為，對當事人造成二次傷害；並（2）透過減少個資外洩、非法散布之行為，保護隱私。PIPC 將強化相關機構之線上回覆系統（Online Response System, ORS），將 AI 技術（包含機器學習）納入檢測程序。此外，PIPC 將強化與網路服務提供者（Internet Service Providers, ISPs）、韓國警察廳（National Policy Agency）間的協作與合作體系（collaboration and cooperation systems）。

此計畫包含五個主要重點，分述如下：

1. 先進的個資外洩檢測系統

首先，將原本關鍵字的檢測系統轉為納入 AI 技術的檢測系統，以反應數位環境中個資外洩的樣態，已由文字轉為影像之趨勢。因此，PIPC 將開發對話型（conversational）關鍵字，可有效檢測約 470 萬個國內外網站之個資外洩。此外，個資之目標範圍將從結構化資料（structured data）擴大至包含身分證號碼（resident registration numbers, RRN）與電話號碼之影像資料。為因應深偽技術而急速增加之 AI 生成資料，檢測系統將逐步升級，以便檢測並移除影像中的個人資料（包含人臉）。

除上述措施外，PIPC 將強化通知與報告程序，使個人資料處理者得以盡早因應個資外洩。協調系統（coordination system）亦將針對「尋找我外洩的個資」（Finding My Leaked Personal Data）之服務範圍，由暗網（dark web）上的當前的帳號資訊擴展至電子郵件、電話號碼，並與韓國網路安全中心（Korea Internet Security Center, KISC）共享暗網之監控狀況。

2. 迅速地採取措施，如：封鎖涉及個資外洩及非法散布之貼文

本報告之智慧財產權歸屬於國發會

PIPC 計劃積極利用由 15 家國內外主要搜尋引擎與社群媒體平臺（包括 Naver、Kakao、Google 及 Meta）組成的熱線（hotline）合作網路，迅速地封鎖有關個資外洩的貼文。透過系統化業務特定回應措施（systematizing business specific response measures）及升級之檢測分類模型，PIPC 將「刪除線上非法交易個資之貼文的週期」自平均 24.8 天縮短為 18.9 天。此外，PIPC 將定期與事業共享包含個資外洩之資料，確保事業於 AI 模型之訓練資料集中排除該資料。

3. 加強打擊個資之非法市場

為根除包含個資之貸款資料庫（loan databases）的非法市場，PIPC 將加強與負責調查個資非法交易之韓國警察廳合作。PIPC 與韓國網際網路振興院（Korea Internet & Security Agency, KISA）將透過剖析個資非法交易之貼文，生成並提供必要的客制化資料，藉以支援調查機構快速追捕犯罪者。韓國仁川警察廳已與 KISA 已簽署備忘錄（MOU），共同協作調查個資非法市場，2024 年上半年已逮捕 11 名非法交易者。

4. 加強預防性檢查，以防止個資外洩

自 2024 年 9 月起，公部門應達到更高的個資保護標準。PIPC 計劃針對經評估不具備適當之保護措施的公共機構進行預防性檢查，並擴大「違反揭露標準」之範圍（expand the scope of breach disclosure standards）。此外，監管機構將考慮新興技術與產業之變化，制定中長期調查路線圖。2025 年將設立「數位鑑識實驗室」，以確保個資外洩之數位證據，如：電子形式軌跡資料（Log）文件與後設資料（metadata）。

5. 加強公共參與與回應之基礎建設

本報告之智慧財產權歸屬於國發會

個資處理者將進行自願審查（voluntarily review），以確認是否個外洩，資料保護監管機構亦將向中小企業（Small and Medium-sized Enterprises, SMEs）及傳統型商店（mom-and-pop businesses）提供培訓、諮詢與技術支援，以防止個資外洩及重複違規。對於多次洩漏大量個資者，PIPC 將支援其進行補救措施，以確保合規。

於 AI 及資料經濟時代，由於個資為推動此一轉型的關鍵之一，PIPC 將盡最大努力防止資料外洩及濫用，並以公眾信任為基礎，打造安全的數位環境。

資料來源：

1. PIPC, Notice / Press Release, PIPC to Prevent Identity Theft and Secondary Harm by Strengthening Measures against Personal Data Exposure and Illegal Markets, 2024-10-25, https://m.pipc.go.kr/eng/user/ltn/new/noticeList.do (last visited 2024/11/01)
2. PIPC, PIPC to Prevent Identity Theft and Secondary Harm by Strengthening Measures against Personal Data Exposure and Illegal Markets, 2024-10-25, https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do (last visited 2024/11/01)

陸、 數位服務

一、 日本

(一)2024 年 10 月日本發布參與 G7 數位與科技部長會議成果，並提供包含公部門使用 AI 與數位身分等參考文件

日本數位廳於 10 月 16 日發布、10 月 25 日更新七大工業國集團（Group of Seven, G7）數位與科技部長會議之資料。本次會議係由義

本報告之智慧財產權歸屬於國發會

大利擔任主席國並主持相關會議，並於 15 日發布聯合聲明，後續也於 OECD 網站發布會議資料。

除聯合聲明外，數位廳新聞稿主要說明日本數位廳參與該會議成果與提供 3 份會議資料，包含公部門使用 AI 與數位身分等，具體內容係供 G7 成員參考。3 份文件摘要如下：

1. 公部門運用 AI 之工具包（Toolkit on AI in the Public Sector）

   此文件包含公部門運用 AI 之趨勢、最佳實踐、政策架構，及 G7 促進 AI 之措施。具體之重點包含：在公部門如何實現安全、可靠及值得信賴之 AI 系統，如 AI 相關之國家戰略與政策、治理架構、保護措施；公部門面臨 AI 之當前趨勢，如預期效益與影響，及面臨挑戰之政策選擇；以及公部門運用 AI 解決方案之發展歷程，如構想、原型設計及試行等。此一工具包之目的在於讓公部門及利害關係人於規劃運用 AI 時，可以了解其風險，並將 G7 對 AI 之原則轉換成實際政策或措施。

2. 數位政府服務綱要（Compendium of Digital Government Services）

   此文件內容為 G7 成員間，關於數位公共基礎設施（Digital Public Infrastructure, DPI）之互通規劃，及透過數位科技提供公共服務之案例與解決方案。除簡介 G7 數位政府服務外，具體內容包括存取公共服務之數位身分解決方案、公部門之資料與資訊共享，以及單一數位報關、支付服務等案例。

3. 數位身分措施之對應演練（Mapping Exercise of Digital Identity Approaches）

   由於 G7 各國皆有數位身分相關措施，例如：歐盟建立數位身分架構規則（Regulation (EU) 2024/1183，the European

本報告之智慧財產權歸屬於國發會

Digital Identity Framework）、日本在行政程序中確認本人身分方法指引（DS-500，行政手続におけるオンラインによる本人確認の手法に関するガイドライン）、或美國 NIST 數位身分指引（SP-800-63-3，Digital Identity Guidelines），此一文件具體內容以支援數位身分相關措施為主，透過演練以掌握 G7 共同的概念、定義，以及採用相關國際標準及其方法。

資料來源：

1. デジタル庁, G7 デジタル・技術大臣会合の開催結果, 2024-10-25, https://www.digital.go.jp/news/53ed2e40-a8be-4249-869d-e94f4f9a28fa (last visited 2024/11/06)

柒、 競爭法制

一、 國際會議

(一)7 大工業國組織（G7）之競爭法主管機關及政策制定者於義大利舉行競爭高峰會，探討 AI 相關競爭議題

7 大工業國組織（G7）之競爭法主管機關與其國家政策制定者(指政策制定關聯部會之負責人)於 10 月 4 日，以數位競爭（Digital Competition）為主題，於羅馬舉行競爭高峰會（G7 Competition Authorities and Policymakers' Summit）。本次會議係由義大利競爭管理局（Autorità Garante della Concorrenza e del Mercato, AGCM）主辦，著重討論因 AI 技術，尤其是生成式 AI（Generative AI）基礎模型以及演算之快速發展與應用所引發之競爭議題，會後並發布新聞稿彙整本次會議重點。

新聞稿指出 G7 國家之競爭法主管機關今年初成立之 AI 工作小組，對於 AI 技術堆疊與演算法可能導致之潛在競爭問題進行討論，大

本報告之智慧財產權歸屬於國發會

致歸納以下幾點重要之競爭問題，尤其涉及 GenAI 層面之問題，摘述如下：

1. 關鍵輸入控制：對關鍵 AI 資源投入（crucial AI inputs）之控制可能使少數事業占據關鍵市場地位，此類事業可能透過現存或新出現之瓶頸（bottlenecks）以限制市場新進參與者進入市場。能源之取得亦可能成為新的瓶頸，而其取得之難度可能隨 AI 部署之擴大及 AI 模型與複雜度之增加，而逐漸提高。

2. 消費選擇之限制：現今具市場主導地位之 AI 技術平臺，可能透過自我偏好（self-preferencing）、綑綁銷售（bundling）或搭售（tying）等方式限制消費者選擇，進一步提高中小型事業進入 AI 市場之門檻。

3. 市場控制力之擴張：於現今數位市場中具備強大影響力之事業，可能利用網絡效應（network effect）、資料反饋循環（data feedback loop，一種堆砌資料獲取反覆訓練大型 AI 模型之能力）或跨生態系（cross-ecosystem）之整合等能力，將控制力延伸至其他 AI 相關市場，增加市場進入壁壘並限制競爭。

4. 數位巨擘與 AI 事業策略聯盟：擁有大量資源之大型數位事業，與具 AI 技術之事業間，所存在之複雜的合作夥伴關係與佈局，可能會抑制 AI 相關市場之競爭。尤其大型數位事業可能自 AI 事業網羅關鍵人才，形成策略聯盟（strategic alliances），且於規避結合審查之同時，亦達成鞏固市場優勢地位並弱化 AI 市場競爭之目的。

5. AI 促進之勾結：AI 與演算法使事業間能更容易互相勾結，包含針對價格或薪資之協調、共享競爭相關之敏感資訊、監督市場訂價與採行價格歧視等，損害消費者權益與市場競爭。

本報告之智慧財產權歸屬於國發會

以上為本次高峰會提及之主要競爭問題，同時並就各競爭法主管機關與相關政策制定者可為之政策作為，提出以下指導原則，包含：

1. 公平競爭（Fair Competition）：須採取相關作為保持 AI 市場之競爭，不至於因為現存事業之有害競爭的作為，損害市場競爭。政策目標在於避免大型事業利用其市場優勢地位限制或排除市場競爭，或利用 AI 技術堆疊出新興之競爭瓶頸，參與不公平交易作為、以及阻礙有利於競爭之創新等。此外，必須避免事業利用 AI、機器學習或演算法規定市場競爭，例如不當共享競爭敏感資訊、利用演算法進行價格勾結之行為等。

2. 公平獲取與機會（Fair Access and Opportunity）：確保 AI 關鍵資源輸入得以公平地被取得，對於 AI 之發展與部署有其必要性，其中包含 AI 晶片、以及開發下游應用程式所需之 AI 基礎模型等資源。市場之開放性（openness）發展，亦可促進市場進入，例如要求公開 AI 模型之訓練資料等，得以減少市場進入障礙，提供給新進市場之 AI 事業更多機會。

3. 消費選擇權（Choice）：確保消費者與事業能透過獲取明確資訊，在多樣化之 AI 產品服務間，明確選擇所需之 AI。

4. 互通性（Interoperability）：推動技術標準之開放，以促進創新，降低市場力量集中之風險，並防止消費者或事業被鎖定於封閉之生態系。同時，資料可攜（data portability）之發展，亦可降低鎖定風險並帶動競爭。未來政策上將嚴格審查關於互通性要求將損害 AI 模型或系統之隱私與安全性的相關主張。

5. 創新（Innovation）：應支持新興之 AI 技術與商業模式，並確保 AI 之透明度與問責機制，提升用戶對 AI 之信任。

6. 透明度與問責（Transparency and Accountability）：AI 使用者應了解訓練 AI 模型使用之資料類型與來源，並了解模型限制

本報告之智慧財產權歸屬於國發會

與風險;AI 開發者/經營者應對 AI 系統中可控制之部分負責，確保事業及消費者充分了解 AI 系統相關之風險與漏洞，並得到充分保護。

整體而言，G7 強調 AI 技術發展雖然帶來相當程度創新潛力，但亦伴隨競爭問題，尤其需要注意關鍵資源限制，以及大型數位事業及 AI 事業對市場之控制與影響等，需採取相關政策作為以確保 AI 相關市場於保持有效競爭。

資料來源：

1. G7 Competition Authorities and Policymakers' Summit, Digital Competition Communiqué, 2024-10-17, https://en.agcm.it/dotcmsdoc/pressrelease/G7%202024%20-%20Digital%20Competition%20Communiqu%C3%A9.pdf (last visited 2024/10/20)

捌、 網路/資訊安全與韌性

一、 歐盟

(一)2024 年 10 月歐盟 NIS 2 指令要求各國轉換成內國法之期限已至，歐盟發布該指令首部實施規則，以強化關鍵實體與相關網路安全

歐盟執委會（European Commission, EC）於 2024 年 10 月 17 日發布新聞，宣布修正後之《歐盟高度共通程度之資安措施指令》(Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, NIS 2 Directive）之內國法轉換時間已屆，並公布依前開指令所訂定，針對關鍵實體（critical entities）及網路安全之實施規則（implement regulation），強化網路安全風險管理及數位基礎建設與服務事業就重大事件向主管機關通報之義務。

本報告之智慧財產權歸屬於國發會

NIS 2 Directive 之修訂，主要係因各國對於前一版指令（指Directive (EU) 2016/1148）之實施有差異，且面臨網路安全之新興威脅，如勒索軟體、供應鏈安全等需調整指令涵蓋之對象及部分網路安全之要求，新指令規範對象從提供基本服務相關利害關係人之安全，擴大適用範圍至基本服務營運商（Operator of Essential Services, OES）、數位服務提供者（Digital Service Providers, DSPs）之安全，並重視關鍵實體韌性（critical entities resilience, CER）。

此外，為強化關鍵實體韌性，2022 年還一併通過 2 個相關指令，包含：針對金融領域之數位營運韌性（Directive (EU) 2022/2556，as regards digital operational resilience for the financial sector），及針對關鍵實體韌性之定義、識別及領域等（Directive (EU) 2022/2557，on the resilience of critical entities）。以 Directive (EU) 2022/2557 為例，關鍵實體包含：能源、運輸、銀行、金融基礎設施、醫療、飲用水、廢水、數位基礎設施、公共行政、太空，以及食品生產、加工與配送，共 11 類等領域。

執委會於新聞稿內說明自 10 月 18 日起，各成員國應採取必要措施，如監督或執法，以落實 NIS 2 Directive 相關規範。而本次通過公布首部對於關鍵實體及網路安全之實施規則，則主要將適用於特定類別之數位服務事業，諸如雲端運算服務提供者、資料中心服務提供者、網路市集、網路搜尋引擎及社群網路平台等。規則並就不同服務類型定義相關事件被視為重大事件之要件，以利事業遵循。

資料來源：

1. EC, New rules to boost cybersecurity of EU's critical entities and networks, 2024-10-17, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5342 (last visited 2024/10/30)
2. EUR-Lex, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high

本報告之智慧財產權歸屬於國發會

common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), 2022-12-27, https://eur-lex.europa.eu/eli/dir/2022/2555/oj (last visited 2024/10/30)

(二)2024 年 10 月歐盟通過《網路韌性法》，針對於歐盟境內提供連網功能之軟硬體數位產品，建立網路安全要求

2024 年 10 月 10 日歐盟理事會（European Council）通過《網路韌性法》（Cyber Resilience Act, CRA），為歐盟境內提供連網（internet-connected）軟硬體之數位產品，制定網路安全要求。訂定本法之目的，在於填補法律漏洞（fill the gaps），連結並完善現行歐盟之網路安全立法框架，鏈結包括《歐盟網路與資訊系統安全指令》（Directive on Security of Network and Information Systems, NIS Directive）、《歐盟實施高度共通程度之資安措施指令》（Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, NIS 2 Directive）及《歐盟網路安全法》（the EU cybersecurity act）等規範，以確保具有數位元件（digital components）之產品，例如：「物聯網」（Internet of Things，IoT）產品，於整個供應鏈與生命週期皆符合網路安全要求。

CRA 規範重點摘要如下：

1. 適用 CRA 之產品範圍

除現行歐盟規則已另行規定網路安全規定之產品，例如：醫療設備、航空產品及汽車外，CRA 適用於歐盟範圍內直接或間接與其他設備或網路連接之所有軟硬體產品的整體生命週期（設計、開發、生產及上市階段）。CRA 規範之目的在於讓消費者於選擇及使用具有數位元件之產品時，可將網路安

本報告之智慧財產權歸屬於國發會

全納入考量，故須建構規範使其易於識別具有網路安全功能之軟硬體產品，例如於產品上帶有 CE 標誌說明已符合歐盟法令之要求等。

2. 製造商義務

為確保具有數位元件之產品投入市場的網路安全，CRA制定製造商於產品設計、開發及生產之基本義務。要求製造商應確保具備數位元素之產品不會受到未經授權的接取（unauthorized access），以及基本功能之持續可用。製造商必須以限制表面攻擊（surface attacks）之角度進行產品設計、開發與生產，並能夠立即修復漏洞，進行有效之定期測試。同時，針對網路安全評估層面，製造商必須於產品於整個生命週期皆持續評估並降低產品之網路風險，並於整合第三方產品時，應進行盡職調查（due diligence），確保第三方元件不會損及產品之網路安全，包括採用尚未用於商業活動之免費及開源軟體。

製造商於將產品投入歐盟市場前進行該產品之合規評估（Conformity assessment），其方式可依據產品本身之性質，選擇透過內部控制或第三方評估等適當之程序。對於產品漏洞層面，製造商必須遵循並維持「漏洞處理程序」使個人或組織得以向製造商通知漏洞，並對相關漏洞進行修補、記錄及揭露；同時必須於售後五年內提供漏洞修補之支援。若所製造之產品出現任何被利用之漏洞，或有影響產品安全之嚴重事件發生，製造商必須於獲知事件發生之 24 小時內向國家電腦安全事件回應小組（Computer Security Incident Response Team, CSIRT）及歐盟網路安全局（EU Agency for Cybersecurity, ENISA）進行預警通知，並於 72 小時內提出完整通知，並於採取矯正或緩和措施後 14 天內提出最終報告。對於用戶，製

本報告之智慧財產權歸屬於國發會

造商亦須予以通知，必要時並須告知可採取那些措施以降低該漏洞可能導致之影響。

故整體而言製造商於產品生命週期義務包括：(1) 於設計、開發及生產具有數位元件之產品時，應為「網路安全風險評估；(2) 於設計及開發產品時，應為「盡職調查」；(3) 於產品投入市場前，應為「合規評估」；(4)於產品投入市場時，應為「漏洞處理」；(5) 為客戶提供網路安全支援，於產品出現漏洞及發生影響產品之安全性事件時，應履行通報及通知義務。

3. 「經濟運營商（economic perator）之義務」及「免費與開源軟體（free and open-source software）」相關規定：

CRA 為經濟運營商制定基本網路安全義務規定。所謂經濟運營商，包含製造商、分銷商及進口商，確保當具有數位元件之產品投入市場時，經濟運營商得以充分發揮其於供應鏈之作用及責任。執委會將會對於經濟營運商提供適當指導，以協助其遵循 CRA，尤其對於微型或中小型企業部分。相關指導將特別針對遠端資料處理以及對於自由或開源軟體開發人員之影響、如何認定對數位產品支援期限的要件等相關事宜。

免費或開源軟體僅有在該軟體有於歐盟市場供應，並用於商業活動，方有 CRA 之適用。而 CRA 於前言第 18 點並說明，就是否用於商業活動部分，基本商必須考量開發與供應階段之區別，亦即採用該免費或開放軟體之產品或並未被製造商銷售或貨幣化（monetised），則該軟體不應被視為用於商業活動。而若該軟體被其他製造商整合至其他具數位元素之產品，則應以原來之免費或開源軟體（原始軟體組件）是否被原始製造商貨幣化作為是否用於商業活動之判斷。開源軟體

本報告之智慧財產權歸屬於國發會

管理者（open-source software steward）應以可驗證方式，制定及記錄網路安全政策，促進應用該軟體開發數位產品之開發人員得以有效處理漏洞。

4. 「具有數位元件之產品」之安全符合性認定（Conformity of the product with digital elements）：

具有數位元件之產品，符合歐盟官方公報已發布文獻相關之協調標準（harmonised standards），或經歐洲網路安全認證計畫（the European cybersecurity certification schemes）頒布歐盟符合性聲明或證書，應推定符合 CRA 之基本網路安全義務。

制定具有數位元件之產品增加「CE 標誌」之規則及條件，以及合規評估程序。尤其要求 CE 標誌應已明顯、清晰且不可消除之方式黏貼於具有數位元件之產品上，若為軟體形式之產品，則必須黏貼於歐盟符合性聲明，或該產品刊登或附隨之網站上（website accompanying the software product）。

5. 合規評估機構（conformity assessment bodies）之通知：

歐盟會員國應指定一個「主管機關」（notifying authority），該主管機關負責制定並執行「評估、指定、通知及監督合規評估機構」之必要程序。

6. 市場監督與執法（Market surveillance and enforcement）：

國家市場監管機構（national market surveillance authorities）負責會員國境內之市場監管。會員國得指定任何現有或新機構為本法執行之市場監督機關，並要求經濟經營者必須與市場監管機關及其他主管機關充分合作。

本報告之智慧財產權歸屬於國發會

CRA 於 10 月 10 日通過後，經歐盟理事會主席及歐洲議會主席簽署，並於歐盟官方期刊公布 20 天後生效。為使製造商、通報機關及會員國有適應新規定之過渡時間，CRA 訂有不同之規範適用期限，其中事件通報義務於公告後 21 個月適用，其餘義務則於 36 個月後適用。

資料來源：

1. EUROPEAN UNION, Cyber resilience act: Council adopts new law on security requirements for digital products, 2024-10-10, https://www.consilium.europa.eu/en/press/press-releases/2024/10/10/cyber-resilience-act-council-adopts-new-law-on-security-requirements-for-digital-products/ (last visited 2024/11/06)
2. EUROPEAN UNION, Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber resilience act), 2024-10-23, https://data.consilium.europa.eu/doc/document/PE-100-2023-REV-1/en/pdf (last visited 2024/11/06)
3. JD SUPRA, New EU Cybersecurity Obligations for Connected Devices: What You Need to Know, 2024-11-01 , https://www.jdsupra.com/legalnews/new-eu-cybersecurity-obligations-for-9743633/ (last visited 2024/11/06)

二、 中國大陸

(一)2024 年 9 月中國大陸國務院通過《網路資料安全管理條例》

中國大陸國務院總理李強於 2024 年 9 月簽署國務院令，公布《網路資料安全管理條例》(網絡數據安全管理條例，下稱《條例》)，旨於規定網路資料處理活動，保障網路資料安全，促進網路資料合理有效之利用，保障個人及組織權益，維護國家安全及公共利益。《條例》共 9 章節 64 條，於 2025 年 1 月 1 日起施行。

本報告之智慧財產權歸屬於國發會

以下為《條例》對網路資料安全管理之重要內容：

1. 總則規定及一般規定：

鼓勵網路資料於各產業及領域創新應用，促進開發利用及產業發展。禁止非法網路資料處理活動。對網路資料實施分類分級保護,制定網路資料安全行為規定以加強事業自律,並積極參與網路資料安全相關之國際規則及標準制定。規定網路資料處理者須建立網路資料安全管理制度、安全事件因應方案、安全風險報告並提供符合相關國家標準之網路產品與服務等義務。

2. 個人資料保護規定：

(1) 制定處理個人資料規則,規定網路資料處理者處理個人資料時，須依法向個人告知並取得同意。

(2) 規定網路資料處理者,提供方便支持個人行使權利之方法及途徑，不得設置不合理條件限制個人之合理請求。

(3) 規定使用自動化蒐集技術蒐集個人資料之保護義務。

(4) 規定網路資料處理者,須提供個人資料移轉請求之途徑。

(5) 規定網路資料處理者,應定期自行或委托專業機構對其處理個人資料為法遵審計。

(6) 規定網路資料處理者，處理 1000 萬人以上個人資料，依處理重要資料之網路資料處理者之規定。

3. 建立重要資料安全：

(1) 依資料分類分級保護制度，制定重要資料目錄。

(2) 規定網路資料處理者，識別及申報重要資料義務。

本報告之智慧財產權歸屬於國發會

(3) 規定網路資料安全管理機構及網路資料安全負責人之責任。

(4) 規定重要資料風險評估及報告之具體內容要求。

4. 網路資料跨境安全管理：

(1) 規定網路資料處理者，得向境外提供個人資料之條件。

(2) 規定得依締結或參與國際條約及協定向境外提供個人資料。

(3) 規定於中國大陸境內運營中之資料處理者所蒐集與產生之重要資料，向境外提供該些資料，須通過資料出境安全評估。未被相關地區及部門通知或公告為重要資料，不須為申報資料出境安全評估。

5. 網路平臺服務提供者義務：

(1) 明確規定網路平臺服務提供者及第三方產品與服務提供者之網路資料安全保護義務。

(2) 應用程式發行平臺服務提供者，須建立應用程式認證規則，並為網路資料安全相關認證。

(3) 明確規定依自動化決策方式向個人推送個人化資訊及廣告，須設置易於理解之存取及操作之個人化（個性化）推薦關閉選項。

(4) 規定大型網路平臺服務提供者，須發布個人資料保護社會責任年度報告。於跨境提供網路資料，須遵守國家資料跨境安全管理規定。

6. 主管機關相關之監管規定、違反規定之法律責任及相關名詞解釋之補充規定。

本報告之智慧財產權歸屬於國發會

資料來源：

1. 人民網，網絡數據安全管理條例，2024-10-10，http://cpc.people.com.cn/BIG5/n1/2024/1010/c64094-40335877.html (last visited 2024/10/21)

2. 人民網，李強簽署國務院令公布《網絡數據安全管理條例》，2024-10-01，http://cpc.people.com.cn/BIG5/n1/2024/1001/c64094-40332179.html (last visited 2024/10/21)

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」委託研究計畫

國內法規環境建構幕僚協助與新興議題之因應事宜

中華民國 113 年 12 月

國內法規環境建構幕僚協助與新興議題之因應事宜

項次 1. 法制幕僚意見詢問

壹、 歐盟人工智慧法案之重點與產業影響（2024 年 5 月 24 日）

一、 背景

歐洲理事會於 2024 年 5 月 21 日正式批准人工智慧法(Artificial Intelligence Act, AIA)，為全球首創以風險為基礎之 AI 監管法案，本法案將於歐盟官方公報上公佈 20 日之後生效並分階段適用，就其正式通過之規範重點進行了解，並初步了解其通過可能對產業之影響。

二、 研析建議

(一)歐盟人工智慧法(AI Act)摘要說明[300]

1. 法案目的

本法立法目的係透過訂定統一之法律架構，尤其針對 AI 系統的開發、進入市場、提供服務與使用層面之規範，以改善歐盟內部市場之運作。同時促進以人為本且值得信賴之 AI 運用，確保 AI 相關活動得以符合歐盟基本權利憲章規定之健康、安全與基本權保障(包括民主、人權及環境之保護等)。歐盟強調本法並非規範 AI 系統於其生命週期內所有層面亦非規範技術本身，而係基於風險之程度，設立監管標準，以協調 AI 與人類基本權益之間的衝突，並提供專門領域如軍事、國防及研究目的之系統相對豁免。最終期望得以促進歐盟市場開發與採用安全可靠之 AI 系統，並刺激歐洲對 AI 投資與創新。

2. 重點內容

[300] Artificial Intelligence Act of 21th May 2024, https://data.consilium.europa.eu/doc/document/PE-24-2024-INIT/en/pdf , last visited 2024/5/23

本報告之智慧財產權歸屬於國發會

(1) 建立風險分級及監管機制

歐盟要求對 AI 之開發與使用必須進行識別及評估風險及潛在影響，並對這些風險進行分級：

I. 具不可接受之風險而禁止使用之 AI 類型：

歐盟對嚴重侵害人類權利之應用及服務，包括認知行為操控、隨機面部識別擷取、情緒識別、敏感資訊擷取、社會評分等 AI 技術運用，歸類為不可被接受的風險，於歐盟單一市場原則禁止使用；僅有「即時」遠端生物辨識(Remote Biometric Recognition, RBI)技術運運係為保護人類之公益目的的特殊情況下，才可例外開放。具體禁止範圍如下：

i. 使用潛意識、操縱或欺騙手段來扭曲個人或特定群體之行為並影響其作成明智之決策，從而造成重大傷害。

ii. 利用與年齡、殘疾或社會經濟環境相關的脆弱性來扭曲個人或特定群體行為，造成重大傷害。

iii. 以生物辨識分類系統推斷具敏感性之屬性(如：種族、政治觀點、工會會員資格、宗教或哲學信仰、性生活或性取向等)，但合法取得的生物辨識資料集的標籤或過濾或執法部門對生物辨識資料進行分類時除外。

iv. 社會評分，即根據社會行為或個人特徵對個人或特定群體進行評估或分類，從而對這些人造成有害或不利的差別待遇。

v. 僅根據分析或人格特徵來評估個人實施刑事犯罪的風險，除非用於增強基於與犯罪活動直接相關的客觀、可驗證事實的人類評估。

本報告之智慧財產權歸屬於國發會

vi. 透過從網路或監控錄影無目的地抓取臉部影像以編譯臉部辨識資料庫。

vii. 於工作場所或教育機構中的情緒推斷，除非出於醫療或安全原因。

viii. 在執法公共場所進行「即時」遠端生物辨識，但以下情況除外：

A. 尋找失蹤者、綁架受害者、遭受人口販運或性剝削的人；

B. 防止重大和迫在眉睫的生命威脅或可預見的恐怖攻擊；

C. 識別嚴重犯罪（例如謀殺、強姦、武裝搶劫、麻醉品和非法武器販運、有組織犯罪和環境犯罪等）的嫌疑犯。

II. 高風險 AI 類型，得於符合一定條件下於歐盟使用：

對於雖運用風險高，但於可事先識別並經評定而取得授權者，在遵守一系列要求及義務的前提下，可於歐盟市場內開發或使用高風險 AI 系統。高風險 AI 系統之分類，主要依據 AIA 第 6 條之原則進行，亦即該 AI 系統是否係被用於產品之安全組件或其本身為指定歐盟立法(於 AIA 附件一詳列)涵蓋之產品，且該 AI 安全組件或產品需經過第三方合格評估，方得進入市場或使用者，即會被認定為高風險 AI。除了前述附件一涉及歐盟相關法規所規範之安全組件外，另須注意附件三 臚列之其他高風險 AI 清單類型。然而雖屬於附件三所列高風險 AI 清單，但不會對於自然人之健康、

本報告之智慧財產權歸屬於國發會

安全或基本權構成重大損害風險的情況下，則不會將該 AI 應用視為高風險。

i. AIA 附件三[301]所列高風險 AI 類型大致包括：

A. 生物識別技術：遠端生物特徵識別系統、生物特徵分類（利用敏感或受保護屬性及特徵做判斷）、情感識別

B. 關鍵基礎設施：關鍵數位基礎設施管理和營運、道路交通或供水、燃氣、供暖或供電的安全元件。

C. 教育及職業培訓：確定入學或錄取、分配自然人至教育及職業機構、評估學習成果、評估教育水準、監測教育機構或考試違禁行為

D. 就業、工人管理和自營職業：招聘或甄選自然人、工作任務分配或監測評估人員績效

E. 基本私人服務以及基本公共服務和福利：是否有資格享受公共事務之福利，包括醫療保健及給與、減少、撤銷或收回此類福利之系統、與人壽或監控相關之風險評估及定價系統、緊急呼叫系統（以 AI 替代員警、消費員、醫療救助人員等角色時）

F. 執法部門：評估刑事犯罪受害者風險、測謊或類似工具、評估自然人犯罪或再犯罪風險、或評估自然人或群體的人格特徵或過去的犯罪行為、於偵查、調查或起訴刑事犯罪過程中對自然人進行特徵分析。

[301] Id, at 384-389

本報告之智慧財產權歸屬於國發會

G. 移民、庇護和邊境管制管理：測謊或類似工具、評估打算進入或已經進入會員國領土的自然人可能構成的風險、協助評估審查庇護、簽證或居留許可的申請、用於偵查或識別自然人之系統（核查旅行證件除外）

H. 司法和民主進程：協助司法單位研究及解釋事實及法律之系統、影響選舉投票行為之系統

ii. 雖屬高風險 AI 清單範圍但不致造成重大損害之判斷，可參考以下原則：

A. 該 AI 系統執行單一狹義之程式任務；

B. 該系統僅係用於改善先前已完成之人類活動結果；

C. 該系統係用於檢測決策模式或與先前決策模式的偏差，並不意味著在未經適當人工審查的情況下取代或影響先前完成的人工評估；或者

D. 該系統係執行與附件三中列出的相關的評估的準備任務。

iii. 對高風險 AI 系統供應商（開發商）之要求（第 8~25 條）

A. 建立貫穿高風險 AI 系統全生命週期的風險管理系統

B. 進行資料治理，確保訓練、驗證和測試資料集具有關連性、具有足夠的代表性，並儘可能沒有錯誤並根據預期目的完成。

本報告之智慧財產權歸屬於國發會

C. 確保起草技術文件以證明合規性，並向當局提供評估合規性之資訊。

D. 設計用於記錄保存的高風險 AI 系統，使其能夠自動記錄與識別國家級風險和整個系統生命週期中關於重大修改之相關事件。

E. 設計用於記錄保存的高風險 AI 系統，使其能夠自動記錄與識別國家級風險和整個系統生命週期中的重大修改之相關事件。

F. 向下游部署者提供使用說明，以確保後者符合規定。

G. 所設計之高風險 AI 系統，允許部署人員實施人工監督

H. 所設計之高風險 AI 系統，達到適當水平之準確性、穩健性及網路安全性。

I. 建立品質管理提醒，確保合規。

(2) 通用 AI（General-purpose AI, GPAI）之定義與義務

I. GPAI 模型是指一種 AI 模型，包括使用大規模自我監督進行大量資料訓練時，表現出顯著的通用性，並且無論模型以何種方式進入市場，都能夠勝任執行各種不同的任務，且可以整合到各種下游系統或應用程式中。這不包括在市場上發布之前用於研究、開發和原型設計活動的 AI 模型。

所有 GPAI 模型供應商必須：

i. 制定技術文件，包括訓練和測試過程以及評估結果

本報告之智慧財產權歸屬於國發會

ii. 撰擬相關說明，提供給打算將 GPAI 模型整合到自己的 AI 系統中的下游供應商，以便後者了解該 AI 功能及限制並能夠遵守相關法令

iii. 制定尊重著作權指令之相關政策

iv. 發布有關用於訓練 GPAI 模型的內容的足夠詳細的摘要。

除上述四項義務外，有系統性風險之 GPAI 模型供應商還必須：

i. 執行模型評估，包括進行和記錄對抗性測試 (adversarial testing)

ii. 評估和減輕可能之系統性風險，包括來源

iii. 追蹤、記錄並向 AI 辦公室和相關國家主管機關報告嚴重事件和可能的糾正措施，不得無故拖延。

iv. 確保足夠的網路安全保護等級。

II. GPAI 系統是指基於通用 AI 模型的 AI 系統，能夠服務多種目的，既可以直接使用，也可以整合到其他 AI 系統中。GPAI 系統可能被歸為高風險 AI 系統或被整合到其中。若被整合，GPAI 系統供應商應與該高風險 AI 系統供應商合作已確保後者符合規範。

(3) 建立沙盒機制支持創新措施

本法案提供創新之法律架構，建立 AI 監管沙盒為新創之 AI 系統之開發、測試和驗證提供可控制之環境，允許在現實條件下測試創新之 AI 系統，將分階段之義務透過 AI 參與沙盒來履行。

本報告之智慧財產權歸屬於國發會

(4) 新的治理架構

為確保 AIA 法案之實施，成立新的管理機構，包括於歐盟委員會內 AI 辦公室，負責整個歐盟之 AI 共通規則執行。成立獨立專家科學小組，支持本法案所定相關之執法活動。由各成員國代表組成 AI 委員會，就一致有效地實施本法案向委員會及成員國提供建議及協助。另對於利害關係方，建立諮詢論壇，成為產官學界更新提供技術專業知識及建議之管道。

(5) 處罰

對於違反 AIA 之規範，將處以最高 35,000,000 歐元的行政罰鍰，或者，如果違法者是企業，最高可達其全球年營業額的 7%。以較高者為準。違反高風險義務相關義務者得處以最高 15,000,000 歐元的罰鍰。對於應要求向公告機構或國家主管機關提供不正確、不完整或誤導性資訊的，應處以最高 7,500,000 歐元的罰鍰，或者，如果違法者是企業，則最高可處企業上一財政年度的全球年營業額總額 1%的行政罰鍰。（以較高者為準）。

(二)產業影響

儘管 AIA 不直接拘束 AI 的「利用者」，惟通用性 AI，例如生成式 AI 本即可廣泛應用至各種產業領域，故只要其 AI 系統之影響擴及至歐盟境內，無論該 AI 系統的提供者或用戶身處何處，即有 AIA 之適用空間，並按其可能產生的風險適用本法案既有的「風險級別」分層管理規範。例如，企業將生成式 AI 應用在「聊天機器人」對外服務客戶，屬於「低風險」級別，而應符合「透明度」相關要求。因此，對於擬應用相關 AI 技術之事業單位而言，應對 AIA 則須採取行動盤點營運所用之相關 AI 技術，識別其於 AIA 規範的「風險級別」，以對

本報告之智慧財產權歸屬於國發會

應實施法遵程序。AIA 之通過帶動歐盟實務上對於可能影響之產業的評論，僅摘要相關文獻對於特定產業影響之資訊供參考：

1. 保全業與安保設施

AIA 的重要核心旨在兼顧基本權利保障和公共安全維護的前提發展 AI 技術。根據 AI 系統的潛在風險對 AI 系統進行分類，特別針對第一類無法接受高風險之應用進行嚴格控管，這類 AI 由於對人類構成嚴重威脅，因此徹底禁止特定用途，其中就包括大規模社會監控技術之應用，例如以行為、社經地位、個人特徵為基準的社會評分系統，非針對性的遠端即時生物特徵辨識系統，預測個人是否犯罪的預防性執法系統等。然將涉及生物辨識之系統歸類在不能接受的風險引發不少爭論，尤其當面臨基於國家安全、人身安全或預防性執法之情事時，各會員國起初對於有條件地適度開放即時性的遠端生物特徵辨識系統猶存歧見，依照現行通過之法案，係禁止使用「透過網路或閉路電視攝影中非針對性地抓取臉部肖像來創建或擴充臉部辨識資料庫」的 AI 系統，原則限制在公共區域出於執法目的使用即時性的遠端生物識別系統，以免 AI 系統淪為大規模監控的工具，故僅能開放非即時性辨識，但例外在特定情境、嚴格定義的特殊條件下，倘基於緊急危難或急迫危險，例如逮捕恐怖份子，或尋找重大犯罪之被害人或失蹤兒童，允許開放即時性的辨識。故無論執法部門或安保公司建置部署監控措施前需要對其 AI 技術進行全面檢視，確保符合該法案例外允許使用遠端生物識別系統之要求。

2. 金融業

AI 可用於金融服務中的信用評分標準和理財風險評估，然而若其決策過程缺乏透明度，則可能導致不公平的結果；若是 AI 的決策錯誤或是龐大金融資料庫之管理缺失，亦可能

本報告之智慧財產權歸屬於國發會

導致重大金融損失，故在 AIA 分類系統歸屬於高風險類別。僅在那些透過演算法增強客戶體驗、欺詐檢測、客戶生命週期價值預測和模式分析等對個人決策沒有直接影響的應用程式，可能只包含有限或最小的風險。

具體應用上，以金融 GAI 理財機器人為例，目前理財機器人可分為「諮詢建議型」、「資產管理型」。前者是藉由收集大量投資與產業變化的金融數據配合投資申請人的投資喜好與風險承受比率，將所有具有不同權重的參數，透過人工經驗設計自動化演化法運算，產出一個比較客觀中立的投資建議規劃，提供投資申請人一份參考報告資料。後者則除具有上述「諮詢建議型」功能外，還附加直接自動化進行投資申請人的投資比例分配與調整等作業，被認為近似代客操作。但是其他衝擊與法律風險，如理財機器人自動生成資訊是否切實滿足說明義務及防免利益衝突功能尚難準確判斷；理財機器人出錯如操作、運用不當或當機致出現錯誤之責任歸屬不明等問題，依照現有規範體系，提供服務之金融機構乃終局負責人，須對其使用或經由外包的金融工具和服務承擔最終責任，同時歐盟金融監管機構針對其他現有法規範評估，終局負責人在解釋上亦可援用《數位營運韌性法案》（Digital Operational Resilience Act, DORA）中為所謂的「關鍵第三方服務供應者」概念的監督框架課予其相應之責任。

而目前理財機器人規範之重點方向，在演算法審查機制，及理財機器人服務如何透過既有證券投資信託之相關法規範，藉由提高罰鍰金額等強化監理之面向，惟另從產業創新及效能提升之角度，歐盟金融監管機構在自我影響評估中，認為應協同搭配《歐盟資料法》和《歐盟資料治理法》等歐洲資料戰略的治理藍圖，發揮在塑造歐洲金融領域 AI 使用格局方向上的關鍵作用，有助於公共部門資料庫的二次利用或從

本報告之智慧財產權歸屬於國發會

連網裝置存取個人資料集，使金融機構開發出更具創新性和客製化的產品，以利提供優化的服務，從而擴大數位競爭優勢。

3. 醫療暨器材設備業

對於醫療設備製造商而言，倘若醫療設備運用 AI 技術或支援機器深度學習功能的設備，屬於 AI 產品，故有 AIA 之適用，遂要求產品需印有歐洲合格認證的 CE 標誌(CE Marking)，另擔負評估程序之成本，促使將 AI 模型投入到其產品中的軟體開發商和設備製造商（無論是作為行業支援工具還是作為醫療設備軟體）應更積極在精準醫療之外，於設計和實施過程中考慮多項要求，如病患隱私、資安風險評估、透明性揭露義務、穩健的資料治理流程、網路系統安全保障、防免演算法歧視等，以證明產品製造商或服務提供者確保產品符合相應的歐盟指令。

具體而言，醫療器材及體外診斷醫療器材若使用高風險類別的 AI 系統(非僅用於醫療文件之撰寫)，程序上可以透過內部控制（亦即自我聲明）或第三方機構的認證以符合要求，且同時各自進行在歐盟醫療器材法規(Medical Device Regulation, MDR)和體外診斷醫療器材法規(In Vitro Diagnostic Medical Devices Regulation, IVDR)框架下由第三方機構評定之程序，為免除繁瑣程序，目前規劃將 AIA 定義下的產品清單交由第三方機構，統一由其同步進行該法案要求的合格認證程序。另外在該產業之供應鏈環節，如果經銷商、進口商或第三方以商標形式或其名義將高風險 AI 系統的醫療設備投入市場或提供服務，倘期間有修改系統的預期用途，將被視為 AIA 所定義的供應商，擴大其責任範圍，如商品製造人責任。

本報告之智慧財產權歸屬於國發會

4. 運輸業

按 AIA 原先之劃分依據，應用在交通運輸領域的 AI 技術,因其動輒對生命身體傷害以及財產上損失造成重大損害,理應被歸類為高風險類別。但基於鼓勵智慧運輸創新發展的立場，該法案並不直接適用於機動車輛，包括其內部所配置的設備和零組件，故歐盟境內的自駕車不落入法案之射程範疇。主管機關看似偏向採取去管制化的政策，但這並不表示自駕車未受任何形式的監管，其乃透過獨立規範之框架進行特別管制，係以車輛歐盟型式許可(EU type approval)中的 2018/858 規則進行規範，該規則規定自駕車從生產到上市整個過程的安全要求，以及上市前及上市後的市場監督機制，須符合本規則之管制規定及自駕車及其系統、零件等技術要求等程序及要件者，才可以取得「歐盟型式許可」,亦即歐規自駕車。另規定車輛市場監督機構(market surveillance authorities) 的義務，應該定期檢查，核實車輛、系統、部分及單獨技術之元件是否符合相關規定要求，應通過元件檢查，以及在適當情況下依據樣本進行實驗室測試及道路測試，並以「風險評估」做為車輛測試及驗證之基礎。

而 AIA 通過後，該監管框架預計將參酌法案的具體條款進行調整，驗證自駕車合規性及從事風險評估的基礎，以確保自駕車高標準功能安全及系統安全。

5. 娛樂及影視產業

於音樂、影視、遊戲和廣告業等事業所使用的各種 AI 的模型在 AIA 屬於有限風險或極低風險之類別，其中包括用於創建個人化體驗與增強消費體驗的演算法，以及用於廣告行銷之應用程式，由於這些技術未對人類或公共安全造成巨大威脅，首重資訊透明及使用相關技術之揭露即可大量投入使

本報告之智慧財產權歸屬於國發會

用，僅須留意如何改善 AI 系統中關於演算法產生基於性別、種族、年齡之潛在歧視及偏見，進而引發對個別用戶之平等權侵害與市場壟斷之疑慮，因而須以適當之方法舉措保障用戶對演算法管理之知情權與自動化決策之解釋權。

6. 基礎模型的開發供應商

尤其對大型語言模型(Large Language Models)的開發商及供應商而言，AIA 之規範架構對其產生直接拘束效力，特別在涉及智慧財產權侵權之爭議，為與《數位單一市場著作權指令》之體系相稱，例如第三方進行「文字和資料探勘」（Text and Data Mining）之豁免，或者賦予原著作權人之「退出」（opt-outs）機制，因而在不損害歐盟所保護基本權(含著作權)之前提下預防生成內容違反歐盟既存之法律，遂連帶與之產生勾稽，比方說該法案即針對生成式 AI 發生的著作權爭議特別規範 AI 模型的開發商必須說明哪些資料被用於訓練 AI 模型，負有「記錄並公開基礎模型使用受著作權法保護之培訓數據的詳細摘要」之義務，包含用於訓練模型的主要資料集、提供其他資料來源的敘述性說明等。

此要求意在擴大揭露所有訓練資料，以便第三方權利行使，惟通常在培訓大型語言模型的數據資料往往超過數十億件著作，光進行摘要作業就對企業之成本負擔甚鉅，況「摘要」必須達到何種程度才符合法定的「詳細」要件，則有待新成立的 AI 辦公室（AI office）向外界提供摘要的範本以供詮釋。另外，由於投入訓練的各式資料集多半是由第三方提供，僅憑 AI 開發商及供應商的資源可能無法詳盡釐清及溯及查核每項資訊的原始來源及其正確性，倘若發生權利紛爭情事，無疑是向權利人提供侵權之證據，不利其後續訴訟程序中之攻防主張，增添其被訴機會。因此，法案所課予之揭露義務為

本報告之智慧財產權歸屬於國發會

這類基礎模型的開發商及供應商額外新增生產成本與法律風險。

(三)美國於 AI 領域監管之作為

美國作為 AI 研發大國，於 2018 年起即由產業出發，制定相關自律之指引。為因應發展與使用安全可信的 AI 之國際趨勢，美國總統拜登於 2023 年 10 月 30 日簽署 AI 行政命令，要求各機關於期限內訂定相關指引，並設定國家 8 大優先發展議題：

1. AI 安全標準

各主管機關就其管轄權責範圍要求建立可靠性與最佳實踐方法之指引，各機關應評估關鍵基礎建設中使用 AI 之風險，並制定對應之安全指引，要求國安機關進行實際測試，利用 AI 技術發現與修復政府軟體網路系統之漏洞。要求國安部門對於濫用 AI 開發生化武器、核武等重大災害之風險與防範評估。各相關部會就共同管轄之事項，應合作評估並訂定相關安全監測標準。

2. 維護財產權與人權

強調 AI 之創新應保障基本人權，司法部門及各機關應避免侵犯隱私、減少因歧視而造成之其他危害，鼓勵監管機構合法地使用 AI 工具。應就標記 AI 合成內容與偵測生成式 AI 進行兒少保護提供相關指引。

3. 促進創新與競爭

美國對於移民及勞工相關部門應採取各項吸引留人人才之措施，包括放寬 AI 人才工作簽證之限制，修正 AI 高階人才居留簽證，推動 AI 研究補助計畫，建立至少 4 個新的國家 AI 研究中心，提供研發協助，促進相關技術之良性競爭，避

本報告之智慧財產權歸屬於國發會

免 AI 關鍵資源被他國控制之狀況。制定以 AI 竊取智慧財產因應方案之指引。

4. 保護個資隱私

為確保個資之利用不侵害基本權利，行政管理預算局與聯邦隱私委員會將合作評估機關採用強化隱私科技（PETs），並促進推動隱私之研究協作網路（RCN）。

5. 維護勞工權益

強調 AI 發展不應侵犯勞工權利，降低工作品質或導致勞動市場之不利影響，用 AI 帶歧視之演算法篩選面試之機會等導致勞工受到不公平之情形，應健全國內相關勞動法令之修訂，制定反僱用歧視指引與僱主運用 AI 指引。

對於工作環境及機會，應提升 AI 作為生產工具之培訓，支持人機共創之機會，促進工作場合在不影響人類基本權利之情況下使用 AI，提升效率。

6. 保障消費者、病患及學生

處理個人資料時應促進各部門保護美國消費者免受 AI 詐騙、歧視及隱私之威脅，擬定醫療使用 AI 之政策框架，強調教育應用領域之使用規範，確保安全、可靠並符合法律規範之使用。

7. 強化國際領導地位

拜登政府要求聯邦政府各機關依照以上 8 大重點議題進行細部任務分工，針對 AI 治理進行實際作為，受到指派的機關包含美國商務部、預算管理局（OMB）、國務卿、以及各大行政部會部長/首長，多數機關必須要在指定期限內進行指引制定、政策匯報或是其他與產業相關之實際作為。

本報告之智慧財產權歸屬於國發會

8. 政府使用 AI 負責有效率

政府應訂定聯邦機關（構）使用 AI 指引，以確保政府使用之創新與風險管理，強化 AI 使用之透明度。預算管理辦公室(OMB)已於 2024 年提出包含各部會需釋出 AI 使用清單，包括哪些 AI 有安全風險及其管理、對政府自有之 AI 原始碼、模型、資料等在無風險之前提下進行開源等措施。

(四)小結

歐盟 AIA 係全球第一部詳細建立 AI 監管制度之法案。透過建立風險分級與罰則，保障人權並將標準推向國際。該法案對於 AI 系統施加了嚴格的限制，包括通用 AI 應尊重歐盟著作權之要求、模型訓練方式透明度揭露、例行測試及充分網路安全保護。歐盟規範較強調對於使用者端之保護，認為處理技術時應有足夠信任、透明與問責、處罰並行，才得以確保技術快速變化下仍符合歐盟對於權益保護之價值。該法案之禁止使用類型將於法案生效後 6 個月內適用，而關於 GPAI 相關義務及規則於生效後 12 個月後適用，其餘原則上應於法案生效後 24 個月完成適用，部分高風險 AI 放寬至生效後 36 個月完成。由於其罰鍰金額可最高到 3500 萬歐元或其全球收入之 7%，故各大科技巨頭皆密切關注本法案實際後續執行狀況。除 AI 研發國家外，使用整合之商品或產業要進入歐盟市場時，也應注意風險分級，並確保符合該法規之規範。

不同於歐盟直接規範監管機制，美國與目前其他大多數國家，係先以政府確認 AI 發展近年之國家政策、技術及產業發展方向，訂定方向指引，並要求各主管部會配合實施或由其制定指引及修改法令。美國於法令政策制定上更偏向於促進技術發展，監管部分則主要以羅列義務或產業自律之方式提出，尚未出現針對違反 AI 所訂定特定罰則。

我國 AI 法令現況，政府尚未訂立整體性共通遵守框架及發展方向，然某些特殊產業如金融、醫療等由於技術快速發展，主管機關已

本報告之智慧財產權歸屬於國發會

先訂定相關使用 AI 之原則。目前我國之立法狀態較雖較偏向於美國以指引先於法令修訂之模式進行，先促進產業利用發展 AI。然而是否應納入歐盟 AI 法案相類似之監管機制，乃取決於我國對於 AI 發展之政策傾向創新還是監管，以及考量是否有足夠之風險評估專業人才、監管人力及經費等資源支撐。亦或是另以上位法要求各部會制定符合其領域之監管制度，於我國現況而言更具彈性。

參考資料：

1. Artificial Intelligence Act of 21th May 2024, https://data.consilium.europa.eu/doc/document/PE-24-2024-INIT/en/pdf (last visited 2024/5/23)

2. Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI, https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/ (last visited 2024/5/23)

3. Briefing EU Legislation in Progress, Artificial intelligence act, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf (last visited 2024/5/23)

4. Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ (last visited 2024/5/23)

5. The European Artificial Intelligence Act: Impact for Medical Devices, https://www.emergobyul.com/news/european-artificial-intelligence-act-impact-medical-devices (last visited 2024/5/24)

6. The EU AI Act: an impact analysis (part 1), https://www.engage.hoganlovells.com/knowledgeservices/news/the-eu-ai-act-an-impact-analysis-part-1 (last visited 2024/5/24)

本報告之智慧財產權歸屬於國發會

7. Impact of the AI Act on the MedTech and Life Sciences Industry, https://qbdgroup.com/en/blog/impact-of-the-ai-act-on-the-medtech-and-life-sciences-industry/ (last visited 2024/5/24)

8. The impact of the AI Act on the facilities Industry, https://bidvestnoonan.co.uk/the-impact-of-the-ai-act-on-the-facilities-industry/ (last visited 2024/5/24)

9. Navigating the EU AI Act – implications for different industries, https://www.linkedin.com/pulse/navigating-eu-ai-act-implications-different-industries-dottir-ttnpf/ (last visited 2024/5/24)

10. AI Act and its impacts on the European financial sector, https://www.eiopa.europa.eu/publications/ai-act-and-its-impacts-european-financial-sector_en (last visited 2024/5/24)

11. The EU AI Act: Open-Source Exceptions and Considerations for Your AI Strategy, The EU AI Act: Open-Source Exceptions and Considerations for Your AI Strategy | Orrick, Herrington & Sutcliffe LLP - JDSupra (last visited 2024/5/24)

12. EU AI ACT: HOW FAR WILL EU COPYRIGHT PRINCIPLES EXTEND? https://www.morganlewis.com/pubs/2024/02/eu-ai-act-how-far-will-eu-copyright-principles-extend (last visited 2024/5/24)

13. 王志誠，人工智慧在金融業運用之法律風險及監控，當代法律，第 28 期，2024 年 4 月，頁 11-25。

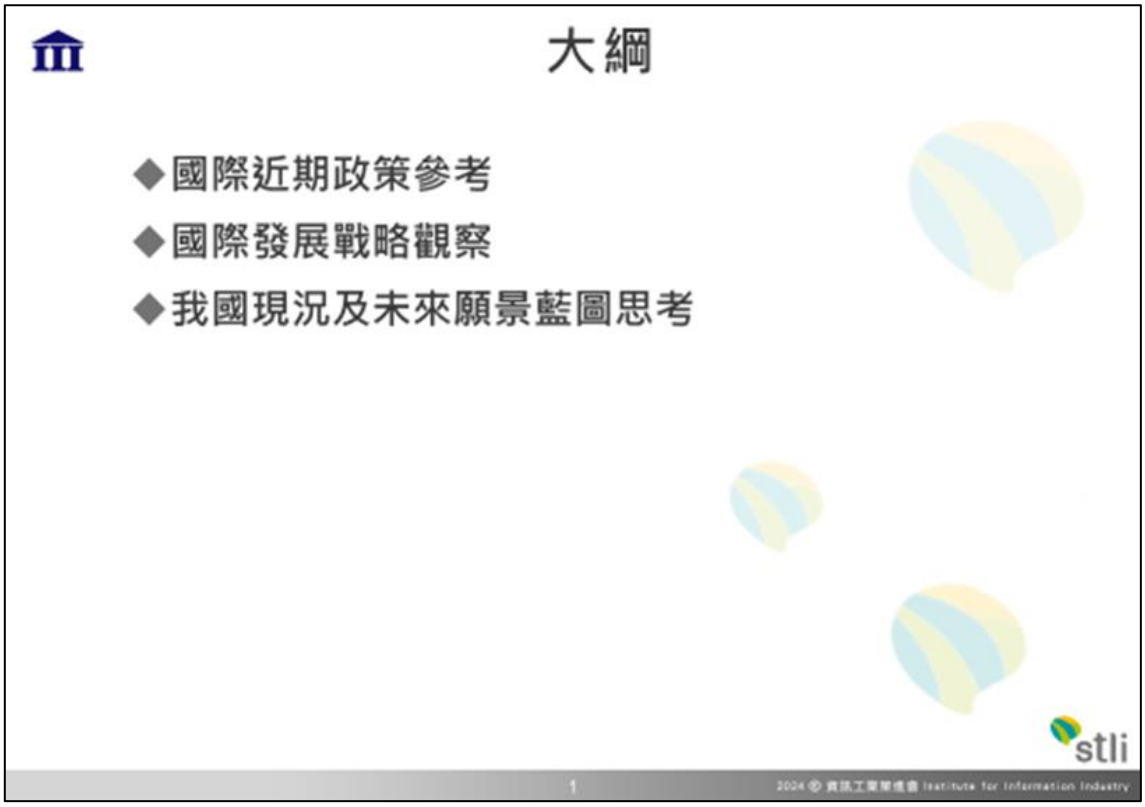
14. 楊惟任，人工智慧的挑戰和政府治理的因應，國會季刊，第 46 卷第 2 期，2018 年 6 月，頁 67-83。

15. 楊智傑、鄭富源，歐盟人工智慧法與生成式 AI 規範，國會季刊，第 52 卷第 1 期，2024 年 3 月，頁 1-30。

16. 洪德欽，歐盟自動駕駛車之發展策略與法律規範，歐美研究，第 50 卷第 2 期，2020 年 6 月，頁 349-431。

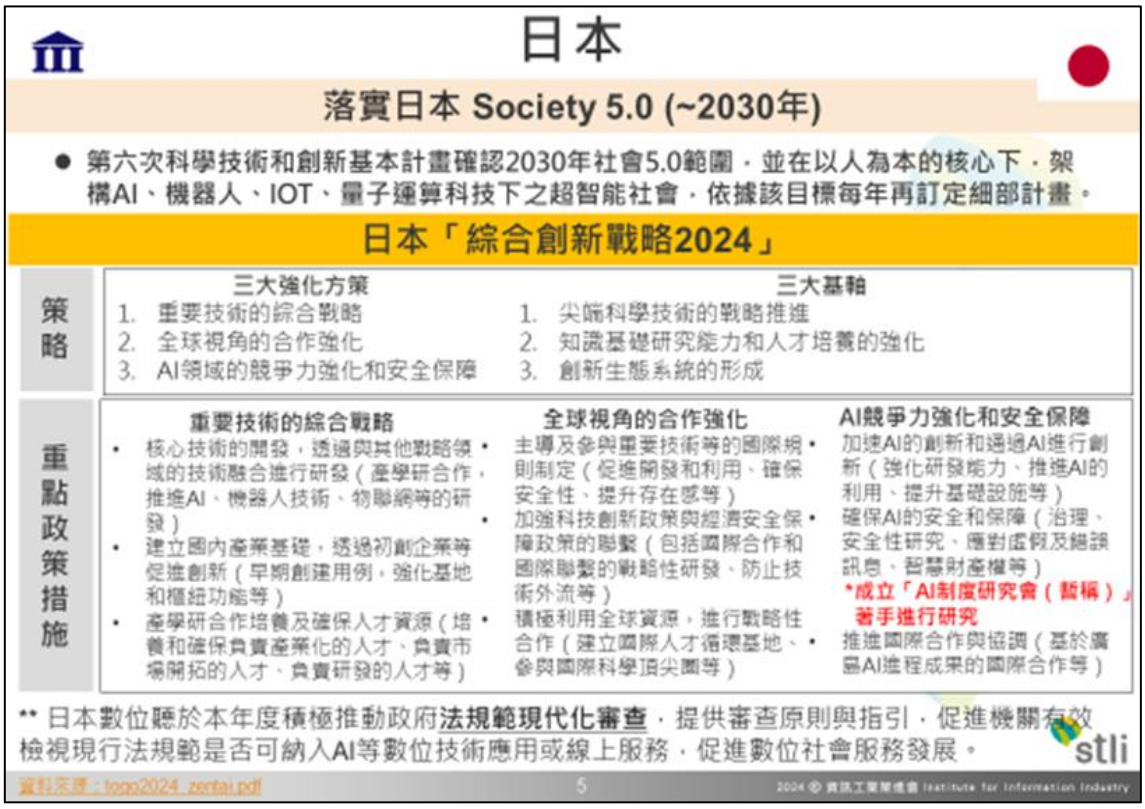
本報告之智慧財產權歸屬於國發會

貳、 數位國家法制政策藍圖思考



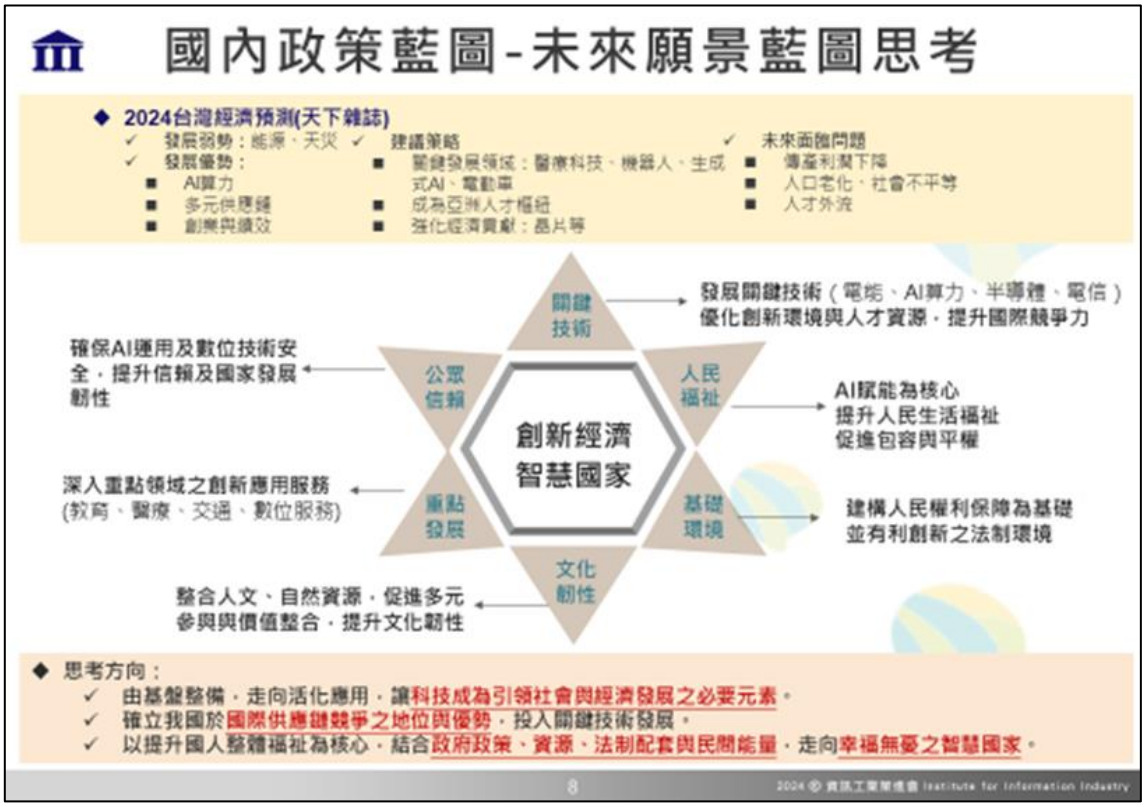
本報告之智慧財產權歸屬於國發會

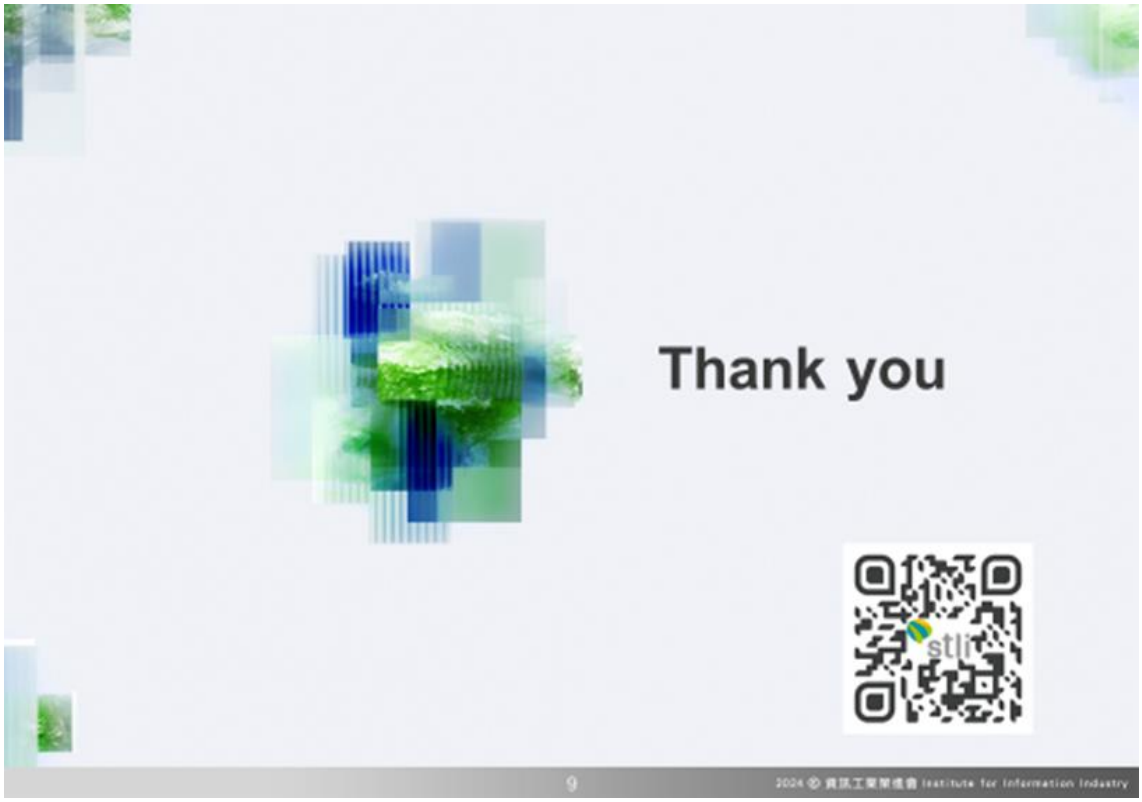
本報告之智慧財產權歸屬於國發會



本報告之智慧財產權歸屬於國發會

本報告之智慧財產權歸屬於國發會





本報告之智慧財產權歸屬於國發會

項次 2. 工作會議討論

壹、 第一次工作會議

一、 會議日期: 2024 年 4 月 22 日(星期一)下午 2 時

二、 會議地點/方式：國家發展委員會法制協調處 605 會議室

三、 出席人員：

(一) 國發會：吳欣玲副處長、溫俐婷專門委員、林馨文簡任視察、鄭美華科長、陳韻如、謝雨航、黃大洲

(二) 資策會：陳益智主任、邱映曦資深協理、陳姿文、林彥甫

四、 會議重點摘要：

(一) 4/23「數位政策法制協調專案會議」工作會議提報資料討論

1. 國發會說明行政院數位政策法制協調會今年已進行之進度：

(1) 本年度於 3/4 曾舉辦一場工作會議，請各分組進行議題提報彙整。盤點內容包括法制、技術或相關計畫，不限法制政策。

(2) 政委期許數位政策法制非單點呈現，應由點線面構築整體政策規劃，且指示數位醫療以及由 AI 展演之智慧醫療是人工智慧在精準醫療面向上的重大發展，應重點關注這方面之議題。

(3) 個資分組和資料創新分組法制面可能有議題重疊，惟若改以技術層次觀察，部分議題無法視為單純個資議題，如數據公益運作、資料二次利用或自動化決策，此是由於資料之應用、儲存和蒐集，不應只限個資議題分類，

本報告之智慧財產權歸屬於國發會

若與 AI 結合之資料運用，就數位前瞻政策立場，仍偏重在創新應用的層面，故應歸入資料創新分組之中；然若創新應用的過程產生保護個資的爭議，則應納入個資分組。

(4) 政委認為數位政策法制之路徑規劃仍處於較鬆散之架構，宜以議題(主題)陳列之方式推展，並對應至各部會所關注之重心，呈現政策規劃的時程。

2. 資策會意見說明：

就各部會提案，嘗試以議題式表單方式，以 AI 角度切入，呈現各部會提案與議題間之連動關係。(現場提供表格參酌)

(二)「前瞻數位科技法制政策變革趨勢研析」委託研究計畫執行情形說明

1. 本專案已於 4/16 決標。

2. 基於年度雙月報提交次數要求，本月（4 月）仍將提交一份雙月報，惟以月底為繳交期程。

3. 為使焦點議題順利擇定，以進行後續趨勢分析及意見溝通，專案企劃書規劃 6 月底前擇定 2 項焦點議題，可於 5 月份行政院大會結束後陸續進行。

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：2024 年 6 月 20 日(星期四)下午 3 時

二、 會議地點/方式：國家發展委員會法制協調處 605 會議室

三、 出席人員：

(一) 國發會:吳欣玲代理處長、溫俐婷專門委員、林馨文簡任視察、許容禎專員、陳韻如專員、謝雨航科員

(二) 資策會：陳益智主任、邱映曦資深協理、林彥甫副研究員

四、 會議重點摘要：

本次工作會議將討論兩項議題，其一、針對國科會預定於 6 月 27 日召開之人工智慧基本法草案推動溝通協調會議，就會議簡報內容及對該草案規劃方向可提出之建議進行討論。其二，係就「前瞻數位科技法制政策變革趨勢研析」委託研究計畫第一階段焦點議題進行討論與擇定。

(一) 針對「人工智慧基本法草案推動溝通協調會議」之討論意見

針對國際 AI 主要立法模式層面，現階段除歐盟以其數位歐洲整體政策考量，訂定以風險為導向之監管專法外，國際上尚無其他類似專法之訂定。會議簡報提及之美國，係以高度技術創新為考量，作為目前全世界領先之 AI 創新國家，以行政命令先行揭示聯邦政府立場；英國於 2023 年即開始致力於透過國際人工智慧高峰會促進國際 AI 監管框架之一致發展，今（2024）年 5 月於韓國召開第 2 屆高峰會並發表首爾宣言；日本則期許成為國際上對AI最友善之國家，以政策指導先行。故人工智慧法制政策之安排，國際趨勢上按國家或區域組織之發展策略有從法制高度監管到以政策或指導為主軸之低度監管等態度差異，可以光譜方式呈現說明；另補充目前主要國

本報告之智慧財產權歸屬於國發會

家包括英、日、韓等，因人工智慧高峰會正在進行國際共通監管邏輯之討論評估，故仍需觀察其走向。

(二)針對國科會提出之人工智慧基本法草案推動架構規劃，預計可提出之建議

1. 現階段國發會就國內 AI 發展主要有兩大方針：一為推升 AI 價值鏈微笑曲線，另一則為深化 AI 生態及充實 AI 產業人才與產業 AI 化。目前在微笑曲線層面，臺灣主要之發展在研發端，另一端之應用端(包括產業應用)則發展比例較小，例如我國智慧應用服務僅占全球 1%等。未來政策上須持續推動以使曲線兩端達到平衡，如以國內具優勢的半導體產業為基盤，輔以 AI 來推動產業的護國群山，持續往微笑曲線的兩端強化。將以此政策目標作為基礎，進行對 AI 基本法草案架構之建議。

2. 就草案推動架構，可從產業促進、信賴保障提升、政策協調三個面向提供建議：

(1) 產業促進層面

I. 鬆綁法制障礙建議調整文字，以進行法規調適為方向。

II. 建議除目前所提之推動發展與獎補助外，另評估新增於金融、租稅層面之獎勵措施，或穩定、充足政府預算編列等發展措施。

III. 確認架構中之公平與不歧視是否涵蓋市場公平競爭之規劃，若未涵蓋則建議補充。

IV. 架構中之促進 AI 實驗沙盒結果落地，若以基本法之性質，建議改為促進創新實驗環境之完備。

本報告之智慧財產權歸屬於國發會

(2) 信賴保障提升層面

I. 提升使用者保護以促進信賴：將對使用端信賴保障法制化，除架構中已納入之風險分級與驗證機制外，建議應明確須建構對消費者之事前保障機制，包括事前安全檢測、監控、揭露或避免歧視之相關要求。

II. 建構適切之救濟求償或保險制度：搭配對消費者之事前保障，亦須建構對應之救濟求償或保險機制，以促進消費者信賴而有意願利用或參與人工智慧相關之產品或服務。架構中有提及問責原則，惟其範圍為何，需予以釐清。

(3) 政策協調層面

基於 AI 自研發至應用之跨域特性，相關法制政策需進行整體協調規劃，以收綜效。故可建議於基本法架構納入政府須建構法制政策協調機制或平臺之相關文字。

(三)「前瞻數位科技法制政策變革趨勢研析」計畫焦點議題擇定

1. 為使焦點議題順利擇定，按企劃書規劃建議於 6 月底及 8 月底各進行 2 項焦點議題擇定。並於 6 月底擇定後再進行 2 項擇定之焦點議題趨勢分析說明。

2. 經本次討論，計畫焦點議題擇定 3 題：

(1) AI 著作權相關議題：針對 AI 研發過程之訓練資料取得層面，如何平衡著作權人之風險與 AI 之發展，諸如兼顧原權利人之保障及如何促進 AI 訓練資料取得等法制面議題。

本報告之智慧財產權歸屬於國發會

(2) AI 應用之消費者保護相關議題：有關建立可信賴 AI 之消費者保護相關議題，諸如對消費者之揭露、演算法歧視、提升消費者信賴等問題。

(3) AI 或演算法運用之勞工權益相關議題：涉及運用 AI、演算法、數位平臺等數位工具於職場的勞工權益相關議題，諸如對運用演算法管理之績效評估、工作分派等可能之歧視，或輔以影像工具進行勞工工作情況監督管理等。又此議題亦可能衍生進一步之焦點議題，可觀察其後趨勢再予評估。

本次先行擇定 3 項焦點議題，資策會將按原定計畫時程，先以上述(1)(2) 2 項議題進行期中之焦點議題趨勢分析說明。

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：113 年 8 月 28 日(星期三)下午 4 時

二、 會議地點/方式：國家發展委員會濟南辦公室 703 會議室

三、 出席人員：

(一) 國發會：温俐婷專門委員、林馨文簡任視察、許容禎科長、陳韻如專員、謝雨航專員、廖晨向科員

(二) 資策會：陳益智主任、邱映曦資深協理、洪亮瑄副研究員

四、 會議重點摘要：

(一) 本研究計畫第 4 項焦點議題擇定為「AI 與個資監管」。

(二) 查企劃書(第 25 頁)規劃於 9 月中提出第 3 項及第 4 項焦點議題趨勢分析說明，惟考量第 4 項議題於 8 月 28 日擇定，衡量資料蒐集及研究時程，請研究團隊於 9 月 30 日前提出第 4 項焦點議題（AI 與個資監管）趨勢分析說明；至第 3 項焦點議題（AI 與勞工權益）趨勢分析說明仍請研究團隊依企劃書規劃時程，於 9 月 15 日前提出。

(三) 關於期中報告審查會議審查委員郭麗珍教授建議於報告附上重要外國法規為附件一事，考量法規全文篇幅過長，將採取表格方式呈現「領域、法規完整名稱、法規超連結」。

(四) 研究團隊將於 10 月份雙月報增加歐盟 EIDAS 相關資料。

本報告之智慧財產權歸屬於國發會

肆、 第四次工作會議

一、 會議時間：113 年 11 月 14 日(星期四)下午 2 時 30 分

二、 會議地點/方式：資策會科技大樓 803 會議室

三、 出席人員：

(一) 國發會：林馨文簡任視察、許容禎科長、陳韻如專員、謝雨航專員

(二) 資策會：陳益智主任、邱映曦資深協理、陳姿文研究員

四、 會議重點摘要：

(一) 協助研析數位政策法制協調專案會議事宜

(密不錄由)

(二) 智慧國家法制政策藍圖方向建議

研究團隊已於本次會議提供智慧國家法制政策藍圖之相關建議及參考資料，若有其他議題或討論事項，再請研究團隊協助提供幕僚意見。

(三) 期末報告與工作會議事宜

1. 本案 113 年期程將屆，爰本會已預先安排期末審查會議。為配合審查期程，請研究團隊預先於 11 月底整理 12 月國際觀測雙月報，納入期末報告，於期末審查時一併審查，再依審查意見進行修正。

2. 第 5 次工作會議請研究團隊配合本會需求時程召開，倘因工作會議期程較晚，未及納入期末報告審查之報告版本，會議記錄得於期末報告最終版本再行列入。

本報告之智慧財產權歸屬於國發會

五、 散會（下午 3 時 50 分）

本報告之智慧財產權歸屬於國發會

伍、 第五次工作會議

一、 會議時間：113 年 11 月 29 日(星期五)下午 5 時

二、 會議地點/方式：國家發展委員會濟南辦公室 605 會議室

三、 出席人員：

(一) 國發會：林馨文簡任視察、許容禎科長、謝雨航專員

(二) 資策會：陳益智主任、邱映曦資深協理、陳姿文研究員

四、 會議重點摘要：

(一) 數位政策法制協調專案會議幕僚意見

(密不錄由)

(二) 期末報告與工作會議事宜

1. 本次工作會議紀錄請團隊於確認後納入期末報告；倘確認時程未及於期末報告審查前完成，會議紀錄得於期末報告最終版本再行列入。

2. 有關 114 年度委託研究計畫，請依會議討論方向，於 12 月 6 日前提供工作計畫項目與報價。

六、 散會(下午 6 時)

本報告之智慧財產權歸屬於國發會

附錄一：國際趨勢觀測重點法案清單

一、 資料治理

法案(中文)	法案(英文)	法案連結
歐盟資料法	Data Act	https://eur-lex.europa.eu/eli/reg/2023/2854
歐洲互通法	Interoperable Europe Act	https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32024R0903
歐洲健康資料空間規則	European Health Data Space	https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2250
2024 網路安全法(修正) (新加坡)	Cybersecurity (Amendment)Act 2024	https://sso.agc.gov.sg/Acts-Supp/19-2024/Published/20240704?DocDate=20240704
網路安全法(英國)	Online Safety Bill	https://www.legislation.gov.uk/ukpga/2023/50/enacted
資料利用與近用法草案(英國)	Data Use and Access Bill	https://bills.parliament.uk/publications/56527/documents/5211

二、 AI 法制政策

法案(中文)	法案(英文)	法案連結
人工智慧公約(歐盟)	Artificial Intelligence Pact	file:///C:/Users/yingniguo/Desktop/AI_Pact_commitments_t0y6WevzGO7IiNoOsCT9GdhwXY_107430.pdf

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)	Artificial Intelligence Act	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689
猶他州人工智慧政策法案(美國)	Utah Artificial Intelligence Policy Act	https://le.utah.gov/~2024/bills/static/SB0149.html
保護消費者免受人工智慧欺騙法草案(美國)	Protecting Consumers from Deceptive AI Act	https://www.congress.gov/bill/118th-congress/house-bill/7766/text
田納西州確保肖像、聲音和圖像安全法案(簡稱:貓王法案-美國)	Ensuring Likeness Voice and Image Security Act	https://legiscan.com/TN/text/HB2091/id/2900923
賓州不公平貿易行為和消費者保護法(美國)	Unfair Trade Practices and Consumer Protection Law	https://www.attorneygeneral.gov/wp-content/uploads/2018/02/Unfair_Trade_Practices_Consumer_Protection_Law.pdf
科羅拉多州人工智慧消費者保護法草案(美國)	AI Consumer Protection Bill	https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf
科羅拉多州公平競選行為法(美國)	Fair Campaign Practices Act	https://www.cde.state.co.us/sites/default/files/documents/cdelib/librarydevelopment/publiclibraries/librarydistrictinformation/download/pdf/faircampaignpracticesact.pdf
生成式 AI 著作權揭露法案(美國)	Generative AI Copyright Disclosure	https://www.congress.gov/bill/118th-congress/house-

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
	Act of 2024	bill/7913/text
晶片及科學法案(美國)	CHIPS and Science Act	https://www.nist.gov/system/files/documents/2023/06/23/CHIPS-CFF%20NOFO%20Amendment%201%20Redline.pdf
OECD 人工智慧原則	OECD Principles on Artificial Intelligence	https://one.oecd.org/document/C/MIN(2024)16/FINAL/en/pdf
首爾宣言 (人工智慧首爾高峰會)	Seoul Declaration 의한 서울선언	https://womennetwork.metropolis.org/sites/default/files/pages/docs-media/docs/declarationwomennetworkseoul.pdf
美國加州人工智慧透明度法案	California AI Transparency Act	https://digitaldemocracy.calmatters.org/bills/ca_202320240sb942
SB 1047 法案(美國加洲- 又稱安全創新之前瞻人工智慧模型法案)	SB-1047，Safe and Secure Innovation for Frontier Artificial Intelligence Models Act	https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB1047
散布、播送及陳列不實性影像法案(美國愛荷華州)	HF2240，A bill for an act relating to harassment by the dissemination, publishing, distribution, or posting of a visual depiction showing	https://www.legis.iowa.gov/legislation/BillBook?ga=90&ba=HF2240

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
	another person in a state of full or partial nudity or engaged in a sex act that has been altered to falsely depict another person, and making penalties applicable.	
散布、播送及陳列與兒少性剝削有關之性影像法案(美國愛荷華州)	SF2243，A bill for an act relating to sexual exploitation of a minor by the creation, adaptation, or modification of a visual depiction to give the appearance that an identifiable minor is engaged in a prohibited sexual act or the simulation of a prohibited sexual act, and making penalties applicable	https://www.legis.iowa.gov/legislation/BillBook?ga=90&ba=SF2243
培育原創、促進藝術與保障娛樂安全法(美國參議院)	Nurture Originals, Foster Art, and Keep Entertainment Safe（NO FAKES）Act	https://www.congress.gov/bill/118th-congress/senate-bill/4875/text
保護美國人免受外國對手應用程式侵害法	Protecting Americans from Foreign Adversary	https://www.congress.gov/bill/118th-congress/house-

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
案(美國)	Controlled Applications Act	bill/7521/text

三、 數位監管

法案(中文)	法案(英文)	法案連結
歐洲媒體自由法案(歐盟)	European Media Freedom Act	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1083
數位市場、競爭及消費者法(英國)	Digital Markets, Competition and Consumer Act	https://www.legislation.gov.uk/ukpga/2024/13/enacted
特定數位平臺透明度及公正性提升法案(日本)	特定デジタルプラットフォームの透明性及び公正性の向上に関する法律案	https://laws.e-gov.go.jp/law/502AC0000000038
數位身分憑證暨數位憑證之聯邦法案(瑞士)	Federal Act on Electronic Identity Credentials and Other Electronic Credentials	https://www.parlament.ch/en/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=64096#votum15
數位服務法(歐盟)	Digital Services Act	https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN
數位市場法(歐盟)	Digital Markets Act	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925&qid=173275

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
		8369955

四、 數位身分

法案(中文)	法案(英文)	法案連結
歐盟內部市場電子交易之電子身分認證及信賴服務規則	electronic Identification, Authentication and Trust Service	https://eur-lex.europa.eu/eli/reg/2014/910/oj
資料保護與數位資訊法草案(英國)	Data Protection and Digital Information Bill	https://bills.parliament.uk/publications/55222/documents/4745
數位身分法案(澳洲)	Digital ID Bill	https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/s1404_aspassed/toc_pdf/2316120.pdf;fileType=application%2Fpdf

五、 數位政策

法案(中文)	法案(英文)	法案連結
虛實整合產業促進法(韓國)	가상융합산업 진흥법	https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%80%EC%83%81%EC%9C%B5%ED%95%A9%EC%82%B0%EC%97%85%20%EC%A7%84%ED%9D%A5%EB%B2%95/(20352,20240227)

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
虛實整合產業促進法施行令(韓國)	가상융합산업 진흥법 시행령안	https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%80%EC%83%81%EC%9C%B5%ED%95%A9%EC%82%B0%EC%97%85%20%EC%A7%84%ED%9D%A5%EB%B2%95%20%EC%8B%9C%ED%96%89%EB%A0%B9
線上安全法(英國)	Online Safety Act	https://www.legislation.gov.uk/ukpga/2023/50

六、 資訊隱私

法案(中文)	法案(英文)	法案連結
美國隱私權法案	American Privacy Rights Act	https://www.congress.gov/bill/118th-congress/house-bill/8818/text
HB 第 1130 號法案：生物辨識識別碼及資料之隱私(美國科羅拉多州)	HB 24-1130：Privacy of Biometric Identifiers & Data	https://leg.colorado.gov/sites/default/files/2024a_1130_signed.pdf
SB 第 41 號法案：兒童線上資料隱私權保護(美國科羅拉多州)	SB 24-041：Privacy Protections for Children's Online Data	https://leg.colorado.gov/sites/default/files/2024a_041_signed.pdf

七、 網路/資訊安全與韌性

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
網路韌性法(歐盟)	Cyber Resilience Act	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454
網路團結法(歐盟)	Cyber Solidarity Act	file:///C:/Users/yingniguo/Desktop/COM_2023_209_1_EN_ACT_part1_v6_ix21csehiaUu6DJoJI4cTZYIfGk_95049.pdf
網路安全法(歐盟)	Cybersecurity Act	https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881
韓國資訊通信網路利用促進及資訊保護法(資訊通訊網路法)	정보통신망 이용촉진 및 정보보호 등에 관한 법률(정보통신망법)	https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EB%A7%9D%EC%9D%B4%EC%9A%A9%EC%B4%89%EC%A7%84%EB%B0%8F%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%93%B1%EC%97%90%EA%B4%80%ED%95%9C%EB%B2%95%EB%A5%A0
兒童資料保護法案(美國-紐約州)	the Child Data Protection Act	https://www.nysenate.gov/legislation/bills/2023/S7695/amendment/A
聯邦兒童線上隱私權保護法	the federal Children's Online Privacy Protection Act	https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312

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
公部門網路安全強化及信任建立法案(加拿大)	Strengthening Cyber Security and Building Trust in the Public Sector Act	https://www.ola.org/en/legislative-business/bills/parliament-43/session-1/bill-194
歐盟高度共通程度之資安措施指令(歐盟)	Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union	https://eur-lex.europa.eu/eli/dir/2022/2555

本報告之智慧財產權歸屬於國發會

附錄二：期中審查會議記錄及意見回應說明

「前瞻數位科技法制政策變革趨勢研析」

委託研究計畫期中審查記錄及意見回應說明

委員	編號	會議記錄及建議	研究團隊回應
郭教授麗珍	1	有關國際法制政策測，希望研究團隊能將重要法案的原文資料或提供其有效的網址超連結，整理作為期末報告附件 提供委託機關後續參考。	1. 感謝委員建議。 2. 已於期末報告附錄二提供國際趨勢觀測重點法案清單及連結。
	2	研究團隊研析國外法制 發展與我國消費者保護法(下稱消保法)之差異 建議從我國消保法架構觀察有無可以對應分析之部分，或是否可能涉及其他法律。期中報告第 36 頁提到英國數位標籤制度，係產品安全標籤 CE 等標示數位化機制 ，可能涉及產品安全，歐盟對於 AI 產品責任部分也有發展，建議研究團隊依研究範圍評估是否納入討論。	1. 感謝委員建議。 2. 已於焦點議題 2 第參部分我國法制概況，補充我國其他法制相關部分，並就消保法可能相關之規範進行闡述。 3. 基於計畫研究期程及設定之焦點研析範圍，係以計畫觀測期間之國際法制趨勢發展為討論核心。近年確實有些 AI 產品責任之發展，包括歐盟之人工智慧責任指令，然截至計畫焦點討

本報告之智慧財產權歸屬於國發會

			論完稿之 11 月仍未有確定內容提出。故已於焦點議題 2 第壹部分背景說明第六段予以補充相關資訊，並說明不列入本次研析範圍。
		關於消費者保護議題的範圍，贊同章老師意見，依我國的法制結構，消費者保護不只涉及消費者，如果不是最終使用、最終消費，可能會涉及民法。各國法制有所不同，我國消保法為民法的特別法，而德國是將消保法融入民法，議題範圍需視本計畫需求與研究範圍進行分析與建議。	1. 感謝委員建議。 2. 已於焦點議題 2 第壹部分背景說明最後面說明，國際趨勢相關法制面所稱之消費者與我國消保法之消費者可能有別，尚包括非基於消費關係之 AI 商品服務之使用者。並於第參部分我國法制概況，補充我國其他法制。 3. 基於本計畫性質與期程，焦點議題探討僅先針對國際趨勢及對應我國相關規範情形進行討論，作為未來法制政策議題探討之參考，故委員提及更深層之各國法制結構差異等深化研究層面，有後續研究之重

本報告之智慧財產權歸屬於國發會

			要性，惟計畫期程範圍有限，本次不列入研析。
	3	數位平臺也是發展中之重要議題，建議評估是否進一步討論平臺監督問題，例如報告第42頁觀察到日本數位平臺透明度法案執行情形。重要議題如勞工權益，研究團隊已納入焦點議題，以及媒體自由議題，報告第34頁觀測到歐盟媒體自由法案涉及之等。	1. 感謝委員建議。 2. 本計畫就焦點研析部分主要係以本年度與主管機關會議擇定之4項焦點議題為限，故部分觀測到之國際發展因未被選定，而未納入焦點。 3. 就委員提及之平臺監督及媒體自由之議題確實有其重要性，故已於第二分項之項次5,法制政策綜整建議一、(二)其他數位法制政策，3.數位監管層面將數位平臺監管與歐盟媒體自由法之發展列入年度國際趨勢重要觀察。
章兼任助理教授忠信	1	消費者保護議題之部分，雖然委託機關焦點議題為AI應用與消費者保護法之關係，建議研究團隊考慮增加研究範圍至所有使用到AI的人，而不限於我國現行消	1. 感謝委員建議。 2. 已於焦點議題2第壹部分背景說明最後面說明，國際趨勢相關法制面所稱之消費者與我國消保法之消費者可能有

本報告之智慧財產權歸屬於國發會

		保法下之終端消費者。	別，尚包括非基於消費關係之 AI 商品服務之使用者。
	2	有關訓練生成式AI而使用著作之議題，實際上涉及著作利用之利益分配問題，目前主要有兩種解決方式：法定授權或商業授權。商業授權例如Open AI跟媒體、出版社合作授權，獲得可信賴之資料，以解決生成式AI資料不即時、不具正確性的問題。另又如Adobe提出新的商務模型，約定權利人將資料放上作品利用平臺即為同意，而使用者使用該平臺資料則不會造成侵權，且權利人可分紅，亦是可研究的方向。	1. 感謝委員建議。 2. 有關強化或建立 AI 訓練資料與生成結果使用收益分配機制，已於研析小結中說明，雖日本與新加坡給予 AI 學習使用著作權作品合法空間，但日本於前揭指引中仍限制排除已經以收費方式提供的資料庫等不合理損害著作權人權益的利用方式。 3. AI 訓練資料如何簡便、經濟、明確有效的取得，從國際立法例上，尚未見有法制面的明顯事例，然於實際商業授權操作上，Adobe 提出新的商務模型約定權利人將資料放上作品利用平臺即為同意，而使用者使用該平臺資料則不會造成侵權，且權利人可分紅，自是政府可鼓勵

本報告之智慧財產權歸屬於國發會

			的方向。於法制面若能同時賦予據以取得授權者免受侵權追訴的法律效力，相關機制將能更具誘因、可長期持續而且無須政府資源投入。
	3	有關外國立法例，考量美國州、參議院之立法草案，可能不夠全盤性，建議觀察美國專利商標局(USPTO)或著作權局(US Copyright Office)等相關主管機關資訊較為全面；至是否納入中國大陸之法規，請研究團隊斟酌。	1. 感謝委員建議。 2. 已於報告增加美國著作權局(US Copyright Office)有關其著作登記指引的重點、「著作權與人工智慧議題徵詢通知(Copyright Office Issues Notice of Inquiry on Copyright and Artificial Intelligence)」的調查事項，以及該局對 AI 系統引發的著作權法和政策問題所發表的研析報告容。 3. 至於中國大陸之法規，考量目前對象已具代表性，而其 AI 發展規範有其特別的政策考量，亦非計畫規格要求，故暫不納入觀測範圍。

本報告之智慧財產權歸屬於國發會

	4	有關揭露義務，建議強調透明性義務，如類比AI應用與藥品，不具透明性則無法檢測使用過程的風險，就不能提供公眾使用，以確保公眾利益不被侵害。	1. 感謝委員建議。 2. 趨勢分析過程各國規範發展提及揭露或告知義務等層面，因焦點部分係整理計畫過程趨勢發展之情形，故就用語部分會以所觀察到之法規或指引文獻用語及討論範圍為主，故仍保留揭露義務。透明性義務部分則可能大於揭露義務之範圍，感謝委員提點，後續若有更深入之討論則可對透明性義務部分加強論述。
中原大學法學院黃助理教授絜	1	期中報告第146頁註腳21所列網址已失效，建議研究團隊更新網址。	1. 感謝委員提醒。 2. 已更正網址。
	2	有關外國立法例，美國除觀察各州州法外，著作權局網站設置 AI 專區，建議可參考該專區之資料。經濟合作暨發展組織(OECD)推動之人工智慧全球夥伴聯盟 (Global Partnership on	1. 感謝委員建議。 2. 已將著作權局及 OECD 網站納入觀察。

本報告之智慧財產權歸屬於國發會

		Artificial Intelligence, GPAI)，近幾個月提出相關專題報告，建議研究團隊可留意相關資料。	
	3	有關期中報告第161頁，提到人為介入AI創作之著作權議題，建議可納入法院見解供研析。另外美國田納西州特別關注鄉村歌手的著作，聲音可能被作為AI訓練模型或詐欺，而涉及著作權使用的利益衡量。可延伸對應臺灣娛樂產業如何保障聲優權利等議題，不過此部分或已非著作權議題。	1. 感謝委員建議。 2. 關於聲音之權利確實是值得關注之議題，此部分已非著作權或消費者保護相關規範可以具體解決，而涉及 AI 應用下是否有必要考量新興權利之問題。因超過焦點議題探討範圍，但有其重要性，故已納入第二分項項次 5 法制政策綜整建議，提醒長期規畫應考量 AI 發展之新興權利問題。

本報告之智慧財產權歸屬於國發會

附錄三：期末審查會議記錄及意見回應說明

「前瞻數位科技法制政策變革趨勢研析」

委託研究計畫期末審查記錄及意見回應說明

委員	編號	會議記錄及建議	研究團隊回應
東吳大學法學院章兼任助理教授忠信	1	人工智慧(AI)與智慧財產權的法制政策除法律層面討論之外，尚需考慮行政之協助，各機關嘗試以行政指引協助提醒注意及運用可能之問題，其中「透明性」是AI治理中最重要的原則，讓相關人能知悉運用 AI 可能造成之後果及應負之責任；將 AI 比擬為很有效的藥，如需供公眾使用，須揭露其成分、製程及可能之副作用。故AI之監管，主管機關須以公權力須介入要求揭露義務，出於公平、合理及公共利益之角度，明確規範哪些行為不可為。	1. 感謝委員建議。 2. 透明性確實為目前國際AI治理之重要原則，報告當中已多有摘述，後續研究亦將持續關注透明性之議題。
	2	除著作權外，另外一個智慧財產權議題係營業秘密，該權利為產業競爭相當重要之資產，若產業使用營業秘	1. 感謝委員建議。 2. 本次焦點議題為著作權，營業秘密議題或可

本報告之智慧財產權歸屬於國發會

		密訓練 AI，且未進行足夠之保護措施，恐將無營業秘密可言。	做為其後追蹤研究主題參考。
	3	有關 AI 訓練與其訓練素材之「合理利用」或其他可能性，建議國家政策應避免為推動 AI 發展，而忽視權利人之權利。訓練 AI 時對著作之利用，可否認定其符合合理使用，各國雖有討論，但皆未有明確定論。如是，恐將導致 AI 研發者無償利用他人作品卻靠訓練後之系統獲得利益。報告提及 AI 訓練他人著作應對應給予權利人對價之配套措施，性質上應非「對其有適當補償」，建議修改為「獲得適當報酬」。	1. 感謝委員建議。 2. 報告提到之補償部分為所參考韓國指引文獻之用語，為確保趨勢之整理之內容符合實際國際文獻之說明，故此次仍維持「適當補償」之用語。 3. 委員所提應該是「獲得適當報酬」之概念，可作為後續機關進行法制政策規劃之參考。
	4	AI 訓練對於著作之利用，究竟屬著作權法上之特定權利，或應新增其他新的權利，尚有討論空間，例如 AI 訓練若有重製行為，則有重製權授權問題；若僅依靠「看」而不必重製作品亦可達到訓練目的，則是否對權	1. 感謝委員建議。 2. 本次報告意見與委員相同，建議對於 AI 議題除現有之權利規範外，亦得考慮建立新興權利之可能性。

本報告之智慧財產權歸屬於國發會

		利人之權利有影響，亦即報告所提的新興權利考量等。	
	5	AI治理中，利用人之責任亦十分重要，現行法令規範，係依故意或過失，負擔刑事或民事責任；但AI利用往往難以判斷故意或過失，或應由開發者或利用者負責，還是有其他責任之歸屬，尚無定論，建議主管機關將AI使用者是否有必要免除其使用AI的某些侵權責任納入政策思考。	1. 感謝委員建議。 2. 此建議為對於 AI 整體法制面向之建議，可納入後續相關機關政策評估之參考。
國立政治大學法學院劉教授定基	1	關於綜整建議，建議於短期建議納入相關立法方向或實例，例如我國已公告之AI基本法草案。此外，短期建議中，各領域主管機關提供相關指引有其必要性。建議各部會可思考自身法令是否足以因應AI之發展，若認為現行法已足以適用並不需要修訂，則建議提供相關指引，說明現行條文如何適用在該領域之AI相關風險或責任，讓民眾有所依循。	1. 感謝委員建議。 2. 已於綜整建議中之短期建議部分加入第(3)點，建議加速推動 AI 基本框架法制之通過，建立並強化各界對國內整體法制政策推動之共識。指引或指導原則之建構則已於建議(2)提出。

本報告之智慧財產權歸屬於國發會

	2	歐洲理事會之AI框架公約，2024年開放各國簽署，雖然是抽象的框架，惟監管立場迥異之歐盟與美國皆有簽署，可見其重要性。建議研究團隊適當將此發展補充在短期建議中，做為我國應納入共通性監管框架性立法的正當性基礎。	1. 感謝委員建議。 2. 已於綜整建議中之短期建議(3)部分，搭配 AI 基本法，補充說明歐洲理事會之 AI 框架公約簽訂之啟示。並配合建議加速 AI 基本法等框架性法制之推動。
	3	有關綜整建議之中長期建議，宜說明共通性作用法為何。若是指類似AI法(AIA)這類具體的監管法令，則可搭配前述短期建議中之監管基本框架，延伸出具體監管規範內容。	1. 感謝委員建議。 2. 中長期建議之共通性作用法規範，確實係對應基本法以外，針對 AI 開發者、部署者或使用者之共通性規範要求。可能可參考歐盟 AIA 之監管規範，但仍需考量我國情與 AI 發展情形。原建議當中已有列出部分共通性議題，如避免開發會出現歧視結果之 AI，對於部署者要求必須讓參與之使用者知曉或了解其正在利用 AI 或被 AI 分析，AI 可能對他作哪些方面之決定或可能產生甚麼影響，有

本報告之智慧財產權歸屬於國發會

			無申訴的機會。以及要求事業若運用 AI 於業務各層面，必須有適當之人為監控或定期檢測評估等。以及對於 AI 資料取得應用可能面臨之共通問題等。 3. 至於若要更進一步就各議題提出監管規範內容，基於 AI 基本法之配套作用法規範已有分工，則建議由部會就所轄事務及法制進行考量，議題範圍過大，於本次研析將先不予延伸。
	4	關於AI個資隱私焦點議題分析國內外比較部分，歐盟資料保護監管機關(EDPS)文件可對應我國行政院及所屬機關(構)使用生成式AI參考指引，此份指引層級較高且對我國公務機關有拘束力，建議補充相關比較，或提供我國行政院是否應調整該指引之建議。	1. 感謝委員建議。 2. 已於焦點議題 4 第三部分我國法制概況增加「行政院及所屬機關(構)使用生成式 AI 參考指引」，亦補充金管會之「金融業運用人工智慧(AI)指引」做為我國法制現況之說明之一。並簡單補充其與 EDPS 指引之差異。

本報告之智慧財產權歸屬於國發會

	5	針對個資保護特定應用上，如利用網路爬取資料(data scraping)內含個資之狀況，於我國是否適用個資法及如何適用之議題，亦請予以補充。2024年全球隱私大會(GPA)就該議題已透過與業界就資料抓取和隱私保護的初步聯合聲明提出部分看法，於現行個資法體制下或有可參考之處。	1. 感謝委員建議。 2. 已取得所述 GPA 文件，因該文件為較為廣泛之資料抓取問題，並要求具市場控制力之事業及平臺必須採取措施避免資料非法抓取。由於該文件並非針對 AI 個資保護議題探討之文獻，將納入後續資料隱私議題之追蹤分析，本次結案報告文稿暫不補充。
	6	AI勞動議題中，歧視亦為勞工權益保護之重要議題，美國除勞工部外，公平就業機會委員會(EEOC) 2023及2024年亦有相關指引可參考，建議予以補充。	1. 感謝委員建議。 2. EEOC 確實於 2023 年有公布一份提供雇主參考之 AI 指引。今年度則是發表一個聲明，說明 EEOC 於 AI 之角色。基於本次焦點係以本年度觀察之發展為趨勢分析之範圍，故 2023 年指引將不予納入，但於該篇焦點之背景說明最後，補充 EEOC 於 2023 指引及 2024 年聲明之兩份

本報告之智慧財產權歸屬於國發會

			文件資訊及註腳連結，以提供後續相關主管機關參考。
個人資料保護委員會籌備處	1	報告第559頁所提「歐盟、澳洲及新加坡…資料保護影響評估」置於設立資料保護專員項下，似有誤植，建議調整。	經查該段為誤植，已修正。
	2	報告第 535 頁所提歐盟個資保護委員會(EDPB)針對資料保護機關在 AIA 上之角色發佈聲明，建議歐盟各會員國指定個人資料保護機關(DPA)作為 AI 之監管機關，請問實際上歐盟各國是否遵照辦理，或是有指定其他機關情況，如有相關資訊建議研究團隊可以再補充實際運作情形供主管機關參考。	1. 感謝籌備處。 2. 歐盟 EDPB 之聲明係今年中才發布，故現階段尚未有實際執行之資料及報告出來。後續若有追蹤到相關發展，可再提供參考。

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
/邱映曦計畫主持.
-- 初版. -- 臺北市 : 國發會, 民 113.12
面: 表，公分
編號: (113) 020.0902 (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：邱映曦
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 113 年 12 月
版次：初版　　刷次：第 1 刷
編號：(113) 020.0902　(平裝)

本報告之智慧財產權歸屬於國發會