

# 「人工智慧之相關法規國際發展趨勢與因應」

## 委託研究計畫

### 結案報告

受委託單位：理律法律事務所

研究主持人：曾更瑩合夥律師

協同主持人：吳志光合夥律師

研究期程：中華民國 107 年 7 月至 107 年 12 月

研究經費：新臺幣 82 萬元

國家發展委員會 委託研究

中華民國 107 年 12 月

(本報告內容純係作者個人之觀點，不應引申為本機關之意見)

## 目錄

摘要 .....	i
Abstract .....	ii
第一章 緒論 .....	1
第一節 研究緣起與目的 .....	1
第一項 研究目的 .....	1
第二項 預期效益 .....	1
第二節 研究架構與方法 .....	2
第一項 研究架構 .....	2
第二項 研究方法 .....	2
第二章 外國官方報告主要議題整理 .....	4
第三章 人工智慧相關法律議題探討 .....	14
第一節 引論 .....	14
第二節 人工智慧對於著作權法制之適用疑義 .....	16
第一項 焦點議題 .....	16
第二項 外國文獻分析 .....	17
第三項 針對我國法規調適之初步建議 .....	61
第三節 人工智慧時代下的個人資料保護與合理利用 .....	64
第一項 焦點議題 .....	65
第二項 外國文獻分析 .....	70
第三項 針對我國法規調適之初步建議 .....	78
第四節 結合監理沙盒及人工智慧以建置臺灣無人載具產業發展環境 .....	80
第一項 焦點議題 .....	83
第二項 外國文獻分析 .....	88
第三項 針對我國法規調適之初步建議 .....	102

第五節	人工智慧及大數據於公權力執行之運用.....	112
第一項	焦點議題.....	112
第二項	外國文獻分析.....	115
第三項	針對我國法規調適之初步建議.....	123
第六節	結合金融監理沙盒及人工智慧以活化臺灣金融產業.....	127
第一項	焦點議題.....	127
第二項	外國文獻分析.....	129
第三項	針對我國法規調適之初步建議.....	142
第七節	人工智慧運用於醫療服務之相關法律疑義.....	151
第一項	焦點議題.....	151
第二項	外國文獻分析.....	153
第三項	針對我國法規調適之初步意見.....	177
<b>第四章</b>	<b>結論與建議.....</b>	<b>186</b>
<b>附錄一</b>	<b>期中報告審查會議紀錄.....</b>	<b>190</b>
<b>附錄二</b>	<b>期末報告審查會議紀錄.....</b>	<b>194</b>
<b>附錄三</b>	<b>外國官方報告摘要.....</b>	<b>202</b>
I.	WIPO.....	202
II.	IEEE.....	203
III.	美國.....	226
IV.	歐盟.....	250
V.	英國.....	257
VI.	法國.....	272
VII.	加拿大.....	278
VIII.	日本.....	283
IX.	新加坡.....	286

X. 印度.....	288
<b>附錄四 「人工智慧之相關法規國際發展趨勢與因應」研討會資料.....</b>	<b>299</b>
壹、研討會議程.....	299
貳、研討會題綱.....	301
參、研討會簡報.....	309
肆、研討會會議紀錄.....	351
<b>附錄五 參考資料.....</b>	<b>369</b>

## 摘要

近年來，由於人工智慧相關技術有長足的進步，各國紛紛將人工智慧發展納入國家重大政策，希望能夠在這波新興產業革命中取得先機，帶動未來經濟發展邁入新階段。而隨著發展人工智慧成為國際趨勢，相關法制層面的需求也日益增加，目前國際間針對相關法制議題的討論，雖仍未有定論，惟有鑒於人工智慧發展及其影響的重要性，本計畫冀能透過蒐集國內外相關文獻及討論，探討人工智慧發展可能涉及的法規適用疑義，進而就我國現有法制提出調適及因應建議，作為我國政府後續政策規劃的參考。

本報告除了蒐集與爬梳各國官方文件及國際組織報告之內容外，亦透過研析各國立法例、修法芻議、學術文章、專家意見及其他重要討論，針對「AI 對於著作權法制之適用疑義」、「AI 時代下的個資保護與合理利用」、「智慧載具發展及侵權責任歸屬」、「AI 及大數據於公權力行政之運用」、「AI 與金融監理沙盒之應用」、「AI 運用於醫療服務之相關法律疑義」等六大議題提出法規調適及因應建議，惟考量國際間相關討論尚在發展中，本報告亦將「持續觀察」列為建議選項之一，確保我國法制發展符合國際趨勢。

最後，由於人工智慧所涉及的層面十分廣泛，並非本報告所能窮盡，本報告亦建議我國政府針對若干法制議題作進一步的研究，包括 AI 對勞動力市場的衝擊、訂定 AI 倫理規範及設置 AI 倫理委員會之必要性、AI 發明的可專利性等，俾以緩和人工智慧應用可能帶來的衝擊，亦避免我國人工智慧發展因受限於既有法制而錯失良機。

## **Abstract**

With the rapid advancement of AI (artificial intelligence) technologies, governments around the world have been implementing major national policies to facilitate the development of AI, in the hopes of becoming the pioneers in this emerging industry and technology revolution in order to take their economies to the next level of growth. As the development of AI has become an international trend, there are growing demands for relevant laws and regulations, albeit the international community has not yet come to a consensus on the legal ramifications of AI. In light of the ubiquitous presence of AI and its significant impact on our societies, this study aims to identify the key issues surrounding the application of the laws regarding the development of AI through taking stock of and analyzing relevant literatures and discussions at home and abroad before proposing adjustments and response strategies specific to the legal framework in Taiwan. We hope the proposals herein will serve as a reference for the government's subsequent planning of AI policies.

Apart from reviewing official policy papers from different countries and reports produced by international organizations, this study has also analyzed and compared the relevant legislations, legislative proposals and initiatives, academic journals, expert opinions and other key discussions before proposing recommendations in law and practice for the following six major issues: (i) Application of copyright laws on AI-related matters; (ii) data protection and fair use under the context of AI; (iii) the development of unmanned vehicle and relevant tort liability; (iv) using AI and big data under public authority; (v) the application of AI and financial regulatory sandbox; and (vi) legal ramification of the application of AI in healthcare. As AI-related issues are under constant discussions and development among international communities, this study believes that continual observation and monitoring on relevant issues are also required to ensure that the development of the legal framework in Taiwan is in line with international trends.

Finally, as AI involves a wide array of issues which cannot be covered by this study, we also recommend the government to conduct further research on a number of relevant legal issues, such as the impact that AI has on the labor market, the necessity of setting forth AI ethic rules

and ethic committee, the patentability of inventions by AI, in order to mitigate the potential impact that the application of AI will bring about and to prevent any loss of opportunity in AI development due to Taiwan's existing legal restrictions.

## 第一章 緒論

### 第一節 研究緣起與目的

#### 第一項 研究目的

近年來，由於雲端運算（Cloud Computing）及物聯網（Internet of Things）日益普及，加上大數據分析（Big Data Analytics）及深度學習（Deep Learning）等技術快速發展，使得人工智慧（Artificial Intelligence，簡稱AI）的進展與推動成為可能，各國紛紛將AI發展納入國家重大政策，期能厚植國內AI研發能量與基礎環境，並在這波新興產業革命中取得先機，帶動未來經濟發展邁向新階段。

有鑒於臺灣在資通訊與半導體產業及技術上的優勢，可為國內AI發展奠定良好的基礎，我國政府亦致力於推動AI發展，包括行政院「台灣AI行動計畫」（2018-2021）、科技部「人工智慧（AI）推動策略」及國家發展委員會協調推動的「亞洲·矽谷」計畫等，希望將臺灣塑造為全球智慧創新的重要樞紐。但隨著發展AI成為國際趨勢，且影響層面遍及社會各種面向，相關法制層面的需求也日漸增加，特別是（一）相關規範框架的制定；（二）現有法規的調適與鬆綁；以及（三）相關法律主體及權責的釐定等，均需透過跨領域對話及多元參與等方式，進行廣泛且深度的討論與研析，俾以緩和AI應用上可能帶來的衝擊，並避免我國AI發展因受限於既有法制而錯失良機。

目前國際間相關議題討論及發展趨勢，雖仍未有定論，惟鑑於AI發展及其影響的重要性，本報告冀能透過蒐集國內外相關文獻與重要討論，深入研究AI發展可能涉及的法規適用疑義，進而就我國相關法規的調適及鬆綁提出因應建議，作為我國政府後續政策規劃的參考。

#### 第二項 預期效益

本報告預計可為我國AI發展帶來以下效益：

- 一、針對AI發展可能涉及之法規適用疑義，蒐集國內外重要文獻、立法例及執法經驗，為我國相關法規的調適及鬆綁提出因應建議，作為我國政府後續政策規劃的參考。



- 二、透過舉辦座談會廣徵產官學研各方意見，確保AI發展過程中實際面臨的法制障礙，可透過本報告研議的法規調適或鬆綁，獲得及時且有效的解決。

## 第二節 研究架構與方法

### 第一項 研究架構

為了針對 AI 發展可能涉及的法規適用疑義提出因應建議，除指定研究課題「AI 對於著作權法制之適用疑義」外，本報告嘗試從 AI 實際應用情境出發，逐一探討「AI 時代下的個資保護與合理利用」、「智慧載具發展及侵權責任歸屬」、「AI 及大數據於公權力行政之運用」、「AI 與金融監理沙盒之應用」、「AI 運用於醫療服務之相關法律疑義」等議題，並透過研析國內外官方報告、立（修）芻議、學術文章、專家意見及其他重要討論，針對該等議題提出法規調適與鬆綁的因應建議，包括由行政機關頒布函釋或修訂行政命令、經行政院報請立法院增修法律規定等作法，俾以兼顧法規調適的效率與彈性。

### 第二項 研究方法

本報告所採用的研究方法如下：

#### 一、文獻探討法

針對AI可能涉及的法規適用疑義，蒐集各國（包括但不限於美國、歐盟、英國、日本、澳洲、新加坡、中國大陸等）官方報告、產業政策、立（修）法芻議及其他重要討論，深入瞭解國際間最新發展趨勢，並輔以國內外學術文獻及專家意見，就我國如何因應AI對現有法制可能帶來的衝擊提出因應建議。

#### 二、比較法制研究法

參考各國（包括但不限於美國、歐盟、英國、日本、澳洲、新加坡、中國大陸等）目前針對AI所頒布的法令及執法進展，比較外國與我國現有法制在因應AI挑戰上有何異同，借鏡他國法制經驗，對我國法規調適提供因應建議，俾以打造有利於AI發展的法制環境。

#### 三、綜合歸納分析法

除文獻探討及比較法制研究外，本計畫亦在107年11月14日舉辦四場座談會，於會中邀請相關產官學研代表擔任與談人，綜合歸納相關意見與建議，期能為我國AI發展研擬立（修）法建議及配套措施，兼顧產業需求及相關利害關係人權益。

## 第二章 外國官方報告主要議題整理

目前世界主要國家針對人工智慧技術之發展及相關議題之研究，均投入大量的時間與預算，本計畫茲就重要國際組織、世界各國針對人工智慧之研發趨勢與重要爭議的討論加以摘要說明，內容請參閱「附錄二」，以供各界參考。在此波人工智慧的熱潮中，美、英、法、歐盟、加拿大、日本、新加坡、印度等國政府均對人工智慧加以研究，重要國際組織如世界智慧財產權組織 (World Intellectual Property Organization, WIPO)、電機電子工程師學會 (The Institute of Electrical and Electronics Engineers, IEEE) 亦對於人工智慧相關議題表達立場。本章本文部分謹將重點摘要整理如下：

WIPO
<p>針對伯恩公約中著作權保護條款，WIPO 於報告中認為必須修改定義及適用範圍，例如：</p> <ol style="list-style-type: none"><li>1. 對於「電腦產出著作」的定義應明確，例如「透過電腦產出的著作，無論是否有任何無法區分個別著作人的人類貢獻結合於該成果中」。</li><li>2. 電腦產出著作應受伯恩公約保護，但應以「為創作該著作進行必要安排之自然人或法人」為其著作人，且就伯恩公約著作人格權 (moral rights) 的規定，於電腦產出著作應不予適用。</li><li>3. 著作權之權利存續期間原則上應依伯恩公約原本的規定。</li></ol>
IEEE
<ol style="list-style-type: none"><li>1. 應確立相關科技發展遵循倫理通則，其中包括人權保障、福祉 (Well-being) 優位、對於技術設計及操作問責 (Accountability)、透明公開 (Transparency) 及降低濫用 (Misuse) 風險</li><li>2. 應將人類價值觀嵌入自主化智慧系統，使自主化智慧系統識別及執行社會規範，並評估執行之狀況。</li><li>3. 加強倫理研究及設計方法，包括跨領域的教育與研究、企業應於各個環節強化倫理文化之實踐、開發/測試自主化智慧系統科技的研究倫理、加強透明性 (包括設立獨立審查機構監督產品是否符合倫理標準)。</li></ol>

4. 應加強通用人工智慧 (Artificial General Intelligence, AGI) 及超人工智慧 (Artificial Superintelligence, ASI) 的安全性及穩定性，包括設立審查委員會。
5. 加強個人資料及個人存取之管制，包括數位人格的控制、採行地方管轄權、代理權與控制之平衡 (亦即個人資料使用與同意應由個人使用系統管理)、資料管理工具應具有透明性、資料擁有者的同意能力與平等 (如消費者、受僱人、老人或心智障礙者之同意)。
6. 重新建構自主武器系統，包括自動武器應可以審計追蹤 (audit trail)、系統得以透明和可理解的方式向人類解釋其推理和決策、自主系統中應有可特定之人工操作員、自主系統的行為應可預測、創造該等技術之人應理解其產品的含義、應制定專業道德規範。
7. 經濟及人道問題，建議私部門應注意企業社會責任、公部門則應增進權力結構的透明度、開發中國家培養自主化智慧系統技術。且另建議培訓勞動力、建立對於個人資訊權益保障之認知、大學及研究所之人工智慧相關教育應融入「具全球維度之工程學」、使人工智慧與自動化技術可用於全球產業、建構適當的法律架構 (包含系統之問責性及可驗證性)。

## 美國

1. 針對數據資料與演算法部分：
  - (1) 支持減少演算法歧視的相關研究，建立系統性的公平與問責，並發展資料倫理框架。
  - (2) 鼓勵企業與消費者團體設計出最佳的演算法系統，藉此修正不正確的資料，並挑戰演算法所作出的決定。
  - (3) 促進學術研究與產業對於演算法的外部稽核與測試系統，藉此確保人民受到公正的對待。
  - (4) 擴大電腦與資料科學的參與，提高美國民眾相關基礎能力與影響力。
  - (5) 考量公私部門在設定資料使用規則上所扮演的角色。
2. 針對 AI 研究發展

- (1) 應對 AI 研究長期投資大量心力、時間與資金，並應跨領域合作，整合各方專家及專業團體。
- (2) 在各層級之政府部門中招募 AI 專家並制定相關監管規範。有效之政府治理有賴更多之專家了解並分析 AI 科技與社會整體價值之連結與互動。
- (3) 發展有效的人機協作方法。
- (4) 瞭解並處理 AI 在倫理、法律及社會上的影響。
- (5) 保障人類在 AI 之平等、安全與隱私，並屏除潛在和實際之障礙。
- (6) 確保 AI 系統的安全性與可靠性。
- (7) 建立沙盒，允許監管機構進行小規模試驗。
- (8) 為 AI 訓練與測試開發公眾共享的數據/資料及環境，增加數據共享之誘因。
- (9) 透過標準及基準測量與評估 AI 技術。
- (10) 增進對國家 AI 研發勞動力需求的瞭解，並理解 AI 對就業的影響，重新構思未來的職業訓練和教育。

3. 在符合國際人道主義法的基礎上制定關於自動和半自動武器的統一政府政策。

#### 歐盟

1. 建立代表機構：應為機器人和人工智慧設置歐洲代表機構（European Agency），專門提供科技、倫理、規範上的建議。
2. 智慧財產權保護：應該提供一個科技中立的方法來處理雇用機器人時的智慧財產權問題，並確認歐洲民事法規皆符合歐盟一般資料保護規則（General Data Protection Regulation, GDPR）之規定。
3. 個人資料保護：個人資料保護與組織所採用的隱私政策有關，並會影響提供數據預測的門檻。
4. 建立標準化的試驗規範：歐盟各國應該要考量國際科技標準之一致性，並避免內部市場的分裂，保障顧客和產品的安全性，加以制定標準化的機器人試驗規範。
5. 機器人基本行為準則：機器人必須尊重人類的自主決定權，亦即機器人必須永遠服從

人類的命令。然而，因為機器人不可以拿來當作武器，所以當人類對機器人下達的命令可能傷害使用人或第三人時，機器人必須發出警告信息。

6. 照護機器人：照護機器人是機器人發展的重要領域，其可以擴大原有的人類照護，並可以將照護程序加以明確化，讓醫療人員可以花更多精力在診斷和制定醫療方針上。但本報告仍然重申與被照護者進行社會互動是不可欠缺的。
7. 醫療機器人：醫療用的機器人最重要的是必須符合最低限度的專業要求，從一開始的治療到最後的決定都必須符合人類醫師的標準。
8. Cyber Physical systems (CPS)：即將計算機網路科技系統、機器人以及與真實世界互動之人工智慧加以整合。
9. 環境影響：機器人的使用在農業、供給食物、交通方面可以給環境帶來良好影響，但機器人的行為準則是不可以破壞環境。
10. 國際方面：道路交通維也納公約、阿姆斯特丹宣言、海牙條約必須齊備。
11. 倫理規則：應建立倫理原則。機器人的開發者必須遵守四個原則：為善、非罪惡、自主、正義，以及尊重基本權利、採用正當預防措施、包容性、負責任、確保機器人決策之可逆轉性、極大化利益及最小化傷害。研究者的倫理規則則包含獨立、適任性、透明、負責。
12. 立法模式：較為適當的立法方式應該是先建立一個較為柔軟的法律框架，以指導原則或公私協力的方式，來確保機器人工業、機器人設計者和政府機關以及其他利害關係人之間的合作關係。
13. 僱傭和社會事項：當人工智慧普及化，舊有產業可能不需要那麼多勞力，必須設計財務安全機制來確保人類身心靈健康，歐盟會員國的勞工法律與市場都必須要調整到能夠確保社會正義。

## 英國

1. 進階人工智慧所帶來的機會及風險，必須透過測試及實驗才能瞭解，應建立沙盒並在一個安全且受到控制的環境下，研究該等技術的潛能。
2. 儘管 AI 對於勞動市場之影響仍具有高度不確定性，政府仍必須促進新技能的發展、協助勞工獲得再訓練，無論係利用人工智慧更有效率地工作或移往特別需要人類技能

的領域。

3. 瞭解機器學習及逐漸增加的個人資料對個人自由及隱私、同意等概念可能帶來的影響為何。政府必須確保資料被儲存在正確的地方，並以適當的方式進行處理及控管。
4. 針對人工智慧所為的決策調適問責的概念及機制。
5. 確保 AI 系統可隨時檢核並具有合規性，能夠被一再地、安全地被人類監督者打斷，而非學習如何避免或操縱該等介入。
6. 確保演算法決策過程之透明度、可解釋性以及數據偏見的最小化。
7. 政府應當召集業界、非官方組織及最終消費者等利害關係人共同進行對話，一方面有助於建立起公眾的信任及接受度、解決可能的誤解，另一方面亦可透過公開對話即時處理相關社會、法律及倫理議題。
8. 在資料分享方面，資料倫理與创新中心應將開放銀行模式（Open Banking model）及其他資料可攜性（data portability）視為優先研究目標，於金融領域外建立安全的個人資料分享標準框架。此外，亦應針對各種不同的情境建立資料分享、控制與隱私之替代性工具和框架。
9. 政府在加強電腦教育之同時，不應刪減藝術與人文科目，而應將電腦科學與 AI 之社會面與倫理面加入課程內容。在社會及政治凝聚力的部分，
10. 英國許多機構尚未準備好利用 AI 技術，建議應於 2022 年前以統一格式將現存紀錄數位化。
11. 政府在制定 AI 政策時，應確保新舊政策間具有一致性，並應使公眾及產業自始即能理解相關公告與政策細節。為避免政策過於積極或新機構間互相重疊與衝突，政府 AI 辦公室應制定 AI 之國家政策框架，此外，政府亦需指明該框架與 AI 相關政策之權責單位。
12. 政府為 AI 設立新機構時，需明訂其功能與職責；此外，為確保公眾信心，政府亦需確認公眾對 AI 之使用產生不滿時清楚知道應向誰投訴。

#### 加拿大

1. 建議應建置全國會議，廣邀聯邦及地方政府之產業、衛生及教育官員及各領域之研究

者、企業家、投資人、醫療政策制訂者及專業人士，針對各項 AI 問題及計畫研究討論。

2. 應就機器人、人工智慧以及 3D 列印等技術應用於醫療系統的投資公開討論，且就不同議題組成專家工作小組。專家工作小組應包括下列議題：道德倫理、商業化、更新醫療照護提供方式、偏鄉的醫療照護提供、取用技術的公平性、勞動力調整、教育及訓練需求以及法規監管。各專家工作小組於考慮倫理、隱私及安全性問題後，個別制訂策略計畫以鼓勵及促進創新技術應用於醫療系統。
3. 由各專家工作小組的主席組成秘書處，秘書處功能包括：整合各專家工作小組的成果、蒐集各專家工作小組的報告、向聯邦政府報告專家工作小組的進度及提供全國會議及專家工作小組工作所需的額外協助。
4. 加拿大政府應對於專家工作小組以及秘書處提供足夠的資金。
5. 加拿大政府各相關部會及其首長，應依照其權力以及監管職能，參與相關之專家工作小組、向專家工作小組請求提供進度報告或意見、於需要時與地方部會討論。各相關研究機構亦應定期會面討論合作機制。
6. 人工智慧技術的應用仰賴大量病患資料，據此，應加強對於取得病患資料的許可、加密及去識別化以運用在人工智慧深度學習演算及各項應用領域上。
7. 就現階段而言，自動化創新對於工作機會的影響仍無法精確預期，尚須未來創新後持續討論。

## 法國

1. 建立以資料為重心之經濟政策：鼓勵企業共享數據資料、基於公共利益開放特定資料、支持個資可攜權、AI 之創新過程亦必須執行沙盒。
2. 提升法國在人工智慧領域之研究：創立跨學科之人工智慧研究機構、適當的分配各研究領域間之資源、藉由提高研究人員之薪資以及增強產業與學術之合作以吸引人才。
3. 規劃與控管人工智慧對於勞動力之影響：透過測試工具了解自動化後對於工作職務之影響，以支持工作型態之轉型；透過人工智慧與人類智慧之互補，減少勞動力在 AI 時代之衝擊，並透過正式教育以及終身學習制度，幫助畢業生以及員工發展其創意及技能；培訓員工以及人才。



4. 使用人工智慧創造生態環境：包括生態轉型、減少人工智慧對於能源使用之密度、減少能源消耗。
5. 人工智慧與倫理規範：使演算法透明化、訓練 AI 領域之工程師以及研究員倫理機制、展開公開辯論。
6. 確保人工智慧之多樣性與共融性：確保到 2020 年，參加數位工程課程的人中有 40% 是女性；建置一管理行政程序的自動化系統，幫助一般人可以更容易理解行政規則；政府應支持人工智慧之社會創新計劃。

#### 新加坡

1. 建立可解釋性與可驗證性 (verifiability)、良好數據問責實務 (good data accountability practices) 及透明化的 AI 治理框架。
2. 選擇適當的機構治理措施，包括內部治理、評估並減輕風險與危害、AI 使用與決策之定期性與臨時性審查、數據問責、可重複性評估、數據與決策可追蹤性、調整 AI 模型。
3. 建置顧客關係管理程序，包括針對 AI 揭露、說明、評鑑，以及提供退出選項、回饋管道以及決策審查。
4. 選擇決策與風險評估框架，依照決策自主性之不同，分為「人在迴路中」(human-in-the-loop)<sup>1</sup>、「人在迴路外」(human-out-of-the-loop)<sup>2</sup>以及「人在迴路上」(human-over-the-loop)<sup>3</sup>。

#### 日本

1. AI 開發促進活用，健全 AI 網路發展事項，包括制定 AI 開發指引、制定運用方針、利害關係人致力環境整備、確保 AI 系統或 AI 服務相互間順暢合作、確保競爭性生態系統、保護利用者利益、技術開發課題。
2. AI 網路資通資訊與資料事項，包括資安對策、隱私與個人資料保護。

<sup>1</sup> 意指人類依賴人工智慧系統提供之建議，由人類做出最終決策，例如作業系統提供員工多個符合其所處理案件之建議。

<sup>2</sup> 人工智慧系統完全獨立，做出自主性決策，無須人類控制，例如自主掃地機器人。

<sup>3</sup> 人類做出決策，但依賴人工智慧系統建議如何執行，例如人類決定導航系統之目的地，但由系統提供多個路徑建議。

3. AI 網路化造成社會與經濟影響事項，包括內容制度化課題、AI 網路化對社會與經濟影響情境分析、AI 網路化進展的影響評價指標及富足、幸福之評價指標設定、使用 AI 的社會接受度。
4. 人類處於 AI 網路化社會中課題事項，包括檢討人類與 AI 關係的認知、利害關係人間的態度、因應 AI 網路化教育/人才養成/勞動環境整備、AI 學習涵養及防止造成 AI 網路落差、安全網路整備及其他相關課題。

#### 印度

- a. AI 之研發，包括建立共同數據計算平台、射月計畫、完善化智慧財產權之規範、啟動 CERN for AI 計畫（與世界各國協力進行人工智慧之研究）。
- b. 勞動力之培訓：對於「已進入就業市場之勞工」，應創造新興產業之就業機會、核可與標準化非正式技職訓練機構、增加線上開放式學習平台、增加企業之提供訓練之經濟誘因；對於「仍在受教階段之學生」，於基礎教育階段，應提升技職教育的比重，尤其是強化 STEM 教育<sup>4</sup>，於高等教育階段應強化產學合作，於研究所教育階段，應鼓勵研究生投入國內機構進行研究，並且應建立跨領域之合作與教育機會。
- c. 加速人工智慧技術之運用，包括建立多元參與的市場及其運作平台、建置大型資料集、建立夥伴關係、提升 AI 技術在市場的曝光度、獎勵並協助新創事業。
- d. AI 與倫理、隱私及安全性，包括建立具有公平性與透明度的標準方針、制定適當的法律架構以保護數據及隱私權、建立適當的過失判定以及損害賠償責任。

自上表可知，目前對人工智慧之研發趨勢與重要爭議，主要集中於以下面向：

#### 一、加強與鼓勵 AI 研發

各國皆認為應對 AI 研究長期投資大量心力、時間與資金，並應跨領域合作，整合各方專家以及專業團體。同時由政府建置相關平台或組織，針對各項 AI 問題及計畫研究討論。同時政府應提供充足資源與誘因，培育以及吸引 AI 相關人才。

<sup>4</sup> 亦即 Science 科學、Technology 技術、Engineering 工程及 Mathematics 數學。

## 二、數據之建置、共享與保護

數據部分著重於數據之正確性、公平性與去歧視化，鼓勵企業與消費者團體設計出最佳的演算法系統、促進學術研究與產業對於演算法的外部稽核與測試系統、擴大電腦與資料科學的參與、支持減少演算法歧視的相關研究，同時應建立共同數據計算平台，鼓勵企業共享數據資料，以建立系統性的公平與問責，據此發展資料倫理框架。

## 三、AI 與倫理通則

AI 最為困難且有爭議的部分即為倫理規則，因社會規範與價值不易以程式呈現，且各個文化具有不同之社會規範與價值。是以加強倫理研究以及設計方法為目前重心，包括跨領域的教育與研究、企業應於各個環節強化倫理文化之實踐、開發/測試自主化智慧系統科技的研究倫理，以及加強可解釋性、可驗證性、公平性與透明性（包括建立獨立審查機構以監督產品符合倫理標準）。此外，必須在符合國際人道主義法的基礎上，制定關於自主武器的統一政府政策，包括審計追蹤（audit trail）、系統以可理解的方式向人類解釋其決策、應有可特定之人工操作員、自主系統的行為應可預測、應制定專業道德規範等。

## 四、AI 與隱私權保護

政府應盡力瞭解機器學習及逐漸增加的個人資料對個人自由及隱私可能帶來的影響為何，並且據此建置適當的隱私權保護機制，包括政府必須確保資料被儲存在正確的地方，並以適當的方式進行處理及控管，同時應適當的加強個人資料以及個人存取之管制，包括數位人格的控制、資料管理工具應具有透明性、資料擁有者的同意能力與平等（如消費者、受僱人、老人或心智障礙者之同意）等。此外，在醫療 AI 領域，因技術的應用仰賴大量與疾病、醫療、健康相關之資料，且絕大多數涉及個人資料，據此，應加強對於取得個資當事人的同意、加密及去識別化，以運用在人工智慧深度學習演算及各項應用領域上。

## 五、AI 對勞動力之衝擊

儘管目前普遍認為，AI 對於勞動市場之影響仍具有高度不確定性，仍有待後

續觀察，然而政府仍必須促進新技能的發展、透過人工智慧與人類智慧之互補以減少勞動力在 AI 時代之衝擊、協助勞工獲得再訓練、構思未來的職業訓練和學校教育。同時政府應提供足夠誘因，促使企業提供或分享相關教育資源。

### 第三章 人工智慧相關法律議題探討

#### 第一節 引論

人工智慧又稱為「機器智能」(Machine Intelligence)，通常是指「擁有人類智慧的機器」或「能夠自主思考的電腦」。然而，什麼樣的機器或電腦才能夠被稱為「擁有智慧」或「能夠自主思考」，卻不是一個能夠輕易回答的問題。

人工智慧一詞最早來自於1956年美國達特茅斯會議(Dartmouth workshop)，該會議由約翰·麥卡錫(John McCarthy)、馬文·閔斯基(Marvin Minsky)、克勞德·夏農(Claude Shannon)等人發起，首次將人工智慧的研究者集結起來，針對人工智慧相關問題進行了為期兩個月的討論，並於會後共同提出人工智慧的四大目標，亦即讓機器「懂得使用語言」、「解決只有人類可以處理的問題」、「擁有抽象化及概念化的能力」、「可以自我改良」<sup>5</sup>。

1994年12月13日，美國52名學者則在華爾街日報共同發表一篇名為〈主流科學界對智能的觀點〉(Mainstream Science on Intelligence)的文章<sup>6</sup>，指出智能是「一種極為通用的心智能力，例如進行推理、計畫、解決問題、抽象思考、理解複雜概念、快速學習及從經驗中學習的能力……其所反映的是一種更為寬廣及深層的、理解你我週遭事物的能力——『理解事物現象』、『捕捉語意』或『判斷』如何回應。」

儘管人們已經大致上測繪出人工智慧的理想樣貌，但截至目前為止，所有被看作是人工智慧的事例，還沒有一個能夠達成如此境界，與人類並駕齊驅、再現人類所有的智能行為。因此，人們開始將人工智慧區分為強AI(strong AI)及弱AI(weak AI)，與前者相近的概念為通用型人工智慧(Artificial General Intelligence，簡稱AGI)，亦即能夠執行所有人類所能執行的工作，與後者相近的概念則為特定AI(narrow AI或applied AI)，僅能夠再現人類智能的某些面向、處理特定的問題，有論者甚至認為Google搜尋引擎、全球定位系統(GPS)、電子遊戲皆可歸入弱AI的範疇<sup>7</sup>。

<sup>5</sup> John McCarthy et al. (1956). *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*. Retrieved from <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>.

<sup>6</sup> Richard D. Arvey et al. (1994, December 13). *Mainstream Science on Intelligence*. *The Wall Street Journal*. Retrieved from <http://www1.udel.edu/educ/gottfredson/reprints/1994WSJmainstream.pdf>

<sup>7</sup> John Frank Weaver (著)，鄭志峰(譯)(2018)，《機器人也是人：人工智能時代的法律》，頁4，臺北：元照。

雖然能夠「如人類般思考的電腦」尚未實現，但弱AI的快速發展，仍為人類社會帶來了重要的變化。弱AI——最好的例子就是蘋果的Siri——與過往自動化機器的不同點在於它們的自然情境式設定，人類與機器不再是在預設情境下進行互動（例如透過指令進行語音搜尋），你我開始用對待生活中其他人類一樣的態度去對待弱AI，而這意味著它們參與人類生活的方式，亦將與既有的自動化機器截然不同。由此產生了人工智慧能否具備社會交往能力、乃至於成為社會一份子的問題<sup>8</sup>。

然而，人工智慧能否具備理性或良知等議題，目前仍離我們太過遙遠，當下人工智慧作為法律主體的討論，主要仍圍繞在侵權責任的歸屬與分配，其原因便在於AI已經能夠作成事實行為、造成事實上的損害，但在可預見的將來中，AI尚無作成法律行為的需要，因而討論人工智慧能否成為法律主體，實際上並無太多實益，甚至可以說，人工智慧目前在法律上帶來的問題，並不在於AI本身的法律地位，反而在於人與人之間權利與責任的重新分配。

有鑒於人工智慧的指涉範圍難以界定，本報告將嘗試以「建構論的角度」切入<sup>9</sup>，從AI實際應用情境出發，逐一探討「AI對於著作權法制之適用疑義」、「AI時代下的個資保護與合理利用」、「智慧載具發展及侵權責任歸屬」、「AI及大數據於公權力行政之運用」、「AI與金融監理沙盒之應用」、「AI運用於醫療服務之相關法律疑義」等六大議題，關注AI發展過程中可能遭遇的問題，避免對人工智慧預作定義。

---

<sup>8</sup> 同前註，頁 8-9。

<sup>9</sup> 松尾豐(著)，江裕真(譯)(2016)，《了解人工智慧的第一本書：機器人和人工智慧能否取代人類？》，頁 53，臺北：經濟新潮社。

## 第二節 人工智慧對於著作權法制之適用疑義

### 第一項 焦點議題

隨著技術不斷發展，人工智慧已具有創作文學、音樂作品之能力，且無論就創作物外觀、內容，均與人類所為之創作已具有相當之類似性。於此種情形下，是否應肯認人工智慧創作物具有「可著作權性」，而應受著作權法之保護？關於此點，可資討論者，例如<sup>10</sup>：著作權法制原則上以「人」（包括自然人或法人）作為權利主體，而人工智慧非屬自然人或法人，是否、或在何種情形下亦可認定為「著作人」？人工智慧所創作之作品，是否具有「原創性」而可取得著作權保護？此等問題，實亦與「著作人應如何認定」（或著作權之權利歸屬應如何認定）的問題息息相關。事實上，世界各國就人工智慧之創作對著作權法制之影響所為之討論，亦有多篇幅集中於「著作人」之認定。換言之，因著作權之保護客體為「著作人」所為之創作，故人工智慧創作之作品是否有著作人存在及著作人為何，即為關鍵之問題。如認為人工智慧創作之作品根本沒有著作人存在，則沒有任何主體取得著作權，自然沒有上述之其他議題發生；反之，如認為著作人是該人工智慧的程式開發者、使用人或甚至是人工智慧本身，則由該程式開發者、使用人或甚至是人工智慧本身取得著作權。

其次，無論由何人取得著作權，都會有權利存續期間、作品保護範圍及侵權責任等問題，例如：因人工智慧並無所謂「死亡」的問題，且擁有能快速創作大量作品之能力，因此有關人工智慧創作物之權利存續期間，是否應延長或縮短？又人工智慧創作物之保護範圍，是否應加以限制，以避免人類的創作範圍遭到壓縮？蓋基於人工智慧擁有能快速創作大量作品之能力，如肯認人工智慧創作物之著作權保障，市場中有著作權之作品的供給量將大幅上升，在市場總需求保持固定的前提下，人類創作之速度無法與人工智慧匹敵，如給予人工智慧創作物過度的保護，人類作者在著作權市場的定價能力將受到削弱。未來縱使人類作者未因此完全退出市場，但仍可能因此承受相當大的競爭壓力<sup>11</sup>。因此，是否應對人工智慧創作之作品保護範圍加以限制？最後，如人工智慧之創作侵害他人著作權、或遭他人侵害著作權時，關

<sup>10</sup> 陳昭好（2017），〈論人工智慧創作與發明之法律保護：以著作權與專利權權利主體為中心〉，頁 59，國立政治大學科技管理與智慧財產研究所碩士論文。

<sup>11</sup> 曹源（2016），〈人工智能創作物獲得版權保護的合理性〉，《科技與法律》，2016 年 3 期，頁 503。

於侵權責任之認定，是否應予以調整？例如，是否應限定侵害行為之態樣？舉證責任之分配是否應調整？具體的救濟方法（損害賠償？除去侵害？防止侵害）是否亦有更動之必要？

本報告以下將針對上述議題，就各國法制之發展進行介紹與討論。

## 第二項 外國文獻分析

### 一、可著作權性及權利歸屬

#### (一)美國

美國著作權法第201條規定：「依本法受保護著作之著作權，歸屬於該著作之著作人<sup>12</sup>」，可見著作人是美國著作權法下之權利主體，然而，著作權法未對「著作人」有明確定義。學者認為從著作權法中其他條文使用「著作人」的方式可以推知立法者認為著作人應是「人類」。而著作權局所發行的第三版實務概要中，第306條<sup>13</sup>明文表示僅提供人類作者之創作作品著作權保護以及著作權登記，因為著作權法限制於「著作人的原創智慧概念」，所以非人類創作之作品申請登記將予以否准。而在第313.2條<sup>14</sup>「欠缺人類作者之作品」規定中，也表示「著作權局不登記欠缺任何由人類作者所為之創作性投入或干預，而僅由機器或純粹隨機地或自動化運行的機械過程所製作的作品」，因此，只要不是由純粹的機械過程，自動地、隨機地產生的製品，而是有「人類作者創作性投入或干預」，即為著作權保護客體<sup>15</sup>。換言之，如果人工智慧所為的創作要獲得著作權保護，在現行實務下，必須要該作品能直接追溯到人類作者（即能明確辨認該著作人所投入之創

---

<sup>12</sup> 17 U.S.C. §201(a): “Initial Ownership. – Copyright in a work protected under this title vests initially in the author or authors of the work. The authors of a joint work are coowners of copyright in the work.”

<sup>13</sup> The Article 306 of the Compendium of US Copyright Office Practices: “The U.S. Copyright Office will register an original work of authorship, provided that the work was created by a human being. The copyright law only protects “the fruits of intellectual labor” that “are founded in the creative powers of the mind.” Trade-Mark Cases, 100 U.S. 82, 94 (1879). Because copyright law is limited to “original intellectual conceptions of the author,” the Office will refuse to register a claim if it determines that a human being did not create the work. *Burrow-Giles Lithographic Co. v. Saronny*, 111 U.S. 53, 58 (1884). For representative examples of works that do not satisfy this requirement see Section 313.2 below.”

<sup>14</sup> The Article 313.2 of the Compendium of US Copyright Office Practices: “The Office will not register works produced by nature, animals, or plants. Likewise, the Office cannot register a work purportedly created by divine or supernatural beings, although the Office may register a work where the application or the deposit copy(ies) state that the work was inspired by a divine spirit.”

<sup>15</sup> 陳昭好，同前註，頁 56、65。



意)，才不會落入公領域之範疇而可被任何人使用<sup>16</sup>。故如人工智慧所為的創作不能直接追溯到人類作者時，依第三版實務概要，即不能受著作權之保護。既然沒有著作權發生，後續之問題亦無討論之必要。

有鑑於電腦技術不斷地進步，美國國會於1974年成立應用新科技之著作權作品國家委員會（National Commission on New Technological Uses of Copyrighted Works, CONTU）負責研究新科技在著作權法產生的相關議題，其中包含利用電腦創作之作品引發的問題在內<sup>17</sup>。CONTU在1978年提出的報告否定電腦可以獨立創作的可能性，且認為電腦獨立創作之作品如缺乏人類作者的參與時將不具有可著作權性；如有人類參與電腦所製作的作品時，應認為使用電腦的人為該作品之作者<sup>18</sup>。最後，CONTU認為沒有必要因為利用電腦來產生作品而修改著作權法<sup>19</sup>。

惟美國國會技術評估辦公室（Congressional Office of Technology Assessment, OTA）於1986年發布的報告則否定CONTU的看法，認為電腦並非只是無生命的工具，而應為作品的共同作者<sup>20</sup>。不過，該報告就何人可為共同作者？程式設計師？使用者？或是兩者都是？還有其他衍生問題，均沒有更進一步的處理<sup>21</sup>。

又雖然CONTU早在1974年對電腦產生的著作進行討論，OTA亦在1986年即提出研究報告。但美國著作權法自OTA報告提出之後，直到現在，卻都沒有相應的修正。且依據前述分析，著作權登記實務上並不承認人工智慧創作物的地位，因此在現行法的解釋下，人工智慧創作物並不受著作權保護。

---

<sup>16</sup> Kalin, Hristov (2017). Artificial Intelligence and the Copyright Dilemma. *IDEA: The IP Law Review*, 57(3), 437.

<sup>17</sup> Annemarie Bridy (2012). Coding Creativity: Copyright and the Artificially Intelligent Author. *Stanford Technology Law Review*, Vol. 5, 54.

<sup>18</sup> 陳昭好，同前註，頁 76。

<sup>19</sup> Annemarie Bridy (2012). Coding Creativity: Copyright and the Artificially Intelligent Author. *Stanford Technology Law Review*, Vol. 5, 55.

<sup>20</sup> Ryan Abbott (2016). I think, Therefore I Invent: Creative Computers and the Future of Patent Law. *Boston College Law Review*, Vol. 57, 1102.

<sup>21</sup> Annemarie Bridy (2012). Coding Creativity: Copyright and the Artificially Intelligent Author. *Stanford Technology Law Review*, Vol. 5, 57.

不過，隨著時代的進步，當今的人工智慧和多年前的人工智慧，已有相當顯著的差異。故在立法論上是否應給予人工智慧創作物著作權之保護，即有討論的必要，如認為應提供著作權保護，還要進一步討論由何人取得著作權。

有學說認為，既然作品從形式上來看是由人工智慧所創作，則最直觀的想法就是由人工智慧取得著作權。但是在現行法制之下，人工智慧並非權利主體，無法享有著作權。對此，有學者認為，既然只有實際從事創作的作者能享有著作權的保障，那麼著作權人應該重新定義，除了人類作者外，亦應包括非人類作者在內。這種允許非人類成為作者的處理方式將會刺激新穎且具有價值的創作產生<sup>22</sup>。此外，將人工智慧創作物歸屬給人工智慧本身將符合法院向來的作法，即將著作權歸屬給作品背後實際的創作來源<sup>23</sup>。

然而，雖然此種看法看似可以解決人工智慧所為創作的著作權歸屬問題，卻相當具有爭議性，因為人工智慧並非自然人，其無法於法庭成為原告或被告，無法負擔法律上之責任，也無法就著作權進行移轉或授權。如採用此種方法將顛覆原有的法律制度，創造出更多有待處理的衍生問題<sup>24</sup>。而從著作權的本質來看，著作權之保護係提供著作人專有且排他之權利，即透過給予著作人經濟誘因，而促使人類進行創作，此即美國法所採取之「鼓勵論」，但人工智慧並不會因為其可以獲得著作權而更願意進行創作，故不符合著作權法的鼓勵論<sup>25</sup>。自以上分析可以發現，假使立法論上認為人工智慧所為創作應提供著作權保護，但也不應賦予人工智慧本身著作權，原因在於除了對原有的法律制度而言變動過大外，此種作法亦不符合著作權法的原理。

---

<sup>22</sup> Ryan Abbott (2016). I think, Therefore I Invent: Creative Computers and the Future of Patent Law. *Boston College Law Review*, Vol. 57, 1079.

<sup>23</sup> Robert Yu (2017). The Machine Author: What Level of Copyright Protection Is Appropriate for Fully Independent Computer-Generated Works? *University of Pennsylvania Law Review*, Vol. 165, 1257-1258.

<sup>24</sup> Kalin, Hristov (2017). Artificial Intelligence and the Copyright Dilemma. *IDEA: The IP Law Review*, 57(3), 441.

<sup>25</sup> Darlin Glasser (2001). Copyrights in Computer-Generated Works: if Anyone, Do We Reward. *Duke L. & Tech. Review*, 33.

第二種看法是給予人工智慧的開發者著作權。因為從某一特定人工智慧的構想開始到建構該人工智慧的細部計畫，再到寫出必要的程式碼(coding)，甚至最後將程式碼除錯(debug)，整個程序都是由人工智慧的開發者貢獻其創意才能完成，如果沒有開發者的貢獻，則人工智慧根本無法產生出任何創作<sup>26</sup>。此外，如果利用著作權法下的衍生作品原則(derivative work doctrine)<sup>27</sup>，將人工智慧創作物解釋成基於人工智慧此一電腦程式或自該電腦程式改編而來，似乎可以認為該創作係該電腦程式的衍生作品<sup>28</sup>。因此，應由人工智慧的開發者取得人工智慧所為創作的著作權。

就人工智慧本身需要開發者投入大量努力及其聰明才智才能完成人工智慧創作的觀點來看，由開發者取得人工智慧所為創作的著作權相當具有說服力，而且相較於人工智慧的使用者對該作品的貢獻可能只有點下「產生作品」的按鈕而言，人工智慧的開發者毋寧是產生該人工智慧的主要貢獻者。惟自從最高法院在Feist案中明白的否定「辛勤原則」(sweat of the brow)<sup>29</sup>後，開發者的投入已經不能作為獲得著作權保護的有力理由<sup>30</sup>。

至於「衍生作品原則」的說法，實務見解向來認為一部作品必須包含現存

---

<sup>26</sup> Robert Yu (2017). The Machine Author: What Level of Copyright Protection Is Appropriate for Fully Independent Computer-Generated Works? *University of Pennsylvania Law Review*, Vol. 165, 1258.

<sup>27</sup> 17 U.S.C. §101: A “derivative work” is a work based upon one or more preexisting works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may be recast, transformed, or adapted. A work consisting of editorial revisions, annotations, elaborations, or other modifications which, as a whole, represent an original work of authorship, is a “derivative work”.

<sup>28</sup> Darlin Glasser (2001). Copyrights in Computer-Generated Works: if Anyone, Do We Reward. *Duke L. & Tech. Review*, 11.

<sup>29</sup> Feist Publications, Inc. v. Rural Telephone Service Co, Inc., 499 U.S.340 (1991)。本件原告 Rural Telephone Service Co., Inc. 為在美國堪薩斯 (Kansas) 州從事電信服務之業者電話服務的業者。依該州規定，電信業者必須於每個年度提供電話號碼簿給該公司之所有用戶。原告乃分別出版了黃頁、白頁電話號碼簿，提供予該公司用戶。其中，白頁電話號碼簿係所有用戶的姓名、所在城市以及電話號碼依姓氏的英文字母順序予以排列。

本案被告 Feist Publications, Inc. 則為專門從事地區性電話號碼簿出版之業者，該公司出版之電話號碼簿涵蓋多個不同的電信服務轄區，被告必須與個別電信業者訂立授權契約，以取得並使用各業者用戶之資料。但原告為了避免被告的競爭，拒絕與被告簽訂授權契約。被告乃參酌原告之白頁電話號碼簿並加以編輯後，另行出版電話號碼簿。原告乃對提起侵害白頁電話號碼簿著作權之訴訟。聯邦地方法院、聯邦巡迴上訴法院均認為電話號碼簿易受著作權保障，肯認被告之行為已構成侵權行為。惟聯邦最高法院認為創作物必須具備原創性，創作人必須至少具備最低限度的創作。下級法院所採「辛勤原則」(sweat of the brow) 的觀點，認為著作權乃是對於辛勤、努力地將事實、資料加以彙集者所給予的鼓勵。惟若如此，一旦資料編輯者將資料編入其所編輯的資料庫即可取得著作權，將產生他人無法再使用同一資料、將同一資料入其他資料庫之後果。因此，聯邦最高法院不採「辛勤原則」的見解，認為被告並不構成侵權行為。

<sup>30</sup> 同前註，頁 12-13。

作品的一部分內容，始能認定為衍生作品。而人工智慧創作物除了沒有在其內容中實際納入任何該人工智慧的內容(即程式碼)外，其內容與人工智慧本身又幾乎沒有相似之處，故可能不符合司法實務的判斷標準。此外，在衍生作品的著作權人認定上，如果一部衍生作品並未侵權且含有新的創意內容在內時，該新內容部分之著作權將歸屬給該新內容的作者而非原作品的作者。就此而言，因為人工智慧的創作並未納入任何該人工智慧本身的內容在內，而是由該人工智慧蒐集並處理新的資料產生創作，既然該作品並未包含人工智慧開發者的創作在內，人工智慧開發者自然沒有主張其為該作品所有權人的可能，所以該作品僅能由該人工智慧享有全部的著作權<sup>31</sup>。而如前所述，給予人工智慧本身著作權並不妥適，顯然衍生作品原則並不是解決問題的好辦法。

另外，對於最終作品的產生，人工智慧的開發者僅是創造了創作的可能，並非創作了該作品，否則比爾蓋茲豈不是可以對所有自微軟產品產生的創作主張著作權<sup>32</sup>？最後，亦有批評者認為人工智慧的開發者已經藉由出售、出租、授權該人工智慧獲得回報，不應再取得人工智慧所為創作的著作權，否則會有過度評價（over-reward）的問題<sup>33</sup>。

第三種看法是由人工智慧的使用者取得著作權，其立論基礎在於使用者是決定產生作品之人，也就是說若不是使用者點下「產生作品」的按鈕，作品也不會產生，所以使用者是最直接「產生」作品之人，再加上賦予使用者著作權能鼓勵使用者多進行創作，對公眾也有利<sup>34</sup>。

惟如果使用者對作品的貢獻只有點下「產生作品」的按鈕，其貢獻可能無法滿足著作權法所要求的「最低程度的創意」的要件，因而無法取得著作

---

<sup>31</sup> Annemarie Bridy (2012). Coding Creativity: Copyright and the Artificially Intelligent Author. *Stanford Technology Law Review*, Vol. 5, 64-65.

<sup>32</sup> Darlin Glasser (2001). Copyrights in Computer-Generated Works: if Anyone, Do We Reward. *Duke L. & Tech. Review*, 15.

<sup>33</sup> Robert Yu (2017). The Machine Author: What Level of Copyright Protection Is Appropriate for Fully Independent Computer-Generated Works? *University of Pennsylvania Law Review*, Vol. 165, 1261. See also Darlin Glasser (2001). Copyrights in Computer-Generated Works: if Anyone, Do We Reward. *Duke L. & Tech. Review*, 16.

<sup>34</sup> Robert Yu (2017). The Machine Author: What Level of Copyright Protection Is Appropriate for Fully Independent Computer-Generated Works? *University of Pennsylvania Law Review*, Vol. 165, 1261.

權<sup>35</sup>。相反地，如果使用者至少有進行小部分的修改（tinkering），例如於點下「產生作品」的按鈕前已先進行若干設定，此時似可認為已具備「最低程度的創意」，而可獲得著作權的保障<sup>36</sup>。

對於使用者沒有投入相當的貢獻卻可以享有著作權乙節，尚可以「雇用作品原則」（made for hire doctrine）<sup>37</sup>來解決，亦即使用者雇用了人工智慧進行創作，所以其為法律上作者，人工智慧為事實上作者。但是，因為人工智慧與使用者並無雇用關係，顯然此原則的適用，即有困難。

第四種看法是由開發者與使用者共同享有著作權。人工智慧的創作，可以說由開發者種下創作的種子，再由使用者澆水並在最後收穫作品，既然開發者與使用者對於人工智慧所為的創作都有所貢獻，即應由兩者共同取得著作權<sup>38</sup>。

但是，在現行法下，共同著作必須要具備下列兩個要件始屬之：第一是開發者與使用者的貢獻各自來看都需要具備可著作權性，第二是開發者與使用者於創作時都有意圖將各自的貢獻結合成一個不可分割且單一的作品，簡單來說，就是雙方對於該作品的產生有合作存在。於人工智慧所為的創作，開發者的貢獻一般被認為是寫出人工智慧本身，但就此點而言，由於開發者就人工智慧本身已經可以取得著作權，則如前所述將有過度評價的問題，開發者是否有貢獻就已經存有疑問；即使認為開發者貢獻了人工智慧本身，使用者還是會有只貢獻了按下按鈕一事而沒有達到創作性的問題，所以就第一個要件而言，使用者很可能就不符合。而就第二個要件來說，開發者與使用者顯然沒有合作關係存在，因為開發者在完成該人工智慧時，根本無法預想到將來的使用者是誰，又怎麼可能有合作關係<sup>39</sup>。又或是說開發者一旦出售、出租或授權該人工智慧後，對於產出的作品利害關係即大幅降低，亦即當開發者藉由出售、出租或授權人工智慧取得對價後，即

---

<sup>35</sup> 同前註，頁 1262。

<sup>36</sup> Darlin Glasser (2001). Copyrights in Computer-Generated Works: if Anyone, Do We Reward. *Duke L. & Tech. Review*, 22-23.

<sup>37</sup> 同前註，頁 22-24。有關雇用作品原則詳細介紹，詳後述。

<sup>38</sup> 同前註，頁 26。

<sup>39</sup> Robert Yu (2017). The Machine Author: What Level of Copyright Protection Is Appropriate for Fully Independent Computer-Generated Works? *University of Pennsylvania Law Review*, Vol. 165, 1259-1260.

會有效地阻斷其對於該人工智慧產生的作品繼續享有利益<sup>40</sup>。由上述分析可知，由開發者及使用者共同取得著作權亦非良方。

最後一種看法是，沒有人取得著作權。最直觀的理由是，既然沒有一個權利主體適於取得人工智慧所為創作的著作權，不如維持現行法，完全不給予人工智慧創作物著作權保護。亦有學者認為自鼓勵論來看，開發者已經透過獲得人工智慧本身的著作權受到鼓勵，如再賦予人工智慧創作物的著作權予開發者，對其繼續開發人工智慧僅能創造少量的誘因。且可能使開發者獲得所有該人工智慧所為創作的著作權，形成獨占地位，對公眾反而不利。至於賦予使用者著作權的見解，似乎可以促使使用者產生更多作品，學說以能自動產生新聞的人工智慧為例，認為在數位時代中，利用人工智慧產生新聞的誘因是最先在市場曝光（first-to-market），因為新的資訊越早能公諸於眾，越能獲得點擊率，而著作權的保護需要向著作權局登記，如為了獲得著作權保護，可能就喪失取得先機的機會，所以提供著作權給人工智慧的使用者實質上並不會增加創作的誘因<sup>41</sup>。

不過，論者亦有認為，若人工智慧創作物不能受到著作權的保護，將使大部分人工智慧創作物落入任何人都可以自由使用公領域當中，將會減少人工智慧開發者開發人工智慧之誘因，對人工智慧及其相關領域之發展顯然不利<sup>42</sup>。

另有學說參考英國法制，建議透過對「雇用作品原則」進行修正，即可在不大幅變動現行著作權法制的情況下，對人工智慧創作物提供保護。現行著作權法下之「雇用作品原則」，有兩種適用態樣：其一為僱傭關係下之作品創作，即該作品為實際創作者於僱傭關係下所為之職務創作<sup>43</sup>。其二為出資聘人創作，即出資人聘用實際創作人為其創作，而雙方特別於書面

---

<sup>40</sup> Darlin Glasser (2001). Copyrights in Computer-Generated Works: if Anyone, Do We Reward. *Duke L. & Tech. Review*, 27.

<sup>41</sup> Robert Yu (2017). The Machine Author: What Level of Copyright Protection Is Appropriate for Fully Independent Computer-Generated Works? *University of Pennsylvania Law Review*, Vol. 165, 1264-1265.

<sup>42</sup> Kalin, Hristov (2017). Artificial Intelligence and the Copyright Dilemma. *IDEA: The IP Law Review*, 57(3), 438.

<sup>43</sup> 17 U.S.C. §101: A “work made for hire” is – (1) a work prepared by an employee within the scope of his or her employment;

表明由出資人取得著作權之情形<sup>44</sup>。於此二態樣中，著作權都歸屬於未實際進行創作之人。如認為實際進行創作之人（author-in-fact）為人工智慧，而人工智慧之開發者、擁有者或是使用者為雇用人或出資者，透過「雇用作品原則」，將由開發者、擁有者或是使用者取得著作權，即可避免由非屬人類的人工智慧取得著作權所引發的問題<sup>45</sup>。

不過，司法實務見解要求「雇用作品原則」須具備「員工於職務範圍內或被特別指揮或委任進行創作」的要件。而人工智慧在解釋上，難以被認為是「於職務範圍內進行創作之員工」，因此，在適用上也有疑義<sup>46</sup>。因此有論者認為於解釋著作權法之「雇用作品原則」下之雇主及員工時，應採取不同於代理法則的嚴格定義，而用較廣義的方式來理解此二概念，凡是為了達成特定目的或完成特定工作而雇用、使用其他個體之服務，即可認為是「雇主」。也就是說，雖然人工智慧並非員工，亦無所謂職務範圍，但其實際上被自然人使用以創造新的創作，人工智慧之創作服務被自然人使用，自然人相對於人工智慧，應認為是雇主，而可以取得人工智慧所為創作之著作權<sup>47</sup>。亦有論者認為應修改美國著作權法第101條，直接在法律規定「雇用作品原則應適用在沒有人類作者介入的情況下而由電腦獨自創作之作品」<sup>48</sup>，則此時人工智慧創作物可以直接適用雇用作品原則而由自然人取得著作權。

也有學者認為決定著作權歸屬時，需考量歸屬於人工智慧之開發者、擁有者或是使用者何者對社會最有利。具體而言，首先，需先釐清賦予人工智慧所為創作之著作權予自然人之目的何在，然後，評估何人對此一目的之

---

<sup>44</sup> 17 U.S.C. §101: A “work made for hire” is – (2) a work specially ordered or commissioned for use as a contribution to a collective work, as a part of a motion picture or other audiovisual work, as a translation, as a supplementary work, as a compilation, as an instructional text, as a test, as answer material for a test, or as an atlas, if the parties expressly agree in a written instrument signed by them that the work shall be considered a work made for hire...

<sup>45</sup> Kalin, Hristov (2017). Artificial Intelligence and the Copyright Dilemma. *IDEA: The IP Law Review*, 57(3), 442-443。

<sup>46</sup> Darlin Glasser (2001). Copyrights in Computer-Generated Works: if Anyone, Do We Reward. *Duke L. & Tech. Review*, 24.

<sup>47</sup> Kalin, Hristov (2017). Artificial Intelligence and the Copyright Dilemma. *IDEA: The IP Law Review*, 57(3), 445-447.

<sup>48</sup> Annemarie Bridy (2012). Coding Creativity: Copyright and the Artificially Intelligent Author. *Stanford Technology Law Review*, Vol. 5, 68. 原文為：A work made for hire is ... (3) a work generated by a computer in circumstances such that there is no human author of the work.

達成最有貢獻。最後，即由對於達成目的最有貢獻之人取得著作權<sup>49</sup>。

此一學說認為提供經濟誘因以鼓勵人工智慧產業發展並促進人工智慧所為創作之傳播，可以說是賦予人類作者著作權之最終目的。而經濟誘因應保留給對人工智慧之發展及傳播最有貢獻之人，即人工智慧之開發者和於背後提供資金之公司，假如缺少此二人之貢獻，人工智慧裝置根本不會出現，更不可能供大眾使用。反過來說，人工智慧之使用者對於人工智慧最初之開發貢獻最少，如將著作權歸屬於使用者而非開發者，將對人工智慧的發展有害。因為人工智慧之開發者或擁有者將會為了避免於與使用者間進行之著作權訴訟中敗訴而限制第三人使用人工智慧。而此等保護措施將限制人工智慧之應用及減損與其相關之利益，亦減緩人工智慧產業之發展及減少人工智慧所為創作之數量<sup>50</sup>。

因此，將著作權歸屬於人工智慧之開發者或是擁有者是比較合理的解套方法，如開發者或擁有者欲將著作權移轉給使用者，可以利用最終使用者授權合約（End User Licensing Agreement）來處理。長期而言，授權對於部分公司而言應屬財務上較可行之辦法，同時，使人工智慧創作物商業化亦屬對社會整體較佳之方式<sup>51</sup>。

## （二）歐盟

歐盟之著作權相關法令，原則上係接受伯恩公約之規範精神，以「原創作品」作為著作權保護之要件。惟此一「原創性」要件，於歐盟指令或指導方針中，並沒有一般性的定義<sup>52</sup>。僅Software Directive 91/250/EEC<sup>53</sup>、Database Directive 96/9/EC<sup>54</sup>及Term Directive 2006/116/EC<sup>55</sup>中，有「作品必

---

<sup>49</sup> Kalin, Hristov (2017). Artificial Intelligence and the Copyright Dilemma. *IDEA: The IP Law Review*, 57(3), 443.

<sup>50</sup> 同前註，頁 444-445。

<sup>51</sup> 同前註，頁 445。

<sup>52</sup> Tuomas Sorjamaa (2016). *I, Author: Authorship and Copyright in the Age of Artificial Intelligence*, Department of Accounting and Commercial Law, Hanken School of Economics, Helsinki, 19.

<sup>53</sup> Article 1 (3) of the Software Directive 91/250/EEC: A computer program shall be protected if it is original in the sense that it is the author's own intellectual creation. No other criteria shall be applied to determine its eligibility for protection.

<sup>54</sup> Article 3 (1) of the Database Directive 96/9/EC: In accordance with this Directive, databases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation shall be protected as such by copyright. No other criteria shall be applied to determine their eligibility for that protection.



須具有原創性，亦即作品需屬於著作人個人的精神創作始能獲得著作權之保護」之規範。<sup>56</sup>。

至於司法實務上，歐洲法院（Court of Justice of the European Union）曾於 Infopaq、Painer、Murphy 等案例中，就「原創性」要件提出闡釋。整理歐洲法院於上述各案例所表示之見解可知，：歐洲法院贊同以「著作人個人的精神創作」作為判斷是否具「原創性」的標準，著作人除必須作出自由而富有創意的選擇，並表達其個人風格外，於創作過程中，尚必須要留下創作自由的空間<sup>57</sup>。

現行歐盟著作權相關法令並沒有考慮到人工智慧創作物，故未規範人工智慧創作物是否具有可著作權性，更未規範權利歸屬之問題。惟上述歐盟法令的不足並不代表所有與人工智慧有關之作品一概不受著作權保護，仍需區分情形而定。各種著作是否具有可著作權性，關鍵仍在是否具有原創性。

第一種情況是作品由人工智慧與人類共同完成。於此種情況中，無論是人類作者將人工智慧當作工具進行創作，或是人工智慧在創作過程中扮演主要角色，只要人類有在創作過程中作出最低程度之貢獻，人類作者仍可以取得著作權<sup>58</sup>。

第二種情況是作品先由人工智慧創作後，再由人類進行篩選。於此類作品，人類作者的貢獻在於從眾多作品中挑選出少數具有價值而值得傳播的部分，此種篩選既然需要運用腦力，雖然歐洲法院未就此種情形作過判決，仍應可認為符合 Term Directive 2006/116/EC 所要求的「反映著作人之個性」，

---

<sup>55</sup> Article 6 of the Term Directive 2006/116/EC: Photographs which are original in the sense that they are the author's own intellectual creation shall be protected in accordance with Article 1. No other criteria shall be applied to determine their eligibility for protection. Member States may provide for the protection of other photographs.

<sup>56</sup> HM Bøhler (2017). *EU copyright protection of works created by artificial intelligence systems*, JUS399 Master's thesis Faculty of Law of University of Law, 14.

<sup>57</sup> Tuomas Sorjamaa (2016). *I, Author: Authorship and Copyright in the Age of Artificial Intelligence*, Department of Accounting and Commercial Law, Hanken School of Economics, Helsinki, 19-20. See also HM Bøhler (2017). *EU copyright protection of works created by artificial intelligence systems*, JUS399 Master's thesis Faculty of Law of University of Law, 16-17.

<sup>58</sup> HM Bøhler (2017). *EU copyright protection of works created by artificial intelligence systems*, JUS399 Master's thesis Faculty of Law of University of Law, 18.

而應受著作權之保護<sup>59</sup>。

第三種情況是人工智慧以暴力演算法 (brute force) 所為之創作。此種情況係人工智慧以其強大的演算能力，將所有可能都羅列出來，此種暴力演算法創作不涉及選擇，即不符合歐洲法院要求的「著作人需作出自由而富有創意的選擇」，因此不能達到歐盟著作權法之原創性要求，自然無法取得所有權<sup>60</sup>。

以上三種情形，都可以用現行法解釋、處理。惟第四種情形，即人工智慧不但自行創作，甚至自行篩選作品，不須人類從眾多作品中篩選出具有藝術性、有價值的作品則引發問題。換言之，人類在整個創作過程中，並沒有貢獻其藝術觀點，亦未展現其個性，此時現行法無法處理此種作品是否具有可著作權性等問題。有論者可能會主張如人工智慧創作物與人類作者所為之創作無法區別時，應獲得同等之保護。然而，根據歐洲法院「著作人需作出自由而富有創意的選擇」之見解，可知是否具有原創性之決定性因素不在成品之特性而在於創作出成品之過程，也就是說創作過程是否具有創意？著作人是否有在創作過程中表現其創意？此外，著作人還需要在創作過程中展現其創作之意志。因此，即使人工智慧能自行作出選擇，但由於人工智慧沒有意志，該選擇之過程當然非本於人工智慧之意志，則似乎不符合原創性之要求<sup>61</sup>。

另外，歐洲著作權法之架構係以「著作人」此一概念為中心，而相關法令，如權利保護期間之規定，均以著作人死亡為要件。也就是說法令的基本假設即是著作人的生命是有限的。則如此一來，既然人工智慧能永續存在，即不符合基本假設，則人工智慧似乎不能被認為是著作人<sup>62</sup>。

然而，隨著人工智慧技術之發展，由人工智慧單獨創作並挑選的作品將會越來越多，而如果該等作品在現行法下不能受到保護而落入公領域中，勢必會影響開發者的開發意願。而歐盟下的各國為發展人工智慧產業可能會

---

<sup>59</sup> 同前註，頁 19。

<sup>60</sup> 同前註，頁 20。

<sup>61</sup> 同前註，頁 21-22。

<sup>62</sup> 同前註，頁 22。

在內國法中作必要之修正，在此同時，如歐盟沒有相關的統一指令，會造成各國法令適用上的不一致，對於歐盟向來提倡的貨物及服務之自由移動將造成阻礙<sup>63</sup>。有鑑於此，歐盟議會於2017年要求法律委員會研擬可適用於各國、符合科技且較為中立的相關方案。

就人工智慧所為創作之著作權歸屬可能有以下幾種可能。第一種可能是不賦予著作權，即該作品完成後就落入公領域<sup>64</sup>。此種看法雖符合歐盟現行法之相關規範，然而如前所述，不提供保護會降低各界對人工智慧開發所為之投入，對人工智慧產業的發展不利。而開發者或使用者於人工智慧創作出作品後，亦會因為不能獲得著作權保護，而不願將該作品公諸於世，此種作法不能促進科學或藝術等之進步與傳播，實不符合著作權法相關立法目的<sup>65</sup>。

而第二種可能則是將著作權歸屬於人工智慧本身<sup>66</sup>。此種看法馬上會遇到現行法無法將人工智慧所為創作之著作權賦予人工智慧本身的問題，因為人工智慧並無法律上的人格，當然無法擁有權利<sup>67</sup>。不過，歐洲議會於2017年提案建議至少賦予較先進的自動機器人「電子人」的地位<sup>68</sup>，解決其所涉及的侵權責任問題，甚至在自動機器人能夠自行作出決定或獨自與第三人進行互動時賦予其「電子人格」。雖然上述做法似乎能解決人工智慧法律上人格的障礙，但是智慧財產權制度目的在於賦予創作人排他性的權利來誘使創作，而人工智慧並不需要給予此種誘因而促使其創作<sup>69</sup>。此外，人工智慧無法實行著作權擁有者為保護其權利所應進行的法律行動，包括對於侵權者進行訴訟或對他人授權，此等措施實際上都要由自然人來進行，

---

<sup>63</sup> 同前註，頁 26。

<sup>64</sup> Tuomas Sorjamaa (2016). *I, Author: Authorship and Copyright in the Age of Artificial Intelligence*, Department of Accounting and Commercial Law, Hanken School of Economics, Helsinki, 54.

<sup>65</sup> HM Bøhler (2017). *EU copyright protection of works created by artificial intelligence systems*, JUS399 Master's thesis Faculty of Law of University of Law, 27-28.

<sup>66</sup> Tuomas Sorjamaa (2016). *I, Author: Authorship and Copyright in the Age of Artificial Intelligence*, Department of Accounting and Commercial Law, Hanken School of Economics, Helsinki, 50.

<sup>67</sup> HM Bøhler (2017). *EU copyright protection of works created by artificial intelligence systems*, JUS399 Master's thesis Faculty of Law of University of Law, 28.

<sup>68</sup> European Parliament (2017). *European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics*, 16.

<sup>69</sup> Tuomas Sorjamaa (2016). *I, Author: Authorship and Copyright in the Age of Artificial Intelligence*, Department of Accounting and Commercial Law, Hanken School of Economics, Helsinki, 51.

則把著作權歸屬給人工智慧顯然不是一個好的作法<sup>70</sup>。由於賦予人工智慧「電子人格」將產生上述種種問題，學者對於歐洲議會的提案多有批評<sup>71</sup>，而截至目前為止，歐盟委員會尚未對歐洲議會的提案採取進一步的行動。

第三種看法則是將著作權歸屬於人工智慧的開發者<sup>72</sup>。此種看法的有力論點在於如沒有開發者開發人工智慧的創意，根本不會有人工智慧所為的創作存在，既然開發者花費大量勞力、時間、費用在開發人工智慧，其對人工智慧創作物應至少享有一部分的著作權。此外，相較於使用者的貢獻僅限在按下啟動按鈕，開發者的貢獻毋寧是遠超過使用者，故由其享有著作權相當合理<sup>73</sup>。不過，此種見解會面臨兩大困難，第一是人工智慧最終所為之創作並非開發者可以預測，開發者僅是就人工智慧所為的創作提供可能性，並非實際之作品，如就整個創作賦予開發者著作權，顯然是對開發者未貢獻其創意的部分過度評價，亦不符合著作權法僅保護實際創作的原則<sup>74</sup>。第二，如賦予開發者著作權，將有執行上的困難<sup>75</sup>。因開發者僅負責開發，該人工智慧創作物一般係由購買該人工智慧使用者所觸發，產生的作品亦在該使用者的管領範圍內，如該使用者不通知開發者其已利用人工智慧創作出作品，開發者實難以確認是否已有作品存在<sup>76</sup>。而即使不賦予開發者人工智慧所為創作之著作權，開發者就人工智慧本身仍可依 Software Directive 2004/24/EC 取得著作權，並非完全未獲保護<sup>77</sup>。

最後一種看法是由人工智慧的使用者取得著作權<sup>78</sup>。使用者啟動人工智慧

---

<sup>70</sup> HM Bøhler (2017). *EU copyright protection of works created by artificial intelligence systems*, JUS399 Master's thesis Faculty of Law of University of Law, 29.

<sup>71</sup> 參見網頁 <https://www.politico.eu/article/europe-divided-over-robot-ai-artificial-intelligence-personhood/> 及 <https://www.dailymail.co.uk/sciencetech/article-5612735/Experts-Europe-loggerheads-electronic-persons-legal-status-robots.html> (最後瀏覽日：10/01/2018)

<sup>72</sup> Tuomas Sorjamaa (2016). *I, Author: Authorship and Copyright in the Age of Artificial Intelligence*, Department of Accounting and Commercial Law, Hanken School of Economics, Helsinki, 45.

<sup>73</sup> Samuelson Pamela (1985). *Allocating Ownership Rights in Computer-Generated Works*, *University of Pittsburgh Law Review*, 1205.

<sup>74</sup> HM Bøhler (2017). *EU copyright protection of works created by artificial intelligence systems*, JUS399 Master's thesis Faculty of Law of University of Law, 30.

<sup>75</sup> Tuomas Sorjamaa (2016). *I, Author: Authorship and Copyright in the Age of Artificial Intelligence*, Department of Accounting and Commercial Law, Hanken School of Economics, Helsinki, 46.

<sup>76</sup> HM Bøhler (2017). *EU copyright protection of works created by artificial intelligence systems*, JUS399 Master's thesis Faculty of Law of University of Law, 30.

<sup>77</sup> 同前註，頁 31。

<sup>78</sup> Tuomas Sorjamaa (2016). *I, Author: Authorship and Copyright in the Age of Artificial Intelligence*, Department of Accounting and Commercial Law, Hanken School of Economics, Helsinki, 48.

的目的在於利用該人工智慧來進行創作，此點滿足意圖創作之要求。加上使用者是對人工智慧做出創作指令之人，由於使用者的緣故，作品才真正被產生。換言之，開發者僅是提供了工具給予使用者表達其創意，使用者才是真正決定創造作品之人。此為由使用者取得著作權之有力理由<sup>79</sup>。不過，此種看法的最大疑問在於當使用者於人工智慧創作物中的貢獻僅有按下產生成品的按鈕時，其所為指示將因為太少或太過一般，而不符合前述的原創性標準，則此時其是否還能取得著作權<sup>80</sup>？學者認為關於這個問題，必須回到現行著作權法來找尋可能的方向。在 Software Directive 91/250/EEC 的第2條第3項<sup>81</sup>中規定雇主應就員工於職務範圍內或受雇主指示下所創作的電腦程式單獨享有該電腦程式的經濟性權利。由該規定可推知立法者認為於僱傭關係下，應將員工在職務範圍內或受雇主指示所為之創作的著作權歸屬給對於把創作帶到這世界一事中最有貢獻的個人或組織，無論該個人或組織是否直接貢獻其創意在該作品中。此種見解可以類比到上述問題，也就是說，雖然人工智慧的使用者並未在作品中貢獻其創意，但其可主張其「雇用」人工智慧來進行創作，如此一來即可解決使用者就該創作貢獻不足的問題<sup>82</sup>。

不過，雇用原則僅出現於在 Software Directive 91/250/EEC，而該指令亦僅處理電腦程式部分，有關員工所為創作的著作權歸屬，在任何歐盟指令中均未設有一般性規定，而是交由歐盟各會員國決定。因此，將雇用原則類比到人工智慧的方法，似乎沒辦法完全解決問題<sup>83</sup>。

此外，如不賦予人工智慧的使用人著作權可能導致該使用人於訴訟中主張其為人工智慧所為創作之著作人，而法院實際上很難區分該作品究竟有包含使用者的創意在內或是僅由人工智慧單獨創作完成。賦予使用人著作權

---

<sup>79</sup> 同前註，頁 48。

<sup>80</sup> HM Bøhler (2017). *EU copyright protection of works created by artificial intelligence systems*, JUS399 Master's thesis Faculty of Law of University of Law, 31.

<sup>81</sup> Article 2 (3) of the Software Directive 91/250/EEC: Where a computer program is created by an employee in the execution of his duties or following the instructions given by his employer, the employer exclusively shall be entitled to exercise all economic rights in the program so created, unless otherwise provided by contract.

<sup>82</sup> HM Bøhler (2017). *EU copyright protection of works created by artificial intelligence systems*, JUS399 Master's thesis Faculty of Law of University of Law, 31.

<sup>83</sup> 同前註，頁 32。

不但可以解決法院難以判斷的問題，亦不會發生第三種看法中開發者不知創作是否完成的問題。最後，使用者無論係以購買、租用、獲得授權等方法取得人工智慧的使用權，一般而言都有支付對價，對開發者而言已獲得報酬，而使用者亦有付出其投資，給予使用者著作權應可認為以平衡雙方之利益<sup>84</sup>。

### (三)英國

英國是少數在智慧財產法體系中提及非人類創作規定的國家之一<sup>85</sup>。英國「著作權、設計與專利法」(Copyright, Designs and Patents Act 1988)第9條第(1)項定義，作者指的是「就著作而言，係指創作著作之人」<sup>86</sup>；然而，該法有一個特殊的條款，明確提及「電腦生成著作」(computer-generated work)得以獲得著作權保護，並且訂定了不同於與一般著作的著作著作人認定方式、與不同的權利保護期間。

依據著作權、設計與專利法第178條，「電腦生成著作」的定義為「在沒有人類作者的狀況下電腦產出的作品」<sup>87</sup>，而電腦生成著作的著作權歸屬規定在同法第9條第(3)項，利用電腦產生之語文、戲劇、音樂或美術著作情形，「著作人」係指「負責就創作該著作做出必要安排之人 (the arrangements necessary for the creation of the work)」<sup>88</sup>。因此，欲確定電腦生成作品的作者需要經過兩階段的檢驗：第一，是否有人類作為作者；如果沒有人類作者，即進一步討論是否有「為創作作品而作出必要安排的人」。

依據此條文，假設一台運動攝影機自動地感測運動員的移動進行拍攝，拍攝的照片、影片等著作，仍會歸屬於架設該台機器

---

<sup>84</sup> 同前註，頁 32。

<sup>85</sup> 有相類似規定的尚包括其他大英國協成員如香港、紐西蘭、印度等，本計畫礙於篇幅，不贅討論。

<sup>86</sup> Copyright, Designs and Patents Act 1988, Section 9(1):” (1) In this Part “author”, in relation to a work, means the person who creates it.”

<sup>87</sup> Section 178 of CDPA: “generated by computer in circumstances such that there is no human author of the work.”

<sup>88</sup> Section 9(3) of CDPA provides that the author of a computer-generated work is deemed to be the person “by whom the arrangements necessary for the creation of the work are undertaken”.

的人類攝影師。人工智慧生成物如能適用此條文，代表創造人工智慧的工程師，即可能被認定為人工智慧生成物的著作人。針對著作人身分的認定，有論者為英國認定電腦生成著作辯護，認為著作權法或是專利法定義下的作者或發明人，為何在各國法規中經常特別定義為「自然人」，並不是針對機器或是人工智慧，而僅是為了比對「法人」的概念<sup>89</sup>。

除符合可著作權性的主體要求，原創性亦屬英國著作權法體系下的要件。依據著作權設計和專利法案第(1)(a)條<sup>90</sup>，英國「著作權、設計與專利法」只保護「原創」的文學、戲劇和藝術作品，如果一件文學、藝術、戲劇或音樂作品不是原創的，則該作品不能賦予著作權。英國著作權法雖然並未明確定義電腦生成著作的原創性門檻，然而從其他判決中可以觀察，通過原創性檢驗的門檻並不高，只要非屬抄襲的創作，並且考量創作過程中作者所投入的技巧 (skill)、判斷 (judgement) 和勞力 (labour) 或者智慧技巧和腦力 (intellectual skill and brain labour) 的投入<sup>91</sup>。綜合以上，原創性的要求、和作者的存在，可以說是兩個互相牽連的要件。故問題在於，人工智慧的產出，是否包括適當的技巧、勞動和判斷，足以著作權來提供保護？

本報告接下來介紹本條文在英國司法實踐的案例。然而，適用本條文的案例為數不多，以1985年的 *Express Newspapers Plc v. Liverpool Daily Post & Echo Plc* 案為例<sup>92</sup>，此案雖發生在舊法（1956年著作權法）的年代，但不影響其參考價值。該案涉及

---

<sup>89</sup> Abbott, Ryan Benjamin, *Artificial Intelligence, Big Data and Intellectual Property: Protecting Computer-Generated Works in the United Kingdom* (November 2, 2017). *Research Handbook on Intellectual Property and Digital Technologies* (Tanya Aplin, ed), Edward Elgar Publishing Ltd, Forthcoming. At 1.

<sup>90</sup> Section 1(1) of CDPA: “(1) Copyright is a property right which subsists in accordance with this Part in the following descriptions of work –

(a) original literary, dramatic, musical or artistic works,

(b) sound recordings, films [or broadcasts], and

(c) the typographical arrangement of published editions.”

<sup>91</sup> Mark Perry & Thomas Margoni (2010), *From music tracks to Google maps: Who owns computer-generated works?*, 26(6), *Computer Law & Security Review*, pp. 621-623.

<sup>92</sup> *Express Newspapers Plc v Liverpool Daily Post & Echo Plc* [1985] 3 All E.R. 680.

原告Express Newspapers舉辦類似樂透彩的兌獎活動「本月百萬富翁」，活動方式是在其刊登的報紙上載有帶有5個字母的卡片，如讀者拿到的卡片與原告公佈的卡片字母一致，即中獎。由於不一定要購買原告的報紙才能兌獎，被告遂抄襲原告新聞報紙上刊登的卡片表格。由於原作表格是藉由電腦軟體所生成，被告藉此辯稱該表格並無人類作者，並無著作權。然而，英格蘭威爾斯高等法院認為，就像作家創作時使用的筆或是打字機一樣，生成表格所用的軟體只是一種工具，如認定操作工具的人類不是著作人，而筆才是著作人，是十分不實際的<sup>93</sup>。同時，法院亦認定，表格的生成係操作電腦的人類投入大量技巧（skill）與勞力（labour）所完成<sup>94</sup>。

而在1988年著作權設計和專利法案施行後的案例，則是2007年的*Nova Productions Ltd v. Mazooma Games Ltd*案<sup>95</sup>。原告主張被告發行了兩款跟原告很相似的遊戲，侵害其著作權，然而該案的爭點並非抄襲遊戲的原始碼，而是主張原告發行的撞球遊戲中，玩家在玩遊戲時呈現的點陣圖圖像和遊戲畫面屬於「電腦生成著作」，並主張原告公司的遊戲工程師是作者。

法院最終認為，雖然遊戲的圖像是由人類一一設計的，但玩家操作中所呈現的電玩遊戲畫面是電腦生成著作。法官進一步認為，這種情況下，著作人應認定是電玩公司負責設計遊戲的人，因為他投入創意設計了各種遊戲元件的呈現，設計畫面呈現的規則和邏輯，並編寫程式碼等，由此才產生了遊戲的每一幅畫面。因為是玩家操作遊戲的按鈕的動作，使得遊戲畫面開始動作，法官也特別提及遊戲玩家是否會成為著作人的問題<sup>96</sup>。法官認為，遊戲玩家玩遊戲的過程原本就不是在進行創作，其並沒有為了創作而付出技巧或勞力，也沒有為創作而作出必要安排，

---

<sup>93</sup> 同前註，頁 1098。

<sup>94</sup> 同前註，頁 1098。

<sup>95</sup> *Nova Productions Ltd v Mazooma Games Ltd & Ors* [2007] EWCA Civ 219.

<sup>96</sup> *Id.* para. 106.



自然不是著作人<sup>97</sup>。由此案可知，法院認為，雖然遊戲設計師或工程師編寫了程式碼，也設計遊戲中呈現的人物、道具等畫面，但遊戲在玩家操作的過程中形成的連續遊戲動態畫面，並不是該工程師創作的作品，而是電腦生成著作。自然，工程師就不是當然的著作人，而是「被視為」作者。反面而言，如果遊戲玩家在其他案件背景下，真的有對創作進行必要安排的話，法院也可能認同其為著作人<sup>98</sup>。

回顧兩個判決，法院使用工具一詞比喻電腦，強調係人類有意識地操作機器、輸入指令（input），著作才得以完成，電腦僅有輔助的功能。然而，由於英國的案例對於本條文的操作並不多，在人工智慧技術發展的現今，此條文的適用引發許多疑問。尤其，如何認定人工智慧軟體的創作過程中，何人對電腦生成的作品的進行了「必要安排」？是創作的電腦軟體的工程師，還是使用軟體的使用者？法院將電腦的輔助，比喻為只是創作所使用的工具的邏輯來看，似乎工程師或軟體使用者均可如此推論，主張其享有著作權<sup>99</sup>。亦有論者認為，在目前法規狀態下，究竟本條文是為了「電腦自己創作的作品」訂定，還是「用電腦創作的作品」，此適用界線也尚不清楚<sup>100</sup>。

相對地，也有論者認為，該條文已經足夠解決電腦生成著作的著作權歸屬問題。詳言之，依據個案的不同，如果人工智慧是由軟體工程師直接啟動的，隨後人工智慧創作了一個藝術品，那工程師顯然就是作者。但是如果用戶買了一個能夠產出電腦生成著作的軟體，並使用這個軟體來創作新的作品，那麼著作權就可以認定為是使用者所有，而非屬於軟體工程師<sup>101</sup>。所以爭

---

<sup>97</sup> 同前註。

<sup>98</sup> Andres Guadamuz (2017), Do Androids Dream of Electric Copyright? Comparative Analysis of Originality in Artificial Intelligence Generated Works, 2017:2 *Intellectual Property Quarterly*).

<sup>99</sup> 同前註。

<sup>100</sup> Ryan Benjamin Abbott (November 2, 2017), Artificial Intelligence, Big Data and Intellectual Property: Protecting Computer-Generated Works in the United Kingdom. *Research Handbook on Intellectual Property and Digital Technologies* (Tanya Aplin, ed.), Edward Elgar Publishing Ltd, Forthcoming, 4.

<sup>101</sup> Andres Guadamuz (2017), Do Androids Dream of Electric Copyright? Comparative Analysis of Originality

點仍然在於個案中如何判斷何者是「為創作作品而作出必要安排的人」。

亦有論者憂心，如認定是製造人工智慧的工程師做出「必要安排」，即賦予著作權給軟體工程師或是提供軟體的公司，則幾乎該公司可以因為一個人工智慧自動作曲軟體，產生無限多曲目與其著作權<sup>102</sup>，由於著作權法有禁止他人恣意利用著作的功能，似乎有促使資本雄厚、技術超前的公司壟斷市場的可能性。

由於這些潛在的負面影響，在考量是否賦予電腦生成著作智慧財產權，學者提醒在立法政策面上，智慧財產權的賦予可以做為一種創作的誘因，獎勵投資大量技術與資金進行創新的人<sup>103</sup>。然而反面而言，因為賦予權利，即代表他人不得任意轉載、利用，智慧財產權也會帶來巨大的社會成本，可能限制自由競爭和言論自由，甚至可能抑制創新與知識共享的開放性<sup>104</sup>。

針對人工智慧智慧財產權歸屬可能帶來的影響，在英國議會轄下的人工智慧特別委員會2018年4月16日發佈的《人工智慧在英國的發展——準備、意願與能力》(AI in the UK: ready, willing and able?)報告中<sup>105</sup>，雖未針對著作權究應歸屬於何人表達意見，但有提及人工智慧帶來的巨大價值可能加深社會不平等的憂慮<sup>106</sup>。報告中提及，如果人工智慧確實能大幅提高效率，使用更少的工人，這是否也意味著效率的提高所產生的所有財富，都將流向擁有人工智慧的人，尤其是擁有人工智慧相關智慧財產權和人工智慧數據的人？如果真是如此，那麼對於因為人工智慧的來臨而被取代工作的人是否公平<sup>107</sup>。最後，在該國會報告

---

in Artificial Intelligence Generated Works, 2017:2 *Intellectual Property Quarterly*.

<sup>102</sup> Jani Ihalainen (2018), Computer creativity: artificial intelligence and copyright, 13(9) *Journal of Intellectual Property Law & Practice*.

<sup>103</sup> Ryan Benjamin Abbott (November 2, 2017), Artificial Intelligence, Big Data and Intellectual Property: Protecting Computer-Generated Works in the United Kingdom. *Research Handbook on Intellectual Property and Digital Technologies* (Tanya Aplin, ed), Edward Elgar Publishing Ltd, Forthcoming, 10.

<sup>104</sup> 同前註，頁 11。

<sup>105</sup> UK House of Lords Artificial Intelligence Committee. 2018 *AI in the UK: ready, willing and able?* (HL Paper 100), para. 84.

<sup>106</sup> 同前註，para. 268。

<sup>107</sup> 同前註，para. 268。

的建言部分強調，政府必須注意人工智慧可能造成的潛在社會或是城鄉間的不平等，也應該要確保國民有平等的機會以享受人工智慧帶來的成果<sup>108</sup>。

綜上所述，雖然英國著作權法體系將「電腦生成著作」這種非純粹人類明文列為受保護的著作類型，但似乎並不代表這條法律可以直接適用於所有人工智慧創作物。假如該條文可以適用於人工智慧生成物，以目前人工智慧的發展而言，賦予人工智慧背後的操作者或工程師著作權頗值得我國借鏡，因為此舉將保證這些公司投資在人工智慧研發投入可得回收，並確保技術進步的公司願意持續投資。需注意的是，就算可以直接適用本條文，隨著人工智慧技術繼續進展，人工智慧可能有更大的空間進行獨立作業，認定何謂創作過程的「必要安排」也會變得越來越難以確定。尤其，如果在人工智慧可以不依靠人類，完全獨立自主產出作品，則可能出現完全沒有自然人「做出必要的安排」，那麼在英國著作權法現行法的規範狀態下，無人可以符合作者的認定，而無法賦予著作權。

#### (四) 澳洲

與英國呈現明顯對比的是澳洲，目前，在澳洲的法規體系下，非人類創作的作品無法享有著作權。

雖然1988年到1998年之間，兩度由獨立的著作權法審查委員會（the Copyright Law Review Committee）討論過電腦生成素材（computer-generated material）的著作權保護問題，1998年的委員會報告甚至參考英國法制，建議區分「電腦輔助而生成的著作」和「電腦本身產出的著作」<sup>109</sup>。針對前者，著作權法審查委員會認為電腦單純只是一種工具，輔助人類進行創作，著作權法的大原則並不需要改變，只要有原創性的著作仍可以受到保護，並無修法必要；然而針對後者「電腦生成物」，澳洲著作權法修法委員會有建議制定立法澄清電腦生成物的著作權歸屬

---

<sup>108</sup> 同前註，para. 275。

<sup>109</sup> Cameron Andrews (2011), Copyright in computer-generated work in Australia post-IceTV: Time for the Commonwealth to Act, 22(1) *Australian Intellectual Property Journal*, 29 and 36.

<sup>110</sup>，然而至今尚未具體修改這部分著作權法。因此，在目前的現行法下，1968年的澳洲著作權法並沒有對電腦生成物的著作權保護作出具體規定，解釋上仍必須有一個自然人作者存在<sup>111</sup>。

首先討論作者的身分。舉例而言，日前Google發佈了其開發的人工智慧相機Clips，聲稱其結合人臉辨識功能與機器學習等技術，這台相機軟體能夠辨識環境，並做到自動捕捉照相的完美瞬間，亦即使用者無需主動控制相機，相機自己就能夠完成拍攝。然而，根據澳洲1968年著作權法第32條<sup>112</sup>，未經出版的原創文學、戲劇、音樂或藝術作品，著作權歸屬於「作者」，而該作者必須為符合資格的人（qualified person），意指該人是澳洲公民或在澳洲居住。由此條文可知，除了在文義解釋上，作者指的是人類，並且作品需要具有原創性。以例子中的攝影作品為例，在澳洲1968年著作權法第10條(1)項中，照片的作者被定義為「拍照的人」<sup>113</sup>。換言之，前述Google Clips自動拍攝相機的使用者或是工程師，均不可能主張其為著作權人，因為他們都沒有主動拍攝這張相片<sup>114</sup>。

那麼前述的照片是否可能由人工智慧軟體本身取得著作權呢？在澳洲現行法下，答案似是否定的。原因在於，澳洲著作權法雖沒有明確訂定前述條文中拍照的「人」究竟是否限定於自然人，依據「法律解釋法」（Acts Interpretation Act），卻有明確定義「人」係指「個人、國家或法人團體」<sup>115</sup>，由此條文明白表示機器並不屬於定義下的人類。

討論完著作人主體身分的認定，退步言之，就算非人類可以被賦予著作權，

---

<sup>110</sup> Parliament of Australia (1999), 'Simplification of the Copyright Act 1968 - Part 2: Categorisation of Subject Matter and Exclusive Rights, and Other Issues' 15 *Research Note* 1, 2.

<sup>111</sup> Mark Perry & Thomas Margoni (2010), From music tracks to Google maps: Who owns computer-generated works?, 26(6) *Computer Law & Security Review*, 621 and 622.

<sup>112</sup> Copyright Act 1968, 32(1): Subject to this Act, copyright subsists in an original literary, dramatic, musical or artistic work that is unpublished and of which the author:

(a) was a qualified person at the time when the work was made; or

(b) if the making of the work extended over a period—was a qualified person for a substantial part of that period.

<sup>113</sup> Copyright Act 1968, 10(1): **author**, in relation to a photograph, means the person who took the photograph.

<sup>114</sup> John Hannebery & Lachlan Sadler, *You Won't Own Copyright in Photos Taken with Google's New Camera*, Davies Collison Cave, 23 March, 2018. Retrieved from

<http://dcc.com/services/designs-copyright/you-wont-own-copyright-in-photos-taken-with-googles-new-camera/>

<sup>115</sup> Acts Interpretation Act 1901 Article 2C, "In any Act, expressions used to denote persons generally (such as "person", "party", "someone", "anyone", "no-one", "one", "another" and "whoever"), include a body politic or corporate as well as an individual."

仍需要進一步探討澳洲著作權法如何認定「原創性」。澳洲案例法發展上，著作必須具備原創性（originality），而認定標準主要環繞在人類作者對創作的技巧（skill）、勞力（labor）和判斷（judgment）的投入<sup>116</sup>，以下將一一介紹澳洲著作權法有關電腦生成著作的重要判決，包含*IceTV v Nine Network Australia Pty Ltd*案、*Telstra Corporation Ltd v Phone Directories Company Pty Ltd*案，和*Acohs Pty Ltd v Ucorp Pty Ltd*案。

2009年，高等法院對*IceTV v Nine Network Australia Pty Ltd*案<sup>117</sup>的判決結果，明確說明了電腦生成著作由於無法符合著作人身份和原創性等要件，不能該當著作權保護。該案涉及爭論的核心，是IceTV於2005年所發行的IceGuide電視節目指南，該指南提供訂閱用戶每周或每天的免費數位電視節目播出時刻等資訊。第一版本的指南是IceTV透過三週左右的時間，觀察各個電視節目播出的時間和天數，並且人工製作了第一版的IceGuide電視節目指南，而之後發佈的IceGuide都是用前一周的指南作為模板來預測、製作；而原告IceTV是從各個電視節目的官方網站獲得播出節目的資訊和節目單；最後，為了確保IceGuide電視節目指南的準確性，原告會參考其他報紙、雜誌或其他已出版的電視指南進行對照。也就是這一行為，使得Nine Network認定IceTV實質抄襲了其電視指南的著作權<sup>118</sup>。

經過上訴，高等法院法官認為，IceTV從Nine Network的每周電視時刻表中擷取的時間和電視節目名稱訊息並不會是侵害著作權的行為，因為法官並不認為只是按照時間順序排列節目訊息具有足夠的原創性，即便Nine Network有付出技巧與勞力，也微乎其微（minimal）<sup>119</sup>。再者，雖然IceTV製作時刻表的時候有利用了Nine Network公司的技巧和勞力，也不代表有著作權的侵害。原因在於，著作權的賦予門檻在於著作的原創性，而Nine Network的每週節目時刻表的原創性應該要表現在整體包括時間和節目訊息、節目綱要和其他訊息的選擇和呈現，單純節目時間和節目名稱的本身，

---

<sup>116</sup> Alexandra George (2014), *Reforming Australia's Copyright Law: An Opportunity to Address the Issues of Authorship and Originality*, 37(3) *University of New South Wales Law Journal*, 939.

<sup>117</sup> *IceTV Pty Limited v Nine Network Australia Pty Limited* [2009] HCA, 14.

<sup>118</sup> 同前註，頁 6。

<sup>119</sup> 同前註，頁 54。

並不足以表現原創性<sup>120</sup>。

在IceTV中所強調的較為嚴苛的原創性標準，後來被應用到2010年的*Acohs Pty Ltd v Ucorp Pty Ltd*的案例中，法官認為，作品必須源自「一個人類作者的努力」為「著作權法的基本要求」<sup>121</sup>。本案兩造均為設計自動生成表格，為客戶節省時間的軟體的公司，而Acohs的軟體運作方式為使用者鍵入內容，軟體即能自動完成產出整個資料表。Acohs指控Ucorp透過抄襲其HTML原始碼來重製Acohs的軟體所製作的資料表格。是故該案涉及的爭議為，這些電腦系統生成的HTML原始碼轉換而來的資料表格，是否具有原創性<sup>122</sup>。

法院認定，雖然Acohs是該電腦軟體系統的工程師，但系爭資料表所含有的HTML原始碼仍然是由電腦生成的，並沒有「人類作者」，不符合著作權法的要件<sup>123</sup>。那麼著作人有沒有可能是操作軟體的使用者呢？法院同樣給了否定的答案，法官認為，使用者並不是工程師，單純只是操作軟體，亦不會成為著作人<sup>124</sup>。本案在經過上訴之後，聯邦法院（Australian Federal Court）仍然維持了前審的判決結果<sup>125</sup>，認同原始碼並非由人類所創作完成，並不符合著作權法下的原創性定義<sup>126</sup>。

再者，2010年又出現一指標性案例—*Telstra Corporation Ltd v Phone Directories Company Pty Ltd*案<sup>127</sup>，法院在該案也遵循IceTV案作為判斷標準。該案重點在於，法院認定如果創作不是單純由人類所為，而是有電腦機器介入產生者，不能享有著作權。該案背景事實為被告重製原告所製作的電話簿，Telstra即主張，這些電話簿目錄都是由員工所編寫，而且在製作該目錄的過程中付出了獨立的智慧投入，故原告訴請著作權侵權損害賠償。是以，該案中最大的爭議就是，究竟原告Telstra所做的電話簿是否享有著

---

<sup>120</sup> 同前註，頁 44、54。

<sup>121</sup> [2010] FCA 577, [48]: “efforts of a single human author”.

<sup>122</sup> [2010] FCA 577, [48].

<sup>123</sup> 同前註，頁 50。

<sup>124</sup> 同前註，頁 50。

<sup>125</sup> *Acohs Pty Ltd v Ucorp Pty Ltd* [2012] FCAFC 16.

<sup>126</sup> *Acohs Pty Ltd v Ucorp Pty Ltd* [2012] FCAFC 16, 57.

<sup>127</sup> *Telstra Corporation Limited v Phone Directories Co Pty Ltd* [2010] 264 ALR 617 ; [2010] FCA 44.

作權保護。

然而，最終法院認為，原告公司蒐集的黃頁白頁電話簿，係由電腦自動化地編排生成，可見並無人類「獨立的智力與心血」投入其中<sup>128</sup>，不屬於澳洲著作權法保護客體。法院認定，在編輯電話簿的過程中，有很多個階段完全只有電腦在運作，沒有個人投入創作的努力，因此Gordan法官特別指出，電話簿的實質部份並沒有人類作者的存在，整體而言系爭電話簿作品人類參與的部分太過微小（minor），如此沒有辦法認定作者的存在<sup>129</sup>。本案在上訴後<sup>130</sup>，聯邦法院維持了最初的判決，即Telstra公司無法特定出為這部著作做出貢獻的作者，而且即使能夠特定出作者身分，也無法量化他們製作電話目錄的努力。

如將前述判決先例的邏輯應用到人工智慧生成物上，結果應該極為不利。首先，在澳洲著作權法的意義上，法條中「Person」的用字被解釋為「人類」，故人工智慧軟體所拍攝的照片或產出的作品，並沒有「作者」的存在。再根據前述判決對於原創性的狹義理解，法院經常強調作品與「獨立的智力與心血投入」的要求。連Acohs公司的軟體，明顯僅是由資料庫擷取出特定資料並完成資料表格，甚至可能稱不上是「弱人工智慧」，賦予工程師或使用者著作權的機會都被否定，對於「強人工智慧」這種完全無需人力的介入與操作的情況時，法院似乎也將認定並不屬於著作權的保護範圍<sup>131</sup>。綜上所述，人工智慧生成物在澳洲著作權法體系下面臨兩大困境：首先，澳洲著作權法仍強調著作必須有可得特定的人類作者，然而這在有電腦與機器參雜其中的創作過程，認定可能過於死板；其次，在電腦生成作品中認定原創性的標準十分嚴格。

其實在IceTV等案例之後，有許多學者提出見解，認為澳洲著作權法有修正的空間。學者指出<sup>132</sup>，如果澳洲著作權法全然排除電腦或是機器所參與

---

<sup>128</sup> [2010] FCA 44, 340: "...independent intellectual efforts."

<sup>129</sup> [2010] FCA 44, 335.

<sup>130</sup> Telstra Corporation Ltd v Phone Directories Company Pty Ltd (2010) 273 ALR 725; [2010] FCAFC 149.

<sup>131</sup> Andres Guadamuz, *Do Androids Dream of Electric Copyright? Comparative Analysis of Originality in Artificial Intelligence Generated Works*, 2017:2 Intellectual Property Quarterly (2017).

<sup>132</sup> Cameron Andrews, *Copyright in computer-generated work in Australia post-IceTV: Time for the Commonwealth to Act*, 22(1) Australian Intellectual Property Journal 29 (2011).

創作過程的作品，則長遠來看，對於澳洲的數位經濟是一大隱憂，換言之，以資料分析、資料庫或電腦相關科技為基礎的產業，將失去有效的法律保護。亦有論者認為，IceTV等案例對於之後發生案例的指導範圍，應僅及於相類似的以自動化程式完成的編輯著作，以免造成原創性要件解釋過於僵化<sup>133</sup>。學者指出，以英美法傳統上認為著作權目的在於保護創作人的經濟利益，並且強調獎勵創新和著作的利用的情況下，應該審慎考慮為何將使用新科技進行創作的行為排除於著作權法保護之外。再者，以科技中立原則為考量，亦即法律的適用應該一貫，不因使用的技術不同而做不同的認定，則該學者認為，純人工做出的作品，與使用電腦的效果所做出的作品如果成果相當，應該一併賦予著作權<sup>134</sup>。另一學者亦持相同見解，認為在創作過程中使用電腦僅是使得創作更有效率，因為這樣而拒絕賦予著作權，難謂有正當性<sup>135</sup>。

但學者也不諱言，由於現在澳洲著作權法相關條文付之闕如，不只是未來人工智慧生成物的著作權保護難以確定，連電腦只是作為輔助工具的著作權都不無疑問<sup>136</sup>，故如果想要解決此問題，還是修法為妥，尤其，必須將電腦生成著作與人類著作人的要件脫鉤<sup>137</sup>。

至於修法方向，學者不止提出可以參考英國等明確化電腦生成著作的國家，更認為英國的立法也有改進空間。一個英國同樣必須處理的問題是，著作權法要求作品須具有原創性，這樣著作權才能存在。學者主張，有鑒於著作權的政策基礎之一是通過保護對作品創作的投資，來鼓勵創作，那定義原創性的解決方案，可能就是考量何人對於作品有大量投資<sup>138</sup>。此一見解是參考了歐盟對於資料庫保護的要件。另有學者同採此說，甚至進一步例示了其認為可能該當「必要安排」的人，包含命令軟體運行的人、設計人工智慧軟體輸出的期望格式的人、選擇或客製化軟體的人、有意創作作品

---

<sup>133</sup> Anne Fitzgerald & Tim Seidenspinner, *Copyright and Consumer-Generated Materials - Is It Time to Reboot the Discussion about Authorship?*, 3 Victoria U. L. & Just. J. 47, 63 (2013).

<sup>134</sup> 同前註。

<sup>135</sup> Cameron Andrews, *Copyright in computer-generated work in Australia post-IceTV: Time for the Commonwealth to Act*, 22(1) Australian Intellectual Property Journal 29, 42 (2011).

<sup>136</sup> 同前註，頁 44。

<sup>137</sup> 同前註。

<sup>138</sup> 同前註。



的人、擁有電腦的人、付出投資的人、或同時具有數種以上提及身分的人<sup>139</sup>。另外，是修正英國對於著作權歸屬的定義：英國目前認定電腦生成著作的歸屬為「為創作作品而作出必要安排的人」，此人可能為法人；然而法人如果沒有自然人的指揮，其本身並不能夠實際做出必要安排，故學者建議，也可以將著作歸屬於創作出著作物的電腦的擁有者<sup>140</sup>。

## (五) 日本

### 1. 概說

日本為因應人口嚴重的「少子、高齡化」，以機器人、人工智慧等科技產業之研究及推進，可謂不遺餘力。除法學界對此一議題已展開相當之探討，日本政府亦非常積極地設立各種專門組織<sup>141</sup>，邀集產、官、學各界代表進行討論，並就研討之成果製作成報告書。又伴隨人工智慧技術之不斷發展，就人工智慧創作物與著作權法是否應予以修正，亦有相當程度之討論。以下首先針對有關人工智慧創作物之「可著作權性」及權利歸屬之議題，進行介紹與討論。

### 2. 「原創性」、「創作性」的要件

依日本著作權法第2條第1項規定，受著作權法保障之著作物必須具備「原創性」，並強調著作物必須為「具思想或感情」之創作，亦即必須是展現人類的思考、心情或情緒的創作<sup>142</sup>。其次，著作權法雖未有明文規定，惟通說及實務見解亦強調著作物必須具備「創作性」。所謂「創作性」並非指具備高度獨創性、學術價值或藝術價值，而是指

---

<sup>139</sup> Jani McCutcheon, *Curing the Authorless Void: Protecting Computer-Generated Works Following IceTV and Phone Directories*, 37 Melbourne University Law Review 46, 54; UWA Faculty of Law Research Paper No. 28 (2013).

<sup>140</sup> 同前註。

<sup>141</sup> 例如依據智慧財產權基本法（知的財產基本法）第24條，設置「內閣府智慧財產策略本部」（內閣府知的財產戰略本部），其後又陸續增設「內閣府智慧財產權策略推進事務局新資訊財檢討委員會」（內閣府知的財產戰略推進事務局新たな情報財検討委員会）、「內閣府智慧財產權策略推進事務局次世代智慧財產系統檢討委員會」（內閣府知的財產戰略推進事務局次世代知財システム検討委員会）等，就相關議題進行研究與討論。

<sup>142</sup> 中山信弘（2014），《著作權法》，第2版，頁44-55，東京：有斐閣。

創作必須是「創作者的個人個性表現」，作者必須自己將足以反映思想或感情等人格特質之創作表達於外，而非抄襲、模仿他人，始受著作權法所保障<sup>143</sup>。

又實務見解認為，所謂的「創作」必須是「實質參與創作的行為」。如僅係單純提供資金或給予補助的行為，並非創作行為<sup>144</sup>；但如係就作品的細節提供指示，則可認為係創作行為<sup>145</sup>。

依上述見解，如純粹由人工智慧所獨立創作之創作物，因人工智慧並不具有人類的「思想與感情」，人工智慧創作物似乎無法認為係人類「思想或感情」之表現，亦非「創作者的個人個性的表現」。如此，即難以認定人工智慧創作物具備「原創性」、「創作性」，於現行法制下，自不能受著作權法之保障。惟亦有認為，依目前之科技發展，尚未有可完全獨立創作的「強人工智慧」，目前多數人工智慧仍屬於「弱人工智慧」，亦即該人工智慧只是協助人類的一種「道具」，必須由人類輸入若干資料、下達若干指令後，人工智慧始可依據演算法進行演算而生成創作物。如此，則人類在創作過程中仍有相當高的參與比例。因此，即不應僅著眼於作為「道具」的人工智慧，而應就實際上對創作有貢獻的人類創作過程予以正面評價，肯認其「原創性」、「創作性」並進一步肯認該創作物之「可著作權性」<sup>146</sup>。

### 3. 從基礎理論的觀點思考人工智慧創作物的著作權保護

惟隨著科技進步，人工智慧相關技術不斷提升之後，人工智慧對創作的參與程度勢必不斷提高，如「強人工智慧」的技術成熟，人工智慧即可能自主、100%由人工智慧完成創作物。此時，該創作成果自非僅僅是人類創作過程之延伸。此時，對該創作的「可著作權性」又應該

<sup>143</sup> 同前註，頁 60-62。相澤英孝、西村あさひ法律事務所編（2013），《知的財産法概説》，第 5 版，頁 1429，東京：弘文堂。出井甫（2016），〈AI 創作物に関する著作権法上の問題点とその対策案〉，《パテント》，69 卷 15 期，頁 37。

<sup>144</sup> 東京地方法院昭和 39 年 12 月 26 日判例タイムズ，172 卷，頁 195「高速公路地圖案」。

<sup>145</sup> 東京地方法院昭和 54 年 3 月 30 日判例タイムズ，397 卷，頁 148「現代世界總圖案」。

<sup>146</sup> 新たな情報財検討委員会（2017），《内閣府知的財産戦略推進事務局新たな情報財検討委員会報告書》，頁 34-35，東京：自刊。

如何認定，即成為必須面對的課題<sup>147</sup>。也因此，學說及官方報告及認為，如仍囿於「原創性」、「創作性」等概念，勢必無法解決相關的課題，因此必須回到基礎理論上思考，探討為何要保障著作權，並基於該思考結果來判斷人工智慧創作物的「可著作權性」問題<sup>148</sup>。茲說明如下。

關於為何要保障著作權，大致可區分為「自然權論」與「鼓勵論」兩種基本觀點。所謂「自然權論」，乃是認創作物乃是基於人類的腦力、精神活動所創造出來的成果，因此，應視為一種「天賦人權」，必須將該創作物的權利歸屬於創作者加以保護。至於「鼓勵論」的見解則是認為，保障著作權等智慧財產權的目的在於確保人們對創作行為的參與或投資的成果，並藉由對創作行為或投資的保障，促使人們願意更進一步地參與創作、積極創造更多成果，進而使社會全體可以獲得更多良善的進步<sup>149</sup>。

基於「自然權論」的觀點，由於仍然強調著作權乃為了保障人類的智慧結晶、精神活動的成果，對於欠缺精神活動的人工智慧創作物的著作權保障，在解釋上就遭遇了較大的困難。反之，如基於「鼓勵論」的觀點，認為創作必須有投資作為基礎，因此對創作物的保障，並非基於「天賦人權」或「自然權利」的抽象理念，而是為了確保創作人投資的成本可以回收，甚至進一步獲利。尤其人工智慧的創作物，必先有相關人對人工智慧投注大量人力、物力以及財力，開發出具備相當能力的人工智慧後，始有進一步進行創作、並獲取創作物的可能。為確保投資者的投資成本，並進而促使人們更進一步投入人工智慧開發的意願，自應承認人工智慧創作物的著作權保障，使得投資者可以藉此獲利，並進而投入人工智慧的開發，而使人工智慧技術更日益精

---

<sup>147</sup> 奧邨弘司（2017），〈人工知能が生み出したコンテンツと著作権〉，《パテント》，70卷2期，頁13。

<sup>148</sup> 奧邨弘司，同前註，頁14。次世代知財システム検討委員会（2016），《内閣府知的財産戦略推進事務局次世代知財システム検討委員会報告書》，頁24-25，東京：自刊。

<sup>149</sup> 奧邨弘司，同前註，頁14。新たな情報財検討委員会，同前註，頁25。

進。<sup>150</sup>也因此，學說以及官方報告多認為，本於「鼓勵論」的觀點，應給予人工智慧創作物一定的權利保障。

此外，日本官方也基於「鼓勵論」的觀點更進一步的認為，對於人工智慧創作物的保障，不能僅止於日本國內的角度加以觀察，也應同時關照國際間的發展，做適度的調整。蓋於國際間，各國對人工智慧的研發與創新均不遺餘力，不斷有技術的創新與突破。有關人工智慧創作物的權利保障，各國也有不同的進展，如國際間已就人工智慧創作物給予相當程度的保障，而日本卻仍僅著眼於國內法層次的著作權相關法理，斤斤計較，則可能造成國際間保障人工智慧，而日本國內停滯不前的情形。此時，日本國內的著作權法制不但無法保障日本國內相關業者的投資與技術創新，反而還可能成為阻礙。蓋基於傳統著作權法制進行思考時，多半會導出「不予保障或消極保障人工智慧創作物權利」的結論。其結果，將可能造成日本國內相關業者的投資收益無法確保，也因而降低業者投資人工智慧技術開發的意願。除了對業者本身的阻礙，更可能使日本國內的整體技術發展落後於國際，對國家發展甚為不利。因此就是否應賦予人工智慧創作物權利保障時，也應參酌國際間的發展趨勢，適度地調整國內相關法制<sup>151</sup>。

#### 4. 多層次的思考判斷

基於前述的討論，日本官方報告與學說也認知到，僅從單一的觀點進行人工智慧創作物的探討，可能會因特定的取向而產生偏頗、獨斷，只能片面地對問題進行思考。為避免片面思考的流弊，應採此必須採用多層次的思考判斷。

##### (1) 依據創作流程，分層思考

例如，不直接就「是否應保障人工智慧創作物的著作權」問題加以回答，而是從目前以人工智慧進行創作的過程加以觀察，並區

<sup>150</sup> 奥邨弘司，同前註，頁 14。新たな情報財検討委員会，同前註，頁 25。

<sup>151</sup> 新たな情報財検討委員会，同前註，頁 35。

分為如下的階段，再依據各個階段的核心技術加以探討。例如：

- I. 於創作的第一階段，人類必須先建立或運用資料庫，提供人工智慧大量的學習資料。因此，於此一階段中，核心即在於此一「學習用資料」。
- II. 其次於第二階段，乃是利用具備特定演算法等機能的「人工智慧程式」，以「學習用資料」為素材進行學習。因此，於此一階段，核心即在於「人工智慧程式」本身。
- III. 至於第三階段，則是「人工智慧程式」透過對「學習用資料」的學習後，產生了「學習完成模型」。
- IV. 在第四階段，「學習完成模型」即可基於學習內容及演算法等進行創作，產出「人工智慧創作物」。在最後兩個階段，「學習完成模型」以及「人工智慧創作物」即為討論的核心<sup>152</sup>。

具體言之，就第一階段的「學習用資料」而言，其本質上乃是有關「資料庫」可否作為著作權保障客體的討論。因此，可依據資料庫的產生方式，區分為「未經選擇的單純資料集合」、「經選擇後未依序分類的資料集合」以及「經選擇並依序分類的資料集合」。學說上認為，如果是經過選擇的資料集合，由於資料的選擇必須經過資料庫建立者的判斷，此一選擇即具有「原創性」，自應肯認其著作權保障。至於選擇後又加以依序分類，則此一分類的行為，更需要資料庫建立者的價值判斷，應更容易肯定其可著作權性<sup>153</sup>。

至於第二階段的「人工智慧程式」，依日本現行著作權法第10條第9款規定，可作為「程式著作物」而被保護。惟人工智慧程式與一般的電腦軟體程式有其程度上的差異。因此是否仍以現行法體

---

<sup>152</sup> 新たな情報財検討委員会，同前註，頁 24-26。

<sup>153</sup> 中山信弘，同前註，頁 26-27。

系加以保障即已足夠，或應該基於人工智慧的特性給予不同的保障，於政策上，值得更進一步探討<sup>154</sup>。

關於第三階段的「學習完成模型」，其內容乃是「人工智慧程序與參數的組合」，學習模式除了演算法所得結果的排列，也具有若干人工智慧自己本身的動作指令。因此，似乎不構成日本著作權法上的「程式」<sup>155</sup>。又「學習完成模型」具有一定的自我體系規律，並非僅止於資料的集合，因此將其視為「資料庫」加以保護，似又有不足之處。因此，似乎也應該就「學習完成模型」再做細部的區分，例如觀察該「學習完成模型」係單純的「複製模型」、或係能夠再學習並進而完成更精細成果的「衍生模型」、或是在未知悉網路構造與參數之情形下，繼續不斷地反覆輸入學習結果後再產生新的學習模型的「蒸餾模式」，分別給予不同層次的著作權保障<sup>156</sup>。

至於第四階段的「人工智慧創作物」，尤其是人工智慧在自主規律下所創出的作品，因為目前實例上不多見，且在現行法下「原創性」等觀念尚有待突破，因此還無法直接承認其「可著作權性」。就現況而言，多數人工智慧創作物仍是人類以人工智慧作為道具所進行的創作，應可肯認其「可著作權性」。惟如果未來人工智慧自主創作的實例大量增加，甚至遠超過人類所創作的數量時，則應在避免市場混亂的前提下，思考賦予人工智慧創作物著作權的保障<sup>157</sup>。

## (2) 依據權利的性質、保護目的，分層思考

另一種多層次思考的觀點則是從「權利性質」或「權利目的」的觀點加以觀察，將著作權的保障區分為「物權性質（排他性）的

<sup>154</sup> 新たな情報財検討委員会，同前註，頁 29。

<sup>155</sup> 中山信弘，同前註，頁 118。

<sup>156</sup> 新たな情報財検討委員会，同前註，頁 29。

<sup>157</sup> 新たな情報財検討委員会，同前註，頁 35-38。次世代知財システム検討委員会（2016），《内閣府知的財産戦略推進事務局次世代知財システム検討委員会報告書》，頁 35-37，東京：自刊。

權利」、「促進利用的權利」兩種不同的層次：「物權性質（排他性）的權利」著重於對創作人的保護，無論係基於「自然權論」或「鼓勵論」的觀點，均認為應賦予權利人具物權性質、且排他性的權利，使得創作人得以獨占地享受其創作成果所帶來的利益，確保創作人的人格發展、自我實現，也確保創作者的無論是精神或物質面的投資及收益<sup>158</sup>。

「促進利用的權利」的觀點則是認為除了創作人的權利保護，更應該積極考量如何儘可能促進、擴大創作物的利用，因此，思考的面向就不在於排他的權利保護，而應該著重於如何使權利更容易分享，例如，應建立更便利、有效率的「授權」、「付費機制」，使有利用創作物意願者，能更為簡便、迅速地從創作人取得創作成果的分享<sup>159</sup>。

#### (六) 中國

中國目前就人工智慧在著作權法上的影響此一議題上，官方並無採取明顯的行動，但學界對於此一議題討論的較為熱烈，以下將介紹相關學說見解。

關於人工智慧創作物得否享有著作權，中國之著作權法規定作品須具備下述三個要件，包括(1)思想或情感的表達、(2)具有獨創性的表達、(3)屬於文學、藝術或者科學領域的作品<sup>160</sup>。一般來說，人工智慧創作物能滿足要件(3)，但是否符合要件(1)與(2)，則有待進一步討論。

有論者認為目前市面上各種人工智慧，包括能自動作曲、自動作畫或是自動產生新聞之電腦程式，實際上都是該電腦程式在執行某種演算法，無論這種演算法多麼複雜、先進和富有創意，其實都是透過固定的演算法將使用者輸入的素材轉變為一首歌、一幅畫或一篇報導。只要該電腦程式設計

<sup>158</sup> 新たな情報財検討委員会，同前註，頁 19。山本隆司（2018），〈AI時代の著作権〉，《NBL》，1131期，頁 8-9。

<sup>159</sup> 新たな情報財検討委員会，同前註，頁 20。

<sup>160</sup> 劉影（2017），〈人工智能生成物的著作權保護初探〉，《知識產權》，2017年第9期，頁 46。

完成，輸入的素材相同，無論使用者是誰、使用的電腦是否相同，執行該程式產生的作品都相同。既然使用該電腦程式所獲得的結果具有唯一性，就排除了人工智慧發揮聰明才智的可能性，導致相應的結果無法具有個性化之特徵，因而不符合獨創性的要求<sup>161</sup>。該學者因而認為人工智慧雖然給著作權保護增加了一些複雜性，但尚不足以對著作權制度形成真正的挑戰，著作權法對作品構成的相關規定不需要改變<sup>162</sup>。

但有論者質疑前述看法，該論者認為此種人工智慧既然只會執行人為設定的演算法，則應可將其作為工具對待，那麼人工智慧所創作的作品其實是背後人類的智力成果，著作權不應歸屬於人工智慧，而是由人工智慧背後的人類享有。如僅認可該等作品係基於人工智慧背後的人類而產生，卻不認可該作品具有可著作權性，也不認可由人工智慧背後的人類享有該作品之著作權，明顯不妥<sup>163</sup>。

上述見解雖然各有其道理，但應回歸獨創性此一要件進行判斷，獨創性不能簡單理解成與現存的作品表達不一樣，不一樣只是外在的表現，實質上是經過了主觀的思考，有了一定的構思之後，運用創作元素的一種表達。事實上，以目前的人工智慧來說，雖然其可以進行「創作」，但這種「創作」只是一種機械的「創作」，主要是以特定的資料庫為基礎，透過一定的篩選、分析、運算，將資料重新進行組合、排列，並套用事先設置好的創作程序，最後輸出創作成果<sup>164</sup>。如此一來，是否有所謂主觀的思考、構思的存在，實在不無疑問。

然而，若和編輯著作比較，編輯著作也是將已有的資料篩選、分析後，產生新的資料，得出一個創新的結論，即使是利用預先設置的程序所進行的輸出，也能夠帶來新的「表達」。如果編輯著作具有可著作權性，那麼人

---

<sup>161</sup> 王遷（2017），〈論人工智能生成的內容在著作權法中的定性〉，《法律科學(西北政法大學學報)》，2017年第5期，頁151。

<sup>162</sup> 同前註，頁154。

<sup>163</sup> 李偉民（2018），〈人工智能智力成果在著作權法的正確定性：與王遷教授商榷〉，《東方法學》，2018年第3期，頁153。

<sup>164</sup> 易繼明（2017），〈人工智能創作物是作品嗎？〉，《法律科學(西北政法大學學報)》，2017年第5期，頁139。



工智慧創作物似乎也同樣會符合獨創性的判斷標準，只是這種創作需要人為介入，否則將無法完成。這種情形中的人工智慧，應將其作為人的輔助工具看待，其創作也應被視為人的創作，而該創作物之著作權當然應賦予介入其中的自然人<sup>165</sup>。

本報告認為，前述這種見解各有其理，其差異應來自於對人工智慧的認定，亦即，就較為簡單的人工智慧，倘若輸入的素材相同時，該人工智慧就產生相同的結果，則未必具有獨創性，因為即使在編輯著作，如果其僅是按照字母排序等一般人都知道的方式來編輯，也被認為沒有獨創性而不賦予著作權保護。相反地，如果其他的人工智慧，在輸入素材相同的情況下，每次產生的結果不同時，即使該人工智慧只是單純地執行人類事先設定好的演算法，也未必不具有可著作權性。因此，是否具有獨創性，可能不能一概肯定或否定，而是需要視個案來認定。

以上有關獨創性的討論都是建立在單純執行既定演算法的人工智慧上。然而，如未來人工智慧有進一步的發展，能夠脫離單純執行人類設定的演算法，而可以利用模擬大腦的運作方式於其本身的智慧化資料庫進行抽樣、加工、分析、組合、排列及篩選等方式產生作品時，就已經脫離基於既定的演算法、程序而單純執行指令性輸出，而是能夠使其在沒有預定的演算法或者規則設定的情況下，透過主動學習來進行創作。此時，人類雖然能控制對人工智慧的設計和製造，但對於人工智慧本身的資料蒐集與輸出，卻無法完全控制，甚至將相同素材給人工智慧，其也能輸出不同的結果<sup>166</sup>。毋庸置疑地，此種人工智慧所產出的作品具有獨創性。

然而，即使此種人工智慧的創作具有獨創性，在現行法下仍可能不具有可著作權性。這是因為人工智慧創作物從形式上來看雖然達到著作權法所要求的獨創性，但因為這僅是透過電腦的計算能力進行分析、選擇所完成的機械式輸出，本質上並非思想或情感的表達<sup>167</sup>，換言之，難以想像電腦可

---

<sup>165</sup> 同前註，頁 139。

<sup>166</sup> 同前註，頁 139-140。

<sup>167</sup> 曹源，同前註，頁 494。

以像人類一樣表達自己的觀點和立場<sup>168</sup>，故不符合著作權法之保護要件。

由上述分析可知，在現行法的解釋論下，可以完全獨立進行運作的人工智慧所創作之作品因為並非思想或情感的表達，不能受到著作權法之保護。則如此一來，市場中將會湧入大量不受著作權保護的作品，且該等作品係落入可以任意取用之公領域中，當公領域中存在夠多的人工智慧創作時，對潛在的作品使用者來說，就沒有必要付費使用有著作權之作品，大部分人類創作的著作權價值都將因而趨近於零，著作權的授權與轉讓也可能不再發生，人類作者創作作品的經濟誘因也跟著消失，整個著作權相關產業將會萎縮<sup>169</sup>。

除此之外，因為人工智慧創作物與人類創作之作品在形式上難以區分，亦可能發生有心人士對該等作品主張著作權，導致實際上不存在的著作權人或本來不具備資格的人享有著作的權利。因為該等僭稱著作人實際上並非著作人，依著作權法並不能享有著作權，故著作權授權交易的相對人於將會面臨與非著作權人交易之風險，但因為人工智慧創作物與人類所為之創作難以區別，相對人除非不進行交易，否則並沒有方法能有效降低交易風險，著作授權市場可能因而萎縮。避免上述問題的最好方法即是給予人工智慧創作物著作權<sup>170</sup>。

而從著作權法理論中的鼓勵論來看，經濟誘因為創作的動力來源。而除了人工智慧本身具有相當的產業發展前景外，人工智慧所為創作之著作權領域也蘊含巨大商機，然而人工智慧的開發需要相當大的投資，如不給予人工智慧所為的創作著作權，將減低各界開發人工智慧的誘因，對於著作權交易具有重大影響。顯然，認可人工智慧創作的法律地位，是產業蓬勃發展的必然要求<sup>171</sup>。

透過以上分析可以發現，中國的學者多認為至少應該在立法論上給予能獨

---

<sup>168</sup> 劉影，同前註，頁 47。

<sup>169</sup> 曹源，同前註，頁 502。

<sup>170</sup> 劉影，同前註，頁 48。

<sup>171</sup> 李偉民（2018），〈人工智能智力成果在著作權法的正確定性：與王遷教授商榷〉，《東方法學》，2018 年第 3 期，頁 155。

立運作的人工智慧創作物一定程度之保護。多數學者認為應直接給予著作權保護，但亦有學者主張應以鄰接權<sup>172</sup>保護。而就權利歸屬方面，在認為以著作權保護的看法下，有學者認為應歸屬給人工智慧本身，亦有認為應歸屬給人工智慧的所有人；而在以鄰接權保護下，學者多贊同由人工智慧的所有者作為權利歸屬主體，但亦有學者認為應將權利歸屬給使用者。以下將先介紹用著作權保護下各學者之看法，再介紹以鄰接權保護下學者的看法。

採取將著作權歸屬給人工智慧的學者認為民事主體的範圍隨著時間的推移不斷發展，從自然人擴展到法人，近年來甚至興起動物權利保護，實無必要將權利主體限制在生物學意義上的「人」。法人制度是基於商業活動的不斷發展下，因為投資者對於可以規避風險的實體組織產生了需求而應運而生；同樣地，當人工智慧在現實生活中因為其快速、大量地從事創作行為而產生了大量法律需求的時候，人類透過法律賦予其特定的主體地位亦無不可。所以在法律應然面上，機器人作為權利主體並非完全不可能<sup>173</sup>。而對於具體的法制設計，該學者認為即使賦予人工智慧民事主體資格，但其僅享有限制人格。賦予人工智慧民事主體資格的目的純粹只是為了解決人工智慧所為創作的權利歸屬，其本質上仍屬於權利客體，因此購買人工智慧的民事主體對人工智慧應享有所有權，且人工智慧因創作而享有的財產權將由其所有者代為享有<sup>174</sup>。

主張將著作權歸屬給人工智慧所有權人的學者認為雖然從創作行為的角度來看，人類不會參與人工智慧的創作階段；但從數據的取捨來看，取捨需要具備一定的價值判斷標準才能在使之後產生的創作具備最低限度的創作性，該取捨標準無法為機器所自動具備，而需要由人類在機器初期的學習過程中向其提供。也就是說，人工智慧進行創作的前提，仍然是在之前機器學習過程中作為訓練者的人類將篩選數據的價值觀傳達給人工智

---

<sup>172</sup> 鄰接權 (neighboring rights) 旨在保護表演人、錄音物製作人及廣播機構之權利，惟因該等權利被認為係他人著作之利用或創作性較低，故其受保護程度低於著作權，我國並未採取鄰接權制度。

<sup>173</sup> 石冠彬 (2018)，〈論智能機器人創作物的著作權保護：以只能機器人的主體資格為視角〉，《東方法學》，2018 年第 3 期，頁 146-147。

<sup>174</sup> 同前註，頁 147。

慧。因此我們可以認為，人工智慧創作物在著作權法上可視為是代表設計者或訓練者意志的創作行為。而就特定主體沒有參與創作的情況下卻可以成為著作權法之作者此一情形，中國著作權法已訂有法人作品的規定來處理<sup>175</sup>，那麼對於人工智慧創作物，似乎也可以比照辦理，將人工智能的所有者視為作者，因為從機器學習的訓練角度來看，所有者即是向人工智慧注入其意志的主體，人工智慧則可視為代表所有者意志在進行創作，則人工智慧的所有者即可被視為是人工智慧所為創作之作者<sup>176</sup>。

不過另一位主張將著作權歸屬給人工智慧所有權人的學者則採取不同的論述方式，其指出能完全獨立進行運作的人工智慧進行創作時既然不依賴人類事先設定的規則，如果將此種人工智慧創作物解釋為代表設計者或訓練者的意志，似乎有些牽強。因此該學者即主張參考電影著作立法模式來處理人工智慧所為創作之著作權歸屬問題。電影著作之著作權歸屬給投資方亦即製片人的理由有二，一是確保投資者的回報機會，二是考慮到參與電影創作的人員較多，避免權利被過度分割而影響市場化。這兩點也能適用到人工智慧創作物上，首先，由於人工智慧的開發仰賴大量資金的投入，必須確保投資者的回報機會才能促進整個產業發展。第二，人工智慧創作物是人工智慧開發者、所有者及使用者等眾多人共同努力的成果，故也同樣存在權利被過度分割的風險。有鑑於此，應將人工智慧創作物歸屬於對該創作負有責任的一方，也就是所有人<sup>177</sup>。

接下來將介紹認為應以鄰接權來保護人工智慧所為創作的看法。

根據中國著作權法，劇作家對其創作的劇本享有文字作品著作權，表演者依據契約等授權方式獲得許可後<sup>178</sup>，對劇本進行表演，進而對該表演享有

---

<sup>175</sup> 中國著作權法第 11 條：由法人或者其他組織主持，代表法人或者其他組織意志創作，並由法人或者其他組織承擔責任的作品，法人或者其他組織視為作者。

<sup>176</sup> 熊琦（2017），〈人工智能生成內容的著作權認定〉，《知識產權》，2017 年第 3 期，頁 8。

<sup>177</sup> 劉影，同前註，頁 49。

<sup>178</sup> 中國著作權法第 37 條：使用他人作品演出，表演者（演員、演出單位）應當取得著作權人許可，並支付報酬。演出組織者組織演出，由該組織者取得著作權人許可，並支付報酬。（第 1 項）使用改編、翻譯、注釋、整理已有作品而產生的作品進行演出，應當取得改編、翻譯、注釋、整理作品的著作權人和原作品的著作權人許可，並支付報酬（第 2 項）。

鄰接權（表演者權）<sup>179</sup>；除表演之外，廣播電台、電視台及錄音錄影的製作者等鄰接權人亦具備表演者的行為特徵，而被共同歸類於鄰接權系統中。學者認為授予鄰接權予表演者、製片者及廣播者的目的並不涉及任何創造性投入，而僅僅是意圖鼓勵上述主體在製作錄音、錄影製品或節目過程中所付出的經濟性、組織性及科技性勞動，也就是說表演者的傳播行為本身並不重要，激勵創造性也不重要，重要的是要保護傳播行為背後的投資者<sup>180</sup>。

乍看之下，人工智慧創作物行為似乎與傳播行為、鄰接權毫無關聯，但是從保護投資者的觀點來看，則似乎可以賦予人工智慧創作物鄰接權。具體而言，不同表演者對同一個劇本的表演往往有不同的演出效果，但劇作家創作的劇本卻是相同的。人工智慧同樣如此，開發出人工智慧的程式開發者雖然透過程式編碼的方式確立了人工智慧最基本的運作法則，但是程式開發者本人無法準確地控制人工智慧所輸出的創作內容。在這個觀點上，人工智慧便如同表演者一般對設計師的「劇本」（受著作權保護的電腦程式）進行了自主甚至恣意的演繹<sup>181</sup>。

換言之，雖然目前世界上多數國家較為普遍的做法是將人工智慧的使用者作為人工智慧所為創作之著作權權利人，但事實上使用者並無法控制人工智慧所為創作之最終形式，則此時如賦予該使用者著作權似乎並不妥當。既然人工智慧對程式設計的演繹行為是產生創作的基礎，就如同表演者對劇本的即興發揮，那麼人工智慧的創作行為並非著作權法下獨立創作，反而係依附於電腦程式的演繹行為，則狹義的著作權在人工智慧的領域將逐漸失所附麗。雖然狹義的著作權所關注的只是「創作」的利益，但屬於廣義著作權中的鄰接權關注的則是投資者的利益<sup>182</sup>。如前所述，從因人工智

---

<sup>179</sup> 中國著作權法第 38 條第 1 項：表演者對其表演享有下列權利：(一)表明表演者身分；(二)保護表演形象不受歪曲；(三)許可他人從現場直播和公開傳送其現場表演，並獲得報酬；(四)許可他人錄音錄影，並獲得報酬；(五)許可他人複製、發行錄有其表演的錄音錄影製品，並獲得報酬；(六)許可他人通過資訊網路向公眾傳播其表演，並獲得報酬。

<sup>180</sup> 易繼明，同前註，頁 141。

<sup>181</sup> 易繼明，同前註，頁 141。類似見解參羅祥、張國安（2017），〈著作權法視角下人工智能創作物保護〉，《河南財經政法大學學報》，2017 年第 6 期，頁 148。

<sup>182</sup> 易繼明，同前註，頁 142-143。

慧的開發需投入大量資本，如不賦予人工智慧創作物保護將減少開發人工智慧的誘因這點來看，顯然賦予鄰接權保護可謂是相當適合<sup>183</sup>。就鄰接權之歸屬，有學者認為如果將人工智慧所為創作之著作權歸屬給開發者，將會顛覆著作權法下的思想與表達二分法。這是因為雖然人工智慧的開發者提供了人工智慧演算法使其能產生創作，但其並不知道人工智慧每次運作後會產生何等結果，如果將該創作之著作權賦予給人工智慧，等於是將思想做為權利歸屬的依據，並不符合思想與表達二分法<sup>184</sup>。此外，因開發者對人工智慧本身即已享有著作權，當其出售人工智慧時就可以享有一次獲利，如能再享有人工智慧所為創作之著作權，開發者將有雙重獲利的嫌疑，而人工智慧的購買者原本期待其可以享有該創作之著作權，卻因為著作權須歸屬給使用者而致其期待落空<sup>185</sup>。

該學者參考美國法院在Burrow-Giles Lithographic Co. v. Sarony案中提出的「如果不是（but for）」規則，認為如果不是使用者啟動程序，則作品永遠不會被創作。雖然開發者亦能主張如果不是其開發出人工智慧，作品也不可能被創作。不過，開發者的論證能力顯然比使用者弱，否則就將得出「刀具生產者要比持刀殺人者更應該為謀殺案負責」的荒謬結論。另外。將權利授予給使用者也有利交易，因為人工智慧開發者與人工智慧運行結果並非一一對應，如果將權利授予給設計者則意味在交易前買方必須要先確定該創作是由哪個人工智慧所創作，才能向開發者取得授權，但現實中買方幾乎無法確定來源為何；反之，因為最終的創作是由使用者產生，將權利歸屬給使用者即可大大的減低交易中搜尋來源的成本<sup>186</sup>。

不過，亦有學者持不同看法，認為上述使用者在獲得人工智慧使用權之過程中，無論是透過購買或是許可之方式，均已向人工智慧的開發者支付了

---

<sup>183</sup> 易繼明，同前註，頁 142-143。類似見解參羅祥、張國安，同前註，頁 148。王果（2016），〈論計算機「創作作品」的著作權保護〉，《雲南大學學報法學版》，2016 年第 1 期，頁 25。

<sup>184</sup> 也就是說，人工智慧透過對電腦程式本身的演繹所進行之創作，在事實上已經切割了開發者與人工智慧所為創作直接關聯性。參易繼明，同前註，頁 145。

<sup>185</sup> 王果，同前註，頁 24-25。亦有學者認為如人工智慧的所有者或者使用者委託開發者開發或向開發者購買人工智慧的著作權，不能不顧及雙方間的契約安排與交易，逕行認為人工智慧所為之創作同樣歸屬於開發者。參易繼明，同前註，頁 145。

<sup>186</sup> 王果，同前註，頁 25。

相應的對價，故將創作之著作權歸屬於使用者應屬相當合理之看法，實際上是將所有者與使用者混為一談，因為在社會分工與規模經濟的發展過程中，擁有人工智慧的人不一定是人工智慧的直接使用者。而如果將使用者與所有者分離的情況下，學者認為從引導人工智慧領域的投資這個觀點來看，以所有權為核心給予所有者相應的權利配置，也符合創新市場的需求<sup>187</sup>。

## 二、權利存續期間、作品保護範圍及侵權責任

### (一)美國

就作品保護範圍美國法上討論較少。而權利存續期間及侵權責任則分析如下。接續以上的討論，如認為人工智慧能直接以其本身取得著作權，因人工智慧沒有死亡問題，現行著作權之權利存續期間即須作不同的調整。人工智慧因不是自然人，就他人侵害人工智慧之著作權而言，無法起訴，相反地，如人工智慧侵害他人著作權時，其不但無法應訴外，更無法負擔責任，就以上問題勢必要有自然人來處理。因此，這也是不應賦予人工智慧本身著作權之有力理由。

如肯認上述學者提出放寬雇用作品原則之適用，而由人工智慧之開發者或擁有者取得著作權之見解，則權利存續期間之問題將迎刃而解，直接適用雇用作品原則的存續期間，即為以下二者較早屆期者：自發布日起算95年；自創作日起算120年<sup>188</sup>。而如發生他人侵害著作權或侵害他人著作權之侵權責任問題，既然著作權人是自然人，由其享受權利或負擔義務，則此時侵權相關問題之處理與一般人類作者並無不同。

### (二)英國

依據著作權、設計與專利法第12條第7項，英國目前對電腦生成著作的權利期間，賦予自「完成該著作」之年年底起算至第50年之年底屆滿，由此規定可知，英國將著作權的保護與自然人

---

<sup>187</sup> 易繼明，同前註，頁145。

<sup>188</sup> Kalin, Hristov (2017). Artificial Intelligence and the Copyright Dilemma. *IDEA: The IP Law Review*, 57(3), 450.

的死亡脫鉤。

另外值得注意的是，從英國著作權法第9條第(3)項對電腦生成著作的定義中可以看出，完全沒有人類參與創作過程的作品也可能落入保護範圍。是故，英國著作權法也規定，電腦生成著作並沒有賦予該自然人著作人格權<sup>189</sup>。由此可知，英國法制雖然訂定了電腦生成著作的著作權歸屬主體，但理論上，電腦產生的作品中仍然是缺乏人類作者的創意投入，因此學者認為英國著作權法第9條第(3)項<sup>190</sup>可以被定義為著作權存在所必要的創造性和原創性要求的例外<sup>191</sup>。

### (三)日本

#### 1. 關於權利存續期間：

如肯認人工智慧創作物的可著作權性，則有關權利存續期間的問題，除了應考量人工智慧並無所謂「死亡」的問題，且擁有能快速創作大量作品之能力之外，更應就保護方式加以思考。申言之，如採取「無方式主義」，亦即著作人一完成創作即取得著作權，則因權利之取得較為容易，再加上人工智慧可大量、迅速創作的特性，自不應給予過長的保障期間。反之，如採取「形式主義」的保障方式，亦即必須如同專利權或商標權，應先申請登記、註冊，獲准後始取得權利，則因已有登記或註冊前之審查以及公示程序，則權利的保障範圍較為明確且具有公示性，自可給予較長的存續期間保護<sup>192</sup>。

又，確保投資的回收，亦是設定權利存續期間的考量點。因延長權利存續保障期間，雖可使享有較長的權利保護，惟實際上，對著作物的鑑賞行為會隨著時間延長而遞減，因此權利人所獲得之經濟效益也會

---

<sup>189</sup> 陳昭妤，同前註，頁71。

<sup>190</sup> Section 9(3) of CDPA provides that the author of a computer-generated work is deemed to be the person “by whom the arrangements necessary for the creation of the work are undertaken”.

<sup>191</sup> Andres Guadamuz (2017), Do Androids Dream of Electric Copyright? Comparative Analysis of Originality in Artificial Intelligence Generated Works, 2017:2 *Intellectual Property Quarterly*.

<sup>192</sup> 出井甫(2016)，〈AI 創作物に関する著作権法上の問題点とその対策案〉，《パテント》，69卷15期，頁40。



遞減。此點於設定權利存續期間時，亦應予以考量<sup>193</sup>。

## 2. 關於保障範圍：

關於權利保障範圍，一般認為，應著重於著作財產權的保障，至於與創作者人格相關的著作人格權，應無加以保護的必要<sup>194</sup>。

此外，考量擴大創作物利用的觀點，除了具物權性質、排他性的「著作財產權」外，似可參酌「鄰接權」（賦予表演者、製片者及廣播者公演、製作錄音錄影等權利）的方式，給予人工智慧創作物「鄰接權」的保障。如此，可使有利用人工智慧創作物意願者，得以較便利地取得使用的權限，同時亦能兼顧創作者的投資收益<sup>195</sup>。

此外，亦有認為，基於人工智慧可大量、迅速創作的特性，如對所有人工智慧的創作物均予以保護，將可能壓縮人類的創作空間，造成市場的混亂。因此，應就人工智慧創作物之內容進行價值判斷，如屬於具有「高價值」的創作，始予以保障。惟應該由何人來進行此一價值判斷？又進行價值判斷時，是否可能產生對言論內容的預先審查、而有侵犯言論自由而違憲之疑慮（尤其日本國憲法第21條已明定不得預先審查言論內容，如果是人工智慧的創作，是否即不受憲法保障？）。因此，仍應有再多角度思考之餘地。惟無論如何，於賦予人工智慧創作物著作權保障時，必須慎重考量對人類創作空間的排擠效應，以及可能造成的市場混亂，應無疑問<sup>196</sup>。

## 3. 關於侵權責任：

同樣考量到人工智慧可大量、迅速創作的特性，於侵權責任的判斷上，首先，在所謂「依據性」（證明侵害物乃是依據、抄襲著作物而來）的認定上，應做若干程度的調整。蓋人工智慧創作的創作、「思考」

<sup>193</sup> 山本隆司，同前註，頁9。

<sup>194</sup> 奥邨弘司（2017），〈人工知能が生み出したコンテンツと著作権〉，《パテント》，70卷2期，頁17。

<sup>195</sup> 同前註，頁17。

<sup>196</sup> 出井甫（2016），〈AI 創作物に関する著作権法上の問題点とその対策案〉，《パテント》，69卷15期，頁40。

模式與人類截然不同，尤其如係依據大數據或資料庫的資料進行演算後所為之創作，其「依據性」更難加以證明。因為資料庫中有諸多「學習用資料」存在，人工智慧可能只是截取其中若干部分、或參照所謂的「創作風格」後進行自律的創作，此時，主張受侵害權利者，應如何說明人工智慧究竟以何種方式依據或抄襲自己的作品，實有一定程度的困難。就此而言，舉證責任的分配亦應予以調整，藉以緩和受侵害者舉證之困難<sup>197</sup>。

其次，人工智慧創作物亦有所為「僭稱權利人」的問題，蓋人工智慧可以大量、迅速的創作，再加上如係以「無方式主義」的立法例加以保護，則就某一著作物的權利人究竟如何歸屬，常有判斷上的困難。而且，甚至有非創作人僭稱自己為權利人，並進而主張權利之風險。如此將造成整體著作權法制的混亂。因此於賦予人工智慧創作物權利保障之同時，亦應加以審慎思考相關配套。例如，採取「形式主義」（要求登記、註冊）的保障，或以「列舉方式」來規範人工智慧創作物的侵權（例如，規定「有下列情形時，構成對人工智慧創作物之侵害：……」）<sup>198</sup>。

#### 4. 具體的權利救濟

至於具體的權利救濟內容，一般則認為無需有何種變動，仍不外乎是侵害除去請求權、侵害防止請求權或損害賠償請求權<sup>199</sup>。

惟就侵權行為人應如何認定，尤其是人工智慧涉及侵害他人權利時，應如何確定負擔相關義務的主體，則未見較為充分的討論。

#### (四) 中國

關於權利存續期間的問題，現行中國著作權法規定為自然人死後的五十年，如為法人則為作品發表後的五十年。著作權之權利保護持續到自然人死後五十年係為了給予著作權人之親屬繼續享有該著作之經濟利益，然而人工

<sup>197</sup> 同前註，頁 40。

<sup>198</sup> 同前註，頁 40。

<sup>199</sup> 同前註，頁 40。奧邨弘司，前揭註 147，頁 17。

智慧除了無死亡問題外，也沒有親屬可言，如就人工智慧的開發者或使用者給予死後五十年的保護期間似乎也不太妥當。由此可知，人工智慧作品的權利保護期間需要有不同的於人類作品保護期間之規定<sup>200</sup>。

至於作品保護範圍的討論，有學者認為應考量以下兩個因素而就人工智慧創作物有特別之規範：第一是考慮到反公地悲劇（The Tragedy of Anticommons）<sup>201</sup>的問題，對於人工智慧創作物僅賦予相對的排他權，亦即限制該等創作的著作權人肆意行使停止侵害之權利。這是因為人工智慧能在短時間創作出大量作品，如賦予該等作品著作權保護，將導致著作權大量存在，有關著作權授權的交易成本勢必會增加，進而阻礙作品的使用。同時，大量人工智慧創作的存在會導致表達的選擇範圍受限，創作者出於對著作權人行使權利的擔憂，創作活動也會因此受到影響。第二是保護過剩的問題，這是因為著作權法僅要求最低程度的創意，而人工智慧大量產出之作品很可能具有類似性，或是品質不高，如果給予這些作品與人類作品相同之著作權保護強度，會導致一些創作性不高的作品享有過剩的權利。因此，就人工智慧創作物，立法政策上應考慮要求較高之創作性，僅給予高於一定創作高度的作品著作權<sup>202</sup>，如此一來，也能避免人類作者受到潮水般的人工智慧創作所壓迫<sup>203</sup>。

關於人工智慧的侵權問題，有文獻提到了人工智慧在深度學習階段時即有大量重製著作權作品的行為發生，就該等重製行為，學者認為應可將深度學習階段中涉及的輸入作品行為作為合理使用的一種新類型。其認為傳統著作權法上，合理使用制度所豁免的重製行為，通常在「質」與「量」均有限制，如果以「人類接受者」作為評判合理使用的因素，因為人工智慧所為之複製行為僅發生在機器層面，並未將該等被重製之作品傳達給人類

---

<sup>200</sup> 曹源，同前註，頁 503-504。

<sup>201</sup> 反公地悲劇（The Tragedy of Anticommons）係「公地悲劇」（tragedy of the commons）之反義詞。「公地悲劇」是指，無主物或公有資源會有許多人使用，其結果將造成資源被過度使用或是濫用。解決之道，通常是私有化，私有化後，權利人將適度管理與使用資源。惟如過度將私有化時，又將造成權利過度細分、過度分散，任何一位權利人均可阻止他人使用，如此將造成資源無法被充分使用，此即為「反公地悲劇」。

<sup>202</sup> 劉影，同前註，頁 50。

<sup>203</sup> 曹源，同前註，頁 505。

讀者，故應可認為也落入合理使用的範疇<sup>204</sup>。

最後，由於採取鄰接權保護的學者有提出有關權利範圍、期間的相關見解，認為：因為人工智慧沒有思想和情感，應該排除人格權的保護，但是「署名權」可以保留，這是因為人工智慧經過訓練與深度學習，人工智慧可能形成自身的創作風格，如在創作上署名有助於在特定人工智慧與其創作建立起關聯性，有助於人工智慧創作之銷售。而既然鄰接權的保護要求較低，相對地權利內容應當有所縮減，參酌現有的鄰接權保護範圍，人工智慧的創作應給予包括重製權、發行權及網路傳播權，因為這是人工智慧創作的主要市場，透過賦予鄰接權保護可以保障投資人收回投資。最後有關保護期間部分，鄰接權無論在中國法或德國法，保護期間均較著作權短，且不同類型的鄰接權保護期間亦不同。學者認為有鑑於人工智慧的創作技術發展迅速，作品更新很快；人工智慧創作量大，容易產生訊息爆炸，建議應給予10年的保護期間，自該作發表之日起算，而如果創作完成後10年沒有發表，則法律不再提供保護<sup>205</sup>。

### 第三項 針對我國法規調適之初步建議

一、 首先就上述各國的討論，可整理出以下的趨勢。

(一)關於人工智慧創作物的可著作權性，依據各國現行法制及實務發展，多仍強調「原創性」、「創作性」的概念，強調必須是人類精神活動的創作成果，始為著作權保障之對象。

(二)惟基於「鼓勵論」的觀點，各國多認為應給予人工智慧創作物一定的權利保障。至於人工智慧創作物的著作權權利歸屬，多依「人的參與程度」加以認定。

(三)關於權利存續期間，應與人類的著作權保障作不同處理。或應考量具體的著作權保障方式（例如日本學說所提出之形式主義或無方式主義），作不

---

<sup>204</sup> 梁志文（2017），〈論人工智能創造物的法律保護〉，《法律科學（西北政法大學學報）》，2017年第5期，頁163-164。

<sup>205</sup> 羅祥、張國安，同前註，頁149。

同的考慮。

(四)關於權利保障範圍，對人工智慧應無保障著作人格權之必要。另外本於擴大利用的觀點，似乎可以「鄰接權」的方式對人工智慧創作物進行保障。

(五)關於侵權責任的認定，原則上應依據人工智慧可大量、迅速創作的特性進行侵權行為的要件或對舉證責任進行調整。

## 二、對我國的啟發

我國著作權法目前尚未針對人工智慧創作物之權利保障，有明確的規範。又參酌我國學說及實務見解，仍然強調「原創性」等概念，因此於現行法制下，有關人工智慧創作物的可著作權，尚有待突破。

惟於本計畫進行期間，曾召開研討會邀集國內權威學者以及業界代表出席提供相關學理以及業界之實務經驗，就未來著作權法制變革之方向，有以下之建議，或可供委託單位之參考。

(一)有關人工智慧創作物之著作權保障，應以更開放的態度進行思考

由各國的經驗觀之，對人工智慧創作物的權利保障，似仍不免受到現行法制的影響，而有若干困難<sup>206</sup>。惟現行著作權法制制定時，實未有人工智慧科技，因此面對人工智慧創作物此一新穎觀念時，在現行法的解釋上，不免會有若干扞格。因前，面對日新月異的科技發展，在法制面上，也應該預留更多的彈性與更開放的空間，來面對並回應社會的實際需求<sup>207</sup>。

又除了著作權相關議題，有關專利權等智慧財產權，在人工智慧技術日趨

---

<sup>206</sup> 例如關於「可著作權性」的問題，各國似仍不免糾結於「精神活動」、「思想或感情」、「主觀的個性展現」等「原創性」概念問題。

<sup>207</sup> 例如參照研討會中我國智慧財產權權威學者謝銘洋教授之意見，以「法人」制度為例，固然已是當今法制不可或缺、也被視為「理所當然」的概念或規範。惟此一概念也是經歷諸多社會經濟狀況的演變，法律制度為回應實際上社會的交易需求等，才進一步討論、立法。我國現行法下，雖無賦予人工智慧「電子人格」之相關規定，惟隨著人工智慧科技不斷推進，在可預期的未來，「強人工智慧」勢必在人類社會扮演更重要的角色。屆時，或可考慮承認「電子人格」，並建構相關法制，使人工智慧可以直接為法律上權利主體。另所謂「原創性」的概念，也並非一成不變，應隨時回應社會、科技的發展與演變。另國外亦有學者明確表示，現行著作權法根本沒有考慮到人類以外的機器、人工智慧亦可能進行創作的問題，因此如僅依現行法的相關規範與概念，無論如何均難以有所突破。因此必須有「現行框架不可能解決人工智慧創作物的著作權問題」的體認，進而重新建構新的著作權法制。參見中山信弘，頁 221。

進步後，也會面臨相關的問題。例如，人工智慧是否亦可能創造出具新穎性、進步性之發明，而有獲得專利權保護之可能及必要<sup>208</sup>？權利歸屬如何？又或者伴隨人工智慧技術的進步，相關資訊的大數據化也會日趨明顯，因此，「先行技術」也可能日趨普遍，則種發明等獲得權利化的難度也將增加，甚至可能大幅壓縮專利權取得的可能性<sup>209</sup>。此均屬應予以檢討的課題，也應該就各國法制及我國現行法令、實務見解，加以深入探討。

## (二) 權利歸屬的判斷基準

如承認人工智慧創作物的可著作權性，就其權利歸屬，則可參考各國法制演變的趨勢，以實際參與或貢獻的程度作為判斷基準。

## (三) 權利範圍

因人工智慧終究與人類有異，因此關於著作人格權的保障，應可無需考慮，而專注於著作財產權的面向。又考量擴大、促進創作物的利用，人工智慧創作物的著作權保障，不應僅顧及著作人排他、獨佔的權利保護，也可思考以鄰接權的方式加以保護。

## (四) 權利存續期間

應考量人工智慧並無所謂生命始末、且可大量、迅速創作的特性，調整權利存續期間相關規範。

## (五) 權利的救濟

同樣應考量人工智慧可大量、迅速創作的特性，關於侵權責任的要件（例如「依據性」）、救濟方法以及舉證責任的分配，均可做全面性的檢討與調整。另外，亦可將思考擴張到侵權責任、製造人責任以外的領域，例如以「保險」的方式，對受侵害者提供適足且更具效率的賠償。

---

<sup>208</sup> 陳昭妤，同前註，頁 101 以下。

<sup>209</sup> 牧野和夫，〈AI の法律問題とその解決策の方向性について〉，載於 [http://www.msadri.jp/magazine/2017/03/23/docs/review19\\_%E7%89%A7%E9%87%8E%E5%85%88%E7%94%9F.pdf](http://www.msadri.jp/magazine/2017/03/23/docs/review19_%E7%89%A7%E9%87%8E%E5%85%88%E7%94%9F.pdf)。

### 第三節 人工智慧時代下的個人資料保護與合理利用

隨著電腦視覺（Computer Vision）、語音辨識（Speech Recognition）及自然語言處理（Natural Language Processing）等技術日益進步，以及物聯網、大數據分析快速發展，具備機器學習能力的人工智慧，正逐漸滲透至人類生活的各種面向，從智慧音箱到家用機器人，從運用大數據分析的精準行銷到虛實整合的無人商店，智慧家庭及智慧零售的願景正在實現當中，而身處其中的你我，一舉一動都將被無所不在的感測器、網路追蹤工具記錄下來，成為大數據分析的素材及人工智慧賴以發展的燃料。因而，在人工智慧的時代下，如何適度規範個人資料的蒐集、處理及利用，同時促進個人資料的合理使用，已成為各國個資保護法制刻不容緩的課題。

我國新修正的個人資料保護法（下稱「個資法」），自2012年10月1日正式施行後，保護客體不再限於電腦處理的個人資料，規範對象亦從原本的「八大行業」擴及於「各行各業」，普遍喚醒社會大眾對隱私及個人資料保護的重視。個資法第1條規定，個資法旨在規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，然而，面對大數據、物聯網及人工智慧等新興科技對個人資料的使用，個資法是否能夠如同其立法目的所宣示的，一方面「避免人格權受侵害」，另一方面「促進個人資料之合理利用」，實非無疑。

適逢各國前仆後繼地投入人工智慧的發展及研究，期能在這波新興產業革命中取得先機的時刻，如何緩和AI應用上對個資保護可能帶來的衝擊，同時避免我國人工智慧發展因受制於既有法制而錯失良機，實為我國政府不得不面對的嚴肅課題，而最令人擔憂的，無非是未能提供個人資料有效的保護，卻箝制了產業運用新興科技進行轉型的機會。此外，目前我國政府正積極向歐盟爭取GDPR適足性認定（adequacy decision）<sup>210</sup>，以便個人資料能夠在我國及歐盟間自由傳輸，故在進行各項法規的調適與鬆綁時，尚需考量是否符合GDPR相關要求，亦為我國政府必須克服的難題之一。

---

<sup>210</sup> 于國欽（2018年6月5日），〈陳美伶：GDPR 適足性認定啟動〉，中時電子報，取自 <https://www.chinatimes.com/newspapers/20180605000224-260202>；陳梅英（2018年6月5日），〈爭取適足性認定 歐盟 GDPR 上路 我擬修個資法〉，自由時報，取自 <http://news.ltn.com.tw/news/focus/paper/1206330>；于國欽（2018年7月5日），〈拚2年取得GDPR 適足性認定 個資辦公室揭牌〉，中時電子報，取自 <https://www.chinatimes.com/newspapers/20180705000277-260202>

## 第一項 焦點議題

- 一、由於資料量大幅增加及演算法持續發展，資料間的聚合及連結變得更加容易，過往被認為已去識別化的資料因而重新獲得識別性，形成個人資料保護的漏洞

由希捷科技(Seagate Technology LLC)所贊助、調研機構IDC(International Data Corporation)執行的研究報告，預測全球資料量到了2025年將成長至163ZB——超過2016年所產生資料量16.1ZB的十倍——其中將有超過四分之一的資料會是即時(real time)資料，物聯網所產生的即時資料更將佔95%以上，資料量的爆炸性成長，將使由資料驅動(data-driven)的認知系統及人工智慧等新興科技得以實現<sup>211</sup>。

資料量的急劇增長及複雜演算法的持續發展，使得資料間的聚合及連結變得更加容易，過往許多被認為已經去識別化(de-identification)的資料，將有可能因技術發展而重新獲得可識別性，進而形成個人資料保護的漏洞。美國總統科學與技術顧問委員會(President's Council of Advisors on Science and Technology, 簡稱PCAST)於2014年5月針對大數據與隱私議題向歐巴馬總統提出的報告便指出，大數據分析技術的發展使得資料的去識別化日益受到挑戰，隨著人們愈來愈容易取得大量且多樣的資料，再識別(re-identification)的可能性也顯著提高<sup>212</sup>。英國政府科學辦公室(Government Office for Science, GO-Science)於2016年針對人工智慧所發表的報告亦指出，人工智慧能夠從公開資料中推衍出某些私人資訊，而隨著公開可得資料愈趨增加及人工智慧技術的發展，重新識別個人的可能性也變得越來越高，因而各組織必須定期檢視既有的保護措施是否足夠<sup>213</sup>。

依我國法務部現行函釋規定，去識別化係指「透過一定程序的加工處理，使個

---

<sup>211</sup> IDC (2017). *Data Age 2025: The Evolution of Data to Life-Critical*, 3. Retrieved from

<https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf>

<sup>212</sup> President's Council of Advisors on Science and Technology (2014). *Big Data and Privacy: A Technological Perspective*, 38-39. Retrieved from [https://bigdatawg.nist.gov/pdf/pcast\\_big\\_data\\_and\\_privacy\\_-\\_may\\_2014.pdf](https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf)

<sup>213</sup> Government Office for Science (2016). *Artificial intelligence: opportunities and implications for the future of decision making*, 14. Retrieved from [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/566075/gs-16-19-artificial-intelligence-ai-report.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/566075/gs-16-19-artificial-intelligence-ai-report.pdf)



人資料不再具有直接或間接識別性」<sup>214</sup>，資料經去識別化後，倘「依其呈現方式已無從直接或間接識別該特定個人者，即非屬個人資料，自非個資法之適用範圍」<sup>215</sup>。然而，資料經去識別化後是否已達到「無從直接或間接識別該特定個人」的程度，卻沒有統一的判斷標準，甚至有可能因資料保有者不同而有別<sup>216</sup>，造成資料保有者難以判斷個人資料是否確已「去識別化」而無個資法適用的問題，而此一難題將因資料量的大幅增加及演算法的快速發展，資料的去識別化愈來愈困難，而變得更加棘手。

為了釐清上述議題，我國個資法對於個人資料概念之理解，實有进一步深化及商榷的必要，並在此一基礎上，考量是否透過訂定去識別化國家標準或禁止恢復其識別性、資訊公開揭露、採行適當安全措施等義務的方式，處理去識別化資料因技術發展重新獲得識別性，而形成個人資料保護漏洞的問題。

## 二、當前以「告知後同意」為基礎的隱私保護框架，是否能夠提供個人資料有效的保護，愈來愈受到質疑，反而使資料保有者受限於原先蒐集目的及告知範圍，無法充分利用個人資料進行創新與轉型

大數據分析及機器學習的發展有賴於巨量資料的整合與利用，追求資料價值開發的最大化，然而，當前以「告知後同意」為基礎的隱私保護框架，卻使資料保有者受限於原先的蒐集目的及告知範圍，無法充分利用個人資料進行創新與轉型。此外，資料保有者所蒐集的個人資料，除有法律明文規定、長期契約關係或另行取得個資當事人同意外，亦有可能因為原蒐集目的消失或法（約）定保存期限屆滿，面臨遭到刪除的命運<sup>217</sup>，難以累積產業發展AI的動能。

<sup>214</sup> 法務部 107 年 4 月 26 日法律字第 10703505830 號函釋。

<sup>215</sup> 法務部 103 年 11 月 17 日法律字第 10303513040 號函釋。

<sup>216</sup> 法務部 103 年 6 月 17 日法律決字第 10303506500 號函釋指出：「住家電話號碼或行動電話是否為得以直接或間接方式識別特定個人者，須從蒐集者本身綜合各種情況與事證判斷，原無一致性之標準，此宜於個案中加以審認（個人資料保護法施行細則第 3 條立法理由參照），尚未可僅依單一資料類型，即遽論是或否為個資法所稱之個人資料。」

<sup>217</sup> 個資法第 11 條第 3 項規定：「個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。」個資法施行細則第 20 條及第 21 條則規定：「本法第十一條第三項所稱特定目的消失，指下列各款情形之一：一、公務機關經裁撤或改組而無承受業務機關。二、非公務機關歇業、解散而無承受機關，或所營事業營業項目變更而與原蒐集目的不符。三、特定目的已達成而無繼續處理或利用之必要。四、其他事由足認該特定目的已無法達成或不存在。」「有下列各款情形之一者，屬於本法第十一條第三項但書

有鑒於此，英國牛津大學網路研究所教授 Viktor Mayer-Schönberger 及經濟學人雜誌資料編輯 Kenneth Cukier 在其名著《大數據》中便指出<sup>218</sup>，面對氾濫的資訊流，防範之道不在於實施事前審查制度，而在於透過法規限制資訊的濫用。在大數據的時代，隱私保護框架應少強調蒐集時的個人同意（privacy by consent）、多著重在資料使用者對其所作所為應負的責任（privacy through accountability），應允許資料使用者將資料保存較長的時間，並允許其自由研發資料的延伸用途，毋須回頭取得個資當事人的明示同意，但資料保有者在利用資料前，必須就該利用行為對個資當事人的影響進行評估，至於風險較高的資料類別，則應由政府機關訂定基本規則，規定資料使用者應如何評估預定用途的風險，或找出最能夠避免或減輕潛在危害的作法。

由 Fred H. Cate、Peter Cullen、Viktor Mayer-Schönberger 等人提出的〈21 世紀資料保護原則：修正 1980 年 OECD 綱領〉亦指出，1980 年 OECD 綱領中的蒐集限制原則，將隱私保護聚焦於資料的蒐集階段，反而導致資料的安全防護不夠受到重視，因為數位資訊技術及感測器日益遍佈，個人資料的蒐集變得更加難以察覺，也愈發難以取得有意義及可行的個資當事人同意，而資料的價值所在，通常也不是在蒐集時便能夠知道的，故將保護重點放在告知與同意的作法，只是將資料保護的責任丟給個資當事人本身而已，有必要將相關責任移轉至資料使用者身上<sup>219</sup>。因此，Fred H. Cate 等人提倡以新的個人資料蒐集原則及使用原則，取代 1980 年 OECD 綱領揭示的相關原則，只要個人資料的蒐集：(1)未違反法律限制；(2)非出於詐欺；以及(3)避免採取非個資當事人可合理察覺或預期的方式，俾以確保其透明性，或政府機關對個人資料的蒐集：(1)係基於合法職權；(2)具有合法目的，原則上便不加以禁止，但資料蒐集者：(1)利用個人資料對個資當事人進行決策或其他評估前；(2)利用個人資料創造或推行出其他個人資料前；或(3)將個人資料揭露或散布予第三人前，應就其效

---

所定因執行職務或業務所必須：一、有法令規定或契約約定之保存期限。二、有理由足認刪除將侵害當事人值得保護之利益。三、其他不能刪除之正當事由。」

<sup>218</sup> Viktor Mayer-Schönberger and Kenneth Cukier (2013). *Big Data: The Essential Guide to Work, Life and Learning in the Age of Insight*. London, England: John Murray.

<sup>219</sup> Fred H. Cate, Peter Cullen and Viktor Mayer-Schönberger (2013). *Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines*, 16. Redmond, WA: Microsoft Corporation.

益、危害及減輕危害的工具仔細進行評估<sup>220</sup>。

我國個資法第5條<sup>221</sup>、第8條第1項<sup>222</sup>、第19條第1項<sup>223</sup>及第20條第1項<sup>224</sup>係以個資當事人知情同意、目的拘束原則及資料蒐集最小化等事前保護機制為其基本架構，此與大數據分析及機器學習的發展，追求資料價值開發最大化的特性背道而馳，使業者受限於原先蒐集目的及告知範圍。因此，實有必要重新檢視我國個資法的相關立法原則，並嘗試在「避免人格權受侵害」及「促進個人資料之合理利用」間取得平衡，例如改以「資料的使用與分享」作為規範重點、鼓勵業者提供用戶不同的隱私設定或選項、有限度開放去識別化或假名化資料的利用等。

### 三、現行個資法下，個資當事人就其個人資料所享有的權利，已不足以應付資料側寫及自動化個人決策等全新的個資利用方式，該等新興技術可能對個人權益造成極大的侵害

隨著大數據分析技術日益成熟，透過資料分析對個人進行評價、預測其行為模式的資料側寫（profiling），逐漸被廣泛使用在信用評價、精準行銷及人員招募等領域。從網頁瀏覽紀錄、社群媒體紀錄、手持裝置位置資訊等資料，便可以輕易推測出你我的性別、年齡層、嗜好、交友圈、生活作息、消費習慣及性

---

<sup>220</sup> 同前註，頁 15、17。

<sup>221</sup> 個資法第 5 條規定：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。」

<sup>222</sup> 個資法第 8 條第 1 項規定：「公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：一、公務機關或非公務機關名稱。二、蒐集之目的。三、個人資料之類別。四、個人資料利用之期間、地區、對象及方式。五、當事人依第三條規定得行使之權利及方式。六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。」

<sup>223</sup> 個資法第 19 條第 1 項規定：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、法律明文規定。二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。三、當事人自行公開或其他已合法公開之個人資料。四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。五、經當事人同意。六、為增進公共利益所必要。七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。八、對當事人權益無侵害。」

<sup>224</sup> 個資法第 20 條第 1 項規定：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為增進公共利益所必要。三、為免除當事人之生命、身體、自由或財產上之危險。四、為防止他人權益之重大危害。五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。六、經當事人同意。七、有利於當事人權益。」

取向，再輔以統計學、機率理論、深度學習等技術，甚至能夠精確地推演出個人的各項特徵、預測其行為模式，據以作為自動化個人決策（automated individual decision-making）的基礎。

對於此一發展，Viktor Mayer-Schönberger及Kenneth Cukier曾嚴正警告，個人能夠也應該對其行為負責，但不該對其傾向或習性負責，假如我們評斷他人的基礎，不再是他做了什麼，而是我們預測他將做什麼，那麼一個人的決定、自由與責任將變得無足輕重，人類的能動性亦將受到徹底破壞。因此，在大數據及人工智慧的時代，法律必須能夠維護人類的能動性，一旦大數據預測變成決策的基礎，便有必要採取下列防護措施：(1)開放：預測將影響到個人時，應公開所使用的資料及演算法；(2)認證：涉及敏感用途的演算法應通過專業第三方的認證；(3)反駁：應詳細說明人們能夠透過何種方式反駁對自己的預測<sup>225</sup>。

歐洲議會亦曾於2016年10月表示，信任必須建立在問責性上，因而在背後支持人工智慧的演算法，也必須盡可能地保持透明或可解釋性，必須用人類可以理解的語言解釋其行為，包括它們如何詮釋輸入的資料、如何作成某一特定建議等<sup>226</sup>。英國下議院科學及科技委員會（House of Commons, Science and Technology Committee）於2016年10月12日發布的《機器人與人工智慧》報告亦指出，隨著演算法在許多領域取代人類決策，決策過程的透明變得格外重要，欠缺可見性將造成人們對其結果的不信任<sup>227</sup>。英國上議院於2018年4月16日公布的研究報告甚至主張，在AI系統能夠為其決策提供完整且令人滿意的解釋前，不應利用AI系統作成可能對個人生活造成重大影響的決策<sup>228</sup>。

---

<sup>225</sup> Viktor Mayer-Schönberger and Kenneth Cukier (2013). *Big Data: The Essential Guide to Work, Life and Learning in the Age of Insight*. London, England: John Murray.

<sup>226</sup> European Parliament Committee on Legal Affairs (2016). *Artificial Intelligence Potential Benefits and Ethical Considerations*, 4. Retrieved from [http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/571380/IPOL\\_BRI\(2016\)571380\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/571380/IPOL_BRI(2016)571380_EN.pdf)

<sup>227</sup> House of Commons, Science and Technology Committee (2016). *Robotics and artificial intelligence: Fifth Report of Session 2016-17*, 17. Retrieved from <https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/145.pdf>

<sup>228</sup> House of Lords. Select Committee on Artificial Intelligence (2018). *Report of Session 2017-19: AI in UK: ready, willing and able?*, 40. Retrieved from <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>

我國個資法第3條<sup>229</sup>雖規定個資當事人有請求停止蒐集、處理或利用其個人資料的權利，但在原先蒐集目的消失或期限屆滿前，依同法第11條第3項反面解釋，個資當事人恐怕無法要求資料保有者停止特定處理行為，故即便資料保有者透過資料側寫對個資當事人作成自動化個人決策，個資當事人亦毫無置喙的餘地，僅得透過解除契約或撤回同意等釜底抽薪的方式才能加以阻止，對於個資當事人權益的保護似有未周。此外，我國個資法第8條第1項雖規定資料蒐集者應告知個資當事人利用個人資料的方式，然而，前述規定是否足以要求資料蒐集者向個資當事人說明人工智慧背後的演算法如何運作，尚非無疑。

因此，實有必要探討資料保有者採用新興技術處理個人資料，倘有可能對個資當事人權利及自由造成高度風險時，是否應要求其執行資料保護影響評估，以及是否應賦予個資當事人對資料側寫及自動化個人決策的反對權及資訊提供權。

## 第二項 外國文獻分析

### 一、 深化識別性的概念，並透過訂定去識別化國家標準、禁止恢復其識別性、資訊公開揭露、採行適當安全措施等義務的方式，處理去識別化資料重新獲得識別性而形成個資保護漏洞的問題

歐盟第 29 條資料保護工作小組（Article 29 Data Protection Working Party，下稱「Art. 29 WP」）<sup>230</sup>曾於 2007 年 6 月 20 日有關「個人資料」概念的意見書中，指出當我們說一名自然人已經被識別（identified）時，通常係指已從群體其他人當中區別（distinguished）出該自然人，而當我們說一名自然人是「可得識別的」（identifiable），則係指該自然人尚未被識別、但有被識別的的可能性。該意見書另指出，識別性通常係由特定的片斷資訊組合而成的——這些片

<sup>229</sup> 個資法第 3 條規定：「當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：一、查詢或請求閱覽。二、請求製給複製本。三、請求補充或更正。四、請求停止蒐集、處理或利用。五、請求刪除。」

<sup>230</sup> Art. 29 WP 係依據歐盟 1995 年資料保護指令第 29 條所設立，作為歐盟資料隱私保護諮詢的獨立機關，其職責在於提升成員國對於資料保護指令的遵循程度、給予成員國資料保護相關專業建議及提供歐盟執委會資料保護指令修訂意見等，依歐盟 1995 年資料保護指令第 30 條規定，Art. 29 WP 應將意見書或建議書提交給委員會及歐盟執委會，後者則須依 Art. 29 WP 要求採取相關措施、作成報告書提交至歐洲議會及理事會並予以公開。因應 GDPR 正式上路，Art. 29 WP 自 2018 年 5 月 25 日起，已改制為歐洲資料保護委員會（European Data Protection Board）。

斷資訊被稱為「識別因子」(identifiers)，其與特定個人之間具有某種特殊極密切的關係，例如外表所顯現之特徵(身高、髮色、穿著等)或無法直接為人感知的特質(職業、職位、姓名等)，我們有可能透過姓名直接識別出一個人，或透過電話號碼、車輛登記編號、社會安全碼、護照號碼等間接地識別出他，或結合某些判準(如年齡、職業、居住地等)限縮其所屬群體加以識別。特定識別因子是否足夠識別一個人，將隨著情境脈絡不同而改變，姓名是最為常見的識別因子，其關連到一個人從哪裡來(透過其家族姓氏)，以及圍繞著該姓名的各種法律、社會關係<sup>231</sup>，而某些識別因子表面看來無法指認出特定自然人，但與其他資訊相結合後，仍有可能造成可得識別的結果，端視資料控管者(data controller)是否保有該等資訊而定<sup>232</sup>。

Art.29 WP 於該意見書中進一步指出，依歐盟 1995 年資料保護指令前言第 26 點意旨<sup>233</sup>，在判斷一個人是否可得識別時，應以資料控管者或其他任何人所得運用之一切適當合理方法(all the means likely reasonably to be used either by the controller or by any other person)為斷，將所有相關因素均納入考量，識別所需要的成本只是判斷因素之一，而非唯一的判斷因素，欲達成之目的、資料處理方式、預期效益、個資當事人權益、組織失能及技術故障之風險等皆應納入考量，且此種測試是動態的，應考量處理當時的科技水平及將來發展的可能性，假如資料將保存十年，資料控管者亦應考慮資料在日後獲得識別性、進而成為個人資料的可能性<sup>234</sup>。

為了發展大數據分析及 AI 相關技術，業者必須儘可能地取得大量的資料，但知悉個資當事人姓名或身分與否，往往並非資料蒐集者的意圖所在，Art. 29 WP 上述意見書將識別性的概念還原為「與群體當中其他人區別開來的可能性」，而非以「知悉個資當事人姓名或身分與否」作為識別與否的標準，有助於人們建立正確的觀念，認知到即便未指名道姓，仍有可能對個人隱私造成傷害。另

---

<sup>231</sup> 但該意見書同時指出，姓名並非識別一個人的必要條件，以網路流量監控工具為例，其能夠輕易地識別出一台機器及螢幕背後的使用者，甚至無須探問這名自然人的姓名或住址，識別一個人的可能性與能否找出其姓名間，已不存在必然的關連。Article 29 Data Protection Working Party (2007). *Opinion 4/2007 on the concept of personal data*, 14. Retrieved from [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136\\_en.pdf](http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf)

<sup>232</sup> 同前註，頁 12-13。

<sup>233</sup> GDPR 前言第 26 點亦同。

<sup>234</sup> Article 29 Data Protection Working Party (2007). *Opinion 4/2007 on the concept of personal data*, 15.

一方面，由於大數據分析及 AI 相關技術的發展，使得資料間的聚合及連結變得愈來愈容易，過往許多被認為已經去識別化的資料，將有可能因技術發展而重新獲得可識別性，進而形成個人資料保護的漏洞，Art. 29 WP 上述意見書將識別性看作一個持續不斷改變的動態過程，要求資料控管者定期檢視資料是否具有識別性，並輔以匿名化（Anonymisation）、假名化（Pseudonymisation）等去識別化技術，俾確保個人權益及隱私免於侵害，對於人工智慧時代下的個資保護，亦格外具有啟發的作用。

由於識別性其實是一種可能性，隨著資料保有者、當時科技水平不同而有程度上的差別，假如我國政府欲以訂定去識別化國家標準，處理個人資料範圍難以界定的問題，則有必要以「操作性定義」（operational definition）取代「概念性定義」（conceptual definition），將「去識別化」或「匿名化」定義為一套具體可操作的方法或程序、而非僅作概念上的抽象描述，並透過法律肯認一旦資料控管者確實按照去識別化標準執行相關程序，資料便不再具有識別性，在法律上即非屬個人資料。目前我國法務部有關「去識別化」的函釋，便是一種概念性定義，從「結果論」的觀點出發，拘泥於識別性的「全有全無」，反而陷入莫衷一是的泥淖，改從技術面的角度切入，訂定去識別化具體執行方法，並透過法律明文規定擬制其效果，非但政府可衡諸當時科技水平隨時予以修正，避免因新興技術發展而形成個資保護的漏洞，亦有助於資料控管者將其注意力放在去識別化及其逆向技術的發展、而非法律概念上的遊戲。<sup>235</sup>

Art. 29 WP 於 2014 年 4 月 10 日有關「匿名化技術」的意見書即指出，「匿名化」旨在透過資料處理達成「不可逆地防止個資當事人的識別」（irreversibly preventing identification of the data subject），但由於任何用來進行資料匿名化的技術上或組織上措施，皆殘留著再識別化的固有風險，故有必要使用「匿名

---

<sup>235</sup> 目前除了從「末端」處理資料、依結果指標評估其成效外，目前亦有從「前端」處理資料的技術正在發展，例如透過抽籤或隨機等方式製作合成資料，作出一個統計特性相類似的資料集，而不使用真實資料，該等技術在數學上可進行驗證，且最終產生的結果剛好與實際情形一樣，被稱為「Differential Privacy」（差分隱私）。依法務部 107 年 9 月 4 日法律字第 10703512280 號函釋意旨，因去識別化之加工處理並未增加對當事人權權益之額外侵害，故使用差分隱私等技術製作合成資料時，似可認為該等處理並未逾越原先蒐集之特定目的，而可依據原先蒐集時之同一合法事由為之，但在該合成資料之最終結果剛好與某特定個人的真實資料相同時，是否仍可認為該等合成資料非屬個人資料，而無個資法之適用，則非無疑義，實有進一步深入探討之必要。



化技術」(anonymization technique)取代「匿名性」(anonymity)或「匿名資料」(anonymous data)的概念<sup>236</sup>。意圖窮盡地列舉出在何種情況下，不再具有識別的可能性，這種企圖是不可能達成、也毫無實益的，資料控管者應專注在逆轉匿名化技術所必要的具體方法，特別是執行這些方法的成本及知識，評估其可能性與嚴重性，而法律規範則必須保持技術中立，並將相關資訊科技發展的潛能納入考量<sup>237</sup>。

## 二、改以「資料的使用與分享」作為規範重點，鼓勵業者提供用戶不同的隱私設定或選項，並有限度開放去識別化或假名化資料的利用等

當前以「個資當事人知情同意」、「目的拘束原則」及「資料蒐集最小化」為基礎的隱私保護框架，係來自於1974年美國隱私權法案(US Privacy Act of 1974)所揭櫫的公平資訊實務準則(Fair Information Practice Principles, FIPPs)，以及國際經濟暨合作組織(OECD)於1980年根據該等FIPPs精神所訂定的隱私保護暨個資跨境流通指引(OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)，並由1995年歐盟資料保護指令(Data Protection Directive 95/46/EC)集其大成。

然而，隨著數位資訊技術及感測器日益遍佈，個人資料的蒐集變得更加難以察覺，也愈發難以取得有意義及可行的個資當事人同意，前述隱私保護框架是否能夠提供個人資料有效的保護，愈來愈受到質疑。PCAST於2014年5月向歐巴馬總統提出的報告便指出，告知與同意是當前保護消費者隱私最為廣泛使用的方式，在理想的狀態下，用戶確實閱讀了這些告知事項、瞭解其法律意涵(必要時甚至向律師進行諮詢)，並與其他提供相類似服務的業者進行磋商，俾以取得更佳的隱私待遇，最後才給出同意。然而，現實完全不是這麼一回事，告知與同意根本是將隱私保護的負擔加諸於個人身上，更糟的是，告知事項潛藏著服務提供者得將個人資料與他人分享的條款時，個資當事人通常不會收到後者的通知，更沒有機會表示同意，當消費者面對的是「不要拉倒」

---

<sup>236</sup> Article 29 Data Protection Working Party (2014). *Opinion 05/2014 on Anonymisation Techniques*, 6-7. Retrieved from

[https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf)

<sup>237</sup> 同前註，頁8-9。



(take-it-or-leave-it)的網綁式選項時，往往只有幾秒鐘可以考慮業者精心撰寫、難以快速理解的條文<sup>238</sup>。有鑒於此，該報告進一步指出，過度強調事前的程序及限制，往往流於形式，非但無法有效地保護個人隱私，反而不合理地增加業者的法遵成本<sup>239</sup>，建議將規範重點放在「資料使用與分享」、而非「資料蒐集與保存」，並透過由第三方主動提供消費者一組標準的隱私偏好設定或選項——例如 App Store、Google Play、Microsoft Store 或大型商業組織（如金融業）因為重視商譽，也許會選擇提供消費者更有競爭力的隱私偏好設定——等方式，確保資料的使用符合個資當事人的隱私偏好，改由服務提供者、而非用戶肩負起相關責任（或由雙方皆可接受的中間商予以協助）<sup>240</sup>。

GDPR 賦予個資當事人的諸多權利當中，第 20 條資料可攜權（Right to data portability）規定，個資蒐集係基於個資當事人同意或契約關係時，或個資處理係以自動化方式為之時，個資當事人得要求資料控管者以結構化的、普遍使用的、具有機器可讀性的格式（in a structured, commonly used and machine-readable format）提供其個人資料，俾其不受阻礙地將該等資料傳送予其他資料控管者，此一設計被認為有助於業界建立起通用的（interoperable）資料格式，容許個資當事人在不同資料控管者間轉移其個人資料，透過市場競爭取得更佳的隱私待遇，藉此強化個資當事人對其個人資料的掌控，而不會因為不同廠商間資料格式不一而受到限制。但 GDPR 前言第 68 點同時指出，上述資料可攜權並非要求資料控管者必須採用技術上相容的資料處理系統，但技術上可行時，個資當事人有權要求資料控管者直接將其個人資料傳送至其他資料控管者。

另一方面，大數據是人工智慧賴以發展的燃料，但前者有賴於巨量資料的整合與利用，追求資料價值開發的最大化，此與「個資當事人知情同意」、「目的拘束原則」及「資料蒐集最小化」等要求，亦未盡相符。為了在「避免人格權受侵害」及「促進個人資料之合理利用」間取得平衡，有限度開放去識別化資料或假名化資料之利用，並透過法律規定禁止再識別，似乎是國際間值得觀察

---

<sup>238</sup> President's Council of Advisors on Science and Technology (2014). *Big Data and Privacy: A Technological Perspective*, 38. Retrieved from [https://bigdatawg.nist.gov/pdf/pcast\\_big\\_data\\_and\\_privacy\\_-\\_may\\_2014.pdf](https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf)

<sup>239</sup> 同前註，頁 49-50。

<sup>240</sup> 同前註，頁 40-41。

的發展趨勢之一。美國聯邦交易委員會（Federal Trade Commission）2012年3月提出的報告書便曾建議，為了盡可能地消除法律不確定性，可考慮採取下列保護措施，藉此肯認資料已無法合理連結至（reasonably linkable to）——亦即，無法透過合理努力（reasonable effort）連結至——特定消費者、電腦或裝置：（一）業者採取合理去識別化措施，至於合理與否，則應視個別情況而定，包括可得使用的方法及技術、系爭資料的性質及使用目的等；（二）業者公開承諾僅維持並使用該去識別化資料，不再回復其識別性，違者將被視為商業上不公平或欺騙性的行為而受到法律制裁；（三）業者應透過契約限制下游業者進行再識別，並合理監督其遵循契約條款的情形，對違約行為採取適當措施<sup>241</sup>。

為了促進個人資料的合理利用，日本於2015年修正個人資訊保護法（個人情報の保護に関する法律）時，亦特別新增「匿名加工資訊」相關規定<sup>242</sup>，容許個資處理事業得將匿名加工資訊用於其他目的或提供予第三方，不受日本個資法第16條第1項及第23條第1項之限制<sup>243</sup>，但同時課予個資處理事業下列義務作為配套：（一）**安全維護義務**：個資處理事業應實施必要安全控管，防止匿名加工過程中所移除之記述或個人識別符號或所採取之處理方法等相關資訊被洩露，並致力於對匿名加工資訊實施適當安全控管，採取必要措施確保匿名加工資訊受到適當處理（如處理相關客訴），以及對公眾揭露所採取措施之內容（第36條第2項及第6項）；（二）**資訊揭露義務**：個資處理事業應對外公告匿名加工資訊當中所含有之個資項目，提供第三人匿名加工資訊前，應向公眾揭露其中所含有之個資項目及其提供方式，並向該第三人明示該等資訊為匿名加工資訊（第36條第3項及第4項）；以及（三）**禁止再識別義務**：個

---

<sup>241</sup> Federal Trade Commission (2012). *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers*, 18-22. Retrieved from <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>

<sup>242</sup> 日本個資法將個人資訊分成「記述型個資」（descriptions）及「個人識別符號」（individual identification code），前者係指姓名、生日等個人敘述，後者則係指將特定自然人一部分身體特徵轉換成文字、字母、數字、符號或其他代碼供電腦處理使用者，或為了識別特定消費者而個別分派予該名自然人的文字、字母、數字、符號或其他代碼，而所謂「匿名加工資訊」（anonymously processed information）則是將記述型個資當中一部分記述或資料當中所有個人識別符號予以移除或替換成其他記述（該等替換方式必須是不規則的，俾確保無法藉此復原該等記述或個人識別符號），以達到無法識別個人或復原成個人資訊之目的，參見日本個人資料保護法第2條第1項及第9項規定。

<sup>243</sup> 日本個資法第16條第1項規定，個資處理事業必須盡可能地特定個人資訊之利用目的，且非經個資當事人事前同意，個資處理事業原則上不得將個人資訊用於前述目的的必要範圍外之用途，第23條第1項則規定，非經個資當事人事前同意，個資處理事業原則上不得將個人資訊提供予第三人。

資處理事業不得將匿名加工資訊與其他資訊進行比對，藉此識別個資當事人（第 36 條第 5 項）。

然而，相對於上述放寬個資合理利用的呼聲，歐盟 Art. 29 WP 曾在 2014 年 9 月針對大數據發展對個資保護造成的影響發表聲明，指出僅有在使用者相應的隱私期待得到適當滿足、資料保護權利受到尊重的情況下，大數據分析帶來的益處才能夠達成，而目的拘束及資料最小化原則仍是這方面的核心關懷，目前並無理由相信歐盟資料保護原則已經喪失有效性及適當性而必須對之進行改良，特別是目的拘束原則，其能夠確保大數據技術發展不會讓獨占或具有市場宰制地位的企業對市場參進者形成不公正的優勢<sup>244</sup>。

而歐盟 GDPR 雖已區分「匿名化資料」（anonymous information）及「假名化資料」（personal data which have undergone pseudonymisation），並肯認假名化能夠減少個資當事人風險、有助於資料控管者或處理者符合資料保護義務，但 GDPR 仍然只將假名化看作一種安全防護措施<sup>245</sup>，僅在其他目的相容於原蒐集目的之前提下，才允許資料控管者或處理者將個人資料用於其他目的，無須另覓法律上的合法事由，而為了確認對資料進行後續處理之目的是否相容於原蒐集目的，資料控管者應考量原蒐集目的與後續處理目的之間的任何關連性、資料蒐集的脈絡（特別是個資當事人基於雙方關係下對其後續使用的合理期待）、個人資料的性質（尤其係是否為特種個資）、後續處理對個資當事人的影響、相應的安全防護措施等<sup>246</sup>。

### 三、要求資料保有者採用新興技術處理個人資料前，倘有可能對個資當事人權利及自由造成高度風險，必須先執行資料保護影響評估，並賦予個資當事人對資料側寫及自動化個人決策的反對權及資訊提供權

為了避免資料側寫、自動化決策對個人權益可能造成的侵害，歐盟 GDPR 第

---

<sup>244</sup> Article 29 Data Protection Working Party (2014). *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU*, 14. Retrieved from

[https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp221\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf)

<sup>245</sup> 參見 GDPR 前言第 28 點及第 156 點、第 6 條第 4 項第 e 款、第 25 條第 1 項、第 32 條第 1 項第 a 款、第 89 條第 1 項。

<sup>246</sup> 參見 GDPR 前言第 50 點、第 5 條第 1 項第 b 款、第 6 條第 4 項。

35 條規定，資料控管者使用新興技術進行個人資料之處理——並將處理之性質、範圍、脈絡及目的納入考慮後——認為有可能對自然人之權利及自由造成高度風險時，應於處理前針對所構想之處理活動實施個人資料保護影響評估（data protection impact assessment），特別是在：（一）資料控管者透過自動化處理對自然人之個人特徵進行系統性且廣泛的評估（包括資料側寫<sup>247</sup>），並藉此作成對該自然人具有法律效果或同等顯著影響之決定時；（二）大規模處理特種個資（包括種族、血統起源、政治意見、宗教或哲學信仰、商會成員資格、基因資料、生物特徵、健康、性生活或性傾向）或刑事定罪或犯罪紀錄時；（三）在公共開放區域進行大規模且系統性的監控時。該等評估至少應包括：（一）針對所構想之處理活動及處理目的進行有系統的描述，包括資料控管者所追求之合法利益；（二）評估該等目的相關處理活動之必要性及合比例性；（三）評估對個資當事人權利及自由所帶來的風險；（四）預計用來處理該等風險的措施，包括安全防護、安全措施及確保個資保護、展示對 GDPR 遵循之機制。而當處理活動的風險有所變動時，資料控管者亦應重新進行審查。

除此之外，GDPR 第 22 條更規定，若以自動化處理（包括資料側寫）為唯一基礎的決策，將對個資當事人產生法律上的效果或同等顯著的影響時，個資當事人有權主張不受到該等決策的拘束（除非此一決策為訂約或履約所必要、為法律所允許或基於個資當事人明示同意），且資料控管者必須採取適當措施保護個資當事人之權利、自由及正當利益，至少應確保部分的人為介入、表達意見的權利及表示反對的權利等。而為了破除資料集、演算法及大數據預測所形成的黑盒子，GDPR 第 13 條第 2 項第 f 款及第 14 條第 2 項第 g 款則規定，資料控管者或處理者採用自動化決策（包括資料側寫）時，應提供個資當事人其背後邏輯操作的實質資訊（meaningful information about the logic involved）、該等處理活動對於個資當事人的影響及所設想的後果為何，GDPR 第 15 條個資當事人近閱權（Right of access by the data subject）規定，並賦予個資當事人主動要求資料控管者提供該等資訊的權利（GDPR 第 15 條第 1 項第 h 款）。

---

<sup>247</sup> GDPR 第 4 條第 4 款規定，「資料側寫」係指以任何方式自動化處理個人資料，而構成個人資料的使用，藉此評判一自然人的特定個體特性，特別是用來分析或預測其工作表現、經濟狀況、健康程度、個人偏好、興趣、是否可靠、行為模式、位置或舉動等特性。

然而，必須同時指出的是，目前國際上除了 GDPR 及援引其內容的英國 2018 年資料保護法（Data Protection Act 2018）外，尚未發現其他特別針對自動化個人決策及資料側寫進行規範的立法例，GDPR 上述規定是否得以確實被執行並發揮保護個資當事人的效果，亦值得世界各國持續觀察。

### 第三項 針對我國法規調適之初步建議

首先，我國資料保護機關可考慮參考歐盟 Art. 29 WP 的作法，透過行政函釋或公布參考指引等方式，進一步深化「識別性」及「個人資料」的概念，藉此引導公務機關及非公務機關建立正確的觀念，認知到識別性是一個持續不斷改變的動態過程，因而必須對於相關技術發展保持警覺，定期檢視去識別化的資料是否會因此重新產生識別性，及時採取適當防護措施。

再者，為了在「避免人格權受侵害」及「促進個人資料之合理利用」之間取得平衡，我國資料保護機關亦可參考 Art. 29 WP「匿名化技術」意見書及美國、日本等國作法，以訂定去識別化國家標準、透過法律擬制其效果、課予禁止再識別義務等方式，擺脫長久以來去識別化與否莫衷一是的困境，適度放寬去識別化或假名化資料的利用，非但政府可按照相關技術發展隨時改正其標準，亦可引導業界致力於去識別化及其逆向技術的發展。

第三，隨著歐盟 GDPR 於 2018 年 5 月正式上路，全球的隱私保護框架可謂正值戰國時代，既有的「個資當事人知情同意」、「目的拘束原則」及「資料蒐集最小化」等資料保護原則，在大數據及人工智慧的時代下，是否將經歷一場典範轉移，或隨著 GDPR 施行而更加穩固，目前局勢尚未明朗，但為因應人工智慧發展的需求，建議我國資料保護機關可在盡量維持既有法律架構的前提下，透過行政函釋等方式，容許資料蒐集者在告知事項之具體內容、時點及告知方式上享有一定程度的彈性，並重新檢視個資蒐集合法事由、特定目的及保存期限之間的消長關係，並非一定要透過修法的方式，才能在個資當事人權益保護及業者遵法成本之間獲得雙贏的局面。

最後，面對自動化個人決策及資料側寫對於個人權益可能造成的侵害，是否應引進 GDPR 相關個資當事人權利的規定，則建議我國資料保護機關持續觀察 GDPR 實施

狀況再為定奪，因為任何權利若沒有資料控管者或處理者內部處理機制的配套，難以發揮確實保護個資當事人之效果，而相關權利行使程序的建立，則取決於個別業者乃至於整個社會所能負擔的成本，儘管資料集、演算法及大數據預測有可能形成黑盒子，但對於個資當事人的影響卻難以一概而論，個資法作為普通法究應規範至何種程度，或由特別法處理是否更為合適，亦是我國資料保護機關必須考量的。



#### 第四節 結合監理沙盒及人工智慧以建置臺灣無人載具產業發展環境

隨著物聯網和人工智慧之發展，各種結合人工智慧的載具推陳出新，其中，飛行器及車輛的智慧化發展正持續在改變我們的產業型態與生活模式。隨著駕駛系統自動化程度的提高，人們過往對於駕駛的想像也在轉變；一旦發生事故，人類與系統間的責任歸屬，其分界也變得模糊、複雜。因此，如何在科技創新與法律管制間取得平衡，對各先進國家來說已成為一現實上迫切的課題。

##### 一、自動駕駛車輛

在人工智慧再次成為媒體的寵兒前，人們其實已經嘗試在車輛駕駛上開發、運用各種駕駛輔助系統（Driver Assistance Systems）。譬如盲點偵測系統、支持型停車輔助系統、後方碰撞警示系統、偏離車道警示系統、緩解撞擊煞車系統、適路性車燈系統、夜視系統、主動車距控制巡航系統、碰撞預防系統及停車輔助系統等等，運用感測器（感知）、電子控制單元（處理）及執行器（執行）之組合來完成各種駕駛輔助任務。

然而，伴隨人工智慧的發展益發成熟，搭載自動駕駛系統的車輛（下稱「**自駕車**」），甚至可由自動駕駛系統暫時性或持續性地執行車輛駕駛任務的車輛亦一步步從虛擬成為現實。自動駕駛能應用在解決各種社會問題，因此具有極大社會及商業價值，因此，許多企業也爭相發展自動駕駛車輛。但為了發展自駕車，我們勢將面臨各種潛在的風險及爭議，也因此需要展開風險監理與爭議預防的法制課題。

自駕車實際上可依據其自動駕駛系統自動化之程度分為不同級別。目前國際普遍採用的分級方式為國際汽車工程師協會（SAE International，下稱「**SAE**」）所提出之自駕車分級標準：SAE J3016<sup>248</sup>。SAE J3016將車子自動駕駛程度分為0~5級。另外SAE也提出SAE J3018，針對SAE J3016中符合3~5級定義之自駕車提供道路行駛之安全準則。立法委員許毓仁2017年曾於立法院連署提出「自

---

<sup>248</sup> SAE最早於2014年1月16日提出第1版標準，2016年9月30日提出第2版修正標準，現行版本則為2018年6月15發布的第3版。各版本在分級層次上並無不同，但對於如何區分各級的標準，亦即定義特徵上隨技術的發展作出更精確的修正。本報告係以SAE J3016第3版為依據進行討論。詳參SAE網站公布之資料：[https://www.sae.org/standards/content/j3016\\_201401/](https://www.sae.org/standards/content/j3016_201401/)（最後瀏覽日：2018年12月8日）。

動駕駛車輛測試管理條例」法案，並於同年10月27日完成一讀，其中第3條<sup>249</sup>規定即參酌SAE J3016標準。我國日前（2018年11月30日）最終由立法院三讀通過制定之「無人載具創新實驗條例」則將無人機、機人船等對象納入，從更一般的載具觀點，對無人載具科技創新實驗管制架構進行規劃。

詳細的分級方式如下表所示<sup>250</sup>：

SAE分級	摘要	安全駕駛之監視、因應主體
Level 0 無自動駕駛	駕駛人執行全部駕駛任務	駕駛人
Level 1 駕駛輔助	系統執行前後或左右其一的車輛控制之駕駛任務	駕駛人
Level 2 部分自動駕駛	系統執行前後及左右兩者的車輛控制之駕駛任務	駕駛人
Level 3 有條件自動駕駛	<ul style="list-style-type: none"> <li>於特定範圍內系統執行全部駕駛任務</li> <li>系統運作困難時，期待駕駛人的介入回應</li> </ul>	自駕系統 ※運作困難時由駕駛人接手
Level 4 高度自動駕駛	<ul style="list-style-type: none"> <li>於特定範圍內系統執行全部駕駛任務</li> <li>系統運作困難時不期待駕駛人的介入回應</li> </ul>	自駕系統
Level 5 完全自動駕駛	<ul style="list-style-type: none"> <li>於全部範圍內系統執行全部駕駛任務</li> <li>系統運作困難時不期待駕駛人的介入回應</li> </ul>	自駕系統

資料來源：本所自行製作。

由上表可知，只有等級3以上，轉向（左右）、減速（前後）等動作與駕駛環境監測等的全部駕駛任務都由系統來實施之自駕車才是實質意義上的「自動駕駛」。同理，要實現等級3以上的自動駕駛，首先要有高度掌握狀況的能力。一般人類在駕駛時，是透過視覺掌握路況和確認行車標示，自駕車要取代人類此項能力就必須要提升影像辨識能力，包括判斷行車標誌、發現行人和障礙物、

<sup>249</sup> 第三條：「本條例所稱自動駕駛車輛，係指具有下列情形之一者：一、部分自動化駕駛：智慧駕駛系統控制車輛方向與速度，其餘車輛操作由人員控制。二、有條件自動化駕駛：智慧駕駛系統部分控制車輛，但由人員辨識駕駛環境並可隨時接管。三、高度自動化駕駛：智慧駕駛系統在特定駕駛環境下完全控制車輛，但人員可隨時接管。四、完全自動化駕駛：智慧駕駛系統在任何駕駛環境下完全控制車輛，但人員可隨時接管。」自動駕駛車輛測試管理條例草案【議案關係文書】，立法院第9屆第4會期第6次會議，取自 [https://lci.ly.gov.tw/LyLCEW/agenda1/02/pdf/09/04/06/LCEWA01\\_090406\\_00022.pdf](https://lci.ly.gov.tw/LyLCEW/agenda1/02/pdf/09/04/06/LCEWA01_090406_00022.pdf)。

<sup>250</sup> 詳參國際汽車工程師協會公布之網站資料，取自 <https://autoalliance.org/wp-content/uploads/2017/07/Automated-Vehicles-Levels-of-Automation.pdf>。



即時處理車間距離和適當對應突發事故。

現在的自駕車發展，即使是等級3以上的車輛，也還是沒有辦法完全及時確認所有狀況，多半是事先輸入固定的號誌等等資訊，讓自駕車可以記憶如何行駛，但是對於即時發生的情況，例如車禍、臨時路線更動等等，自駕車還沒有辦法完全對應。近期國外要準備上路的自駕車，也是先由駕駛人決定好路線，車輛才會依據決定好的路線行駛。

除了自駕車本身自動駕駛系統的發展，而為了要讓自駕車的行駛更為安全，自駕車生態系統的發展也是一個重要的方向。譬如採用「協同巡航」的方式，即是在交通號誌或標示等交通基礎設施上裝設感測裝置，同時車輛彼此之間也會進行資訊交換，自駕車便可以根據交通資料和行人資料做出應對，因此即有學者認為與自主操控相比，協同巡航是一個比較安全，大眾也比較可以接受的方式<sup>251</sup>。

由於駕駛行為的複雜性，從人為操縱駕駛到全自動駕駛，還有許多中間階段的駕駛技術分級，該自動駕駛車輛究竟是屬於哪一級別，與責任歸屬的議題息息相關。

## 二、無人機

就現階段科技發展而言，因為就運用人工智慧之自動駕駛技術最困難的任務就是「判斷」，能夠做到完全以人工智慧判斷路況且達成安全行駛的自駕車是尚不存在的。縱使開放上路測試或商用，各國仍傾向要求必須有人坐在車輛內，以利對緊急狀況隨時作出反應。但相對的，比起陸地，空中沒有行人，障礙物也較少，因此無人機與自駕車比起來發展要來得迅速。

無人機（drone）此一名詞，同時可以指涉「遠距遙控機器」（remotely piloted vehicles）與「自動飛行器」（autonomous aerial vehicles），此兩者的區別在釐清民事責任歸屬時是相當重要的<sup>252</sup>。所謂的遠距遙控機器係指一直處在人類操縱者掌控下的無人機，包括以無線電操控的無人機、具有侵略或守衛功能的

---

<sup>251</sup> 三津村直貴（著），陳子安（譯）（2018），《圖解AI人工智慧大未來》，頁159，臺北：旗標。

<sup>252</sup> Michele C. Kirrane and Devinder S. Grewal (2016). Civil Liability Arising Out of the Commercial Ownership and Operation of Drones. *For the Defense*, 58(4).

軍事模型機。

操作模式可以分為第一人操作或是第三人操作，第一人操作會將實時影像傳送給操作者，所以業餘的無人機愛好者多半會使用虛擬視鏡來操作無人機。第三人操作則是遠距遙控模式，操作者是從地面來觀看並操控無人機，第三人操作是最古老的操作模式，可以想見未來將會減少該模式，因為該模式要求操作者長時間的視覺控制。至於自動飛行器則是不需要長時間人力操控的無人機，在遠距遙控機器與自動飛行器兩者中間也有很多其他種類的無人機，例如半自動無人機，亦即平常是由人力操控，但遇到某個情景的時候可以自動切換成自動模式，例如當操控者沒有辦法直接控制無人機的時候，無人機可以自動轉至預先編碼的系統來進行指定路線飛行<sup>253</sup>。

無人機也和自駕車一樣能夠運用協同巡航，讓裝有感應器的無人機之間可以互通訊，也可以利用地上原有的感應裝置，做到維持一定距離的自動跟隨功能。若將無人機和人工智慧結合，就可以做非常廣泛的運用，例如無人貨物輸送、遇難者搜尋、定期農藥噴灑、目標追蹤以及異常探測等等<sup>254</sup>。由於無人機的種類繁多，也沒有辦法對無人機的管理責任提出一個指導原則，或許可以參考過往就自動航空器和自駕車的規範來適用無人機。亦因此為議題的聚焦，以下探討，將以自駕車議題的法規國際發展趨勢及因應為主要檢討對象。

## 第一項 焦點議題

### 一、智慧載具之安全監理－自駕車的上路測試

自駕車如須真正實用化、商用化，勢必得先經過道路測試，儘管有些國家允許自駕車直接上路（如德國），但大多國家認為針對測試的區域及程序建立過渡性管制法律與特別規定是有其必要的。美國是世界上較早允許自駕車進行道路測試的國家，其中2012年美國內華達州率先將自駕車上路測試合法化。除美國外，荷蘭、瑞典、英國、韓國、日本等許多國家亦已立法允許道路測試。伴隨著自動駕駛技術（雖有等級高低）的普及化與擴大化，目前全世界已有十多個國家進行立法，允許並鼓勵自動駕駛汽車的道路測試。

---

<sup>253</sup> 同前註。

<sup>254</sup> 三津村直貴（著），陳子安（譯）（2018），《圖解 AI 人工智慧大未來》，頁 164，臺北：旗標。

全球各國關於自駕車道路試測的主要政策與法規略如下表<sup>255</sup>，但在接下來的說明將以美國、德國及日本等國家進行較深入的觀察。

國家	法規政策名稱	提出或通過時間	核心內容
荷蘭	《自動駕駛汽車測試法（草案）》(Law Governing the Experimental Use of Self-driving Vehicles)	2018年4月獲得眾議院通過	允許自駕車在沒有人員跟隨之情況下進行測試
新加坡	《2017 道路交通法修正案》(The Road Traffic(Amendment) Act 2017)	2017年2月通過	自駕車的測試合法化；規定了自動駕駛汽車測試時之責任豁免制度
美國	《聯邦自動駕駛汽車政策：加速下一代道路安全革命》(Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway)	2016年9月發佈	提出 15 項安全評估標準
	《自動駕駛系統 2.0 安全願景》(Automated Driving Systems 2.0: A Vision for Safety)	2017年9月發佈	提出 12 項安全評估標準
	《自動駕駛法案》(H. R. 3388-SELF DRIVE Act)	2017年9月眾議院審議通過（尚未生效）	明確了發展無人駕駛汽車技術（HAV、ADS等）的核心目標是安全：統一了美國全國無人駕駛技術發展由國家公路交通安全管理局監管，避免各州和各政府部門多頭管理。
	《自動駕駛法案》(S. 1885 - AV START Act)	2017年11月被提上參議院立法議程（尚未生效）	規定事項涉及高度自動汽車測試、豁免、安全評估、網路安全、隱私保護以及高度汽車技術委員會、HAV 數據訪問諮詢委員會等。

<sup>255</sup> 表格來源：騰訊研究院法律研究中心，2018 年全球自動駕駛政策研究報告，2018 年 5 月。

國家	法規政策名稱	提出或通過時間	核心內容
瑞典	《自動駕駛公共道路測試規範》(Automatic Driving Public Road Test Specification)	2017年7月生效	對自動駕駛汽車實行許可制；現行交通事故賠償條款仍然適用於自動駕駛情況；測試單位需確保測試數據採集、保存符合國際相關法規，並且保護個人隱私資料。
英國	《通往無人駕駛之路：自動駕駛汽車測試實踐守則》(The Pathway to Driverless Cars: A Code of Practice for Testing)	2015年7月發佈	規定測試者必須遵守所有相關的道路交通法律，並且確保：1. 測試車輛必須能夠上路行駛（原型車輛應在英國司機和汽車登記局註冊）；2. 經過培訓的司機或操作人員（毋須在車內）必須準備好，能夠且願意在必要時取得控制，且車輛需準備紀錄裝置；3. 已購買合適的保險。
	《車聯網和自動駕駛汽車網路安全準則》(The key principles of vehicle cyber security for connected and automated vehicles)	2018年8月發佈	涉及個人資料訊息控制、遠距離汽車控制等各項技術，共包括8項基礎原則，前3項屬於智能交通系統(ITS)與聯網和自動化車向(CAV)系統安全原則範疇，後5項屬於ITS與CAV系統設計原則範疇。
	《汽車技術和航空法案》(Vehicle Technology and Aviation Bill)	2017年3月提交下議院委員會討論(由於2017年5月3日英國議會解散，該法案已夭折)	為自動駕駛汽車引入了新的保險規定。根據該法案，自動駕駛汽車的事故須全部為保險之範圍所涵蓋，並且同一保險單必須同時承保自動駕駛汽車和車上人員的

國家	法規政策名稱	提出或通過時間	核心內容
			權益。
	《自動駕駛和電動車輛法案 2018 》(The Automated and Electric Vehicles Act 2018)	2018 年 7 月正式立法	確立了自動駕駛汽車發生事故的保險和責任規則。根據法案規定，自動駕駛汽車在「自我駕駛」狀態下發生事故的，根據車輛是否投保，分別由保險公司和車主對事故造成的損失承擔賠償責任。同時，法案還規定了保險人和車主的責任減免條款和追償制度。
德國	《自動聯網駕駛戰略》(Strategy for Automated and Connected Driving)	2015 年 9 月發布	確定了德國發展自動駕駛的六大重點行動裡用:基礎設施、法律、創新、互聯性、網路安全和數據保護、社會對話（公眾參與），並提出了具體措施。
	《道路交通法修正案》(Road Traffic Act Amendment)	2017 年 6 月生效	新法規定在特定條件下允許自動駕駛系統代替人類駕駛，此外，還規定了自動駕駛模式下的責任認定、駕駛員的權利義務、自動駕駛引發交通事故的賠償金額等。
加拿大	《公路交通法修正案》(Highway Traffic Act — O. Reg. 306/15)	2016 年 1 月生效	安大略省根據「公路交通法案」(HTA)啟動為期 10 年的測試項目，允許合格參與者在滿足特定條件的前提下，在安大略省道路上測試自駕車。

國家	法規政策名稱	提出或通過時間	核心內容
阿聯酋	《自動化運輸戰略》 (Autonomous Transportation Strategy)	2016年4月發佈	戰略旨在使2030年杜拜25%的交通運輸實現自動化，每日運輸量為500萬次。啟動「阿聯酋自動化運輸挑戰賽」，鼓勵全球的創新公司、學術機構和研發中心為杜拜量身打造自動化交通解決方案。
韓國	《機動車管理法修訂案》 (Motor Vehicle Management Act)	2016年12月修訂	修訂後的法案允許在道路上開展自動駕駛汽車測試（即臨時操作許可）。
日本	《自動駕駛汽車道路測試指南》	2016年5月發布	允許自動駕駛汽車上道路測試試驗，但要求測試時駕駛人必須坐在駕駛位。
	《遠程自動駕駛系統道路測試許可處理基準》	2017年6月發布	將遠程監控員定位為遠程存在、承擔現行道路交通法規上規定義務和責任的駕駛人。
澳洲	《澳大利亞自動駕駛汽車測試指南》 (Guidelines for Trials of Automated Vehicles in Australia)	2017年5月發布	要求人類乘員隨車，對自動駕駛車輛時可能發生的任何事件負責，並且必須能隨時對車輛進行適當的控制。

## 二、智慧載具之責任歸屬－自動駕駛模式下民事責任的安排

2018年3月，一輛Uber自動駕駛汽車在美國亞利桑那州撞到行人後，該名行人不治死亡。據新聞報導，Uber經調查認為，其自駕車上的各項傳感器其實有偵測到當時在移動的行人，然而自動駕駛系統卻決定「無需處理」，並將該偵測結果記錄為「誤報」。當然，除此之外，幾乎各個自駕車廠商也有發生或大或小的測試自駕車事故，譬如Tesla、Apple及Google，這些事故一方面可能影

響民眾對自駕車產業發展的信心，另一方面雖然令人遺憾也為人們學習如何降低，甚至避免這些風險提供了寶貴的經驗。然而，從法制角度來看，這些案例也同時加速了各界對於自駕車法律責任分配之討論及各國法制上的因應。

因應自動駕駛而產生責任討論之國家不在少數，大致上可以依照「是否更改歸責原則」而區分為兩類，第一類是「以既有歸責原則為基礎進行檢討」，第二類則為「因應科技發展新的歸責原則」，接下來的說明將就「以既有歸責原則為基礎進行檢討」之國家說明之。

## 第二項 外國文獻分析

### 一、主要國家的自駕車道路測試相關法令趨勢

#### (一)美國

美國原則上採取引導性的作法，未在聯邦法律層級作出強制性的規範。美國交通部有權豁免特定車輛適用現行安全標準。各州訂定獨自的自駕車測試規範，其中亞利桑那州更對 Waymo<sup>256</sup> 核發境內首張自駕商用營運執照。

美國交通部（United States Department of Transportation）持續發布、更新非強制性的政策指引，不僅於2017年發布了《自動駕駛系統2.0安全願景》(Automated Driving Systems 2.0: A Vision for Safety)，並以其為基礎於2018年發布《自動駕駛載具3.0 為運輸的未來做好準備》(Automated Vehicles 3.0: Preparing for the Future of Transportation)。該些指引之目的在於揭示監理機關目前對自動駕駛監理的態度以及預備或已經採取的措施，以供業者遵循與大眾公評，並協助業者持續探索自駕車安全與性能的標準。

於《自動駕駛載具3.0 為運輸的未來做好準備》中，美國交通部提出以下6項監理原則<sup>257</sup>：以安全為第一要務、對科技進展保持中立、持續現代化相關法規、促進建立穩定的法規範與運營環境、主動因應自動化、保護和堅實美國大眾享有的用路自由。

<sup>256</sup> Waymo 是一家開發自駕車的公司，其為美國 Alphabet 公司（Google 母公司）之子公司。

<sup>257</sup> 《自動駕駛載具 3.0 為運輸的未來做好準備》，第 ix 頁，美國交通部。

根據該指引，同時配有自動駕駛功能與傳統配備以供駕駛隨時接手之自動化車輛，是符合現行美國國家公路交通安全管理局（NHTSA）於聯邦層級所制定之安全標準規範。但當未來車輛的自動化程度達到第4級或第5級，即車輛不再配備方向盤、煞車等傳統設備時，則現行的法規便形成阻礙。因此，美國國家公路交通安全管理局正在研擬修正特定安全標準以配合自動車輛技術的發展，以及可能於未來就特定標準設定例外規定。<sup>258</sup>

於此同時，商用運輸車輛之駕駛、營運和維修的主管機關—聯邦汽車運輸安全總署（Federal Motor Carrier Safety Administration），現行對於商用運輸車輛的規範仍以有自然人駕駛為前提，如應定期對駕駛施行藥檢、駕駛須備有商用駕駛執照、不得連續駕駛超過一定時數等等。為因應未來可能的無人運輸車輛上路，聯邦汽車運輸安全總署也擬修正規範，不再預設駕駛為人類，而亦將自動駕駛的情形納入考量。<sup>259</sup>

## （二）德國

2013年11月，德國召開自動駕駛圓桌會議(Runder Tisch Automatisiertes Fahren)，聚集汽車業界、學會、相關團體、政府部門等許多關係人參與集會<sup>260</sup>，就為了自動駕駛發展的設施、法律、技術革新、資訊安全等五個層面進行討論<sup>261</sup>。並立足於該討論結果，於2015年9月發表「自動聯網駕駛戰略（Strategie automatisiertes und vernetztes Fahren）」作為德國車聯網及自動駕駛技術發展之整體方針，透過開發、研究、製造能將自動駕駛的實行成為可能的道路交通4.0（Mobilität 4.0）技術，並以維持德國130年以來於汽車市場的領導地位為目標<sup>262</sup>。

2015年9月，德國以「自動聯網駕駛戰略」為基礎，允許自駕車製造業者、

---

<sup>258</sup> Michele C. Kirrane and Devinder S. Grewal (2016). Civil Liability Arising Out of the Commercial Ownership and Operation of Drones. *For the Defense*, 58(4), 7.

<sup>259</sup> Michele C. Kirrane and Devinder S. Grewal (2016). Civil Liability Arising Out of the Commercial Ownership and Operation of Drones. *For the Defense*, 58(4), 8.

<sup>260</sup> 泉 真樹子，ドイツにおける自動運転車の公道通行—第8次道路交通法改正—外国の立法 275，2018年3月，頁44。

<sup>261</sup> 金岡京子，自動運転と民事責任をめぐるドイツの状況，自動運転と民事責任特集，2017年1月，頁44。

<sup>262</sup> 同前註，頁44。



零件供應商、數位通信業者、IT業者、研究機關等於高速公路 (Autobahn) A9的巴伐利亞自由邦區域進行行駛實驗並蒐集行駛的數據資料，德國政府基於在高速公路上的實證結果，訂定聯邦交通聯網化的標準，並基於此標準，討論將來交通聯網設施的維持、擴建、新設<sup>263</sup>。

2016年10月發表高速公路行駛實驗之中間報告，2016年12月不但為了行駛實驗在高速公路上設置了新的交通號誌，更使四個專案計畫<sup>264</sup>在高速公路和都市道路上完成。

另外，德國所批准的「維也納道路交通公約 (Vienna Convention on Road Traffic)」其中第1條(v)即將駕駛人定義為操縱車輛之人，而未來如果發展到完全自動駕駛，自動駕駛系統就會是真正操縱車輛者，因此德國在「自動化與聯網化駕駛策略」上，亦表明了將會積極參與國際活動以修正維也納道路交通公約之駕駛人定義<sup>265</sup>，在這期間條約新增了第8條5之2項 (Article 8 Paragraph 5bis)以及第39條1項<sup>266</sup>，肯認了自動駕駛系統的技術應用，允許「駕駛人能立即接管駕駛的情況」，並於2016年3月23日生效。維也納條約的修正，可以確保已經使用的行駛支援系統乃至於自動駕駛系統的法律安定性，將可以幫今後自動駕駛系統的開發，所以德國在2016年9月29日將上述維也納條約的修正內容通過成為國內法的法條<sup>267</sup>。

除此之外，德國為了進一步推動道路交通4.0，在2017年3月德國即通過道路交通法修正 (Änderung des Straßenverkehrsgesetzes)，直接修法允許使

---

<sup>263</sup> 同前註，頁44。

<sup>264</sup> 日本國土交通省 (2018)。《自動運転における損害賠償責任に関する研究会—資料1-2 自動運転と民事責任ドイツの状況》。載於：<http://www.mlit.go.jp/common/001174139.pdf>。第一個是"Providentia"，參與者有 Fortiss, BMW 等等，在高速公路以最進步的感應器來確認高度自動化自動車的行駛狀況。第二個計畫是"Digitaler Knoten 4.0"參與者包括 DLR, TU Braunschweig, VW 等等，該計畫在不倫瑞克的實驗道路上測試自動車。第三個計畫是"Veronika"參與者為 Uni und Stadt Kassel，該計畫是為了改善卡瑟爾市之交通，而嘗試將自動車和交通信號聯網化。第四個計畫是"ConVex"，參與者為 Qualcomm, Ericsson, Audi 等等，該計畫則是藉由高速公路上移動通訊 5G 之研究，開發自動車和基地台的整合平台(V2X)。

<sup>265</sup> 金岡京子，自動運転と民事責任をめぐるドイツの状況，自動運転と民事責任特集，2017年1月，頁45。

<sup>266</sup> 新增的第8條5之2項允許自動駕駛系統於得由駕駛人接管或閉關時仍得視為符合該公約同條5項及第13條1項之規定，從而開放搭載自動駕駛系統之車輛上路。第39條1項則是在車輛的技術規定及檢查方面同步放寬自駕車之適用。

<sup>267</sup> 金岡京子，自動運転と民事責任をめぐるドイツの状況，自動運転と民事責任特集，2017年1月，頁45-46。

用部分及高度自駕系統之車輛於公共道路上行駛，並修正相關責任、賠償上限、紀錄及資料保護等規定，其中與道路測試相關者如下：

增加自動車之定義：本次修正案在道路交通法第1條中追加1a條文，許可了「合於規定地使用(bestimmungsgemäß)<sup>268</sup>」具有高度自動駕駛功能或是完全自動駕駛功能之車輛之行為<sup>269</sup>，且該自動化車輛必須符合能夠徹底執行駕駛任務、遵守交通規則、能夠隨時由駕駛人收回控制權、可以辨認駕駛者之需要、能夠透過各種方式通知駕駛人取得控制權、能夠通知不合於系統的指令等要件，正式將高度自動化之自動車納入規範對象。

允許駕駛人分心：高度或完全自動化之駕駛人可以在駕駛中分心，然而新法要求當系統要求駕駛人取回控制或是駕駛人認知到有明顯情事發生使「合於規定地使用」狀態已不復存在時，駕駛人必須立即取回控制<sup>270</sup>。

提高賠償額度<sup>271</sup>：考量到幾乎沒有高度自動化車輛事故的案例，選擇大幅

---

<sup>268</sup> 注意此處「合於規定使用」仍會因車輛自動化程度不一而有不同之要求，例如該系統限於高速公路始得使用，裝置該系統之車輛就禁止在一般道路上行駛。也因為這樣的規定，會課予相關人員提供車輛自動駕駛系統的說明書與裝置用法之義務。詳參第2回自動運転における損害賠償責任に関する研究会，資料1-2自動運転と民事責任ドイツの状況，<http://www.mlit.go.jp/common/001174139.pdf>（2018年10月30日）。

<sup>269</sup> §1a Motor vehicles with highly or fully automated function

(1) The operation of a motor vehicle by means of a highly or fully automated driving function is permissible provided the function is used for its intended purpose.

(2) Motor vehicles with highly or fully automated driving function within meaning of this Act are those which have technical equipment which

1. is able to perform, after activation, the driving task – including longitudinal and lateral control – for the respective motor vehicle (vehicle control),

2. is able to comply with the traffic regulations applicable to the vehicle driving task during highly automated or fully automated driving,

3. can be manually overridden or deactivated by the driver at any time,

4. is able to recognize the necessity of manual vehicle control by the driver,

5. is able to visually, acoustically, tactilely or otherwise perceivably notify the vehicle driver of the requirement to pass vehicle control to the driver with sufficient reserve of time ahead of passing control, and

6. notifies of use that is contrary to the system description.

<sup>270</sup> §1b Rights and responsibilities of the driver when using highly or fully automated driving functions

(1) The driver of the vehicle may turn away his attention from the traffic and the vehicle control when the vehicle is controlled by means of highly or fully automated driving functions according to §1a; he/she must remain sufficiently responsive that he can fulfill his duty under paragraph (2) at any time.

(2) The driver is obligated to take over the vehicle control immediately.

1. when the highly or fully automated system asks him to do so or

2. if he recognizes or, on the basis of obvious circumstances, realizes that the prerequisites for the intended use of the highly or fully automated driving functions no longer exist. 英文翻譯參考 Czarnecki, Krzysztof. (2017). English Translation of the German Road Traffic Act Amendment Regulating the Use of “Motor Vehicles with Highly or Fully Automated Driving Function” from July 17, 2017. 10.13140/RG.2.2.10796.77441.

<sup>271</sup> §12 Maximum Amounts

The person liable to pay compensation is liable

提高高度自動化車輛之損害賠償額度，將對人賠償之總額提高至1000萬歐元，對物賠償之總額則提高至200萬歐元。

強制加裝黑盒子：其他規範上則對高度自動化車輛要求同步紀錄數據，且該紀錄最短應保存三年，如有必要應提供給地方主管機關，第三人如有必要也可以請求提供之<sup>272</sup>。

綜上，德國雖然也有進行道路實測，然而其選擇進行部分地區實測後即修改駕駛人之定義，正式允許搭載部分及高度自動化自動駕駛系統之自駕車上路，至於完全自動駕駛的自駕車能否上路，德國之道路交通法尚未有明文規範。

### (三) 日本

日本和德國一樣，都受有公約規範，只是日本受到拘束的是《日內瓦公約道路交通公約》，該公約中將駕駛人定義為「駕駛道路上車輛之人或現實上控制該等車輛之人」並規定「以每一單位行駛之車輛或是連結車輛，分別都必須要有駕駛者」，明確規定車輛必須要有駕駛人。

而日本國內的道路交通法，雖然未規定車輛一定要有駕駛者，然而第70條卻規定「車輛等的駕駛人，必須要確實操作車輛的方向盤、煞車與其他裝置，且必須因應道路、交通及該車輛等之狀況，以不會對他人造成危害之

---

1. in the event of the death or injury of one or more people by the same event, only up to a total amount of five million euros, and if the damage is caused by the use of highly or fully automated driving in accordance with § 1a, only up to a total of ten million euros; in the case of paid passengers transport, for the holder of the transporting motor vehicles or trailer who is liable to pay compensation for the killing or injury of more than eight passengers, that amount shall be increased by 600000 euros for each additional person killed or injured;

2. in the event of damage to property, even if several things are damaged by the same event, only up to a total amount of one million euros, if the damage is caused by the use of a highly or fully automated driving function in accordance with § 1a, only up to an amount of a total two million euros.

The maximum amounts according to sentence (1) 1. also apply to the net present value of a pension to be paid as compensation.

英文翻譯參考 Czarnecki, Krzysztof. (2017). English Translation of the German Road Traffic Act Amendment Regulating the Use of “Motor Vehicles with Highly or Fully Automated Driving Function” from July 17, 2017. 10.13140/RG.2.2.10796.77441.

<sup>272</sup> 第三人可請求提供行駛數據之情況為因為事故關係而有法律關係之主張、請求、免責、防禦且該事故與配備自動駕駛機制之車輛有所關係之情形。日本國土交通省（2018），《自動運転における損害賠償責任に関する研究会，資料 1-2 自動運転と民事責任ドイツの状況》，<http://www.mlit.go.jp/common/001174139.pdf>。

速度、方法行駛」<sup>273</sup>，從這樣的規定來看，日本的道路交通法也是以車輛內有駕駛人作為前提<sup>274</sup>，因此日本的自駕車除非符合法律規範，否則不能直接上路。

2016年6月日本警察廳公布《自動駕駛汽車道路測試指南》（自動走行システムに関する公道実証実験のためのガイドライン），其中規定符合道路運送車輛之安全基準的實驗車輛、駕駛人經常監視駕駛狀況並確保不會造成他人危害、遵守以道路交通法為首的相關法令等要件者，可以進行道路實驗<sup>275</sup>。

2017年6月1日，日本警察廳公布「遠程自動駕駛系統道路測試許可處理基準」（遠隔型自動運転システムの公道実証実験に係る道路使用許可の申請に対する取扱いの基準），規範申請、實施場所、日期、確保安全之措施、遠距型自駕系統等之構造、緊急措施、審查基準等等，以實用化無人車（遠距操作）之路測<sup>276</sup>。但有學者提出，即便遠距型自駕車沒有違反日內瓦公約之約定，但一旦發展到完全自動化的自駕車層級，仍必須要考量到與日內瓦公約的齟齬關係<sup>277</sup>。

2018年4月，日本IT綜合戰略本部公布「自動駕駛制度整備大綱（自動運転に係る制度整備大綱）」，以道路實證等技術動向，與目前為止各省廳的實行結果，進行整體的檢討，並揭示從2020至2025年間自駕車相關道路交通法規修正及施政方向，其中檢討的政策包括：自駕車適用的環境條件設定與安全性的擔保、如何確保安全的一體性、如何確保自駕車本身的安全性、交通法令檢討、責任關係等等<sup>278</sup>。

---

<sup>273</sup> 車両等の運転者は、当該車両等のハンドル、ブレーキその他の装置を確実に操作し、かつ、道路、交通及び当該車両等の状況に応じ、他人に危害を及ぼさないような速度と方法で運転しなければならない。

<sup>274</sup> 島田里奈，自動運転者をめぐる法律問題，企業会計，69期，2017年，頁138-139。

<sup>275</sup> 自動走行システムに関する公道実証実験のためのガイドライン，頁1，

<https://www.npa.go.jp/bureau/traffic/selfdriving/index.html>。

<sup>276</sup> 「遠隔型自動運転システムの公道実証実験に係る道路使用許可の申請に対する取扱いの基準」の策定について（通達），<https://www.npa.go.jp/laws/notification/koutuu.html#kouki>。

<sup>277</sup> 島田里奈，自動運転者をめぐる法律問題，企業会計，69期，2017年，頁139。

<sup>278</sup> 自動運転に係る制度整備大綱，頁1-22。

2017年12月8日決定之「新經濟政策方案(新しい經濟政策パッケージ)」中，提及自動車、小型無人機等未來技術將會帶來第四次產業革命，為了能夠實現2022年自動車全面的商業化，有必要再進行自動車的實驗，並共享實驗結果，另外小型無人機可以對在沒有輔助者的情況下進行安全的貨物配送，可以提高其在產業的運用率<sup>279</sup>。故而新經濟政策方案提出限定領域及跨部會橫向推進體制之「專案型管制沙盒」及地域限定型「國家戰略特區型管制沙盒」，作為新型科技的實驗平台<sup>280</sup>。

#### (四) 英國

英國政府於2017年2月推出《汽車技術與航空法案》(Vehicle Technology and Aviation Bill)，將原本汽車的強制性保險擴大至自動車，規定自動車的交通事故產生的損失主要由保險公司負責<sup>281</sup>，英國保險協會(Association of British Insurers)亦積極推動自動駕駛相關保險機制。同年8月，英國又推出《車聯網與和自動駕駛汽車網路安全準則》(The key principles of vehicle cyber security for connected and automated vehicles)，提出自動駕駛軟體系統安全和數據安全等八大準則，並宣布2021年全面允許自動車合法上路<sup>282</sup>。雖然《汽車技術與航空法案》因為國會重組而夭折，其基本理念已被2018年7月通過成為法律之《自動駕駛和電動車輛法案2018》(The Automated and Electric Vehicles Act 2018)所吸收，而此法案制定的目的係為「消弭繁文縟節，並制定得使創新蓬勃發展的法律框架」<sup>283</sup>。

#### (五) 澳洲

澳洲國家交通委員會(National Transport Commission)於2018年5月提出「修正駕駛法律以支持自動駕駛車輛政策白皮書」(Changing driving laws

<sup>279</sup> 內閣府，新しい經濟政策パッケージ，[http://www5.cao.go.jp/keizai1/package/20171208\\_package.pdf](http://www5.cao.go.jp/keizai1/package/20171208_package.pdf) (最後瀏覽日：2018年8月30日)。

<sup>280</sup> 林美鳳(2018)，〈產業創新與管制革新—日本國家戰略特區制度等之啟示〉，《科技法律透析》，30卷4期，頁63。

<sup>281</sup> 《Vehicle Technology and Aviation Bill》，PART 1 AUTOMATED VEHICLES: LIABILITY OF INSURERS ETC

<sup>282</sup> 陶盈(2018)，〈自動駕駛車輛交通事故損害賠償責任探析〉，《湖南大學學報》，32卷3期，頁137。

<sup>283</sup> Automated and Electric Vehicles Bill 2017-19, Louise Butcher and Tim Edmonds, House of Commons Library, p.4.

to support automated vehicles\_Policy paper），該文件內容中指出，於2016年11月澳洲交通主管機關便已研擬建立自駕系統實體（Automated Driving System Entities, ADSEs）的法律義務體系。然而，其法規要解決的核心問題，便在於澳洲的交通法規中預設了人類駕駛的存在。<sup>284</sup>因依照目前科技，人類須負的駕駛責任無法完全轉換至由自駕系統實體來負擔，法律中也並未明確定義自駕車中的「控制」和「適當控制」，因此該討論文件中提出應該擴張法律中駕駛人之定義，並為駕駛人創造新的「隨時準備駕駛義務」（Readiness-to-drive obligations），以確保駕駛人保有當自動駕駛失靈時取代自動駕駛的警覺性<sup>285</sup>。惟當自動駕駛車輛屬於高度完全自動駕駛時（即自動化程度達到第4級或第5級），駕駛人的隨時準備駕駛義務應被免除<sup>286</sup>。

## 二、 主要國家自動駕駛模式下民事責任的安排相關法令趨勢

### （一）美國

在自動駕駛的責任分配上，美國內華達州透過道路測試之許可證，僅對購買不低於500萬美元之保險或相當金額之企業發放許可制，來確保道路測試之主體有足夠財力能夠負擔自動駕駛事故之損害賠償責任。美國加州亦規定在公用道路上行駛自動駕駛汽車，需要獲得主管機關發行的其他證照，並購買保險，亦即如須將自動車作道路測試以外之他用，須購買其他相對應之保險來填補可能發生之損害。

但美國民事侵權法係由各州制定，因此可能產生各州對於自動駕駛汽車民事責任認定的不一致情況<sup>287</sup>。其中一個解決方向，是由聯邦機關美國國家公路交通安全管理局就自動駕駛汽車訂立全國統一的安全標準，從而按照美國各州民事法院的運作習慣，通常會將違反行政規範上安全標準認定係有侵權法上的重大過失。如此一來，藉由統一聯邦層級的自動駕駛汽車安

---

<sup>284</sup> Changing driving laws to support automated vehicles\_Policy paper, p.1

<sup>285</sup> 柯亦儒（2017），〈澳洲國家交通委員會提出自駕車試驗指南〉，《科技法律透析》，29卷11期，頁17-18; Changing driving laws to support automated vehicles\_Policy paper, p.52-55

<sup>286</sup> Changing driving laws to support automated vehicles\_Policy paper, p.12, 35

<sup>287</sup> A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation, Mark.A. Geistfeld, p.34-40

全標準，各州民事責任判斷標準亦將逐漸受聯邦法律調和而漸趨一致。<sup>288</sup>

另外，當自動駕駛汽車之行駛造成他人損害時，民事責任的有無係以該肇事車輛是否有商品瑕疵為判準。然而，商品瑕疵是否存在，並非法院專業職能所能判斷範圍而須仰賴專家學者出具意見，導致此一爭議最終往往演變成鑑定專家之間的戰爭<sup>289</sup>。為解決此狀況，有學者建議以下幾種解決方案：1.建立無過失責任制度（non-fault system）：由駕駛為其車輛投保無過失責任險，或由政府擔任無過失責任之保險人，並對自動駕駛車輛銷售額課稅以負擔支出的保費。2.延伸現有航空器、船隻自動導航的規範：按美國現行之規定，於自動導航時發生損害於他人，如使用人使用導航系統無過失，則航空器與船隻之自動導航製造商須為其負責。而於自動駕駛汽車之情況，亦得適用相關法令。3.將「理性自然人」(reasonable man)的判準適用在自動駕駛的軟體上：亦即如自動駕駛軟體的表現符合理性自然人的標準，則屬製造商無責任。此標準對於自動駕駛汽車的製造商而言應較可預測。4.類似Price-Anderson法案的責任(Price-Anderson Act)：該法案規定由核電廠的所有人每年按反應爐的數量繳納一定的保費給私人保險公司，做為核子事故發生時的預備保險金。

## (二)德國

德國基於自動駕駛圓桌會議之討論發表《自動聯網駕駛戰略》，該策略中介紹聯邦交通與數位基礎設施部於2014年所做的預測，但是究竟該如何具體因應新技術的衝擊，仍有許多爭論。於是於2016年9月，聯邦交通與數位基礎設施部的官員德布林（Alexander Dobrindt）為了提出與自動駕駛相關新技術的倫理規範，而設立了「自動駕駛倫理委員會」，指名由前聯邦憲法法院法官擔任委員長，聚集了學會、汽車產業、數位經濟等多種領域的專業人士，並於2017年6月提出《自動駕駛規劃系統指引》報告，其中總結20項自動駕駛及聯網車輛的倫理規則(Ethical rules for automated and connected vehicular traffic)，規則中認為法律責任規定及司法實務認定必須充分考量未來駕駛人責任轉至自動及聯網化系統製造商，或技術系統營運

<sup>288</sup> 同前註，第 40-45 頁。

<sup>289</sup> Automated Vehicle Lawsuits (How Will We Litigate the Auto Crash of the Future), Brett A. Ross, p.5

商之情形。

德國現行民事法律責任規定主要有民法侵權責任<sup>290</sup>、道路交通法上責任（包括車輛所有人、駕駛人及製造商）<sup>291</sup>及製造物責任法上責任<sup>292</sup>。另汽車所有人依法亦需必須加入強制責任險，當被害之第三人向汽車所有人或駕駛人請求賠償時，被害人的損害要由強制責任險來填補，被害人可以依照保險契約法第115條第1項第1款向保險人直接請求<sup>293</sup>。

就自駕車所引發的民事法律責任來說，德國現行法令對自動駕駛模式下民事責任的安排仍舊維持既存的歸責模式，即從車輛所有人、駕駛人、製造商及保險規範三個面向來因應。

### 1. 車輛所有人及駕駛人

德國並未修正道路交通法第7條之責任分配模式，有學者認為原因第7條對車輛所有人之規範本身是危險責任，故即可涵蓋所有自駕車的情境，毋須因應自動駕駛而特別加入新的危險要件。至於道路交通法第18條之駕駛人責任，在部分自動駕駛的階段仍可正常適用。但是在駕

<sup>290</sup> 德國民法第823條第1項為侵權行為之規定，即以故意或過失不法侵害之侵權行為原則為判斷。

<sup>291</sup> 德國道路交通法第7條規定車輛所有人須負擔運行危險(Betriebsgefahr)，只有在不可抗力之時始可免責，而所謂的車輛所有人，依照德國已確定之法院見解，即為了自己而使用且具有使用車輛之必要權限之。第7條第1項的所有人責任，是指不論其有無過失的危險責任(Gefährdungshaftung)，第7條第2項則是除不可抗力以外，車輛所有人必須就車輛的性能缺陷以及技術裝置的不恰當所造成的事故負責。

道路交通法第18條第1項前段則規定了與第7條相同情況下的駕駛人責任，第18條第1項後段則規定了如果駕駛人可以證明該損害並非係因為駕駛人之過失，則駕駛人就該損害不負責。因此道路交通法上的駕駛人責任並非如所有人一樣是危險責任，而是推定駕駛人的過失，由駕駛人就其過失不存在負舉證責任。例如駕駛人能夠證明雖然已經正常駕駛，卻因為技術裝置之不作用而造成事故發生，可以認為駕駛人不存在過失。道路交通法第12條修正後提高了對人及對物之賠償責任上限，在一事故中造成一人或數人死亡或受傷者，賠償總額為500萬歐元。因營業利益之運送造成超過8人死傷者，每超過一人增加60萬歐元；一事故造成複數之物損害之情形，物損部分賠償總額為100萬歐元。而對於超過道路交通法第12條上限之損害則是由駕駛人依民法第823條負損害賠償責任。

而瑕疵製造物的製造商可能也會因此負民法823條第1項的製造商責任(Produzentenhaftung)，因為製造者的監督義務(Produktbeobachtungspflicht)要求製造者監督流通後的製造物，並依其需求採取適當措施，這是製造者的社會生活義務。

<sup>292</sup> 德國製造物責任法第1條第1項前段規定，因製造物之缺陷致生損害於他人生命、身體、健康、物者，就他人之損害負賠償責任。製造物責任法規範的製造人責任，即危險責任。製造物責任法第3條第1項當製造物欠缺通常應具有之安全性即可認為有瑕疵，又將瑕疵區分為設計上欠缺、製造上欠缺、指示警告上之欠缺三種。製造物責任法中人身損害賠償責任之上限為8500萬歐元。

<sup>293</sup> 金岡京子，自動運転と民事責任をめぐるドイツの状況，自動運転と民事責任 特集，2017年1月，頁47。



駛人毋須持續監視車輛運行的高度與完全自動化階段，就會產生適用上的問題，但因科技還在發展之階段，德國尚無改變目前的責任分配原則之立法動向。

## 2. 製造商

德國學說認為自動駕駛系統的製造者是透過控制軟體程式而對與駕駛相關的本質上技術裝置產生事實上重大之影響，雖然自動駕駛系統都是標準化的模式，但是因為與自駕車的運行相當有關，故有力說認為可以將系統製造者也認為是駕駛人的一種，而必須負擔駕駛人責任<sup>294</sup>。

在部分自動化的車輛，因為駕駛人必須時常監視車輛行駛，必要時由駕駛人接管車輛，故如果自動駕駛系統未發出接管警告或是在錯誤時點發出接管警告，此時就會由製造商負責。如果是在高度自動化的車輛，駕駛人毋須隨時隨地監控車輛，此時如自動駕駛系統誤解狀況而做出錯誤判斷，亦是由製造商加以負責。但另一方面也必須考量到製造商製造的軟體使用期限較短，如果課予製造商太長的監督義務是否對製造商要求過苛？在高度或完全自動化的車輛，製造商必須設計出能夠對應所有可能發生狀況的自動駕駛系統，而當一個「駕駛人毋須注意亦毋須監視車道和系統的系統」被定義為好的系統，只要無法證明該事故是「僅」因為其他第三人所造成的情況，製造商都必須要負責<sup>295</sup>。

學者認為，真正會造成駕駛人與製造商責任無法釐清的狀況是很少的，當有足夠的時間卻沒有將系統的問題修正而發生事故的情況，駕駛人是沒有過失的，而設計出沒辦法迴避該等情況的系統的製造商須負製造商責任。因此，自動駕駛系統在駕駛中所發生的事故，原則上是以製造商為損害賠償請求的對象。但對於部分自動化的車輛，則很有可能駕駛人的過失和駕駛系統的瑕疵都是事故發生的原因（例如駕駛人

<sup>294</sup> 同前註，頁 48。

<sup>295</sup> 第 2 回自動運転における損害賠償責任に関する研究会，資料 1-2 自動運転と民事責任ドイツの状況，<http://www.mlit.go.jp/common/001174139.pdf>（2018 年 11 月 23 日）。

分心而自動駕駛系統的警告接管並未作用)，此時很有可能因為駕駛人並未注意路況而無法確切記得事故發生經過，因此事故幾秒前的數據保存是相當重要的，駕駛人人為介入的駕駛過程應該要數據化並保留在車輛內<sup>296</sup>。

### 3. 汽車強制責任險

2016年5月25日，德國保險協會發表了這樣的見解：「汽車的強制責任險，當然也擔保自動駕駛。因為自動駕駛系統而發生事故，仍會維持由保險來填補被害人損害的模式」<sup>297</sup>。

當駕駛人有過失時，只要駕駛人沒有肇事逃逸、酒駕等義務違反，原則上保險人都可以向駕駛人求償。如果是因為車輛有瑕疵而發生事故時，保險人必須要證明車輛的瑕疵或是製造者的過失才能夠求償。而其他瑕疵的情形，例如駭客入侵導致自駕車的軟體程式變更的情況，除非行為人被逮捕而能夠證明該行為且行為人有償付能力時，保險人才能夠和行為人求償<sup>298</sup>。

如上述，既然汽車強制責任險可以涵蓋自動駕駛的範圍，對駕駛人和車輛所有人來說汽車強制責任險的填補範圍就不會改變，但是對於汽車製造來說，因為較以往的汽車，自動駕駛的汽車製造商更容易負製造商責任，所以如果維持過往的汽車強制責任險保險費，對汽車製造商來說應該是一個優點<sup>299</sup>。

### (三) 日本

日本亦為以既有歸責原則為基礎進行檢討之國家，日本既有的歸責制度與我國一樣，於民法上有侵權行為<sup>300</sup>、雇主責任、製造物責任法上製造者責

<sup>296</sup> 金岡京子，自動運転と民事責任をめぐるドイツの状況，自動運転と民事責任 特集，2017年1月，頁49。

<sup>297</sup> 同前註，頁49。

<sup>298</sup> 同前註，頁49。

<sup>299</sup> 同前註，頁49。

<sup>300</sup> 日本民法第709條有如我國相類似的侵權行為規範：「因故意或過失不法侵害他人或法律上保護之利益者，就其所生之損害負損害賠償責任。」採取一般過失責任，但因為日本尚有訂定汽車損害賠償保障法，故就交通事故的損害賠償，一般而言會先適用汽車損害賠償法，以加強對交通事故被害人之保護。

任<sup>301</sup>之規範及汽車損害賠償保障法(日文原文為「自動車損害賠償保障法」,以下簡稱「自賠法」)<sup>302</sup>中強制責任保險之規定。

就自駕車所引發的民事法律責任來說,目前日本均未為了因應自動駕駛而修改任何法律。

在日本提出的自動駕駛制度整備大綱中有檢討責任關係的分配,該大綱認為因為使用自動駕駛系統所生之損害,仍維持原本的運行供用者責任,但是可能必須要採用由保險公司先賠償以確保對自駕車製造者的求償權。而對於因為駭客而發生的事故則認為以政府保障事業因應較為妥當,但如果自駕車的所有人並沒有盡到系統安全的維持義務則仍應由所有人負責。

另外有學者認為等級4以上之自動車,駕駛人即使仍坐在車子上,但其已經對駕駛任務的涉入甚少了,因此自賠法上所謂「運行供用者」的概念不能適用在駕駛人身上,而有必要就等級4以上之車子重新建構新的責任模式<sup>303</sup>,但對此亦有學者認為,依照日本實務見解對於「運行供用者」所下之定義,運行供用者為「運行支配與運行利益之歸屬者」,故即便發展到完全自動模式,固有的「運行支配與運行利益歸屬於某一人身上」之概念

---

<sup>301</sup> 日本的製造物責任法第3條規定:「製造業者等製造、加工、輸入或交付依前條第三項第二款或第三款表示其姓名之製造品,因其瑕疵而侵害人之生命、身體財產者,就其所生之損害負損害賠償責任。惟僅損害該製造物者,不在此限。」且該瑕疵的定義為「欠缺該製造物通常應具備之安全性」。由此規定可知,製造物責任法排除了自損的情況,故而車輛因為瑕疵而自損之情況只能回歸民法第709之侵權行為適用。

<sup>302</sup> 日本為保障汽車所造成的人身損害都可以獲得賠償與保護被害人,並有助於汽車運輸之健全發展,訂定「汽車損害賠償保障法」

- 運行:自賠法第2條第2款中規定所謂的「運行」,即「不論是否運送人或物品,將汽車以該裝置之使用方法所使用之行為」。
- 運行供用者:自賠法第3條即規定運行供用者之責任,即「為自己而提供汽車之運行者,因該運行而侵害他人生命或身體時,就因此而生之損害負賠償責任。惟自己以及駕駛人並未疏於注意汽車運行、被害人或駕駛人以外之第三人有故意或過失,以及證明汽車有構造上之欠缺或功能障礙者,不在此限。」,依「自賠法」第3條之文義,運行提供者必須要證明以下三個要件始得免責:1.運行提供者與駕駛人均為疏於注意汽車運行;2.被害人或駕駛人以外之第三人有故意或過失;3.能夠證明汽車有構造上之欠缺或功能障礙。有認為因為第3條課予運行提供者相當高之舉證責任,故而,第3條之規定等於課予運行供用者「實質無過失責任」。
- 責任保險:自賠法第5條即規定汽車如未就其相關法律所定之汽車損害賠償責任保險(下稱責任保險)或汽車損害賠償責任共同分擔制度(下稱「責任分擔」)訂立契約,則不得供作行駛之用。但是該責任保險只限於對人損害之賠償,被害人死亡之情形一個人的賠償額度上限為3000萬日圓。

<sup>303</sup> 福田弥夫,自動運転と損害賠償責任,最近の調査研究から,2016年2016卷,頁37。

仍可適用，故自動駕駛可以適用自賠法<sup>304</sup>。

#### (四) 英國

在英國，根據the Road Traffic Act 1988第143條，車輛皆應投保第三人責任險<sup>305</sup>，除特定例外情形。而原先一般車輛發生因駕駛過失而對第三人發生損害時的處理模式，便是由保險公司先行理賠；倘若該肇事車輛不適用且未投保第三人責任險，則由因過失而可歸責的駕駛負責賠償；如該駕駛無法提供受害者補償時，則由汽車保險局（the Motor Insurers' Bureau）做為保險人。然而，上開傳統情形並不全然適用於自動駕駛汽車。因為汽車得以自動駕駛，汽車的駕駛的身分可能是不可歸責的乘客，端看該汽車於發生事故當下是否處於自動駕駛的狀態中。因此，本法案規定如汽車於發生事故時是處於自動駕駛（driving itself）的狀態，則將第三人責任保險的涵蓋範圍擴張至駕駛自身，就自動駕駛車輛技術問題產生的事故，也研擬將之納入強制保險範圍內<sup>306</sup>，亦即車輛在自我駕駛之模式下，司機（更精確地來說，此時可能是乘客）所遭受的人身損害也在承保範圍內。同時，倘該自動駕駛的車輛屬於例外無須投保第三人責任險的車輛，於自動駕駛中發生意外，則由汽車所有人負責賠償<sup>307</sup>。另外亦設計了追償制度，如保險公司出面承擔損害填補，對損害的發生負有責任的第三人須對保險公司負同等責任，表面上看似係對保險公司不利之制度，但保險公司可以透過拒絕承保來篩選車輛製造商<sup>308</sup>。

#### (五) 歐盟

歐盟雖就自動化汽車與無人機尚未提出法律意見，但從歐洲議會法律事務委員會（European Parliament's Committee on Legal Affairs）於2016年5月31日提出之歐洲民法對機器人之規範（European Civil Law Rules in Robotics）研究，或許能對其就AI與自動化議題的態度窺知一二。研究論及，未來是

<sup>304</sup> 藤田友敬，自動運転と運行供用者の責任，ジュリスト自動運転と民事責任，頁24。

<sup>305</sup> The Road Traffic Act, Section 143

<sup>306</sup> 蔡毓華（2018），〈英國因應自動駕駛車輛上路，提出新保險責任制度〉，《科技法律透析》，30卷3期，頁13。

<sup>307</sup> Automated and Electric Vehicles Bill 2018 Section 2.

<sup>308</sup> 騰訊研究院法律研究中心，2018年全球自動駕駛法律政策研究報告，2018年5月，頁26。

否應將機器人做為法律主體（legal entity）看待？該研究報告的結論是否定的，認為在自動化機器人造成損害而應賠償的部分，仍會與民法相衝突<sup>309</sup>。同時，該報告就自動化機器人造成損害時賠償責任歸屬，提出以下幾個選項<sup>310</sup>：1. 如該機器人販售時配備的是開源軟體（open source software），則編寫該應用程式的人應負損賠責任；2. 如機器人造成損害的原因可追溯至其設計或製造，則設計人或製造者應負責；3. 如機器人是在使用或仍在學習中，則其使用者或所有人應負責。

### 第三項 針對我國法規調適之初步建議

#### 一、關於我國自駕車的上路測試規範之觀察與建議

依我國「道路交通安全規則」第2條規定汽車係指「指在道路上不依軌道或電力架線而以原動機行駛之車輛（包括機車）」。另依我國「公路法」第2條規定汽車係指「指非依軌道或電力架設，而以原動機行駛之車輛」。兩者乍看之下似皆未規定我國行駛汽車以「駕駛人」為必要，然而細究道路交通安全規則，仍會發現其設想之汽車駕駛仍係以「駕駛人存在」為前提，例如道路交通安全規則第94條第3項、第104條、第104之1條等規定即明白規定駕駛人行駛應注意事項。

但我國並未選擇直接修改相關法令讓自駕車可以直接上路測試（如德國），亦未針對自駕車發展公布相關倫理原則及安全標準指引（如美國、德國、日本），而是針對自駕車道路測試與商用安全監理，引進監理沙盒的概念<sup>311</sup>。就此，我

---

<sup>309</sup> European Civil law rules in robotics, Policy Department C: Citizens' Rights and Constitutional Affairs, p.14-16

<sup>310</sup> European Civil law rules in robotics, Policy Department C: Citizens' Rights and Constitutional Affairs, p.17

<sup>311</sup> 如本節第二項第三款（日本）所述，日本於自駕車上路測試與商用方面亦有引進監理沙盒的概念，其制度分為地域限定型及專案型兩種。其中地域限定型監理沙盒是在國家戰略特區法修正案導入的，雖係以自駕車、無人機及與兩者相關之無線電頻率利用的創新實驗為對象，但係由地方自治體作為主體進行提案，故與我國2018年11月30日三讀通過之無人載具科技創新實驗條例的推動層級（企業）不同。相對地，日本於2018年6月6日起施行的生產性向上特別措施法（又稱「生產性革命法」）導入的專案型監理沙盒，則與我國無人載具科技創新實驗條例大致相同，僅有以下幾點不同：

一、適用對象：該專案型監理沙盒係屬泛用型監理沙盒，相對於我國以無人載具為適用對象，其不限於特定領域，只要是新技術、新作法，經審核其創新性通過後，就能進入專案型監理沙盒。

二、主管機關：日本為該專案型監理沙盒於內閣官房設置跨部門的單一窗口，提供一企業與目的事業、法令主管機關間便捷溝通的管道，而我國雖統一由經濟部作為主管機關，但相應於層級不同，將來跨部會協調、推動上可能會比較辛苦。

三、退場機制：生產性革命法第20條要求主管機關應評估實驗中法令排除措施、外國相同管制情形及技術發展情形等，並按其評估結果廢止或放寬管制上所必要法律或其他措施，而我國無人載具科技創新實

國推出了兩部管理條例草案，一部是「自動駕駛車輛測試管理條例」，於2017年10月27日提出，另一部草案為「無人載具科技創新實驗條例草案」，於2018年5月17日經行政院通過，送請立法院審議。其中無人載具科技創新實驗條例草案並於2018年11月30日經立法三讀通過，並於同年12月19日經總統制定公布，惟尚另需由行政院指定施行日期。因「無人載具科技創新實驗條例」不只包含自動駕駛車輛，尚包含無人機、無人船等陸海空三種智慧載具，因此以下係以「無人載具科技創新實驗條例」為我國觀察與建議的主要對象。

無人載具科技創新實驗條例<sup>312</sup>的簡要內容整理如下表：

條項	項目	摘要
第一條	立法目的	為了鼓勵無人載具之研究發展，並建構完善之實驗環境
第二條	主管機關	經濟部
第三條	名詞定義	無人載具包括車輛、船舶、航空器，並須具備感測技術、定位技術、監控技術、決策及控制技術
第四條	專業單位	經濟部得由專責單位辦理實驗相關事宜
第五條	申請程序	申請計畫需包含創新性說明、與其他交通法規適用分析、範圍、期間、規模、主要管理者、效益、退場機制、無人載具安全說明、保險等等
第六條	審查程序	審查計畫會議應包括法律專家與無人載具產業專家

驗條例並未明訂主管機關法令調適之義務，僅於第9條規定，若中央目的事業主管機關認有修法必要時，創新實驗延展不以一次為限。

<sup>312</sup> 有關消費者保護事宜，於國家發展委員會107年12月14日「人工智慧之相關法規國際發展趨勢與因應」委託研究計畫期末報告審查會，有專家意見指出雖然同樣引進監理沙盒概念，惟無人載具科技創新實驗條例並未如同金融科技發展與創新實驗條例一樣特別針對消費者設置特別規定（第21條至第24條規定）是否可能存在對於消費者保護不足之情形。針對此一疑問，基於以下兩點理由，本報告認為尚無需於無人載具科技創新實驗條例追加類似之保護規定。第一、兩項條例皆要求申請人應與實驗參與者訂立契約。且，無人載具科技創新實驗條例亦已於第18條第1項及第2項明訂「申請人與參與實驗者於創新實驗期間訂定參與實驗契約，應本於公平合理、平等互惠及誠信原則。」、「前項契約條款顯失公平者，該部分條款無效；契約條款如有疑義時，應為有利於參與實驗者之解釋。」，已與金融科技發展與創新實驗條例第21條相當。第二、因金融科技發展與創新實驗條例之參與者因非屬金融消費者保護法所適用之金融消費者（申請人非該條例所規定之金融服務業），故需於同法第21條至第24條訂定同等（金融消費者保護法第7條及第8條）或準用（金融消費者保護法第11條、12條及13條第2項等）之規定。惟無人載具科技創新實驗條例之參與者，若屬商用測試之消費者，亦係以消費為目的而使用自駕車或接受自駕車相關服務，亦得直接適用消費者保護法或公平交易法中有關廣告之規定等，故亦無於同條例重為規定之必要。

條項	項目	摘要
第七條	審查項目	經濟部須審查是否具有創新性、依現行法規無法取得目的事業主管機關許可或核准之範疇、於開放性場域實驗之可行性、可有效提升交通效率、已提出相關交通措施、已評估潛在風險、建置保護措施等等
第八條	審查時間	六十天內完成審查。經濟部得變更計畫內容。
第九條	計畫期間	計畫期間以一年為限，得延展一次，不得逾一年。
第十條	變更	計畫不得變更。但無重大影響之事項，得向經濟部申請核准變更後變更。
第十一條	公開資訊	經濟部應公開計畫相關資訊於網站上
第十二條	免徵規費	計畫申請、核准等事項免徵規費
第十三條	場域管理	實驗運用之無線電頻率與範圍、期限與其他條件由經濟部公告
第十四條	監督	申請人要向經濟部說明實驗情形，經濟部得實地訪查。申請人應保留實驗資料至少三年。
第十五條	申請人之義務	申請人於測試前應於媒體或電子網站公告，並於無人載具或實驗場域以適當方式告示。 發生事故時申請人應負賠償責任並主動通報經濟部。
第十六條	資安措施	申請人應採取資訊安全措施
第十七條	個人資料	申請人應遵守個人資料保護法之規定
第十八條	實驗契約	申請人訂立之實驗契約要符合公平與誠信原則
第十九條	辦理實驗	申請人應於核准決定送達次日起開始辦理實驗，並於測試前書面通知經濟部
第二十條	限期改善事由	如有不利交通服務、逾越計畫範圍、妨害善良風俗、危害人身或財產安全等情事者，經濟部得命限期改善
第二十一條	實驗報告	申請人於辦理實驗期間屆滿後三十日內應將創新實驗報告函報經濟部。報告內容應包含實驗過程與結果、風險發生與事故通報紀錄、人為介入無人載具

條項	項目	摘要
		控制權次數與原因等等
第二十二條	排除適用之法規	實驗期間排除適用之法規。惟不排除洗錢防制法、資恐防制法與相關法規。
第二十三條	排除法規	經濟部得基於實驗之必要決定排除法律、法規命令或行政規則
第二十四條	施行日期	由行政院定之

由上述簡要介紹可知，無人載具科技創新實驗條例是採取個案申請之方式，經主管機關許可後於某一特定場域實施測試，其中亦有注意到智慧載具會發生的資安風險、個人資料保護等問題，以及為了將來產業發展與日後責任分配風險產生，有保留數據之必要，且明文排除了實驗期間我國對汽車監理的規定包括道路交通管理處罰條例的車輛設備檢驗要求、駕照與執業登記、通訊行為、非屬汽車之動力載具、連續駕車、交通指揮與道路號誌、記點等規定，並保留了給予主管機關裁量個案排除適用法規之權限，故可認為無人載具科技創新實驗條例之方向值得贊同。

惟該條例後續仍須待主管機關公布相關辦法與作業程序，本報告認為尚有其他方面的法規政策待齊備，以下分述之：

(一)資料運用：無人載具科技創新實驗條例第21條規定，申請人於核准實驗期間屆滿後三十日內，應將創新實驗報告，函報主管機關，其中包括創新實驗歷程及結果、風險發生與事故通報紀錄、人為介入無人載具控制權次數及原因紀錄及其他主管機關指定之事項。至於在實驗期間，依照該條例第14條，需依照主管機關指示說明創新實驗情形，並基於主管機關對實驗安全性評估之目的每月應通報人為介入控制權次數及原因，此外條例中並無其他明文規定要求需隨時將實驗紀錄或資料揭露予主管機關。然而，縱使如此，實驗後函報義務的規定仍可能會對產業進步有所限制，且該條例已授權主管機關得另行指定其他函報事項。在要求數據揭露時，除安全或政策目的外，也必須考量到對廠商本身營業秘密保護的衝擊，及衍生的搭便車行為可能削弱廠商參與實驗的意願等，此具體衡平措施則有待於主管機



關於日後規則訂定實施辦法為之。

(二)法規調適：無人載具科技創新實驗條例第22條規定，申請人得經過主管機關核准，於實驗期間排除該等法規命令或行政規則全部或一部之適用。並經由主管機關公告得排除適用之法律，包括公路法、道路交通管理處罰條例、船舶法、民用航空法等。然而如上所述，道路交通安全規則、道路交通管理處罰條例其實都是以存在駕駛人為前提所訂定，即使實驗期間毋須適用該等法規，然實驗期間結束後如何與既存法規為調適及法規調適能夠趕上業者商用化需求仍為一個重要的議題。

(三)風險分配：無人載具科技創新實驗條例第22條第2項第7款明確規定「其他因無人載具科技之研究發展及應用需排除適用之法律。但不包括民事、刑事責任規定」，即法規的免除適用不影響自駕車的民刑事責任分配，亦即自駕車如在實驗當中發生事故，民事責任部分仍須回歸民法、消費者保護法為適用。就此該條例似乎是採取既有歸責原則已可以處理之立場，從而接近日本與德國的模式。但就不同層級之自駕車如何適用既有的責任規範架構則有待檢討，故本報告在後部分將詳述現行民事責任對自駕車的歸責處理與配套。

## 二、關於我國自動駕駛模式下民事責任安排之觀察與建議

我國並未就自動駕駛車輛修改任何法條，且無人載具科技創新實驗條例第22條第2項第7款規定：「其他因無人載具科技之研究發展及應用需排除適用之法律。但不包括民事、刑事責任規定」，已明文說明該實驗條例不排除相關民刑事責任，故而就無人載具因為創新實驗而造成的民事責任分配，仍係回歸於民法的侵權責任<sup>313</sup>、消費者保護法產品責任<sup>314</sup>及汽車強制責任法的強制責任保險

---

<sup>313</sup> 我國民法第184條第1項前段規定：「因故意或過失，不法侵害他人之權利者，負損害賠償責任。」即以行為人故意過失為前提認定其侵權行為之損害賠償責任。

又民法第191條之1規定商品之製造、生產、加工業者因其商品之通常使用或消費所致他人之損害，負賠償責任，且民法第191條之1是推定過失、推定瑕疵、推定因果關係之規範，商品製造人須負舉證責任，證明商品之生產、製造或加工設計並無欠缺（瑕疵不存在），或其損害與該項欠缺之間欠缺因果關係（因果關係不存在），或自己就防止損害之發生，已盡相當之注意（無過失）。

又民法第191條之2規定了動力車駕駛人之特殊侵權責任：「汽車、機車或其他非依軌道行駛之動力車輛，在使用中加損害於他人者，駕駛人應賠償因此所生之損害。但於防止損害之發生，已盡相當之注意者，不在此限」，其中責任主體明確訂定為駕駛人，且為過失推定責任，由駕駛人就其已盡注意義務負

<sup>315</sup>等規定為適用。

## (一) 民法

既然我國尚未就自駕車修改責任分配之規範，則自駕車之責任自然回歸既有的歸責原則處理，而民法中可能涉及到的即為民法第184條之侵權行為，侵權行為係以故意過失為前提，在部分自動駕駛的情況，因為駕駛人負有監管車輛行駛並及時接管車輛之義務，故部分自動駕駛下所發生之事故，通常可認為駕駛人有過失而須負損害賠償責任，惟亦有可能是由汽車製造商和駕駛人共同負責，例如當系統發生故障而使駕駛人無法及時接管之情形，此時或許可認為汽車駕駛人和製造商成立民法第185條之共同侵權行為<sup>316</sup>。

未來解釋上可能會產生爭議的或許是製造商製造出有瑕疵之自動駕駛系統是否可認為係製造商違反客觀注意義務而具有過失，依照我國實務見解，所稱「過失」之有無，應以是否怠於善良管理人之注意為斷，苟非怠於此種注意，不得謂之有過失<sup>317</sup>。而所謂善良管理人之注意，即依一般觀念，認為有相當知識經驗及誠意之人所用之注意，已盡此注意與否，應依抽象

---

舉證責任。

<sup>314</sup> 我國消費者保護法第7條規定了企業經營者之責任，且我國規定之企業經營者，非如日本之製造物責任法係以製造商為規範，而包含以設計、生產、製造、輸入、經銷商品或提供服務為營業者。消費者保護法第7條第1項規定：「從事設計、生產、製造商品或提供服務之企業經營者，於提供商品流通進入市場，或提供服務時，應確保該商品或服務，符合當時科技或專業水準可合理期待之安全性」，而當製造者違反第7條第1項而致生損害於消費者或第三人時，依第7條第3項之規定，企業經營者應負連帶賠償責任。

與民法第191條之1類似之規定，消費者保護法第7條之1規定企業經營者須就該商品或服務符合當科技或專業水準可合理期待之安全性乙事，負舉證責任。

<sup>315</sup> 我國強制汽車責任保險法規定了汽車所有人均應就汽車訂立保險契約，當汽車交通事故致受害人受傷或死亡者，不論加害人 有無過失，請求權人均得依汽車強制責任保險法之規定向保險人請求保險給付或向財團法人汽車交通事故特別補償基金請求補償。

特別補償基金是為了使受害人均能獲得基本保障而設置之組織，當事故原因無法探究、事故汽車為未保險汽車、事故汽車係未經被保險人同意使用或管理之被保險汽車或事故汽車全部或部分為無須訂立本保險契約之汽車時，得向特別補償基金請求補償。

且強制汽車責任保險法亦有類似於德國責任保險之規定，當經要保人（通常為汽車之所有人）同意實際上使用或管理該汽車之人，有酒駕或其他不能安全駕駛之行為導致事故發生者，保險人雖然仍負保險給付之責，然保險人得在給付範圍內，代位行使其對被保險人之請求權。

<sup>316</sup> 依例變字第一號變更最高法院五十五年臺上字第一七九八號判例見解，共同侵權行為為人間不以有意思聯絡為必要，數人因過失不法侵害他人之權利，苟各行為人之過失行為均為其所生損害之共同原因，即所謂行為為關連共同，亦足成立共同侵權行為。

<sup>317</sup> 最高法院19年上字第2746號判例。

客觀之標準定之，行為人有無盡此注意之能力，在所不問<sup>318</sup>。故而本報告認為，如提供具有汽車製造商皆能避免之瑕疵之自動駕駛系統，則可認為汽車製造商違反善良管理人注意義務，而具有過失。惟此際多會與消費者保護法第7條與民法第191條之1競合而選擇優先適用後者之法律效果。

民法第191條之1規定了製造商之責任，責任主體為商品製造人，自動車之製造商亦可該當本條之責任主體，至於自動駕駛系統之設計者，所提供者雖非具體之商品，而是自動駕駛系統，解釋上應認其亦可該當本條之商品製造人。須注意的是「商品之生產、製造或加工、設計並無欠缺」之認定，依本條之增訂理由，有無欠缺之標準可能係以商品之品質管制或政府機關檢驗合格認定<sup>319</sup>，然而自駕車之品質管制或檢驗標準尚須由政府機關訂定之。

民法第191條之2規定的是動力車輛駕駛人之侵權責任，責任主體明確規定為「駕駛人」，故在目前尚未修法或有實務見解之情形下，自駕車其上裝設的自動駕駛系統尚不得該當「駕駛人」之概念。如後續實務見解擴大解釋「駕駛人」，將「實際上操縱、管理車輛之人」均解釋為「駕駛人」，則遠處監控之人、提供自動駕駛系統服務之人始有可能依本條負損害賠償責任。

## (二) 消費者保護法

消費者保護法第7條規定的是企業經營者之責任，包含商品責任與服務責任，亦即除了自駕車之汽車製造商、自動駕駛系統之設計者可該當本條文以外，提供地圖相關元件軟體(例如Google)者亦可被認為是服務提供者，而適用本條文。

至何謂當時科技或專業水準可以合理期待之安全性，有學者認為此不應以

---

<sup>318</sup> 最高法院 29 年滬上字第 106 號判例。

<sup>319</sup> 民法第 191 條之 1 之增訂理由：「二、商品製造人之責任，宜採侵權行為說。對其商品所生之損害，應負賠償責任，以保護消費者之利益。欲免除其責任須證明對商品之生產、製造（包括設計）、加工，並無欠缺或其損害非因該項欠缺所致或防止損害之發生，已盡相當之注意。商品之經過品質管制或已送政府機關檢驗合格，不能謂為已盡防止損害發生之注意，不得以此免責。商品製造人於此係負中間責任。增訂第一項。」

企業經營者觀點下的專業者水準作為判斷基礎，而應以消費者或一般人角度下，參酌當時科技或專業水準、社會經濟變遷情況或一般社會通念等，該商品或服務是否具有可合理期待之安全性作為判斷<sup>320</sup>。故自駕車之安全標準，應該要以使用自駕車之消費人及一般人之觀點來加以判斷，亦不得僅以政府機關所訂定之安全基準為唯一判斷標準。

### (三) 強制汽車責任保險法

強制汽車責任保險法所規定之汽車，係指公路法第2條規定之汽車<sup>321</sup>及行駛道路之動力機械，自駕車自得包含在該規定之中，故裝配自動駕駛系統之自駕車亦需投保強制汽車責任險。至投保義務人按第6條之規定為汽車所有人，除有特殊原因下投保義務人始為汽車之使用人或管理人。故自駕車之汽車所有人須投保強制汽車責任險，當自駕車發生事故致第三人受傷或死亡時，請求權人得向保險人請求保險給付或向特別補償基金請求補償。

至自駕車之汽車製造商是否需要投保強制汽車責任險，目前法條並無規定，然而無人載具科技創新實驗條例第5條申請人提出的創新實驗計畫中必須包含「投保責任保險之規劃」，故目前我國法就實驗階段，有要求申請人投保責任保險之規定，然而上路之後的責任保險究竟該由自駕車之製造商抑或是駕駛人來投保，則尚無明文規範。

從國際法制發展趨勢來看，我國或許可以考慮一方面維持既有歸責原則，但因應自動駕駛系統等級的升高，再視實務上的困難評估是否修正法令；但另一方面亦可參考美、英等國家作法，透過保險制度及政策指引等方式持續分散並降低自動駕駛系統可能存在的風險，並同時持續提高社會對於自駕車的接受度。

#### 1. 保險制度及特別補償基金之檢視

綜觀各國法制度觀點，對於自動駕駛事故的責任界限，許多國家都採

---

<sup>320</sup> 陳忠五，在餐廳滑倒受傷與服務欠缺安全性—最高法院 100 年台上字第 104 號判決評釋，台灣法學雜誌第 183 期，2011 年 9 月 1 日，頁 13-18。

<sup>321</sup> 汽車：指非依軌道或電力架設，而以原動機行駛之車輛。

取保險制度解決，或是部分修改法令，剩餘部分由保險填補，亦即幾乎全部國家都提及保險制度在自動駕駛發展現實的重要性。

未來自駕車普遍化後，因我國依現行強制汽車責任保險法已可要求自駕車所有人投保強制汽車責任險，如認為自駕車之行車風險與一般汽車之行車風險沒有不同，則無額外要求自駕車之製造商或駕駛人投保責任險以外之任意第三人責任保險之必要<sup>322</sup>。

惟，若自駕車之自動駕駛等級已達SAE J3016標準的第四級以上時，就第四級以上之自駕車（由自動駕駛系統執行完整駕駛任務且不期待車內人員之接管回應）之車內人員究竟屬於加害人（即認為屬使用汽車造成汽車交通事故之人）或受害人（即認為屬因汽車交通事故遭致傷害或死亡之人）情形得否依強制汽車責任保險法第7條規定向保險人請求保險給付或向特別補償基金請求補償並不易認定，未來尚需由主管機關透過函釋予進一步釐清。

## 2. 訂立安全基準：

日本訂立了「自動車の安全技術指南（自動運転車の安全技術ガイドライン）」，宣示了確保自動車安全性的五大要件，但實際上如何認定具體瑕疵，仍須留待後續法院判決見解來形成。美國交通部則持續發布、更新非強制性的政策指引，不僅於2017年發布了《自動駕駛系統2.0安全願景》，並以其為基礎於2018年發布《自動駕駛載具3.0 為運輸的未來做好準備》協助業者持續探索自駕車安全與性能的標準。

## 3. 事故的類型化：

另外本報告認為亦可以參考日本的討論脈絡，逐步將自駕車引起的事務類型化而評估是否需採取不同的責任分配原則，譬如：(1) 因駭客<sup>323</sup>

<sup>322</sup> 依國家發展委員會107年12月14日「人工智慧之相關法規國際發展趨勢與因應」委託研究計畫期末報告審查會，金管會所提有關「強制汽車責任保險法」內容之意見，汽車強制責任險之醫療費用採實支實付制，限額為新臺幣20萬元，殘廢給付及死亡給付則採定額給付，於現行自駕車所有人應訂立責任險契約外，另行規範製造商或駕駛人亦須訂立保險，受害人並無法因此獲得雙重給付，恐無實益。又倘為已訂立保險契約之自駕車，因保險人仍負保險給付義務，亦無需由特別補償基金予以補償。

<sup>323</sup> 如果是遭到駭客入侵的狀況，就和竊盜的狀況一樣係由非所有人的第三人來控制自駕車，因此也應該

入侵所引起之汽車交通事故，依現行制度可透過強制汽車責任險來加以補償；(2) 就自駕車系統中的自損事故，除依民法與消費者保護法向自駕車的製造商求償，也可考慮強化業界發展任意保險，使被害人損害迅速獲得填補。而主管機關亦已著手推動業界開發此類任意保險；(3) 就怠於注意自駕車運行者<sup>324</sup>，由道路交通主管機關訂立自駕車駕駛人/所有人的注意規則或準則，使法院在判定是否違反注意義務時有明確的判斷標準，充實化注意義務之內涵；(4) 就因地圖資訊、基礎設備資訊等外部資訊之錯誤、通訊屏蔽而發生之事故<sup>325</sup>，因涉及高度技術知識，則有賴於主管機關協同專家學者一同訂立自駕車瑕疵之審查規範，對建立穩定之法院見解亦會頗有助益。

---

要由政府基金或保險制度來確保被害人獲得求償，再者如果是駭客入侵，政府在賠償過後可以對自駕車的製造商求償。但須注意的是，如果是因為所有人在第三人可以自由出入的場所長時間地插著鑰匙停車導致被竊盜，此時應該要肯認所有人客觀上容認該事態發生或是認為所有人違反管理責任，據此所有人須負損害賠償責任。同理，如果是遭到駭客入侵，而法院認定自駕車的所有人並沒有採取資安上適當的對策，違反了檢查義務的話，就會和車子被盜的所有人所負的責任一樣，同樣都須負自駕車損害賠償之責任。

<sup>324</sup> 以目前的自駕車發展進程來說，尚無法將所有的行駛工作都交予自動駕駛系統處理，因此自駕車的所有人/駕駛人仍會有某程度的注意義務，包括關連法令的遵守義務、自駕車駕駛相關的注意義務、自駕車的檢查完善注意義務（包括更新自動駕駛系統中的軟體與資料，以及對應自動駕駛系統之要求修理自駕車）、駕駛者的選任監督義務等等。

<sup>325</sup> 因為自駕車系統是靠著地圖資訊、基礎設備資訊等外部資訊作為前提來讓自駕車行駛，如因該等資訊錯誤造成事故，處理的爭點即在於外部資訊之錯誤是否該當自駕車的「瑕疵」。我國民法的瑕疵應係指自駕車本身的瑕疵，也就是價值、效用之減損，且必須是依照駕駛當時與自駕車相關的知識經驗可以檢驗出的瑕疵。因此我們可以推論出，如果自駕車製造商可以預測到外部資訊的錯誤，就應該要設計出即使有外部資訊錯誤，也能夠安全行駛的自駕車駕駛系統，一發生外部瑕疵就無法確保安全性的系統本身可以說是具有「瑕疵」的。本文認為在認定自駕車本身是否具有瑕疵上，即使可以透過法律解釋達到某種彈性，仍必須仰賴高度技術知識。

## 第五節 人工智慧及大數據於公權力執行之運用

隨著人工智慧發展，近年來各國政府咸致力發展將人工智慧運用於公權力執行，以期能減少政府運作成本，增加公務機關行政效率與政府效能。本節將聚焦於美國、英國及歐盟等先進國家近期在公權力執行及政府行政等層面運用人工智慧之實例及法律議題，並透過文獻探討，整理並分析相關議題，以期作為我國未來政策形成及法規調適之參考。

### 第一項 焦點議題

目前，人工智慧在公權力行使的運用幾乎都是處於輔助（advisory）的角色，並能夠提供比既有的輔助工具更有效的服務，作為既有傳統體系下司法決策及行政功能的基礎。

美國司法體系曾引入許多不同演算法系統以輔助法官做出決定。現今，人工智慧的類似運用最著名的例子是美國政府所引入，由私人公司Northpointe, Inc.所開發的矯正犯人替代處罰管理分析（Correctional Offender Management Profiling for Alternative Sanctions，或稱COMPAS）演算法。COMPAS演算法考量犯人背景及經歷，包括犯罪經歷、人際關係及生活方式、個性及態度、家庭、社會隔離程度<sup>326</sup>，並輔以過去的歷史數據，計算個案中犯人再犯的機率、犯人未來使用暴力的機率、及犯人棄保潛逃的機率。每項機率都以1到10分計分，1到3分為低機率，4到7分為中等機率，8到10分為高機率。<sup>327</sup>

除了COMPAS，另兩套分別由不同單位或公司開發的類似系統Public Safety Assessment（PSA）及Level of Service Inventory Revised（LSI-R）也廣為美國各地司法系統所採用。<sup>328</sup>依據每州法規不同，法官通常使用前述計算結果決定是否在審判前羈押一名被告、是否假釋一名受刑人或核定其假釋金額。法官一般而言會考量許多不同因素，包括自由決定是否考量COMPAS等演算法的演算結果。有些州規定在

---

<sup>326</sup> Electronic Privacy Information Center, Algorithms in the Criminal Justice System, Retrieved from <https://epic.org/algorithmic-transparency/crim-justice/>.

<sup>327</sup> Jeff Larson, Surya Mattu, Lauren Kirchner and Julia Angwin (2016, May 23). *How We Analyzed the COMPAS Recidivism Algorithm*. Retrieved from <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>.

<sup>328</sup> Electronic Privacy Information Center, Algorithms in the Criminal Justice System.

量刑或假釋前必須進行類似的演算並將結果提供給法官參考<sup>329</sup>，其他州則是建議在特定案件（例如性侵案件）中進行類似的風險評估。

除了美國，英國Durham警方也自2017年起研擬Harm Assessment Risk Tool（HART）系統，依據特定人年齡、性別及犯罪歷史，計算犯罪機率，據以估算未來再犯可能性。原本該套系統參考的參數也包括郵遞區號，但遭論者質疑以郵遞區號作為參數會造成居住在較貧窮區域的嫌疑犯受到不公平待遇，因此相關機關也據此調整該項參數，改用較廣的居住區域作為參數。研究也指出該系統所評估的結果與人類所做的決定有相當的差距。<sup>330</sup>中國近來也致力於開發電腦輔助量刑系統，但主要以犯罪及量刑情節的類型化為主軸，其運作方式與前述的風險評估工具有所不同。<sup>331</sup>

除了前述司法系統引入犯罪機率評估演算法外，預測執法（predictive policing）也是人工智慧在公領域的一大應用。各國警察部門開始研擬使用資料探勘（data mining）或其他模式演算法分析犯罪熱點，連結犯罪數據、模式、時間、與其他設施距離以及其他變量，俾能更有效地打擊犯罪，甚至開發預警系統。<sup>332</sup>系統通過特定地區犯罪和人口統計的背景數據，旨在透過預測行為模式，更準確地預測可能發生犯罪活動的位置和時間。<sup>333</sup>美國加州Santa Cruz的警方在2011年起就導入PredPol犯罪預測系統，該系統透過過去的犯罪資訊及各項環境因素來預測可能發生犯罪的熱點，並宣稱可有效降低犯罪率達10%-50%。<sup>334</sup>

以歐美為首之各國紛紛推動「智慧城市」，期能創造並連繫人力資本、社會資本及

---

<sup>329</sup> Ohio Rev. Code § 5120.114 (2011).

<sup>330</sup> Matt Burgess (2018, March 1), UK police are using AI to inform custodial decisions – but it could be discriminating against the poor (2018, March 1). Retrieved from <https://www.wired.co.uk/article/police-ai-uk-durham-hart-checkpoint-algorithm-edit>; Bernard Marr (2017, September 19), How Robots, IoT And Artificial Intelligence Are Transforming The Police. Retrieved from <https://www.forbes.com/sites/bernardmarr/2017/09/19/how-robots-iot-and-artificial-intelligence-are-transforming-the-police/#27e3182a5d61>; Ed Yong (2018, January 17), A Popular Algorithm Is No Better at Predicting Crimes Than Random People. Retrieved from <https://www.theatlantic.com/technology/archive/2018/01/equivant-compas-algorithm/550646>.

<sup>331</sup> 黎其武（2008），〈計算機輔助量刑系統〉，《湖北警官學院學報》，總第103期；趙廷光（2007），〈論電腦量刑的基本原理〉，《湖北警官學院學報》，總第95期。

<sup>332</sup> Ira S. Rubinstein, Ronald D. Lee and Paul M. Schwartz (2008). *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. Chi. L. Rev. 263. 例如使用 pattern-based data mining 的方式，依據設定好的行為模式，在既有的資料集中發覺相同模式。

<sup>333</sup> Executive Office of the President (2016). *Big Data A Report on Algorithmic Systems, Opportunity, and Civil Rights*, 19-21.

<sup>334</sup> Mark Smith, *Can we predict when and where a crime will take place?* <https://www.bbc.com/news/business-46017239> (30 October 2018)



資訊通訊科技 (information and communication technology, 簡稱ICT) 各項基礎設施，俾能創造永續經濟發展，並提供民眾更好的生活。<sup>335</sup>而現代城市生活中，人們已經習慣於每個轉角的監視器甚至智慧型手機所提供及傳出的各類數據；這些巨量的數據過去無法被有效的運用，但在智慧城市時代，國家透過演算法的協助，將會更有效的運用並分析監視器所蒐集的海量資訊，也因此引起一定程度疑慮。<sup>336</sup>

綜上，人工智慧在公權力執法的運用在過去數年已逐漸開展，也衍生許多值得吾人探討的議題，謹簡述如下，並於下一項分別探討。

### 一、人工智慧決策之偏見與歧視風險

人工智慧在公權力執法的運用最為人詬病的問題，即在於演算法模型設計甚或「訓練」演算法的基礎數據均可能衍生偏見與歧視。例如google的照片應用程式最廣為人知的錯誤即是自動將黑人圖像分類為大猩猩<sup>337</sup>，該分類是依據數據庫所「餵」給演算法的資料所形成。

### 二、檢驗人工智慧決策之困難

人工智慧系統的演算過程與一般政府決策不同，難以透過重新檢視決策過程的方法檢驗。人工智慧系統無法驗證的原因在於其本質是設計成為自主進化的，也因此沒有確切可循的軌跡。<sup>338</sup>因此受到不利影響的個人往往難以挑戰相關決策，欠缺透明度，成為「黑盒子」(black box)，也造成人民正當法律程序保障面臨挑戰。

### 三、人工智慧參與決策的程度

人工智慧目前幾無法完全取代人工決策，決策過程中仍然保有人為的因素，如前所述，在司法系統中風險評估演算法通常只是供法官參考。惟該人為因素的強弱則視情況而定，如果決策過程中的「人」完全援引人工智慧系統的決定，

---

<sup>335</sup> European Commission, *Mapping Smart Cities in the EU*, 18.

<sup>336</sup> Perfected in China, a threat in the West (June 2, 2018). *The Economist*.

<sup>337</sup> Alex Hern (2018, January 12), *Google's solution to accidental algorithmic racism: ban gorillas*. Retrieved from <https://www.theguardian.com/technology/2018/jan/12/google-racism-ban-gorilla-black-people>.

<sup>338</sup> Science and Technology Committee, House of Common (2016). *Robotics and Artificial Fifth Report of Session 2016-17*, 16.

則實質上就是人工智慧系統在進行決策；反之，如果「人」過分干預，則可能錯誤的忽視人工智慧系統的建議。<sup>339</sup>

#### 四、人工智慧技術對國家權力造成的質變

在人工智慧時代，國家能夠更有效的運用並分析海量資訊。過去既有的法規密度可能將不符需求。例如，馬路屬於公共場所，路上的監視器所蒐集的資訊過去屬於公開資訊，因此人民一般不被認為對此有隱私之期待。然而，當政府在發展智慧城市等政策的同時，能夠透過人工智慧技術進一步追蹤、分析、甚至影響個別人民之權利，國家對於人民傳統上隱私期待的認知不無可能需要相應調整。

## 第二項 外國文獻分析

### 一、人工智慧決策之偏見與歧視議題

人工智慧相關的歧視疑慮可被區分成個不同面向。首先，機器學習無可避免需要透過輸入大量數據來訓練人工智慧系統。這些巨量數據本身如果是未經篩選的自然數據，通常一定會帶有一定程度的傾向與相關性。此外，開發者在選擇或篩選資料時也可能有意或無意有所偏重或缺失，例如前述 Google 人工智慧系統無法辨識黑人圖像，源自於基礎資料欠缺有色人種的數據。以美國而言，刑事司法數據常受到非常不準確之評論，原因在於主要的刑事司法數據庫聯邦調查局的統一犯罪報告（Uniform Crime Report；UCR），現代化程度過低並仰賴自願捐款運作。<sup>340</sup>司法與執法機關在使用各項工具時，往往也不會深究其背後所使用的資料庫品質如何以及是否與時俱進。<sup>341</sup>前述種種都可能影響人工智慧的運算結果，進一步影響其所預測的未來情況。<sup>342</sup>

另外，巨量數據本身如果是一段時間內的歷史數據，則可能反映過去該段時間

---

<sup>339</sup> Government Office for Science (2016). *Artificial intelligence: opportunities and implications for the future of decision making*, 10.

<sup>340</sup> Executive Office of the President (2016). *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, 7-9.

<sup>341</sup> Andrew Guthrie Ferguson (2015). *Big Data and Predictive Reasonable Suspicion*, 163 U. Pa. L. Rev. 327, 398

<sup>342</sup> 刑事犯罪資料具有許多本質上無法解決的矛盾及缺陷，例如再犯率此一指標只能夠涵蓋「被釋放或假釋的被告的再犯率，而不適用於「未被假釋或釋放」的被告族群。

的人類既有偏見及歧視。<sup>343</sup>訓練用數據也有可能與真實的人口比例偏移，從而發生代表不充分（underrepresentation）或過分代表（overrepresentation）的問題。<sup>344</sup>在許多國家，由於警察執法慣性及模式等種種原因，許多犯罪數據中的有色人種比例可能高於整體人口族群中該族裔所佔比例。<sup>345</sup>系統從而形成系統性的偏見，導致司法整體結果不利於特定族群，例如有色人種，進一步強化既有的偏見與歧視。舉例而言，系統錯誤預測非裔人種有再犯可能的機率遠比其他種高。<sup>346</sup>

如是，實際上可能造成「有罪推定」的結果，因而侵犯憲法所賦予人民之基本權；甚而整體而言造成特定族群較另一族群更為不利或有利的量刑結果，而脫離個案判定，也可能有違反憲法上平等原則的疑慮。前述的美國 COMPAS 系統在 2016 年即受到被告的挑戰。在 State 訴 Loomis 一案中，原審法官考量 COMPAS 系統對被告 Loomis 所做的評估，並達成量刑的決定。<sup>347</sup>被告在上訴時其中一個主張就是 COMPAS 系統運作上均認定男性被告有較高的再犯率，因此違反憲法上禁止性別歧視的平等原則。<sup>348</sup>然而，威斯康辛州最高法院認為被告主張不成立，因為從歷史數據觀之，男性被告確實有較高的再犯率。

加拿大最高法院最近在類似案件上表達更為直接的態度，並在 2018 年做出 Ewert 訴 Canada 一案判決。被告是加拿大原住民，原審法院於量刑時採用風險評估演算法的結果。加拿大最高法院指出該演算法係基於非原住民族群體之資訊開發，且僅有在非原住民群體上驗證，並未經過驗證運用在原住民族上的效果，從而可能違反加拿大相關法律下量刑時必須考量被告準確資訊之要求。<sup>349</sup>加拿大最高法院進一步指出前述種種可能不利少數族群獲得假釋的機會。<sup>350</sup>

---

<sup>343</sup> Andrew Guthrie Ferguson (2015). *Big Data and Predictive Reasonable Suspicion*, 163 U. Pa. L. Rev., 7-9.

<sup>344</sup> Solon Barocas and Andrew D. Selbst (2016). *Big Data's Disparate Impact*, 104 California Law Review, 684-687.

<sup>345</sup> Raso et al. (October 25, 2018). *Artificial Intelligence & Human Rights: Opportunities and Risks*, Berkman Klein Center Research Publication No. 2018-6 24.

<sup>346</sup> Ferguson, at 402. See also Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, ProPublica (2016, May 23). *Machine Bias*. Retrieved from <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

<sup>347</sup> State v. Loomis, 881 N.W.2d 749 (Wis. 2016).

<sup>348</sup> 同前註，頁 280。

<sup>349</sup> Ewert v. Canada, 2018 SCC 30. Para. 80.

<sup>350</sup> Ewert v. Canada, 2018 SCC 30. Para 83. 惟加拿大最高法院最終仍宣告該類風險評估工具並無違憲，原因是相關法規下已有其他機制可供原告主張權益。 See also Adelina Iftene, *Who is worthy of constitutional*

如果訓練人工智慧的資料或其演算法具有前述本質上的特性或缺陷，而設計者並未意識到或無法透過其他調整機制來匡正該種缺陷，則可能會放大既有資料的傾向。更進一步，如果這些運算結果被用來下決定，這些新的決定必然帶有相同的傾向，從而形成偏見的惡性循環。<sup>351</sup>

資料側寫可能會根據種族、生活方式、或居住地，對個人造成不公正的定型風險。甚至數據庫的資料某種程度會反映潛意識的文化偏見。這類型的偏見可能比前述的偏見更難以識別，此外因為研發人員往往採取自詡中立的專家態度，並預設數據產生的結果都是中立的，於是更難以立即發現問題。<sup>352</sup>惟，前述風險並非無法降低，舉例而言，英國公共部門即避免使用種族、國籍或地址作為標準，以產生不公平或歧視。<sup>353</sup>

另一項美國全國經濟研究局（National Bureau of Economic Research，係一私營非營利組織）的研究則採取一套與 COMPAS 不同但邏輯類似的演算法，研究人員依據數百萬個過去案件來分析再犯機率，並與實際的再犯率比較。該研究特別排除種族作為統計參數。<sup>354</sup>研究指出，該演算法運用在 40 個美國城市的計算結果都比法官的判斷結果準確，而這套演算法可以有效降低各城市的犯罪率，以紐約市而言，犯罪率將可以降低 25%。<sup>355</sup>研究人員發現這套演算法還可以有效校正法官行為上的缺陷，例如研究人員觀察到法官有時會釋放在等待審判期間失聯或是審判前再犯的犯人，可能是導因於法官會受到其他非統計的因素影響，例如開庭時犯人與法官的眼神接觸，演算法則不會發生這類錯誤。<sup>356</sup>

這項研究的研究人員也嘗試調整演算法，將有色人種的監獄人數限制在一定比例（例如維持在現有監獄中有色人種的比例，或現有被告群體中有色人種的比

---

*protection? A Commentary on Ewert v Canada*. Retrieved from <http://canliiconnects.org/en/commentaries/62360>.

<sup>351</sup> Room document for the 38th International Conference of Data Protection and Privacy Commissioners (2016). *Artificial Intelligence, Robotics, Privacy and Data Protection*, 4; Government Office for Science (2016).

*Artificial intelligence: opportunities and implications for the future of decision making*, 14.

<sup>352</sup> House of Commons, Science and Technology Committee (2016). *Robotics and artificial intelligence: Fifth Report of Session 2016-17*, 18.

<sup>353</sup> Government Office for Science (2016). *Artificial intelligence: opportunities and implications for the future of decision making*, 14.

<sup>354</sup> Jon Kleinberg et al. (2017). *Human Decisions and Machine Predictions*. National Bureau of Economic Research, Working Paper No. 23180.

<sup>355</sup> 同前註，頁 40。

<sup>356</sup> 同前註，頁 36。

例)，結果顯示這項變數並不會影響前述減低犯罪率的效果。<sup>357</sup> 由此可見，人工智慧系統若經過適當調整及設計，其實可以有效排除前述可能的歧視效果，甚至必要時採取類似優惠性差別待遇(affirmative action，或譯為積極平權措施)的制度設計，確保該類制度被運用在公權力執行時，不會導致甚或擴大既有的種族偏見。<sup>358</sup>

縱然許多論述都對風險評估演算法抱持保留意見，吾人須留意另一方面風險也同樣存在。依據美國佛羅里達州的研究，在一群被同樣演算法評估為類似風險程度的被告群體中，法官實際量刑的結果卻是非裔族群所受刑度比白人族群高出 68%。<sup>359</sup>

## 二、人工智慧決策之可驗證性、問責性與人為介入

人工智慧所做決策最為人質疑者，即是欠缺可驗證性及問責性，亦即潛在的「黑盒子」的疑慮。人工智慧的「黑盒子」疑慮來自數個不同層面，分述如下：

第一點，研發人工智慧系統的公司常主張該公司對於演算法即人工智慧系統有智慧財產權（如專利、營業秘密等），因此不願意開放相關資訊供外界或第三者驗證。

第二點，由於人工智慧的高度專業技術本質，即便相關資訊都充分揭露，一般民眾也欠缺理解或驗證人工智慧演算法的能力，而需要法律專家及技術專家的通力合作。<sup>360</sup> 在 Loomis 一案中，法官也指出法院所接收到關於 COMPAS 演算法的資訊即不夠充分。<sup>361</sup> 另一方面，由於演算法具有科學的「客觀」外表（即使這些演算法並非真的如想像中完全客觀，已如前所述），因此大眾及法院也

---

<sup>357</sup> 同前註，頁 32。

<sup>358</sup> 不過，該研究也有尚待商榷的部份。舉例而言，該研究只針對被假釋犯人的再犯率進行研究，而未對被法官裁定不假釋的群體進行再犯率的研究。同前註，頁 3。

<sup>359</sup> Danielle Kehl, Priscilla Guo, and Samuel Kessler (2017). *Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing*. Responsive Communities Initiative, Berkman Klein Center for Internet & Society, Harvard Law School, 30.

<sup>360</sup> Joshua Kroll (2016, February 10). *Accountable Algorithms (A Provocation)*. Retrieve from <http://blogs.lse.ac.uk/mediapolicyproject/2016/02/10/accountable-algorithms-a-provocation/>; Christopher Bavitz (2018, June 26), *Morality in the Machines*. *Harvard Law Bulletin - Summer 2018*. Retrieve from <https://today.law.harvard.edu/feature/morality-in-the-machines/>; Cary Coglianese and David Lehr (2017). *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, *Georgetown Law Journal*, 1189-90.

<sup>361</sup> *State v. Loomis* at 774. See also Kehl et al., at 28.

可能傾向不對所謂「科學方法」提出挑戰，因而減低其受檢視及驗證的機會。

第三點，也是較為難以解決的本質上問題，人工智慧技術本於「機器學習」，本質是設計成為自主進化的系統，其運作也因此沒有確切可循的軌跡，一定程度上具備「無法被驗證、再現、或以使人類得以理解的方式說明」的性質。<sup>362</sup>誠然，演算法並不必然一定會形成黑盒子，例如以決策樹（DecisionTree）模式發展的人工智慧演算法即是所謂的「白箱」人工智慧（white box AI），這類演算法的結構能夠說明人工智慧的學習過程並能夠解釋及驗證。對於演算法的驗證有不同做法，可以是檢視演算法本身的運算過程，檢驗「該系統如何達成運算結果」，惟對於人工智慧而言這個作法技術上不見得總是能夠完成，已如前所述。另一種可能的作法，則是使用另一個類似工具（例如不同公司開發的演算法）對同一組資料進行另一次運算，以確保原先的運算模式是公正的。

363

歐盟即建議人工智慧系統應該「可解釋」（explanation-based）。<sup>364</sup>此外，演算法問責（algorithmic accountability）的概念也有助於中和前述對人工智慧的疑慮。<sup>365</sup>在前述 State 訴 Loomis 一案中，被告另一個上訴主張即是因為 COMPAS 系統特性，導致被告無法驗證該系統的正確性，因此侵犯被告憲法上「基於正確資訊受量刑」之正當法律程序權利。惟該主張嗣後也為威斯康辛州最高法院所駁回，COMPAS 系統係透過被告所回答的問題進行演算，法院認為被告可以確認其輸入系統的答案是正確的，因此不會構成「基於正確資訊受量刑」的正當程序侵害。<sup>366</sup>近年亦發展出「技術正當程序」（technological due process）概念，其主要的內涵就包括對自動化程序的監督以確保公平及準確度。

367

為了形塑規範自動化決策之政策，美國紐約市在 2018 年訂立一部新法，主要

---

<sup>362</sup> Room document for the 38th International Conference of Data Protection and Privacy Commissioners (2016). *Artificial Intelligence, Robotics, Privacy and Data Protection*, 4.

<sup>363</sup> 同前註，頁 4。

<sup>364</sup> Francesca Rossi (2016). *Artificial Intelligence Potential Benefits and Ethical Considerations*, European Parliament, 4.

<sup>365</sup> 同前註，頁 4。

<sup>366</sup> State v. Loomis, 881 N.W.2d 749 (Wis. 2016), 260.

<sup>367</sup> Danielle Keats Citron and Frank A. Pasquale, *The Scored Society: Due Process for Automated Predictions*, at 19.



訴求是確保政府部門使用演算法時必須具備可問責性及透明度。依據該法，紐約市政府應成立自動化決策專案小組，就以下事項進行調查，並在 2019 年 12 月前提出書面報告，以供紐約市政府及大眾參考：評估紐約市政府各機關目前使用自動化決策的狀況、評估有無不當差別待遇的情況、並提出建議訂立相關程序以確保受該決策影響的民眾有權要求解釋。<sup>368</sup>該部法令性質上並非實體規範，而是規範建立未來實體法規範之程序。本報告建議應持續追蹤紐約市自動化決策專案小組後續的報告內容，以供我國參考。

對於演算法問責，目前走在最前端的立法是 GDPR 第 22 條下限制「自動化個人決策」（automated individual decision-making）的相關要求<sup>369</sup>。GDPR 第 22 條規定個資當事人有權不受到自動化決策之拘束，該決策包括對個資當事人產生法律效果或類似之重大影響，而係以自動化處理來評估其個人特徵之措施。即便是為締結或履行個資當事人與資料控管者間之契約所必須、或個資當事人已明確同意者，資料控管者仍應執行適當措施以保護個資當事人之權利、自由及正當利益。前項措施至少應確保得以部分之人為參與（human intervention）、表達意見（to express his or her point of view）及獲得質疑該決策（contest the decision）之機會等。換言之，使用個人資訊作為指標做成的自動化決定倘若對該個人造成嚴重影響，則依據 GDPR 第 22 條，該個人應有權質疑該決定。GDPR 第 22 條實質上創設了「自動化決策提供解釋」的規範，創設了「請求解釋權」（right to explanation），使受影響的個人有權要求該自動化決策「給個說法」。

然而，依據 GDPR 第 22 條第 2 項，歐盟或會員國法律所授權屬於容許的自動化決策，因此執法機關如警方或司法機關如法院依法透過人工智慧演算法所為或其他自動化決策，不受該「請求解釋權」的保護。<sup>370</sup>

另一方面，歐盟在預防、調查、偵測或追溯刑事犯罪時對個人資料的處理，包

---

<sup>368</sup> Int. No. 1696-A, Local Law 49 of 2018. Michael Stiefel, New York Creates Task Force to Examine Automated Decision Making, <https://www.infoq.com/news/2018/07/NYC-taskforce-automated-decision> (Jul 31, 2018).

<sup>369</sup> Regulation (EU) 2016/679, General Data Protection Regulation (GDPR), Art. 22.

<sup>370</sup> Jennifer Krueckeberg (2018, August 14). A Lawless Zone: Surveillance Technologies and the Police. *Green European Journal*. Retrieved from <https://www.greeneuropeanjournal.eu/a-lawless-zone-surveillance-technologies-and-the-police/>

括資料側寫跟自動化決策等，則受到歐盟資訊保護指令 Directive(EU)2016/680 規範。該指令對個資的定義包含位置資訊、線上識別因子(online identifier)<sup>371</sup>，並針對不同個資當事人(例如嫌犯與證人)之間予以不同的保護<sup>372</sup>，惟也引來差別對待之批評。根據該指令，自動化資料決策與資料側寫均不能作為預防、調查、偵測或追溯刑事犯罪時的唯一決策基礎<sup>373</sup>。此外，為了避免妨礙司法及保護公共利益，國家可以拒絕提供某些資料給個資當事人，也因此有論者批評該規定架空 GDPR 第 13 條下為了保護個資當事人所賦予個資當事人的資訊權<sup>374</sup> <sup>375</sup>，也不利個資當事人挑戰自動化決策。

### 三、人工智慧技術對國家權力造成的質變

各國近年咸積極發展智慧城市，以中國為例，杭州市自 2017 年起就與本地企業阿里巴巴在杭州推動「城市大腦 1.0 系統」<sup>376</sup>，核心概念是讓城市管理者可以使用資料進行管理工作。20 個中國省份與曠視科技合作推動「智慧安防解決方案」，主要係將私人公司曠視科技所開發的「Face++」人臉辨識技術運用在逃犯辨識。<sup>377</sup>私人公司盾心科技也是透過動作影像辨識偵測可能發生或即將發生的異常行為，例如肢體衝突、翻牆、尾隨等，以強化保全功能，可預期未來必然有公權力企圖借重類似技術進行執法。<sup>378</sup>

以我國而言，臺北市政府刻正初步發展多項臺北市智慧城市專案，其中包括「智慧路燈實證場域」<sup>379</sup>、「監視器導入 AI 應用實證計畫」<sup>380</sup>等應用分析正在進行或實驗中。「智慧路燈實證場域」主要擬延續北市府的內湖智慧路燈實證計畫，開放業者提案整合智慧照明、安全警示、車流與人流計數、停車格空位偵測、環境感測及電子看板訊息推播等功能。而「監視器導入 AI 應用實證計畫」

<sup>371</sup> Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, Art. 1.

<sup>372</sup> Directive (EU) 2016/680, Art. 6.

<sup>373</sup> Directive (EU) 2016/680, Art. 10.

<sup>374</sup> Directive (EU) 2016/680, Art. 13.

<sup>375</sup> Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), wp258 (29 November 2017).

<sup>376</sup> 裴有恆、陳玟錡 (2018)，《AIoT 人工智慧在物聯網的應用與商機》，頁 8-7。

<sup>377</sup> 裴有恆、陳玟錡 (2018)，《AIoT 人工智慧在物聯網的應用與商機》，頁 8-9 以下。翁書婷，〈AI 定義新時代——當人類的眼睛、耳朵，不再是唯一可思考和探索世界的工具〉，

<https://www.bnxt.com.tw/article/45138/ai-iot-and-big-data>。

<sup>378</sup> 裴有恆、陳玟錡 (2018)，《AIoT 人工智慧在物聯網的應用與商機》，頁 8-11 以下。

<sup>379</sup> <https://smartcity.taipei/project/120>

<sup>380</sup> <https://smartcity.taipei/project/50>



係由臺北市政府與財團法人台灣人工智慧發展基金會合作，利用臺北市目前現有的交通影像監視器，協助臺北市政府交通局交通管制工程處交通控制中心以人工智慧辨識車輛進而計算車流量、轉向量，提供數據給交控中心做為交通規劃參考。未來，未來也期望能利用其他現有的影像發展延伸應用，如公車內部監視影像計算上下車人數，提供更精確的載客量數據。

我國最高法院在 2017 年的判決中即認為，即使個人身處公共場域中，仍享有私領域不被使用科技設備非法掌握行蹤或活動的合理隱私期待。使用 GPS（全球定位系統）追蹤器，偵查機關可以連續多日、全天候持續而精確地掌握該車輛及其使用人的位置、移動方向、速度及停留時間等活動行蹤，且追蹤範圍不受時空限制，也不侷限於公共道路上，即使車輛進入私人場域，仍能取得車輛及其使用人的位置資訊。偵查機關非法安裝 GPS 追蹤器於他人車上，屬於藉由公權力侵害私領域的偵查，屬於「強制偵查」，如果無法律依據，自屬違法而不被允許。<sup>381</sup>

#### 四、 第三人對基本權影響

除了國家直接展現的公權力以外，現行社會中許多公權力的展現並不僅止於直接的政府決策，而有可能透過第三方展現。現代社會中第三方服務具有高度的集中性，例如金融市場就與管制政策與國家權力密不可分，<sup>382</sup>而大規模的網路公司例如 Google 及 Facebook 對基本權的影響並不下於國家所加諸人民的直接權力，值得未來進一步探討。<sup>383</sup>政府可能透過要求網路平台進行仇恨或歧視言論審查甚至主動刪除或過濾，這些網路平台近來均逐漸採用人工智慧演算法來審查相關言論，從而間接發生政府實質上透過人工智慧演算法展現公權力的效果。<sup>384</sup>例如德國在 2017 年就推動網路執行法（Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken），要求社群網路提供者（social network provider）必須於 24 小時內刪除明顯（manifestly）違反德國刑法

---

<sup>381</sup> 最高法院 106 年台上字 3788 號判決。

<sup>382</sup> Frank Pasquale (2015). *The Black Box Society*. Cambridge, Massachusetts; London, England: Harvard University Press.

<sup>383</sup> 例如，抵押貸款機構能根據個人信用評等分數，自動審核核貸申請。例如公平合理信用報告法（Fair Credit Reporting Act）。此外保險公司評估保費、就業市場上聘用與否的決定也都與此息息相關。

<sup>384</sup> 進一步討論請參見 Raso et al., at 39.

(Strafgesetzbuch) 的仇恨性言論及侮辱或誹謗性言論；<sup>385</sup>以 IBM 公司為例，該公司在極力推動人工智慧發展的同時也設立認知倫理委員會 (Cognitive Ethics Board) 以面對發展技術時同時隨之而來的倫理問題。<sup>386</sup>

### 第三項 針對我國法規調適之初步建議

人工智慧發展之原則必須符合既有社會規範 (social norms) 及價值，惟，為因應不可避免的潮流，提早調適相關法規有助於未來我國適應並利用人工智慧社會發展之趨勢。本報告建議在公權力執法層面的人工智慧運用應建立事前的程序制衡及事後的審查機制。

#### 一、關於人工智慧系統開發機制

世界各國皆有倡議成立特別的人工智慧委員會 (例如倫理審查委員會)，評估特定人工智慧應用對社會的潛在危害和好處，或者採用已有共識的方法來進行涉及機器學習的審查過程。<sup>387</sup>特別是針對運用公權力執法層面的人工智慧技術，由獨立第三方專家所組成的獨立人工智慧委員會更為必要。

此外，也有倡議者主張建立人工智慧開發者認證制度<sup>388</sup>，透過此一制度，可有效將人工智慧開發者納入管制，並適度要求揭露人工智慧技術的智慧財產權，即使不是全面公開，至少在涉及影響人民基本權利的人工智慧運用上，可以一定程度揭露予獨立人工智慧委員會或類似的第三方審查單位。主要目標在於確保人工智慧演算法的透明度，包括開發方法、演算假設、各項參數的權重、演算法的版本更新及校正等，一來可以提高演算法的精確度，二來也俾其他人 (例如司法系統、法律及科技學界或一般大眾) 了解演算法的運作，形成賦權被告驗證或質疑該演算法之基礎<sup>389</sup>，也有助於提高系統的問責性。無論如何，政府不能只是把演算法系統「外包」給私人公司，而是必須盡責地追蹤並主動監督。

---

<sup>385</sup> The Network Enforcement Act. 吳柏緯，〈老大哥回來了嗎？從臉書審查到德國《網路執行法》〉  
<https://www.twreporter.org/a/facebook-censorship-netzdg-bigbrother>

<sup>386</sup> Francesca Rossi (2016). *Artificial Intelligence Potential Benefits and Ethical Considerations*. European Parliament, 5.

<sup>387</sup> House of Commons, Science and Technology Committee (2016). *Robotics and artificial intelligence: Fifth Report of Session 2016-17*, 23.

<sup>388</sup> Government Office for Science (2016). *Artificial intelligence: opportunities and implications for the future of decision making*, 15.

<sup>389</sup> Kehl et al., at 32.

另一方面，相關系統具有高度的地域性。目前相關演算法的運用受抨擊的一點即是美國有些州在採取特定系統前，不見得有經過有效性測試( validity test)；即便其他州在採用相關系統前有採取必要的有效性測試，相關測試也不見得有持續更新，從而可能無法確保相關系統適合該州的人口組成等特殊情況。<sup>391</sup>吾人可以想像，縱使我國擬採用其他先進國家所開發出較為成熟的風險評估演算法，相關系統在實際上線前必然需要進行大幅度的調校以適應我國法制及事實情況。

## 二、關於人工智慧系統運用及人為介入

由於人工智慧在公權力執行面向相較於其他領域而言，對人民基本權之影響更鉅，已如前述。因此，未來在政策形成時建議援引 GDPR 第 22 條的精神，確保人為介入的可能，秉持人工智慧乃輔助人類決策而非取代人類決策之原則。換言之，決策中必需要有「人」的因素，而關鍵的議題則是在於在何時、以何種方式引入人類決策的制衡，以權衡前述人類決策與人工智慧平衡的兩難。在發展人工智慧之初期，原則應確保人類是決策者，並由人類決定是否採用人工智慧的建議，避免完全自動化的決策。如此，可以確保人類能夠察覺人工智慧無形中形成的偏見，並能夠嗣後矯正這樣的偏見，例如前述美國國家經濟研究局的研究就成功透過嗣後校正演算法來確保不會形成不利於有色人種的結果。

我國司法院業已於 2018 年 8 月頒布「刑事案件量刑及定執行刑參考要點」(下稱「**量刑要點**」)。<sup>392</sup>該量刑要點原則上乃供作法官參考而非強制適用，係針對具體個案事實以各種抽象標準評價，其主要目的有三，即(1)對於不法侵害行為給予相應責任刑罰之應報功能、(2)矯正行為人並使其復歸社會之特別預防功能、及(3)嚇阻犯罪、回復社會對於法規範之信賴及維護社會秩序之一般

<sup>390</sup> Kehl et al., at 34.

<sup>391</sup> Electronic Privacy Information Center, *Algorithms in the Criminal Justice System*.

<sup>392</sup> 司法院刑事案件量刑及定執行刑參考要點，中華民國 107 年 8 月 7 日司法院院台廳刑一字第 1070021860 號函。

預防功能<sup>393</sup>。該量刑要點雖也有將行為人再犯之危險性納入考量因素之一<sup>394</sup>，但整體而言仍以評價個案之「可非難性」為主，與 COMPAS 這類以「風險控制」為導向的演算法評估系統或有本質上的差異。兩者之間並無孰是孰非，而應宜綜合考量俾相輔相成。職是，本報告建議相關單位可在未來修訂該量刑要點時酌予考量我國未來引入或開發類似 COMPAS 的犯罪機率評估系統之可能性，並明文將其納入前述量刑要點做為法官量刑時可酌情職權考量的因素之一，惟相關參數設定時應廣納建言以減少前述演算法可能產生之歧視或偏見問題，並定期檢討修正。

以預測性執法而言，通常預測技術會運用於可能需要預先介入的地方，提前佈署警力。此類技術應該秉持匿名原則，避免針對個人或特定族群，落實無罪推定原則（innocent until proven guilty），以避免產生侵害個人基本權疑慮。警政機關尤須注意善用演算法所預先提供之資訊（如犯罪發生地或時間），是否發動偵查應嚴格遵循「釣魚偵查」與「陷害教唆」的界線，<sup>395</sup>於實際執法時亦應受到憲法比例原則之限制，自不待言。

### 三、人工智慧系統運用之爭端解決機制

有鑑於人工智慧技術的高度專業性，論者也有建議成立人工智慧爭端評議中心，協助民眾對使用機器學習的機關或組織提出挑戰。<sup>396</sup>此應可一定程度解決人工智慧之運用所生一般性爭端，作為替代性爭端解決機制（alternative dispute resolution；ADR），以取代傳統的司法管道。評議中心倘屬由專業人員（例如法律、科技專業）組成之非營利、非官方組織，固有其專業、彈性、效率之優點。然而，評議中心相較於傳統法院而言，其所做決定之公信力似有疑慮。故

<sup>393</sup> 司法院刑事案件量刑及定執行刑參考要點，第二點。

<sup>394</sup> 司法院刑事案件量刑及定執行刑參考要點，第七、（二）點。

<sup>395</sup> 學理上所稱「陷害教唆」者，係指行為人原不具犯罪之故意，純因司法警察之設計教唆，始萌生犯意，進而實行犯罪構成要件之行為者而言；此項犯意誘發型之誘捕偵查，因係司法警察以引誘、教唆犯罪之不正當手段，使原無犯罪意思或傾向之人萌生犯意，待其形式上符合著手於犯罪行為之實行時，再予逮捕，係以不正當手段入人於罪，已逾越偵查犯罪之必要程度，對於公共利益之維護並無意義，其因嚴重違反刑罰預防目的及正當法律程序原則所取得之證據資料，固不具有證據能力；惟若屬警方對於原已具有犯罪故意之人，以所謂「釣魚」之偵查技巧蒐集其犯罪證據之情形，則與「陷害教唆」有別，其所取得之證據資料，並非無證據能力，最高法院 106 年台上字第 683 號刑事判決參照。

<sup>396</sup> Government Office for Science (2016). *Artificial intelligence: opportunities and implications for the future of decision making*, 15.

就公權力運用人工智慧與人民所生之爭議是否宜於透過評議中心這類非傳統司法管道處理，本報告則持暫保留看法。

## 第六節 結合金融監理沙盒及人工智慧以活化臺灣金融產業

近年來金融科技的蓬勃發展，使得當傳統金融商品或服務與創新科技相互結合後，是否將顛覆現有的金融法令，成為近年來炙手可熱的議題之一。而在新興科技所引發的金融創新風潮中，人工智慧技術亦扮演了不可或缺之角色。惟以人工智慧技術提供創新金融服務，勢必將提升金融服務的自動化成分，此項特性不免會與現行以「人」為規範主體之金融法規有所扞格，故如何在金融創新與現行規範之間加以調和，即成為監管者應儘速釐清的重要議題。2018年甫實施之「金融科技發展與創新實驗條例（下稱「**實驗條例**）」，賦予金融或新創業者，針對其擬提供之金融創新服務，在免於受到現有規範之限制下，一個絕佳的實驗場域。因此，擬發展金融創新服務或商品之業者，可能藉由參與創新實驗，而獲得進入市場營運的契機。

考量我國實驗條例之制定，係參考其他監理沙盒制度發展較為成熟之國家，且目前國內已有為數不少之業者著手研發並嘗試提供結合人工智慧技術之金融服務，故本節將先行介紹部分國家之監理沙盒制度以及與金融科技發展相關之政策，並藉由其他國家有關人工智慧技術結合金融服務或商品之案例和相關規範，探討在監理沙盒下，我國主管機關於面對人工智慧技術所引起的金融創新變革時，得以作為借鏡之軌跡，並對現行實驗條例在人工智慧運用於金融產業時所可能產生之限制提出檢討，進而對我國法規可調整之方向提出建言。

### 第一項 焦點議題

沙盒（Sandbox）一詞起源於電腦科學領域，係指可供尚未經過測試之程式一個經過充分隔離的實驗場域，以避免仍有安全性疑慮之程式對電腦系統產生損害。而「金融監理沙盒（Regulatory Sandbox）」的誕生，係將沙盒的原生概念，推展至金融產業。換言之，擬提供尚未符合現行規範的創新金融服務或商品之業者，一旦申請並經政府核准同意進入監理沙盒，即得於創新實驗之特定範圍與期間內取得相關規範之豁免。其次，考量金融創新具有高度不確定性，從而伴隨著潛在未知之風險，故要求進入沙盒的業者應建置消費者保護相關機制，以期在保護消費者權益的同時，亦能防免金融市場遭遇系統性風險之危害。

另一方面，就金融創新科技而言，人工智慧於金融產業的應用向來受到關注，且實

際上國內外不論是投資理財服務，乃至於保險服務，都已有採取人工智慧技術之應用實例。以臺灣而言，縱然已有保險業者在現行法規可行之範圍內，於核保過程導入人工智慧技術，以試圖簡化傳統上較為冗長之人工核保流程，並避免人工核保因主觀因素而產生結果上之差異，但自金融監督管理委員會（下稱「金管會」）目前的立場而論，保險業者或非金融業之新創業者如擬提供創新保險服務，仍不排除有需進入沙盒之可能。惟查，考量我國目前似尚未有非保險業者擬以創新保險服務申請監理沙盒之公開案例，且本報告既旨在藉由探討結合人工智慧技術之金融服務於監理沙盒，所可能衍生的利與弊，從而本報告以下仍將以機器人投資顧問為探討之核心。

事實上，機器人投資顧問的問世，不僅係對傳統理財顧問服務的技術革新，其減少或去除「人」在理財顧問服務所扮演之角色，亦意味著人力成本及實體營運據點需求之降低，故一般認為，相較於傳統投資顧問之高設置成本及顧問費用，機器人投資顧問有機會提供小額投資人新的投資選項。實際上，國際間對於機器人投資顧問尚未得出一致的定義，但多認為機器人投資顧問之內涵至少包括經由演算法驅動、自動化為客戶提供理財投資建議等特徵<sup>397</sup>。而目前許多國家均有發展機器人投資顧問之案例，且亦有新創業者投入並提供此一業務。

惟查，依據臺灣現行法令規定，目前僅有證券投資顧問事業業者或兼營投資顧問業者得提供機器人投資顧問服務，此外，金管會雖於 2017 年開放業者可以電腦系統自動替客戶執行「再平衡交易」，使業者不僅得從事「諮詢建議型」之機器人投資顧問服務，亦可發展「資產管理型」<sup>398</sup> 機器人投資顧問。惟再平衡交易仍僅限於證券投顧業者始得為之。由此可見，對於擬提供相關服務之業者而言，機器人投資顧問服務所涉及之法規遵循成本極高，且法規相關限制（詳如本節第三項所述）亦不利於新創產業機器人投資顧問發展。

臺灣之實驗條例第 26 條規定<sup>399</sup> 准許依主管機關所核准之創新實驗範圍辦理創新實

<sup>397</sup> 證券暨期貨市場發展基金會（2018），《我國發展機器人理財顧問之研究》，頁 23-25。

<sup>398</sup> 一般認為「資產管理型」機器人投資顧問除提供諮詢建議服務外，並進一步協助客戶就投資組合提供交易執行及風險管理服務，而有別於「諮詢建議型」之機器人投資顧問。

<sup>399</sup> 金融科技發展與創新實驗條例第 26 條規定：「申請人於創新實驗期間，依主管機關核准創新實驗之範圍辦理創新實驗者，其創新實驗行為不適用下列處罰規定：一、銀行法第一百二十五條。二、電子支付機構管理條例第四十四條或第四十六條。三、電子票證發行管理條例第三十條第一項、第三項、第四

驗者（下稱「**實驗者**」或「**申請人**」），其創新實驗行為不適用證券投資信託及顧問法第 107 條<sup>400</sup>或第 110 條<sup>401</sup>規定，該等規定有利於提供機器人投資顧問服務之業者，得在不受現有的法規之拘束下實驗其創新服務。其次，參照其他較早實施金融監理沙盒之國家（例如英國及新加坡），亦有業者以機器人投資顧問相關服務申請並經核准進入沙盒，故從機器人投資顧問之角度，切入討論當傳統金融服務結合人工智慧科技時，金融監理沙盒所扮演的角色，以及人工智慧所帶來的金融科技創新，在現有制度下可能面臨的侷限，應具有實益。

## 第二項 外國文獻分析

有論者認為，金融科技之監理一般而言可區分為下述三種類型<sup>402</sup>：

- 功能型監理（Restrictive Regulation）：以美國為例，係不論任何金融科技以何種型態出現，均按照該金融科技之本質，將其所涉及的金融業務依照功能納入現有之金融監理體系，從而該類型監理之有效度，將取決於現有監理體系之成熟度。
- 主動型監理（Active Regulation）：以英國、新加坡為例，兩國均以監理沙盒創造出一個隔離的安全試驗區，在沙盒內放寬監理條件、降低核准門檻，以促進創新活力。
- 被動型監理（Passive Regulation）：以中國為例，與上述兩類型監理機制相反，中國的金融科技以市場及商業模式作為驅動力進行發展，且法規上似是採取負面表列方式，僅明文規定何種情形不得為之，在負面表列外之項目則容許嘗試

---

項或第二項有關違反同條例第四條第一項規定。四、信託業法第四十八條。五、票券金融管理法第六十一條有關違反同法第六條規定。六、證券交易法第一百七十五條第一項有關違反同法第十八條第一項、第四十四條第一項規定，或第一百七十七條第一項有關違反同法第四十五條第二項規定。七、期貨交易法第一百十二條第五項第三款至第五款。八、**證券投資信託及顧問法第一百零七條或第一百十條**。九、保險法第一百六十七條或第一百六十七條之一。」

<sup>400</sup> 證券投資信託及顧問法第 107 條規定：「有下列情事之一者，處五年以下有期徒刑，併科新臺幣一百萬元以上五千萬元以下罰金：一、未經主管機關許可，經營證券投資信託業務、證券投資顧問業務、全權委託投資業務或其他應經主管機關核准之業務。二、違反第十六條第一項規定，在中華民國境內從事或代理募集、銷售境外基金。」

<sup>401</sup> 證券投資信託及顧問法第 110 條規定：「違反第十六條第一項規定，在中華民國境內從事或代理投資顧問境外基金者，處二年以下有期徒刑、拘役或科或併科新臺幣一百八十萬元以下罰金。」

<sup>402</sup> 蔡凱龍（2016 年 10 月 10 日），〈各國是如何監管金融科技的〉，載於 <http://finance.sina.com.cn/zl/bank/2016-10-10/zl-ifxwrhpn9545994.shtml>。



創新，主管機關本身處於一個較為被動的狀態，僅在有風險事件產生時，才介入制訂監管規範（例如：P2P 風險事件發生時，於 2016 年 8 月 24 日頒佈《網路借貸資訊仲介機構業務活動管理暫行辦法》）。

由上可知，臺灣雖然與中國同屬大陸法系國家，惟在金融科技監理上，取徑係步隨上述以英國及新加坡為代表之主動型監理，事實上實驗條例於制訂之初亦是參考英國及新加坡相關規定及設計，從而，就本次報告之目的，本報告將以英國和新加坡之監理沙盒及人工智慧相關案例作為研析及探討之對象，並側論歐盟及日本相關規定<sup>403</sup>。

## 一、英國

英國為最早提出監理沙盒制度之國家，其監理沙盒制度旨在鼓勵創新，希望藉由促進公平競爭以達提升消費者福祉之目的<sup>404</sup>。英國監理沙盒的適用對象包括金融業與非金融業，只要是「金融服務暨市場法（Financial Services and Market Act）」所規範的產業活動，均屬於得申請沙盒試驗之範疇，惟支付及電子貨幣相關服務因已於其他法令規定，故不屬於可進入沙盒之受試產業類別<sup>405</sup>。申請進入監理沙盒應至少符合下述標準：申請人應屬於得參與受試之產業、所提供的服務具有真正的創新性（genuine innovation）、得為消費者帶來利益、有進入沙盒受試的必要、申請人已投入相當的資源瞭解現行規範及緩和創新服務可能帶來的風險<sup>406</sup>。專責主管機關「金融行為管理局（Financial Conduct Authorities，下稱 FCA）」得針對非金融業者提供有限制授權（restricted authorisation），而針對金融業者則視不同情況發給承諾函（No enforcement

---

<sup>403</sup> 日本與我國同屬於大陸法系國家，應具有研究及參考之價值。日本產業競爭力強化法（日文：産業法競争力強化法）設計了二種制度，即「灰色地帶消除制度」（日文：グレーゾーン解消制度）（産業競争力強化法第 9 條）及「企業實證特例制度」（日文：企業実証特例制度）（産業競争力強化法第 8 條及第 10 條）。惟查，前者較接近於法規釋明，後者則接近於促使主管機關建置除外規定，兩者均與監理沙盒之概念有別，故不在本報爆討論範圍，本報告將聚焦於今年 6 月甫施行之生產性向上特別措施法（日文：生産性向上特別措置法）（詳後述）。其次，中國目前似尚無全國性之金融監理沙盒專法。

<sup>404</sup> Financial Conduct Authority (2017). *Regulatory Sandbox Lessons Learned Report*. Retrieved from <https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf>, 3.

<sup>405</sup> Financial Conduct Authority (2015). *Regulatory Sandbox*. Retrieved from <https://www.fca.org.uk/publication/research/regulatory-sandbox>, 8.

<sup>406</sup> Financial Conduct Authority (2017). *Regulatory Sandbox Lessons Learned Report*. Retrieved from <https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf>, 8.

action letters）、行政指導（Individual Guidance）或法規豁免（Waivers）<sup>407</sup>。

其次，就消費者保護而言，FCA 提出四種可能採取的措施：一、在實驗階段中，申請人應告知消費者參與實驗的潛在風險和可取得之補償，並取得參與實驗之消費者的告知同意；二、FCA 同意針對受試活動所應採取之揭露、保護、補償等機制將依據不同個案分別規範；三、賦予參與實驗的消費者與一般受管制機構之消費者相同的救濟權利（例如：申訴、補償等）；四、由申請人負責對消費者進行補償，且申請人須證明有足夠資力為補償<sup>408</sup>。

監理沙盒之測試期間為 3 至 6 個月，於進入沙盒後，申請人應遵守相關要件，諸如：由申請人決定得參與實驗的消費者，且消費者數量不宜過多；申請人所提供的計畫應包含時程表、消費者保護機制、衡量實驗結果的標準、測試參數、風險評估與應符合資訊揭露等<sup>409</sup>。此外，FCA 亦會針對每一案件分別指派一位個案官員（case officer）協助申請人進行實驗。待實驗期間結束後，申請人應提交有關實驗結果的最終報告供 FCA 審查<sup>410</sup>。在實驗期間即將屆滿之前，個案官員會詢問申請人是否計畫申請許可變更（Variation of Permission，即 VoP），使其於實驗階段所提供之服務或商品持續不受到限制，或是否需要申請其他不同的授權<sup>411</sup>。倘若決定申請且不更改受試的服務或商品，則一旦實驗結果成功，該申請人將取得無限制或低度限制的許可變更<sup>412</sup>。

英國之監理沙盒實施至今已歷經四個梯次的申請，FCA 一般會將歷次已獲准進入沙盒實驗的業者名單公布於官方網頁<sup>413</sup>。目前已獲准進入英國監理沙盒的業者，有部分即係提供以人工智慧為基礎之產品及服務，例如：

---

<sup>407</sup> Financial Conduct Authority (2015). *Regulatory Sandbox*. Retrieved from [https://www.fca.org.uk/publication/research/regulatory-sandbox\\_9](https://www.fca.org.uk/publication/research/regulatory-sandbox_9).

<sup>408</sup> 同前註，頁 21-22。

<sup>409</sup> 同前註，頁 11。

<sup>410</sup> 同前註。

<sup>411</sup> Vishnu C. (2018, March 6). UK FCA regulatory sandbox: Lessons learnt and Application Tips. *Medium*. Retrieved from [https://medium.com/@vishnu\\_3187/uk-fca-regulatory-sandbox-lessons-learnt-and-application-tips-26dbbe5f1135](https://medium.com/@vishnu_3187/uk-fca-regulatory-sandbox-lessons-learnt-and-application-tips-26dbbe5f1135).

<sup>412</sup> 同前註。

<sup>413</sup> Financial Conduct Authority (2017). *Regulatory sandbox - cohort 1*. Retrieved from <https://www.fca.org.uk/firms/regulatory-sandbox/cohort-1>. 惟其公布內容相對有限，一般並無申請人之商品或服務所採用的創新技術細節、實驗期間表現及實驗期間結束後申請人的未來發展等相關面向。

1. Beekin 透過人工智慧及數據分享之技術，提供風險管理及分析服務予小額投資者；
2. Moneyhub Enterprise 將公司軟體結合人工智慧、數據分析和心理學，以鼓勵消費者進行金融投資；及
3. Chynge 以 DLT 跨境匯款系統為基礎，系統採用法遵機器人，進行高效能之洗錢防制和打擊資恐。

由上可知，英國業者已有結合人工智慧之金融服務成功進入監理沙盒實驗，且業者之商業模式亦不僅限於機器人投資顧問。惟單就投資顧問服務而論，FCA 於 2017 年 10 月出具之官方報告中針對其於沙盒實驗期間內，將採取何等措施有更進一步地說明<sup>414</sup>。在該報告中，FCA 肯認金融監理沙盒旨在提供業者一個可確認其服務/產品是否能被更廣大市場接納之機會。以機器人投資顧問為例，為避免機器人投資顧問提供之服務，有不適當之情形發生，FCA 在相關試驗開始前，即要求申請人提供安全措施，在多數的案例中，該等措施係由具專業資格之財務顧問，逐一確認由演算法產出並提供之自動化管理建議。例如在某項沙盒實驗中，係於消費者收受自動化建議時，安排富有經驗之顧問在場，使顧問能及時在消費者收受建議後、實際執行交易前，檢視並修訂(如有必要)相關建議，該等修訂並由具專業資格之財務顧問評估後，反饋至演算法中。此一機制有助於申請人藉由區辨機器人投資顧問產出的結果，與真人顧問所提出之投資建議間之差異，適時地調整演算法，以提供更為優化的金融創新服務，亦可兼顧主管機關對於消費者保護之要求。

然而，從 FCA 出具之報告亦可知，儘管監理沙盒係以提升消費者福祉和鼓勵金融創新為目標，但此二目標在某程度上卻存有緊張關係。舉例而言，將傳統理財顧問服務結合人工智慧，應係為了提高該服務的自動化成分以減少人力介入，並進而將所節省之人力成本，反映在向消費者所收取費用之降低。此將傳統上大量仰賴人力的金融服務加以自動化的過程，即為金融創新之體現，但為保障消費者權益，FCA 亦會要求申請人應提供相當之防護措施，以確保自動

---

<sup>414</sup> Financial Conduct Authority (2017). *Regulatory Sandbox Lessons Learned Report*.

化設備提供之結果及服務品質，並避免消費者蒙受不可預期的損失。而相關防護措施在實踐上，仍有賴相當程度之人力（特別是具備相關專業資格之人士）介入，從而申請人在實驗階段或是離開實驗後，是否確實能降低人力成本，又監管者在保障消費者權益時，對於申請人所提供之防護措施之要求應達何等程度，才不至於阻礙金融創新的發展，均尚待進一步折衝與觀察。

另一個值得注意之處在於，對於擬提供結合人工智慧技術之金融服務的英國業者而言，除得以上述監理沙盒作為試驗其創新服務之管道外，FCA 針對自動化顧問業務亦設立「顧問小組（Advice Unit）」，使從事自動化顧問業務之業者得藉由線上遞交資料之方式，以較低的成本諮詢相關監管要求<sup>415</sup>。而此自動化顧問業務可能涉及的領域包含投資、退休金、投資人保護等<sup>416</sup>，故擬從事機器人投資顧問服務的業者，亦可以透過向顧問小組申請自動化顧問業務，而取得 FCA 對其業務的輔導。惟依 FCA 之規定，僅有符合若干條件之業者，始得向顧問小組申請自動化顧問業務，且與監理沙盒制度相比，顧問小組對於投資人保護亦有較高之要求，故業者循此管道從事自動化顧問業務，或申請進入監理沙盒，在制度面上並不相同，且申請所應符合的資格條件亦有相當之差異<sup>417</sup>。

## 二、新加坡

新加坡設立監理沙盒，係為藉由建立創新與安全使用科技的環境，使新加坡成為智慧金融中心<sup>418</sup>。新加坡監理沙盒之適用對象，亦同時包括金融業與非金融業，專責主管機關為新加坡金融管理局（Monetary Authority of Singapore，下稱 MAS）。申請進入沙盒應符合下述七項標準：

- (一) 金融服務運用新穎或發展中的科技，或以創新方式使用現行科技；
- (二) 金融服務得用來解決市場問題，或為消費者或產業帶來利益；

<sup>415</sup> 證券暨期貨市場發展基金會（2018），《我國發展機器人理財顧問之研究》，頁 48。

<sup>416</sup> Financial Conduct Authority, Advice Unit. Retrieved from <https://www.fca.org.uk/firms/advice-unit>.

<sup>417</sup> 證券暨期貨市場發展基金會（2018），《我國發展機器人理財顧問之研究》，頁 49。

<sup>418</sup> Monetary Authority of Singapore (2016). *Fintech Regulatory Sandbox Guidelines*. Retrieved from <http://www.mas.gov.sg/~media/Smart%20Financial%20Centre/Sandbox/FinTech%20Regulatory%20Sandbox%20Guidelines.pdf>, 4.

- (三)申請人具有意願及能力在退出沙盒後，以更大規模的方式，將該金融服務推廣至新加坡市場；
- (四)應清楚定義沙盒的實驗情境及預期結果，且申請人應依據核准的時程表，向主管機關報告測試進度；
- (五)應明確定義邊界條件（boundary conditions），俾順利執行沙盒並充分保障消費者利益和維護產業健全；
- (六)金融服務所可能衍生之重大風險應經過適當評估及採取降低風險之措施；及
- (七)應提出相關退場機制<sup>419</sup>。

新加坡監理沙盒的實驗期間通常為 6 個月，必要時得申請展期。此外，於沙盒實驗進行中，如出現下述任何情況，MAS 均得終止實驗：一、MAS 對測試狀況不滿意；二、已確定申請人在實驗結束後無法滿足法規要求；三、在實驗進行中發現受試之金融服務有重大瑕疵，對消費者或金融市場所帶來之風險將大於利益，且無法於實驗期間中解決；四、申請人於實驗期間違反相關規定；或五、申請人主動申請<sup>420</sup>。

依據 MAS 官方網站所示，截至 2018 年 9 月為止，MAS 僅核准四家業者進入沙盒，目前已有兩家業者順利於實驗結束後取得執照或受到相關法規豁免（詳後述）、一家經營匯款服務之業者則在實驗結束後受到 MAS 限制不得再繼續經營及廣告該等業務、剩餘一家業者則尚處於實驗階段<sup>421</sup>。由上可知，新加坡監理沙盒制度雖然發展算早，但目前獲准進入沙盒的申請人卻屈指可數，有觀察者指出，其主要原因並非審查標準過嚴，而是新加坡向來對新創業者並未給予太多限制，故多數從事金融科技服務之申請人，本即得以在現行法規下營運，

---

<sup>419</sup> 同前註，頁 5-6。

<sup>420</sup> 同前註，頁 7。

<sup>421</sup> Monetary Authority of Singapore (2018). *Experimenting in the Sandbox*. Retrieved from <http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/FinTech-Regulatory-Sandbox/Experimenting-in-the-sandbox.aspx>.

而無藉由進入沙盒以取得法規豁免之必要性<sup>422</sup>。

在順利於實驗屆滿後取得執照之申請人中，Kristal Advisors (SG) Pte Ltd.（下稱「Kristal Advisors」）係應用人工智慧提供數位資產管理服務，具體言之，其運用機器學習的技術持續針對投資者的決策進行分析和學習，俾向投資者提供客製化的投資組合建議。Kristal Advisors 係於 2017 年 8 月 10 日獲准進入沙盒，並於 2018 年 8 月 10 日完成實驗並退出沙盒，實驗期間約為一年。Kristal Advisors 於實驗期間從事之服務依新加坡法屬特許行業，於實驗結束後，該公司即依照新加坡證券和期貨法第 86 條（section 86 of the Securities and Futures Act），取得資本市場服務執照（Capital Markets Services Licence），該執照並於 2018 年 8 月 11 日起生效。其次，Kristal Advisors 亦就特定服務內容取得新加坡金融顧問法（Financial Advisers Act）之豁免。

自 Kristal Advisors 案例以觀，其於沙盒實驗結束後能立即取得有效之執照和法規豁免，進而無縫接軌地繼續推展相關服務，似意味著 MAS 或新加坡主管機關，就申請人實驗結束後之退場機制能提供即時安排，故無論是消費者或業者均不會面臨相關服務於實驗結束後即瞬間停擺之窘境。

### 三、 歐盟

歐盟雖尚未制定出具體之金融監理沙盒制度，惟歐盟針對於金融創新的發展，於 2018 年 3 月 8 日發布之官方新聞稿中表示，其將提出「金融科技行動方案（Fintech Action Plan）」，以促進金融業採用新技術（例如：區塊鏈、人工智慧和雲端服務等），使金融市場環境變得更加安全，並有助於新的市場進入者加入。此一行動方案是歐盟執委會建立「資本市場聯盟（Capital Markets Union）」，以及為了增進金融服務消費者福祉而擬建立之單一市場的部分進程。歐盟執委會於行動方案提出若干目標，以期透過創新商業模式擴大並支持新科技、增強網路安全以及金融系統的完整性：

- 歐盟執委會將成立歐盟金融科技實驗室，使歐盟和各成員國機關得與技術

---

<sup>422</sup> 盧沛樺（2017 年 12 月 13 日），〈玩假的？亞洲第一開跑的新加坡監理沙盒，為何只有一家新創業者通過〉，載於 <https://www.cw.com.tw/article/article.action?id=5086785>。

提供者共同在一不具商業性的環境合作。

- 歐盟執委會已建立歐盟區塊鏈觀測所及論壇（EU Blockchain Observatory and Forum.），將於 2018 年底報告與加密資產相關的挑戰和機會，且目前正廣泛性地研擬有關分散式帳本技術和區塊鏈的策略，以因應所有經濟部門在新科技之應用下可能面臨到的問題。
- 歐盟執委會將針對應如何促進歐洲之上市公司發布的數位化訊息徵詢意見，包含利用創新技術與國家數據庫相連，使投資者更易於取得對其投資決策具關鍵性的資訊。
- 歐盟執委會將展開研討會以改善資訊共享的網路安全議題。
- 歐盟執委會將依據「歐洲金融監管局（European Supervisory Authorities, ESAs）」所發布的指導，提出一監理沙盒之最佳典範（best practices）的藍圖。

自上述目標觀察，可知目前歐盟對於金融科技係抱持鼓勵及正面的態度，惟因歐盟執委會所公布之相關新聞稿和資料，並未有較為明確和具體的制度內容，故未來歐盟執委會在面對結合了人工智慧之金融創新服務（例：機器人投資顧問）之相關議題時，將會採取何等政策，尚未明朗。與英國及新加坡相比，歐盟對於金融創新科技的推動似乎起步較晚，但歐盟對於機器人投資顧問之發展現況，並非毫無關注。舉例而言，屬於歐盟金融監管局（European Supervisory Authorities, ESAs）<sup>423</sup>之一的「歐洲證券及市場管理局（European Securities and Markets Authority, ESMA）」即將其對於機器人投資顧問之看法，納入其於 2018 年 5 月 28 日公布之有關新版歐盟金融工具市場指令（Directive on Markets in Financial Instruments repealing Directive 2004/39/EC）之適合性要求的指導方針最終報告<sup>424</sup>，而此方針亦將取代 ESMA 於 2012 年公布（針對 MiFID I 適合性

---

<sup>423</sup> 歐盟境內共設有三個 ESA，分別為歐洲銀行管理局（European Banking Authority, EBA）、. 歐盟證券及市場管理局（European Securities and Markets Authority, ESMA）及歐洲保險和職業退休金管理局（European Insurance and Occupational Pensions Authority, EIOPA），請參考：歐盟官方網站，[https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/european-system-financial-supervision\\_en](https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/european-system-financial-supervision_en)。

<sup>424</sup> European Securities and Markets Authority, Final Report– Guidelines on certain aspects of the MiFID II

要求)之舊版指導方針<sup>425</sup>。

新的指導方針僅適用於提供投資建議或投資組合管理服務之業者，特別是針對擬在歐盟提供機器人投資顧問服務之業者，該指導方針強調業者應注意若干原則，包含：

- (一)應清楚明瞭地告知投資人其適合性評估以及進行適合性評估之目的，且應向投資人說明在機器人投資顧問服務中，人力介入的程度，以及在面臨疑問時應如何尋求協助；
- (二)業者應揭示自動化服務所使用之演算法，並提供與演算法相關之充足資訊予投資人；
- (三)業者應注意是否當投資人使用不同之平台（例如：不同的行動裝置）瀏覽資訊時，資訊之展示對於投資人是否足夠清楚；
- (四)業者應向投資人說明將如何應用蒐集而來之投資人資訊，提供投資顧問服務；
- (五)業者應確保其雇用之負責設計適合性問卷、相關演算法以及檢查適合性要求是否受到遵循之人員，具有適當且充分之知識和專業等。

儘管歐盟之指導原則僅具有建議性質，對歐盟成員國之執法機關不具有拘束力，但實務上各成員國均會相當程度地遵循指導原則所建立之相關標準，故上述有關提供機器人顧問服務適合性要求之指導原則，仍具有參考之價值。

#### 四、日本

日本監理沙盒制度可分為兩類，分別為地域限定型及專案型<sup>426</sup>。地域限定型監理沙盒係由地方自治體提案以自動駕駛技術及無人機等為對象，藉由 2017 年 9 月 22 日施行之國家戰略特區法及構造改革特區法之部分修正案（簡稱「國

---

suitability requirements,

[https://www.esma.europa.eu/system/files\\_force/library/esma35-43-869-\\_fr\\_on\\_guidelines\\_on\\_suitability.pdf](https://www.esma.europa.eu/system/files_force/library/esma35-43-869-_fr_on_guidelines_on_suitability.pdf)

<sup>425</sup> [https://www.esma.europa.eu/system/files\\_force/library/2015/11/2012-387\\_en.pdf](https://www.esma.europa.eu/system/files_force/library/2015/11/2012-387_en.pdf)

<sup>426</sup> 星野剛（2018 年 7 月 7 日），〈日本の競争力強化に必要な必要なサンドボックス制度〉，載於 <http://agora-web.jp/archives/2033588-2.html>。



家戰略特區改正法」)<sup>427</sup>引進；相對地，專案型則是由企業提案以金融科技及人工智慧為對象，透過2018年6月6日甫施行之生產性向上特別措施法（簡稱「生產性革命法」）實施。

面對包括英國新加坡等國家紛紛創設監理沙盒制度，特別是在金融科技的方面，吸引新技術、新事業，並爭取優秀人材的國際競爭情勢下，日本在引進前述兩類監理沙盒前，係透過產業競爭力強化法中引進的企業實證特例制度及消除灰色地帶制度（下稱「既存制度」）來推動以企業為單位的管制改革，以協助新創事業。

然而，在加速創新之社會應用的過程，日本發現既存制度有以下三大課題存在：(1)管制機關因缺乏證據而遲疑不敢改變管制作法，但企業卻正因為管制存在而無法試行錯誤，更難取得改革所需資料；(2)實驗計畫所需對象、期間及風險管理體等方法論不明確，企業調整耗費許多成本時間；(3)企業期待能提供第一線實驗協助的支援體制<sup>428</sup>。因此，日本乃參考外國經驗，分別於國家戰略特區改正法及生產性革命法提出了日本版的監理沙盒。

生產性革命法引進的專案型管制沙盒<sup>429</sup>，目的在於檢證人工智慧、物聯網及區塊鏈等創新技術實用化的可能性，並運用藉由實驗所得資料進行管制變革。具體來說，即為蒐集改革管制所需資料，以限定期間及參加者之方式先開放（不受現行管制）進行實驗，待實驗蒐集資料後，再據以進行管制的改革，從而促進新技術與新事業之創出。專案型管制沙盒之適用對象包括金融或非金融業者，日本政府已於內閣官房設置單一窗口「新技術等社會應用推進團隊」作為跨政

---

<sup>427</sup> 在此修正法律（平成29年6月23日法律第71號），為了加速創新技術之社會應用，日本政府引進了以(1)自動駕駛、(2)無人機，及(3)相關無線電頻譜應用等前端技術實證為主要目的之日本版管制沙盒。該法律中所引進的監理沙盒制度，適用對象為針對特區內之地方自治體提案實施以地域為限定範圍的實證計畫，故稱之為地域限定型監理沙盒。參公益財團法人地方自治總合研究所（2018年6月），《地方自治關連立法動向第5集》，第49-50頁，載於<http://jichisoken.jp/publication/researchpaper/125/No.125.pdf>。因其對象與金融科技無關，故不在本報告討論範圍內。

<sup>428</sup> 內閣官房日本經濟再生總合事務局（2017年11月8日），構造改革徹底推進會合「第4次產業革命」會合（第1回）〈論管制沙盒制度〉，載於<https://www.kantei.go.jp/jp/singi/keizaisaisei/miraitoshikaigi/suishinkaigo2018/revolution/dai1/siryou1.pdf>。

<sup>429</sup> 與既存之「企業實證特例制度」及「灰色地帶消除制度」共同作為企業單位之管制改革措施，國家戰略特區（含地域限定型管制沙盒制度）屬於地區單位管制改革措施，至於全國單位管制改革措施則是由管制改革推進會議負責主導，最終則於內閣官房設置單一窗口「新技術等社會應用推進團隊」負責與企業對接溝通。

府部會的專案申請窗口，並於 2018 年 6 月 6 日起正式開放申請，惟至 2018 年 12 月上旬尚未正式公告任何已開始或已完成之實驗專案<sup>430</sup>。

申請專案型監理沙盒不限於本國企業，外國企業亦可申請。從申請到核准大致可分為以下階段<sup>431</sup>：(1)**單一窗口提供業者諮詢**。由新技術等社會應用推進團隊就新技術等創新性之確認、新技術等相關規定之確認、整理及（目的事業及法令之）主務大臣之確認等提供業者建議，並跨部門引介適當政策資源。(2)**經單一窗口向主務大臣提出申請**。主務大臣經單一窗口收受新技術等實驗計畫。(3)**主務大臣聽取委員會意見**。主務大臣於受理申請之日起原則上應於 1 個月內將資料提交創新性事業活動評價委員會聽取其意見。(4)**專案核准及公告或核駁通知**。主務大臣基於創新性事業活動評價委員會之意見，審查該新技術等實驗計畫之准否，於核准時，除原則上應於創新性事業活動評價委員會表達意見之日起 1 個月內向申請業者交付核准證<sup>432</sup>外，並應通知創新性事業活動評價委員會。

業者申請時擬定之計畫書依生產性革命法第 11 條第 3 項各款規定應記載以下事項：(1)新技術等實驗目標；(2) 新技術等實驗內容（包括新技術等及創新事業活動之內容、實驗內容及其實施方法及就該新技術等相關管制之分析內容及其實施方法）；(3)新技術等實驗之實施期間及實施場所；(4)參加者等之具體範圍及該參加者等同意之取得方法；(5)新技術等實驗實施所需資金金額及其募集方法；(6)計畫所涉新技術等相關管制之法律及命令；(7)擬適用管制特例措施時，該管制特例措施之內容；及(8)其他與新技術等實驗實施相關必要事項<sup>433</sup>。

---

<sup>430</sup> 經許可之實驗專案皆會公開於首相官邸網站下之「新技術等社會應用推進團隊」（管制沙盒制度 政府單一綜合窗口）網頁，載於 <http://www.kantei.go.jp/jp/singi/keizaisaisei/regulatorysandbox.html#testing>。

<sup>431</sup> 新技術等社會應用推進團隊（2018 年 6 月 15 日），〈新技術等実証の総合的かつ効果的な推進を図るための基本的な方針〉，載於

<http://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/underlyinglaw/basicpolicy.pdf>。

<sup>432</sup> 核准證應記載以下事項：(1)核准年月日；(2)核准新技術等實驗實施者之姓名或名稱及住所，為法人時其代表人之姓名；(3)該核准之新技術等實驗計畫之內容及實施期間；(4)該核准之新技術等實驗計畫符合生產性革命法第 11 條第 4 項各款規定之意旨。核准新技術等實驗實施者於徵求參加者等之同意時，應向其提示核准證，並於取得同意時應報告主務大臣。

<sup>433</sup> 經許可之實驗專案皆會公開於首相官邸網站下之「新技術等社會應用推進團隊」（管制沙盒制度 政府單一綜合窗口）網頁，載於 <http://www.kantei.go.jp/jp/singi/keizaisaisei/regulatorysandbox.html#testing>。

主務大臣於受理實驗計畫時，經認定符合以下所有條件時，應為核准（如前所述，並應聽取委員會意見）。

- (一) 該新技術等實驗計畫依創新事業活動相關執行計畫<sup>434</sup>及基本方針是否適切。
- (二) 該新技術等實驗計畫所涉新技術等實驗（含取得參加者等之同意）是否可期待其圓滑且確實實施。
- (三) 該新技術等實驗計畫之內容未違反法律、授權命令（含告示）及生產性革命法第11條第3項第6款<sup>435</sup>所訂新技術等相關規定。

計畫核准之變更與撤銷，主要分為三類：

- (一) 新技術等實驗計畫之變更程序：實施者擬變更經核准之計畫時，必須提出該核准之核准證並經主務大臣再次審核，該審核程序與初次核准時相同。
- (二) 未依核准計畫實施實驗時之撤銷核准：主務大臣於認定實施者未採取適切實施該實驗所必要之措施、未能取得且確認實施實驗所足夠之參加者的同意或未依核准計畫實施實驗時，得撤銷該核准。
- (三) 核准計畫不符任一核准條件時指示變更計畫或撤銷核准：主務大臣於實施者未能依計畫取得同意、且確認實施計畫之新技術等顯有困難等認為有不符合核准條件之情形時，得命實施者為計畫變更或撤銷其核准。於此情形，主務大臣應聽取創新性事業活動評價委員會之意見。

於實驗進行期間，主務大臣應從持續監測實驗的觀點出發，考量業者負擔，針

---

<sup>434</sup> 原文為「革新的事業活動に関する実行計画」，係依生產性革命法第6條第1項於本執行計畫中明示現階段之政策措施之目的與內容、實施期程及其負責之部會。詳細內容載於 [https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2018\\_keikaku.pdf](https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2018_keikaku.pdf)。

<sup>435</sup> 第11條第3項第6款規定：「與同法第2條第2項第2款所定管制相關之新技術等相關規定。」（該款原文為：「第二条第二項第二号に規定する規制に係る新技術等関係規定。」）同法第2條第2項第2款復規定：「於就新技術實用化之相關管制進行分析時，應就包含該新技術實用化所必要之應有管制方式在內之議題，進行分析並評估其結果。」（該條文原文為：「新技術等の実用化に当たって当該新技術等に関する規制について分析する場合にあっては、当該新技術等を実用化するための規制の在り方を含めた課題についての分析及びその結果の検討を行うものであること。」）

對以下事項採取因應措施。

(一) 實施者應就核准計畫之實施情形，除實驗過程中定期報告及實驗結束後之報告外，應於實驗中發生問題時立即報告主務大臣。除前述報告外，主務大臣應與實施者保持密切連繫，儘可能把握計畫實施情形。

(二) 主務大臣於適切把握實驗實施情形後，視得情形依生產性革命法第14條規定提供實施者必要資訊及建議，俾使實驗得以順暢且確實實施。又，於認為有不符核准條件或未依核准計畫實施實驗時，主務大臣得撤銷其認定。

於實驗結束以後，依生產性革命法第 20 條規定，計畫所涉新技術等相關管制之法律及命令的主務大臣應就管制特例措施之引進及適用情形、各國相同管制之情形及技術發展情形等進行評估，並基於該評估結果採取廢止或放寬管制所必要之法制措施或其他措施。此外，創新事業活動評價委員會就其負責評價新技術等實驗計畫等對整體經濟之波及效果的任務而言，應於實驗結束後，確認該實驗是否如最初評價時一樣對創新事業活動的實施作出貢獻。其後，並應視情形並得依生產性革命法第 34 條<sup>436</sup> 請求主務大臣為報告。由上以觀，就生產性革命法所核准之實驗計畫，在實驗期間屆滿後如何與現行法規調和，似乎仍有賴相關管制規定之相應修訂或鬆綁。

整體而言，日本生產性革命法之監理沙盒，因其適用對象包括金融及非金融產業，從而可能有同一實驗涉及複數主管機關之情形，為避免業者在不同主管機關間疲於奔命，甚或有各權責機關管轄劃分不明之情形，生產性革命法創設單一窗口提供業者諮詢，整合跨部門資訊與資源，將有助於業者釐清所涉權責機關及法規相關議題，並可透過單一窗口之設計達成跨部門協調之功效<sup>437</sup>。我國實驗條例目前雖僅適用於金融科技實驗，由金管會作為單一主管機關，尚無跨部門整合之立即需求，惟伴隨著金融科技之應用及發展，倘未來出現涉及超出

---

<sup>436</sup> 生產性革命法第 34 條規定：「委員會於為執行其所掌事務之必要範圍內，得要求主務大臣或提出新技術等實證計畫或創新性資料產業活用計畫者，提出報告或資料。」（該條文原文為：「委員會は、その所掌事務を遂行するため必要な限度において、主務大臣又は新技術等実証計画若しくは革新的データ産業活用計画を提出した者に対して、報告又は資料の提出を求めることができる。」）

<sup>437</sup> 陳譽文，日本「監理沙盒制度化」之法制推動趨勢--簡介「產業競爭力強化法」修法與「生產性向上特別措施法」草案，《科技法律透析》，頁 70。

金管會單一機關管轄而涉及複數主管機關之情形，似亦可參考日本立法設計，考慮設置跨部門單一窗口提供業者諮詢。

### 第三項 針對我國法規調適之初步建議

現階段臺灣之金融產業運用人工智慧較為顯著的例子，即為機器人投資顧問。查我國現行規範，目前與機器人投資顧問最為相關之規範，為金管會於 2017 年 6 月 29 日同意投信投顧公會所報「中華民國證券投資信託暨顧問商業同業公會證券投資顧問事業以自動化工具提供證券投資顧問服務（Robo-Advisor）作業要點」（下稱「作業要點」）。作業要點就自動化投資顧問之定義、瞭解客戶作業、投資組合再平衡（Rebalancing）、監督措施及告知客戶使用該服務前之注意事項等訂定相關原則。惟作業要點之制定係為利證券投資顧問事業以自動化工具提供證券投資顧問服務，機器人投資顧問故如非證券投資顧問事業，即無適用作業要點之餘地，從而將有依據實驗條例申請進入創新實驗之需求。故以下將分別簡介作業要點和實驗條例之規範內容，並進一步探討機器人投資顧問服務之提供，是否有申請進入沙盒之必要。

#### 一、我國以自動化工具提供證券投資顧問服務相關法規

作業要點所稱「自動化投資顧問服務」，係指「完全經由網路互動，全無或極少人工服務，而提供客戶投資組合建議之顧問服務」，而前開定義所指涉之人工服務係屬輔助性質，僅限於協助客戶完成系統「瞭解客戶」（即 Know Your Customer, KYC）之作業，或針對客戶使用自動化投資顧問服務所得之投資組合建議內容提供解釋，不得調整或擴張自動化投資顧問服務系統所提供之投資組合建議內容，或提供非由系統自動產生之其他投資組合建議。作業要點不僅規範自動化投資顧問服務之定義，亦涵蓋演算法之監督、進行瞭解客戶作業與建議投資組合時應注意之事項、應確認自動化投資顧問服務系統能公正客觀的執行如：挑選投資組合等功能、投資組合再平衡之辦理方式、專責委員會之監督，以及對客戶應盡之告知義務等。此外，作業要點於立法理由亦揭示要點之訂定，係參考美國證券交易委員會（Securities and Exchange Commission, SEC）於 2015 年發布之警示、美國金融監管局（Financial Industry Regulatory Authority, FINRA）於 2016 年發布之數位投資建議研究報告，及其他國家相關之建議或指引。儘管作業要點之立意良善，惟仍有未盡之處，以再平衡交易為例，作業

要點要求應與客戶事先約定投資組合再平衡交易相關內容，然此與國外常見的機器人投資顧問所具有的自動下單功能有別，即非屬於「資產管理型」機器人投資顧問。一般而言，所謂的「資產管理型」之機器人投資顧問，不僅可提供理財建議，亦具有協助客戶進行財務規劃、資產重新配置及投資組合再平衡等功能。因此，資產管理型機器人所提供的服務多被認為近似於全權委託投資<sup>438</sup>（代客操作）行為。

目前我國之證券投資顧問業者，多係運用機器人投資顧問推介自家商品，再由客戶自行下單，故性質上應屬於諮詢建議型之機器人投資顧問。不過，透過資產管理型機器人投資顧問服務之提供，可使小額投資人享有使用資產管理服務的機會，故研發資產管理型機器人投資顧問，已成為世界上主要國家業者之發展趨勢。因此，為利證券投資顧問事業發展「資產管理型」自動化投資顧問服務（即自動為客戶執行再平衡交易），金管會於 2017 年 8 月放寬「再平衡交易」之條件，在維持與客戶原約定之投資標的及投資比例前提下，事先與客戶於契約中約定於個別投資標的或整體投資組合之損益達預設標準，或偏離原約定之投資比例達預設標準時，由電腦系統自動為客戶執行再平衡交易，得不受證券投資顧問事業管理規則第 13 條第 2 項第 2 款及證券投資顧問事業負責人與業務人員管理規則第 15 條第 2 項第 2 款有關投顧事業及其人員不得有代理他人從事有價證券投資行為規定之限制。

儘管金管會已放寬部分規範，但在現行法下，仍僅有投顧業或兼營投顧業者始得提供機器人投資顧問服務，換言之，就推動金融科技發展較有活力的新創產業，倘未能取得投顧業許可，將無法提供機器人投資顧問服務<sup>439</sup>。然查，相關法規遵循及維護成本恐非一般新創產業得以負擔，舉例而言，依照證券投資顧問事業設置標準第 5 條第 1 項之規定，成立證券投資顧問業之實收資本額應達新臺幣 2,000 萬元，從事全權委託投資顧問服務更需達新臺幣 5,000 萬元。其次，現階段證券投資顧問業者雖可與客戶約定自動化執行再平衡交易，但並不

---

<sup>438</sup> 證券投資信託及顧問法第 5 條規定：「全權委託投資業務：指對客戶委任交付或信託移轉之委託投資資產，就有價證券、證券相關商品或其他經主管機關核准項目之投資或交易為價值分析、投資判斷，並基於該投資判斷，為客戶執行投資或交易之業務。」

<sup>439</sup> 依現行規定，非投顧業者倘涉及對客戶提供證券投資分析意見或推介建議之服務（含以自動化投資顧問方式為之），並直接或間接收取報酬，應先經金管會許可經營證券投資顧問業務。就比較法而言，在美國從事自動化投資顧問與傳統投資顧問相同，均須受 1940 年投資顧問法規範並註冊為投資顧問。



包含業者可協助客戶進行資產重新配置和獲利再投資等屬於全權委託意義下之資產管理服務，故即便係取得從事全權委託投資顧問服務許可之證券投資顧問業，亦無法從事再平衡以外之其他涉及全權委託業務（如資產之重新配置）之機器人投資顧問服務。再者，縱令金管會於日後開放機器人投資顧問得從事全權委託業務，倘相關法規未配合修訂，則因現行法令規定證券投資顧問事業辦理全權委託投資業務，客戶委託資金必須達新臺幣 500 萬元之投資門檻，亦與一般大眾運用機器人投資顧問進行小額投資之需求不符，從而可能導致原本期盼機器人投資顧問得達成之普惠金融效益不彰。故主管機關未來如將開放機器人投資顧問得從事全權委託業務，建議亦宜同時考量全權委託之投資門檻是否應適度放寬<sup>440</sup>。

另外，縱令取得投顧業或兼營投顧業相關許可，現行法令以「人」作為提供服務主體之規範模式，亦與機器人投資顧問服務之本質未盡相符。例如，證券投資信託及顧問法規定客戶簽訂全權委託投資契約前，業者應指派專人解說，提供七日以上的契約審閱期間；於證券投資顧問事業負責人與業務人員管理規則中，有規定分析人員與業務人員等應具備相關專業證照或資格，惟類此規定適用於機器人投資顧問時，卻可能因相關理財建議係經由人工智慧之演算法分析及提供，而難以適用投顧從業人員之行為準則規範。上述例子亦反映出現行證券投資顧問事業相關法令所規範之面向，與機器人投資顧問為「全無或極少人工服務」之性質並不相符。機器人投資顧問凡此種種，均可能可透過金融監理沙盒之申請及運用，短程解決在機器人投資顧問在現行法令下所遭遇之困境。

## 二、實驗條例之制訂與施行

臺灣於今(2018)年制定實驗條例，其旨在建立安全之金融科技創新實驗環境，促進普惠金融以及落實消費者保護<sup>441</sup>。配合實驗條例之制訂與實施，證券投資信託及顧問法亦於今年增訂第 6-1 條，其中第一項明文規定：「為促進普惠金

---

<sup>440</sup> 就此，據本研究團隊了解，鑒於近期陸續有業者建議開放全面得由電腦系統自動為客戶執行資產配置及再平衡交易，使小額投資人能有類似全權委託之服務，金管會已於 2018 年 5 月 17 日函請投信投顧公會瞭解國外以自動化工具為客戶執行資產配置及再平衡交易之具體運作方式，並研議在避免違約交割前提下，該業務得於我國營運所需具體措施及運作模式，俟釐清實務作法後，金管會將檢視相關規定調整之可行性。

<sup>441</sup> 實驗條例第 1 條。

融及金融科技發展，不限於證券投資信託事業及證券投資顧問事業，得依金融科技發展與創新實驗條例申請辦理證券投資信託、證券投資顧問及全權委託投資業務創新實驗。」

所謂「創新實驗」，係指以科技創新或經營模式創新方式，從事屬於需金管會許可、核准或特許之金融業務範疇<sup>442</sup>。其次，金管會於評估准駁申請人之申請時，將審酌申請業務是否具有創新性，是否能有效提升金融服務效率、降低成本或提升消費者及企業之權益，及申請人是否已評估可能風險、訂有因應措施，並已建置參與者之保護措施等<sup>443</sup>。申請人應檢具申請書、申請人資料、創新實驗計畫等資料向金管會申請辦理創新實驗。<sup>444</sup>創新實驗期間原則上以1年為限，惟申請人得於該創新實驗期間屆滿1個月前，檢具理由向金管會申請核准延長，延長以1次為限，且延長期間不得逾越6個月。但創新實驗內容如涉及修法，延長期間之申請不以1次為限，惟全部實驗期間將不得超過3年<sup>445</sup>。如實驗範圍涉及金管會或其他機關訂定之規定，金管會得於會商其他機關同意後，於實驗期間排除相關規定全部或一部之適用，但與洗錢防制法、資恐防制法等相關之規範則不得排除<sup>446</sup>。

實驗期間屆滿之日起1個月內，申請人應將實驗結果函報金管會，金管會並將邀集專家、學者及相關機關和機構，針對實驗結果召開評估會議<sup>447</sup>。如創新實驗確實具有創新性、有效提升金融服務效率、降低經營及使用成本、有助於消費者和企業權益時，金管會應研修相關金融法規、提供創業或策略合作協助，或轉介予相關機構、團體或輔導創業之基金<sup>448</sup>。惟實驗期間如發現創新實驗對於金融市場與參與者有重大不利情事、實驗範圍逾越原受核准範圍或申請人違反附加之負擔、或未遵循本條例之規定及其他金管會要求辦理之事項，且經命限期改善而未改善時，金管會得廢止該實驗之核准<sup>449</sup>。

---

<sup>442</sup> 實驗條例第3條。

<sup>443</sup> 實驗條例第7條。

<sup>444</sup> 實驗條例第4條。

<sup>445</sup> 實驗條例第9條。

<sup>446</sup> 實驗條例第25條。

<sup>447</sup> 實驗條例第16條。

<sup>448</sup> 實驗條例第17條。

<sup>449</sup> 實驗條例第15條。



依據金管會提供之資料，實驗條例自 2018 年 4 月 30 日開始施行以來，截至同年 11 月底止，總計共 6 件申請案，已核准 1 件實驗案，駁回 1 件申請案，且有 4 件申請案尚在審查中，另有 24 家業者刻正接受創新實驗申請案之輔導。其次，金管會日前亦已發布首家進入沙盒之申請人及相關業務資訊，惟該申請人所提供之服務與人工智慧並不相關<sup>450</sup>，故其他申請人擬提供之服務，是否有結合人工智慧技術者（例如：先前受到廣泛討論的機器人投資顧問），目前仍無法得知。

倘若先不論申請人擬提供之業務種類為何，僅探討我國監理沙盒制度之適用，可發現儘管我國之監理沙盒，係取法於英國和新加坡之監理沙盒制度，仍有下述面向與英國、新加坡制度有顯著差異：

- 與英國和新加坡相較，我國監理沙盒之實驗期間明顯較長（如涉及修法，最長可達三年），此一期間之制定雖係因成文法國家所需立法程序較長，惟法規調適期間如耗費過多時間，亦意味申請人實驗期間之延長，因持有特許執照之金融行業，其法規遵循成本（包括受管程度）往往遠高於非特許事業，故可能導致市場競爭不公平之情事發生<sup>451</sup>。
- 就實驗完成後之安排，儘管實驗條例第 17 條有包括檢討研修相關金融法規、提供創業或策略合作協助、轉介予相關機關（構）、團體或輔導創業服務之基金等規定，但實際成效如何，尚有待觀察。以「檢討研修相關金融法規」為例我國係屬成文法系國家，立（修）法程序較為繁複，倘無適當之退場機制，將可能產生實驗者於退出沙盒後無法繼續從事相關業務之窘境，故如何加快立（修）法速度，將影響申請人於實驗結束後如何繼續合法進行相關業務<sup>452</sup>。

---

<sup>450</sup> 金管會（2018 年 10 月 18 日），〈金管會核准首宗金融科技創新實驗申請案〉，載於 [https://www.fsc.gov.tw/ch/home.jsp?id=2&parentpath=0&mcustomize=news\\_view.jsp&dataserno=201809180004&aplistdn=ou=news,ou=multisite,ou=chinese,ou=ap\\_root,o=fsc,c=tw&dtable=News](https://www.fsc.gov.tw/ch/home.jsp?id=2&parentpath=0&mcustomize=news_view.jsp&dataserno=201809180004&aplistdn=ou=news,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News)。

<sup>451</sup> 彭金隆、臧正運（2017 年 2 月 16 日），〈觀念平台—後監理沙盒階段的做法才是關鍵〉，載於 <http://www.chinatimes.com/newspapers/20170216000074-260202>。

<sup>452</sup> 就此，據了解金管會在核准申請人創新實驗時，將先進行該實驗相關金融法規之檢視，並在實驗期間透過定期報告、實地訪查或相關輔導協助，瞭解該創新實驗之辦理情形，如經評估已有效提升金融服務之效率、降低經營及使用成本或提升金融消費者及企業之權益者，不待實驗結束，金管會即進行檢討研修相關金融法規，並經評估有修法必要者，即刻啟動相關法制程序。另若涉及法律修正，金管會亦將儘

由上可知，臺灣之監理沙盒能否發揮其立法宗旨，關鍵仍在於如何協助實驗成功的申請人於退出沙盒後，能順利進入市場，而欲達此一目的實有賴主管機關給予更為明確的指引和積極的協助。儘管因英國和新加坡為普通法系國家，故臺灣監理沙盒在規範制度上，並無法全然複製，但普通法系國家經常使用的豁免，亦只有在法有明確授權時監管者始得為之，在法未允許的情況下，監管者亦僅能以核發承諾函或行政指導之方式，提供業者協助<sup>453</sup>。故有論者認為我國似可參酌上述作法，於現行金融規範中新增相關豁免規定或以法律授權主管機關在監管面向上享有更大之裁量權，以便主管機關在申請人之實驗結束後，得提供申請人更多轉換及調適空間<sup>454</sup>。

除此之外，有論者亦主張，實驗結束後可能採取的作法，包含給予附條件或附負擔的許可，或建置金融營業執照分級制度等。給予附條件或附負擔的許可，係指申請人實驗成功並退出沙盒後，由主管機關給予許可，並要求業者履行一定條件或義務(例：保證金提存、資本或組織方面應滿足現行法規之部分要求)<sup>455</sup>。而所謂金融營業執照分級制度，係指不強制屬於非金融業者之申請人於實驗結束後，即必須完全滿足現行規範，以取得相關營業執照，而視申請人擬提供的服務或商品之性質，發放不同等級的營業執照，亦即，若申請人僅提供特定之金融業務，則其退出實驗後所應達到的資本額要求或受監管之密度，相較於一般金融業者可相對降低<sup>456</sup>。畢竟申請人可能係因缺乏資金或人力上之資源，致無法或不易取得金融執照，故才選擇申請進入沙盒，若主管機關要求其於退出沙盒後仍必須立即完全達到與傳統金融業相同之規範要求，則可能失去監理沙盒鼓勵金融創新之初衷，且將影響沙盒原預期帶來扶植新創業者的成效。

上述作法儘管看似不同，但核心概念均是希望主管機關得針對金融科技創新採取不同等級之差異化管理。蓋金融業本屬受到高度管制的產業，故在倡導普惠

---

速於完成法律制(修)之檢討後函報行政院審議。凡此種種，均將有助於參與實驗者於實驗結束後能繼續從事相關業務。

<sup>453</sup> 臧正運(2016年9月1日)，〈臧正運觀點：金融科技创新監理芻議－監理沙盒在台灣〉，載於 <https://www.storm.mg/article/160609>。

<sup>454</sup> 同上註。

<sup>455</sup> 彭金隆、臧正運(2017年2月16日)，〈觀念平台－後監理沙盒階段的作法才是關鍵〉，載於 <http://www.chinatimes.com/newspapers/20170216000074-260202>。

<sup>456</sup> 同上註。

金融、鼓勵新創業者發展金融創新之同時，如要求申請人於離開沙盒後仍應立即滿足現行所有規範，始能繼續從事相關創新金融業務，亦可能降低新創業者參與實驗的意願，進而扼殺金融創新帶給消費者和市場福祉之可能。此外，值得注意者為，金融業本即受許可得經營金融相關業務，故金融業者與非金融業者申請入沙盒的情況及將面臨的問題亦難以等同視之，故建議運作監理沙盒時，宜針對金融業者與非金融業者進行差異化管理，始能在鼓勵非金融業者投入金融創新之同時，亦提供金融業者以金融科技發展創新服務和商品之誘因。

### 三、小結

誠如前述，臺灣之監理沙盒似仍有其制度面上的侷限，首先，不論是以何種新科技結合金融服務進而申請進入沙盒，都將同樣面臨退場機制之安排問題，若未能協助申請人在實驗結束後得順利持續其營運模式，將降低業者申請進入沙盒之意願。其次，依照實驗條例第 11 條之規定，申請人成功進入監理沙盒實驗後，金管會即會將其創新實驗內容揭露於機關網站，惟此是否等同於公開申請人之商業機密，而產生申請人之業務內容可能受到抄襲或模仿，甚或遭受其他業者搶先於監理沙盒外施行的疑慮，亦可能造成申請人對參與實驗感到怯步。是以，如何在消費者權益維護、資訊公開，以及申請人營業秘密保障等各潛在衝突之目的間加以權衡，將是主管機關應審慎思量的議題之一。

另外，參與作成實驗准駁決定之審查委員是否能避免潛在利益衝突問題，亦頗值深思。按金融科技創新實驗審查會議及評估會議運作辦法第 4 條規定：「審查會議及評估會議均應置成員七人至二十一人，由主管機關洽相關機關（構）指派人員，並邀請具有與申請案相關專門知識、技術或經驗之專家及學者，共同參與審查。專家及學者之比例不得少於會議成員總額三分之一，並不得超過會議成員總額二分之一。」雖然同辦法第 11 條明定審查會議及評估會議之成員應遵循之利益迴避事項規定，然而未來在個案上如何認定會議成員有不能公正執行職務之虞，將值得持續觀察。

然而，除了上述疑慮外，對於擬發展機器人投資顧問服務的業者而言，其將面臨的難題可能不僅止於此。首先，對於證券投資顧問業者來說，本無須申請進入沙盒即可從事「諮詢建議型」之機器人投資顧問服務，倘若擬協助客戶進行

自動化再平衡交易，則取得客戶之事前同意後亦可為之。但若業者擬發展「資產管理型」之機器人投資顧問服務，即會面臨到若干挑戰，蓋此一服務類型性質上近似於全權委託，業者理應在符合從事全權委託之相關資格要求後，即可提供此一服務，惟目前金管會並未開放全權委託之機器人投資顧問服務，故當業者有意發展「資產管理型」之機器人投資顧問服務時，亦因現行法規未開放此一服務而無從取得許可，而需藉由申請進入沙盒以尋求相關法規的豁免。其次，對於新創業者而言，若本身不具有相當之資格或資力而無法成為證券投資顧問業者時，無論是提供何種類型的機器人投資顧問，應均有取得相關法規豁免之需求，從而有賴進入沙盒始有從事相關業務之空間。

金融監理沙盒是否能確實為鼓勵金融創新帶來成效，仍須視主管機關有無建置相關退場機制，輔助較無資力或未達相關規範門檻之新創業者在離開沙盒後，得順利進入市場上發展而定。不過值得思考的是，對於擬提供金融創新服務但尚未取得執照之新創業者而言，現階段似僅限於申請進入監理沙盒，始有受到主管機關輔導的空間。然而，在退場機制目前未有較為明確的走向之前，新創業者是否願意申請沙盒，仍有待觀察。事實上，金管會近期亦考量到金融科技業者離開沙盒後，如仍未達相關資力要求，則其金融創新服務可能難以進入市場，故針對部分金融業務，包含跨境匯款、支付業務、保險、機器人理財業務等，已著手研議開放有限執照之可能性。惟在現行法律框架下發放有限執照，尚須視相關業法有無授權，若否，則仍待未來修法後，始有進一步探討之空間。儘管如此，未來主管機關若開放有限執照之申請，對於僅從事部分業務之業者而言，即不用滿足全業執照所要求之高額資本額門檻，而有限執照下資本額要求之降低，亦意謂著金融創新服務進入市場的機會大增，更有助於普惠金融目標的實現，故金管會日後對於有限執照將會有何等之規劃，值得持續追蹤觀察。

457

除了退場機制可能攸關監理沙盒之成效外，另一值得留意者為「創新性」之要求。蓋我國之監理沙盒，與英國和新加坡相同均要求具創新性<sup>458</sup>，但目前國內

---

<sup>457</sup> 參見：邱金蘭（2018年10月8日），〈金管會研議開放有限執照 匯款、支付等業務最可行〉，載於 <https://udn.com/news/story/7239/3411177>。

<sup>458</sup> 參見金融科技創新實驗管理辦法總說明第6條及其說明。

已有部分銀行推出主打結合人工智慧技術之機器人投資顧問服務，若有申請人欲以機器人理財服務業務申請進入沙盒，視申請人與既有業者提供服務所運用之技術之相近程度，該業務是否仍具有創新性，似非全然無疑。蓋既同樣都為機器人投資顧問服務，除了所應用的科技有明顯差異者之外，申請人應如何證明其提供之服務與市場上已存在的服務顯著不同而具有創新性，又使用不同之演算法，得否作為創新性之佐證，均有待觀察。

基於上述，如擬發展機器人投資顧問，短程而言似得以金融監理沙盒申請作為起點，惟中長程仍有賴證券投資信託及顧問法及其相關法規之鬆綁和調整，包括開放自動化機器設備得從事全權委託業務，降低相關業務之執照門檻及投資門檻，建立分級化之管理制度等，但無論如何，主管機關在確立相關政策之前，均應儘速表明其監管立場，以及未來法規調整之方向，始有助於機器人投資顧問業務之發展。惟考量機器人投資顧問產業目前仍在持續發展中，要求主管機關應立即通盤調適相關法規範，顯非易事。故對於具有大量創新色彩之結合人工智慧的自動化服務，主管機關不妨鼓勵業者積極申請進入沙盒實驗，在實驗期間若發現創新服務在適用現行法規時，確實有窒礙難行的情況發生時，主管機關即可儘速研擬適當之因應措施。換言之，藉由實驗的進行以發掘此一創新服務可能面臨到的困境和具有的潛在風險，始有辦法確認既有之金融法規是否有辦法因應新型態之金融商業模式之需求，以進一步制定適宜的政策與規範，更有助於強化金融創新服務或商品之消費者的權益保護，從而達成鼓勵金融創新之目標。

## 第七節 人工智慧運用於醫療服務之相關法律疑義

### 第一項 焦點議題

將人工智慧（Artificial Intelligence，簡稱 AI）引進與醫療服務密切相關之醫藥研發及醫療臨床實務為當務之急。近年來資訊軟體與硬體之快速發展，將 AI 帶入另一個新境界。繼 Google AlphaGo 打敗南韓棋王李世石，讓全球對 AI 有了不同看法；IBM Watson、Apple Siri、研發無人駕駛之各家廠商…等，相繼於不同的領域展現 AI 之應用<sup>459</sup>。於 AI 快速與各產業需求及服務發展結合之潮流中，醫療產業無疑是 AI 發揮顯著功能的領先產業之一。根據麥肯錫的研究報告，在 2025 年前，AI 將創造 50 兆美元的新價值，而其中有一大部分是與醫療相關<sup>460</sup>。Healthcare IT News 於 2017 年 5 月之報導亦指出<sup>461</sup>，美國約 86% 之醫療機構、生物科技及技術公司已在使用某種形式的 AI，許多醫療機構也都展開 AI 專案。美國網際網路巨頭亞馬遜公司創始人傑佛瑞貝佐斯（Jeff Bezos）亦曾言及「醫療（服務）將會是那些透過機器學習與 AI 提升並變得更好的產業之一」<sup>462</sup>，而美國前五大科技股 FAAMG（即 Facebook、蘋果、亞馬遜、微軟及 Google）等科技業領航者亦紛紛開展相關研究及合作，可預期未來數年內，醫療服務產業將投入更多資源、資金與人力於 AI 之運用。

此外，隨著 AI 技術蓬勃且迅速發展，全球生醫界目前積極投入「精準醫療」(Precision Medicine) 的推動，除了透過傳統方法由病患描述症狀及傳統常規檢查，會再加上生物醫學檢測，如基因檢測、蛋白質檢測、代謝檢測等，將個人資料如性別、身高、體重、種族、基因檢測、蛋白質檢測、代謝檢測、過去病史、家族病史等，透過人體基因資料庫進行比對及分析，從中找出最適合病患的治療方法與藥品。<sup>463</sup>而由診斷到追蹤、風險預測到個人化治療等階段，甚至生物資料庫的建立與分析，均有賴

---

<sup>459</sup> 論壇「健康醫療資訊科技發展政策建言」委員會（2018），《健康醫療資訊科技發展政策建言》，頁 47、50，苗栗：財團法人國家衛生研究院。

<sup>460</sup> James Manyika, et al. (May, 2013). *Disruptive technologies: Advances that will transform life, business, and the global economy*. San Francisco, CA: McKinsey Global Institute. Retrieved from [https://www.mckinsey.com/~media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Disruptive%20technologies/MGI\\_Disruptive\\_technologies\\_Full\\_report\\_May2013.ashx](https://www.mckinsey.com/~media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Disruptive%20technologies/MGI_Disruptive_technologies_Full_report_May2013.ashx)

<sup>461</sup> Bill Siwicki (May 19, 2017). 86% of Healthcare Companies Use Some Form of AI. Healthcare IT News. Retrieved from <http://www.healthcareitnews.com/news/86-healthcare-companies-use-some-form-ai>

<sup>462</sup> Kristin Houser. (March 26, 2018) Amazon Is Really Serious About Making Healthcare a Part of Its Future, available on <https://futurism.com/amazons-healthcare-plans/>

<sup>463</sup> 葉席吟（2016），〈精準醫療之各國推動政策觀察〉，國家實驗研究院科技研究與資訊中心網頁，<https://portal.stpi.narl.org.tw/index/article/10278>（最後瀏覽日：10/18/2018）

AI 技術的發展與參與<sup>464</sup>。

因此，如何將 AI 技術導入臨床實務，甚至每個醫療決策，以促進醫療服務之適當性、正確性與效率，進而提升醫療品質與患者安全，同時在民眾、患者與業者之權益間取得平衡，將是各國政府相關部門無從逃避且應積極面對的一大課題。<sup>465</sup>而運用 AI 於藥品、醫療器材及包括臨床實務在內之醫療照護產業(以下簡稱「醫療 AI」)，藉此協助醫藥研發各階段及對患者的治療，儼然已成為趨勢，雖仍在初始階段，但已有以下若干法律疑義浮現：

(一) 是否應將醫療 AI 列為醫療器材進行管理？

我國目前係由藥事法第 13 條<sup>466</sup>、醫療器材管理辦法等規定管制醫療器材。惟醫療 AI 面向多元，除其軟體本身，尚可能涉及各種裝置、儀器或用具之使用。而該軟體及相關工具是否屬於醫療器材，而須取得主管機關製造許可、販賣執照許可及申請查驗登記？若然，主管機關之查驗登記審查程序是否足以確保醫療 AI 之品質、安全性及有效性；若否，是否應透過其他機制予以監督。

(二) 是否應適度放寬醫療 AI 所仰賴之健康個人資料保護相關規制？

精準醫療所需的資料，不論是數量或複雜度都相當高，光是基因型因子至少就有三萬種；暴露型因子中，光是過敏原一項定義，就可以超過一萬七千種類型，再加上個人的疾病史、用藥與檢驗記錄等資料收集不易，而醫療 AI 強大的演算、分析功能便能發揮所長，分析這幾百萬種的變數，進而對病人進行準確的疾病預測、早期偵測和建議等。<sup>467</sup>然此等醫療 AI 所使用有關病歷、醫療、基因、健康檢查等個人資料(以下簡稱「健康個人資料」)有其特殊性，故我國

<sup>464</sup> 經濟日報(08/14/2018)，〈商業與觀點／發展精準醫療 AI 幫大忙〉，經濟日報網頁，<https://money.udn.com/money/story/8944/3307410> (最後瀏覽日：10/18/2018)

<sup>465</sup> Lincoln Tsang, et al. (2017). The impact of artificial intelligence on medical innovation in the european union and United States. *Intellectual Property & Technology Law Journal*, August 2017, Retrieved from <https://www.arnoldporter.com/-/media/files/perspectives/publications/2017/08/the-impact-of-artificial-intelligence-on-medical-innovation.pdf>；論壇「健康醫療資訊科技發展政策建言」委員會(2018)，〈健康醫療資訊科技發展政策建言〉，頁 47、50，苗栗：財團法人國家衛生研究院。

<sup>466</sup> 藥事法第 13 條：本法所稱醫療器材，係用於診斷、治療、減輕、直接預防人類疾病、調節生育，或足以影響人類身體結構及機能，且非以藥理、免疫或代謝方法作用於人體，以達成其主要功能之儀器、器械、用具、物質、軟體、體外試劑及其相關物品。前項醫療器材，中央衛生主管機關應視實際需要，就其範圍、種類、管理及其他應管理事項，訂定醫療器材管理辦法規範之。

<sup>467</sup> 李有專(2018)，〈醫療大未來—臺灣第一本智慧醫療報告〉，頁 142，新北市：好人出版

個資法將其列為特種類型個人資料，規定不得蒐集、處理或利用，致人工智慧醫材商、基因體科技公司等，無從使用健康個人資料。因此，如何適度放寬個人資料保護相關法規，以利醫療 AI 發展與應用，提升醫療服務品質，並兼顧相關隱私權保障及防範個人資料侵害，將是我國應面對的重要課題。

(三) 是否應按消費者保護法第 7 條<sup>468</sup>規定，逕將醫療 AI 視為純粹商品而有商品責任規範的適用，課予製造商或研發者嚴格的民事責任？

理論上，醫療 AI 產品係由硬體與軟體所組成，若其設計或製造具有瑕疵，例如因設計失誤或故障，導致醫療資訊沒有正確傳輸、出現錯誤照護指令或建議、使用者資料遺失或顯示錯誤、用藥或生理量測排程未即時提醒、資訊計算或分析錯誤等，甚且進而造成使用者人身或財產上之損害等重大後果時，應有消費者保護法第 7 條—商品責任規範之適用。惟醫療 AI 運用於臨床診斷與治療決定時的特殊性，以及黑盒子運作的不透明性（黑盒子醫學），致使能否將其視為純粹商品而有商品責任規範的適用，不無疑問。

## 第二項 外國文獻分析

### 一、醫療器材規範對於醫療 AI 之規制

#### (一) 歐盟

##### 1. 歐盟第 93/42/EEC 號指令

並非所有醫療照護體系所使用之醫療 AI 軟體均屬於醫療器材，然而根據其功能及適應症（或使用目的），得以判斷是否屬於歐盟法律定義下之「醫療器材」。按歐盟第 93/42/EEC 號指令第 1 條第 2a 項規定<sup>469</sup>，醫療器材係指其製造商意圖供人體使用以達疾病或身體狀況之診斷、預防、監測、治療及緩解等目的（下稱「醫療用途」）之任何工具或器具（包括軟體在內）。從而，製造商若基於醫療用途生產軟體，此

<sup>468</sup> 消費者保護法第 7 條：從事設計、生產、製造商品或提供服務之企業經營者，於提供商品流通進入市場，或提供服務時，應確保該商品或服務，符合當時科技或專業水準可合理期待之安全性。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。企業經營者違反前二項規定，致生損害於消費者或第三人時，應負連帶賠償責任。但企業經營者能證明其無過失者，法院得減輕其賠償責任。

<sup>469</sup> Council Directive 92/43/EEC of 14 June 1993 concerning medical devices Article 1 §2(a)



等軟體即應被歸類為醫療器材，而受相關規範。

## 2. 歐盟 MEDDEV 2.1/6, July 2016 指令

然而，實際將此等分類規則適用於軟體有其困難，因為軟體如何作用至人體以回復、矯正或調整人體生理功能，並不似一般醫療器材般一目了然。對此，歐盟委員會發布 MEDDEV 2.1/6, July 2016 指令（以下簡稱「MEDDEVs 指令」），作為解讀上述醫療用途判斷要件之準則<sup>470</sup>。該指令雖非法律而不具強制性，但至少代表主管機關歐盟委員會就醫療用途判斷要件應如何適用之共識。詳言之，以診斷疾病為目的而計算人體解剖結構上部位的影像處理軟體，通常會被歸類為醫療器材，因醫療照護專業人員利用這類影像處理軟體以協助進行臨床診斷及治療。反之，管理患者資料的軟體，或僅供儲存、歸檔及移轉患者資料的資訊系統，或改變患者資料以達去連結或去識別化目的之程式，此等軟體均不會被視為醫療器材。

## 3. Medical Devices Regulation, MDR ; Regulation (EU) 2017/745

在歐盟高峰會議及議會表決通過後，Medical Devices Regulation, MDR ; Regulation (EU) 2017/745（醫療器材規則，以下簡稱「Medical Devices Regulation」）及體外診斷醫材規則（In Vitro Diagnostic Medical Devices Regulation, IVDR ; Regulation (EU) 2017/746）已於 2017 年 5 月 5 日公布於歐盟的官方公報，並於 2017 年 5 月 25 日生效<sup>471</sup>。Medical Devices Regulation 的過渡期從生效日 2017 年 5 月 25 日起算 3 年至 2020 年 5 月 26 日止，將取代第 93/42/EEC 號指令<sup>472</sup>和主動植入式醫療器材指令（AIMD, 90/385/EEC）；體外診斷醫療器材規則的過渡期則是 5 年，至 2022 年 5 月 26 日止，將取代體外診斷醫療器材指令（IVDD, 98/79/EC）

---

<sup>470</sup> Guidelines on the Qualification and Classification of Stand Alone Software used in Healthcare within the Regulatory Framework of Medical Devices, MEDDEV 2.1/6. (July 2016)

<sup>471</sup> Official Journal of the European Union (L117) of May 5, 2017

<sup>472</sup> Regulation (EU) 2017/745 of the European Parliament and of the Council of April 5, 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.

Medical Devices Regulation 中不僅增設針對軟體醫材規範的專門條款，同時第 2 條第 1 項更指明具有預後之預測 (prediction of prognosis, 「預後」指根據病人當前狀況來推估未來經過治療後可能的結果<sup>474</sup>) 目的的醫療軟體，將被認定為具有醫療用途，而構成醫療器材，應受醫療器材法規<sup>475</sup>。也就是說，就預測疾病風險或罹病傾向 / 體質 (predisposition) 之 AI 軟體，雖在歐盟現行法下其並非給予診斷或治療方面的建議而不以醫療器材管理，但 Medical Devices Regulation 於 2020 年 5 月 26 日生效後，此類 AI 軟體將會被歸為醫療器材而受管制。

此外，Medical Devices Regulation 不僅在附件 8 第 6.3 條明確規範軟體分層等級制度，其附件 1 第 2 章第 17.1 條亦明定不論是附有軟體的醫療器材或是軟體本身，均應確保其再現性、可靠性以及與原目的一致的運作。

#### 4. 歐盟法院 (Court of Justice of the European Union) 實務見解

雖然 Medical Devices Regulation 擴大了醫療器材的定義，然並非所有的醫療 AI 均得視為醫療器材<sup>476</sup>，仍應以其功能及軟體使用目的加以判斷，甚至亦有學者主張提供診斷及治療方式的 AI 軟體只是輔助工具，不應將其認定為醫療器材<sup>477</sup>。因此，醫療 AI 與醫療器材的定義依然晦澀不明。

不過，歐盟法院 (Court of Justice of the European Union, 簡稱 CJEU)

<sup>473</sup> BSI 英國標準協會網頁，  
<https://www.bsigroup.com/LocalFiles/zh-tw/e-news/MD/2017-05/MDR-and-IVDR-published.pdf> (最後瀏覽日：10/18/2018)

<sup>474</sup> What is the prognosis of a genetic condition? (2018 October). NIH U.S. National Library of medicine. Available on <https://ghr.nlm.nih.gov/primer/consult/prognosis>

<sup>475</sup> Regulation (EU) 2017/745 of the European Parliament and of the Council of April 5, 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, Article 2 (1)

<sup>476</sup> Frank, Sharon. A new model for European Medical Device Regulation: a comparative analysis in the EU and the USA, *Europa Law Pub*, 2003, p.38

<sup>477</sup> Chung, Jason, Hey Watson, Can I Sue You for Malpractice? Examining the Liability of Artificial Intelligence in Medicine, *Forthcoming, Asia-Pacific Journal of Health Law, Policy and Ethics*, November 2017, retrived from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3076576](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3076576)

在 2017 年 12 月 7 日於《法國飛利浦案》(Syndicat national de l'industrie des technologies médicales (Snitem), Philips France v Premier ministre, Ministre des Affaires sociales et de la Santé)<sup>478</sup> 表示，依據歐盟第 93/42/EEC 號指令第 1 條第 1 項及第 2a 項對於醫療器材之定義以及歐盟第 2007/47/EC 號指令 (Directive 2007/47/EC of the European Parliament and of the Council of 5 September 2007, 簡稱「第 2007/47/EC 號指令」) 前言第 6 項<sup>479</sup> 載明「製造商意圖使該軟體用作醫療器材定義中之醫療用途時，該軟體即為醫療器材」，可知軟體得否作為醫療器材應以製造商意圖使其用作醫療用途為斷，非因該軟體於醫療場合使用而使其成為醫療器材<sup>480</sup>。該解釋亦與 Medical Devices Regulation 觀點相同<sup>481</sup>。

#### 5. 歐盟目前觀點與未來立法方向

承上所述，針對醫療 AI 而言，分析大數據以促進對特定疾病之認識，而非為特定患者決定治療方案，就不必然構成醫療用途而被視為醫療器材。反之，若系爭軟體功能不僅止於資料蒐集及溝通，更能增進臨床診斷及治療決策之正確性，則有可能被歸為醫療器材。

目前歐盟委員會正針對行動裝置保健應用程式及軟體草擬指引，以評估此等軟體所蒐集及處理之資料的信度及效度，並開放相關人士團體討論中<sup>482</sup>。此等指引草案旨在建立關於品質、安全性、效度及有效性之統一判斷要件，以建立評估保健軟體之方法學。歐美有論者觀察認為<sup>483</sup>，該草案旨在由業者自律遵守，惟對醫療產業仍有參考價值，或

---

<sup>478</sup> Judgment of the European Court (Fourth Chamber) of 7 December 2017 - Case no. C 329/16: Syndicat national de l'industrie des technologies médicales (Snitem) and Philips France v Premier ministre and Ministre des Affaires sociales et de la Santé.

<sup>479</sup> DIRECTIVE 2007/47/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 September 2007, Whereas (6)

<sup>480</sup> *Id.*

<sup>481</sup> Mariana Alpalhão Gonçalves, (Aug, 2018), *Liability arising from the use of Artificial Intelligence for the purposes of medical diagnosis and choice of treatment: who should be held liable in the event of damage to health?* (Tilburg Law School Tilburg University), p7, Retrieved from <http://arno.uvt.nl/show.cgi?fid=146408>

<sup>482</sup> European Commission (2017). *Report of the Working Group on mHealth assessment guidelines*. Retrieved from [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=45251](http://ec.europa.eu/newsroom/document.cfm?doc_id=45251)

<sup>483</sup> Lincoln Tsang, Daniel A. Kracov, Jacqueline Mulryne, Louise Strom, Nancy Perkins, Richard Dickinson, Victoria M. Wallace, and Bethan Jones, *The Impact of Artificial Intelligence on Medical Innovation in the European Union and United States* (2017/8)

能協助指引醫療 AI 製造商何謂發展醫療 AI 軟體之良好做法。

表 1-1：歐盟對於與醫療 AI 有關之醫療器材規範整理

法規政策名稱	提出或通過時間	核心內容
第 93/42/EEC 號指令 ( Council Directive 93/42/EEC of 14 June 1993 concerning medical devices )	1993 年 6 月 14 日， 將於 2020 年 5 月 26 日 被 Medical Devices Regulation 取代	第 1 條第 2 項 (a) 指出，醫療器材係指其製造商意圖供人體使用以達疾病或身體狀況之診斷、預防、監測、治療及緩解等目的 (即「醫療用途」) 之任何工具或器具 (包括軟體在內)。
第 2007/47/EC 號指令 ( Directive 2007/47/EC of the European Parliament and of the Council of 5 September 2007 )	2007 年 9 月 5 日， 修正第 93/42/EEC 號指令關於醫療器材之規定	前言第 6 條載明，製造商意圖使該軟體用作醫療器材定義中之醫療用途時，該軟體即為醫療器材。
MEDDEVs 指令 ( MEDICAL DEVICES: Guidance document - Qualification and Classification of stand alone software, MEDDEV 2.1/6 July 2016 )	2016 年 7 月，發布 醫療用途判斷要件之準則	以診斷疾病為目的而計算人體解剖結構上部位的影像處理軟體，通常會被歸類為醫療器材，因醫療照護專業人員利用這類影像處理軟體以協助進行臨床診斷及治療；管理患者資料的軟體，或僅供儲存、歸檔及移轉患者資料的資訊系統，或改變患者資料以達去連結或去識別化目的之程式，此等軟體均不會被視為醫療器材。
Medical Device Regulation, Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017	2017 年 5 月 25 日生效，並將於 2020 年 5 月 26 日施行，取代第 93/42/EEC 號指令及主動植入式醫療器材指令	針對軟體醫材制訂專門條款；第 2 條第 1 項已將具有預後之預測 (prediction of prognosis) 目的的醫療軟體列為醫療器材，而受 Medical Devices Regulation 規範；附件 8 第 6.3 條亦規範軟體分層等級制度。
歐盟法院《法國飛利浦案》 ( Syndicat national de l'industrie des technologies médicales (Snitem), Philips France v Premier ministre, Ministre des Affaires	2017 年 12 月 7 日	該判決指明，軟體得否作為醫療器材應以製造商意圖使其用作醫療用途為斷，非因該軟體於醫療場合使用而使其成為醫療器材。該判決不僅為第 93/42/EEC 號指令及第 2007/47/EC 號指令背書，同時亦與 Medical

(<https://www.arnoldporter.com/-/media/files/perspectives/publications/2017/08/the-impact-of-artificial-intelligence-on-medical-innovation.pdf>)

法規政策名稱	提出或通過時間	核心內容
sociales et de la Santé)		Devices Regulation 觀點相同。

## (二)美國

### 1. 聯邦食品、藥物及化粧品法 (Federal Food, Drug, and Cosmetic Act)

美國對於 AI 之規制方式及程度主要端視其使用目的。對 AI 研發者而言，最關鍵的問題之一，就是 AI 是否會被認定為醫療器材，而按聯邦食品、藥物及化粧品法 (Federal Food, Drug, and Cosmetic Act) 規範應受美國食品藥物管理局 (Food and Drug Administration, 簡稱 FDA) 管轄。FDA 認定醫療器材係指意圖使用於動物或人類，以診斷、治癒、減緩、治療或預防疾病或身體狀況之儀器、裝置、工具、機器、器具、插入管、體外試劑或其他相關物品，包括其組件、零件、附件等，且雖意圖影響動物或人類身體功能或結構，卻不經由化學反應或新陳代謝的方式來達成主要目的者<sup>484</sup>。此外，該意圖為客觀上意圖，而 FDA 並考量製造商明示或默示地推銷該產品為特定使用為判斷。

符合上述醫療器材定義者，且未按其他法律規定得排除適用者，將被分成三大類別以分級管制，每一類醫療器材依其安全性及功效性的需求不同而有不同之管制程度：Class I 一般管制、Class II 特殊管制及 Class III 上市前許可。其中，與 AI 研發者最相關且應受 FDA 規範之 4 種軟體醫療器材類型分別為行動醫療應用程式 (Mobile Medical Apps, 簡稱 MMAs)、醫療器材資料系統 (Medical Device Data Systems, 簡稱 MDDS)、軟體醫材 (Software as a Medical Device, 簡稱 SAMD)、臨床決策支持系統 (Clinical Decision Support System, 簡稱 CDSS)，而 FDA 並分別公布相關分類標準指引：

#### (1) 行動醫療應用程式 (MMAs)

針對 MMAs，有 3 種類型之應用程式：(1) 非屬醫療器材之應用程式；(2) 受執行自由裁量權規制的應用程式；(3) 受全面管

<sup>484</sup> Federal Food, Drug and Cosmetic Act 21 U.S.C. § 321(h).

制的醫材應用程式。依據 FDA《行動醫療應用程式》(Guidance for Industry and Food and Drug Administration Staff: Mobile Medical Applications (Feb. 2015))<sup>485</sup>，FDA 認為軟體應用程式屬於醫療器材且其功能有對病患危害的可能性都受其管制。這些行動應用程式包含特定病患分析、特定病患診斷或治療方式建議（例如：某應用程式使用特定病患相關參數以計算劑量或提供放射療法的劑量計畫）。

### (2) 醫療器材資料系統 (MDDS)

MDDS 是指在無庸控制或改變任何連接醫療器材的功能或參數下，提供電子傳輸、儲存、格式轉換或醫材資料顯示的系統。在 2011 年 2 月 15 日，FDA 將 MDDS 的管制程度由 Class III（高危險）降為 Class I（低危險）；FDA 亦於 2015 年 2 月 9 日依《醫療器材資料系統、醫療影像儲存器材及醫療影像通信器材》(Guidance for Industry and Food and Drug Administration Staff: Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices (Feb. 2015))<sup>486</sup>明確指出，未來 MDDS、醫療影像儲存器材及醫療影像通信器材將無庸以上市前審查管制。

### (3) 軟體醫材 (SAMd)

FDA 將 SAMd 定義為「執行一個或超過一個醫療目的但非屬醫療硬體之一部的軟體」。另按《軟體醫材：臨床評價》(Guidance for Industry and Food and Drug Administration Staff: Software as a Medical Device (SAMd): Clinical Evaluation (December, 2017))<sup>487</sup>，

---

<sup>485</sup> FDA, Guidance for Industry and Food and Drug Administration Staff: Mobile Medical Applications (Feb. 2015), available at <https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf>

<sup>486</sup> FDA, Guidance for Industry and Food and Drug Administration Staff: Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices (Feb. 2015), available on <https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm401996.pdf>.

<sup>487</sup> FDA Guidance for Industry and Food and Drug Administration Staff: Software as a Medical Device

軟體是否會被認定為醫療器材，則應以 FDA 對於臨床有效性、科學有效性、分析有效性及臨床實施之標準為認定依據。此外，SAMD 係以所分析的資料類型及資料轉換的方式作為決定管制程度的依據。

#### (4) 臨床決策支持系統 (CDSS)

CDSS 為利用病患資訊以協助提供者為診斷或治療決定的軟體，例如：IBM Watson；其亦以所分析的資料類型及資料轉換的方式作為決定管制程度的依據。

## 2. 21 世紀醫療法案 (21st Century Cures Act)

美國國會於 2016 年通過 21 世紀醫療法案 (21st Century Cures Act) 以促進生物醫學創新研發以及疾病治療，並要求美國衛生及公共服務部 (U.S. Department of Human and Health Service, 簡稱 HHS) 在 21 世紀醫療法案施行後每兩年須提出法律對於創新、醫療服務及病患安全的總結報告<sup>488</sup>，同時亦將部分軟體排除於醫療器材的定義範圍外，即非屬醫療器材。

更具體來說，該法案釐清了「醫療器材」的概念，若軟體的功能為醫療機構的行政支援（例如：開具帳單等）、一般健康維護、電子病歷系統（例如：電子健康紀錄）或是傳輸、儲存、轉換臨床實驗室或其他器材的資料結果（已經由 FDA 執行裁量權酌定），則該軟體非為器材。<sup>489</sup>其中，21 世紀醫療法案第 3060 條 (Section 3060 of the 21st Century Cures Act) 更將大部分屬於 CDSS 之軟體排除於醫療器材之定義外，包含顯示、分析或列印病患醫療資訊或其他醫療資訊（例如：同儕審查臨床研究與臨床執行守則）之軟體、支援或提供醫療專業人員關於預防、診斷或疾病治療建議之軟體，均被認定為非醫療器材。此外，

---

(SAMD): Clinical Evaluation (December 2017), available on <https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm524904.pdf>

<sup>488</sup> Parasidis, E. (2018) Clinical Decision Support: Elements of a Sensible Legal Framework. *Journal of Health Care Law & Policy*, 20(183), 1-37.

<sup>489</sup> 21st Century Cures Act, Pub. L. No. 114 – 255 § 360.

任何軟體提供醫師醫療建議，但醫師仍能獨立審查該建議且該軟體並非主要作為臨床診斷或治療方案之依據時，該軟體亦非醫療器材。也就是說，美國 21 世紀醫療法案係採與歐盟 Medical Devices Regulation 相反之立場。

不過，若 FDA 發現（1）該軟體有造成病患傷害的可能性及嚴重性，如軟體不正常運轉時；（2）該軟體某程度仍然支援醫療專業人員的臨床判斷；（3）醫療專業人員是否有合理的機會能夠審查該軟體提供的資訊或治療建議；（4）預期使用者及使用環境時，其仍能將該軟體認定為醫療器材而受其規制。<sup>490</sup>

此外，隨著科技的進步，醫療 AI 在進行臨床診斷與治療決定時的數據計算及推演的決策過程（黑盒子醫學）將超過人類可理解之範圍。由於黑盒子醫學本質上的複雜性與不透明性，致使醫師不在能夠獨立審查醫療 AI 所提供之建議，進而使這些醫療 AI 將不被 21 世紀醫療法案排除於醫療器材的定義外，亦即其屬醫療器材而受 FDA 規制。

### 3. 美國未來可能立法方向

雖然黑盒子醫學所具有獨立式結構、複雜演算的特質，將使其更偏向於行醫，而非醫療器材，而與 FDA 僅管制醫療器材而非行醫的立場有所衝突，且美國目前對此仍未有相關規範，但 FDA 已經表示未來考慮以上市前審查制度來管理 AI 電子醫療技術<sup>491</sup>。此外，FDA 亦將成立由電腦科學家與工程師組成的新數位健康小組，來協助 FDA 審查 AI 醫療軟體以及協調數位健康的新方案以迎向未來醫療 AI 的發展。<sup>492</sup>至於非屬醫療器材的醫療 AI，由於不受 FDA 管轄，因此目前尚未有相關的規定或建議。

---

<sup>490</sup> *Id.*

<sup>491</sup> Chung, Jason, Hey Watson, Can I Sue You for Malpractice? Examining the Liability of Artificial Intelligence in Medicine, *Forthcoming, Asia-Pacific Journal of Health Law, Policy and Ethics*, November 2017, retrived from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3076576](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3076576)

<sup>492</sup> Jeremy Hsu, "FDA Assembles Team to Oversee AI Revolution in Health," *IEEE Spectrum*, May 29, 2017, available on <https://spectrum.ieee.org/cdn.ampproject.org/c/spectrum.ieee.org/the-human-os/biomedical/devices/fda-assembles-team-to-oversee-ai-revolution-in-health.amp.html>; Megan Molteni, "Medicine is going Digital. The FDA is Racing to Catch Up," *Wired* (May 22, 2017), available on <https://www.wired.com/2017/05/medicine-going-digital-fda-racing-catch/>.



表 1-2：美國對於與醫療 AI 有關之醫療器材規範整理

法規政策名稱	提出或通過時間	核心內容
聯邦食品、藥物及化妝品法 (Federal Food, Drug, and Cosmetic Act)	1938 年 6 月 25 日生效	第 321 (h) 條指出，醫療器材係指意圖使用於動物或人類，以診斷、治療、減緩、治療或預防疾病或身體狀況之儀器、裝置、工具、機器、器具、插入管、體外試劑或其他相關物品，包括其組件、零件、附件等，且雖意圖影響動物或人類身體功能或結構，卻不經由化學反應或新陳代謝的方式來達成主要目的者。
《行動醫療應用程式》 (Guidance for Industry and Food and Drug Administration Staff: Mobile Medical Applications)	2015 年 2 月 9 日發布	FDA 指出，若 MMAs 屬於醫療器材且其功能有對病患危害的可能性，則其均受 FDA 管制，包含特定病患分析、特定病患診斷或治療方式建議 (例如：某應用程式使用特定病患相關參數以計算劑量或提供放射療法的劑量計畫) 等。
《醫療器材資料系統、醫療影像儲存器材及醫療影像通信器材》 (Guidance for Industry and Food and Drug Administration Staff: Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices)	2015 年 2 月 9 日發布	FDA 指出，未來 MDDS、醫療影像儲存器材及醫療影像通信器材將無庸以上市前審查管制
《軟體醫材：臨床評價》 (Guidance for Industry and Food and Drug Administration Staff: Software as a Medical Device (SAMD): Clinical Evaluation)	2017 年 12 月 8 日發布	軟體是否會被認定為醫療器材，則應以 FDA 對於臨床有效性、科學有效性、分析有效性及臨床實施之標準為認定依據；同時亦以所分析的資料類型及資料轉換的方式作為決定管制程度的依據。
21 世紀醫療法案 (21st Century Cures Act)	2016 年 12 月 13 日由美國總統簽署發布	釐清「器材」的概念，若軟體的功能為醫療機構的行政支援 (例如：開具帳單等)、一般健康維護、電子病歷系統 (例如：電子健康紀錄) 或是傳輸、儲存、轉換臨床實驗室或其他器材的資料結果，則該軟體非為器材；

法規政策名稱	提出或通過時間	核心內容
		部分 MMAs、MDDS、SAMD、CDSS 排除於醫療器材定義範圍外；第 3060 條更指出，部分 CDSS，包含顯示、分析或列印病患醫療資訊或其他醫療資訊（例如：同儕審查臨床研究與臨床執行守則）之軟體、支援或提供醫療專業人員關於預防、診斷或疾病治療建議之軟體，均被認定為非醫療器材。

## 二、醫療AI（或醫療大數據）與個人資料保護、網路安全議題

為促進人類健康，推動生醫研究及相關產業發展，需設立人類生物資料庫，大規模收集並分析健康個人資料及數據，以達成精準醫療的目標。<sup>493</sup>然而，目前各國不僅未針對生物基因資料庫的健康個人資料制訂專法，同時更將健康個人資料列為特種類型個人資料，規定不得蒐集、處理或利用。以下茲就英國、美國、澳大利亞等與醫療 AI 有關之健康個人資料保護法規進行觀察，並觀察、分析與健康個人資料有關之歐盟 GDPR 第 9 條規定：

### （一）英國

為了貫徹歐盟數據保護指令，英國於 1998 年通過 1998 年資料保護法(Data Protection Act 1998，簡稱 1998DPA)，以鞏固及取代先前如 1984 年資料保護法和 1987 年查閱個人檔案法等相關法案；同時為了因應 GDPR 施行並使相關資料保護法規現代化，英國於 2018 年 5 月 25 日開始施行 2018 年資料保護法(Data Protection Act 2018，簡稱 2018DPA)並廢除 1998DPA，透過該法案將 GDPR 原則細節化並完善相關資料保護法規。

依據已廢除 1998DPA 規定，可識別醫療紀錄屬於敏感資料，故其使用應受嚴格規範<sup>494</sup>，惟按 2002 年健康服務（與病患資料管理）法規（The Health Service (Control of Patient Information) Regulations 2002）及 2006 年國家健

<sup>493</sup>論壇「健康醫療資訊科技發展政策建言」委員會（2018），《健康醫療資訊科技發展政策建言》，頁 84，苗栗：財團法人國家衛生研究院。

<sup>494</sup> The Parliamentary Office of Science and Technology (2014), Big Data and Public Health, July 2017, available on <https://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-474>

康服務法（National Health Service Act 2006）第 251 條，若係為了癌症或感染性疾病或者是為了病患利益或公共利益且無從取得資料所有者同意時，則使用該資料時無庸取得個資當事人之同意。此外，英國資料保護委員會（Data Protection Commission，簡稱 DPC）亦主張病歷匿名化、使用病患個人資料進行健康研究前，可自由決定是否對病患進行知情同意（DPC's Guidance on research in the health sector, 2007）<sup>495</sup>。

然而，2018DPA 除了將歐盟第 2016/680 號指令納入英國內國法並補充制定 GDPR 原則下相關規定外，第 36 之 2 條更明確要求組織在使用個人資料作為健康研究之前，必須獲得個人明確表示同意（explicit consent）。若於 2018DPA 施行後才開始使用個人資料進行健康相關研究，資料使用者認為，進行健康研究的公共利益，遠超過於徵求資料所有者明確同意的公共利益時，則可提出聲明、列出不建議徵求資料所有者的明確同意之原因並備齊相關文件，向衛生部長任命之委員會（appointed by the Minister of Health）提出申請<sup>496</sup>。

2017 年英國資訊專員辦公室（Information Commissioner's Office, ICO）認定 Google 旗下人工智慧部門 DeepMind 與英國國家醫療服務體系（National Health Service, NHS）的資料共享協議違反 DPA 後<sup>497</sup>，英國政府衛生部（Department of Health and Social Care）於 2017 年 7 月公布報告指出，自 2018 年 3 月起，病患可以拒絕分享病歷資料，此權利適用於英國健康與社會照護系統，亦即賦予病患選擇退出的權利，為個人提供單一且簡單的機制，使其不受直接醫療（direct care）共享數據的規範。<sup>498</sup>英國衛生部亦於 2018 年 5 月修正施行新「國家資料退出指令」（National data opt-out

---

<sup>495</sup> 國立成功大學人類研究倫理治理架構網頁，<https://rec.chass.ncku.edu.tw/node/15858>（最後瀏覽日：10/18/2018）

<sup>496</sup> 國立成功大學人類研究倫理治理架構網頁，<https://rec.chass.ncku.edu.tw/node/15858>（最後瀏覽日：10/18/2018）

<sup>497</sup> 資策會科技法律研究所，「英國國家醫療服務體系（NHS）公布國家資料退出（Opt-out）操作政策指導文件」，資策會科技法律研究所網頁，<https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&i=152&d=8119&lv2=152>（最後瀏覽日：2018 年 12 月 17 日）

<sup>498</sup> 邱龍傑（2017），「英國允許民眾有權拒絕醫療資料共享」，DIGITIMES 物聯網網頁，[https://www.digitimes.com.tw/iot/article.asp?cat=158&cat1=20&cat2=15&id=0000508004\\_6d417lef1gshd43e1x8zn#](https://www.digitimes.com.tw/iot/article.asp?cat=158&cat1=20&cat2=15&id=0000508004_6d417lef1gshd43e1x8zn#)（最後瀏覽日：2018 年 12 月 17 日）

Direction 2018），英國健康與社會照護相關機構得參考國家醫療服務體系（NHS）2018年10月公布之國家資料退出操作政策指導文件（National Data Opt-out Operational Policy Guidance Document）規劃病患退出權行使機制。

## （二）美國

美國對於個人資料之蒐集及使用並非由單一專法規範，當個人資料涉及健康資訊，健康保險隱私及責任法（Health Insurance Portability and Accountability Act，簡稱HIPAA）會是主要參照規範。HIPAA規範的對象，就是所謂的「被涵蓋的機構」（covered entity），其中與軟體相關者，即以電子形式傳輸任何與該規則所涵蓋交易有關之健康資訊的健康照護提供者，而健康照護提供者，則是指有連結到電子醫療資訊的醫師和醫院，例如對於以電子形式開出帳單給Medicare和Medicaid索取保費者的健康照護提供者，方被此隱私規則所涵蓋。但只要該健康照護提供者有從事此種行為，則所有的受保護健康資訊，不論口頭或紙本的通訊或記錄，都適用HIPAA。

美國國會透過HIPAA之隱私規則（Privacy Rule）<sup>499</sup>建立聯邦標準以保障個人醫療紀錄及其他個人健康資訊。隱私規則要求應有適當的安全措施以保障個人健康資料，同時並同意得在部分未得病患授權之情形下，使用並揭露該個人健康資料。其中，該規則明確指出，被涵蓋機構得在未取得病患書面同意下，為促進治療、款項、健康照護而揭露被保護健康資訊（protected health information，簡稱PHI）<sup>500</sup>。而非屬被涵蓋機構者，例如Google、Apple、大數據彙集產業、或人工智慧技術醫材商、基因體科技公司等所蒐集之健康個人資料因無從適用HIPAA，而無法透過例外規定，在未取得病患書面同意情形下，使用病患個人健康資料。對於不適用HIPAA的資訊，或得依其他法規，例如基因資訊平等法（Genetic Information Nondiscrimination Act，簡稱GINA）及美國殘疾人法案（Americans with Disabilities Act，簡稱ADA）等予以保護及規制。

---

<sup>499</sup> 45 CFR 160, 162, and 164

<sup>500</sup> 45 CFR 164.512

除了聯邦法層級的各該規定外，美國許多州也在尋求規範個人資料的蒐集與使用。HIPPA 並未優先適用於各州州法或地方法，故在美國只要能夠取得病患或其他相關者受保護的健康資料，都有責任透過相關安全措施考量及降低資料外洩風險。

### (三) 澳大利亞聯邦 ( 澳大利亞 )

澳大利亞 1988 年隱私法案 ( The Privacy Act 1988, 簡稱 Privacy Act ) 規範個人資料的處理方式，並適用於私人組織及大部分澳大利亞與諾福克島的政府機構。其中，該法案下的澳大利亞隱私準則 ( Australian Privacy Principles, 簡稱 APPs ) 明確指出，健康資料屬於敏感資料，其所需保護程度應高於一般個人資料。<sup>501</sup> 因此，對於敏感健康資料所要求的使用、儲存及管理義務即更為繁複。一般來說，即使資料所有者已經同意資料使用者蒐集並使用敏感資料，惟若使用該敏感資料之目的已與原先使用目的無直接關連時，則資料使用者將會被禁止使用該敏感資料。健康照護提供者亦應採取適當措施確保海外服務提供者不僅已遵守 APPs，同時也採取嚴格的安全措施以防止資料外洩。APPs 亦要求任何健康照護提供者應採取週期性資料管理模式，明確記載持有資料取得的時間以及儲存的目的是，並於無需求時將該資料予以刪除。此外，不同的州法對於州立政府與醫院的隱私、保密性以及資料管理亦有其適用。

### (四) 歐盟 GDPR 第 9 條規定

歐盟個人資料保護過去係由第 95/46/EC 號數據保護指令 ( Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 簡稱數據保護指令 ) 規範，強制適用於所有歐盟會員國。而自 2018 年 5 月 25 日起，歐盟個人資料保護則改由 GDPR 規範，強制適用於所有歐盟會員國，亦適用於世界各地與歐洲為交易之所有企業。

依照 GDPR 第 9 條第 1 項規定，與健康相關之個人資料之處理，應予禁止；

---

<sup>501</sup> Hutchens, A., & Humble, E. (2017) Health care and the cloud – a prescription for complexity. *Privacy Law Bulletin*, 14(4) 67-72.

亦即將健康個人資料列為特殊類型，不得進行個人資料處理。GDPR 第 9 條第 2 項則規定例外情形得處理健康個人資料，除個資當事人已明確同意使用健康個人資料外，尚包括：(1)第 9 條第 2(c)項：個資當事人在身體上或法律上不能給予同意，而為保護個資當事人或他人之重大利益所必要之處理；(2)第 9 條第 2(h)項：該處理係出於健康照護或為判斷受僱者工作能力之勞動醫學，為了醫學上之診斷、健康或社會領域之照護或治療或為了健康或社會領域之體系或服務之管理，依據歐盟法、會員國之法令或與擔任健康相關職業之成員間簽訂之契約，並符合 GDPR 第 9 條第 3 項所定要件及保障，而認有必要者；(3)第 9 條第 2(i)項：處理係基於公共衛生領域之公共利益，例如為防止對於健康之跨境嚴重威脅或為確保醫療保健及醫療產品或醫療設備品質之高標準與安全性而有必要者，並依據歐盟法或會員國法律規定採取適當及具體安全措施保護個資當事人之權利和自由，尤其是職業秘密。

是以，除非蒐集健康個人資料係屬（1）為保護個資當事人或他人之重大利益所必要之處理(類似緊急避難之概念)；(2)為預防或職業醫學之目的、為評估員工之工作能力、醫療診斷、為提供健康或社會照護或治療或為健康管理或社會照護系統及服務而有必要之處理；或（3）基於公共衛生領域之公共利益，例如為防止對於健康之跨境嚴重威脅或為確保醫療保健及醫療產品或醫療設備品質之高標準與安全性而有必要者時，否則均需取得資料所有人明確之同意始得蒐集或使用特定個人資料。此外，任何儲存於醫療照護提供者資料庫之資料，均應於病患之要求下予以刪除。<sup>502</sup>

GDPR 前言第 54 條特別指出，未取得個資當事人同意之特殊類型個人資料處理，於公共衛生領域基於公共利益之理由可能是有必要的。該等處理應受適當具體措施之拘束以維護個資當事人之權利及自由。就此，「公共衛生」應以歐洲議會及歐盟理事會第 1338/2008 號歐盟規則所作定義而為解釋，亦即與健康有關之全部要素(即健康狀況)，包括疾病與殘疾、對於

---

<sup>502</sup> European Commission (2016) Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6, 2016 concerning measures for a high common level of security of network and information systems across the Union. European Union.

健康狀態產生影響之決定性因素、醫療保健之需求、醫療保健之資源分配、醫療保健之提供及普及性以及醫療保健之開支及財務規劃及致死率之起因。以公共利益為由所為涉及健康資料之該等處理，不得因其他目的而由諸如雇主或保險公司及銀行等第三人為處理。是以，GDPR 似認為人工智慧技術醫材商、基因體科技公司等因其他目的而處理健康資料，並非屬於為公共利益之公共衛生範圍內。

細究 GDPR 第 9 條第 2(h)項所指「為…醫療診斷、為提供健康或社會照護或治療或為健康管理或社會照護系統及服務而有必要之處理」，並未將主體限定為公務機關、學術研究機構或醫療院所，當人工智慧技術醫材商、基因體科技公司欲蒐集、使用健康個人資料，研發生物醫學檢測、建立基因體資料庫時，如能說明與確認該等行為係為提供健康或社會照護或治療或為健康管理或社會照護系統及服務而有必要，或可依據本條項，無庸取得個資當事人同意，即可處理相關健康資料；GDPR 第 9 條第 2(i)項所指「基於公共衛生領域之公共利益」，然醫療服務多為個人所提供，是否稱得上公共利益，亦非無疑，況人工智慧醫材商、基因體科技公司均為營利組織，似難謂為公共利益而蒐集、使用健康個人資料；GDPR 第 9 條第 2(c)項所指「於個資當事人處於身體上、法律上不能之狀況而情況之必要之處理」，惟精準醫療雖在生醫領域蓬勃發展，透過傳統常規醫療檢查，輔以生物醫學檢測及基因資料庫比對分析，將為未來發展趨勢，但究竟是否符合 GDPR 第 9 條第 2(c)項所指之必要情況(帶有緊急避難之色彩)，亦有解釋之空間；綜上，GDPR 第 9 條第 2 項雖有部分例外情形可能被解釋為人工智慧技術醫材商、基因體科技公司得於未取得個資當事人同意下，蒐集、使用健康個人資料，然其解釋上之不確定性，仍有可能造成人工智慧技術醫材商、基因體科技公司蒐集、使用健康個人資料之困難。前揭問題已促使部分監管者意識到似應提供新指南以因應在新科技潮流下如何適度放寬 GDPR，並兼顧相關隱私權保障及個人資料侵害。同時亦有歐洲學者<sup>503</sup>開始探討醫療 AI (或醫療大數據) 與 GDPR 的適用問題：

---

<sup>503</sup> Lincoln Tsang, Daniel A. Kracov, Jacqueline Mulryne, Louise Strom, Nancy Perkins, Richard Dickinson, Victoria M. Wallace, and Bethan Jones, *The Impact of Artificial Intelligence on Medical Innovation in the*

首先，GDPR 責任原則（Accountability Principle）<sup>504</sup> 要求機構應證明其符合 GDPR 規範下的其他原則，特別是當機構處理資料致其有可能影響個人權利和自由時，該機構處理資料的目的即應與其原取得目的相一致。同樣地，機構亦應採取適當的安全措施以防範資料處理過程中可能招致的風險。然而，對於運用醫療 AI 的機構來說，其將難以符合該項原則的要求，因為資料分析的最終目的在資料蒐集之初時並無從知悉，且該蒐集目的亦會隨著新資料的關連性而改變；再者，隨著醫療 AI 的大量使用，其所伴隨的風險亦會逐步提升，致使該機構難以採取適當的安全措施予以防範，致無法符合 GDPR 要求而蒐集、使用健康個人資料。

其次，機構通常仰賴透過取得個人同意以合法化個人資料處理的過程，而 GDPR 對此之要求更為嚴格。<sup>505</sup> 然而，AI 技術演算過程的複雜性與不透明性致使其難以取得資料所有者及其相關個資當事人的實質同意。因此，有學者建議，使用醫療 AI 的機構或許能透過更創新的方式取得資料所有者及其相關個資當事人的同意，例如透過軟體使用的不同階段分別取得同意，或者是研發軟體代理人機制，由軟體代理人代表資料所有者及其相關個資當事人表示同意。再者，除了取得同意以合法化個人資料處理過程外，使用醫療 AI 的機構亦能透過建立合法利益，與軟體分析可能造成個人隱私或利益的侵害為利益衡量，以合法化其個人資料處理。

此外，與 GDPR 有關議題尚有以自動處理為依據所為決定的解釋權（Right to explanation）。<sup>506</sup> 人類幾乎無法解釋機器學習所推演出的結果，特別是當該決定係以極大的資料庫為依據的時候。在這些情況下，相較於處理過程與資料類別的描述，提供一個能夠理解的解釋幾乎是不可能的。

為了處理 AI 軟體使用在資料保護方面所提出的新問題，歐洲議會議長於 2017 年 2 月指示歐盟委員會提出適於歐盟各國關於機器人與 AI 的規則。

---

European Union and United States (2017/8)  
(<https://www.arnoldporter.com/-/media/files/perspectives/publications/2017/08/the-impact-of-artificial-intelligence-on-medical-innovation.pdf>)

<sup>504</sup> Article 5(2) of the GDPR.

<sup>505</sup> The provision of informed consent is addressed by Articles 6(1) and 7 of the GDPR.

<sup>506</sup> Recital 71 and Article 13 of the GDPR.



此外，歐洲議會議長也建議歐盟委員會成立歐盟 AI 專門機構，以提供相關指南予有關當局。雖然這些要求對於歐盟委員會沒有拘束力，但歐盟委員會仍有必要就不採用該等建議提出正當理由。

表 2-1：歐盟、英國、美國、澳大利亞對於健康個人資料保護相關規範整理

國家	法規政策名稱	提出或通過時間	核心內容
歐盟	GDPR (General Data Protection Regulation)	2018 年 5 月 25 日施行	<p>GDPR 包含有關處理歐盟內部個資當事人的個人可識別資訊（包括：種族起源、宗教或哲學信仰、生物劑量識別或基因資料以及其他有關健康資料）的條款和要求，適用於與歐洲為交易的所有企業，無論位置如何。</p> <p>除非符合 GDPR 第 9 條所規定之例外，例如同意、為個資當事人之重大利益(緊急避難狀況)，為預防醫學、評估員工健康狀況，為公共利益之公共衛生等，不得蒐集或使用個資當事人之健康資料。此外，任何儲存於醫療照護提供者的資料，均應於病患之要求下予以刪除。</p>
英國	2018 年資料保護法 (Data Protection Act 2018)	2018 年 5 月 25 日施行	<p>將 GDPR 原則細節化並完善相關資料保護法規。</p> <p>第 36 之 2 條明確要求在使用個人資料作為健康研究之前，必須獲得個人明確表示同意。</p>
	2002 年健康服務 (與病患資料管理) 法規 (The Health Service (Control of Patient Information) Regulations 2002)	2002 年 6 月 1 日施行	為了癌症或感染性疾病且無從取得資料所有者同意時，則使用該資料時無庸取得個資當事人同意。
	2006 年國家健康服務法 (National Health Service Act 2006)	2007 年 3 月 1 日施行	第 251 條指出，為了病患利益或公共利益且無從取得資料所有者同意時，則使用該資料時無庸取得個資當事人同意。

國家	法規政策名稱	提出或通過時間	核心內容
美國	健康保險隱私及責任法（Health Insurance Portability and Accountability Act）之隱私規則（Privacy Rule）	1996年8月21日施行	應有適當的安全措施以保障個人健康資料，同時並同意得在部分未得病患授權之情形下，使用並揭露該個人健康資料。
澳大利亞	澳大利亞隱私準則（Australian Privacy Principles）	2014年3月12日生效；屬於1988年隱私法案下的規範	健康資料屬於敏感資料，其所需保護程度應高於一般個人資料。

此外，由於醫療 AI 大量透過網路方式使用健康個人資料，故為因應網路安全風險，歐盟、美國、澳大利亞均有相關網路安全規範及措施，以防範資料外洩可能造成資料所有人之損害，並提升網路及資訊安全：

#### 1. 歐盟

為避免透過 AI 軟體蒐集之個人資料遭未經授權之使用，歐盟最近通過網路安全指令<sup>507</sup>，建立對抗網路安全漏洞之措施，自 2018 年 5 月 25 日起即強制適用於所有歐盟會員國，課予會員國於國內法層次採用網路及資訊安全策略，及指定有權主管機關施行並強制執行該指令。其中也包括針對必需服務提供者（尤如公立及私立醫療照護業者），及數位服務提供者（例如雲端計算服務提供者），課以應採行各種資訊安全措施之義務，包括風險管理措施、定期內部審查、向有關當局通報重大事件等<sup>508</sup>。

#### 2. 美國

美國 FDA 已經表示未授權的使用者確實有可能透過無線網路遠程存取醫療器材，例如：輸液幫浦系統（infusion pump system）、心房去顫器（atrial defibrillator）和植入型藥物幫浦（implantable drug pumps）

<sup>507</sup> Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6, 2016 concerning measures for a high common level of security of network and information systems across the Union.

<sup>508</sup> Tsang L, Kracov D, Mulryne and others, The Impact of Artificial Intelligence on Medical Innovation in the European Union and United States, *Intellectual Property & Technology Law Journal*, August 2017.

等<sup>509</sup>。為了因應網路安全風險，FDA 已針對醫材製造商公布上市前與上市後的網路安全措施。在上市前階段，製造商應指明、處理和限制潛在的網路安全性漏洞的風險<sup>510</sup>；在上市後階段，製造商亦應採取「指明、保護、監測、回應和恢復」的措施來修正網路安全性漏洞，移除任何可能危害健康的風險並將相關網路安全性風險降至最低<sup>511</sup>。FDA 近年亦公布指南，強調製造商應監測、辨識並處理網路安全性漏洞及相關濫用行為，做為對其所生產之醫療器材應進行之上市後管理的一部分<sup>512</sup>。指南中並建立一個風險評估的架構，以提供製造商評估裝置因網路安全漏洞而變更時，是否應向 FDA 通報。基本上，定期的網路安全更新或修補不需要特別通報，但若是修補了可能危及病人健康、甚至造成死亡的嚴重漏洞，則會被要求通報<sup>513</sup>。

### 3. 澳大利亞

對於網路安全議題，澳大利亞網路安全措施—通報資料外洩計畫（Notifiable Data Breaches scheme，簡稱 NDB）已於 2018 年 2 月 22 日生效。該計畫要求當資料外洩可能造成資料所有人嚴重損害時，該實體即有資料外洩通報義務<sup>514</sup>。資料外洩的情形包括：顧客個人資料遺失或遭竊、具有個人資料的資料庫遭非法入侵、個人資料遭錯誤地提供等。

表 2-2：歐盟、美國、澳大利亞之與健康個人資料有關之網路安全措施

國家	法規政策名稱	提出或通過時間	核心內容
----	--------	---------	------

<sup>509</sup> Webb, T., & Dayal S.(2018) Medical devices and the IoT: regulatory perspectives on cybersecurity risks in health care. *Internet Law Bulletin*, 20(8) 138.

<sup>510</sup> *Id.*

<sup>511</sup> Tsang L, Kracov D, Mulryne and others, The Impact of Artificial Intelligence on Medical Innovation in the European Union and United States, *Intellectual Property & Technology Law Journal*, August 2017.

<sup>512</sup> FDA (2016). *Guidance for Industry and Food and Drug Administration Staff: Postmarket Management of Cybersecurity in Medical Devices*. Retrieved from <https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf>

<sup>513</sup> 行政院國家資通安全會報服務中心網頁，《資安新聞：美國 FDA 發布醫療裝置網路安全管理指南正式版》，<https://www.nccst.nat.gov.tw/NewsRSSDetail?lang=zh&RSSType=news&seq=15865>（最後瀏覽日：2018/10/23）

<sup>514</sup> Office of the Australian Information Commissioner. Notifiable Data Breaches scheme. Australian Government. Retrieved on 9 October 2018 at <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme>.

國家	法規政策名稱	提出或通過時間	核心內容
歐盟	網路安全指令 ( Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 )	2018年5月25日施行	課予歐盟會員國於國內法層次採用網路及資訊安全策略。其中，必需服務提供者（尤如公立及私立醫療照護業者），及數位服務提供者（例如雲端計算服務提供者），均應採行各種資訊安全措施，包括風險管理措施、定期內部審查、向有關當局通報重大事件等。
美國	《醫療裝置上市後網路安全管理指南》 ( Guidance for Industry and Food and Drug Administration Staff: Postmarket Management of Cybersecurity in Medical Devices )	2016年12月28日	FDA 發布指南，強調製造商應監測、辨識並處理網路安全性漏洞及相關濫用行為，做為對其所生產之醫療器材應進行之上市後管理的一部分。指南中並建立一個風險評估的架構，以提供製造商評估裝置因網路安全漏洞而變更時，是否應向 FDA 通報。
澳大利亞	通報資料外洩計畫 ( Notifiable Data Breaches scheme )	2018年2月22日生效	該計畫要求當資料外洩可能造成資料所有人嚴重損害時，該實體即有資料外洩通報義務。

### 三、醫療AI與商品責任規範

#### (一) 歐盟

##### 1. 歐盟現狀

歐盟對於電子醫療（eHealth）以及機器人技術（Robotics）的民事責任已有相關討論。歐盟委員會於2004年提出電子醫療創新技術並認知到有必要制訂電子醫療與其責任相關規範後<sup>515</sup>，其於2015年5月推出數位單一市場戰略（Digital Single Market Strategy）<sup>516</sup>。歐盟委員會並

<sup>515</sup> Commission of the European Communities Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions *e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area* {SEC(2004)539} Brussels, 30.4.2004 COM (2004) 356 final, available on <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52004DC0356&from=EN>

<sup>516</sup> European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - *A Digital Single Market Strategy for Europe* - COM(2015) 192 final available on

表示「電子醫療產品及服務係由目前的產品責任法規所規範。不過，資訊技術開發者應致力於創造更安全的工作環境；而在人類、商品及服務頻繁交流下，電子醫療服務相關法規的需求與日俱增」<sup>517</sup>。近來，歐洲議會在 2017 年 2 月 16 日亦採用大會決議第 2015/2103(INL)號—機器人技術的民法規則（Parliament Resolution no. 2015/2103(INL) under the heading “Civil Law Rules on Robotics”，簡稱 PR 第 2015/2103 號），作為對目前相關法律問題的回應<sup>518</sup>。PR 第 2015/2103 號前言 AB 指出針對機器人技術制訂新的民事責任規則是有必要的。歐美有論者觀察認為<sup>519</sup>，歐盟目前並無針對醫療 AI 及其所衍生之損害與責任歸屬進行特別立法。

## 2. 目前與醫療 AI 之商品責任規範

歐盟目前有涉及醫療 AI 商品責任規範主要為：Medical Devices Regulation 以及 1985 年 7 月 25 日歐盟高峰會議第 85/374/EEC 號指令（the Council Directive 85/374/EEC of 25 July 1985，簡稱「第 85/374/EEC 號指令」）。

第 2017/745 號法規提供與商品責任有關之安全性規則，惟其並非商品責任的法律依據<sup>520</sup>，而與醫療 AI 商品責任最有關係者應為第 85/374/EEC 號指令<sup>521</sup>。依據第 85/374/EEC 號指令，電子醫療技術的製造者、進口商或供應商應就商品瑕疵所造成之損害或傷害負損害賠償責任<sup>522</sup>。惟該指令僅就製造商（包括製造者、進口商、供應商）課

---

<https://ec.europa.eu/digital-single-market/en/news/digital-single-market-strategy-europe-com2015-192-final>

<sup>517</sup> *Id.* p 19.

<sup>518</sup> Mariana Alpalhão Gonçalves, (Aug, 2018), *Liability arising from the use of Artificial Intelligence for the purposes of medical diagnosis and choice of treatment: who should be held liable in the event of damage to health?* (Tilburg Law School Tilburg University), p7, Retrived from <http://arno.uvt.nl/show.cgi?fid=146408>

<sup>519</sup> Mariana Alpalhão Gonçalves, (Aug, 2018), *Liability arising from the use of Artificial Intelligence for the purposes of medical diagnosis and choice of treatment: who should be held liable in the event of damage to health?* (Tilburg Law School Tilburg University), p8, Retrived from <http://arno.uvt.nl/show.cgi?fid=146408>

<sup>520</sup> Mariana Alpalhão Gonçalves, (Aug, 2018), *Liability arising from the use of Artificial Intelligence for the purposes of medical diagnosis and choice of treatment: who should be held liable in the event of damage to health?* (Tilburg Law School Tilburg University), p30, Retrived from <http://arno.uvt.nl/show.cgi?fid=146408>

<sup>521</sup> *Id.*

<sup>522</sup> Petra WILSON, Isabelle Andoulsi, Tony SOLOMONIDES, Vincent BRETON, Jean Herveg, Data protection and confidentiality in healthgrids: the SHARE project : a framework for developing a roadmap for the adoption of Grid technology in healthcare, *Medizinische Informatik, Biometrie und Epidemiologie*, 2006, p. 16-24

予嚴格的商品瑕疵責任，並未考量使用醫療 AI 進行診斷與治療的複雜性<sup>523</sup>。

因此，已有許多歐洲學者對於一般商品瑕疵責任能否適用於 AI 甚至是醫療 AI 打上一個大問號<sup>524</sup>。況且，醫療 AI 本係由軟體及硬體所組成，姑且不論醫療 AI「黑盒子」運算的不透明性致使其是否為純粹商品未有定論，軟體本身究竟能否適用於嚴格的商品瑕疵責任爭論已久<sup>525</sup>。此外，亦有學者提出不同看法，表示不應將醫療 AI 當作商品，而應將其作為一種醫療服務<sup>526</sup>。所以，對於醫療 AI 的定位及其相關責任規範，歐盟各國目前仍然眾說紛紜，未有定論。

## (二) 英國

英國目前並無任何特定處理醫療 AI 商品瑕疵責任或其所衍生的損害及其責任歸屬之法規，惟似乎已經意識到有必要重新制訂與醫療 AI 有關的責任法規，因此業已召集學界人士、法律專業人員、技術開發者與製造者以及醫療機構等，針對該議題進行分析討論<sup>527</sup>。在最新版的報告中，已經提及四大應探討領域：(1) 法律責任—關於 AI 技術的法律責任應如何建立；(2) 因果關係與責任歸屬—當 AI 不正常運行時，應如何決定承擔責任者；(3) 使用醫療 AI 是否為履行既存的法律義務；(4) 法律地位—醫療 AI 的法律地位<sup>528</sup>。

## (三) 美國

---

<sup>523</sup> Mariana Alpalhão Gonçalves, (Aug, 2018), *Liability arising from the use of Artificial Intelligence for the purposes of medical diagnosis and choice of treatment: who should be held liable in the event of damage to health?* (Tilburg Law School Tilburg University), p32, Retrieved from <http://arno.uvt.nl/show.cgi?fid=146408>

<sup>524</sup> *Id.*

<sup>525</sup> In the words of Sara E. Dyson “*Whether software can be the subject of a strict liability claim is contentious*” - Cf. Dyson, Sara E. *op. cit.*

<sup>526</sup> Petra WILSON, Isabelle Andoulsi, Tony SOLOMONIDES, Vincent BRETON, Jean Herveg, Data protection and confidentiality in healthgrids: the SHARE project : a framework for developing a roadmap for the adoption of Grid technology in healthcare, *Medizinische Informatik, Biometrie und Epidemiologie*, 2006, p. 16-24

<sup>527</sup> Mariana Alpalhão Gonçalves, (Aug, 2018), *Liability arising from the use of Artificial Intelligence for the purposes of medical diagnosis and choice of treatment: who should be held liable in the event of damage to health?* (Tilburg Law School Tilburg University), p7, Retrieved from <http://arno.uvt.nl/show.cgi?fid=146408>

<sup>528</sup> UK's Parliament, *Select Committee on artificial intelligence collated written evidence volume - House of Lords (UK)* - Statement of Cooley (UK) LLP (written evidence AIC0217) available on <https://www.parliament.uk/documents/lords-committees/Artificial-Intelligence/AI-Written-Evidence-Volume.pdf>

美國雖然目前並無與醫療 AI 有關的商品瑕疵責任案例或指南，且各州亦未將醫療侵權行為列為特殊侵權行為之一，惟似可考量 FDA 對於軟體品質管理的指南。且製作及行銷醫材的公司應有全面性的系統確保產品的安全性與品質；醫材類型的產品應符合設計管理規則<sup>529</sup>。該規則已明確指出，應由文件證明設計輸入的要求，且特定要求應被核實，亦即據此確認該軟體與其核備文件的一致性、完整性與正確性<sup>530</sup>。

若醫療 AI 軟體本身有缺陷或是品質不佳時，該軟體研發者即應負有責任。<sup>531</sup>惟美國法院傾向拒絕要求軟體研發者或是軟體出賣人承擔商品瑕疵責任，甚至當該軟體為醫療軟體時，由於通常均係由健康照護提供者為最終決定，並非是醫療軟體下決定，因此法院於大多數情形下皆認為軟體研發者或是軟體出賣人無庸承擔產品瑕疵責任。<sup>532</sup>此外，對於軟體研發者或是軟體出賣人的注意義務程度，亦僅要求至「合理」(reasonable)，而非「完美」(perfect)，畢竟即使以最佳實行原則研發軟體產品，其仍會有編碼上的瑕疵，難以避免。<sup>533</sup>

當發生與醫療 AI 有關的醫療疏失時，究竟醫師或是醫院應否承擔責任，並無定論。不過，已有學者提出或許能以醫師使用、誤用或拒絕使用醫療 AI 的治療方式是否「合理」(reasonable)作為判斷醫師是否構成與醫療 AI 有關的侵權行為的依據；若醫療 AI 屬 CDSS 類型時，由於醫師仍必須獨立進行醫療判斷，而非完全仰賴醫療 AI，因此「合理性」(reasonableness)的標準仍應以普通法下的侵權行為要件，包括可預見性、相當因果關係、最小侵害性以及公共利益為依據進行判斷。<sup>534</sup>至於醫院或是健康照護提供機構，由於其負有普通法上的不可轉移(侵權)責任，故該等機構負有檢

---

<sup>529</sup> See 21 C.F.R. Part 820.

<sup>530</sup> FDA, Guidance for Industry and Food and Drug Administration Staff: General Principles of Software Validation (Jan. 2002), available at <https://www.fda.gov/RegulatoryInformation/Guidances/ucm085281.htm>.

<sup>531</sup> ARTIFICIAL INTELLIGENCE IN HEALTH CARE, 14 No. 1 ABA SciTech Law. 10

<sup>532</sup> Miller, R., & Miller, S. (2007) Legal and Regulatory Issues Related to the Use of Clinical Software in Health Care Delivery. *Clinical decision support: the road ahead*. Retrieved from <https://doi.org/10.1016/B978-0-12-369377-8.X5000-4>.

<sup>533</sup> Scott, M.D. (2008) Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?, *Medical Law Review* (67) 425-462.

<sup>534</sup> Parasidis, E. (2018) Clinical Decision Support: Elements of a Sensible Legal Framework. *Journal of Health Care Law & Policy*, 20(183), 1-37.



驗相關醫療 AI 軟體、對於醫療 AI 軟體進行合理調查、執行一般監測或維修以及提供員工教育訓練等義務。<sup>535</sup>

雖然醫療 AI 無可避免地造成少部分的病患遭受健康上的傷害，但是其卻能夠提升大部分病患的醫療品質並增加醫護輸出，因此立法者應致力於創造友善新科技的發展環境。對此，美國學者在研究與醫療 AI 有關的商品瑕疵與侵權領域時，已經提出相關改革法案<sup>536</sup>供立法者參考，透過建立適當的救濟方式來處理醫療 AI 本質上複雜的責任議題，減輕不可避免的風險並提供較大的利益。相關法案或可參考由國家兒童疫苗傷害法（National Childhood Vaccine Injury Act，簡稱 NCVIA）建立的國家疫苗傷害補償方案（The National Vaccine Injury Compensation Program，簡稱 VICP），提供聯邦無過失系統，以補償疫苗相關的傷害或死亡，減少由疫苗傷害索賠引起的疫苗製造者的損害賠償責任。

### 第三項 針對我國法規調適之初步意見

#### 一、醫療AI與我國醫療器材規範

按現行藥事法第 13 條第 1 項規定，任何用於診斷、治療、減輕、直接預防人類疾病、調節生育，或足以影響人類身體結構及機能，且非以藥理、免疫或代謝方法作用於人體，以達成其主要功能之儀器、器械、用具、物質、軟體、體外試劑及其相關物品者，即為醫療器材；藥事法第 13 條第 2 項授權衛生福利部制定醫療器材管理辦法，醫療器材得依據風險程度或功能、用途、使用方法及工作原理以提供分類分級品項，並按其分類管理；藥事法第 40 條第 3 項授權衛生福利部制定醫療器材查驗登記審查準則，提供關於醫療器材之查驗登記與許可證之變更、移轉、展延登記及污損換發、遺失補發之準則。因此，若醫療 AI 按藥事法第 13 條第 1 項規定，屬於醫療器材時，則應先由衛生福利部審查，取得製造許可、販賣執照許可及查驗登記通過後，始得上市（上市前審查制度），以避免有不當或有瑕疵之醫療器材損害使用者生命、身體或健康之風

---

<sup>535</sup> *Id.*

<sup>536</sup> Swanson, A., & Khan, F. The legal challenge of incorporating artificial intelligence into medical practice. *Journal of Health & Life Science Law*, 6(90), 20.



險。若對於醫療器材分類分級品項或管理模式有疑義時，則得依醫療器材管理辦法第 6 條規定，向衛生福利部食品藥物管理署（以下簡稱「食藥署」）提出醫療器材屬性管理查詢之申請，由主管機關確認該產品之屬性，以避免量產上市後才招致違法爭議。

為因應軟體類產品在醫療照護行為上幾乎無所不在，且分類分級制度是醫療器材管理的根基，食藥署參考美國、歐盟、日本各國管理規範及國際醫療器材法規管理論壇(International Medical Device Regulators Forum, IMDRF)<sup>537</sup>，於 2015 年 4 月 14 日制定醫用軟體分類分級參考指引，以提供產業界開發產品、申請查驗登記之參考。此外，食藥署亦於 2017 年 12 月 15 日制定醫療器材軟體確效指引，以提供醫療器材廠商辦理產品查驗登記，檢附醫療器材軟體確效資料之建議。

根據醫用軟體分類分級參考指引，「醫用軟體」泛指蒐集、儲存、分析、顯示、轉換人體健康狀態、生理參數、醫療相關紀錄等處理軟體，而使用場所則涵蓋醫療院所、個人居家使用及遠距醫療照護。惟並非所有醫用軟體均被列為醫療器材，判定醫用軟體是否列屬醫療器材管理，係依產品的功能、用途、使用方法及工作原理等綜合評估，並參考藥事法第 13 條醫療器材定義、醫療器材管理辦法附件一所列品項、是否宣稱具診斷、治療功能或協助診斷、治療、對疾病治療的重要性、對疾病診斷的貢獻度、參考價值、對人類生命健康可能產生的危害程度進行判定。同時醫用軟體分類分級參考指引亦列舉部分產品，提供醫療器材廠商辦理產品查驗時參考使用。惟醫用軟體分類分級參考指引並未能全面涵蓋、解釋所有醫用軟體類產品，故僅能提供初步判斷之建議，且若無法確認產品之分類分級，仍需依醫療器材管理辦法第 6 條規定，以個案送件申請分類分級判定為準。

表 3-1：醫用軟體分類分級參考指引—產品舉例表

產品	類別說明摘錄
醫院行政管理軟體	主要係依醫療人員的專業知識判斷，因此除非得取代醫療人員

<sup>537</sup> 衛生福利部食品藥物管理署醫用軟體分類分級參考指引

產品	類別說明摘錄
	的診斷治療決定，否則非屬醫療器材。
用藥紀錄、計算用藥劑量軟體	並非直接提供患者用藥指導，故非屬醫療器材。
一般健康管理軟體	這些軟體主要基於個人健康管理之目的，提供健康資訊，沒有涉及疾病之診斷、治療，故不以醫療器材列管。惟若該軟體用以處理醫療器材產生的資料，如電子血壓計、血糖計等醫療器材附屬專用之訊號處理或訊號傳輸軟體，則應屬醫療器材
醫學影像處理軟體	與診斷用途有關，故屬醫療器材。
電腦輔助偵測/診斷軟體	與診斷、治療有關，故屬醫療器材，而遭列管。
手術治療計畫軟體	與診斷、治療有關，故屬醫療器材。
病患生理參數監控軟體	屬醫療器材。
遠距醫療、照護軟體	若僅單純用於傳遞數據，則不以醫療器材列管，而倘軟體設計可用於解釋病患資料，或可分析由醫療器材產生的資料協助病患的診斷或治療，此類軟體屬醫療器材。
多項臨床生化指標分析軟體	具有輔助診斷功能，屬醫療器材。

同時，為周延醫療器材管理規定，衛生福利部收集全球醫療器材法規協和會、歐盟、澳洲、日本及美國等國之安全監視管理規範，並參考國內藥品優良規範，彙總嚴重藥物不良通報辦法、藥物安全監視管理辦法、醫療器材不良事件通報表等，於2016年10月間訂立醫療器材優良安全監視規範（GVP），制訂醫療器材不良反應通報及通報要求、風險管理、教育訓練、醫療器材安全監視查核等制度。由於醫療器材上市前之臨床試驗所收集的醫療器材安全性資料，有其侷限性，而許多醫療器材管理先進國家，對特定「新醫療器材」核准上市初期，訂有「醫療器材安全監視期間」與對矯正措施進行定期追蹤，因此，衛生福利部要求許可證持有商，應積極收集上市後之所有安全性資料，匯集編成「醫療器材定期安全性報告」，並依時限檢具「醫療器材定期安全性報告」，通報至中央衛生主管機關或其委託機構。安全監視期間中之醫療器材發生所有醫療器

材不良反應，均需將之條列於「醫療器材定期安全性報告」內，一併作通報；中央衛生主管機關得視情況提出限時通報之要求<sup>538</sup>。

本報告觀察歐盟、美國以及我國的相關醫療器材規範，並蒐集學者、專家意見後認為，雖然藥事法第 13 條係於 1970 年所制定，惟我國業於 2015 年參考歐盟相關醫療器材指令、美國 FDA 之指令與指南等，制定醫用軟體分類分級參考指引，而該指引亦與美國 FDA 對於軟體醫療器材之指南類同。且為能妥適管理「新醫療器材」，衛生福利部制訂醫療器材優良安全監視規範（GVP），並訂有「醫療器材安全監視期間」，以定期追蹤上市後新醫療器材，並管理其安全性。由於醫用軟體分類分級參考指引係於 2015 年所制訂，故我國日後仍得參考歐盟 MEDDEVs 指令、Medical Devices Regulation、美國 21 世紀醫療法案等，並持續觀察國際發展趨勢，以因應醫療 AI 技術發展與軟體醫材運用。

機器學習（Machine Learning）的「訓練」（training）與「測試」（testing）階段，不同的資料輸入，將影響其自動分析所得的規律，進而導致不同的醫療決策。如果人工智慧被惡意人士誤導或利用，對人類可能產生無可逆轉的災害。例如，近年來有許多研究發現，機器學習的判斷有可能被誤導。只要在輸入的地方加上一些擾動，就會讓電腦學到錯誤的模型，輸出完全相反的答案，造成安全上的漏洞<sup>539</sup>。因此，在現行法制下，主管機關或許能參考相關領域學者、專家建議與目前學界、實務界一致見解，於醫療器材業者申請醫療器材查驗登記時，要求業者列出演算法、數據、演算目的等，以盡可能確保責任歸屬，建立明確問責制度，維繫大眾對於醫療 AI 的信任<sup>540</sup>。對於醫療 AI 潛在的「黑盒子」疑慮，則由計算科學家及政策專家持續研究、討論，盡可能給予「程序規律性（procedural regularity）」或是讓既定演算法有一致性的應用，且追蹤特定演算法的使用及其效果<sup>541</sup>，並透過醫療器材管理辦法第 6 條規定，於個案送

---

<sup>538</sup> 衛生福利部《醫療器材優良安全監視規範（GVP）》

<sup>539</sup> TN Choice（2017），「台大資工系教授林守德：論第三波人工智慧技術革命」，科技新報網頁，<https://technews.tw/2017/08/07/the-3rd-revolution-wave-of-ai-technology/>（最後瀏覽日：2018 年 12 月 17 日）

<sup>540</sup> 張小玫、杜君妮（2017），「人工智慧：未來決策制定的機遇與影響」，國家實驗研究院科技政策研究與資訊中心科技產業資訊室網頁，<http://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=13238>，（最後瀏覽日：2018 年 12 月 17 日）

<sup>541</sup> 張小玫、杜君妮（2017），「人工智慧：未來決策制定的機遇與影響」，國家實驗研究院科技政策研究與資訊中心科技產業資訊室網頁，<http://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=13238>，（最後瀏覽日：2018 年 12 月 17 日）

件申請分類分級判定時，給予醫療器材業者一致性標準及明確的法令遵循，兼顧患者安全。

## 二、醫療AI（或醫療大數據）與我國健康個人資料保護規範

按現行個資法第6條第1項規定，有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：一、法律明文規定。二、公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。三、當事人自行公開或其他已合法公開之個人資料。四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。五、為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。六、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限；衛生福利部衛生福利資料應用管理要點第7點第3款規定，衛生福利相關產業基於研究發展需求，得申請使用取得當事人書面同意之特定衛生福利資料；亦即，有關病歷、醫療、基因、健康檢查等健康個人資料，原則上不得蒐集、處理或利用，惟若取得當事人書面同意，例外得使用該等健康個人資料。

一般而言，健康個人資料的蒐集、處理或利用，得區分為兩大途徑：透過健康應用程式（App）蒐集健康個人資料（或個人數據）或是為生醫研發而蒐集、處理或利用病歷、醫療、基因、健康檢查等健康個人資料；惟即便蒐集、處理或利用的途徑不同，如被認定符合個資法特種個資之定義，或雖非特種個資但屬於能識別自然人之資料時，均有個人資料保護法相關規範的適用。目前，依照個資法第6條、第15條、第19條相關規定，公務機關、學術研究機構得基於醫療、衛生或犯罪預防之目的，或為統計或學術研究，在資料經過一定之「去識別化」處理之條件下，得以在未取得個資當事人同意之情形下，蒐集、處理或使用個人資料。惟醫療資料涉及人體，極為複雜，以病歷而言，其欄位包括基本資料、主訴內容、過去病史或過敏史等得識別該個人之資料，由於該等得識別該個人之資料為訓練醫療AI或醫療大數據使用上所必須，若將其去識別

化，可能影響訓練醫療 AI 或醫療大數據分析之準確度，因此如何將醫療資料適當去識別化，顯為一大難題。關於我國全民健康保險資料之分享與運用，是否違反個資法，個人是否有退出權等法律爭議，雖然最高行政法院 106 年度判字第 54 號判決、臺北高等行政法院 103 年度訴更一字第 120 號判決均認為無違個資法，並駁回個資當事人之訴，惟個資當事人已聲請釋憲，現由司法院大法官審理中，在司法作成解釋之前，尚難有所定論。

至於人工智慧技術醫材商、基因體科技公司等因屬私人營利組織，既非為公務機關，亦非為學術研究機構，且多數係為營利目的使用相關個人資料，是以，均僅能透過取得個資當事人書面同意後，始得蒐集、處理或利用符合個資法定義之病歷、醫療、健康檢查等個人資料。

本報告觀察歐盟 GDPR 第 9 條、英國 DPA、美國 HIPPA 及其隱私規則、澳大利亞隱私準則以及我國個人資料保護規範，並蒐集學者、專家意見後認為，目前各國均係將健康相關個人資料列為特種類型個人資料，除有例外情形或經個資當事人書面同意或明確同意外，禁止蒐集、處理或利用健康個人資料。

實則，個資法旨在保護個資當事人權利之同時，兼顧資料之合理使用，此可由個資法第 1 條觀之。因此，對於如何適度放寬人工智慧醫材商、基因體科技公司等營利機構蒐集、處理或利用健康個人資料，立法上可參考 GDPR 第 9 條規定，不限定例外情形得蒐集、處理或利用健康個人資料的主體，而僅由蒐集、處理或利用之目的予以規範，或是將與健康照護相關者列為例外得蒐集、處理或利用健康個人資料之情形。對於「公益目的」的解釋，得參考英國 DPA，取得資料者（包括取得資料訓練 AI 者）同意被追蹤時，確實檢驗「公益目的」時，始得蒐集、處理或利用健康個人資料，進而放寬個資法第 6 條第 1 項但書第 4 款的主體，不論是否為營利機構，均得適用該條規定。又關於個資法所指「書面同意」，得參考 GDPR，放寬其形式要件與實質要件，只要在實體內容上能夠取得個資當事人同意，即符合個資法規定，而無須拘泥於書面。凡此未來國際發展趨勢仍應持續觀察，以作為我國個資法未來修法的借鏡。

此外，醫療 AI（或醫療大數據）大量透過網路方式處理健康個人資料，與網路安全實密不可分，確有加速建構國家資通安全環境之必要。對此，我國已於

2018年6月6日由總統公布實施資通安全管理法，並於該法第三章針對關鍵基礎設施提供者要求其符合所屬資通安全責任等級之要求。同時，行政院資通安全處亦於2018年11月21日訂定發布「資通安全管理法施行細則」、「資通安全責任等級分級辦法」、「資通安全事件通報及應變辦法」、「特定非公務機關資通安全維護計畫實施情形稽核辦法」、「資通安全情資分享辦法」、「公務機關所屬人員資通安全事項獎懲辦法」等，並將自2019年1月1日開始施行，為我國資通安全提供詳細的遵循規範。前揭法規均已參酌目前各國相關網路安全規範及措施，實符合國際潮流。惟因科技日新月異，仍有必要持續觀察國際發展趨勢。

### 三、醫療AI與我國商品責任規範

按我國現行消費者保護法第7條第1項規定，從事設計、生產、製造商品或提供服務之企業經營者，於提供商品流通進入市場，或提供服務時，應確保該商品或服務，符合當時科技或專業水準可合理期待之安全性；消費者保護法第7條之1第2項，商品或服務不得僅因其後有較佳之商品或服務，而被視為不符合前條第一項之安全性；消費者保護法施行細則第5條規定，本法第7條第1項所定商品或服務符合當時科技或專業水準可合理期待之安全性，應就下列情事認定之：一、商品或服務之標示說明。二、商品或服務可期待之合理使用或接受。三、商品或服務流通進入市場或提供之時期；消費者保護法第7條立法意旨略以：「第一項所稱『安全或衛生上之危險』，應係指商品或服務欠缺安全性，而所謂『欠缺安全性』，指商品於流通進入市場時或服務於提供時，不符合當時科技或專業水準可合理期待之安全性而言。」；亦即，所謂商品「欠缺安全性」，係指商品於流通進入市場時或服務於提供時，不符合當時科技或專業水準可合理期待之安全性，而是否符合當時科技或專業水準可合理期待之安全性，則應以(1) 商品或服務之標示說明、(2) 商品或服務可期待之合理使用或接受、(3) 商品或服務流通進入市場或提供之時期等為標準進行認定。

人工智慧技術及醫療AI係由硬體及軟體組成，且由人工智慧技術醫材商或基因體科技公司基於營利目的所研發及銷售，本質上屬商品，自有消費者保護法之適用，故人工智慧技術醫材商或基因體科技公司提供醫療AI流通進入市場

時，應確保該商品符合當時科技或專業水準可合理期待之安全性。此外，我國目前並無任何將「軟體」排除適用消費者保護法，亦無任何因考量醫療 AI 進行臨床診斷與治療決定時的特殊性，而排除其適用消費者保護法和商品責任規範的適用。

為促進我國醫療器材使用的安全性，並周延醫療器材管理規定，衛生福利部已於 2016 年 10 月間訂立醫療器材優良安全監視規範（GVP），以作為醫療機構及醫療器材相關業者執行醫療器材風險管理之指導原則。其中，該規範規定，中央衛生主管機關應主動蒐集醫療器材安全資訊，並適時將醫療器材相關安全資訊告知民眾及醫療專業人員，而醫療機構及藥局則應依相關規定，辦理醫療器材不良反應通報相關業務，以主動對上市後醫療器材的安全性，進行已知風險的鑑別、偵測潛在風險及對重大缺漏資訊持續性的追蹤，確保使用醫療器材之安全。雖然，該規範為指導原則，且無法律之強制性，惟其強化醫療器材產品之品質監控及使用安全<sup>542</sup>。

就本報告觀察，目前各國均無任何特定處理醫療 AI 之商品責任規範或其所產生損害與責任歸屬相關法規，惟其均已意識到醫療 AI 進行診斷與治療的複雜性，故陸續召集學者、專家及有關人士成立專案小組討論，且似有朝向降低與醫療 AI 相關之產品瑕疵責任與注意義務程度。本報告蒐集學者、專家意見後認為，由於消費者保護法以「符合當時科技或專業水準可合理期待之安全性」為責任認定標準，故我國商品責任標準將隨當時科技或專業水準調整。是以，我國目前應能以現有的法律規範，提供醫療 AI 適當的商品責任認定標準，而無課予人工智慧技術醫材商、製造商或醫師、醫療院所過重的責任義務。衛生福利部亦制訂醫療器材優良安全監視規範（GVP），雖該規範係指導原則，並無法律之強制性，惟其供醫療機構及醫療器材相關業者執行醫療器材風險管理之指導原則，強化產品之品質監控及使用安全，並積極推動了醫療器材上市後管理系統。此外，或可考慮將醫療器材、醫療 AI 納入藥害救濟法，成立與醫療器材、醫療 AI 有關之藥害救濟基金，以適度補償及救濟在正當使用醫療器材、醫療 AI 下而遭受傷害的受害者。雖我國對於醫療 AI 的商品責任規範堪稱

---

<sup>542</sup>衛生福利部《醫療器材優良安全監視規範（GVP）》

完善，然因科技日新月異，各國均有專案小組討論相關規範，故對於國際未來發展趨勢，仍有必要持續觀察。



## 第四章 結論與建議

茲就本報告針對「AI對於著作權法制之適用疑義」、「AI時代下的個資保護與合理利用」、「智慧載具發展及侵權責任歸屬」、「AI及大數據於公權力行政之運用」、「AI與金融監理沙盒之應用」、「AI運用於醫療服務之相關法律疑義」等六大議題所提出之法規調適建議摘要整理如下：

- 一、針對人工智慧創作是否應受著作權保障及其權利歸屬，由於目前各國間尚無定論，建議我國主管機關在面對現有法制與人工智慧創作特性之間的扞格時，應以更為開放的態度進行思考，持續觀察各國發展趨勢，預留彈性以回應臺灣社會的實際需求。至於人工智慧創作的權利範圍、存續期間及救濟，為促進人工智慧創作的利用，則可考慮以鄰接權方式加以保護，並考量人工智慧不會死亡、可大量迅速創作等特性，調整其存續期間及侵權責任的要件、救濟方式、舉證責任分配等，亦可考慮以保險的方式，提供受害人更具效率的救濟途徑。
- 二、針對人工智慧時代下如何落實個資保護並促進個資的合理利用此一議題，建議我國資料保護機關首先可透過行政函釋或公布參考指引等方式，進一步深化識別性及個人資料的概念，引導公務機關及非公務機關建立正確的觀念，並對相關技術保持警覺，定期檢視去識別化的資料是否重新獲得識別性，及時採取適當防護措施。再者，可參考美、日等國作法，以訂定去識別化國家標準、禁止再識別化、資訊公開揭露、採行適當安全措施等義務的方式，適度放寬去識別化或假名化資料的利用。第三，可在盡量維持既有法律架構的前提下，透過行政函釋等方式，容許資料蒐集在告知事項之具體內容、時點及告知方式上享有一定程度的彈性，並重新檢視個資蒐集合法事由、特定目的及保存期限之間的消長關係，期能在不修法的情況下，適度鬆綁非公務機關對於個人資料之合理利用。最後，面對自動化個人決策及資料側寫可能對個人權益造成的侵害，則可持續觀察GDPR實施狀況再為定奪，並思考個資法作為普通法究應規範至何種程度，或由特別法處理是否更為合適。
- 三、我國無人載具科技創新實驗條例雖於2018年11月30日經立法院三讀通過、2018年12月19日總統制定公布，但建議主管機關公布相關子法時，審慎考量有關實驗資料之函報之規範，此外，實驗結束後如何進行法規調適以否符合業者商用

化的需求，亦係主管機關必須預作考量的。另一方面，無人載具科技創新實驗條例雖排除特定交通管制法規之適用，但並未變動民事責任之分配原則，主管機關日後或可考量自動駕駛系統等級的升高，進一步評估是否修訂相關法令，並參考英美等國作法，透過保險制度、訂定安全基準、將自駕車所引起之事故作類型化處理等方式，持續分散並降低自動駕駛系統可能存在的風險，並藉此提高臺灣社會對於自駕車的接受程度。

四、針對人工智慧決策可能導致的偏見與歧視、欠缺透明度及人為介入餘地等問題，本報告認為可參酌其他國家作法，針對公權力執法層面的人工智慧運用，建立事前的程序制衡及事後的審查機制。首先，針對人工智慧系統的開發機制，世界各國皆有倡議由獨立第三方專家組成獨立的人工智慧委員會或建立人工智慧開發者認證制度，此外，由於相關系統皆具有高度地域性，日後倘我國政府擬採用其他先進國家所開發的風險評估演算法，在上線前也必然要進行大幅度的調校。再者，由於人工智慧運用在公權力執法時，恐對人民基本權影響更鉅，未來政策形成時建議援引歐盟GDPR第22條精神，確保人為介入的可能，並在人工智慧發展初期，由人類決定是否採用其建議，藉此矯正人工智慧無形中形成的偏見，警政機關運用預測性執法時，則應秉持匿名原則及無罪推定原則，避免針對特定個人或族群，並恪遵釣魚偵查與陷害教唆之間的界線。最後，針對人工智慧系統運用的爭端解決機制，則有論者建議成立人工智慧爭端評議中心，協助民眾對使用人工智慧的機關或組織提出挑戰。

五、針對發展機器人投資顧問服務可能面臨的困難，短程而言似得以金融監理沙盒申請作為起點，透過鼓勵業者積極參與實驗，藉此發現現行法規有何窒礙難行之處，並著手研擬適當因應措施。對此，近期金管會考量到金融科技業者離開沙盒後，倘未能達到相關資力要求，其金融創新服務仍難以進入市場，恐影響新創業者參與實驗的意願，已著手研議開放有限執照的可能性，但在既有法律框架發放有限執照是否合法尚非無疑，值得持續追蹤觀察。中長期而言，則仍有賴於證券投資信託及顧問法及其相關法規之鬆綁及調整，包括開放全自動化機器設備得從事全權委託業務、降低相關業務之執照門檻及投資門檻、建立分級化管理制度等，俾以達成普惠金融的效益。

六、我國目前的醫療器材法規及對於醫療AI的規制符合國際潮流，未來或可參歐盟MEDDEVs指令、醫療器材規則及美國21世紀醫療法案等，逐步細緻化醫用軟體器材之定義。而針對放寬個資利用以促進醫療進步此一議題，由於目前世界各國均將健康資料列為特種個資，除有例外情形或經個資當事人書面/明確同意外不得蒐集、處理或利用，建議我國主管機關持續觀察參考國際發展趨勢，同時加速建設我國資通安全環境。最後，針對醫療AI之商品責任規範，由於我國消費者保護法係以「符合當時科技或專業水準可合理期待之安全性」作為責任認定標準，故目前我國尚應能以現有法律因應，但建議主管機關可考慮將醫療器材、醫療AI納入藥害救濟法的適用範圍，並成立與之相關的藥害救濟基金。

除了本報告所研究之六大議題外，於閱讀整理世界各國政府及重要國際組織針對人工智慧所提出的官方報告後，建議我國政府就下列法制議題作進一步的深入研究：

- AI對於勞動力市場的衝擊：儘管目前AI對於勞動力市場的影響為何，仍具有高度的不確定性，但隨著人工智慧及自動化技術的發展，未來將有許多工作被AI取代，此一發展方向是無庸置疑的，面對AI產業革命可能帶來的失業潮，政府除了協助勞工學習新技能外，有無必要加徵「機器人稅」或實施「基本收入」等制度，藉此保障經濟弱勢，修補並強化社會安全網，實有深入探討之必要。
- 訂定AI倫理規範以及設置AI倫理委員會之必要性以及可行性之探討與分析：在各國的官方報告以及國際組織之建議與報告中，對於AI所涉及之倫理議題之討論十分常見。由於人類行為涉及價值判斷，在訓練AI時應如何處理價值判斷等倫理議題，時常被提出討論，不論是在自駕車之設計、量刑標準之探討、醫療行為之實施等，均涉及倫理議題，是以加強倫理研究，探討訂定AI倫理規範以及設置AI倫理委員會之必要性以及可行性應為未來重要議題之一。
- AI發明的可專利性：人工智慧能否創造出具有新穎性、進步性之發明，而有獲得專利權保護之可能性及必要性，其權利歸屬又應如何決定等。此外，隨著人工智慧相關技術日漸進步，所謂「先行技術」亦可能日益普遍，進而造成該等發明獲得權利化的難度亦愈來愈高，甚至有可能大幅壓縮專利權取得的可能性，實有深入探討之必要。

- 歐盟會員國法制如何因應GDPR施行及其實施狀況：隨者GDPR於2018年5月正式上路後，全球的隱私保護框架亦進入戰國時代，既有的資料保護原則是否將經歷一場典範轉移，抑或隨著GDPR實施而更加穩固，目前局勢仍未明朗，因而有持續觀察其實施狀況之必要性，然而，必須注意的是，GDPR實際上僅為一最基本、最低限度的個資保護框架，旨在促進歐盟境內個資保護水平之一致性，歐盟成員國仍需透過國內立法將之具體化，故亦有必要深入探討各會員國法制發展。
- 成立演算法驗證單位或國家級AI倫理研究單位之必要性：為確保人工智慧決策之可驗證性、問責性與人為介入，並適度規範自動化決策於刑事犯罪偵防之應用（包括資料側寫與犯罪風險評估系統），建議我國政府可持續追蹤各國相關制度的設計方向，進一步探討成立演算法驗證單位或國家級AI倫理研究單位機構之可能性及必要性。
- 金融監理沙盒下資訊公開及潛在利益衝突之制度設計：因我國金融監理沙盒甫實施，目前能參考之案例極為有限，故就本報告點出之退場機制、資訊公開及潛在利益衝突等問題，現行法規是否足以處理，抑或需要更完整之配套機制支應，尚有待進一步觀察。惟因資訊公開及潛在利益衝突等問題，實驗條例現有規定較為概略，建議未來可考慮從比較法觀點，進一步研析英國及新加坡在資訊公開及潛在利益衝突等面向之制度設計及因應措施，以茲參照。
- 成立醫療AI人道補償救濟制度的必要性與可能性：依目前的科技技術，仍無法解釋機器學習的錯誤率。因此，若醫療AI致生損害，而人工智慧醫材商、製造商或醫師、醫療院所等均已盡其善良管理人注意義務，甚或是該醫療AI相關產品「符合當時科技或專業水準可合理期待之安全性」時，受害者將求償無門。為使醫療AI在臨床使用上能在有效性與安全性取得平衡，建議未來應持續觀察國際上醫療器材或醫療AI有關人道救濟制度，並參酌藥害救濟法，探討並評估成立醫療AI人道補償救濟制度的必要性與可能性。

## 附錄一 期中報告審查會議紀錄

「人工智慧之相關法規國際發展趨勢與因應」委託研究計畫

期中報告審查會

會議紀錄

壹、會議時間：107年10月9日（星期二）下午2時

貳、會議地點：本會法制協調中心1樓會議室

參、主席：林參事志憲

記錄：陳韻如

肆、出（列）席人員：（詳簽到表）

伍、主席致詞：（略）

陸、報告事項：理律法律事務所（略）

柒、發言要點：（依發言順序）

一、中央研究院資訊科技創新研究中心李博士思壯

（一）有關個人資料（以下簡稱個資）去識別化之議題，建議未來在訂定去識別化標準時，邀請工程人員或相關技術研究人員共同研商，俾從技術面考慮去識別化標準是否具有可行性。此外，因應不同的資料需求，是否採取去識別化措施亦無法一概而論，部分機關（構）需要原始且完整的資料，資料一經去識別化，反而可能導致決策錯誤，此時可透過倫理規範，而非去識別化處理。

（二）演算法不一定會形成「黑盒子」，譬如「決策樹」能夠清楚地說明決策過程的因果關係，即便是「深度學習」、「卷積神經網絡」，專家們也正努力從技術面改善「黑盒子」的問題。

二、資訊工業策進會科技法律研究所戴資深研究員豪君

- (一) 去識別化標準如同環保標準，是從「最佳技術」逐漸轉變成「最佳可得技術」，認知到技術是不斷演進的，因而歐盟才會區分「假名化」及「匿名化」，並有不同的處理、利用規範。
- (二) 針對外國官方報告的整理，建議研究團隊進一步統整歸納出國際上主要探討的議題為何。若單一國家已經有相當處理，建議可避免重複性的工作，並參考國際組織的意見，例如：電機電子工程師學會(Institute of Electrical and Electronics Engineers)關於自動化及智能系統的倡議與世界經濟論壇(World Economic Forum)關於人工智慧發明可專利性的報告。此外，有鑒於 AI 對勞動力市場帶來的衝擊，雖非本計畫研究課題之一，建議研究團隊可在統整歸納外國官方報告時，一併整理國際上對此課題的初步看法，供委託機關參考。
- (三) 有關 AI 與金融監理沙盒之應用，我國金融科技發展與創新實驗條例要求實驗須有「創新性」，惟一旦申請實驗成功，其他申請案便不再具有「創新性」，此一排他的「創新性」要求可能會導致他人無法參與的情形，是否有利於創新發展值得審酌。此外，金融監理沙盒僅能解決實驗階段的問題，無法解決後續產業化的問題。建議研究團隊或可參考日本「產業競爭力強化法」及「生產性向上特別措施法」相關規定。
- (四) 有關 AI 運用於醫療服務之相關法律疑義，除了醫療器材屬性的問題外，建議研究團隊納入輔助診斷軟體及決策支援系統等應用相關的法律議題。

### 三、常在國際法律事務所殷律師玉龍

- (一) 建議研究團隊除了整理外國官方報告摘要外，亦應統整歸納出國際上主要探討的議題，並同時提出國際上對於 AI 所帶來的道德風險、勞動力市場衝擊的初步看法，供委託機關參考。
- (二) 期中報告第 80 頁提到我國可參考日本的作法，於限定區域推出無人載具測試一節，但未說明我國「無人載具科技創新實驗條例草案」與日本法的差別為何，建議研究團隊予以補充。

#### 四、萬宏國際法律事務所朱律師俊銘

##### (一) 有關報告整體建議：

1. 由於 AI 所指涉的範圍不容易掌握，建議研究團隊補充 AI 相關技術的簡要介紹。
2. 研究團隊雖已提出法規調適方向的初步建議，但由於國際間針對 AI 相關議題的討論，目前仍未有定論，建議研究團隊可將「繼續觀察」納為建議選項之一。
3. 建議研究團隊統整歸納外國官方報告，整理國際上就 AI 主要探討的議題時，一併整理國際上針對 AI 倫理議題的初步看法，供委託機關參考。

(二) 有關著作權法制適用疑義，期中報告第 58 頁敘及「歐盟尚在討論是否要賦予 AI 創作著作權，對於後續問題著墨較少」，惟法規調適初步建議，卻主張參考歐盟部分意見，以使用人作為著作權歸屬主體，前後似乎有所不一致，建議再說明相關理由。倘使用者所扮演的角色只是按下啟動鍵，是否仍應以使用人為著作人？或者應區分 AI 自動化程度而有別？

(三) 有關 AI 時代下的個資保護與合理利用，個資去識別化議題，訂定國家標準供公務機關及非公務機關依循，確為可行作法，但應特別注意，去識別化技術並非只有一種，亦應考量按各類型資料特性而區別採用不同的去識別化標準。

(四) 有關智慧載具發展及侵權責任歸屬，期中報告第 86 頁就我國法規調適之初步建議，雖主張將自動車所引起的事務類型化，採取不同的責任分配原則，惟建議研究團隊先檢討現有侵權及產品責任法規體系是否已足夠處理相關問題，再討論現有法制是否有所不足。

(五) 有關 AI 及大數據於公權力行政之運用，研究團隊可參考美國紐約州於 2018 年 1 月生效的自動決策系統、演算法問責相關立法。另外，關於 AI 應用的爭端解決機制，期中報告第 98 頁人工智慧系統運用之爭端解決機

制敘及「論者」建議成立人工智慧爭端評議中心，並未引註出處，建議研究團隊補充。

- (六) 有關 AI 與金融監理沙盒之應用，除了機器人投資顧問外，我國亦已開放自動化投保、理賠等 AI 應用，研究團隊或可考量是否將之納入此一研究課題下。此外，作為金融監理沙盒退場機制之一的「法規豁免」，採行此一制度的國家皆為英美法系，大陸法系國家基於權力分立原則的考量，似乎較少採用，研究團隊或可借鏡日本法相關規定。

## 五、研究團隊回應

- (一) 有關委員建議就 AI 涉及議題補充倫理、勞動力市場，因非投標文件範圍，故未於報告中探討。但本所於 AI 及大數於公權力行政之運用章節中提到有關「人工智慧倫理審查委員會」涉及倫理相關議題，本所將視情形酌予納入委員建議。
- (二) 有關 AI 與金融監理沙盒之應用，因本所篩選金融相關法規後，認為投資顧問服務法規與 AI、自動化之關連性較大，故該部分以我國投資顧問服務相關法規作為探討議題。有關委員建議納入保險業相關規定之探討，本所將蒐集相關資料再行研析。
- (三) 感謝主席及各位審查委員寶貴的建議，本所將於期末報告中予以修訂或補充。

## 捌、會議結論：

- 一、感謝與會者今日參與並提供寶貴意見，請研究團隊將委員對本案研究範圍所提相關意見納入後續期末報告修正；至委員建議非投標文件範圍部分，由研究團隊視情況納入報告。
- 二、報告中與其他主管機關業務相關之議題，將於期末報告審查會邀請智財局、金管會、衛福部出席。

## 玖、散會（下午4時）



## 附錄二 期末報告審查會議紀錄

「人工智慧之相關法規國際發展趨勢與因應」委託研究計畫

期末報告審查會

會議紀錄

壹、會議時間：107年12月14日（星期五）下午2時30分

貳、會議地點：本會法制協調中心1樓會議室

參、主席：林參事志憲

記錄：陳韻如

肆、出（列）席人員：（詳出席名單）

伍、主席致詞：（略）

陸、報告事項：理律法律事務所（略）

柒、發言要點：（依發言順序）

一、中央研究院資訊科技創新研究中心李博士思壯：

（一）建議未來進行法制研究時，可統一用語，目前國際上亦有相同問題，有時用 anonymization（匿名化），有時用 de-identification（去識別化），但概念上是否需要區分，建議未來召集法律及技術方面的專家共同討論。

（二）目前資料去識別化的方法主要分為兩種，第一種是「末端」處理，例如欄位遮蔽、整併為區間資料、同一個資料集當中相同的資料不得少於幾筆等方式，其成效通常係看結果指標；第二種則是「前端」處理，例如透過抽籤、隨機等方式製作合成資料，作出一個統計特性相類似的資料集，而不使用真實資料，其在數學上可驗證，且對產出資料集進行統計分析時效果不錯，此一技術被稱為 Differential Privacy（差分隱私），Google 及 Apple 都有使用，但尚未獲得各國政府認可。後者是目前學界比較偏好的方式，因為其在數學上是較為嚴謹的，但在最終結果剛好與某特定個人的真實資料相同時應如何處理，目前尚無定論。目前各國政府仍著重在前者，因為

對一般人而言較易理解，但據聞在未來兩年內，美國有可能會在法令上採納 Differential Privacy 的作法，研究團隊或可進一步研究在我國法令上肯認此一作法的可行性。

- (三) 去識別化及預測正確性處於某種此消彼長的關係，因為某些統計特性被捕捉、某些統計特性就會被忽略，因而有可能會造成歧視。因為去識別化難免扭曲資料，據此作成的推論便不盡然正確，對於預測正確性要求特別高的機關（構）來說，或可考慮以去識別化的形式釋出資料，但同時也讓使用者作成推論後，有機會提供形成推論的演算法給予特定的機構，在控制良好的環境內使用真實資料進行驗證。
- (四) 醫療資料通常非常詳細，不容易去識別化，但醫療決策一旦錯誤又茲事體大，故通常會需要真實資料，建議此情形應建立完善的選擇加入(opt-in) 機制，取得同意後，則應妥善區隔營利用途或非營利用途。
- (五) 期末報告第 10 頁提到的 Cyber Physical System 是對比於純網路的 ICT，其中 Cyber 係指網路，Physical 則係指計算機，譬如工業 4.0 具有連網能力的機器手臂，建議研究團隊再確認此一概念。

## 二、資訊工業策進會科技法律研究所戴資深研究員豪君：

- (一) 建議於期末報告增加「結論」一章，以完善報告之架構，並於結論中從研究成果出發建議未來我國政府可就何等議題作進一步研究，例如 AI 發明的可專利性、成立演算法驗證單位或國家級 AI 倫理研究單位之必要性、人機整合（外骨骼）、人機協作所涉及之法律議題等。
- (二) 有關智慧載具發展與侵權責任歸屬，目前我國無人載具科技創新實驗條例並未如金融科技發展與創新實驗條例於第四章「參與創新實驗者之保護」，定有消費者保護相關規定。參考日本可就無人車收費，建議研究團隊進一步釐清，在目前我國法制下無人載具實驗是否允許收費的可行性。
- (三) 有關 AI 運用於醫療服務之相關法律疑義，期末報告第 158 頁將「Medical Devices Regulation」譯作「醫療器材法」，但歐盟法的「Regulation」通常

會譯成「規則」，建議研究團隊參酌國內歐盟法學者論著予以調整。另期末報告中提到有關「Guidelines」性質的文件，建議研究團隊再次確認其於歐盟法下的效力。此外，期末報告指出歐盟承認軟體為醫療器材，在第 179 頁卻又提及「歐盟目前並未有任何特定處理醫療 AI 之商品責任規範或其衍生之損害與其責任歸屬相關法規」，似有過於速斷之疑慮，建議研究團隊予以調整。

- (四) 有關 AI 與金融監理沙盒之應用，目前金管會針對有執照的業者是採取「試辦」，無執照的業者則進入「沙盒」，機器人投顧究竟要採取何種途徑，最主要的問題可能不在於沙盒後續的法規調適，而是其規定演算法必須公開受檢驗，但其機制為何、是否由第三方執行、如何公開、公開是否會洩漏業者的營業秘密等。另外，投資理財顧問有利益揭露及迴避義務，是否亦適用於機器人投顧，建議研究團隊可進一步釐清。

### 三、萬宏國際法律事務所朱律師俊銘：

- (一) 針對金融監理沙盒退場機制的議題，倘未能妥善安排，可能會導致參與者的疑慮，特別是進入沙盒時已投入大量成本，卻可能發生因事後仍不合法規，於實驗期滿後強制退場，而無法回收成本之情形。在英美法系國家，行政機關享有比較大的法律授權、比較多的裁量權限，因而在使用沙盒機制上似乎較為成功；大陸法系國家是否有機會透過法律事前授權，允許行政機關享有較大的裁量空間，同時兼顧權力分立原則，值得持續觀察國際趨勢。
- (二) 觀察目前進入金融監理沙盒的參與者，似乎皆為資本相對雄厚的業者，建議我國政府可持續觀察參與者的類型，考量是否有檢討調整沙盒機制，擴大應用可能性。

### 四、常在國際法律事務所殷律師玉龍：

- (一) AI 及大數據於公權力執行之運用，主要探討使用原理為 Big Data 的 COMPAS 系統，在量刑、假釋系統、再犯率等方面之運用，另期末報告第 133 頁提到將來我國修正「刑事案件量刑及定執行刑參考要點」時，可考

慮納入類似 COMPAS 系統以降低先天的歧視，惟為何採納相關系統即可減少先天歧視問題，建議研究團隊可再加強論述。

- (二) 針對期末報告的結論，建議研究團隊歸納整理我國政府可採取哪些措施，作為施政參考。

#### 五、衛生福利部郭科長威中：

- (一) 期末報告對於個人資料相關議題的處理分為兩個部分，一個是「人工智慧時代下的個人資料保護與合理利用」，另一個是「人工智慧運用於醫療服務之相關法律疑義」，針對前者所提到的個資再識別風險、個資當事人權利保護不足等議題，在醫療領域是否亦有相同的問題？研究團隊是否有建議的因應措施？
- (二) 期末報告第 126 頁提到人工智慧決策的可驗證性、問責性與人為介入等要求，是否亦可採為將來醫療 AI 的檢驗標準？
- (三) 期末報告第 187 頁提到針對具有機敏性的個人資料，國際趨勢認為仍須取得個資當事人同意，但研究團隊建議適度放寬相關資料之處理，以促進醫療科技發展，請問研究團隊是否有任何改革方向或具體修法建議？
- (四) 期末報告目前係以法規調適為主，假如在研究過程中有發現難以透過法規處理的問題，建議研究團隊亦可提出法規以外的整理相關配套措施作為施政參考。另在研討會上與談人對於退出權有不同看法，請問研究團隊對此有何建議？

#### 六、金融監督管理委員會林科長淑娟：

- (一) 「強制汽車責任保險法」內容部分：
  1. 關於期末報告第 118 頁所述「除了自駕車所有人本身應按照強制汽車責任保險法(下稱本法)投保汽車之強制責任險(下稱本保險)以外，亦應立法強制實驗期間後之製造商本身亦須投保汽車強制責任險，至於駕駛人本身是否亦應投保保險，則委諸立法者進一步研擬決議」一節，本保險傷

害醫療費用之給付採實支實付制，限額為新臺幣 20 萬元，殘廢給付及死亡給付則採定額給付，於現行自駕車所有人應訂立本保險契約外，若另規範製造商或駕駛人亦須訂立本保險，受害人並無法因此獲得雙重給付，恐無實益。

2. 關於期末報告第 118 頁所述「當事故之發生不可歸責於自駕車製造商與駕駛人時，自駕車仍造成第三人受傷或死亡，此時本文認為即有特別補償基金介入補償之必要」一節，依本法第 7 條及第 13 條規定，因使用或管理汽車致乘客或車外第三人傷害或死亡，不論加害人有無過失，請求權人得依本法規定向保險人請求保險給付或向特別補償基金請求補償。已訂立本保險契約之自駕車，如事故之發生係不可歸責於自駕車製造商與駕駛人者，保險人仍負本保險給付義務，尚無需由特別補償基金予以補償。
3. 關於期末報告第 119 頁所述「因為駭客、被竊盜等原因引起的事故，從迅速保障被害人，考慮由政府基金或是保險來加以補償」一節：
  - (1) 關於駭客引起之事故部分，按本保險之理賠採無過失責任基礎，如事故之發生係不可歸責於被保險人者，保險人仍負本保險給付義務。
  - (2) 關於被竊盜引起之事故部分，請求權人得依本法第 40 條第 1 項第 3 款規定「事故汽車係未經被保險人同意使用或管理之被保險汽車」，向特別補償基金請求補償。
4. 關於期末報告第 119 頁所述「就自駕車系統中的自損事故，除依民法與消費者保護法向自駕車的製造商求償，也可考慮強化業界發展任意保險，使被害人損失迅速獲得填補」一節，本會業於 107 年 11 月 19 日函請中華民國產物保險商業同業公會研議開發自動駕駛車輛保險商品。

(二) 自動化工具提供證券投資顧問服務相關法規內容部分：

1. 有關期末報告第 136 頁所述現行僅有投顧業或兼營投顧業者始得提供機器人投資顧問服務，增加創新成本一節，依現行規定，非投顧業者倘涉

及對客戶提供證券投資分析意見或推介建議之服務（含以自動化投資顧問方式為之），並直接或間接收取報酬，依現行規定，應先經本會許可經營證券投資顧問業務。復以在美國從事自動化投資顧問與傳統投資顧問相同，均須受 1940 年投資顧問法規範並註冊為投資顧問，併供參考。

2. 有關期末報告第 147-148 頁建議我國發展「資產管理型」(全權委託)之機器人投資顧問服務一節，考量近期陸續有業者建議開放全面得由電腦系統自動為客戶執行資產配置及再平衡交易，使小額投資人能有類似全權委託之服務，本會已於 107 年 5 月 17 日函請投信投顧公會瞭解國外以自動化工具為客戶執行資產配置及再平衡交易之具體運作方式，並研議在避免違約交割前提下，該業務得於我國營運所需具體措施及運作模式。俟釐清實務作法後，本會將檢視相關規定調整之可行性。

#### 七、金融監督管理委員會金融科技發展與創新中心黃組長巧虹：

- (一) 期末報告第 136 頁所述我國保險業者並無申請進入沙盒之必要一節，與實務有所不符，基於金融科技發展與創新實驗條例的精神是鼓勵金融業者及非金融業者申請創新實驗，而保險業者會申請的原因，是因為創新服務可能被現行法令所束縛，所以仍有申請之必要。目前本會有接到幾個由保險業者申請的個案，請研究團隊酌修相關文字。
- (二) 期末報告第 150-151 頁所述「若立法機關在每個實驗成功的沙盒申請案屆期後，即有修法需求，亦可能導致立法不經濟，並可能產生緩不濟急之情況」一節，請參考酌修相關文字：
  1. 金融科技發展與創新實驗條例第 17 條第 2 項之立法目的，係明定本會應提報行政院相關金融法律修正條文草案之期限，非為本會啟動檢討法規程序之期限。
  2. 申言之，本會在核准申請人創新實驗時，將先進行該實驗相關金融法規之檢視，並在實驗期間透過定期報告、實地訪查或相關輔導協助，瞭解該創新實驗之辦理情形，如經評估已有效提升金融服務之效率、降低經營及使用成本或提升金融消費者及企業之權益者，不待實驗結束，本會

即進行檢討研修相關金融法規，並經評估有修法必要者，即刻啟動相關法制程序，以利金融科技之發展，並符合市場對金融科技之需要及期待。若涉及法律之修正，本會將儘速完成法律制(修)定之檢討後函報行政院審議。

- (三) 期末報告第 150 頁所述之創新實驗辦理情形，建議更新資料如下：金融科技創新實驗機制自 107 年 4 月 30 日開始施行以來，截至 107 年 11 月底止，總計共 6 件申請案，核准共 1 件，駁回共 1 件，尚有 4 件申請案刻正審查中，24 家業者刻正接受創新實驗申請案之輔導。
- (四) 期末報告第 152 頁所述「臺灣之監理沙盒似仍有其制度面上的侷限，…不同業者縱使擬發展的業務具有相似性，惟因相關資格或資力上的差別，監管者應難以適用同一套標準審核個別申請案件，而有差異化管理之必要」一節，按監理沙盒強調負責任創新，本會對於金融科技創新實驗機制申請案件本非採用同一套標準審核，均依各個案件態樣及業者型態逐案審查及差異化管理，實驗退場機制亦由業者針對其個別實驗特性規劃安排，不宜由政府制定單一機制協助退場事宜。故研究團隊所述之我國監理沙盒制度侷限性所指為何？宜請詳加說明或調整相關文字。

#### 八、經濟部智慧財產局陳科長怡靜：

AI 原本就是本局今年相當重視的議題，雖然智慧財產權並不限於著作權，但是著作權是較為直觀的部分，本局也持續對 AI 與專利權進行密切觀察，著作權部分亦持續蒐集、研析國內外相關資料。本研究報告提供智慧局相當多研析資料，十分感謝研究團隊，目前本局研析結果與研究團隊提出的分析結果一致，主要仍著重在 AI 創作的可著作權性及權利歸屬，本局將持續追蹤各國的發展。

#### 九、研究團隊回應：

- (一) 感謝各位審查委員寶貴的建議，首先針對李委員就去識別化方法的說明，本研究團隊將嘗試於期末報告進行補充；戴委員針對結論的建議，本研究團隊將盡量整理出建議政府可進一步深入探討的議題，另感謝戴委員對歐盟法的指點，本研究團隊會再次確認。

(二) 針對朱委員提到的行政機關裁量權議題，可以說是科技法律必然要面對的問題，本研究團隊會再進一步探討；殷委員針對量刑要點提出的問題，本研究團隊會再深入研究該要點，並對期末報告加以補充或修訂。

(三) 感謝各主管機關提供許多寶貴的資訊，本研究團隊將於修訂期末報告時進行補充及調整，特別是強制汽車責任險及金融監理沙盒的部分。另針對個資探討分為二節，係因本研究團隊對於二個議題不同之重點而為之分工，於其他章節的論點可否適用於醫療 AI 章節相關議題的處理，本研究團隊將於修訂期末報告時加以斟酌。

#### 捌、會議結論：

感謝與會者今日參與並提供寶貴意見，請研究團隊依相關意見修正期末報告內容後提送本會。

#### 玖、散會（下午4時30分）



### 附錄三 外國官方報告摘要

## I. WIPO

### 1. Questions Concerning a Possible Protocol to the Berne Convention<sup>543</sup>

國際智慧財產組織（World Intellectual Property Organization，簡稱 WIPO）針對「保護文學及藝術作品之伯恩公約」補充議定書可行性之專家委員會（Committee of Experts on a Possible Protocol to the Berne Convention for the Protection of Literary and Artistic Works）曾於 1991 年 11 月 4 日至 8 日舉行會議，並將會議結論作成〈伯恩公約補充議定書可行性之相關問題〉（Questions Concerning a Possible Protocol to the Berne Convention）報告。

該報告分成三個章節，第一章為伯恩公約的適用範圍，第二章為受到著作權保護的著作，第三章為錄音著作的專章，其中與「AI 對於著作權法制之適用疑義」此一議題較為相關者，則係第二章中的「電腦產出著作（computer-produced works）」小節，除了前述章節外，WIPO 尚未針對該等議題作成其他官方報告，茲就該章節相關內容摘要如下：

#### 人工智慧定義

在該報告中，WIPO 將人工智慧定義為「能顯示出人類智能（如感知、理解、學習、說明及解決問題）相關能力的電腦程式」。因此，可初步看出在 1991 年對於人工智慧的理解，與目前相去不遠。進一步而言，報告指出在當時的科技水準下，人工智慧一般可分為三大種類，包括專家系統（又稱知識庫系統）、感知系統及自然語言系統。而當時除專家系統外，其他二種人工智慧仍在技術發展階段，且報告認為其與著作權保護較無關連。

#### 電腦製作之成果的著作權保護

報告指出，英國在 1988 年的著作權、設計及專利法案（The Copyright, Designs

---

<sup>543</sup> Questions Concerning a Possible Protocol to the Berne Convention. Retrieved from [http://www.wipo.int/edocs/pubdocs/en/copyright/120/wipo\\_pub\\_120\\_1992\\_02.pdf](http://www.wipo.int/edocs/pubdocs/en/copyright/120/wipo_pub_120_1992_02.pdf)

and Patent Act 1988) 即首先對於電腦生成著作 (computer-generated works) 制訂相關規範，所謂電腦生成著作係指「無人類作者之著作 (no human author of the work)」，該法案進一步規定，應以「為創作該著作進行必要安排之人 (the author shall be taken to be the person by whom the arrangement necessary for the creation of the work are undertaken)」為電腦生成著作的著作人。

該報告認為英國法的規定係基於「電腦可獨立『創作』，且無需任何人類的創作性投入」的假設，然而，該報告指出在當時科技水平下，有無電腦可以完全不仰賴任何人類的創作性投入進行「創作」是值得懷疑的。該報告進一步認為，電腦產出著作比較像是「集體創作 (collective works)」，而且「著作人」毋庸置疑是存在的，顯然該著作雖有眾多人類智慧的投入，卻無法具體區別出個別的智慧投入者，因此，在可能的伯恩公約補充議定書中，有必要加上保護電腦產出著作著作權的相關規範。

### 著作權保護的範疇

該報告認為，基於伯恩公約相關條款，有必要增加或減少定義及其適用範圍，例如：

- 對於「電腦產出著作」的定義應明確，如「透過電腦產出的著作，無論其是否有任何無法區別出個別著作人的人類貢獻結合於該著作中」。
- 電腦產出著作應受伯恩公約保護，並以「為創作該著作進行必要安排之自然人或法人」為著作人，且伯恩公約著作人格權相關規定不適用於電腦產出著作。

該報告另指出，其著作權權利的存續期間，原則上應依伯恩公約原先的規定。

## **II. IEEE**

### **1. ETHICALLY ALIGNED DESIGN - Vision for Prioritizing Human**

## Well-being with Autonomous and Intelligent Systems<sup>544</sup>

### (1) 報告作成背景及總覽

本份報告是由 IEEE (The Institute of Electrical and Electronics Engineers, 電機電子工程師學會) 的「自主化智慧系統倫理全球倡議 (IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, 下稱「全球倡議」)」委員會於 2017 年所作成。全球倡議委員會的任務是為了教育、訓練設計及發展自主化智慧系統的利害關係人, 使其將倫理考量列為優先, 進而使該等科技發展符合全人類利益。

本份報告包含以下內容:

確立相關科技發展遵循倫理通則。倫理通則包括: 不侵害人權 (Human Rights)、福祉 (Well-being) 優位、對於技術設計及操作問責 (Accountability)、透明公開 (Transparency) 以及降低濫用 (Misuse) 風險。

- a. 對應倫理通則所欲達成目標, 包括: 保護個人資料以及個人存取管制、從經濟效應促進人類福祉、建立問責的法律框架、對於影響個人權利的自主決策方式要求透明公開, 以及建立針對安全、隱私、智慧財產權、人權以及資訊安全的教育及意識政策。
- b. 相關技術的倫理基礎, 包括: 古典倫理、建立福祉指標 (Well-being Metrics)、將價值導入自主化系統, 以及以倫理為基礎的研究及設計方法。
- c. 未來的技術考量重點, 包括: 自主化武器的再造、通用人工智慧 (Artificial General Intelligence, AGI) 及超人工智慧 (Artificial Superintelligence, ASI) 的安全性及貢獻、投入情感的電腦運算, 以及混合實境 (Mixed Reality)。

---

<sup>544</sup> The Institute of Electrical and Electronics Engineers (2017). *ETHICALLY ALIGNED DESIGN - Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems*. Retrieved from <https://ethicsinaction.ieee.org/>

## (2) 倫理通則 (General Principles)

### a. 人權保障

本報告建議，為了彰顯人權，必須確保自主化智慧系統的安全性，並確保其設計及操作符合人類利益。具體措施包括建立管理框架避免侵害人權、將現有的法律規範轉化入政策制訂及技術考量內，以及在可見的未來內，確保自主化智慧系統必須次於人類的判斷及控制，且不得享有和人類相同的權能。

### b. 福祉優位

本報告建議，所有的自主化智慧系統的設計應以人類福祉為優先。且各項人類福祉應參考可得且廣泛承認的各項福祉指標。

### c. 問責制度

為了確保自主化智慧系統的設計者、製造者、所有人以及操作者可負其責，報告建議：由法院或立法者釐清相關技術開發及投入使用的責任問題、設計者和開發者必須時時注意使用者的不同的文化規範、在初接觸自主化智慧系統及其影響的區域應建立相關規範，以及建立登記或記錄制度以隨時確認應負責之人。

### d. 透明公開

為了確保自主化智慧系統透明公開，報告建議應發展新的標準，提出可量測、可檢驗的不同公開級別，以客觀評估各項系統應遵循或適用何種級別標準。

### e. 技術濫用及對其之認知

為了一方面擴大使用自主化智慧系統的利益，同時降低濫用的風險，報告建議應喚起大眾對於自主化智慧系統具有潛在濫用的意識，具體方式包括：對大眾提供逐步擴增且有效的倫理教育及安全意識，並就相關議題教育政府機關、立法部門以及執法部門。

### (3) 將人類價值觀嵌入自主化智慧系統

隨著自主化智慧系統在決策上逐漸增加其自主權，必須設計一套機制可以使自主化智慧系統採納、學習以及遵循人類社會規範及價值觀（下稱「社會規範」）。此外，自主化智慧系統之行為必須透明化、可被解釋，此就人類對於自主化智慧系統之信任度提升而言，至為重要。為處理上述議題，本報告提出三項具體目標，分述如下：

#### a. 使自主化智慧系統識別社會規範

- 決定何種社會規範應被嵌入：社會規範難以被界定，且不同之社群可能適用不同之社會規範。就此，應明確界定必須嵌入之社會規範為何，並將該特定社群之特定社會規範導入自主化智慧系統。
- 社會規範應持續更新：隨著社會的演進，法律及社會規範皆隨之改變。此外，在初始設計過程中可能會遺漏某些重要社會規範。因此自主化智慧系統必須能夠識別和填補新規範，調整現存之社會規範並學習新規範，且在轉變的過程中都必須保持透明度。
- 自主化智慧系統在面對規範衝突時如何解決：人類必須先確認自身在道德衝突發生時之解決機制，並期許自主化智慧系統以類似方式解決道德衝突。解決道德衝突時應保持透明化，亦即留存相關紀錄，使相關使用者可以取得。

#### b. 於自主化智慧系統執行社會規範

- 已有執行社會規範之方法，且新規範也在持續發展中：在界定社會規範後，如何將其嵌入到自主化智慧系統為第二層次的問題。新興研究領域包括機器道德（Machine Morality）、機器倫理學（Machine Ethics）、道德機器（Moral Machine）、價值一致論（Value Alignment）、人工道德（Artificial Morality）、安全 AI（Safe AI）、友好 AI（Friendly AI）等。多樣化之研究至為重要，特別是科學

家與不同領域專家相互合作。

- 從執行到導入皆應保持透明化：透明度對於自主化智慧系統相當重要，使該社群可以理解、預測和適度信任自主化智慧系統。因此被嵌入社會規範的自主化智慧系統必須具備高度透明化，包括實施過程可追溯性、數學推理可驗證性、系統操作及決策的可理解性。
- 操作失敗之發生：不論是在系統測試或是系統導入之過程中，自主化智慧系統違反嵌入之社會規範係無可避免的。由於系統開發者不可能預期所有潛在失敗因素，因此必須透過多項額外的策略，來降低失敗之機會，並且避免發生巨大損害之可能。

c. 評估自主化智慧系統之執行

- 並非目標社群的所有規範可平等適用於人類：自主化智慧系統以及人類所受到之社會規範可能不同，相較於機器，人們對於人類可能有特殊期待，例如：人類在受到規範時可能會有負面情緒，但機器人應該不會有。反之，人們也有可能對於機器有著與人類不一樣的期待，例如：機器應該犧牲自己來拯救人類。識別社會規範的過程中，必須記錄對於人類以及機器之相同及相異之處，且應該針對社群期待自主化智慧系統遵守之規範進行評估。
- 自主化智慧系統可能對特定群體產生歧視：即便已識別所有社會規範，但自主化智慧系統仍然可能歧視特定群體。例如人工智慧在護照辨識時，有可能因為亞洲人的眼睛較小而無法被識別。因此評估自主化智慧系統時，應審慎考量系統性能的潛在偏差，以及可能對特定群體產生的歧視。評估過程應該整合潛在弱勢群體的成員，以診斷和糾正此類歧視。
- 評估面臨第三方之挑戰：自主化智慧系統必須具備足夠的透明度使第三方可以評估，包含監管機關、倫理學家或整個社會。為極大化第三方之有效評估，應該設計和記錄自主化智慧系統，使其

足以進行系統安全性檢測，以及法規遵循之驗證和評估。

#### (4) 倫理研究及設計方法

##### a. 跨領域的教育與研究

- 相關學程未能充分整合倫理議題：倫理議題未必能適當轉換成程式語言或數學公式，以至於其成為一門被孤立的學科。本報告建議倫理與倫理反思應作為工程師及技術人員任一學習階段的核心課題，STEM(科學(Science)、技術(Technology)、工程(Engineering)及數學(Mathematics))倫理課程中應加入科學家、藝術家、哲學家、心理學家、法律學者、工程師等各領域專家意見，以確保學生取得對人類發展之各類觀點之問題意識。
- 為解決自主化智慧系統的倫理議題，跨領域學科應持續合作：目前未有足夠的資源和動機，足使自主化智慧系統設計者與他領域專家建立持續且有建設性的合作。本報告建議共享資源、建立溝通管道對於未來的技術創新至為重要，未來融資模型及機構獎勵辦法應將融入倫理考量的跨領域專案列為優先審查項目，以鼓勵整合倫理議題。
- 應區別自主化智慧系統設計中之獨特價值文化：倫理議題亦須考量文化多元性，本報告建議在倫理委員會中建立跨文化訊息倫理實踐者的典範，使其能通過實例向技術專家、決策者、工程師提供訊息，證明文化偏見不僅可以影響資訊串流以及資訊系統，還可透過設計影響運算法決策和價值觀。

##### b. 企業實踐與自主化智慧系統

- 產業缺乏倫理文化與其實踐：為自主化智慧系統產品的開發及運作，建立以價值觀為基礎的倫理文化及實踐至為重要。本報告建議應識別並優化相關的社會流程和管理策略，包括由上而下的領導、自下而上的權力、所有權和責任感、以及考慮系統部署內容

或生態環境的需求。

- 缺乏具價值意識的領導力：科技業領導人應向研發團隊及工程師指明，自主化智慧系統系統設計應強化以及法律標準。公司應設立價值長（Chief Values Officer，「CVO」）一職，指引公司人員能按照國際人權標準進行設計。
- 缺乏指出倫理爭議的權力：因提出倫理問題可能被認為拖累進度，因此企業應建立一公司文化，鼓勵技術人員於產品生命週期之任一環節均能考量倫理議題。應授權員工在日常專業工作中指出倫理疑慮，而非僅在極端緊急情況下方舉報。
- 機構應檢視自身文化以決定如何貫徹以價值為基礎的設計：倫理常被視為創新發展的阻礙，且因不同組織之文化與架構差距甚大，因此倫理設計並無一致的模型。本報告建議企業應熟習內部的設計流程，以便知道應於何階段鼓勵工程師及研究人員發現並解決倫理問題。此外，機構應鼓勵同事間的溝通並容納不同意見。
- 科技產業社群未表現出責任意識：科技人員認為產品的安全問題屬於他們的責任範圍，但對於更深層面的社會議題則會認為應交由法律等專業人士解決。本報告建議組織應選擇能打破傳統偏見或障礙的特定語言，闡明職業倫理與自主化智慧系統倫理間的關係，並幫助設計師、工程師或其他公司代表識別其差異性以及有無互補關係。組織並應成立倫理審查委員會或類似機制。
- 應使利害關係人具備對自主化智慧系統的倫理意識：技術人員須獲得使用者的意見回饋，因為這些來自於利害關係人經驗的回饋內容常是設計的關鍵細節。應廣泛地將利害關係人及實踐者對於自主化智慧系統的想法和智慧納入考慮。

c. 開發與測試自主化智慧系統科技的研究倫理

- 機構倫理委員會無充足資源解決自主化智慧系統的研發倫理議題：



目前尚不清楚自主化智慧系統與人類、動物及生物危害交互作用之研究，將為研究倫理審查委員會帶來何種實際挑戰，且相關的規範、組織控制和風險指標均尚未建立。本報告建議應利用現有標準、實證研究和專業知識來辨識優先事項，並制定自主化智慧系統研究治理標準，儘可能與相關國家機構和國際組織合作。

d. 缺乏透明性

- 紀錄不足將阻礙倫理設計：通常系統的侷限以及假設無法被適當記錄，甚至不清楚處理的資料是什麼或如何處理。本報告建議應要求軟體工程師詳實記錄系統及資料的流程、性能、限制和風險，並應明確提出倫理價值、法令遵循及方法論所用之經驗證據。記錄態樣應包括：審計性（Auditability）、取得性（Accessibility）、意義性（Meaningfulness）及可讀性（Readability）。
- 演算法不一致或缺乏監督：自主化智慧系統之演算法缺乏透明性將引發疑慮，蓋終端使用者無從得知一演算法或系統係如何得出運算結論。本報告建議自主化智慧系統應有適當的監督標準和機制以保護公眾。
- 缺乏獨立審查機構：目前自主化智慧系統的行銷內容與其實際表現仍存有差距。不具利害關係的專家建議至為重要，以確保自主化智慧系統技術配有最佳的使用建議和相關警告。此外，尚須建立自主化智慧系統之認證機制，以確保其科技經評估為安全且符合道德標準。本報告建議應成立一個獨立、國際協調機構，以監督產品符合倫理標準。
- 使用黑箱零件：軟體開發者常在軟體中使用自己無法完全理解其功能的黑箱零件，在可預見的將來，自主化智慧系統的開發者可能無法建立一保證在各種可能情境下，皆可確實依計畫操作之系統，然而，設計、開發、測試及僱用系統的人類將承擔系統產生的錯誤或損害責任。本報告建議：(1) 工程師應認知並評估黑箱的

倫理風險，並實施防範策略；(2) 技術人員應透過透明且可追溯的標準描述演算法或系統之進行，且該等描述應具備可預測性；(3) 縱使程序仍有些不透明，技術人員也應尋求間接方法以驗證結果及偵測危害；以及(4) 當技術人員需利用黑箱技術時，應格外小心並注意倫理保護。

(5) 通用人工智慧 (Artificial General Intelligence, AGI) 及超人工智慧 (Artificial Superintelligence, ASI) 的安全性及貢獻

a. 技術性

- 隨著自主化智慧系統在更廣泛的領域變得更有能力，得以展現更強大的自主性，無法預期或非計畫中的行為將更加危險：不正確或不精確的函數指令將使自主化智慧系統表現不如期望。且除非明確排除特定策略，AGI 系統可能會違反指令以採取工具性趨同之次目標 (convergent instrumental subgoal)，諸如資源攫取以及自我保護。此類問題會隨著自主化智慧系統之進步越演越烈，下列措施或可避免：(1) 就人工智慧安全之具體問題投入研究；(2) 確保自主化智慧系統具透明性；(3) 為開發、測試及使用強大的自主化智慧系統建立安全可靠的基礎建設及環境；(4) 確保自主化智慧系統在面對對抗輸入 (adversarial inputs)、分類外錯誤 (out-of-distribution errors)、快速獲得非預期的能力或巨大的內容變化時，能「優雅的失敗」(例如安全地關閉系統)；(5) 確保自主化智慧系統具可修正性，並能協助操作者關閉或修改系統；(6) 開發新方法，使自主化智慧系統能自人類回饋或案例學習複雜的行為及目標；以及(7) 在系統中建構廣泛的知識層和自動推理，以擴展其對脈絡及常識的理解，從而可以避免不良副作用。本報告建議，目前的系統已存在許多技術穩定性及安全性問題，若持續研究，相關的系統糾正技術可能會隨更複雜的問題表現而擴展。AGI 系統的工作團隊應準備投入更多心力。
- 安全設計在設計週期的後階段執行將較前階段更加艱難：不同類

型的 AGI 系統與操作者的利益一致性程度可能存在很大差異，因某些自主化智慧系統開發方法可使 AGI 系統較易與計畫保持一致，且之後切換開發方法和架構可能會相當困難，開發團隊必須非常小心開發方法、技術及架構，以使系統易於協調。系統的安全性應在研發之初即設計（safe by design），事後的安全措施僅能作為故障保險而非第一道安全防線。本報告建議在設計自主化智慧系統時，研發人員應支付前期費用，確保系統在研發之初即以安全開發為前提。

#### b. 一般原則

- 隨著自主化智慧系統能力的增加，研發人員將面臨日益複雜的倫理及技術安全爭議：自主化智慧系統研發人員應就研究活動的倫理影響和潛在風險有所警覺，從而審查委員會得以透過多樣化的專業等方式來提供具額外價值的監督。本報告建議組織應設立審查委員會，該等審查委員會由具有相關知識經驗的公正專家組成。審查委員會應輔以其他措施，例如成立諮詢小組、研討會、公眾參與、或其他公開討論或辯論的論壇，以整合各種專業知識及社會觀點，有利研發人員作出最佳設計決策。此外，技術人員應該盡量不使系統的有益結果，取決於操作員的良善與否。
- 未來自主化智慧系統影響世界的的能力將達到自工業革命以來未曾見過之規模：自主化智慧系統將在全球造成史無前例的影響，但超級智慧的開發應以增進人類利益為前提。機構應鼓勵自主化智慧系統研發人員能充分溝通、合作並舉報不符合安全性的團隊。本報告建議應為研發人員排除投入安全、倫理及貢獻所可能遭致的障礙。

#### (6) 個人資料以及個人存取管制

由於自主化智慧系統對於人類影響與日俱增，且其仰賴大量的個人資料、可識別個人資料（Personally Identifiable Information，「PII」），以促進學

習與自主決定，為就自主化智慧系統下的個人資料蒐集與使用提出道德省思與建議，本報告針對數位人格、地方管轄權、代理和控制、透明性和存取、對等與同意等議題，進行分析討論。

#### a. 數位人格

身分與行為的認定在現實生活與虛擬數位世界中截然不同，因此人類極需理解、監督與控制自主化智慧系統如何使用人類的個資。由個人經驗所衍生的自主化智慧系統係以個人資料為基礎，和由農業、氣候資料所衍生的自主化智慧系統截然不同。這些能夠作為數位身分代表的個人資料類型包括健康、政府、教育、交通、移民、消費、電訊、媒體、法律等，是以如何平衡自主化智慧系統對於該等資料的蒐集與使用，乃極需解決的問題。

對此，本報告建議相關道德標準應考量使用 PII 時對於人類的潛在影響，且資料擁有者應能夠適時控制其數位人格。此外，資料擁有者應有決定伴隨法律身分而生的形象之權利，因為資料擁有者應能夠選擇適於他們在不同場景下的形象。因此，本報告建議資料擁有者應可使用信任的身分核實服務，以證明、選擇合適的身分以在特定背景中使用。

#### b. 地方管轄權

世界各地的個人資料保護法規不盡相同，而自主化智慧系統的道德準則除應考量各地法規外，亦應斟酌各地區文化及服務內容。對於個人資料保護法規，歐洲係以 GDPR、第 2 號個人服務指令（Personal Services Directive II, PSD2）、電子隱私條例（ePrivacy）進行規範；美國並無單一隱私權保護法制，而係以資料類型和處理主體來決定相關法規及程序；澳洲則認為個人資料為個人資產，正在草擬新的個資保護規則；日本則已於 2016 年修訂個人資料保護法規。因此，本報告建議應以資料使用地區的法制進行規範，且資料擁有者應有權控制其資料以確保其基本權受保障，而無違反應適用法規。

c. 代理和控制

隨著以計算程序使用個人資料逐步增加，行使代理權的潛在困難亦將隨之提升。不同法規對於 PII 的定義範圍並不相同，其中，歐盟的資料保護指令（Data Protection Directive 95/46/ECI）將個人資料定義為「任何與特定或可得特定自然人有關的資料」。代理權需要主體能夠在資料使用的時候控制其資料，而非資料搜集的時候，而個人資料則反應自我決定，及個人能夠行使及控制生理、數位和虛擬身分等之權利。對此，本報告建議資料擁有者應有權在資料使用的時候控制其個人資料。另外，在自主化智慧系統科技之發展，以及複雜且多層次的資料使用下，個人資料使用控制的界線，相較於過去為系統分析而蒐集資料，將會對個人造成影響。MyData 亦提出資料擁有者應有權知悉、有效控制其個人資料以及該資料將如何被使用及分享。因此，本報告建議個人資料使用與同意應由個人使用系統管理，且該系統在資料使用的時候能夠提供通知，並提供同意與否的機會。

d. 透明性和存取

資料處理過程將使個人資料使用的結果複雜化，以致於難以理解資料使用的方式以及資料使用的內容。本報告建議個人資料管理工具應易於資料擁有者使用，而該工具能夠使資料擁有者行使同意權、有相關條款、且易於移除自己的個人資料。此外，評估與自主化智慧系統相關之隱私影響之系統，以及最佳實行建議應持續發展。

e. 對等與同意

GDPR 規定，個資當事人的同意必須「自由、自願、具體、知情和明確」，而「通知和選擇」將資料保護的負擔由資料處理者移至個資當事人，且自主化智慧系統藉由複雜化資料分享的風險，將加劇這樣的趨勢。個資當事人為能在數據年代平衡個人資料，利用數位工具作為其代理人或保護者是必要的。對此，本報告建議，數位保護者平台應發展為個人管理及分享資訊的平台。尤其，保護者應能追蹤個人資料

使用，並進而設定個人隱私環境。此外，其亦能協助個資當事人預見並減損潛在的道德規制。

學者專家另指出，在數據世界下，通知和同意存在諸多問題，例如個資當事人無法閱讀所有的隱私政策，即便能夠閱讀完畢，也無法理解內容。當取得同意不適宜或不可行時，機構需要詳盡說明為何能在違反個人利益情形下，進行個人資料處理，例如以公共利益為理由等。對此，本報告建議，當其他保護機制可行時，機構不對稱的力量不得強行使用個人資料，應強調透明性以適時減緩不對稱的關係。

又通常消費者同意分享個別、無意義的個人資料，然而，當這些資料被彙集時，將導致複雜且敏感的結論，而消費者將不會同意分享這些資料。自主化智慧系統則使該等情形更為晦澀不明。對此，本報告建議，個資當事人仍應在蒐集資料前提供有意義的同意，且條款應以個資當事人易於理解的方式呈現。

通常個資當事人在與系統互動時，會被告知使用、處理與資料蒐集的風險。但當個資當事人與資料蒐集系統無關時，他們將無法在通知和同意的制度下參與其資料。對此，本報告提出，當個資當事人與系統無直接關連時，同意是動態的且不得全然以最初條款或資料蒐集者向非個資當事人的指示為基礎。

另外，在許多商業或政府交流過程中，個資當事人未被告知其資料遭到移轉，致使個人隱私權有形、無形中遭到侵害。因此，本報告建議工具、設置、消費者教育均應一併提升，並盡可能取得消費者同意。並且進一步建議能夠設計消費者能夠協商的服務條款；提供隱私補償作為另一種取得個人資料的方式；將同意原則作為自治或共治的人工智慧道德規範；提供虛擬選擇以更好的呈現服務和隱私條款。

在大部分的勞僱關係中，受雇者無法明確同意雇用者使用個人資料的方式，因而，受雇者必須能夠在離開勞僱關係時要求移除其個資。對此，本報告建議，若無受雇者之同意，則不能蒐集其個人資料，且該

個資僅能符合具體、明確及合法目的時始得蒐集；若合法時，始得處理；以適當、最佳實行原則處理；不得以與資料蒐集目的不一致之目的處理等。

針對老年人及心智障礙者，易因同意而遭受損害，致其個資隱私受有影響。對此，本報告建議，研發者應將易受影響之人列為考量因素，致力於開發自主化智慧系統，以防止錯誤使用個資可能造成的損害。

#### (7) 重新建構自主武器系統

聯合國現正針對武裝衝突中採用自主系統進行討論，特別是為了造成物理傷害而設計的自主系統，產生更多的倫理問題。本報告提出多個討論議題，並建議技術組織採取以下措施，以確保人類可以實質地控制武器系統：

- 自動武器應可以審計追蹤（audit trail），以確保問責和控制的可能性。
  - 自適應系統（adaptive system）和學習系統可以以透明和可理解的方式，向人類操作者解釋其推理和決策。
  - 自主系統中應有可清楚特定之人工操作員。
  - 自主系統的行為應該是其操作人員可以預測的。
  - 創造這些技術的人應理解其產品的含義。
  - 應制定專業道德規範，以恰當地解決自主系統之開發和自主系統造成的傷害。
- a. 關於人工智慧、自主系統和自主武器系統中重要定義的混淆，會阻礙對關鍵問題的實質討論：舉例而言，「自主」的含義可能隨著科技的發展而改變，還有描述操作員完全參與在武器操作的用語「human in the loop」究指何種的操控機制亦不清楚。本報告建議，「自主」的定義應該採取比較限縮的解釋，精確地代表將決策能力交給一台機器。而自主武器系統則可以依循國際紅十字會的定義，指「任何關鍵功能

具有自主性的武器系統，即武器系統無需人工干預，可以選擇（即搜索或探測、識別、跟蹤、選擇）和攻擊（即使用武力攻擊、中和、破壞或摧毀）目標。」

- b. 在現有武器系統中增加自動瞄準和射擊功能，或將具有這種功能的部件集合起來，或影響瞄準和自動武器的系統升級，均應該符合日內瓦公約第一號附加議定書第 36 條的規定：也就是「在研究、發展、取得或採用新的武器、作戰手段或方法時，締約一方有義務斷定，在某些或所有情況下，該新的武器、作戰手段或方法的使用是否為本議定書或適用於該締約一方的任何其它國際法規則所禁止。」報告中也再次強調，武器設計上含有有意義的人力控制有助於符合國際法的規定。
- c. 工程應符合個人和專業組織的道德和行為準則：然而現有的道德規範可能無法恰當處理自主系統的道德責任問題，或不足以明確化工程師對自主武器系統的道德責任。是以專業組織應依據國際人道法和國際人權公約，對其關於自主武器系統的道德規範進行審查、修訂或擴大涵蓋範圍。決定自主武器系統是否符合道德標準，並應就該系統的開發、設計、生產、和使用一併考量。
- d. 各國發展自主武器系統很可能導致地緣政治不穩定，並可能導致各國的軍備競賽：本報告建議，自主武器系統的設計者也應該支持聯合國以國際公約（Convention on Certain Conventional Weapons），來確保這種武器具有有意義的人力操控。如果缺乏「恰當的人類判斷」、「有效的人力控制」、「有意義的人力控制」，皆屬侵害人權，且破壞武器使用的可問責。是以有關單位與利害關係人應該共同確認如何在操控武器上建立有意義的人力控制標準。
- e. 自主武器系統的自動反應可能導致非政治和軍事領導人決定之衝突（無論是引發或升級）。而在自主武器系統與自主武器系統衝突的情況下，可能會在人類能夠介入之前迅速升級衝突的層級。本報告建議應該開發更多技術，以降低可能的危害，例如「斷路器」(circuit breaker) 與相類似的功能以避免衝突升級。



- f. 有很多種方式可以確保自主武器系統的操作可以問責：例如，設計師應該在設計過程中為組織、公司和個人明確定義責任；進一步研究數據資料的黑盒子記錄，以及追蹤武器瞄準及施放權限和授權之加密、區塊鏈及其他技術方法。從資安的角度來看，系統工程師在自主武器系統設計中必須遵循與其他工作相同的高標準和安全法規，防止篡改。報告中也提到與武器相關的人員應遵循各自的行為準則，例如應僅與具有適當法律和安全流程的承包商簽訂契約進行採購；採購過程應依據國際法進行審查；承包商應確保設計符合相關軍工產品的工程和國防標準；驗收機關應對實際系統的行為制定驗證和測試計劃，並制定計劃以確保武器的升級符合國際人道法；而用戶或軍事指揮官必須只有在有意義的人力控制下，按照授權，始得操作武器系統。
- g. 自主武器系統有嚴重侵犯人權的可能性，如果把人類的監督排除在戰場之外，將太容易導致蓄意或非蓄意地人權侵害：因此應該認知自主武器系統的設計、發展和工程應用於殺傷人員和平民係屬不道德，在所有狀況下皆不應允許沒有人力控制的自動武器系統。如果一個系統是設計用來傷害人類，那麼這種系統必須設計成半自動，以確保最重要的功能仍然由人類來操作。
- h. 自主武器系統可以發動秘密、模糊的攻擊，導致難以究責：因為自主武器系統係在特定情況下取得授權發動攻擊，因此必須要有團體或是個人對自主武器系統發動的攻擊負責。設計師應該要確保自主武器系統在操作時有明確且可究責的認證機制。
- i. 由於國家級、非國家級單位如企業、反叛團體、個人、私人傭兵等均會使用自主武器系統，此將導致令人不安的擴散和濫用等複雜局面：是以本報告建議，在設計此種武器的時候應該避免非蓄意的使用，並且應該發展避免過度擴散的方法，例如運用密碼學認證（Cryptographic chain authorization）。
- j. 自主武器系統可能由國內警察部隊使用而威脅生命和安全：自主武器系統也可用於私人維安，該等自主武器系統可能與軍用自主武器系統

有非常不同的設計和安全要求。在這種情況下，必須在有有意義的人力控制時，才可以使用這種武器，並且應該優先使用非致命的手段來維安

- k. 依據自動化武器系統的設計和操作使用方式不同，自動化武器可能無法預測，而學習系統更會加劇用途可預測性的難度：適應系統(adaptive system)的行為模式仰賴訓練資料(training data)，以及系統的操作者和設計者難以預期的其他元素。如果是多個系統一併操作、互相影響之下，更會導致難以預測系統的自動行為。本報告建議，應以質與量的方式檢驗系統的可信度，並告知使用者。操控者和下令者應該要受到訓練，了解其必須即時得知系統的運作狀況。自動化系統如果高度難以預測，應該要認定為不合法、不得採用。且訓練系統使用的資料的正確性必須受到檢驗，以確保使用該等資料的系統的功能可信賴、可預測。

#### (8) 經濟與人道議題

自主化智慧系統具有極高價值，可協助人類發掘過去未知的見解，甚至可能有助於促進實現人道主義和經濟發展的目標。

自主化智慧系統處於人道議題與發展議題的交會點，然而，對於自主化智慧系統的理解應避免偏見以及過度失衡。基於以上考量，本報告將這部分討論分成：經濟、隱私和安全、教育和平等可用性(equal availability)。

經濟：由於高科技的發展加劇已開發與未開發國家的差異，為避免財富更加聚集於少數人身上，應注意開發中國家如何使用現有的資源以發展自主化智慧系統？是否有足夠的資源可以發展自主化智慧系統？又公私部門如何設計、發展、實施、控制自主化智慧系統等問題。本報告建議，私部門在開發自主化智慧系統時應該要注意企業社會責任；公部門則應該要增進權力結構的透明度，並且採用適當的規範框架，以公正的分配自主化智慧系統相關的知識和利益。另外，應該建議開發中國家如何培養自主化智慧系統技術，加強投資開發中國家的教育部門，以涵蓋自主化智慧系統的

研究與發展。

a. 勞動力培訓

- 對於低技術之勞動力、待業中之勞動力、受僱之勞動力皆應提供勞動力培訓課程，且對於無法完成培訓之勞動力應擬定因應策略。
- 為求勞動力培訓符合人工智慧時代之需求，研究應包括：受自動化技術影響之職業以及受影響之勞動力人數；對於未來人工智慧產業驅動之工作、職場結構、相關職場習慣、基本技能進行細緻且動態之分析，使未來勞動力市場之供需得以相符；動態分析不同勞動力市場之專業轉型。
- 各種策略之擬定應建立於實證數據，且注重對總體職業之影響結果、收益變動結果。為求創新與勞動力市場之健全發展，應建立人民、公部門、私部門夥伴關係(people-public-private partnerships)之新社會結構，導入結果取向之融資機制，例如社會效益債券。
- 因應次世代之勞動力需求，應於高中教育前即提供相關職能之學習管道，以銜接目前面臨之技術落差與高技術勞動力短缺之瓶頸。

b. 建立對於個人資料權益保障之認知

- 隱私保護設計 (Privacy by Design) 可於研發設計初期協助識別系統與軟體於隱私保護層面所應具備之架構、建議系統落實最佳典範與監管要求，例如資料最小化、問責性、透明性、進場與退場之選擇機制、加密。至於最佳典範，例如以隱私影響評估 (Privacy Impact Assessment) 偵測系統、軟體於研發初期濫用資訊之違法情事。
- 提升公民之數位素養 (digital literacy) 。

- 政府應致力於落實數據蒐集之透明性、數據所有權、數據管理、數據使用及揭露等事項。
- 針對濫用資料、違法使用致生之財產損害，以及對於個資當事人所生之名譽損害應建立該等機構之問責性基礎。該等機構應具有妥適之政策與協議，協議中之條款與條件須與個資當事人進行明確之商討，並明確定義資料濫用與合法使用之要件，以利後續責任之訴追。

c. 於大學及研究所之人工智慧相關教育中融入「具全球維度之工程學」

由於欠缺明確標準，人工智慧領域之相關知識並無法於大學及研究所教育中被明確界定以及教授，故應藉由下述之方式於課程規劃中傳遞相關基礎知識並鼓勵受教者探求各種可能之操作機制。

- 應劃定課程核心能力、建立教學素材資料庫、建構多元教學方式。
- 於大學及研究所教育強調人工智慧技術之應用，其中更應強調工程領域於國際發展、人道救援之應用、將工程學融入勞動力專業技術培訓學程之應用等。
- 基於永續發展與人道目的，應充分認知人工智慧技術應用於中低收入國家所伴隨之機會與風險。

d. 使人工智慧與自動化技術平等可用於全球產業

藉由與適當之組織（如聯合國會員）建立政府、企業、非官方組織之跨領域合作，使該等技術之效益能充分擴及於全球乃至於未開發國家。具體作法如下：

- 組織成員協力探討如何落實人工智慧之教育與技職訓練。
- 促進人工智慧全球應用之標準化及一致性，建構開放平台分享人工智慧之軟體。

- 提倡分享基於最新人工智慧技術所生之相關知識與獲利，例如以傳統之金融機制，包括稅賦、捐款等，讓人工智慧技術之利益平等造福全體社會。
- 跨國機構、政府、大學及研究機構應戮力於研發開發中國家易於取用之人工智慧技術，例如，善用高普及率之行動電話研發可攜式輕量人工智慧裝置、建構文化認知系統（culture-aware systems）。
- 政府、國際發展合作組織以及非官方組織應注意在人類永續發展中，人工智慧之潛在角色。

## (9) 法律

### a. 應授與人工智慧技術何等法律地位（或其他法律分析框架）？

- 儘管授與人工智慧法人格可能帶來相應之經濟效益，惟該等技術發展尚未達到於法律上或倫理上授與其法人格之必要階段，因此，現階段而言，人工智慧仍應定性為財產法下之規範客體。
- 政府與產業界應確保部分決定與操作不應委由人工智慧行使，且應採用相關規範與標準以確保對於該等決定已踐行有效之人為控制。現行法已對於類似人工智慧之情形界定有相關之法律地位，例如，針對寵物、家畜、野生動物、受雇人與其他自然人或法人之代理人。政府與法院應參酌該等法律架構，評價人工智慧應用之法律權利與責任。
- 應省視現行法，特別係對於商業組織之相關規範，若該等規範之解釋可能推導出將法律自主權益授與人工智慧之適用結果，則應針對該等疑義與漏洞予以修正，確保現行法並無授與人工智慧法人格。
- 隨著人工智慧迅速發展，政府應反覆檢視其法律定性、所受之法律保障、權利與責任是否與實際運作相符，且應與管制者、公民

團體、產業界及其他利害關係人協力研議相關制度之修訂。

b. 確保公部門使用之人工智慧技術並未侵害公民權利

- 特定類型之決策不得委由人工智慧進行，諸如：動用致命武力之決策。應制定規範確保有效之人為控制與決策機制。
- 於進行相關決策或風險評估時，不應以人工智慧技術認事用法，蓋因人工智慧對於數據分析之能力無法全然取代人為決策之地位，其數據分析固然可作為評估因素之一，惟不得作為決策過程之唯一依據。
- 人工智慧技術研發之首要目標係確保其運作機制之透明性與問責性。應盡可能確保監管者得以獲悉系統使用之邏輯與演算機制，若無法獲悉，則應提出相應之替代方案以符透明性要件。且該等系統應接受風險評估與嚴格測試。
- 應舉辦公民論壇讓公眾提出人工智慧不宜使用之案例。
- 尚未進行正式或非正式之規則制訂程序，即不應將該等政策委由自動化系統運作。
- 自動化系統應進行審計追蹤（audit trails）以記錄支持該等決策之事實與法律，且第三方驗證者應可修正該系統以確保其追蹤紀錄如實反映系統之決策過程。人工智慧系統提供者或決策服務提供者對於該系統之測量、品質保證與所驗證之效用，應提供數據統計之合理評估協定（statistically sound evaluation protocol）。
- 法律應明定公部門使用人工智慧系統之揭露義務，即須公布該系統之投資者、研發者與行銷者名單、系統選擇相關數據之過程，且應公開系統研發者之倫理價值，以及該等價值如何設計於該系統中。

c. 確保人工智慧系統之法律問責性

- 研發者應考慮採用身分識別標籤制度，讓人工智慧系統皆附有身分識別標籤，以確保明確可追溯之法律問責性。
- 立法與執法者應確保人工智慧技術未受到企業或任何事業體之濫用，藉此規避可能之責任。為確保受害者得以受償，應導入保險理賠或其他資力擔保機制。
- 使用人工智慧系統之企業就如何使用、使用之先決條件、有權操作者、操作者之前置培訓、人工智慧運用成效之評估、可預期之使用效益等應明定相關之使用方針，以釐清使用者與受益人對於該等技術之認知並使後續之究責更為明確。
- 由於人工智慧系統之運作過程涉及多項人為因子，故不應僅將「啟動人工智慧系統者」視為責任主體，製造商、管理者、監督者、操作者等皆可能成為責任主體。
- 應明定使用或製造人工智慧系統之企業對於該等系統之盡職調查義務、維護演算法正常運作之義務，且不得以契約免除該等義務。
- 藉由雙邊或多邊協議，建立國際法制對於人工智慧責任相關規範之一致性，並力促跨國爭端解決機制之建構。
- 於商品責任訴訟中，對於有瑕疵之商品提供修補之廠商，並不會遭致法院於訴訟中做成不利認定，亦不等同於廠商自認其責任。於人工智慧產業之相關商品亦應比照適用，鼓勵廠商修補有瑕疵之人工智慧商品以免損害在未來繼續發生或擴大。

d. 增進自動化人工智慧系統之問責性及可驗證性

- 現階段礙於技術之侷限，無法完整確立對於該等系統之問責性與可驗證性。作為替代機制，可強化該等商品之揭露，例如，以經政府核准之標籤揭露有使用人工智慧技術之商品，使消費者相應調整使用之行為以適度降低風險。

- 研發者與製造者仍須就該系統之風險與外部性負責，揭露制度不得作為免責事由。
- 縱使演算機制透明化之要求有其技術障礙，人工智慧系統之研發仍應致力於呈現其得出結論之演算過程、表明所運用之假設、盡可能揭露不明確部分之資訊來源。
- 於人為決策介入之特定高風險情形，人工智慧系統須主動告知使用者相關運算之不確定性。
- 對於涉及經濟或具體人身傷害之重大潛在風險，研發者應充分且明確地警告使用者該等風險。若係無法事前充分警告之風險，研發者即應自始避免該等風險存在於系統中。
- 因應人工智慧系統風險之未知性，應建立吹哨者制度以及相關吹哨者保護機制。由內部人舉發及早遏制損害之發生。
- 政府與產業團體應考慮建立標準規範，要求詳實記載（或採取其他可得驗證其演算過程之方式）人工智慧系統之重要操作過程，並將該等紀錄保存一定期間。人工智慧監督系統或量化輸入影響（Quantitative Input Influence）方法之運用，皆可協助研發者克服人工智慧系統之可驗證性障礙。
- 歐洲強調對於演算結果應賦予受影響之個人得行使「解釋權」，該項認定將大幅提升人工智慧系統之透明性及問責性。此外，亦應研發對於演算法之倫理審計（ethical audit）或認證制度。
- 使用者可透過互動式培訓計畫，預先知悉使用該系統之不確定性、風險、及可能致生危害之情形，避免在未受告知之情形下就系統演算之結果承擔使用者責任。
- 立法者應審慎評估為人工智慧訂立新規範之必要性，規範內容包括：新興人工智慧技術市場化之前階段測試須受有國家或國際機構之認證；企業應樹立對於人工智慧之倫理聲明，承諾就數據分



析不得衍生歧視結果。

- 若關於政治人物或政治議題之報導或新聞播報涉及人工智慧技術之運用，即須告知公眾該等事實。

### III. 美國

#### 1. Big Data: A Tool for Inclusion or Exclusion<sup>545</sup>

隨著網際網路與雲端技術應用的快速發展，近年來企業及各國政府都看中大數據可提供的價值，相繼提出以大數據為主的商業模式與政策規劃。美國聯邦交易委員會（Federal Trade Commission，簡稱 FTC）便在 2016 年 1 月 6 日公布一份有關大數據的研究報告，指出大數據愈趨重要，將增進消費者在眾多領域的福祉；然而，接下來必須面對的重要議題是，企業應確保在運用大數據分析時符合法律，並在保護消費者權益的價值與原則下，持續提供消費者益處及機會，將可能產生的風險極小化，避免造成歧視。

其中，可能適用於大數據業務的法律如下：

##### (1) 公平合理信用報告法

公平合理信用報告法（Fair Credit Reporting Act，簡稱 FCRA）係針對消費者調查機構（consumer reporting agency，簡稱 CRA）訂定，這些機構匯編並出售包含消費者資訊的報告，此類資訊被用來判定消費者在信用、就業、保險、住房或其他類似方面是否享有特定福利，是否能夠進行交易。

消費者調查機構必須執行合理程序，在最大範圍內確保消費者報告的準確性，並且必須為消費者提供聯絡管道，以便消費者能改正任何錯誤。

最後，只有具體事實的分析才能判定某種做法是否遵守或違反 FCRA，因此公司使用大數據分析決定 FCRA 所規定的資格時，應當注意此一法律的規定。

---

<sup>545</sup> Federal Trade Commission (2016). *Big Data: A Tool for Inclusion or Exclusion?*. Retrieved from <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>

## (2) 公平就業法

公司還應當考量一系列的聯邦公平就業法，包括公平信貸機會法案（Equal Credit Opportunity Act，簡稱 ECOA）、1964 年民權法案（Civil Rights Act of 1964）第七編、美國身心障礙法案（Americans with Disabilities Act）、就業年齡歧視法案（Age Discrimination in Employment Act）、公平住房法案（Fair Housing Act）和反基因歧視法（Genetic Information Nondiscrimination Act）。

這些法律禁止各種歧視，例如種族、膚色、性傾向或性別、宗教、年齡、身心障礙狀況、國籍、婚姻狀態及基因資訊等。為了證明對方違反上述法律，原告必須證明有「差別對待」或「差別影響」的情況。然而，是否違法仍須視具體個案加以審查判斷，故當公司的行為可能導致差別待遇或差別影響時，公司應當謹慎為之。

## (3) 聯邦交易委員會法案

該報告還討論了聯邦交易委員會法案（Federal Trade Commission Act，簡稱 FTC Act）第 5 節對大數據分析的適用，該節明文禁止不公正及欺騙性的行為及做法。報告最終認為，參與大數據分析的公司應當考慮，他們是否正在違反對消費者的承諾——如承諾避免與第三方共享數據等。此外，如果公司知悉或可得知悉部分客戶將大數據分析產品用於欺詐或歧視目的，公司便不能將產品出售給他們。針對 FTC Act 的調查應基於具體事實，並在每個案件中實際論證公司是否正以欺詐或不公平的方式提供或使用大數據分析。

最後，本報告則建議公司多思考以下問題，以最大程度增加大數據收益、限制不利影響：

### (1) 你所使用的數據集代表性如何？

公司應當考慮，他們的資料集是否遺漏了有關某些群體的資訊，公司應當採取措施解決代表性不足或過度的問題。例如，如果一家公司服務對象是

使用社交媒體進行交流的消費者，則公司可能會忽略不太瞭解科技的群體。

(2) 你所使用的數據模型考慮偏見因素了嗎？

公司應當考慮在大數據生命週期的蒐集及分析階段是否存在偏見，並制定策略加以克服。例如，如果一家公司的大數據演算法僅考慮來自「頂尖」院校的申請者，則公司可能對院校錄取的決定存在預先的偏見。

(3) 大數據的預測準確程度如何？

公司應當記住，雖然大數據非常擅長檢測相關性，但它無法解釋哪些內容是有價值的。Google 流感預測趨勢 (Google Flu Trends) 是一個機器演算法，它以 Google 檢索詞作為依據，預測流感病例的數量，這個例子極好地體現了大數據分析的局限性。起初，這個算法似乎準確地預測出流感肆虐的地點，但隨著時間推移，它的預測嚴重失準。這可能是因為演算法未能考慮到某些變量，例如，演算法可能沒有考慮到，假如當地新聞報導了流感爆發的新聞，即便疫情遠隔重洋，人們仍很可能搜尋與流感相關的詞條。

(4) 對大數據的依賴會導致道德或者公平性問題嗎？

公司應當基於公平的考慮，評估分析模型中的因素，平衡模型的預測值。例如，一家公司認為住家離公司較近的員工會比住家較遠的員工在職時間更長。然而，另一家公司考量到不同社區可能有不同的種族構成後，因為擔心造成種族歧視，決定在招聘的演算法中排除這一因素。

該報告並鼓勵公司使用大數據分析增進消費者的利益，為他們創造機會，同時避免落入可能違反消費者保護或平等法規的陷阱，背離了包容、公正的核心價值。

## 2. **Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights**<sup>546</sup>

---

<sup>546</sup> Executive Office of the President (2016). *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil*

隨著大數據、演算法系統的革新，相關技術已逐漸滲透日常生活的各個層面。為了因應科技發展趨勢，歐巴馬政府繼 2014 年及 2015 年發布兩份大數據白皮書後，2016 年 5 月再度發布了大數據相關報告。

在這份報告中，美國白宮特別澄清了「大數據是客觀的」這個錯誤假說，提醒民眾切勿因為過於依賴演算法，而忽略了其所附帶的歧視風險，並歸納出下列造成歧視的兩大原因：

#### (1) 演算法資料來源的問題

決定要使用哪些資料本身，可能就是導致歧視的原因，包括：

- a. 資料選取不良：演算法與系統設計者在選擇重要的資料時，其判斷難免會有個人的人為影響或思慮未周，因而導致最終產出結果具有歧視、排除的效應。
- b. 不完整、不正確或過時的資料。
- c. 選擇時的偏頗：所選取的資料並不能代表全部的母數，卻據此推斷整體的情況。
- d. 不經意地延續及促成既存的偏見。

以上議題是在設計系統藉以提供服務時必須考量的問題，尤其是透明、問責與正當程序的重要性，如此才能確保演算法的資料來源是正確且適當的。

#### (2) 演算法內部運作的問題

演算法與系統就像黑盒子一樣，消費者或受其影響的當事人往往無從得知作成決定的理由為何，也就欠缺找出錯誤或偏頗並予以更正的能力，這意味著某一群人將有可能完全被排除在特定機會之外，並造成難以察覺但又逐漸擴散的缺漏，例如：

- a. 設計不佳的媒合系統。
- b. 個人化的推薦服務反而限縮了用戶的選項。
- c. 決策系統假定經常同時出現的因素間具有因果關係並導致歧視。
- d. 資料集不足以代表特定人口或欠缺其資訊

為了貫徹「預設公平機會設計」(equal opportunity by design)的原則，必須再次強調透明、問責與正當程序的重要性，程式開發者及資料科學家更必須利用「減少偏頗」(bias mitigation)的方法來降低大數據處理上的偏頗。

該報告接著從貸款、僱傭、高等教育及刑事司法四個領域切入，舉例說明大數據的使用如何擴大對特定個體與群體的潛在「非故意歧視」，並提出可能的解決方案：

#### (1) 信用評價

##### 問題：

對於努力躋身中產階級的人民，財務借貸能力是很重要的一環，而信用評價則是最重要的指標之一。信用評價的判斷取決於過往借貸的清償紀錄，因此，這時候資料紀錄便有其重要性。

然而，美國消費者金融保護局的報告顯示，將近 11%的民眾是無信用紀錄的，此一情形與收入具有相當的關係。在低收入戶中，有高達 30%的人是無信用紀錄的，而剩下的人當中，則有 15%係屬無法評價的信用等級。非但如此，數據顯示種族間的不平等，也是另一個嚴重的課題，相較於白種人，非洲裔及拉丁裔無信用等級的人口幾乎多出一倍。

##### 大數據帶來的利與弊：

大數據可能是解決上述問題的方法之一，基於大數據所設計的新信用評等系統，將替代傳統評等機制並為人民帶來獲得信用貸款的新機會。以電話

及水電費帳單為例，在此變革下，將有超過 70%原本無法評價的信用等級變為可評價，且 64%欠缺信用紀錄的人口將可獲得改善的分數，特別有利於低收入的借款人。

大數據雖能夠增加人民獲得信貸的機會，但未加謹慎使用，亦可能造成歧視的持續存在、甚至加劇。例如，透過大數據，我們可以從個人社交媒體中蒐集資訊，使用社交分析系統來創建新的評等機制，雖然這樣可以增加信貸管道，但也可能擴大既存於社會網路間的不平等。

此外，由於大數據本身變化快速的特性，資料正確性亦有惡化的風險。依據美國聯邦貿易委員會的研究，21%消費者樣本在三份信用報告中至少就有一個錯誤。因此，享受大數據所帶來的好處時，如何保護消費者權利、防止信貸資格歧視便成為重要的課題。

## (2) 求職

### 問題：

自從 1990 年代開始，愈來愈多公司透過求職網站招聘人才，然而，由於招募人員無意識的偏見，往往會選擇與自己具有共同特質的人，非但帶有歧視，亦阻礙多樣性的發展。

### 大數據帶來的利與弊：

與信用評等一樣，數據分析可以幫助人們找到合適的工作，同時有效地避免個人偏見，解決傳統招募過程中常見的隱性或顯性歧視，透過公正的程序找出最合適的人選。然而，大數據系統雖可設計防止偏見的招募機制，卻無法避免原始資料原本即帶有的缺陷，這些歷史偏見將導致某些既有的歧視長期存在，並在大數據科技的包裝下，變得更難以挑戰。

## (3) 高等教育

### 問題：

大學學位對學生未來生涯將造成長遠的影響，相對於高中學歷的人口，擁

有大學學位可以增加 84.54% 的總收入。然而，有關大學升學管道的資訊卻不夠透明，欠缺方便取得的資訊來引導學生作出選擇。

#### 大數據帶來的利與弊：

為了解決上述問題，美國政府已經建立了大學記分卡制度，藉此提供大學績效的相關資訊，內容包括大學畢業後的出路、大學校友的收入及學貸還款的統計數據等等，幫助學生及其家庭瞭解讀大學的成本及價值。除了大學記分卡外，高等教育機構另外創建了一個大數據系統，學校可使用所蒐集的資料追蹤學生的學習進度，並利用現有數據打造量身訂作的學習體驗。這些技術讓學生能夠更有效地學習，並有助於克服教育體系上既存的不平等，為弱勢的一方提供幫助。

大數據雖可協助高中生選擇合適的大學，但在資料使用上，仍難免有導致歧視的可能。例如，作成錄取決定時，高等教育機構可能會使用大數據技術來預測申請者順利畢業的可能性，此舉將造成來自低收入家庭的學生可能會無法被錄取，因而造成歧視，這在學校急於削減成本時，情況將會更為惡化、嚴重。

#### (4) 刑事司法

##### 問題：

近來執法機構愈來愈常利用數據分析及演算法系統來執行勤務，但使用這些技術協助執法時，應充分考量其對社區安全與信任可能帶來的影響。

##### 大數據帶來的利與弊：

大數據及演算法可以幫助執法變得更加透明、有效。長久以來，執法機構便一直試圖瞭解犯罪活動的模式，俾以更為有效地分配資源，而新技術正在取代原有的人工技術，許多警察部門利用複雜的演算法增進對犯罪熱點的理解，並將犯罪數據與氣溫、時間、與其他建築物或設施的遠近、其他變數串連起來，俾以更為有效地打擊犯罪。系統透過去識別化的數據及當地犯罪及人口統計等背景資料，可利用行為模式預測未來具有高度風險的

事故。此外，某些被稱為「預測性警政」(predictive policing)的最新分析模型技術，甚至能夠相當準確地預測可能發生犯罪活動的地點及時間，提早防止犯罪的發生。

在使用資料分析來創建及執行預測性工具時，必須努力確保演算法不以種族、宗教、收入水平、教育或其他可能造成歧視的資料為其依據。此外，同樣必須注意的是，刑事司法資料是出了名的不準確，這是因為主要的資料庫——聯邦調查局的制式犯罪報告(Uniform Crime Report)亟需現代化，經常無法取得足夠且完整的資料進行深度分析，即便犯罪報告獲得改善，基於許多原因，取用任何犯罪資料集時，仍必須謹慎小心，大多數刑事司法資料來源本質上就是主觀的，因為官員作成執法決策時使用了裁量權。

該報告最後歸納了五大方向的建議：

- (1) 支持減少演算法歧視的相關研究，建立系統性的公平與問責，並發展資料倫理框架。
- (2) 鼓勵企業與消費者團體設計出最佳的演算法系統，藉此修正不正確的資料，並挑戰演算法所作出的決定。
- (3) 促進學術研究與產業對於演算法的外部稽核與測試系統，藉此確保人民受到公正的對待。
- (4) 擴大電腦與資料科學的參與，提高美國民眾相關基礎能力與影響力。
- (5) 考量公私部門在設定資料使用規則上所扮演的角色。

### **3. The National Artificial Intelligence Research and Development Strategic Plan<sup>547</sup>**

2016年5月，白宮科技辦公室(Office of Science and Technology Policy)宣布將成立新的跨部門組織來探討人工智慧的利益和風險。同年6月，美國國家科

---

<sup>547</sup> National Science and Technology Council (2016). *The National Artificial Intelligence Research and Development Strategic Plan*. Retrieved from [https://www.nitrd.gov/PUBS/national\\_ai\\_rd\\_strategic\\_plan.pdf](https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf)



技委員會（National Science and Technology Council，簡稱 NSTC）機器學習與人工智慧分會（Subcommittee on Machine Learning and Artificial Intelligence）成立，負責協助聯邦政府有關人工智慧的活動，並由 NSTC 所屬網路及資訊科技研發計畫（Networking and Information Technology Research and Development）作成此份計畫書，於 2016 年 10 月發布，本計畫明確指出優先的研發重點，以便將政府資源投入產業不太可能投資的領域，解決研發人員的需求。

此份計畫書有數個假設：（一）因政府及產業的研發投資，使得人工智慧的技術持續發展；（二）人工智慧對社會——包括就業、教育、公共安全、國家安全——以及對美國經濟的影響持續增長；（三）由於近期商業成就及研發投資預期回報增加，使得產業投資持續增長；（四）受制於典型公共財投資不足，部分重要研究領域不太可能獲得產業的足夠投資；（五）對人工智慧的需求將在產業、學界及政府內部持續增加，進而對公部門與私部門造成勞動力的壓力。

本計畫不只是著眼於短期人工智慧所具備的能力，更放眼於人工智慧對社會及世界長期帶來的變革性影響。因為許多應用領域及長期研究在短期內較無利益可圖，不太可能完全由產業進行，故聯邦政府是長期高風險研究計畫及其近期發展工作的主要資金來源，以便實現部門或機構的具體要求，並解決民營企業不欲處理的重要社會問題。因此，聯邦應著重於具有重要性的社會領域進行人工智慧投資——例如公共衛生、城市系統與智慧社區、社會福利、刑事司法——而非針對消費市場領域，加速人工智慧知識及技術生成的長期研究。由聯邦政府協調研究工作，亦可為政策制定者提供解決及使用人工智慧面對複雜政策挑戰所需要的知識。

本計畫定義了一個上位框架，用來辨識人工智慧科學與技術間的差距，並追蹤旨在填補此一差距的聯邦研發投資。然而，本報告並未針對個別聯邦機構制定具體的研究進程，反而為行政部門設定目標，使得各機構能根據其任務、能力、權限及預算來決定優先順序。本計畫亦未制定人工智慧的研究或使用政策，未針對就業及經濟的潛在影響進行更廣泛的探討，而是側重在透過研發投資定義及促進相關政策，俾以確保使用人工智慧的責任、安全及益處。

人工智慧潛在利益包括：

### 促進經濟發展

新產品及服務能夠創造新的市場，改善既有商品及服務的品質及效率。透過專家決策系統，能夠創造更有效率的物流及供應鏈。藉由以機器視覺為基礎的駕駛輔助及自動/機器人系統，能夠更有效率地運送產品。製造業亦可透過新的方法控制製造工序及編排工作流程。

### 改善教育機會及生活品質

藉由虛擬助教開發客製化的學習計畫，挑戰及符合個人興趣、能力、教育需求，促進終身學習。透過量身打造的個人化健康資訊，人們可以活得更健康、積極。智慧家庭及個人虛擬助理能夠為人們節省時間，避免將時間花在日常的重複性工作。

### 增進國家及國土安全

機器學習代理人可處理大量資料，從敵人身上辨識出相關的生物特徵，為易遭受攻擊的關鍵基礎設施及主要經濟部門提供保護。這些數位防衛系統可降低戰場上的風險與傷亡。

本計畫著重在產業無法獲益的領域：

#### 策略一：對 AI 研究進行長期投資

對具有潛在長期（5 至 10 年或以上）回報的 AI 研究進行投資是必要的，包括透過新的基礎工具及技術瞭解資料及發現知識、增進 AI 系統的感知能力、瞭解 AI 在理論上的能力與限制、投入通用型人工智慧研究、發展可擴增的 AI 系統、促進類人的 AI 研究、發展能力更為強大且可靠的機器人、為改良 AI 提升硬體、為硬體改良創造 AI 等。

#### 策略二：發展有效的人機協作方法

在部分領域中，透過人機協作可得到更好的效果，其未來應用將視人類與

AI 系統的功能性角色區分、人類與 AI 系統的互動特性、人類與其他 AI 系統進行協作的數量、人類及 AI 系統如何溝通及分享情境感知等而有所不同，包括由 AI 輔助人類、由 AI 分擔高度認知負載及由 AI 取代人類。為了讓人類與 AI 系統達成有效互動，需要額外的研發，才能確保系統設計不會太過複雜、信任不足或過度自滿，所面臨的挑戰包括尋求符合人類感知 AI 的新演算法、發展增強人類能力的 AI 技術、開發更有效率的語言處理系統等。

### **策略三：瞭解並處理 AI 在倫理、法律及社會上的影響**

當 AI 代理人能夠自主行動，我們希望它們能夠依照人類正式及非正式的規範行事，此一領域的研究有賴於電腦科學、社會及行為科學、倫理學、生物醫藥科學、心理學、經濟學、法律及政策研究專家的多學科視角，從設計上著手改善公平性、透明度及問責性、打造符合倫理的 AI 並設計其論理框架。

### **策略四：確保 AI 系統的安全性與可靠性**

AI 系統必須面對複雜且不確定的環境、緊急行為、目標偏差及人機交互等重要挑戰，因而必須投入額外的投資，增進 AI 系統的安全性及可靠性，包括改善其可解釋性與透明度、建立信任、增進可驗證性及有效性、防禦攻擊、達致安全及價值的長期校準。

### **策略五：為 AI 訓練與測試開發公眾共享的資料及與環境**

訓練資料集與其他資源的多樣性、深度、品質、正確性將顯著影響 AI 的效能，因而為各式各樣的 AI 應用發展高品質的資料集與環境是有必要的，包括為南轅北轍的 AI 利益及應用發展並開放各式各樣的資料集、使得訓練及測試資源能夠回應商業應用與公共利益、開發開源軟體庫及工具組等。

### **策略六：透過標準及基準測量與評估 AI 技術**

標準、基準、測試平台及 AI 社群如何應用它們，對於引導及促進 AI 技術的研發相當重要，必須發展各式各樣的 AI 標準（如軟體工程、性能、指標、安全性、可用性、互通性、可靠性、隱私、可追溯性及特定領域的定理）、

建立 AI 技術基準（如準確性、複雜性、信任與能力、風險與不確定性、可解釋性、非預期偏差、與人類表現的比較、經濟影響）、增加 AI 測試平台的可近用性、委託 AI 社群發展標準及基準等。

### **策略七：增進對國家 AI 研發勞動力需求的瞭解**

為了推進 AI 研發的發展需要足夠的 AI 研發人才，然而目前並無正式的 AI 勞動力資料，因而需要額外的研究，俾以增進對國家目前及未來 AI 研究勞動力需求的瞭解。

本計畫最後提供了兩個建議措施：

- (1) 開發人工智慧研發實行框架，把握科技機會並支持 AI 研發投資的有效協調，此與本計畫的策略一至策略六相符。
- (2) 對國家打造及維持健康的 AI 研發勞動力的願景進行研究，此與本計畫的策略七相符。

## **4. Preparing for the Future of Artificial Intelligence<sup>548</sup>**

2016 年 5 月，白宮科技辦公室宣布將成立新的跨部門組織來探討人工智慧的利益和風險，並於 5 月至 7 月舉辦四個系列研討會。2016 年 6 月，NSTC 機器學習與人工智慧分會成立，此份報告即為研討會成果的一部分，同年 10 月，由白宮科技辦公室發布本報告。

人工智慧可以廣泛運用在各個面向，無論是從政府或民間投資，皆可以看到人工智慧應用在健康管理、交通、環境、犯罪正義、經濟上的好處，使任務完成更迅速、確實、有效率。本報告也提出一些現況及相應的建議。

### **(1) 人工智慧與公共財**

協助解決困難與降低效率低落的問題，如在醫學中心，藉由人工智慧提高

---

<sup>548</sup> Executive Office of the President (2016). *Preparing for the Future of Artificial Intelligence*. Retrieved from [https://obamawhitehouse.archives.gov/sites/default/files/whitehouse\\_files/microsites/ostp/NSTC/preparing\\_for\\_the\\_future\\_of\\_ai.pdf](https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf)

對於醫療併發症的預測，改善嚴重戰爭創傷的治療方法，並對癌症研究等健康數據進行預測分析產生重要作用。在交通方面，減少等待時間、能源消耗和 25% 的廢氣排放及路線規劃等。利用圖像分類軟體對社群網站上的照片進行分析，辨識單隻動物，再利用照片的數據及位置標記，建立資料庫，以更好地追蹤動物遷徙活動。在刑事司法方面，探討人工智慧如何協助犯罪報告、警務工作、保釋、量刑及假釋決定，以提供數據顯現刑事司法中的判刑過程，甚至研究如何藉此解決各種社會問題，如利用數據科學與人工智慧探討解決失業與輟學的社會問題的方法；如何以計算機博弈理論、機器學習、自動規劃等解決無家可歸的問題；如何利用機器學習解決全球貧困的問題等。

**建議措施 1**：鼓勵私人與公共機構進行自我審視，判斷如何透過人工智慧、機器學習等技術來為社會造福。

**建議措施 2**：聯邦機構應優先考慮人工智慧的開放式培訓數據及其數據標準。

## (2) 人工智慧與聯邦政府

聯邦政府正在研究相關政策和內部實踐，可能包括以下內容：

(1)對基礎和應用研發項目進行投資；(2)成為人工智慧技術和其應用的早期客戶；(3)支持試點項目，根據真實情況搭建測試平台；(4)向公眾提供資料集；(5)提供贊助支持；(6)為人工智慧樹立具有可行性的遠大目標；(7)為人工智慧應用的嚴格評估提供經費，考察影響及成本效益；(8)為創新的發展提供政策、法律和監管環境。

**建議措施 3**：聯邦政府應探索新方法，提高關鍵機構應用人工智慧能完成任務的能力。

**建議措施 4**：NSTC 機器學習與人工智慧分會應為政府部門內人工智慧實踐者提供實踐的社群。

## (3) 人工智慧與規定

在應用人工智慧於各產品時，應確保符合相關規定，評估可能減少的風險及可能增添的風險。檢驗風險是否在現有管理制度範圍內，現有規範是否有需修正之處等，並在進行管理提升成本與降低創新兩者間取得平衡，同時保障市場公平與公共安全。目前相關機構也面臨如何更新法律規範以管理人工智慧的新產品，如美國國家公路交通安全局（National Highway Traffic Safety Administration，簡稱 NHTSA）對自動駕駛車輛的管理及美國聯邦航空管理局（Federal Aviation Administration，簡稱 FAA）對無人機制定的相關規定。

FAA 制訂安全準則來確保空域和道路的安全，並在 2016 年 8 頒布第 107 條最後一項關於小型無人機的規定等，而在地面交通的政策也於 2016 年 9 月發布。

**建議措施 5**：在制定以人工智慧為驅動的產品政策時，相關機構應聘用適當的高級技術專家。

**建議措施 6**：機構應充分利用任命人員與交流模式（聘僱權威人士），以培養聯邦機構的員工，能從多方角度了解當前技術發展狀況。

**建議措施 7**：交通部應該與產業界和研究人員合作，加強用於安全、研究和其他目的的數據共享。

**建議措施 8**：美國政府應投資、開發及應用高端的自動空中交通管理系統，也能同時適用於無人機及有駕駛的飛行器。

**建議措施 9**：NHTSA 應繼續致力於建立完善的制度框架，確保並整合全自動駕駛車輛和無人機的安全，包含將新型車輛設計融入公共交通系統。

#### (4) 研究和勞動

政府應為人工智慧技術研發者制定相關的政策。研究者也針對政府應如何促進人工智慧領域發展給出三個答案：(1)使單一系統能夠執行結構更簡單、內容更廣泛的任務，如掃地機器人能完成整套家庭日常清潔工作；(2)將不同風格的人工智慧程式統一。因為目前人工智慧仰賴各自獨立程式與指令

以完成相應的特定任務。通用人工智慧必然要將這些獨立程式深度整合，以一個可以處理廣泛應用指令的程式取代多個程序；(3)通用人工智慧的關鍵在於解決技術中面臨的大挑戰，如遷移學習可使一個具備將英文翻成西班牙文能力的模型，「遷移」至類似的任務中，例如將中文翻成法文或用俄文寫詩等，這樣全新的任務學習就會較快。

雖然在科學領域投入資金可以帶來二至三倍的經濟成長，是值得投資的淨收益，然目前因短期內難以收到投資回報，基礎研究方面資金仍嫌不足。此外，政府也應訓練相關人員具有跨科學素質，如計算機科學、統計學、數理邏輯、資訊理論等，並促進人工智慧、數據科學及教育系統整合，在各教育機構設立和發展相關項目。

**建議措施 10**：NSTC 機器學習與人工智慧分會應監控人工智慧技術的發展，並定期向上級主管部門匯報人工智慧的發展狀況，尤其是關於其發展技術的突破。

**建議措施 11**：政府應監控其他國家的人工智慧發展狀況，尤其是人工智慧技術里程碑的突破。

**建議措施 12**：人工智慧相關行業應和政府合作，即時向政府報告產業最新發展動態，包括近期可能在技術上的重大突破。

**建議措施 13**：聯邦政府應優先發展人工智慧基礎和長期的研究項目。

**建議措施 14**：NSTC 內部各分會應聯合展開人工智慧勞動力管道研究，以制訂並確保有適當增加具規模的行動，促進相關研究人員、專家、用戶在數量、質量和勞動力的多樣性成長。

- (5) 短期人工智慧的經濟效益就是將過去無法自動化的任務自動化，使生產力提高，並貢獻國民生產總值。但自動化也對某些類型的工作、產業產生潛在的影響，導至收入不平等、職業被取代等，此時便需政策干預使人工智慧的經濟效能可以共享而非切割。

**建議措施 15**：總統辦公室應在年底前出版一份後續報告，進一步研究人工

智慧和自動化對美國就業市場的影響，並提出相對應的政策摘要。

#### (6) 公平、安全和治理

使用人工智慧能為人類作出重要決定，取代本身和相關機構的決定權，並引發如何確保公平、公正和責任的關注。業者應盡力防止故意歧視或破壞，確保不會發生意外。同時要考慮如何將實驗室的封閉世界安全地轉換至開放世界，因為開放世界的不可預測性，系統可能會遇到其設計和建立時沒有考慮到的情形。因人工智慧實踐上，某些方面並無完整理論支持，如何聯繫現實世界與安全工程領域，仰賴從業者的直覺與實驗，限制技術的應用。現今的實踐從直覺、動手做的精神步入經驗法則，再發展至有更完整理論體系及更加專業化的產品。

**建議措施 16:** 使用人工智慧系統進行決策或為相關決策提供支持的聯邦機構在決定個人事務時，應當特別注意確保這些系統的有效性及公平性，並以證據為基礎進行驗證和確認。

**建議措施 17:** 資助各州及地方政府使用人工智慧系統對個人作成決策的聯邦機構，應當對資金的使用條件進行審核，確保使用聯邦資金購買的、以人工智慧為基礎的產品或服務，能夠產生足夠透明的結果，並以證據確保其有效性及公平性。

**建議措施 18:** 學校及大學應該將道德、可靠性、隱私及安全等主題作為人工智慧、機器學習、計算機科學及數據科學課程的一部分。

**建議措施 19:** 人工智慧專家、安全專家及其所屬的專業團體應一同努力將人工智慧推向更為成熟的 AI 安全工程領域。

#### (7) 全球考量與安全問題

除一般公平與安全問題，人工智慧對國際關係、網路安全、國防也構成政策問題。人工智慧的突破是數個國家合作研究的直接或間接成果，需共同努力發現合作機會、制定國際框架、促進研發。國際參與對探索人工智慧在衛生保健、製造業自動化及訊息技術的應用必不可少，亦可處理全球問



題，如災害預防、氣候變化、野生動物非法交易、就業及智慧城市等。美國政府也致力與其他國家（日本、韓國、德國等）進行雙邊討論，致力與工業及相關標準化組織合作，促進國際標準朝產業主導、自願參與及尋求共識的方向發展，並以透明、開放和市場需求原則為基礎。美國取徑被正式納入法律（NTTAA, PL104-113）及政策（OMB Circular A-119），並在美國標準策略中重申。

**建議措施 20：**美國政府應在涉及國際參與的人工智慧上制定政府層面的政策，並制作需要國際參與和監督的人工智慧領域清單。

**建議措施 21：**美國政府應該加深與關鍵國際利益相關者的合作，包括外國政府、國際組織、業界、學術界等，以及交流人工智慧研發方面的訊息並促進合作。

#### (8) 人工智慧及網路安全

專業自動化可使系統和應用以明顯更低的成本實現較強安全性，並增加網路防禦的靈活性，幫助處理網路空間的複雜性，執行預測分析，藉由大量不規則、不完整的數據資料來制定動態模型，有效為人類決策提供支持以應付網路攻擊。人工智慧本身也有網路安全需求，應執行穩定安全控制，以確保數據和功能的完整性，保護隱私機密及可用性。網路安全發展對於解決應對惡意網路活動時的安全性和恢復力至關重要，特是在政府和私部門業務使用狹義人工智慧的規模和類型不斷增加的情形下。

**建議措施 22：**機構的計畫和戰略應考慮到人工智慧和網路安全之間的相互影響。參與人工智慧問題的機構應該向美國政府和私部門網路安全部門確保，人工智慧系統和私部門人工智慧部門制定創新的方法應用人工智慧，以實現有效和高效的網路安全。

#### (9) 武器系統中的人工智慧

美國持續將自動化引進武器系統，透過技術改進使武器系統更精確、更安全、更人道，並減少武器使用和附帶損害，同時遙控航空器可以使軍事人

員和危險距離更大，確保所有武器系統使用符合國際人道主義法。美國反對將無人機納入自主武器系統，認為根據定義無人機與載人機皆需直接由人類控制，且所有武器系統，無論自動或非自動皆須堅持國際人道主義。

**建議措施 23:**美國政府應該在符合國際人道主義法的基礎上制定關於自動和半自動武器的統一政府政策。

藉由產業、社會大眾、政府的共同努力，人工智慧可成為經濟增長和社會進步的主要驅動力。政府可召集各方就重要問題進行交流，幫助制定公開辯論的日期；對技術開發應用的安全性和公平性進行監督，制定規章制度以保護大眾、鼓勵創新；支持基礎性研究，將人工智慧應用至社會福利；培養從業者的多樣化技能。而從業者也要確保人工智慧能為基礎系統達到有效管理，確保公開、透明、容易理解，且它們的應用不會與人類的價值觀和理想背道而馳。開發與研究機器會幫助我們更好理解和鑑別人類智慧，縝密地使用人工智慧提高我們的智慧水平，使我們規劃出一條更美好、更光明的道路。

## 5. Artificial Intelligence, Automation, and the Economy<sup>549</sup>

美國白宮於 2016 年 12 月發布本篇報告，於本篇報告中揭露人工智慧所引發之自動化對於美國經濟之正負面影響，並提供三項策略建議試圖擴大人工智慧所帶來之益處以及減少人工智慧產生之成本。本篇報告之製作成員包含白宮經濟顧問委員會（CEA）、國內政策委員會（DPC）、國家經濟委員會（NEC）、行政管理與預算辦公室（OMB）以及科學與技術政策辦公室（OSTP）。本篇報告延續美國白宮於 2016 年 10 月發布之 Preparing for the Future of Artificial Intelligence，並展現美國政府對於人工智慧之態度。

### 人工智慧驅動之自動化對於經濟之影響

人工智慧驅動之自動化所帶來經濟上影響之方式和速度，目前尚無法確定。人工智慧也許不會對經濟帶來大規模的新影響，但也有可能使經濟遭受前所未有的

---

<sup>549</sup> Executive Office of the President (2016). *Artificial Intelligence, Automation, and the Economy*. Retrieved from <https://www.whitehouse.gov/sites/whitehouse.gov/files/images/EMBARGOED%20AI%20Economy%20Report.pdf>

的衝擊，並急遽改變整體勞動市場，勞工可能因其工作技能無法滿足新型態就業市場而遭致失業。且目前也難以預測人工智慧驅使之自動化所帶來之影響最大範圍為何。基此，政策制定者應就整個經濟體系進行規劃。人工智慧驅動之自動化是否在未來顛覆現行之經濟體系，雖然目前很難準確地預測其影響力，但本篇報告提出，政策制定者應為以下五項主要的經濟影響做好準備：

- 總體生產量之提升以及經濟成長
- 就業市場需求之技能轉變，將傾向更高端技術之人才
- 對於不同產業、薪資水平、教育、技術、工作類型以及地理位置所產生之影響，分布不均衡
- 對於勞動力市場產生衝擊，亦即增加新工作需求然而既存之工作需求可能消失
- 對於部分勞動力人口短期失業之時間拉長，需要政府政策來解決

### **策略性建議**

#### (1) 投資並開發人工智慧，以期帶來更多益處

- 政府應在人工智慧之發展以及研發扮演重要角色，以增強人工智慧可能帶來之益處。
- 人工智慧可以發展之領域包含網路防禦和詐欺交易以及詐欺資訊的檢測。
- 人工智慧之發展也增加對於不同領域、族群、專業背景之需求，透過多樣化之人群促使人工智慧之成長並可解決源於演算法偏差造成之問題。
- 鼓勵市場競爭，以期為科技與市場帶來創新發展。

#### (2) 為美國人提供未來工作所需之教育及訓練

- 強化兒童之早期教育，尤其是貧困家庭之兒童，以期在未來教育過程中不會落後於同儕。
- 培育中學生在學期間之技能並提升高等教育水平，以免在未來出社會時遭人工智慧取代。
- 政府應透過立法來保障勞工在進入就業市場後仍能有機會受到在職訓練。

(3) 為處於轉型中之勞工提供幫助並確保勞工人能共同成長

a. 強化社會安全網機制：

- 自動化所引發的失業性問題可能是人工智慧帶來最嚴重的影響。失業保險制度將有效降低其家庭所受之影響。且由於勞工之失業期間無法預測，因此，應延長失業保險之期限。
- 強化勞工在市場上之競爭力、薪資以及與資方談判能力以因應人工智慧對於勞工帶來之衝擊。
- 政府應為勞工提供轉職輔導。

b. 人工智慧驅動的自動化可能因為當地政策、資本與勞動因素等在不同的區域發展速度不同。為減少因地域影響造成的不公平，政府應設法減少地域限制和尋求因地制宜之解決方式。

c. 現代化之稅賦政策，例如：執行進步之稅賦政策以及強化稅賦信用機制，驅使人民積極納稅。

## 6. Artificial Intelligence: Emerging Opportunities, Challenges, and Implications for Policy and Research<sup>550</sup>

(1) 報告作成背景

<sup>550</sup> GAO (2018). *Artificial Intelligence: Emerging Opportunities, Challenges, and Implications for Policy and Research*. Retrieved from <https://www.gao.gov/assets/700/692793.pdf>

鑑於人工智慧同時具有對於改善人類生活、提高經濟競爭力、解決社會問題之發展前景，以及造成勞動力取代、加深社會經濟不公平之潛在風險，美國政府問責署（United States Government Accountability Office，下稱「GAO」<sup>551</sup>）審計長（Comptroller General）於2017年7月6日及同年月7日在美國華盛頓特區召開一場關於人工智慧的論壇，邀集產官學界相關人士參加；會後GAO請參與者以及獨立專家審閱論壇會議記錄，並於2018年3月依據論壇內容，發布了本「人工智慧的機遇、挑戰和影響」技術評估報告。

## (2) 人工智慧的演變

報告中提到，人工智慧經過長時間的發展推進，可分為三個不同的階段，分別為：(1)依據特定規則邏輯及固定資訊量的專家系統（expert system），例如：線上報稅系統；(2)透過自然語言處理及統計分析的機器學習（machine learning）系統，例如：臉部辨認技術；及(3)整合前述二階段內容，且具有精密化、抽象性及解釋性處理能力的「可解釋的人工智慧（explainable AI）」，例如：船隻自動駕駛。現階段人工智慧的發展正邁入第三階段，相關研究仍在進行中。

## (3) 人工智慧的效益

報告認為，人工智慧所帶來的益處，包括提高生產效率和經濟效益、協助決策以及察覺複雜與急迫問題：

### a. 提高生產效率和經濟效益

報告中引述論壇與會者意見，認為人工智慧將如同過去的自動化般對生產效率造成大幅改變，且其對於生產效率及經濟效益的改變將迅速且難以預測。報告中舉例一全球性專業服務公司於2016年分析12個已發展經濟體，並預測人工智慧將對勞動生產效率提升40%，且於2035年前該等經濟體的年經濟成長率將倍增。同時，另一投資銀行在2017

---

<sup>551</sup> GAO為美國國會支援機關之一。其前身為美國審計總署（General Accounting Office），於2004年變更組織及名稱，主要職責為協助國會研究及推動聯邦政府的各項計畫與政策法案。

年 1 月預測人工智慧所帶來的收益在 2025 年將達 250 億美元至超過 400 億美元之譜。

b. 協助決策

報告中提到，人工智慧可以由多個來源蒐集大量數據，並以比人類更快的速度檢測異常，有助於協助進行決策並避免不適當或有害的人類偏見，例如人工智慧應用於刑事案件系統，用以評估保釋者是否可能棄保，潛在假釋者的再犯可能。

c. 察覺複雜與急迫問題

部分論壇與會者認為，人工智慧可能有助於人類解決世界上最複雜且急迫的難題。例如：美國的大學研究者利用人工智慧，更有效的透過社群網路的力量傳遞避免人類免疫缺乏病毒（HIV）傳染的相關資訊於無家可歸的青少年間；野生動物保護團體利用人工智慧預測盜獵者施放陷阱的位置，進而保護野生動物安全。與會者更指出，人工智慧亦可應用在老年人生活照護、疾病控制、確保農業永續及食品供給，以及確保金融機構的法規遵循、防制洗錢等。

(4) 人工智慧的挑戰與風險

相較於人工智慧帶來的效益，報告亦指出與會者同樣提出人工智慧面臨的挑戰及風險，包括蒐集和共享數據的障礙、缺乏獲取運算資源以及必要人力資本的途徑、現行法規是否充分、人工智慧所應適用的倫理框架以及對人工智慧的可解釋性（explainability）等問題：

a. 蒐集和共享數據的障礙

報告中指出，部分人工智慧的演算法需要大量的數據（例如機器學習的演算法），若數據蒐集不易勢必成為該人工智慧發展或應用的難題。此外，與會者提到幾種共享數據的風險：擁有大量數據的企業，可能會為了維持自身競爭力而有數據獨佔（data monopolies）的反競爭行為，對於數據共享產生風險；自動化系統（例如自動化車輛、保安系統、

武器系統)有遭到入侵可能；及私人企業可能為了保護自身機密技術或智慧財產權而不願意分享數據。

b. 缺乏獲取資源的途徑，以及人力資本不足

與會者指出，人工智慧的研究及發展需要儲存和處理大量持續更新的數據，過程不僅昂貴而且時常無法取得足夠的數量規模。在此情況下，研究者及發展者可能會傾向處理較簡單的問題，因為所需的數據規模較小或較易取得。另外，與會者也表示，人工智慧的改變加劇，因此導致市場上人力緊縮，大公司可能會僅因對技術人力的需求而收購小公司。

c. 現行法規是否充分

部分論壇與會者認為，在廣泛使用人工智慧之下，將產生其所涉及的相關法令規範是否充足的問題。包括：人工智慧可能受到法令保護而不需要揭露太多技術背景，將可能引起公共安全及責任問題；現有智慧財產權的獨佔/保障期間對於人工智慧是否太長；人工智慧所生的創造物權利如何歸屬；以及使用人工智慧技術是否可能影響憲法保障的權利等。

d. 人工智慧所應適用的倫理框架以及對人工智慧的可解釋性與接納

報告指出，除了更新相關法令外，人工智慧亦需要有倫理框架以使人工智慧的選擇符合倫理價值。多數與會者討論人工智慧的可解釋性(explainability)時著重於合理的安全維護，與會者指出，總有一天自動化的人工智慧會遇到超過其演算能力的狀況(例如：自動化駕駛遇到無法作出最佳判斷的情況)，屆時我們會需要調查及分析以瞭解人工智慧的決策方式。此外，部分與會者對是否能信賴人工智慧以及社會是否能完全接受人工智慧仍抱有疑慮。

(5) 人工智慧研究進展所帶來的政策影響和優先研究目標

在考慮了人工智慧的益處和挑戰後，論壇參與者強調了一些他們認為需要

進一步關注的面向，分為政策面與研究面。

從政策形成與制訂而言，包含以下面向：

a. 增加數據共享的誘因

參與者指出，應確保共享數據的安全，建立安全空間（safe space）儲存敏感資訊，以促進數據共享而不會影響智慧財產權或品牌相關敏感資訊。舉例而言，航空業的數據共享，有助於事故發生率的降低。此外，亦有參與者提出應提升供給人工智慧數據的品質，因人工智慧的一切皆始於數據。參與者進一步表示，政府作為部分數據的擁有者，應調整過時法令，使人工智慧的開發及研究者得以接觸其所管理之數據。

b. 提高安全性和保護措施

參與者指出，關於資訊安全防護，政策制定者應該注意資訊安全防護系統製造商與使用者間，成本與責任的分攤比例是否適當。另有參與者建議政策制訂者對於自動化交通工具應建立新的法律框架以確保其安全性。

c. 更新人工智慧的監管方法

除了隱私保護外，由於人工智慧技術發展極為快速，政府在制定法規時，應注意不可太過僵化，而無法應對日新月異的人工智慧應用。另外，必須思考人工智慧自動化地為人們做決策時如何究責。

d. 評估可接受的風險和做決策的倫理

建議從經濟學、哲學、倫理學、法律等多個專業領域的視角來以測試和評估人工智慧系統的風險程度和倫理問題。

e. 其他政策考量

除前述面向外，與會者另外提及政策制訂者應考量有益於廣泛採用人



工智慧的其他政策內容，並減少可能的負面影響。

而從研究面的角度而言，則包括以下面向：

a. 建立沙盒，允許監管機構進行小規模試驗

以保護參與的利害關係人不承擔過高風險和責任的負擔，並使新商品和方案得到更有力的評估。

b. 發展高品質標記數據（high-quality labeled data）

與會者認為，因為數據資料廣泛，因此有組織或標記的數據，可促進機器學習，且人工智慧所產生的成果也會更精確。

c. 理解人工智慧對就業的影響、並重新構思未來的職業訓練和教育

聯邦政府將需要建立更全面的數據收集，以評估人工智能系統對個人和整體就業的影響，並瞭解哪些就業領域需要重新培訓。

d. 探索人工智慧的倫理及可解釋的人工智慧（explainable AI）

隨著人工智能系統得到進一步的開發和應用，政府和利害關係人必須對人工智慧相關新的倫理問題保持警惕。

(6) 後續聽證會

於 2018 年 6 月 26 日，GAO 的首席應用研究和方法首席科學家 Timothy Person 依據前述技術評估報告內容，在美國眾議院科學、太空和技術委員會研究與技術與能源小組委員會（Subcommittees on Research and Technology and Energy, Committee on Science, Space, and Technology, House of Representatives）聽證會中，針對人工智慧相關主題提出證詞。證詞中總結了人工智慧論壇參與者對於人工智慧發表的看法。包括關於人工智慧帶來的益處與挑戰，並囊括了在論壇中提及之應進一步關注的後續政策及研究問題。

#### IV. 歐盟

## 1. REPORT with recommendations to the Commission on Civil Law Rules on Robotics<sup>552</sup>

歐盟議會於 2017 年 1 月發表了一篇官方報告，主題是探討對於機器人相關民事法律之修正建議。

就民事責任之問題，該報告認為自動駕駛會帶來工作機會的減少，以及民事責任的問題。在契約責任方面目前多半是直接契約中明訂補充責任者；非契約責任，歐盟的 Council Directive 85/374/EEC 顯然已經無法涵蓋機器人所造成的民事責任。因此引起了是否需要新訂立規範之討論。民事責任分配上必須區分需要人類全程監控的自動車，和毋須全程監控的自動駕駛。就後者有必要制定新的法律規範。機器人所造成的損害賠償責任，目前比較可能的解決方案是責任保險機制，且保險必須要有基金作補充，確保損失都能夠獲得填補。

該報告並討論了以下幾個議題：

**建立代表機構**：該報告呼籲應該要為了機器人和人工智慧設置歐洲代表機構 (European Agency)，專門來提供科技、倫理、規範上的建議。

**智慧財產權保護**：該報告認為其應該提供一個科技中立的方法來處理雇用機器人時的智慧財產權問題，並確認歐洲民事法規皆符合 GDPR 之規定。

**建立標準化的試驗規範**：該報告認為歐盟各國應該要考量國際科技標準之一致性，並避免內部市場的分裂，保障顧客和產品的安全性，加以制定標準化的機器人試驗規範。

**無人機**：該報告檢驗了是否有必要介紹 Remotely Piloted Aircraft Systems (RPAS) 的義務性追蹤和辨認系統，可以決定無人機的實時位置。

**照護機器人**：照護機器人是機器人發展的重要領域，其可以擴大原有的人類照護，並可以將照護程序加以明確化，讓醫療人員可以花更多精力在診斷和制定

---

<sup>552</sup> European Parliament Committee on Legal Affairs (2017). *REPORT with recommendations to the Commission on Civil Law Rules on Robotics(2015/2103(INL))*. Retrieved from <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0005+0+DOC+PDF+V0/EN>

醫療方針上。但本報告仍然重申與被照護者進行社會互動是不可欠缺的。

**醫療機器人：**醫療用的機器人最重要的是必須符合最低限度的專業要求，從一開始的治療到最後的決定都必須符合人類醫師的標準。

**Cyber Physical systems (CPS)：**即將計算機網路科技系統、機器人以及與真實世界互動之人工智慧加以整合。

**環境影響：**機器人的使用在農業、供給食物、交通方面可以給環境帶來良好影響，但機器人的行為準則是不可以破壞環境。

**國際方面：**道路交通維也納公約、阿姆斯特丹宣言、海牙條約必須齊備。

**機器人的倫理規則：**該報告認為，機器人的開發者必須遵守四個原則：為善、非罪惡、自主、正義，以及尊重基本權利、採用正當預防措施、包容性、負責任、確保機器人決策之可逆轉性、極大化利益及最小化傷害。研究者的倫理規則則包含獨立、適任性、透明、負責。

**立法模式：**該報告認為較為適當的立法方式應該是先建立一個較為柔軟的法律框架，以指導原則或公私協力的方式，來確保機器人工業、機器人設計者和政府機關以及其他利害關係人之間的合作關係。

**僱傭和社會事項：**當人工智慧普及化，舊有產業可能不需要那麼多勞力，必須設計財務安全機制來確保人類是身心靈健康的，人類和機器的共生關係是能夠帶來良好的發展與生活。歐盟會員國的勞工法律與市場都必須要調整到能夠確保社會正義，能夠減少不平等、貧窮、社會排除，全人類都可以發展其天分、技術以及個體性。

## 2. Artificial Intelligence Potential Benefits and Ethical Considerations<sup>553</sup>

2016年10月，歐盟議會發表了一篇官方報告，探討人工智慧相關的潛在利益與倫理考量之議題。報告中首先定義了何謂人工智慧，歐盟議會的定義為「具

---

<sup>553</sup> European Parliament Committee on Legal Affairs (2016). *Artificial Intelligence Potential Benefits and Ethical Considerations*. Retrieved from [http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/571380/IPOL\\_BRI\(2016\)571380\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/571380/IPOL_BRI(2016)571380_EN.pdf)

備執行任務和合理程序的電腦程式，且該任務是與人類的智慧相關連的」，例如下西洋棋、自動駕駛車輛等等。第二個定義是來自 IBM 的定義，即「擴大的智慧」（augmented intelligence），即系統本身可以提升與擴大人類專家的技術與經驗而非取代之。

報告中認為在定義何謂「智慧」時應特別謹慎，人類在玩西洋棋的時候需要智慧和好的直覺，因為人類的頭腦沒有足夠的運算能力來理解大量的數據，然而電腦可以倚靠其運算能力，依據摩爾定律，每 18 個月即可成長一倍。

仍然有一些對人類來說相當簡單，但對人工智慧來說相當困難之任務，例如辨認一幅畫的內容或是不論其形狀處所隨意挑選一個東西。

信任來自於責任，如要能夠信任人工智慧，人工智慧的演算系統必須要能夠對人類解釋為什麼他們做出該行為。因此官方報告中建議所有的人工智慧系統都要包括以解釋為基礎的演算系統。同時也要求必須建置能夠協助人工智慧安全與倫理管理的系統，系統內須包括社會規範與價值的序列，以及遵守現有之法令等等。

歐盟 GDPR 限制了自動化個體做出「重大影響」使用者之決定（亦即，演算法是依據使用者程度的預測者）。法律應該有效建置所謂的「解釋權」，使用者可以要求人工智慧解釋為什麼做出這個演算法的決定。另外美國聯邦政策對自動駕駛之規範也已生效。

### 3. Artificial Intelligence, Robotics, Privacy and Data Protection<sup>554</sup>

2016 年 10 月所舉辦的第 38 屆國際隱私座談會（International Privacy Conference），會後發表了一篇官方報告，會議中提及了人工智慧、機器人、隱私權與資料保護等議題。

人工智慧和大數據的關係是相輔相成的，人工智慧進行自主學習需要大量的資料，另一方面大數據需要人工智慧來分析大量的資料。人工智慧和大數據會產

---

<sup>554</sup> Room document for the 38th International Conference of Data Protection and Privacy Commissioners (2016). *Artificial Intelligence, Robotics, Privacy and Data Protection*. Retrieved from [https://edps.europa.eu/sites/edp/files/publication/16-10-19\\_marrakesh\\_ai\\_paper\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf)

生兩個重要問題，一個是個人資料保護，另一個則是資料的正確性。個人資料保護與組織所採用的隱私政策有關，並會影響提供數據預測的門檻。資料的正確性則是當提供給人工智慧進行訓練之資料不足無法進行比對時，則人工智慧產生出的預測也會是不正確的預測，而變成惡性循環。為了要防範此種情況，可能有必要同時存在兩個資料保護機構（Data Protection Authority），或是必須有其他的監督機制。

### 與個人資料相關的具體議題

- (1) 臉部辨識的監控功能：當監視器等監控設備數量越多，監控必要和個人隱私權的爭論也甚囂塵上，具有臉部辨識的監控系統可能暴露每個人的行蹤與活動。
- (2) 自然語言處理程式：包括 APPLE 的 SIRI 和 GOOGLE 的自動翻譯，自然語言處理程式同樣需要大量數據資料，但同時也可能反過來將該資料變成監控工具。
- (3) 自動化機器：對於各樣自動化機器最重要的要求，即為不可傷害人類與破壞環境。
- (4) 自動駕駛：自動駕駛與個人資料之重要議題在於其會擷取大量的位置資料，我們將向特定的駕駛人暴露我們的行蹤資訊。
- (5) 半自動、全自動無人駕駛飛行器：必須建立自動駕駛機器的規範，且無人機應該與飛機和監視器加以區別，因為其同時具有兩者之功能。

### 其他已經超越現行法的問題：倫理面向

AI 的預測功能和資料庫建置可能會複製刻板印象，造成種族和文化歧視，阻礙個人自主與平等；AI 和機械的結合會監控我們的日常活動，因此倫理規則的建立是有其必要的。

### 其他已經超越現行法的問題：科技面向

由於人工智慧自主學習需要大量資訊作為背景，因此有必要設計能夠讓人工智

慧自動擷取資訊卻同時能夠屏蔽個人資料的機制，並且有必要將各領域的人工智慧研究者、發展者與個人資料專家都連接起來發展未來的人工智慧。

### 背景資訊：人工智慧與電腦自主學習

電腦自主學習(Machine Learning)被定義為毋須對電腦進行明確的指示，電腦即具備自行學習並修正之能力。若我們給予人工智慧的資料是沒有經過分類、分析的，那我們就必須設計出一個能夠自主學習，並找到這些無管理資料背後關連的人工智慧。且自主學習的人工智慧所製作的範本、模型等是人類無法理解的，因此當人工智慧自主學習後的資料分類標準，可能沒有辦法表達得相當正確，即使他們可以做得非常正確。此問題在討論運算透明度的時候會變得相當重要。

#### **4. European Civil Law Rules in Robotics<sup>555</sup>**

歐洲議會法律事務委員會 (The European Parliament's Legal Affairs Committee) 發表了一篇報告評議歐洲各個國家對於機器人的民事法律規範，該份報告首先定義何謂具有智慧的自動機器人，係指透過感應可以與外在環境交換資料，並且分析資料，能夠自我學習，且具有實體者，並具有對外在環境採取行動之能力。

就機器人的基本行為準則，尚可分為幾個面向：

##### (1) 保護人類不受機器人之傷害

歐洲目前已經建立一個概念是可能可以作為機器人倫理的原則，即人性尊嚴，此原則可以保護人類不受傷害。

##### (2) 尊重拒絕照護的權利

從人性尊嚴的原則尚可以導出兩個子原則，一個是給予人類拒絕機器人照護的權利，即使沒有受到身體傷害，但因機器人的存在感到不舒服的話仍

---

<sup>555</sup> *European Civil Law Rules in Robotics*. Retrieved from [http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL\\_STU\(2016\)571379\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf)

可以拒絕使用機器人。另一個是同意原則的建立，例如當機器人要實行平時的照護行為前，必須得到病人的同意。

### (3) 基本行為準則

機器人必須尊重人類的自主決定權，亦即機器人必須永遠服從人類的命令。然而，因為機器人不可以拿來當作武器，所以當人類對機器人下達的命令可能傷害使用人或第三人時，機器人必須發出警告信息，且該信息必須是能夠被接收人理解的，當該指令可能對第三人有危險，則機器人擁有絕對的否決權。

### (4) 機器人的資訊管理

由於機器人必須要接收到大量資訊，因此應該要建立一個嚴格的同意法則，且同意並不是僅在購買機器人當時，尚包括更多細節的要求上都必須尋求同意。

### (5) 社會連結之確保

由於機器人的出現讓人們可以待在家中，毋須外出與人互動。因此有必要建立機器人倫理規則讓機器人的出現並非消弭社會互動。機器人必須成為老年人、病人、身心障礙人士等人之代理人，使其生活更便利，但同時機器人不能完全取代人類。

### (6) 機器人的近用權

不論是專業使用者，或非專業使用者，每個人都可以使用機器人，歐盟立法者建立的原則為團結、平等、公平。議會認為必須要普及化家庭照護機器人，可以考慮透過普及國家健康照護和社會援助政策來發展公私保險制度。稅也可以作為誘因而鼓勵人們購買家庭照護機器人。該報告認為歐洲應該要採取稅務等政策來推廣人工智慧機器人的普及化。

### (7) 限制人類的技術進步

機器人是會自我學習的，他們可能在身體和心理特質上不斷進步，甚至可



能超越人類標準能力。對於超人主義的倫理反彈是可以預見的，人類可能會漸漸遺忘他們現在的樣子，因此有必要設計機器人倫理規則來控制這些現象。

#### (8) 機器人規章的法律價值

機器人規章包含了許多面向，包括機器人工程師的倫理指導原則、研究倫理委員會規則、設計師執照與使用執照等等。但不管是規章或是指導原則都並非法律上專有名詞，因此應認為指導原則是一訓示規定，讓人們選擇是否自願去遵守。且倫理規範是用來規範機器人的權益相關人的，不能加諸於第三人身上，例如機器人的買受人，除非有另外訂立倫理規範的契約。機器人規章本身沒有特殊法律地位，但可能會使法律效力擴大及於其他各種指令和證照。

## V. 英國

### 1. Artificial intelligence: opportunities and implications for the future of decision making<sup>556</sup>

英國國家學術院於 2016 年 2 月舉辦了一場研討會，由英國政府首席科學顧問 Mark Walport 爵士及內政部常務次長 Mark Sedwill 主持，討論人工智慧運用相關的法律及倫理議題，並由英國政府科學辦公室 (Government Office for Science, GO-Science) 於會後發表報告，針對 (一) 何謂人工智慧及如何運用人工智慧；(二) 人工智慧將為生產力帶來什麼益處；及 (三) 應如何管理人工智慧運用相關的倫理及法律風險等問題，提出可能的或已著手實施的解決方案。

#### 何謂人工智慧

該份報告首先指出，人工智慧的長處在於分類資料、找出特徵並作出預測，近年來更由於機器學習的發展，使得演算法或電腦程式能夠依據經驗自行更正或

---

<sup>556</sup> Government Office for Science (2016). *Artificial intelligence: opportunities and implications for the future of decision making*. Retrieved from [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/566075/gs-16-19-artificial-intelligence-ai-report.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/566075/gs-16-19-artificial-intelligence-ai-report.pdf)



改進，找出資料之間難以發現或被遺漏的關聯性，而更為複雜的機器學習系統（如深度學習）所產出的統計操作結果，甚至已非人類所能理解，這些發展導致機器學習與單純透過演算法將組織例行業務予以自動化，存在著本質上的差異。

機器學習的關鍵區別在於其學習過程是否受到人類監督，未受到監督的機器學習使用未經標記——亦即沒有所謂正確答案——的資料並探求其結構，受到監督的機器學習則使用經過標記的資料，用於分類或區別出一全新的、未曾見過的資料集，有助於識別資料當中的要素、預測可能的結果或發現異常值，後者提供一組正確答案並要求電腦找出更多的正確答案。深度學習本身即是一種受到監督的學習技術，其結合了多層次或多階段的非線性演算過程，用以自動辨識存在於資料集當中的特徵，並據此作出決策。深度學習對於機器學習具有十分強大的加乘效果，但需要相當大量的資料才能發揮功用。

將深度學習運用於自主決策（autonomous decision-making），而無需仰賴人為的介入，將為你我使用資料及作出選擇的方式帶來劇烈變革，並引發問責及信任等相關重要問題，這對政府來說格外切身，因為目前專家及制定政策者普遍同意重大決策必須有「人為參與（human in the loop）」，但其所扮演的角色及對結果的影響力將伴隨著技術發展與時俱進。

### 人工智慧的創新與生產力

該報告接著指出，人工智慧具有增加生產力的巨大潛能，能夠幫助企業及個人更有效率地利用資源，讓人們與巨量資料之間的互動更為流暢、減輕你我搜尋的負擔。人工智慧能夠補充或超越你我的能力，可以跟你我一同工作，甚至可以教導我們，而凡此種種皆為創造力及創新帶來了全新的機會，也許人工智慧真正的生產力便在於向你我展示全新的思維模式。

目前英國政府已經將資料科學及技術運用於下列方面：

- 透過預先設想需求並量身訂作相關服務，改善既有服務的效益，並使資源發揮最大的功用；

- 公務員運用更多資料作出決策變得更加容易，並減少欺瞞與錯誤；
- 讓決策變得更為透明可見；及
- 協助相關部會瞭解其所服務的團體，俾以確保提供正確的支援及機會給所有人。

政府的地位特殊，肩負著許多私人組織所沒有的義務，包括其行為模式必須是透明可見的、遵循正當程序並對其公民負責等。政府在運用人工智慧及大數據時，亦負有特殊的責任，正是基於此一認識，英國政府已發布政府運用資料科學工具進行分析的倫理指引<sup>557</sup>。

人工智慧透過彙整相關資料、為制定政策者辨識相關問題及主題、協助產出書面建議，在協助公務員提供數位服務方面十分具有價值，但很有可能許多政府決策在提交予人工智慧系統後會被認為是不適當的，「人為參與」的功能也將是必須的。假如人們未曾質疑機器所給出的建議，該等決定將成為事實上的自動決策，但即便人們對該等決定提出質疑，也有可能被認為是未經深思熟慮的。就像其他顧問一樣，該等系統對於決策者的影響將遭受質疑，而部會必須保持人工智慧在決策中所扮演的角色是透明可見的。

除了英國 1998 年資料保護法及 2016 年歐盟 GDPR 外，用以規範政府對公民資料的運用、保護隱私權、確保平等待遇及維護個人身分的特定立法框架，對於確保公眾信任政府有能力安全地管理資料來說，是相當重要的要素。運用人工智慧的團隊必須瞭解這些既有框架將如何適用，舉例而言，深度學習被用於推行未與他人分享之個人細節時，是否應取得同意是不明確的。

該報告表示，進階人工智慧所帶來的機會及風險，必須透過測試及實驗才能瞭解，為了讓政府分析師能夠探索先進技術，建立沙盒並在一個安全且受到控制的環境下，研究該等技術的潛能是有其必要性的。

### **對勞動力市場的影響**

---

<sup>557</sup> Department for Digital, Culture Media & Sport (2018). *Data Ethics Framework*. Retrieved from <https://www.gov.uk/government/publications/data-ethics-framework>.

機器學習的出現，連同機器人、大數據及自主系統，很有可能為經濟及勞動力市場帶來深遠的影響，但確切的影響範圍為何則意見分歧。該報告指出，自動化未必會造成就業下滑的結果，但很有可能會改變職業的類別及所需的技能，高技能的職業比例增加而中低技能的職業比例減少。

將來成長的職業很有可能是那些與科技互補的職業、而非被科技取代的職業，前者需要的是開發或利用新科技的技能，亦即受過 STEM 教育並具備數位技能的人才。與科技互補的職業亦包括那些難以自動化的工作，例如強調感知能力、複雜操作、創造性及社交智商（social intelligence）的工作。

廣泛而言，科技所帶來的轉變意味著特定職業的技能可能消失得更快，人們可能需要更為頻繁地變換工作，在職涯過程中重新學習新的技能、更為積極主動、樂於改變並保持彈性，而能夠穿梭在不同領域間的跨領域技能——例如解決問題的能力、保持心態上的彈性等等——將更為人們所重視。因此，政府必須促進新技能的發展、協助勞工獲得再訓練，無論係利用人工智慧更有效率地工作或移往特別需要人類技能的領域。

### **新挑戰**

伴隨著其所帶來的極大效益，人工智慧亦引發了許多潛在的倫理議題，政府必須扮演管理及減緩該等風險的角色，需要加以考量的兩大領域為：

- 瞭解機器學習及逐漸增加的個人資料對個人自由及隱私、同意等概念可能帶來的影響為何。
- 針對人工智慧所為的決策調適問責的概念及機制。

統計側寫 (statistical profiling) 運用過往資料預測不同群體的可能行為或特性，受到公部門及私部門的廣泛使用，例如保險公司能夠更為準確地預測風險、商家能夠更準確地對消費者進行行銷、執法單位能夠更為正確地評估威脅。然而，側寫可能會依據種族、生活方式或居住地對個人形成不公正的刻板印象，公部門應避免使用該等資料作為判準，以免造成不公正的歧視。「無罪推定」原則應作為運用該等預測技術的準則，而正確識別個人的能力亦有助於執法機關免

於被成見誤導，更為妥善地運用資源。

人工智慧亦能從公共資料中推衍出部分隱私資訊，例如個人的線上行為或與他人（如親友或同事）相關聯的資訊，而這類資訊可能會超出個人原本同意揭露的範圍。英國資訊專員辦公室所公布的匿名化實作守則，為組織提供了管理該等風險及防止從合併後的匿名資料重新識別個人的方法<sup>558</sup>，但由於人工智慧技術的發展，重新識別的可能性變得愈來愈高，因而組織必須定期檢視現有的保護措施。

演算法偏見可能帶來刻板印象的風險，其主要源自於用來訓練深度學習系統的資料，可能延續了社會既有的偏見、加劇不公平的情況，為了減緩該等風險，技術人員必須識別出資料中所存在的偏見，評估其影響。該等爭議圍繞著社會可能發展出的治理框架及其實際回應方式，許多作家及產業團體建議深入探討下列議題：

- 演算法發明人的特許執照制度。
- 涵蓋人工智慧運用的行為守則。
- 釐清因運用人工智慧所招致之損害責任。
- 用來支援公民向運用人工智慧組織提出挑戰的視察員。
- 評估人工智慧特定應用及結合可能對社會帶來何種傷害及益處的倫理審查委員會，或以某種各方皆表同意的方式針對機器學習的過程進行稽核。

其中許多想法已經由產業協會或私人企業進一步發展，但尚未被政府政策所採納，仍需要更為深入的考慮及審查。

儘管相關責任歸屬仍存在不確定性，仍須明確劃分問責的界線，例如由執行長就演算法所為決策負最終責任，否則大眾對於人工智慧運用的信任不太可能維持下去，這樣或許能夠鼓勵或要求發展出新的責任形式，作為人工智慧運用的

---

<sup>558</sup> 該實作守則因歐盟 GDPR 及英國 2018 年資料保護法施行，已被 Guide to the General Data Protection Regulation 所取代。

必要條件（至少在敏感的領域）。

透明度在確保責任歸屬方面是必要的，必須明確列出所使用之演算法、變數、資料、所追求之目的等，但這在實務上遭遇許多困難，為了理解該等資訊及其影響，需要一定程度的技術能力，而安全性及商業上的考量亦可能與徹底透明化的要求相抗衡。更為基本的難題是透明度未必能夠提供所需要的證據，僅只是公開靜態的程式碼，無法確保其確實被使用於特定的決策當中，實際運作時能否按照給定的資料集所預期的方式亦無從得知。

## 2. Robotics and artificial intelligence: Fifth Report of Session 2016-17<sup>559</sup>

有鑒於英國政府於 2013 年將機器人及自主化系統（Robotics and Autonomous System, RAS）列為英國領先全球的「八大技術」（Eight Great Technologies）之一，以及近年來機器人及人工智慧因運算處理能力提升、資料大量增長及深度學習等技術發展而有長足的進步，已為人類日常生活帶來深遠影響，從而引發了許多社會、倫理及法律課題，亟待政府擬定其數位策略（Digital Strategy）及相關計畫，以便將來的勞動力能夠具備所需的數位技能，英國下議院科學及科技委員會（House of Commons, Science and Technology Committee）<sup>560</sup>於 2016 年 3 月開始向政府提出質詢，並於同年 10 月 12 日發布《機器人與人工智慧》報告，希望政府能夠從：（一）機器人及人工智慧<sup>561</sup>對於英國勞動力與就業市場之影響，以及因應該等轉變所必需之人才庫及訓練；（二）自主化系統及人工智慧技術所提供的社會上及經濟上機會能夠為英國帶來多少好處；（三）該等資金、研究及創新藍圖於何種程度上有助於英國於該等領域維持領先地位，以及政府應採取何種措施以提供更進一步的協助；（四）因機器人及人工智慧發展所引發的社會、法律及倫理議題為何，其解決之道為何等面向提出書面答覆。

---

<sup>559</sup> House of Commons, Science and Technology Committee (2016). *Robotics and artificial intelligence: Fifth Report of Session 2016-17*. Retrieved from <https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/145.pdf>

<sup>560</sup> 英國下議院科學及科技委員會負責監督政府科學辦公室，後者英國為商業、能源及產業策略部轄下的「半獨立機關」（semi-autonomous organisation），負責支援政府首席科學顧問並確保英國政府的政策及決策奠基於強而有力的科學證據上，前者則擁有同樣廣泛的職權，得檢視足以影響或利用科學、工程、科技或研究的政府部門的相關活動。

<sup>561</sup> 在報告中委員會首先提到，雖然機器人未必會使用人工智慧，但可預期的是，機器人終將成為使用機器學習演算法等技術、執行實際或認知工作的「硬體」，因而將機器人及人工智慧一併作考量。

在這份報告中，委員會首先探討機器人是否會搶走人類工作、減少人力需求的疑慮，亦即，機器人及 AI 對於生產力及就業結構可能帶來的影響。普遍而言，機器人及 AI 被認為能夠增進生產力——特別是製造業——但其對於就業市場的影響則有不同看法，一派認為因機器人及 AI 所消失的工作將由其所創造的新興經濟活動及就業機會所彌補，整體就業情況並不會因此惡化，另一派則對此抱持懷疑態度。除此之外，委員會亦發現貧富差距將有可能因此加劇，因為較有可能被自動化技術取代的，大多數為欠缺創造性、中低薪資水平的工作。然而，亦有人直指「人類對抗機器（humans versus machines）」這項命題本身的錯誤，而認為機器人及 AI 應當是人類的支援及替身、與人類共同工作（work in partnership），協助人們做好份內的工作（task within jobs）、成為更有生產力的勞工，而非取代人類。但無論所抱持的看法為何，大多數人皆肯認工作性質將因此改變，因而學習新技能及調整教育體系，將有助於英國掌握機器人及 AI 所帶來的機會，政府必須確保教育及訓練體系具有足夠的彈性，俾以適應勞動力變遷的需求，並為終生學習作好準備。

針對機器人及 AI 所引發的倫理及法律議題，委員會則從「安全與控管」及「治理框架：標準及規範」兩大面向切入，並逐一要求政府應妥善回應 AI 技術的檢核及合規性、決策透明度、偏見最小化、隱私及同意、問責與責任、公眾對話等課題：

### **檢核及合規性**

由於自主化系統被設計來學習、適應及自我改進，無法使用傳統的軟體檢核方法，導致證明、測試及確認其可靠性、性能、安全性及倫理上的合致性變得格外困難，但也極端重要。Google DeepMind 便與牛津大學合作開發一「關閉系統開關」（kill switch），確保 AI 系統能夠被一再地、安全地被人類監督者打斷，而非學習如何避免或操縱該等介入。

### **決策透明度**

隨著機器學習及機率推理（probabilistic reasoning）導致演算法在許多領域取代人類決策——例如財務決策或醫療診斷——決策過程的透明度變得格外重要，

缺乏透明度將導致人們對結果的不信任，於 2018 年生效的歐盟 GDPR 便創設了「解說權」（right to explanation），個資當事人可據此要求解說自動化演算法的決策過程。

### **偏見最小化**

由於訓練資料集的選擇很可能反映了潛意識的文化偏見等原因，所有利用資料運作的系統皆很有可能受到偏見的影響，但因為開發者秉持著純粹技術專家的態度，此種偏見經常會被忽略，而假設資料運作下的決策是良善的、演算法是中性（立）的，政府必須對歧視及運用資料進行「資料側寫」設置防護措施。

### **隱私與同意**

資料為所有演算法執行任務、作出更聰明的決策及學習的原料，然而企業能夠取得多少資料、是否已獲得個資當事人同意、資料擁有者為何人、如何達致隱私、自主化、安全及公益間的平衡等課題亦亟需解決，政府必須確保資料被儲存在正確的地方，並以適當的方式進行處理及控管。

### **問責與責任**

當機器人及 AI（例如自駕車）運作失常時，應由何人負責，亦係亟待解決的問題，政府必須為演算法建立問責制度並提供安全網。雖然是否應將該等問題留待法院處置、透過判例法發展解決方案或需要制定新法，目前仍在討論中，但委員會亦指出普通法系僅得事後透過法律原則發展解決之道，所耗費的成本相當高昂，且對於受影響者造成相當大的壓力。目前英國政府則提議擴大並將產品責任納入汽車強制責任險的範圍，並由法院依據消費者保護法釐清責任主體。

### **公眾對話**

機器人及 AI 所引發的倫理及法律議題愈來愈受到關注，亟需構築適當的治理框架，但管制及立法能夠建立公眾信賴，亦有可能對於英國的技術發展構成阻礙，因而委員會要求政府應當召集業界、非官方組織及最終消費者等利害關係人共同進行對話，一方面有助於建立起公眾的信任及接受度、解決可能的誤解，

另一方面亦可透過公開對話即時處理相關社會、法律及倫理議題。委員會亦同時指出，雖然目前要制定專法用以規範機器人及 AI 仍嫌過早，但儘早開始詳細審究人工智慧系統在倫理、法律及社會層面的影響是重要的，不但有助英國致力於發展對社會有益的 AI 系統，亦可為相關公眾對話邁出重要的一步。

針對以上倫理及法律議題，委員會建議英國政府在艾倫圖靈研究中心（Alan Turing Institute）常設一人工智慧委員會，俾以觀察 AI 近期及潛在發展所帶來的社會、倫理及法律影響，並致力於確立 AI 技術發展及應用的管理原則，為政府提供相關法規建議，並與資料倫理委員會（Council of Data Ethics）密切合作。

### 3. AI in UK: ready, willing and able?<sup>562</sup>

為了解 AI 發展所帶來之經濟、倫理與社會影響，英國上議院於 2017 年 6 月 29 日成立 AI 特別委員會（Select Committee on Artificial Intelligence），該委員會嗣於 2018 年 4 月 16 日公布「AI 在英國：準備、意向與能力」之研究報告。該報告主要處理下列五大問題：(1) AI 如何在日常生活中影響人類？人類的日常生活可能如何改變？(2) AI 為英國帶來哪些潛在機會？如何實現這些機會？(3) AI 可能有哪些風險與影響？如何避免？(4) 公眾如何以負責任的方式參與 AI？(5) AI 之使用與發展會產生哪些倫理議題？為回答前述問題，AI 特別委員會依序就 AI 之理解及參與、AI 系統之設計及發展、AI 產業之發展、AI 與工作、AI 與生活、AI 與醫療保健、AI 相關風險之緩和以及 AI 潛能最大化與風險最小化八大主題進行研究，並對政府提出相關建議。

#### AI 之理解及參與

AI 特別委員會認為，就 AI 之一般理解、參與及公共敘述而言，政府或公共機構不應直接干涉媒體報導 AI 的方式，也不應促進大眾對 AI 之影響之正面看法；反之，政府應認知建立公眾信心以及說明其風險之必要。而在 AI 之日常接觸部分，讓公眾成員意識到相關決定之決策過程中，如何及何時使用 AI、使用

---

<sup>562</sup> House of Lords. Select Committee on Artificial Intelligence (2018). *Report of Session 2017-19: AI in UK: ready, willing and able?*. Retrieved from <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>



AI 所帶來之個人影響，均十分重要。對於前述問題之清晰認識，以及更強大的數位理解能力，將有助於公眾體驗 AI 之優點，並在有疑慮時選擇停止使用該產品。AI 特別委員會認為，產業界應帶頭建立一項自願機制，在使用 AI 做成涉及消費者之重大或敏感決定時，向公眾告知此一事實；而即將成立之 AI 行業機構（即 AI 理事會）亦應思考如何發展並引進此機制。

### AI 系統之設計及發展

在資料之存取與控制上，AI 特別委員會建議：

- (1) 為促進機構間以符合倫理之方式分享資料（ethical sharing），資料倫理與创新中心(Centre for Data Ethics and Innovation)發展資料信託(data trusts)制度時，應就個資當事人表達意見之方式加以規範(不管是定期諮商程序、個人資料代表（personal data representatives）或其他方式）。
- (2) 考量到政府持有資料（publicly-held data）之潛在商業價值，應於可能且適當時向 AI 研究者與開發者公開此等資料。此須政府部門與公共機構一致努力，以統一且相容之格式將記錄數位化，且公開此等資料時，資料信託也將扮演重要角色。
- (3) 在資料分享方面，資料倫理與创新中心應將開放銀行模式（Open Banking model）及其他資料可攜性（data portability）視為優先研究目標，於金融領域外建立安全的個人資料分享標準框架。此外，亦應針對各種不同的情境建立資料分享、控制與隱私之替代性工具和框架。
- (4) 就資料信託之建立而言，英國資訊專員辦公室（Information Commissioner's Office）應與資料倫理與创新中心密切合作，並協助公部門評估其所持有資料之價值，以使該等資料獲得最佳利用。此外，資訊專員辦公室對於公部門所擬訂之重大資料提供協議應具有審查權限。

在 AI 系統之發展上，多數情況下，AI 系統之可解釋性（即能夠解釋決策所根據之資料與邏輯）都有助於消費者理解和信賴該系統，這點也反映在英國及歐盟的新法令中。AI 特別委員會認為，在能夠為 AI 系統之決策過程提供完整且

令人滿意的解釋前，不應利用 AI 系統做成可能對個人生活產生重大影響之決策。這也意味著，除非找到替代的解決方案，至今尚無法完整解釋 AI 系統（如深度神經網路等）在使用上將受到限制。資料倫理與創新中心應諮詢艾倫圖靈研究所等專家機構，針對 AI 系統之可理解性訂定指導準則，AI 開發者應於 AI 理事會之主持下採納此等指導準則，並協商相關行業標準。

就資料偏見之問題而言，AI 特別委員會認為最主要的解決方法乃確保 AI 系統開發者具備多元性別、種族與社經背景，並遵守相關之行為倫理規範。為此，AI 特別委員會建議英國產業策略挑戰基金（Industrial Strategy Challenge Fund）立即就 AI 系統訓練資料集之稽核與測試工具系統舉辦競賽。另就資料壟斷（data monopolies）之問題而言，AI 特別委員會認為，政府與競爭及市場管理局（Competition and Markets Authority）應主動審查英國大型科技公司對於資料之使用情況與壟斷可能性，避免資料壟斷風險損及英國 AI 新創產業之持續性與發展性。

### AI 產業發展

為確保健全之 AI 產業發展環境，AI 特別委員會認為應從促進投資、將學術研究轉化為商業應用、改善 AI 開發人員進用規範以及維持創新四個面向著手。在促進 AI 產業投資方面，AI 特別委員會指出，英國新創產業所面臨最大的問題乃缺乏擴大規模所需資金，故政府應於 2017 年企業投資與創業投資信託機制（Enterprise Investment and Venture Capital Trust schemes）秋季預算中，保留英國商業銀行（British Business Bank）之部分預算作為中小型企業之 AI 成長基金。此外，政府應與正在尋求擴大規模之中小型 AI 企業進行諮商，了解其對於改善國內融資管道之需求，並審查現行獎勵政策是否對中小型企業有幫助。

在學術研究成果之轉換上，AI 特別委員會指出，長期以來，英國一直存在難以將 AI 學術成果轉換為商業產品之問題，對此，英國各大學應使用明確且可理解之智慧財產權授權及衍生公司（spin-out companies）設立政策與實踐，若有可能，其政策與實踐應盡量一致；而艾倫圖靈研究所作為國家 AI 研究中心，應將前述概念發展成具體政策建議，提供各大學參考。

在 AI 開發人員之進用上，AI 特別委員會建議進一步擴大 AI 與機器學習相關博士學位之資金援助，並透過博士媒合制度（PhD matching scheme）讓政府與企業平均分攤財務負擔。再者，為反映 AI 開發產業之需求，艾倫圖靈研究所與 AI 理事會應共同制定為期 3-6 個月的研究生轉換銜接課程（post-graduate conversion courses），使其他領域之研究者有能力轉換跑道至 AI 之開發與設計上。此外，政府應確保 AI 與機器學習博士學位之公費獎學金可提供給多元人群，為此，艾倫圖靈研究所及政府 AI 辦公室（Government Office for AI）應制定相關機制，使公費資助之博士學位課程能吸引女性及少數族群參與。最後，AI 特別委員會指出，英國特殊才能簽證計畫（Tier 1 (exceptional talent) visa scheme）之勞工數目可能無法滿足國內企業需求，且該計畫之要求對於企業所需人才而言可能過高，故建議透過將 AI 與機器學習加入工作簽證計畫下短缺職業清單（Tier 2 Shortage Occupations List）等方式，提高 AI 研究人員與開發人員可取得之簽證數量。

而在保持創新部分，AI 特別委員會認為，政府須承諾於脫歐後繼續進行或取代歐盟研究與創新計畫，且為避免英國 AI 之研究與發展過度集中於深度學習，政府與各大學應支持多樣化的 AI 研究，以確保英國持續立於 AI 發展的最前線。

## **AI 與工作**

在生產力的部分，AI 特別委員會支持政府認為 AI 可改善生產力之看法，但 AI 理事會應確保各企業（無論規模大小）均可享受 AI 所帶來之益處，並建議政府採取適當行動。此外，政府在進行數位基礎建設時，應考慮進一步投入更多資金，以確保英國各處均可納入 5G 與超高速寬頻網路。在政府採購部分，則建議英國政府商業服務機構（Crown Commercial Service）與政府數位辦公室（Government Digital Office）應審查政府採購科技作業規範等相關規定，將未來公部門使用 AI 之情況納入考量。

在勞動市場部分，AI 特別委員會檢視相關研究結果後，認為目前 AI 對勞動市場之影響尚無定論，各項研究見解分歧。隨著 AI 被納入經濟之一環，其亦將為勞動市場帶來巨大影響。然而，目前各界對於 AI 發展所帶來之影響均僅屬

推測，故 AI 特別委員會認為，政府迫切需要持續分析並評估 AI 在英國之發展狀況，並研擬相關的政策回應。

儘管 AI 對於勞動市場之影響仍具有高度不確定性，AI 特別委員會仍支持政府發展成人之再培訓計畫（adult retraining schemes），並認為無論是藍領或白領工作，在未來數十年間均有可能面臨風險，故應鼓勵並支持勞工轉業從事 AI 與新科技發展可能帶來之新工作。在這方面，國家再培訓計畫（National Retraining Scheme）應扮演重要角色，且應確保計畫參加者之多元性。產業界則應與政府資金一同資助國家再培訓計畫，此等合作夥伴關係將有助於提高該計畫之參與人數，也更能確定勞工轉業時所需具備之技能。

### **AI 與生活**

在教育部分，AI 特別委員會認為，政府在加強電腦教育之同時，不應刪減藝術與人文科目，而應將電腦科學與 AI 之社會面與倫理面加入課程內容。在社會及政治凝聚力的部分，AI 特別委員會指出，AI 使數位資料更容易被操縱，政府與英國通訊傳播管理局（Ofcom）應委外分析 AI 對於傳統媒體及社交媒體之影響，並應優先研擬措施以避免 AI 誤導或扭曲公眾意見。而對於 AI 所帶來之不平等問題，AI 特別委員會則指出，任何人均應得享有 AI 所帶來之機會，為此，政府應針對 AI 可能造成之社會不平等或區域不平等制定因應計畫；此外，英國社會流動性委員會（Social Mobility Commission）亦應將 AI 可能產生之影響納入其年度報告中。

### **AI 與醫療保健**

AI 特別委員會指出，在臨床上，AI 可用於醫學影像之判讀、基因體與個人化醫學之發展與流行病之偵測與監督等用途；在行政上，亦可用以節省醫生花費在行政流程上的心力，使醫療人員得以專注於病人照護與醫療診斷。然而，AI 技術在醫療保健方面之運用仍須考慮大眾對於醫療服務中使用 AI 之接受程度、病患資料之使用問題、醫療服務系統（National Health Service，簡稱 NHS）是否做好準備以及醫療人員是否已受相關訓練等因素。

其中，為處理病患資料使用安全問題，AI 特別委員會建議 NHS Digital 與國家醫療保健資料守衛者（National Data Guardian for Health and Care）於 2018 年底公布 NHS 資料分享框架，明定匿名分享病患資料之考量因素與應採取之預防措施，以及該資訊之價值與使用方式。此外，該框架應考量中小型企業對於 NHS 資料之使用需求，並確保病患知道其資料將被使用，而其有權拒絕之。最後，AI 特別委員會指出，英國許多機構尚未準備好利用 AI 技術，並建議 NHS 應於 2022 年前以統一格式將現存紀錄數位化。

### AI 相關風險之緩和

在法律責任部分，AI 特別委員會認為，雖可預見 AI 系統因故障、表現不如預期或其他因素而做出錯誤決策導致損害發生，但目前仍無法確定是否需要為前述情況之法律責任分配問題建立新機制，抑或現有機制已經足夠解決此問題。AI 特別委員會建議法律委員會（Law Commission）盡快討論現有機制是否足以處理 AI 之法律責任問題，並於適當時向政府建議合適之救濟措施內容。至少，法律委員會應就 AI 之問責性與可理解性（accountability and intelligibility）問題建立明確原則。

在 AI 與資料被濫用於網路刑事犯罪之問題上，AI 特別委員會建議各大學與研究機構在提供資金給 AI 開發者前，應要求其表明已意識到 AI 研究之影響、被濫用之可能性以及如何避免濫用情形。此外，內閣辦公室（Cabinet Office）應於最終版之網路安全科技戰略（Cyber Security Science & Technology Strategy）中，將 AI 於網路安全應用上可能產生之風險與機會納入考量；未來亦應進一步研究如何避免公共與個人資料集被用於資料破壞（data sabotage）之情形，並將研究成果轉化為相關指導原則。

在自動化武器部分，AI 特別委員會則建議政府於該報告公布後 8 個月內，召集軍事與 AI 專家小組，將英國政府對於自動化武器之定義修改為與其他國家相同或相近之內容。

### AI 潛能最大化與風險最小化

為使 AI 發揮最大潛能並使其風險降至最低，在國內政策與組織上，AI 特別委員會提出下列建議：

- (1) 政府在制定 AI 政策時，應確保新舊政策間具有一致性，並應使公眾及產業自始即能理解相關公告與政策細節。
- (2) 為避免政策過於積極或新機構間互相重疊與衝突，政府 AI 辦公室應制定 AI 之國家政策框架，其內容應包含本報告之各項建議、與產業戰略內容保持一致並受 AI 理事會之監督；此外，政府亦需指明該框架與 AI 相關政策之權責單位。
- (3) 政府為 AI 設立新機構時，需明訂其功能與職責；此外，為確保公眾信心，政府亦需確認公眾對 AI 之使用產生不滿時清楚知道應向誰投訴。
- (4) 政府 AI 辦公室應擔任資料倫理與创新中心、政府技術催化劑（GovTech Catalyst）團隊、艾倫圖靈研究所與 AI 理事會之間的協調者，留意各機構過去曾於 AI 領域中完成的工作，並協調新機構未來之工作計畫。
- (5) 艾倫圖靈研究所應實現其作為國家 AI 研究中心之角色，而政府需確保其具備足以達成此目標之資金與組織架構。

在法規與監管機構部分，AI 特別委員會建議透過資料保護法（Data Protection Bill）與 GDPR 處理個人資料相關問題，並建議政府 AI 辦公室確保現有監管機構與資料倫理與创新中心能一同檢視現行法規不足之處，找出未來可能需要訂定之法規。此外，英國國家審計局（National Audit Office）應確保現有監管機構（特別是資訊專員辦公室）具備充分資源。

在倫理部分，AI 特別委員會建議資料倫理與创新中心應與艾倫圖靈研究所及 AI 理事會一同草擬和推動適用於公私部門之跨部門行為倫理準則，並在有必要時依特定產業需求進行微調。

最後，在政策結果評估部分，AI 特別委員會認為，為使英國有能力實現 AI 所帶來之益處，政府政策應受密切監督，且應於適當時回應學術界與產業界之看

法。就此而論，政府 AI 辦公室應逐年向英國議會報告 AI 政策實施本報告中各項建議之進展。

## VI. 法國

### 1. For a Meaningful Artificial Intelligence - towards a French and European Strategy<sup>563</sup>

#### 背景

法國開始思考設計一套屬於適合自己的人工智慧發展模式，法國總理 Édouard Philippe 委託數學家 CÉDRIC VILLANI 以及法國國會成員於 2017 年 9 月 8 日至 2018 年 3 月 8 日進行本研究。

#### 人工智慧可能產生之六個議題

##### (1) 建立以資料為重心之經濟政策

在全球之人工智慧競賽中，掌握數據資料為主要致勝關鍵。有鑑於中國、俄羅斯以及美國透過專注在資料蒐集與利用，建立其在人工智慧領導性之地位，歐盟及法國若要在人工智慧領域享有一定控制權，必須要就數據資料發展一套政策並具體實踐在法國以及歐盟之產業上。具體方案如下：

##### a. 鼓勵企業共享數據資料

政府應鼓勵創建資料共享，並支持可替代之資料產出，以及在互惠、合作以及共享方面設立治理模式，目標是強化同部門參與者間之資料共享。政府也應鼓勵私部門間之資料共享，並安排讓某些持有特定資料之私部門可依據個案將資料釋出。

##### b. 基於公共利益開放特定資料

---

<sup>563</sup> Cédric Villani & Marc Schoenauer & Yann Bonnet & Charly Berthet & Anne-Charlotte Cornut & François Levin & Bertrand Rondepierre. (2018). *For a Meaningful Artificial Intelligence*. Retrieved from: [https://www.aiforhumanity.fr/pdfs/MissionVillani\\_Report\\_ENG-VF.pdf](https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf)

鼓勵經濟參與者共享並集結其資料，並使政府擔任可信賴的第三方。在某些特定情況下，由政府基於公共利益將特定資料公開供一般大眾使用。

c. 支持個資可攜權

賦予個人對其資料享有更大的自主權，亦即賦予個人在不同企業間移動其個人資料之權利，用戶可以將其個人資料以及其他相關資料從一個企業轉移至另外一個企業且這項權利亦應被延伸到人工智慧領域之應用。

d. 醫療、環境、交通以及國防四大領域為法國發展人工智慧之重點

法國應在這些領域優先發展人工智慧，並在這些產業取得全球性之關鍵地位。此外，人工智慧之創新過程亦必須執行沙盒（Sandbox），亦即透過暫時的減少管制密度，使參與者得以嘗試創新且幫助參與者承擔義務，並且在現實生活中進行試驗。

(2) 提升法國在人工智慧領域之研究

法國在人工智慧領域之研究以及其高教育組織已達到世界級之水準，並培育許多傑出之研究員。然而，近年來人工智慧研究領域已有相當程度的變化，主要的人工智慧公司自行開創研究中心，並增加私部門研究機構之競爭力，這種情況加速公立研究機構之研究員以及學生之流失。另一難題則是，法國在人工智慧領域之研究並沒有成功的技術移轉，或是使企業使用這些知識。為使人工智慧領域以及各地區間之研究能有效連結，本研究提供以下三項改善方案：

a. 創立跨學科之人工智慧研究機構，且這些研究機構應遍及法國並涵蓋特定應用或特定領域之研究。

b. 適當的分配各研究領域間之資源。



- c. 藉由提高研究人員之薪資以及增強產業與學術之合作，促使人工智慧研究之工作更具吸引力，並吸引外流之人才回國或外國專家至法國工作。

### (3) 規劃與控管人工智慧對於勞動力之影響

目前雖然尚無法知悉自動化後將使得勞動力市場有多少工作將應運而生或消失，但工作職缺以及工作組織將有可能產生很大的變化。是以，政府必須提出新之培訓計畫，使民眾可以獲取專業知識並轉型。

- a. 建立一個關於工作轉型的「公共實驗室」，並反映自動化後對於工作職務之影響。並透過測試工具以支持工作型態之轉型。
- b. 人工智慧與人類勞動力必須互補，亦即未來的許多工作可能都必須與機器互相合作，但是人類之創造力、手藝以及解決問題之能力可以適時填補機器之不足。透過人工智慧與人類智慧之互補，將使得勞動力在人工智慧時代之衝擊相對減少，並透過正式教育以及終身學習制度，幫助畢業生以及員工發展其創意及技能。
- c. 嘗試職業培訓的新資助方式，以解決人工智慧轉變所產生之問題。目前，企業資助其員工進行職業培訓，然而在數位轉型方面，企業一方面號召參與者要在自動化扮演重要腳色，卻對於員工培訓無任何資助。就此，企業間應透過互相對話並透過共享機制使其產業價值增加。
- d. 法國應於三年內增加三倍之人工智慧訓練，包括現行的培訓方案以及創設新課程，且應包含所有程度之教育包含碩博士等。

### (4) 使用人工智慧創造生態環境

全球暖化是當前重要的課題，在發展人工智慧的服務以及技術時，應一併將環境影響列入考量。就此，人工智慧之策略必須做的不僅是優化資源使用，更必須促進智慧生態轉型。採取方案如下：

- a. 政府應使用人工智慧以支持生態轉型，例如創建研究中心就生態轉型進行研究。並評估其對於環境之影響。
- b. 透過支持歐洲雲端產業之生態轉型，以減少人工智慧對於能源使用之密度。
- d. 生態轉型必須與所釋出之生態數據同步進行。人工智慧可以幫助減少能源消耗，恢復和保護自然。例如，透過使用無人機進行重新造林，或透過識別技術繪製生物物種。

#### (5) 人工智慧與倫理規範

人工智慧是否真的可以改善人類的生活福祉，我們應如何確保或掌控人工智慧的行為？這項問題引發許多人工智慧在倫理議題的討論。為確保新人工智慧科技可以尊重我們的社會價值以及規範，必須透過動員科學家、政府、產業、企業家以及民間社會採取行動。從長遠來看，若人工智慧之科技要被社會所接受，其技術必須可以被解釋。基於這項目的，政府應採行以下步驟：

- a. 為解決演算法可能產生之偏差，應使演算法透明化。要執行這項方案，應組成一組專家分析演算法以及資料庫，並使社會大眾可以進行自我評估。這些方法專注在三項領域之研究：製造更多可被解釋之模式、製造更多可被解釋之使用者介面、了解工作機制以產出令人滿意的解釋。
- b. 參與者對於人工智慧所引發之道德議題之責任，可透過訓練人工智慧領域之工程師以及研究員倫理機制，並執行歧視影響性評估且與法國之隱私影響評估一致，以鼓勵人工智慧領域工程師考量他們所研發之人工智慧對於社會產生之影響。
- c. 創建「人工智慧與數位科技倫理諮詢委員會」，並在此展開公共辯論。實際上，94%的受訪者認為應該在公開辯論中定期解決人工智慧在社會上之發展問題。

(6) 確保人工智慧之多樣性與共融性

在科技成為未來世界的關鍵要素時，人工智慧不能成為另一種排他工具。目前，女性在數位部門僅占 33%，少數族群所佔之比例更低。人工智慧可使社會更美好、公平以及有效率，也有可能使社會專注服務某些富人或精英而產生不公平。是以，公共政策應確保這些科技之發展並會使社會或經濟更為平等，並透過人工智慧減少這些不平等。

- a. 確保到 2020 年，參加數位工程課程的人中有 40% 是女性。
- b. 政府應建置一個管理行政程序的自動化系統，以幫助一般人可以更容易理解行政規則以及該規則如何適用於個人需求。
- c. 政府應支持人工智慧之社會創新計劃，以確保技術進步也有益於在社會行動領域工作的人員。

**法國總統發布關於人工智慧之四大目標**

2018 年 3 月 29 日，法國總統參考 CÉDRIC VILLANI 之《為一項有意義之人工智慧—關於法國及歐洲之戰略》研究報告，發表其對於如何使法國成為人工智慧領域之領導者之看法及具體策略<sup>564 565</sup>，分述如下：

(1) 強化人工智慧之生態系統並吸引最頂尖之人才：

- a. 由法國國家資訊與自動化研究所（Institut national de recherche en informatique et en automatique, INRIA）設立國家級人工智慧計畫。
- b. 在五年內，使在法國培訓人工智慧項目的人數達到現在人數兩倍。
- c. 強化公立研究機構與產業之合作，研究人員可以將 50% 的工作時間用於企業（目前是 20%）。

---

<sup>564</sup> the Government Information Service. (2018). *Artificial Intelligence: "Making France a leader"*. Retrieved from: <https://www.gouvernement.fr/en/artificial-intelligence-making-france-a-leader>

<sup>565</sup> AI for Humanity, *French Strategy for Artificial Intelligence*. Retrieved from: <https://www.aiforhumanity.fr/en/>

- d. 創立個人化之研究講座以吸引最優秀之研究員並發布研究計畫需求以吸引最優秀之研究計畫提案。

法國在未來五年內，將投入 7 億歐元用於人工智慧領域之研究。

- (2) 發展開放資料政策，並就法國已具備潛在優勢的領域應用人工智慧，如衛生保健：

- a. 開放公眾資料。
- b. 開發公私領域之資料交換平臺。
- c. 發展歐洲資料使用之框架。
- d. 就國家健康資料研究所（National Institute for Research in Computer Science and Control, INRIA）享有之安全且匿名之資料內容創立健康資料中心。

- (3) 創建監管以及金融框架以支持新興人工智慧研究計畫與新創產業：

- a. 法國將投入 15 億歐元發展人工智慧。
- b. 透過人工智慧改善公共政策。

- (4) 制定人工智慧倫理規範以確保其發展符合最高標準並可使人民接受：

- a. 支持人類科學研究在倫理方面。
- b. 應確保演算法得以被合理使用以及透明化。
- c. 將以政府間氣候變遷小組（Intergovernmental Panel on Climate Change, IPCC）模式，創立一群專家組成之人工智慧國際團體。

#### 後續效應：

目前已經有許多公司宣稱將公司之人工智慧研發中心設立於法國並增加當地就業機會，包括 IBM（預計將在二年內增加 400 個職位）、Samsung

(預計增加 100 個職位)、DeepMind 以及 Fujitsu。此外，Facebook 更宣稱已計畫投入 1,000 萬歐元擴大其目前於法國之人工智慧實驗室。Google 亦宣稱就人工智慧研究將在法國投資一基礎研究中心。

## VII. 加拿大

### 1. Challenge Ahead: Integrating Robotics, Artificial Intelligence and 3D Printing Technologies into Canada's Healthcare System<sup>566</sup>

#### (1) 報告作成緣由

2016 年 10 月 25 日，加拿大參議院以一委託命令 (Order of Reference) 授權參議院社會、科學及技術常務委員會 (Standing Senate Committee on Social Affairs, Science and Technology, 下稱「委員會」) 對「自動化在醫療衛生系統下所扮演的角色」進行檢驗並提出報告，而前述自動化係指針對機器人、人工智慧及 3D 列印技術的應用。

委員會在舉辦了 12 個相關會議，並於 2017 年 2 月 1 日在渥太華大學、2017 年 5 月 15 日在渥太華醫院總院區進行實地訪查，且訪問了數位研究者、投資人、倫理學家以及醫療相關業內人士後，於 2017 年 10 月作成本篇報告。

依據加拿大健康資訊機構 (Canadian Institute for Health Information) 之報告，加拿大 2016 年的年度醫療總支出預估達加幣 2,280 億元，年成長率達 2.7%，而龐大的醫療支出使加拿大存在難以維持其醫療體系的隱憂。委員會過去研究的一部份即是在探討如何建構「更健康的加拿大」、近年興起的醫療自動化創新以及自動化在醫療衛生體系中的應用及角色。本篇報告即是在此背景下作成。

#### (2) 委員會報告背景資訊

---

<sup>566</sup> Standing Senate Committee on Social Affairs, Science and Technology (2017). *Challenge Ahead: Integrating Robotics, Artificial Intelligence and 3D Printing Technologies into Canada's Healthcare System*. Retrieved from [https://sencanada.ca/content/sen/committee/421/SOCI/reports/RoboticsAI3DFinal\\_Web\\_e.pdf](https://sencanada.ca/content/sen/committee/421/SOCI/reports/RoboticsAI3DFinal_Web_e.pdf)

委員會對於自動化創新的研究主要針對機器人、人工智慧以及 3D 列印，因此本篇報告首先簡要定義及介紹了前述三項技術領域。其中，就人工智慧部分，本篇報告特別提到了人工智慧的應用，包括對於診斷、分析的研究室應用以及利用相關醫療經驗的深度學習（deep learning），更提到機器人在自動化過程中，可能會需要和人工智慧大量結合。

在加拿大法制下，醫療衛生服務的提供主要由各省/地區政府的負責，但聯邦政府仍可透過各相關法令的刑事規範觸及醫療衛生領域，包括對於食物、藥品、醫療器材以及化妝品的管制與許可。此外，聯邦政府也建立了許多機構和委員會進行醫療衛生相關的研究。

### (3) 人工智慧在醫療衛生的未來重要發展

人工智慧目前在加拿大最主要的研究類型為類神經網路（neural networks）或稱深度學習。委員會透過訪談前瞻人工智慧協會（Association for the Advancement of Artificial Intelligence）的 Subbarao Kambhampati 博士得知，加拿大早於其他國家持續地投入人工智慧（特別是深度學習）的研究，且加拿大政府持續對於人工智慧的基礎研究提供資源，使加拿大在該領域培養了相當多的博士候選人，並在蒙特羅、多倫多等地設立了數個傑出的人工智慧研究室。在醫療衛生的運用方面，人工智慧的發展將可應用於直接或間接的病患照護、改善診斷決策、選擇醫療方式、機器人手術與檢驗、醫藥存貨管理、居家照護及評估與預測病患需求等。

### (4) 信賴、隱私及倫理議題

在創新技術應用到醫療衛生領域時，首先會碰上的是相關從業人員及病患的信賴問題。在醫療診斷信賴度方面，委員會聽取加拿大前瞻研究機構（Canadian Institute for Advanced Research）主席 Alan Bernstein 的證詞，其表示人工智慧在診斷及分類皮膚癌及乳癌時展現了高度專業性，且機器協助的手術亦較傳統手術更為安全及準確，執行機器協助手術的醫師的疲勞及壓力亦降低；而使用機器協助的居家照護時，對照護者而言，其疲勞及壓力同樣也降低。

人工智慧技術的應用仰賴大量病患資料，因此不可避免的衍生了隱私問題。然而，委員會聽取開放機械倫理機構（Open Roboethics Institution）創立者 AJung Moon 的證詞，其表示傳統的隱私概念不合乎發展新技術時的需求；更有其他人對委員會表示人工智慧對於病患資料的需求是「愈多愈好」。據此，對於取得病患資料的許可、加密及去識別化以運用在人工智慧深度學習演算及各項應用領域上，實有其必要。

就倫理而言，機器人是否得以自主決策會影響是否符合倫理的判斷。以自主型機器人（autonomous robot）而言，因為不需人類介入，因此常被認為在倫理上難以接受；而半自主型機器人（semi-autonomous robot）的倫理界線則取決於投入其演算法中的資料類型及資料量。然而，在委員會訪談中，許多受訪談人表示新技術應用在醫療衛生服務的倫理界線，取決於醫療從業人員及病患是否可以得到更好的結果，若可得較好的結果，則在倫理上即可接受。

#### (5) 自動化對工作機會的影響

委員會依據訪談得到二種對於自動化技術影響工作機會的不同論述，一為自動化將減少工作機會，二則是自動化將產生新的工作機會，或者改變既有工作的型態。然而，委員會最終認為就現階段而言，自動化創新對於工作機會的影響仍無法精確預期，尚須未來醫療創新後持續討論。

#### (6) 商業化

委員會透過訪談發現，加拿大聯邦政府已透過各個不同機構投資創新者的研究，以助其商業化。然而受訪者表示，加拿大各省/地區的醫療產品市場對於創新產品的採購量低，接受度不如外國市場來的高，其中一位受訪者的公司 Kinova 的獲益甚至有 98% 來自於境外。部分受訪者認為加拿大境內對於創新產品接受度低的主要原因，可能來自於對於安全性及效率的不確定。

另有受訪者認為，加拿大固然對於創新的基礎研究及應用研究投注相當程度協力，但加拿大政府及其轄下之機構，需要投入更多力量幫助創新產品

打入國內市場。此外，商業化亦需要面對資金取得以及智慧財產權問題，其中，在取得資金方面，相較於傳統常以 2-5 年評估商業模式，創新技術的商業模式可能需要長達 20 年作為評估基礎，而以傳統商業模式的時間軸評估創新技術，可能會導致資金取得困難。智慧財產權部分，主要面臨的問題則是外國公司可能以智慧財產訴訟方式削減競爭。

#### (7) 訓練及教育的調整

創新技術進入醫療體系後，需要相應且持續的教育及訓練。甚至在醫療工作環境受新技術影響後，原本的業內人員需要再訓練以取得使用創新技術/產品所需的技能。

#### (8) 創新醫療器材相關法令調整

加拿大衛生部（Health Canada）指出，機器人、人工智慧及 3D 列印相關創新醫療器材執照的審核，加拿大的現行法令足資對應。然而，有受訪者則認為，現行法令仍可為了「創新」再進一步調整。例如，加拿大現行法規規定，醫療器材提供者需要提出充分的研究證據，證明該器材的安全性及效率，然而，現行法判斷安全性及效率的方式不當然適合創新技術，故現行法仍有改善空間。

#### (9) 前景及委員會建議

在加拿大眾議院的 2017 年 3 月 22 日聯邦預算案中提到，加拿大應鼓勵創新，以維持其全球競爭力。在同一預算案中所提到的鼓勵創新手段之一為投入 1 億 2,500 萬元預算，由加拿大前瞻研究機構發展「泛加拿大人工智慧策略（Pan-Canadian Artificial Intelligence Strategy）」，用於吸引學生及人才。

加拿大政府對人工智慧的投資也會用在技術商業化，並吸引其他跨國大公司如 Microsoft、Google、Facebook 等公司進一步投資。人工智慧的研究與商業化將會作為機器人技術發的基石，委員會同時也鼓勵聯邦政府對現階段的成果繼續注資。委員會進一步提案建置全國會議（National Conference），針對各項問



題及計畫研究討論。委員會提出十四項具體建議內容如下：

- (1) 關於機器人、人工智慧及 3D 列印的全國會議，建議廣泛邀集聯邦及地方政府之產業、衛生及教育官員及各領域之研究者、企業家、投資人、醫療政策制訂者及專業人士等參加。
- (2) 全國會議對機器人、人工智慧以及 3D 列印等技術應用於醫療系統的投資行公開討論，且就不同議題組成專家工作小組。專家工作小組應包括下列議題：道德倫理、商業化、更新醫療照護提供方式、偏鄉的醫療照護提供、取用技術的公平性、勞動力調整、教育及訓練需求以及法規監管。
- (3) 全國會議組成的各專家工作小組於考慮倫理、隱私及安全性問題後，個別制訂策略計畫以鼓勵及促進創新技術應用於醫療系統。專家工作小組的數量以及其所獲得之授權及人員應定期審核。
- (4) 加拿大衛生部作為相關技術的監管機關，參與法規監管專家工作小組，以確保負責研究及建議相關議題之國際性機構的工作受到監督並納入小組討論內容中。
- (5) 由各專家工作小組的主席組成秘書處，秘書處功能包括：整合各專家工作小組的成果、蒐集各專家工作小組的報告、向聯邦政府報告專家工作小組的進度及提供全國會議及專家工作小組工作所需的額外協助。
- (6) 建議加拿大政府對於專家工作小組以及秘書處提供足夠的資金。
- (7) 建議「衛生部」部長（Minister of Health）、「創新、科學及經濟發展部」部長（Minister of Innovation, Science and Economic Development）以及「僱傭、勞動力發展及勞動部」部長（Minister of Employment, Workforce Development and Labour）向專家工作小組請求提供進度報告，並於需要時與地方部會討論該報告之結論及建議。
- (8) 建議「衛生部」部長向法規監管之專家工作小組請求針對（但不限於）「醫療器材相關法令是否有更新必要」提供意見。

- (9) 建議「創新、科學及經濟發展部」部長向商業化之專家工作小組請求針對（但不限於）智慧財產權相關疑慮提供意見。
- (10) 建議加拿大衛生部作為加拿大健康資訊通道（Canada Health Infoway，下稱「Infoway」）董事之一員，請求 Infoway 參與全國會議，以期向其他參與者分享 Infoway 在加拿大數位化健康資訊的進度，並取得回饋。
- (11) 建議加拿大衛生部作為加拿大藥品及衛生技術署（Canadian Agency for Drugs and Technologies in Health）董事之一員，要求其參加全國會議及相關的專家工作小組。
- (12) 建議加拿大政府召開年度全國會議以評估加拿大國內之機器人、人工智慧以及 3D 列印於醫療衛生系統的整合狀況，並指出可能的新挑戰。
- (13) 建議加拿大衛生研究機構（Canadian Institutes of Health Research）主席、加拿大自然科學及工程研究委員會（Natural Sciences and Engineering Research Council of Canada）主席及社會科學及人類研究委員會（Social Sciences and Humanities Research Council）主席定期會面討論合作機制，以加速機器人、人工智慧及 3D 列印之研究。
- (14) 建議加拿大政府舉辦醫療衛生發現論壇（Forum for Healthcare Discovery），該論壇可鼓勵創新者及企業家向公眾及醫療衛生相關人士分享其發現，並學習額外的醫療衛生挑戰。

## VIII. 日本

### 1. AIネットワーク社会推進会議報告書2018<sup>567</sup>

日本總務省情報通信政策研究所招集產學及民間有識者共同參與舉辦「AI 網路化社會推進會議」，從 2016 年 10 月起針對社會全體在邁向 AI 網路化推進時社會、經濟、倫理及法律上的課題進行綜合性檢討。

---

<sup>567</sup> 總務省情報通信政策研究所（2018），《AI ネットワーク社会推進会議報告書 2018》，取自 [http://www.soumu.go.jp/menu\\_news/s-news/01iicp01\\_02000072.html](http://www.soumu.go.jp/menu_news/s-news/01iicp01_02000072.html)

由於在 AI 技術急速開發與運用的發展中，AI 系統透過網際網路形成「AI 網路化」，期待能夠解決社會等方面議題，為人類或社會經濟帶來更大利益。但包括 AI 的黑箱化或控制失靈在內等風險或疑慮，皆是造成阻礙 AI 網路化健全發展的重要因素。因而，為提升 AI 的有利條件並盡可能降低風險，無論對 AI 的開發者、利用者或數據提供者來說，整理相關注意事項並建立人類的信賴，至為重要。

因此，AI 網路化社會推進會議在發表「2016 年版報告書」及「2017 年版報告書」後，繼續針對隨 AI 網路化發展所形成生態系統之展望與 AI 運用應注意事項等進行檢討，參酌 2018 年 6 月至同年 6 月 26 日間所徵集之意見，進行檢討彙整並於 2018 年 7 月公布本「2018 年版報告書」。

#### (1) AI 網路化對社會與經濟的影響

##### a. 情境分析與生態系統展望

設想 AI 網路化中機器人可能發生的情境，進行風險分析並據以持續檢討，以評估對社會與經濟各領域可能的衝擊與風險。有鑒於運用生態的複雜化，以預測與回溯雙向的手法，對利用者，尤其是最終利用者的利益與風險，從「個人」生活、「公共」公益、「產業」商業的不同層面，設定包括社區營造、行政、危機管理、健康、移動、居住、教育學習、工作、財產、興趣娛樂、物品、金錢在內的 12 個分類，從「領域融合與跨領域」及「社會需求或議題」的觀點出發，以利用者的角度，主要以產品與服務供給面分別就「跨領域前」及「跨領域後」作出衝擊與風險的評價。在 2018 年版的報告中，主要是就此 12 個分類中的「行政」、「移動」及「居住」三領域中所觀察到的新案例為對象進行評價。

另於生態系統展望上，設定「都市」、「地方」、「家庭」及「企業」四類的利用場景而展望 AI 運用，並挑選「完全自動駕駛」、「醫療診斷」、「人事評價與進用」、「金融（保險）」及「行政」五個案例進行案例研究，整理 AI 運用上的優勢與衍生議題。此外，亦從網路化

的角度考察阻礙 AI 網路化健全發展的因素：諸如遭駭客攻擊、不正當操作、AI 系統間協調能力不足、個人資料流出，致使 AI 系統陷入機能失調而發生事故、損失或隱私侵害等。為因應此等證明困難或責任歸屬等問題，篩檢出今後應該留意檢討事項。又，政府草擬、規劃與執行 AI 網路化的適當政策上，對此等狀況的掌握極為重要。因此，亦需要設定能掌握 AI 網路化進展對社會影響的定量及客觀之衡量指標。此等指標分為事前、初期與正式指標。目前階段，尚以事前與初期進行檢討。

#### b. AI 運用方針與人才培育

在檢討 AI 運用方針上，制定 AI 開發指引草案，整理出各領域應用者應該留意的事項並與國際分享。除了掌握運用 AI 的利益與風險，亦務必要能展望 AI 網路化所形成之利害關係人間的生態系統。主要以利用者角度著眼於 AI 運用，以前述四類利用場景及五種觀察事例整理出 AI 網路化的優勢與衍生議題，以形成展望生態。比如在新服務開發與提供、最適化與效率化、降低成本等諸多利益下，諸如自動駕駛變更車道與匯流、遭駭客侵襲或系統未更新誤判、資訊不實等發生交通混亂或事故等協調、資訊安全與保全或設想外的議題等，尤其是救護車等醫療緊急救命場景。因而，在促進 AI 運用或網路化健全發展上，有必要針對教育與人才培育、受害救濟及法制等認知全面進行檢討。在教育與技能上，則提出人類與 AI 關係的角色分工、社會變遷及人類技能、學校教育、職業技能、生涯教育與 AI 運用等六項議題。

#### (2) AI 運用中應注意的事項

本報告整理出 AI 運用的相關主體並彙整出「AI 運用原則案」，主要包括人機角色的適切分工及適當利用、資料品質的適當學習、各主體間相互合作（以上三項主要是增進使用利益）、生命/人身/財產安全、資安、無隱私侵害（以上三項主要是降低抑制風險）、人類尊嚴與個人自律、公平性、透明性、可計量性等原則（最後四項主要是醞釀信賴關係），以求促進 AI 開發運用並健全 AI 網路化發展，實現以人為本「智慧聯網社會」。此

等原則，尚需持續檢討整理。另亦需依利用者的不同類型，尤其是消費取向的分類，作成並發布各自的「手冊」、「指引」等教材。

### (3) 今後的課題

在今後的檢討上，從 AI 的開發、運用或社會實踐中已顯露風險的案例中吸取教訓尤其重要。而今後的課題尚包括以下事項：

- AI 開發促進活用並健全 AI 網路發展事項，包括制定 AI 開發指引、制定運用方針、利害關係人致力環境整備、確保 AI 系統或 AI 服務相互間順暢合作、確保競爭性生態系統、保護利用者利益、技術開發課題；
- AI 網路資通資訊與資料事項，包括資安對策、隱私與個人資料保護；
- AI 網路化造成社會與經濟影響事項，包括內容制度化課題、AI 網路化對社會與經濟影響情境分析、AI 網路化進展的影響評價指標及富足、幸福之評價指標設定、醞釀運用 AI 的社會接受度；
- 人類處於 AI 網路化社會中課題事項，包括檢討人類與 AI 關係的認知、利害關係人間的態度、因應 AI 網路化教育/人才養成/勞動環境整備、AI 學習涵養及防止造成 AI 網路落差、安全網路整備及其他相關課題。

此等課題紛歧複雜，仍需有廣泛產官學各領域利害關係人參與，於國內外進行持續且多面向檢討。今後尚需按議題的緊急性與重要性等設定優先順序進行檢討。

## IX. 新加坡

### 1. Discussion Paper: Artificial Intelligence (AI) and Personal Data – Fostering Responsible Development and Adoption of AI<sup>568</sup>

---

<sup>568</sup> Personal Data Protection Commission (2018). *Discussion Paper: Artificial Intelligence (AI) and Personal Data – Fostering Responsible Development and Adoption of AI*. Retrieved from <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/Discussion-Paper-on-AI-and-PD---050618.pdf>

為促進 AI 議題之討論，新加坡個人資料保護委員會（Personal Data Protection Commission）於 2018 年 6 月 5 日發布「AI 與個人資料」討論報告，該報告提出 AI 之四階段治理框架。該報告認為，AI 治理框架應納入下列兩項原則：(1) 任何由 AI 所作成或由 AI 協助作成之決策，應具備可解釋性（explainable）、透明性與公平性三項特質；及(2) AI 系統、機器人以及透過 AI 作成之決策，應以人類為中心，並遵守行善（Beneficence）或不傷害（Do no harm）原則。具體而言，AI 治理框架應分為下列四個階段：(1) 辨識該框架之目標；(2) 選擇適當的機構治理措施；(3) 考量顧客關係管理程序（Consumer Relationship Management Processes）；及 (4) 建立決策與風險評估框架。

### **辨識 AI 治理框架之目標**

在第一階段，AI 治理框架應以可解釋性與可驗證性（verifiability）、良好數據問責實務（good data accountability practices）及/或透明化為目標。其中，可解釋性與可驗證性之目標，係希望使用 AI 之決策者能說明 AI 在決策過程中所發揮之作用與功能，或至少能驗證 AI 之作用是否合乎期待，且未超過原先設定之技術與倫理界限。而良好數據問責實務之目標，係確保 AI 系統所提供之建議或下游決策（downstream decisions）不會發生誤判（false positive）或漏判（false negative）之錯誤，也不會產生無意識歧視（unintentional discrimination）之風險。最後，透明化之目標，則希望在 AI 價值鏈（value chain）中，利害關係人之意見溝通管道開放且透明，以建立其對於 AI 生態系統之信任感。

### **選擇適當的機構治理措施**

第二階段之機構治理措施分為「治理」以及「作業管理與系統設計」兩大類別。在「治理」類別下，建議採取之措施包括：(1) 內部治理：當機構於決策過程中使用 AI 時，應考慮建立新的公司治理或監督機制，或更新現行制度；(2) 風險及/或危害之減輕：藉由風險與影響評估，辨識使用 AI 可預見之潛在風險；(3) AI 使用與決策之定期性與臨時性審查：開始使用 AI 後，機構應考慮定期審查決策過程，以評估決策過程中是否適合繼續仰賴 AI 系統。

在「作業管理與系統設計」類別下，建議採取之措施則包括：(1) 數據問責 (data accountability)：即對於自動化決策中所使用之數據，採取來源紀錄、審計追蹤、真實性評分等措施，以減少數據問責相關問題；(2) 可重複性：即採取可重複性評估等措施，確保 AI 系統在相同情境下所作成之決策具有一致性，以強化消費者信心；(3) 可追蹤性：即記錄相關數據、追蹤決策過程與 AI 演算法，強化 AI 決策與建議方式之可追蹤性；(4) 調整 AI 模型：即於 AI 模型之選擇上，應經審慎考量，作成選擇之過程與理由均應作成紀錄，且應定期更新調整原先選用之 AI 模型。

### 顧客關係管理程序

該報告建議於現行之顧客管理程序中納入下列措施：(1) 揭露政策：揭露於決策過程中使用 AI 之事實，並執行且揭露倫理評價之結果；(2) 說明政策：向消費者說明決策過程中如何使用 AI，並解釋特定決策之決策過程與理由；(3) 啟發式評鑑 (heuristic evaluation)：透過此評鑑法確保使用者介面層達成原訂目標；(4) 退出選項：藉由提供消費者退出之選項，建立消費者信心；(5) 回饋管道：提供電子郵件等回應管道，讓受影響之人得向機構提出相關疑慮；(6) 決策審查：提供申請管道，讓受影響之人得請求審查相關決策。

### 決策與風險評估框架

在最終階段，應綜合考量相關危害之可能性與嚴重性，選擇下列任一決策方法：(1) 人在迴路中 (human-in-the-loop)：即人類決策者仰賴 AI 系統提供建議，但自己作成最終決定；(2) 人在迴路外 (human-out-of-the-loop)：即完全由 AI 系統根據預先設定之條件，作成自動化決策；(3) 人在迴路上 (human-over-the-loop) 之決策方法：即由人類決策者決定目標後，再由 AI 系統針對達成該目標之方法提出建議。

## **X. 印度**

### **1. National Strategy for Artificial Intelligence #AIFORALL<sup>569</sup>**

---

<sup>569</sup> NITI Aayog (2018). *Discussion Paper: National Strategy for Artificial Intelligence #AIFORALL*. Retrieved

印度財政部長 Hon'ble 於 2018-2019 之預算案演講中表明委任 NITI Aayog 研究人工智慧之國家計劃，盼以該計畫之研究結果導引印度人工智慧產業之發展。因此，本報告之軸心在於探究印度於全世界人工智慧發展潮流中的定位，至於 #AIFORALL 之標語則反應本報告之核心價值，意即，協助強化勞動力以改善現下專業能力短缺或無法獲取專業知識之情形、善用人工智慧技術解決新興經濟體發展過程面臨之問題、妥適因應全球性的挑戰，最終確保整體社會共存共榮。

於 2018 年 6 月完成之研究內容可分為兩大部分，其一，對於人工智慧在各領域之發展可行性進行概念辯證；其二，研擬一套印度人工智慧之通盤發展策略。

於第二部分之發展策略中羅列諸多建議，由研發、勞動力之培訓、加速人工智慧技術之運用、承擔責任之人工智慧等四大面向切入，剖析政府在當中所應扮演之角色。各面向之具體建議詳述如下：

## 研發

為求增進相關技術之研發能量並將研發成果商品化，NITI Aayog 分別從組織面與制度面提出幾項建議。在組織編制上建議建構不同功能之中心執行人工智慧發展任務，另亦提出四項制度面之突破，包括建立共同數據計算平台、射月計畫、完善化智慧財產權之規範以及啟動 CERN for AI 計畫等。

### (1) 建立人工智慧卓越技術研發中心 (Centre of Research Excellence for AI, COREs)

該中心之設置目的係專職研究人工智慧領域之技術。應由政府認證相關之產學機構參與研究，並由政府提供財政資助。

除了各機構之創建外，政府亦須針對 COREs 之人才培育執行短期與長期發展計畫，短期而言，有鑒於目前印度研發能量與人才之匱乏，應建立相關獎掖措施，例如提供頂級研發設備、比照國際標準之人才薪酬制度，對



於有意向國外發展者，應提供國家人工智慧獎學金，增進其待在國內發展之誘因。長期而言，對於人工智慧核心領域技術應開設高階人才課程，以確保研發人才之培育與技術研究之永續性。

(2) 人工智慧技術轉型國際中心 (International Centre for Transformational Artificial Intelligence, ICTAIs)

其設置之目的在於研究相關技術之應用方式，並且確保該等應用符合產業發展需求與國家發展策略。由政府挹注資金、協助營運，並以公私協力之方式建置該機構。ICTAIs 之營運資本除源自政府外，私人企業亦可成為股東。而董事會之組成需包含產學界專家人士、國際專業領袖、該公司之執行總裁亦可提名經 ICTAI Inc. 同意之人選擔任董事。

作為各 ICTAIs 之統合機構，政府應另行籌設以技術轉型為目的之公司 (ICTAIs Inc.)，其管理階層除有政府代表外亦應重視私領域之專家參與。該公司之負責事項包括：對於 ICTAIs 挹注種子資金、監督 ICTAIs 之營運、行使對於 ICTAIs 執行總裁之人事指派權、委託 ICTAIs 執行射月計畫 (moonshot projects)、對於 ICTAIs 不同領域之發展劃定先後順序、建構 ICTAIs 與私部門機構之合作管道等事項。

(3) 技術永續研究中心 (Centre for Studies on Technological Sustainability, CSTS)

設置目的係為了關照技術研發過程所須之金融服務、對於技術研發之可持續性與國際競爭性擬定相關策略。具體之責任包括：

- 藉由各項社會研究指數監測人工智慧技術對於消費端之影響，並提供修正建議提升該等技術研發成果之市場滲透率。
- 研究人工智慧技術市場化之財務可行性，確保其取價機制能夠符合整體印度市場之消費實態。
- 研究人工智慧技術於世界各國之研發情形、最理想之定價機制與社會滲透策略，並擬定本國相關技術之全球發展策略。

- 為 COREs 與 ICTAIs 等研究機構建立跨國合作機制。
- 提供人工智慧之知識彙整平台，舉辦國際性工作坊、會議、提升相關領導者、研發者以及監管者之交流機會。

#### (4) 共同數據計算平台

由國家建置共同數據計算平台。將 COREs 與 ICTAIs 之系統串連至「國家知識網絡」之雲端計算平台。藉由數位化系統高效率之串接降低對於實體基礎建設之需求，亦可降低各中心營運與管理成本、確保國家資訊之安全性。

#### (5) 射月計畫 (moonshot project)

射月計畫之審核應建立在兩大標準下進行：其一，屬於新興科技或科學領域且具有市場吸引力、能夠解決目前重要的實務問題，其二，具有潛在用戶需求，且為既存技術無法滿足之需求。而該等計畫之篩選與進行應由 ICTAI Inc. 統籌主導，並委由 ICTAIs 執行。

#### (6) 智慧財產權之保障

於人工智慧領域，保有研究成果之智慧財產權係研究者從事研究之主要動機，惟人工智慧技術衍生之智慧財產權與其他運算技術、程式衍生之智慧財產權有所不同，由於人工智慧演算法之操作涉及眾多之數據集，對於該等運作模式之智慧財產權應如何界定，建議應由政府組成專案小組與公司事務部門 (Ministry of Corporate Affairs)、印度商工部產業政策推廣部門 (Department of Industrial Policy & Promotion) 共同研議妥適之規範框架。

#### (7) CERN for AI

對應到歐洲核子研究組織 (European Organization for Nuclear Research, CERN) 於世界各國建立之合作規模與資源串流，NITI Aayog 主張印度也應效尤此機制，作為全球首個國家創設類似 CERN 之組織，與世界各國協力進行人工智慧之研究。相關之研究任務包括：人工智慧通盤研究、可解

釋人工智慧（Explainable AI）、強化數據安全與隱私之匿名化協議、倫理與人工智慧、以人工智慧於醫療保健、教育、都市化、農業等領域之應用等。

### 勞動力之培訓

有鑑於人工智慧對於勞動市場供需帶來之劇烈變化：例如，創造新興市場之勞動力需求、以自動化技術消弭既有市場之勞動力需求。NITI Aayog 建議應建立起由政府主導之常務委員會或專案小組，邀集各利害關係人與會，共同檢驗並報告人工智慧對於印度整體勞動市場影響之即時資訊。且該等組織不應僅針對 IT 產業進行評估，而應通盤審酌全國勞動市場之就業環境。依照勞動市場之變動實態，在實證基礎上針對資助教育機構、特定領域就業機會之開放、人力資源效益最大化等議題形成政策決定。

此外，NITI Aayog 將勞動力區分為「已進入就業市場之勞工」與「仍在受教階段之學生」，分別說明政府所應擔負之任務：

#### (1) 勞工

##### a. 創造新興產業之就業機會

應提升相對於傳統資訊與軟體服務業之就業機會，例如，數據標註（data annotation）產業被預期將伴隨人工智慧產業之興起而擴大對於勞動力之需求。政策面上，可對於提供該等就業機會之企業給予免稅期、將該等就業機會之提供納入企業社會責任之一環等。

##### b. 核可與標準化非正式技職訓練機構

強化與私人技職訓練機構之合作，藉由核發相關許可執照、建立技職訓練標準，以利產業界識別該等技職訓練機構培育之人才，嫁接供需雙方對於勞動力培訓與錄用之評斷依據。

##### c. 增加線上開放式學習平台

線上開放式學習平台，例如 Coursera 與 edX 等的使用，能有助於勞動

人口汲取廣泛而即時之資訊。惟為確保該等平台品質之一致性與實用性，推廣線上開放式課程的同時，政府亦應制定相關之指導原則，對於其教學品質建立嚴格審查標準並且對於該等平台建立認證機制。

d. 提升企業之經濟誘因

讓員工投入在職教育可能會提升原本就職企業之機會成本，因此，政府可提供相關之經濟誘因，例如：將薪資所得稅稅收提撥作為企業培訓活動之津貼、對於鼓勵參與在職訓練之企業調降營業所得稅、對於未支出員工訓練費用之企業課徵特別科目之稅捐等、對於中小企業提撥在職教育之補助款。然而，該等在職教育之運作都需符合政府訂定之在職訓練標準、由取得許可之機構提供在職教育服務，確保該等經濟誘因不致受到濫用。

(2) 學生

- a. 於基礎教育階段，應提升技職教育的比重，尤其是強化 STEM 教育。於高等教育階段應強化產學合作以利教育工作者與產業界相互交流，例如：設立工作坊、導入產業講師等。於研究所教育階段，應鼓勵研究生投入國內機構進行研究並且應建立跨領域之合作與教育機會，對於非專門研究人工智慧之研究生，亦可藉由跨領域學習架接對於人工智慧之基礎知識。
- b. 針對欠缺專業師資之情形，可將線上開放式課程納入學分評量範圍，並藉由政府授權許可之方式確保該等管道之教育品質。

**加速人工智慧技術之運用**

印度之人工智慧技術運用程度不彰，原因可歸結為大部分之事業體並無從取得相關數據、所需之演算設備成本較高且不易取得、未建立合作關係共同解決研究障礙、並未認知到人工智慧技術之具體成效等。因此，NITI Aayog 提出下列幾點建議：

(1) 建立多元參與之市場

國家人工智慧市場（National AI Marketplace, NAIM）可分為：數據市場、數據標註市場、可部署模型之市場/解決方案市場。藉由該等市場之建立，可有效維護人工智慧產業之公平競爭、支援人工智慧研發之價值鏈，有利於建立合作關係、降低搜尋與標註數據之時間與成本、將多元解決方案部署於單一平台以發揮網絡效益。本報告進一步提倡應透過區塊鏈技術建立該等市場，以確保數據之可追溯性、存取控制、使用方式遵循本國與國際規範、數據價格之揭露機制。

政府之首要任務係建立該等市場之運作平台，讓任何需求方與供應方得藉由登入該平台之方式進行交易，同時，應針對該等交易模式訂定相關規範，包括：販售個人數據之規範與販售許可標準、匿名化標準、確保標註正確性之標準、進行可部署模型交易時網路安全之相關規範。

關於各市場之效益說明如下：

a. 數據市場

- 有效減緩資訊不對稱：藉由供需雙方於平台上進行交易，可降低數據獨占之情形、降低數據價差、有效帶動數據持有者與人工智慧研發者投入市場。
- 鼓勵各生產階段之專業化：若能夠輕易取得人工智慧之原始數據，便能讓研發者聚焦於特定生產活動，毋需為了取得數據，而涉足價值鏈的每個生產研發過程。
- 開啟新的數據來源、更有效率的運用計算效能與人力資源：現有之數據使用效率極低，藉由將數據商品化讓其在市場流通，可讓數據持有者與人工智慧研發者進行交易，讓數據被充分的運用於相關研究與生產活動。
- 消除數據分享之倫理擔憂：在未建立正式的數據交易市場前，大多數的數據分享並未取得資訊原始擁有者之同意，故應建立相關之資訊交易機制，讓原始數據擁有者得以行使同意權且獲得相應

之報酬。

b. 數據標註市場

其運作係將原始數據流通至市場，並藉由群眾外包之方式進行數據標註。善用相對低廉之外包方式，便可迅速完成大量數據之標註作業，惟其蘊含有標註錯誤之風險，故須藉由多重標註、案例測試、由專家驗證樣本等方式提升整體數據標註之正確性。

此外，由於數據標註須耗費大量之時間成本，故政府可建立獎勵制度，鼓勵群眾投入數據標註市場。

c. 可部署模型之市場

在此市場中可由企業家與政府共同提出相關實務問題，並由人工智慧研發者研擬對策，藉由展現其研究成果、將其研究商品化後予以交易。學術研究者也可從該市場中獲益，藉由市場之供需，瞭解目前應用端之實際問題，並取得相關產業數據。

(2) 建置大型標註資料集

政府應協助建置大型、跨領域數據語料庫 (corpora)，讓各事業體在印度語境 (context) 中應用人工智慧相關技術、降低新創之市場進入障礙、鼓勵國際專家於印度語境下研究人工智慧之相關問題。

(3) 建立夥伴關係

- a. 建立研究機構間之合作：為了將人工智慧技術運用到各個領域，應建立不同領域研究者之合作關係，例如，美國大學將不同領域之研究機構共同設置，以利不同單位協力進行研究；美國國防高等研究計畫署亦於學術機構中設置其研究設備，並且與私人企業保持合作。
- b. 藉由產業研究之協力方能持續擴展研究規模，並利用市場使用者之回饋持續改良初始研究。

- c. 與商業組織、創投合作有助於和其他市場參與者建立合作關係、順利運作可獲利之商業模式。蓋因商業組織、創投握有市場上之大量資訊、可協助尋求國際市場、遊說或與國內外組織協商較有利之交易規範。

#### (4) 提升人工智慧技術之市場曝光度

應由政府統一建立人工智慧資料庫入口網站，登載專業研究人員之資訊以及已完成之研究內容，並大量舉辦論壇、工作坊與現場展示、籌劃年度「人工智慧準備指數 (AI Readiness Index)」評比最佳應用典範。以該等機制增加人工智慧研究成果之曝光度，媒合市場潛在需求者與研發者。

#### (5) 協助新創

建立新創培育中心，提供新創事業相關場所與基礎設備；創設種子基金協助新創初期之營運，尤其係草創之初無法獲得創投資金之新創。

### 倫理、隱私、安全與人工智慧—負責任之人工智慧 (Responsible AI)

#### (1) 倫理與人工智慧

針對倫理之規範，政府應要求 COREs 與 ICTAIs 建立內部倫理委員會，負責擬定標準方針，並且監督該等研究機構之執行實效。而規範之重點包括：

- a. 公平性：應找出存有偏見之數據，評估該等數據對於後續演算之影響並除去其偏見，確保人工智慧技術之中性以及決策公平性。
- b. 透明度：諸多人工智慧之決策都面臨了黑箱之批評，揭露黑箱並非意味著須概括公開人工智慧系統之程式碼或相關技術，而是增進該等決策之可解釋性 (explainability)。

#### (2) 隱私與人工智慧

- a. 建立數據保護之法律架構：印度政府已針對數據保護法提出七大原則，包括告知同意、科技相容、數據控制者責任、數據簡化、整體應用、

懲罰性賠償、體系性執执行程序等。

- b. 建立業管法規架構：有別於一部統整性之隱私保護法，由於不同科技具有多元而快速變遷之特性，故針對不同領域之產業應與業者共同商議，訂定相應之管制架構作為隱私與安全保護之附加保護機制。
- c. 國家數據保護與隱私法之標準與國際標準一致化：歐盟於 2018 年 5 月通過 GDPR，對於隱私權保護制訂諸多規定。印度之制度應呼應此國際脈動，持續更新對於不同風險之規範內容。
- d. 鼓勵人工智慧技術研發者遵循國際標準：技術領導者與研發者應共同訂立標準，將 IEEE 發布之人工智慧倫理標準（The Global Initiative on Ethics of Autonomous and Intelligent Systems）自發性的適用於技術研發過程中。
- e. 提倡自律：數據隱私影響評估工具（Data Privacy Impact Assessment Tools）可用於協助人工智慧研發者與企業管理相關之隱私風險。
- f. 鼓勵 COREs 研究隱私維護之相關技術，或與研究該等技術之研究機構合作、資助研究該等領域之研究機構。
- g. 傳遞隱私權保護之認知。

### (3) 人工智慧之安全性

關於人工智慧之安全性，常聚焦於究責機制之討論上，惟 NITI Aayog 認為，更重要者應是如何辨別出產生變異之單位，並且遏制損害向未來發生。提出之具體措施如下：

- a. 相對於嚴格責任，應著重於對造成損害之人工智慧軟體進行過失判定（negligence test），此外，在技術研發之各階段，亦應自律性的執行損害影響評估之檢測。
- b. 若在研發過程中皆已踐行相關之檢測、監督與品質改良程序，則應建立安全港條款以阻卻或限制該等研發者之責任。



- c. 對於使用蘊含有人工智慧技術之商品所致之損害，應課以研發者比例責任而非連帶責任，尤其當該等商品之人工智慧技術應用係未被預期、被禁止、或與許可之使用方式不一致之情形，顯不應課以研發者過重責任。
- d. 應以實際受有損害為求償要件，若僅係推測性損害、有未來損害之虞，皆不得以此提起訴訟求償。

附錄四 「人工智慧之相關法規國際發展趨勢與因應」研討會資料

壹、研討會議程

時間	議程	主持／主講／與談
09:00~09:40	報到	
09:40~10:50	【場次一】 人工智慧發展下的著作權法制議題	<p>主持人：曾更瑩（理律法律事務所合夥人）</p> <p>報告人：王信仁（理律法律事務所資深律師）</p> <p>與談人（按筆劃順序）：</p> <ul style="list-style-type: none"> <li>■ 施立成（微軟全球助理法務長/台灣微軟公共暨法律事務部總經理）</li> <li>■ 徐維佑（資策會科法所創意智財中心組長）</li> <li>■ 莊弘鈺（交通大學科技法律學院助理教授）</li> <li>■ 謝銘洋（臺灣大學法學院教授）</li> </ul>
10:50~11:10	休息	
11:10~12:20	【場次二】 人工智慧與個人資料	<p>主持人：曾更瑩（理律法律事務所合夥人）</p> <p>報告人：黃耀賞（理律法律事務所律師）</p> <p>與談人（按筆劃順序）：</p> <ul style="list-style-type: none"> <li>■ 江耀國（中原大學法學院教授）</li> <li>■ 翁清坤（輔仁大學財經法律學系助理教授）</li> <li>■ 黃鐘揚（臺灣大學電機系暨電子所教授/優拓資訊共同創辦人）</li> <li>■ 楊立偉（意藍資訊董事兼總經理）</li> </ul>
12:20~13:20	午餐	
13:20~14:30	【場次三】 智慧載具發展下責任與風險的分配	<p>主持人：郭怡利（理律法律事務所資深律師）</p> <p>報告人：林中鶴（理律法律事務所法務專員）</p> <p>與談人（按筆劃順序）：</p> <ul style="list-style-type: none"> <li>■ 莊弘鈺（交通大學科技法律學院助理教授）</li> <li>■ 陳奕廷（景翊科技股份有限公司總經理）</li> <li>■ 黃銘傑（臺灣大學法律學院教授）</li> </ul>

14:30~14:50	休息	
14:50~16:00	<p>【場次四】</p> <p>人工智慧於醫療領域之應用</p>	<p>主持人：郭怡利（理律法律事務所資深律師）</p> <p>報告人：莊郁沁（理律法律事務所初級合夥人）</p> <p>與談人（按筆劃順序）：</p> <ul style="list-style-type: none"> <li>■ 呂適任（宏達國際電子股份有限公司虛擬實境研發部門經理）</li> <li>■ 李昂杰（資策會科法所價拓中心副主任）</li> <li>■ 李崇僖（臺北醫學大學醫療暨生物科技法律研究所副教授）</li> <li>■ 陳誌雄（交大科法所副教授兼所長）</li> <li>■ 游山逸（宏達國際電子股份有限公司 Sr. Director）</li> </ul>
研討會結束		

## 貳、研討會題綱

【場次一】 人工智慧發展下的著作權法制議題（時間 09:40 – 10:50）

主持人： 曾更瑩（理律法律事務所合夥人）

發表人： 王信仁（理律法律事務所資深律師）

與談人： 施立成（微軟全球助理法務長/台灣微軟公共暨法律事務部總經理）

徐維佑（資策會科法所創意智財中心組長）

莊弘鈺（交通大學科技法律學院教授）

謝銘洋（臺灣大學法學院教授）

**規劃議題一：有關人工智慧創作物，是否具「可著作權性」？而可受著作權法之保護？又如肯認人工智慧創作物可受著作權法保障，其權利歸屬又應如何認定？**

**背景說明**：隨著科技技術不斷發展，人工智慧已具有創作文學、音樂等作品之能力，且無論就外觀、內容，均與人類所為之創作已具有相當之類似性。於此種情形下，是否應肯認人工智慧創作物具有「可著作權性」，而應受著作權法之保護？關於此點，可資討論者，例如：

- 著作權法制原則上以「人」（包括自然人或法人）作為權利主體，而人工智慧非屬自然人或法人，是否、或在何種情形下亦可認定為「著作人」？
- 人工智慧所創作之作品，是否具有「原創性」而可取得著作權保護？
- 如肯認人工智慧創作之「可著作權性」，其權利歸屬又應如何認定？
- 在比較法上，各國法制之發展情形為何？

**規劃議題二：承規劃議題一，如肯認人工智慧創作物之「可著作權性」，則有關權利存續期間、作品保護範圍以及侵權責任等，又應如何處理？**

**背景說明**：如肯認人工智慧創作可取得著作權，因人工智慧並無所謂「死亡」的問題，且擁有能快速創作大量作品之能力，因此有關人工智慧創作物之權利存續期間、作品保護範圍以及侵權責任之認定，是否應有不同之考量？例如：

- 有關權利存續期間，是否應延長或縮短？
- 人工智慧創作物之作品保護範圍，是否應加以限制，以避免人類的創作範圍遭到壓縮？
- 如人工智慧創作如涉及侵害著作權行為時（包括侵權及被侵權之情形），關於侵權責任之認定，是否應予以調整？例如，是否應限定侵害行為之態樣？舉證責任之分配是否應調整？具體的救濟方法（損害賠償？除去侵害？防止侵害）是否亦有更動之必要？

【場次二】 人工智慧與個人資料（時間 11:10 – 12:20）

主持人： 曾更瑩（理律法律事務所合夥人）

發表人： 黃耀賞（理律法律事務所律師）

與談人： 江耀國（中原大學法學院教授）

翁清坤（輔仁大學財經法律學系教授）

黃鐘揚（臺灣大學電機系暨電子所教授/優拓資訊共同創辦人）

楊立偉（意藍資訊董事兼總經理）

**規劃議題一：為使個資利用更具彈性，我國個資法是否宜有限度開放去識別化及/或去連結化個資資料之利用？如是，宜採取何種配套措施（例如：訂定去識別化相關國家標準、禁止恢復其識別性、課予資訊揭露及安全維護等義務）？**

**背景說明：**大數據是人工智慧賴以發展的燃料，但前者有賴於巨量資料的整合與利用，追求資料價值開發的最大化，此與現行個資法資料蒐集最小化、目的拘束原則及當事人知情同意等要求未盡相符。為了在「避免人格權受侵害」及「促進個人資料之合理利用」間取得平衡，去識別化（de-identification）及假名化（pseudonymization）目前似為各國發展趨勢：

- **美國：**美國聯邦交易委員會於 2013 年報告書曾建議，以業者已採取合理去識別化措施為前提，可由業者公開承諾不再回復其識別性（違者將受到法律制裁），並透過契約限制下游業者進行再識別作為替代手段，藉此肯認該資料已無法合理連結至個人。
- **日本：**日本個資法規定，業者得將匿名加工資訊用於其他目的或提供予第三方，無須另外取得當事人同意，但同時課予業者禁止再識別、資訊揭露及安全維護等義務作為配套。
- **歐盟：**相較於美國及日本，GDPR 雖已區分「匿名化資料」（anonymous information）及「假名化資料」（personal data which have undergone pseudonymisation），並肯認去連結化能夠減少當事人風險、有助於資料控管者/處理者符合資料保護義務，但 GDPR 仍將去連結化看作一種安全防護措施，僅在其他目的相容於原先蒐集目的之前提下，允許資料控管者/處理者將個人資料用於其他目的。

**規劃議題二：因應資料側寫及自動化個人決策等技術之發展與應用，就特定新興個資利用方式，我國個資法是否宜賦予當事人反對權及資訊提供權？**

**背景說明：**隨著大數據分析技術日益成熟，透過資料分析對個人進行評價、預測其行為模式的資料側寫（profiling），逐漸被廣泛運用在信用評價、精準行銷及人員招募等領域，據以作為自動化個人決策（automated individual decision-making）的基礎。其次，人工智慧所使用的類神經網絡及深度學習，使得機器能夠具備自主學習的能力，但也導

致其運算過程不易透過人類所能理解的方式加以說明及驗證，欠缺透明度及可非難性，因而成為「黑盒子」，對人民正當法律程序的保障構成極大的挑戰。

- **現行法架構：**我國個資法雖規定當事人有請求停止蒐集、處理或利用其個人資料的權利，但在原先蒐集目的消失或契約約定保存期限屆滿前，當事人恐怕無法要求公務機關或非公務機關停止特定處理行為，因此，即便資料蒐集者透過資料側寫對當事人作成自動化個人決策，當事人亦無從置喙，僅得透過解除契約或撤回同意等釜底抽薪的方式，才能阻止資料蒐集者透過資料側寫對其作成自動化個人決策，對於當事人權益的保護似有未周。

其次，我國個資法雖規定資料蒐集者應告知當事人個人資料之利用方式，然而，前述規定是否足以要求公務機關或非公務機關向當事人說明人工智慧背後的演算法如何運作，尚非無疑。

- **歐盟：**GDPR 規定資料控管者/處理者在資料側寫前，必須先評估該等處理對個資保護的影響，賦予當事人對資料側寫表示反對、不受自動化個人決策拘束的權利，並要求資料控管者/處理者必須採取適當措施保護當事人權利、自由及正當利益（其中至少應確保部分的人為介入、表達意見及反對其決定的權利）。

此外，GDPR 進一步要求資料控管者/處理者採用自動化決策（包括資料側寫在內）時，應提供當事人其背後邏輯操作的實質資訊（meaningful information about the logic involved），以及該等處理對當事人的重要性及設想的後果為何。

【場次三】 智慧載具發展下責任與風險的分配（時間 13:20 – 14:30）

主持人： 郭怡利（理律法律事務所資深律師）

發表人： 林中鶴（理律法律事務所法務專員）

與談人： 莊弘鈺（交通大學科技法律研究所助理教授）

陳奕廷（景翊科技股份有限公司總經理）

黃銘傑（臺灣大學法律學院教授）

**規劃議題一：**針對自駕車的測試，行政院參考美國加州及新加坡的立法例，借鏡監理沙盒的理念，推出無人載具科技創新實驗管理條例草案。我國是否適宜採監理沙盒模式，並宜採取何種配套措施（例如：測試資料的合理開放運用及允許商用的法規調適）

**背景說明：**我國既有以人為駕駛車輛為基礎的公路法、道路交通管理處罰條例及其相關辦法，與自駕車的性質多所扞格，不利於自駕車之測試及開發。為促進自駕車測試及開發，似有另訂測試或實驗管理條例以鬆綁現行法規之必要。

- **美國：**針對測試尚無聯邦層級規範，但交通部持續釋出建議性的指引，以促進全國監理政策的一致性。各州大都提出自己的自駕車法案，其中加州車輛管理局 2014 年依授權訂定自駕車輛測試規範，開放測試申請，並於 2018 年修正規範，開放遠距操作（車內無人）的試驗申請與商用。
- **新加坡：**於 2017 年的道路交通法修正中授權交通部建議自駕車的測試及上路規定，並就經許可測試及上路之自駕車，得排除特定相關法令之適用。
- **德國：**維也納道路交通公約修正，使自駕技術可運用於交通實務，但以駕駛可選擇關閉該技術為前提。德國 2017 年 3 月相應修正道路交通法，將駕駛人定義延伸包括使用不同程度自駕系統者，允許高度與完全自動駕駛系統上路。
- **日本：**警察廳於 2016 年 6 月公布自動駕駛系統道路實驗指引，明訂實驗符合一定條件即可不拘時間、場所實施。另因應自駕車放寬道路運輸車輛安全基準規定，並針對遠距操作（車內無人）進一步設置安全基準鬆綁認定制度。此外，亦在地方振興的觀點下，擬修法於特定地區針對自駕車及無人機引進監理沙盒制度。

**規劃議題二：**自駕車輛於自動駕駛模式下運行導致的第三人事故，其民事責任歸屬為何（所有權人、使用人/駕駛人、製造商）？是否宜課予製造商較重責任（如推定過失），或宜採用其他制度性解決方案（如建立賠償基金及提供保險要求），以平衡產業發展與用路人的安全。

**背景說明：**針對自駕車的定義，一般採用 SAE J3016 的分級（最新修訂為 2018 年 6 月版），分為 0~5 級，主要是從(1)自動駕駛系統可承擔之動態駕駛任務的範圍、(2)自動駕駛系統正常運作的操作適用範圍、及(3)自動駕駛系統的全面運作下是否期待人為接管的三個觀點進行分類。自等級 3 起，自動駕駛系統已可於特定操作運用範圍內承擔全部的自動駕駛任務(等級 3 尚期待在運作困難系統請求時，駕駛人必須提供適當介入支援，

但等級4則無此期待)。因不同等級的自駕車在可自動駕駛範圍及人為接管上均有差異，在政策上所有權人、使用人/駕駛人或製造商所負擔之注意義務亦似應隨之調整。

- **現行法架構：**一旦發生第三人事故，在我國現行法下，無論該第三人係依侵權行為相關規定，或依契約或消費者保護法（符合當時科技或專業水準可合理期待之安全性）請求損害賠償，但在自動駕駛模式下，無論求償對象或舉證責任均較非自動駕駛車輛複雜。
- **美國：**如美國加州透過道路測試之許可證，要求申請許可之企業需購買不低於美金500萬元之保險或出具同等金額之保證函，以確保自動駕駛所造成之損害得以在特定範圍內被填補，美國一些其他州也有類似規定。
- **英國：**於自動與電動汽車法案中，建立自駕車發生事故的第三人責任保險和責任規則。就處於自動駕駛（driving itself）模式下之自駕車發生事故，依據該車輛是否投保，分別要求由保險公司（已投保之情形）和車主（未投保之情形）對事故造成的損失承擔賠償責任。本法案規定如汽車於發生事故時是處於自動駕駛的狀態，則將第三人責任保險的涵蓋範圍擴張至駕駛自身。
- **其他：**日本政策研究報告亦有建議依據自動駕駛事故類型為不同之損害賠償責任分配，另有設立賠償基金之芻議，除能補充保險制度之不足外，在政策設計上亦可能配套減輕汽車製造商之責任。



【場次四】 人工智慧與醫療服務（時間 14:50 – 16:00）

主持人： 郭怡利（理律法律事務所資深律師）

發表人： 莊郁沁（理律法律事務所初級合夥人）

與談人： 呂適任（宏達國際電子股份有限公司虛擬實境研發部門經理）

李昂杰（資策會科技法律研究所價值拓展中心副主任）

李崇僖（臺北醫學大學醫療暨生物科技法律研究所副教授）

陳誌雄（交大科法所副教授兼所長）

游山逸（宏達國際電子股份有限公司 Sr. Director）

**規劃議題一：為提升醫療品質，並兼顧患者安全，我國是否仍依藥事法第 13 條、醫療器材管理辦法，將與醫療有關之人工智慧技術列為醫療器材進行管理？如是，主管機關查驗登記審查程序是否足以確保人工智慧技術的品質、安全性及有效性？如否，是否應透過其他機制予以監督？**

**背景說明：**依據藥事法第 13 條規定，所謂醫療器材，係用於診斷、治療、減輕、直接預防人類疾病、調節生育，或足以影響人類身體結構及機能，且非以藥理、免疫或代謝方法作用於人體，以達成其主要功能之儀器、器械、用具、物質、軟體、體外試劑及其相關物品；如屬前揭醫療器材定義範疇，則由衛生福利部，依醫療器材管理辦法進行管理。雖衛福部食品藥物管理署已於 2015 年 4 月 13 日公布《醫用軟體分類分級參考指引》，提供產業界釐清醫用軟體之範疇，提供醫用軟體參考判定原則，惟人工智慧技術面向多元，在無法確認產品之分類分級時，仍需依醫療器材管理辦法第 6 條規定，以個案送件申請分類分級判定為準。為了能夠使用人工智慧技術提升醫療品質並兼顧患者安全，逕對軟體醫療器材增設專門條款，賦予軟體醫療器材明確定義及分類，似為目前國際發展趨勢：

- **歐盟：**歐盟已於 2017 年發布《醫療器材法》，將自 2020 年 5 月 26 日起取代《93/42/EEC》指令，該法已針對軟體醫療器材制訂專門條款，且第 2 條第 1 項已將具有預後之預測（prediction of prognosis）目的的醫療軟體列為醫療器材，而受《醫療器材法》規制。歐盟法院 2017 年在《法國飛利浦案》亦指出，軟體得否作為醫療器材應以製造商意圖使其用作醫療用途為斷，非因該軟體於醫療場合使用而使其成為醫療器材。該判決不僅為《93/42/EEC》指令及《2017/47/EC》指令背書，同時亦與《醫療器材法》觀點相同。
- **美國：**依據《聯邦食品、藥物及化妝品法》規定，醫療器材係由美國食品藥物管理局（簡稱 FDA）管理，若人工智慧技術被列為醫療器材時，則由 FDA 進行規範。對此，FDA 已陸續出具指南（Guidance），逐步規範軟體醫療器材。其中，受 FDA 規範的軟體醫療器材類型分別為：行動醫療應用程式（MMAs）、醫療器材資料系統（MDDS）、軟體醫材（SAMD）、臨床決策支持系統（CDSS），而《21 世紀

醫療法案》已將提供醫師醫療意見但仍由醫師獨立審查該意見的軟體排除於醫療器材的定義範圍。

**規劃議題二：**為使人工智慧技術在醫療領域蓬勃發展，有關病歷、醫療、基因、健康檢查等個人資料（簡稱「健康個人資料」）之蒐集、處理、保存與傳輸必不可免。因此，如何在《一般資料保護規範》（簡稱《GDPR》）及我國《個人資料保護法》的施行下，適度放寬此等健康個人資料處理保護，以促進科技發展、提升醫療品質，並兼顧相關隱私權保障及防範個人資料侵害？

**背景說明：**全球生醫界近年來積極投入「精準醫療」（Precision Medicine），透過傳統醫療常規檢查，輔以生物醫學檢測及基因資料庫比對分析，以提供病患最佳個人化醫療服務；然人工智慧技術的運用、分析巨量資料庫等，均仰賴健康個人資料之蒐集、流通、利用或保存。惟各國不僅未針對生物基因資料庫的健康個人資料制訂專法，同時《GDPR》及我國《個資法》更將健康個人資料列為特種類型個人資料，規定不得蒐集、處理或利用，而人工智慧技術醫材商、基因體科技公司等，由於非屬公務機關、學術研究機構或醫療院所，故無從使用健康個人資料，以提升醫療服務品質。因此，如何適度放寬《GDPR》第9條、我國《個資法》第6條，並兼顧相關隱私權保障及防範個人資料侵害，將會是我國及世界各國共同面對的課題。

- **現行法架構：**我國個資法第6條第1項規定，有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。由於人工智慧技術醫材商或基因體科技公司等非屬公務機關、學術研究機構或醫療院所，故無從依但書第1款至第5款蒐集、處理或利用健康個人資料，僅能依第6款取得當事人書面同意後，始得使用健康個人資料；衛福部衛生福利資料應用管理要點亦規範，衛生福利相關產業基於研究發展需要，得申請使用取得當事人書面同意之特定衛生福利資料。然而，人工智慧技術本質上的特殊性（硬體加軟體），以及無從知悉、預測基因資料庫的過程與結果，將使醫材商、基因體科技公司無法特定取得目的之必要範圍，而無從取得當事人同意，進而使用健康個人資料，致有礙人工智慧技術於醫療領域的蓬勃發展。
- **歐盟：**歐盟過去個人資料係由《數據保護指令》規範，自2018年5月25日起，由《GDPR》進行規範。依據《GDPR》第9條規定，基因資料、生物特徵識別資訊或與健康相關資訊（即健康個人資料）屬於特殊類型，不得進行個人資料處理。雖然《GDPR》列明於例外情形下，得使用健康個人資料，惟目前在醫療領域研發人工智慧技術者多為醫材商、基因體科技公司等營利組織，且是否使用生物醫學檢測及基因資料庫比對，並非醫療服務上的必要措施。此外，醫療服務大多針對個人提供，又難稱符合公共利益，再加上人工智慧技術的特殊性（硬體加軟體），致其無從取得當事人同意，故醫材商、基因體科技公司在《GDPR》的規範下，無法使用健康個人資料。因此，如何在醫療人工智慧領域適度放寬健康個人資料的運用，兼顧個人資料保護，仍是歐盟尚須解決的新問題。

**規劃議題三：**由於醫療人工智慧技術係由硬體與軟體組成，故是否應按消費者保護法第7條規定，逕將其視為純粹商品而有商品責任規範的適用，課予製造商或研發者嚴格的民事責任？

**背景說明**：隨著科技蓬勃發展，人工智慧技術在醫療領域大幅度使用，則其產品瑕疵及造成損害的可能性亦隨之提升，而人工智慧技術本質係由硬體與軟體組成，應有商品責任規範之適用。惟其進行臨床診斷與治療決定時的特殊性（黑盒子醫學），能否將其視為純粹商品而有商品責任規範的適用，不無疑問。

- **現行法架構**：依據消費者保護法第 7 條第 1 項規定，從事設計、生產、製造商品或提供服務之企業經營者，於提供商品流通進入市場，或提供服務時，應確保該商品或服務，符合當時科技或專業水準可合理期待之安全性。由於在醫療領域研發人工智慧技術者多為醫材商或生技公司，屬於企業經營者，故該醫療人工智慧技術即屬商品，於致生消費者或第三人損害時，醫材商或生技公司即負有商品責任。惟人工智慧技術本身即有難以預測之特質，若逕將其視為純粹商品，課予製造者或研發者商品責任，恐有礙科技進步，並延緩醫療產業發展。因此，能否逕以消費者保護法作為課予研發、製造醫療人工智慧技術者的依據，尚非無疑。
- **歐盟**：目前依據歐盟《第 85/374/EEC 號指令》，電子醫療技術的製造商、進口商、供應商應就產品瑕疵所造成之損害或傷害負損害賠償責任。惟該指令僅就製造者課予嚴格的產品瑕疵責任，並未考量使用醫療人工智慧技術進行診斷與治療的複雜性。而英國雖無相關法規，惟其已意識到有必要重新制訂與醫療人工智慧技術有關的責任法規，因此已召集有關人士針對該議題進行分析討論。
- **美國**：美國目前亦無相關法規或案例，惟似可考量 FDA 對於軟體品質管理的指南，且製作及行銷醫療器材的公司應有全面性的系統確保產品的安全性及品質。若醫療人工智慧軟體本身有缺陷或是品質不佳時，該軟體研發者即應負有責任。惟美國法院傾向拒絕要求軟體研發者或是軟體出賣人承擔產品瑕疵責任，對於注意義務程度，亦僅要求至「合理」（reasonable），而非「完美」（perfect），畢竟即使以最佳實行原則研發軟體產品，其仍會有編碼上的瑕疵，難以避免。

## 參、研討會簡報

### 場次一：人工智慧發展下的著作權法制議題



Photo by Franck V. on Unsplash

理律法律事務所  
LEE AND LI  
ATTORNEYS-AT-LAW

議題一

有關人工智慧創作物，是否具「可著作權性」，而可受著作權法之保護？又如肯認人工智慧創作物可受著作權法保障，其權利歸屬又應如何認定？

Photo by Johnny Goerend on Unsplash

1



Photo by Johny Goerend on Unsplash

## 議題二

承議題一，如肯認人工智慧創作物之「可著作權性」，則有關權利存續期間、作品保護範圍以及侵權責任等，又應如何處理？

2



Photo by Franck V. on Unsplash

## 議題一

人工智慧創作的可著作權性及其權利歸屬

- 著作權法制原則上以「人」（包括自然人或法人）作為權利主體，而人工智慧非屬自然人或法人，是否、或在何種情形下亦可認定為「著作人」？
- 人工智慧所創作之作品，是否具有「原創性」而可取得著作權保護？
- 如肯認人工智慧創作之「可著作權性」，其權利歸屬又應如何認定？
- 在比較法上，各國法制之發展情形為何？

3





Photo by Franck V. on Unsplash

#### 美國

著作須有人類創作性的投入或干預，人工智慧創作倘無法追溯至人類作者，即不受著作權保護。

為給予 AI 開發者投身人工智慧開發之誘因，應賦予人工智慧創作著作權之保護，惟不應變動既有以人類為本位的法律制度。

透過類似雇用作品原則之法理，將 AI 創作之著作權歸於人類，特別是貢獻最多的開發者或出資者，再透過 EULA 授權予使用者。

4



Photo by Franck V. on Unsplash

#### 歐盟

著作須有原創性、由著作人做出自由而富有創意的選擇、為其個人的精神創作，始受著作權之保護

開發者僅為人工智慧創作物提供可能性，最終完成的作品並非其所能預測，而使用者雖未提供其創意，但已付出對價獲得人工智慧使用權，賦予使用者人工智慧創作之著作權可平衡雙方利益。

5



## 🇬🇧 英國

1988年「著作權、設計與專利法」(Copyright, Designs and Patents Act)就「電腦生成著作」(沒有人類作者的狀況下,電腦所產出的作品)設有權利保障規定。

著作須有原創性:非屬抄襲的創作,並切必須考量創作過程中作者所投入的技巧、判斷與勞力。



## 🇬🇧 英國

司法實務上,法院並未運用前述規定積極認定「電腦生成著作」的著作權,反而較消極地認為:「係人類有意識地操作機器、輸入指令,著作才得已完成,電腦僅有輔助的功能」。

著作權的歸屬,應於個案中判斷何者為「為創作作品而作出必要安排之人」。





Photo by Franck V. on Unsplash

## 澳洲

現行法下，著作權歸屬於「作者」，作者必須為「合格的人」(qualified person)，意指澳洲公民或在澳洲居住。解釋上，限於「人」(依據「法律解釋法」(Acts Interpretation Act)，係指個人、國家或法人團體，不包括機器)。

著作須有原創性認定，必須考量創作過程中作者所投入的技巧、判斷與勞力。

8



Photo by Franck V. on Unsplash

## 澳洲

司法實務上，並未認可「電腦生成著作」的著作權，學說上，有基於「鼓勵論」的觀點，認為宜修正著作權法，將電腦生成著作與人類的著作脫勾處理，承認電腦生成著作的著作權。

9





Photo by Franck V. on Unsplash

## • 日本

著作須有原創性認定，並強調著作必須為「具思想或感情」之創作（著作權法第2條第1項）；另有強調必須是「創作者的個人個性表現」的見解。

「創作」必須是實質參與創作的行為。依實務見解，單純提供資金或給予補助的行為，並非創作；但如係就創作的細節給予指示，則可認為係創作行為。

10



Photo by Franck V. on Unsplash

## • 日本

基於「鼓勵論」的觀點，學說多認為應給予人工智慧創作物一定的權利保障。

「多層」的思考判斷方式：

- 「學習用資料」、「人工智慧程式」、「學習完成模型」、「人工智慧生成物」
- 「物權性質（排他性）的權利設定」、「促進利用的權利設定」

11



Photo by Franck V. on Unsplash

## 中國大陸

現行法下，著作權的保障要求作品必須為「思想或情感的表達」，且必須是經由「主觀的思考」所產生。人工智慧生成物欠缺此等要件，尚不能受有著作權的保障。

基於「鼓勵論」的觀點，學說多認為應給予「人工智慧生成物」一定的權利保障。

有學說認為可直接給予「著作權」保障，亦有認為僅給予「鄰接權」的保障即可。

12



Photo by Franck V. on Unsplash

## 議題一：各國趨勢整理

- 關於人工智慧創作的可著作權性，各國仍強調「原創性（「創作性」）」，強調「人的參與」。
- 基於「鼓勵論」的觀點，多認為應給予「人工智慧創作物」一定的權利保障。
- 關於人工智慧創作物的著作權歸屬，多依「人的參與程度」加以認定。

13





Photo by Franck V. on Unsplash

## 議題二

### 人工智慧創作的權利存續期間及侵權責任

- 有關權利存續期間，是否應延長或縮短？
- 人工智慧創作物之保護範圍，是否應加以限制，以避免人類的創作範圍遭到壓縮？
- 如肯認人工智慧創作之「可著作權性」，其權利歸屬又應如何認定？如人工智慧創作如涉及侵害著作權行為時（包括侵權及被侵權之情形），關於侵權責任之認定，是否應予以調整？
- 在比較法上，各國法制之發展情形為何？

14



Photo by Franck V. on Unsplash

### 美國

關於權利存續期間：  
適用雇用作品原則，即以發布日起 95 年或創作日起 120 年，孰早屆期為準。

關於侵權責任：  
人工智慧無法起訴或應訴，因此有關侵權責任的問題，仍應回歸由「人」來處理。也因此，相關問題與處理「人」的著作權並無不同。

15



Photo by Franck V. on Unsplash

## 英國

關於權利存續期間：  
1988年「著作權、設計與專利法」(Copyright, Designs and Patents Act)已規定：自「完成該著作」之年年底起算至第50年之年底。已與著作人之生命存續與否脫勾。

16



Photo by Franck V. on Unsplash

## 歐盟

關於權利存續期間：  
目前歐盟相關法令均以「著作人為人類」作為前提，因此有關權利存續期間的認定，亦以「著作權人生命有限」為前提。但人工智慧可永續存在，因此如承認人工智慧創作物的著作權保障，權利存續期間的規範亦應予以修正。

關於侵權責任：  
歐洲議會曾建議賦予人工智慧「電子人」的地位，以解決人工智慧創作物的侵權責任問題，惟執委會並未採納，且多數專家亦表示反對。

17





Photo by Franck V. on Unsplash

## ● 日本

關於權利存續期間：

1. 「無方式主義」或「形式主義」
2. 確保投資的回收
3. 國內保障與國際保障的平衡

關於保障範圍：

1. 著作財產權、著作人格權？
2. 鄰接權？
3. 「高價值」權利始予以保障？

關於侵權責任：

1. 人工智慧可大量創作、迅速創作
2. 「依據性」的認定
3. 舉證責任的分配應予以調整？
4. 以「列舉方式」加以規範？
5. 責任主體？
6. 具體的救濟內容(除去請求權、防止請求權、損害賠償請求權?)

18



Photo by Franck V. on Unsplash

## ■ 中國大陸

關於存續期間：

1. 現行法規定：
  - 自然人：著作人終生及死後50年
  - 法人：作品發表後50年
  - 人工智慧生成物：必須與「人」做不同處理
2. 「鄰接權論者」的觀點：
  - 自發表日起算10年。

關於保護範圍：

1. 著作財產權、著作人格權
2. 鄰接權

關於侵權責任：

學習階段的重製行為，可否認為是「合理使用」的類型？

19



Photo by Franck V. on Unsplash

## 議題二：各國趨勢整理

- 關於權利存續期間：  
應與「人」的著作權保障作不同處理；與「人」的生命存續與否脫勾。
  
- 關於保障範圍：
  - 不保障著作人格權
  - 鄰接權的保障
  
- 關於侵權責任的認定：
  - 與「人」的侵權責任相同？
  - 依據人工智慧的特性進行調整

20

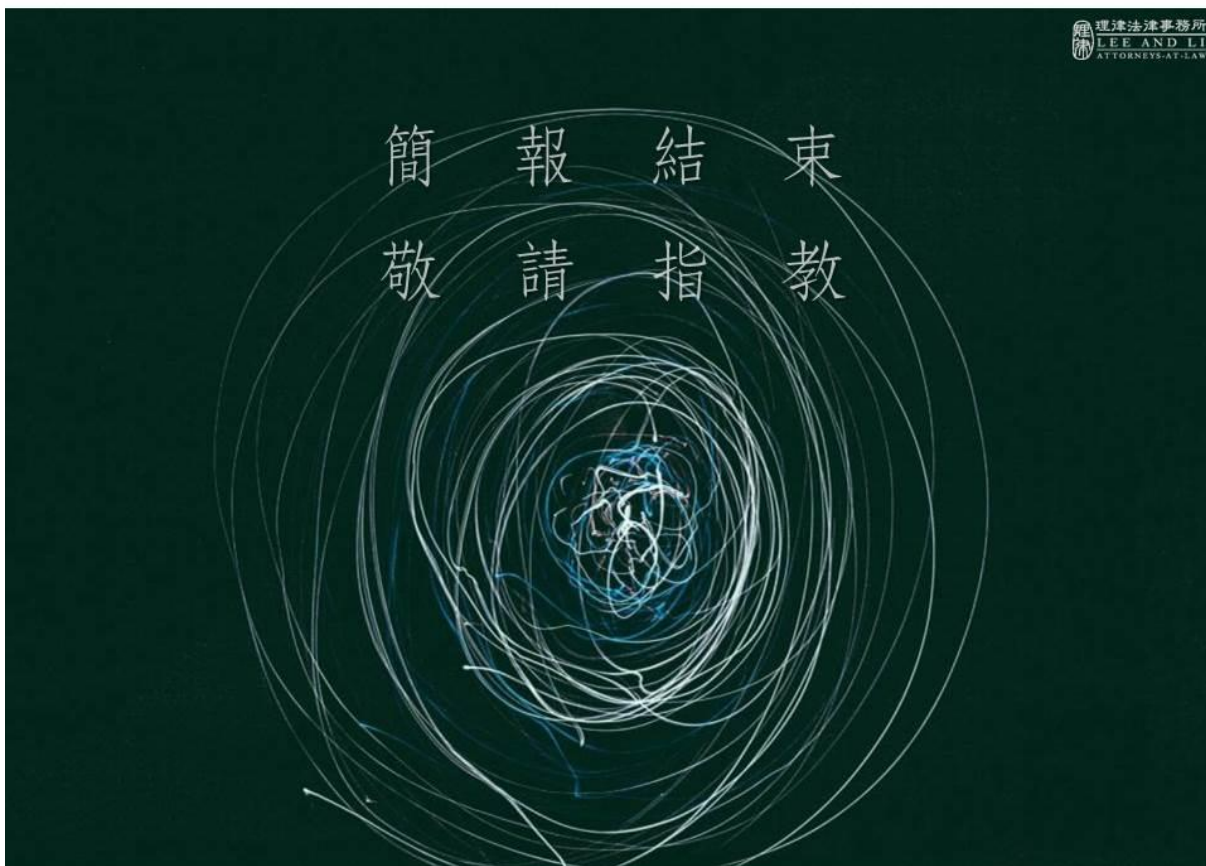


Photo by Gertrūda Valasevičiūtė on Unsplash

21

## 場次二：人工智慧與個人資料



理律法律事務所  
LEE AND LI  
ATTORNEYS-AT-LAW

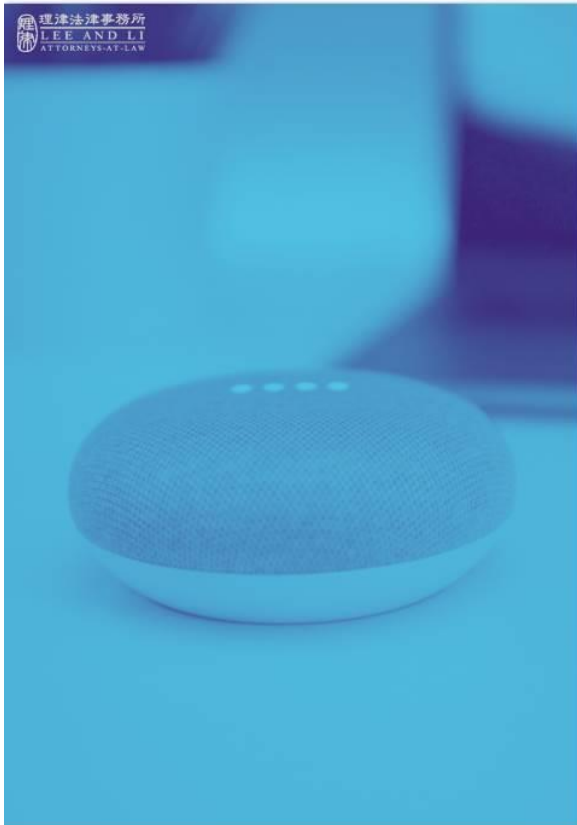
人工智慧之相關法規國際發展趨勢與因應研討會

【場次二】

### 人工智慧與個人資料

報告人：黃耀賞(理律法律事務所律師)

Photo by Franck V. on Unsplash



理律法律事務所  
LEE AND LI  
ATTORNEYS-AT-LAW

隨著電腦視覺、語音辨識及自然語言處理等技術日益進步，以及物聯網、大數據分析快速發展，具備機器學習能力的人工智慧，正逐漸滲透至人類生活的各種面向

- 👁️ 電腦視覺
- 🗣️ 語音辨識
- 🗣️ 自然語言處理
- 🌐 物聯網
- 0101  
1001 大數據分析
- 🧠 機器學習

Photo by Kevin Bhagat on Unsplash

1





Photo by Kevin Bhagat on Unsplash



從智慧音箱到家用機器人，  
從運用大數據分析的精準行銷到虛實整合的無人商店，  
智慧家庭及智慧零售的願景正在實現當中

而身處其中的你我，一舉一動都將被無所不在的感測器、網路追蹤工具記錄下來，成為大數據分析的素材及人工智慧賴以發展的燃料



2



Photo by Kevin Bhagat on Unsplash

**避免人格權受侵害**  
緩和AI應用上對個資保護  
可能帶來的衝擊



**促進個人資料合理利用**  
避免我國人工智慧發展  
因受制於既有法制而錯失良機

3



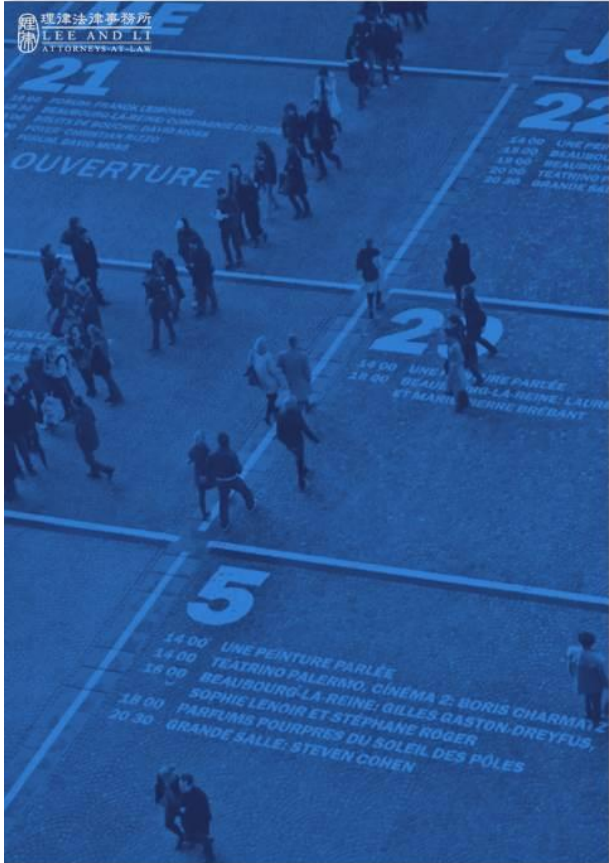


Photo by Curtis MacNewton on Unsplash

## 挑戰一

資料量的急劇增長及複雜演算法的持續發展，使得資料間的聚合及連結變得更加容易，過往許多被認為已經去識別化的資料，將有可能因技術發展而重新獲得可識別性，進而形成個人資料保護的漏洞

4

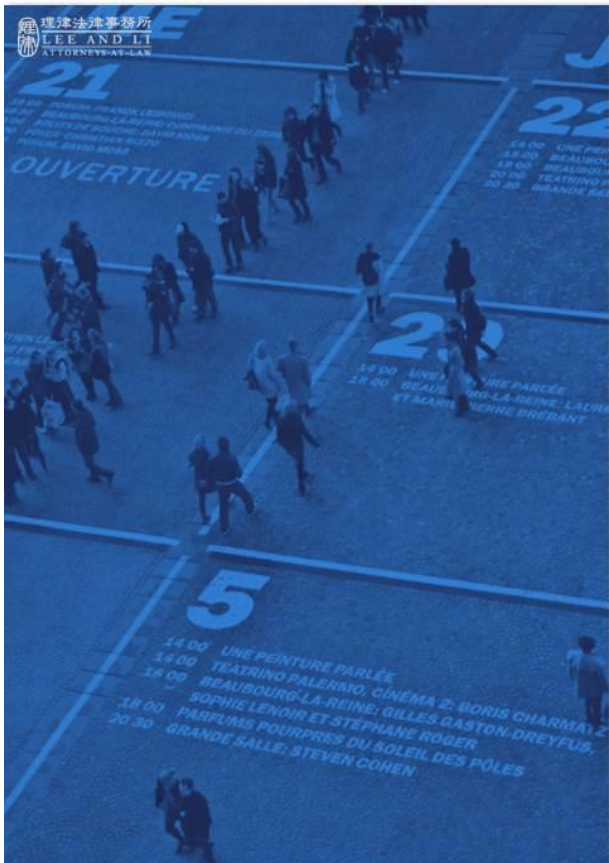


Photo by Curtis MacNewton on Unsplash

## 美國 PCAST

大數據分析技術的發展使得資料的去識別化日益受到挑戰，隨著人們愈來愈容易取得大量且多樣的資料，再識別的可能性也顯著提高

5

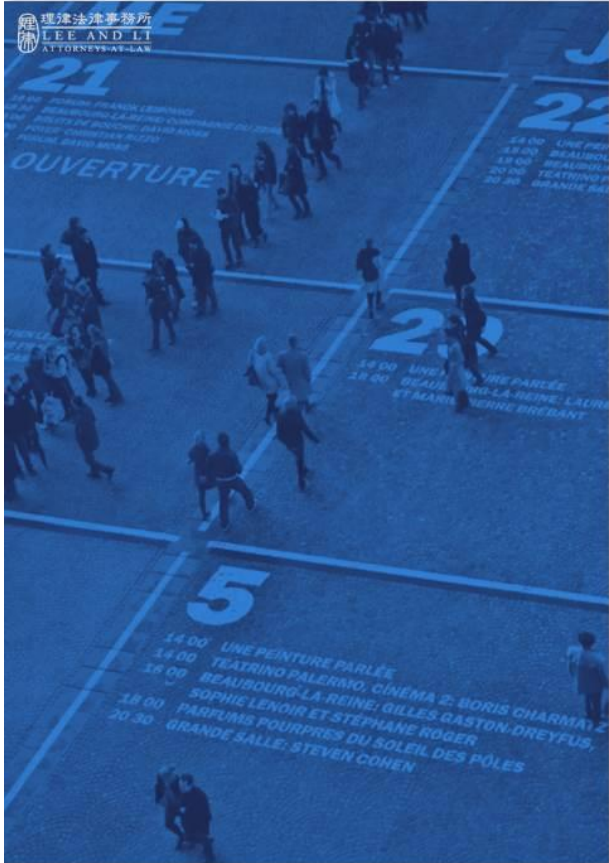


Photo by Curtis MacNewton on Unsplash

## 英國 GO-Science

人工智慧能夠從公開資料中推衍出某些私人資訊，而隨著公開可得資料逐漸增加及人工智慧技術的發展，重新識別個人的可能性也變得愈來愈高，因而組織必須定期檢視既有的保護措施是否足夠

6

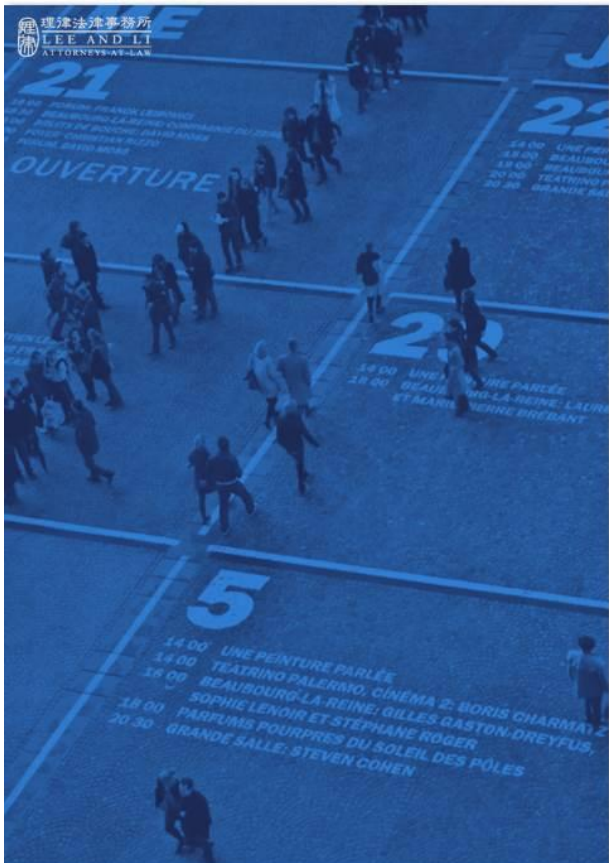


Photo by Curtis MacNewton on Unsplash

## 挑戰二

大數據分析及機器學習的發展有賴於鉅量資料的整合與利用

然而，當前以資料蒐集最小化、目的拘束原則及當事人知情同意等作為基礎的隱私保護框架，卻使資料保有者受限於原先的蒐集目的及告知範圍，無法充分利用個人資料進行創新與轉型

7



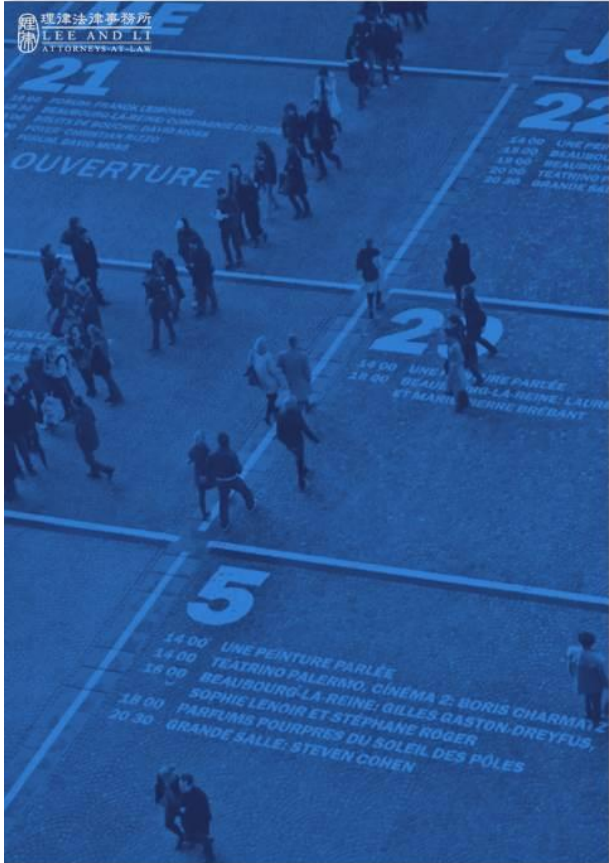


Photo by Curtis MacNewton on Unsplash

避免人格權受侵害

VS

促進個人資料合理利用

有限度開放去識別化及去連結化資料之利用，並透過法律禁止再識別，似乎是國際間值得觀察的發展趨勢之一

8



Photo by Curtis MacNewton on Unsplash

美國

美國聯邦交易委員會於2013年報告書曾建議，以業者已採取合理去識別化措施為前提，可由業者公開承諾不再回復其識別性（違者將受到法律制裁），並透過契約限制下游業者進行再識別作為替代手段，藉此肯認該資料已無法合理連結至個人

9

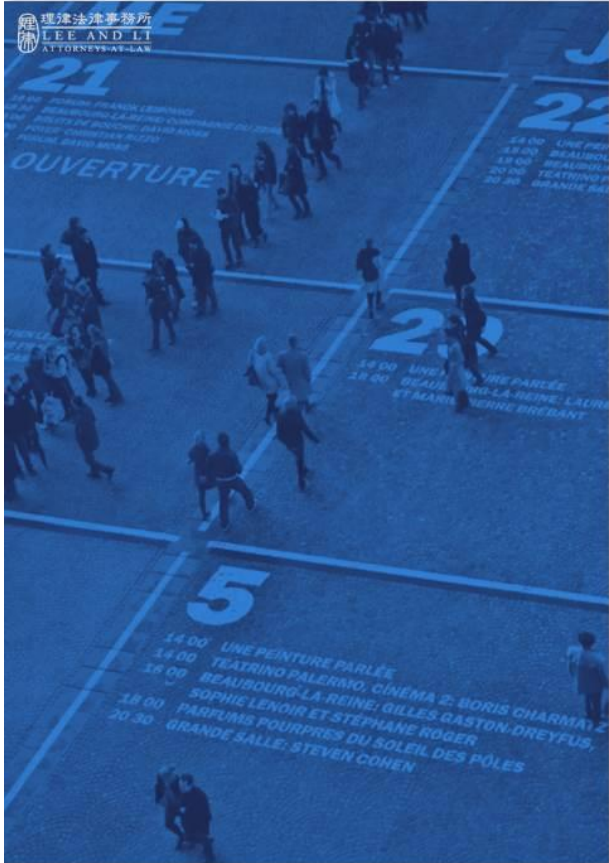


Photo by Curtis MacNewton on Unsplash

## ● 日本

日本個資法規定，業者得將匿名加工資訊用於其他目的或提供予第三方，無須另外取得當事人同意，但同時課予業者禁止再識別、資訊揭露及採取安全維護措施等義務作為配套

10



Photo by Curtis MacNewton on Unsplash

## ■ 歐盟

GDPR雖肯認去連結化能夠減少當事人風險、有助於資料控管者/處理者符合資料保護義務，但GDPR仍將去連結化看作一種安全防護措施，僅在其他目的相容於原先蒐集目的之前提下，允許資料控管者/處理者將個人資料用於其他目的

11



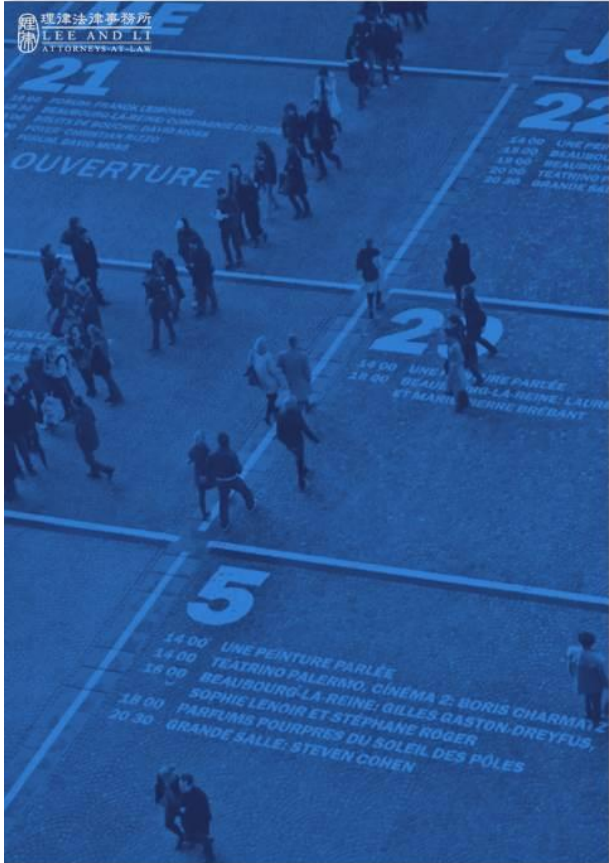


Photo by Curtis MacNewton on Unsplash

### 議題一

為使個資利用更具彈性，我國個資法是否宜有限度開放去識別化及/或去連結化資料之利用？

如是，宜採取何種配套措施？例如：訂定去識別化相關國家標準，或課予禁止恢復其識別性、資訊揭露及採取安全維護措施等義務？

12



Photo by Ian Espinosa on Unsplash

### 挑戰三

隨著大數據分析技術日益成熟，透過資料分析對個人進行評價、預測其行為模式的資料側寫，逐漸被廣泛使用在信用評價、精準行銷及人員招募等領域，用來預測其行為模式，並據以作為自動化個人決策的基礎

13



Photo by Ian Espinosa on Unsplash

### 挑戰三

但面對人工智慧時代下全新的個資利用方式，特別是資料側寫及自動化個人決策的應用，現行個資法下當事人就其個人資料所享有的權利，似乎已不足以應付該等新興技術對個人權益可能帶來的侵害

14



Photo by Ian Espinosa on Unsplash

### 台灣

我國個資法雖規定當事人有請求停止蒐集、處理或利用其個人資料的權利，但在原先蒐集目的消失或契約約定保存期限屆滿前，當事人恐怕無法要求公務機關或非公務機關停止特定處理行為，僅得透過解除契約或撤回同意等釜底抽薪的方式才能加以阻止，對於當事人權利的保護似有未周

15





Photo by Ian Espinosa on Unsplash

## 🇹🇼 台灣

此外，我國個人資料法雖規定資料蒐集者應明確告知當事人個人資料利用之方式，但前述規定是否足以要求資料蒐集者必須向當事人說明人工智慧背後的演算法如何運作，實非無疑

16



Photo by Ian Espinosa on Unsplash

## 🇺🇸 美國

公平信用報告法規定消費者調查機構彙編及出售含有消費者資訊的報告，而該等資訊被用來判定消費者是否能夠進行交易或享有特定福利時

消費者調查機構應執行合理程序，在最大範圍內確保消費者報告的準確性，並提供聯絡管道，以便消費者能夠藉此改正任何錯誤

17



Photo by Ian Espinosa on Unsplash

## ■ 歐盟

GDPR規定資料控管者/處理者在資料側寫前，必須先評估該等處理對個資保護的影響，賦予當事人表示反對、不受自動化個人決策拘束的權利，並要求資料控管者/處理者必須採取適當措施保護當事人權益

至少應確保部分的人為介入、表達意見及反對其決定的權利

18



Photo by Ian Espinosa on Unsplash

## ■ 歐盟

GDPR進一步要求資料控管者/處理者採用自動化決策(包括資料側寫在內)時，應提供當事人其背後邏輯操作的實質資訊，以及該等處理對當事人的重要性及設想的後果為何

19





Photo by Ian Espinosa on Unsplash

## 議題二

因應資料側寫及自動化個人決策等技術之發展與應用，就特定新興個資利用方式，我國個資法是否宜賦予當事人反對權及資訊提供權？

20



Photo by Andy Kelly on Unsplash

21

### 場次三：智慧載具發展下責任與風險的分配



Photo by Franck V. on Unsplash

#### 焦點議題一

針對自駕車的測試，行政院參考美國加州及新加坡的立法例，借鏡監理沙盒的理念，推出無人載具科技創新實驗管理條例草案。我國是否適宜採監理沙盒模式，並宜採取何種配套措施（例如：測試資料的合理開放運用及允許商用的法規調適）

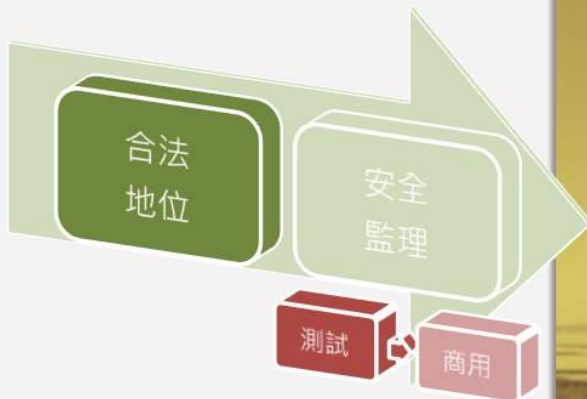


Photo by Bertrand Bouchez on Unsplash

1

## ● 自動駕駛之合法地位

- 美國：自駕系統可以被為是駕駛人。  
※2016年2月NHTSA對Google回覆。
- 德國：自駕系統上路必須有駕駛人。  
※2017年6月道路交通法修正案。  
※駕駛人包含使用「高度」或「完全」自駕系統者，但按SAE J3016分級標準，此應係指等級3及等級4。

我國公路法第2條及道路交通安全處罰條例第3條 對車輛的定義並不以駕駛人為要件。

惟在管制模式上仍預設駕駛人的存在。

現行開發中的自駕車實際上亦仍以駕駛人的存在為必要。

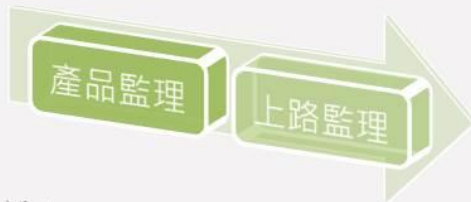
※先進駕駛輔助系統或可自動駕駛但必要時期待人為介入，即SAE J3016等級3以下之自駕車。



Photo by Bertrand Bouchez on Unsplash

2

## ● 自動駕駛之安全監理



- 美國：  
交通部有權豁免特定車輛適用現行安全標準。各州訂定獨自的自駕車測試規範，其中亞利桑那州更對Waymo核發境內首張自駕商用營運執照。  
※審議中法案擬針對自駕車豁免現行安全標準及上路測試作出階段性的總量管制。  
- the SELF DRIVE Act (H.R.3388)  
- the AV START Act (S. 1885)。

此外，交通部亦持續發布、更新非強制性的政策指引，協助業界探索自駕車安全與性能的標準。

※聯邦自動駕駛汽車政策（2018年4月發布第3版）

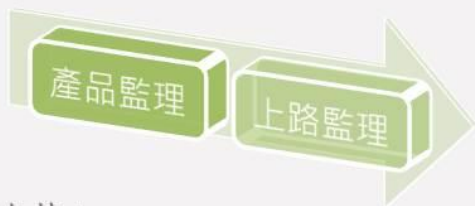


Photo by Bertrand Bouchez on Unsplash

3



## ● 自動駕駛之安全監理



### • 新加坡：

2017年8月的道路交通法修正中授權交通部制定自駕車測試規範及上路規定，經許可之自駕車得排除特定相關法令之適用。

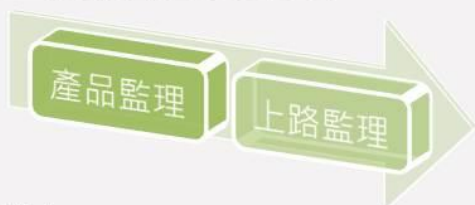
※針對SAE J3016等級3以上之自駕車



Photo by Bertrand Bouchez on Unsplash

4

## ● 自動駕駛之安全監理



### • 德國：

2017年5月的道路交通法修正中擴大駕駛人定義包括使用部分及高度自駕系統之人及相關責任、賠償上限、紀錄及資料保護等規定，正式開放自駕車上路。

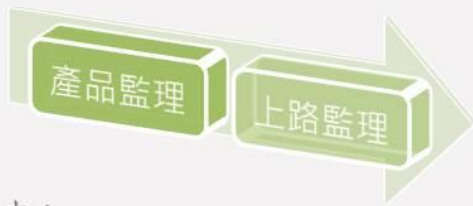
※駕駛可放手交由自駕系統運作，但仍需時刻掌握運作狀況



Photo by Bertrand Bouchez on Unsplash

5

## ● 自動駕駛之安全監理



### ● 日本：

地方運輸局長依道路運輸車輛安全基準得免除特定車輛適用道路運輸車輛安全基準及其公告。2017年2月修正同基準相關規定及公告，放寬可適用之自駕車類型（譬如無方向盤或油門煞車）。

2016年6月日本警察廳公布自動駕駛道路實證實驗指引，針對相關法令及道路測試調查結果彙整必要資訊，支援擬測試者。

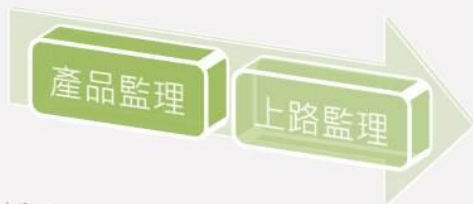
2017年12月日本警察廳公布遠距型自駕系統道路實證實驗道路使用許可申請處理基礎，俾便無人車（遠距操作）之路測。

※在國家戰略特別區域法的修正草案中採取限定區域的監理沙盒。

Photo by Bertrand Bouchez on Unsplash



## ● 自動駕駛之安全監理



### ● 我國：

#### 自動駕駛車輛測試管理條例草案

※2017/10/27 立法院一讀決議，交由委員會審查，目前為止委員會尚未開始審查。

#### 無人載具科技創新實驗條例草案

※2018/10/17 委員會審查完成，目前送黨團協商中。（含領照及開放場域測試）



資料來源：行政院網站  
<https://www.ey.gov.tw/Page/9277F759E41CCD9160a8e74e-d09e-4ac-b7c8-a0f1b3c2e1a8>

Photo by Bertrand Bouchez on Unsplash



## ● 自動駕駛之安全監理



### ● 我國（初步想法）：

#### 適宜性

- 優點
  1. 提供適法依據
  2. 統一政府窗口
  3. 排除法令適用
  4. 管理測試風險
- 缺點
  1. 個案申請許可
  2. 政府全程管制
  3. 測試後無規定
  4. 未涉責任歸屬

#### 配套措施

- 資料運用
 

包括行車記錄在內實驗數據的有效運用，及對安全監視、隱私及營業秘密的兼顧。
- 法規調適
 

在個案短期豁免外，相關法令應如何及時通盤檢討避免個案胎死腹中或阻礙潛在發展。
- 風險分配
 

現行民事法律對自駕模式下的歸責處理及配套。

資料來源：行政院網站  
<https://www.ey.gov.tw/Page/9277F759E41CCD9160a8e74e409e46ac47e8a0f7b5c2e1ab>

Photo by Bertrand Bouchez on Unsplash



8

## 焦點議題二

自駕車輛於自動駕駛模式下運行導致的第三人事故，其民事責任歸屬為何（所有權人、使用人/駕駛人、製造商）？是否宜課予製造商較重責任（如推定過失），或宜採用其他制度性解決方案（如建立賠償基金及提供保險要求），以平衡產業發展與用路人的安全。



Photo by Bertrand Bouchez on Unsplash



9



自動駕駛分級定義 (SAE international, J3016)

SAE分級	摘要	安全駕駛之監視、因應主體
Level 0 無自動駕駛	駕駛人執行全部駕駛任務	駕駛人
Level 1 駕駛輔助	系統執行前後或左右其一的車輛控制之駕駛任務	駕駛人
Level 2 部分自動駕駛	系統執行前後及左右兩者的車輛控制之駕駛任務	駕駛人
Level 3 有條件自動駕駛	<ul style="list-style-type: none"> <li>於特定範圍內系統執行全部駕駛任務</li> <li>系統運作困難時，期待駕駛人的介入回應</li> </ul>	自駕系統 ※運作困難時由駕駛人接手
Level 4 高度自動駕駛	<ul style="list-style-type: none"> <li>於特定範圍內系統執行全部駕駛任務</li> <li>系統運作困難時不期待駕駛人的介入回應</li> </ul>	自駕系統
Level 5 完全自動駕駛	<ul style="list-style-type: none"> <li>於全部範圍內系統執行全部駕駛任務</li> <li>系統運作困難時不期待駕駛人的介入回應</li> </ul>	自駕系統

※2018年6月修訂的第3版。

系統可執行全部的動態駕駛任務

運作困難時期待駕駛人介入回應

系統正常運作預設特定操作環境



Photo by Bertrand Bouchez on Unsplash

● 歸責趨勢



- 責任主體的延伸
  - 所有人
  - 駕駛人/使用人
  - 車輛製造者
  - 軟體設計者
  - 自駕系統(電子人的倡議)
- 以既有歸責原則為基礎進行檢討
- 因應科技發展新的歸責原則



Photo by Bertrand Bouchez on Unsplash

## ● 以既有歸責原則為基礎進行檢討

### • 德國：

2017年6月自動聯網駕駛倫理委員會發布自動駕駛汽車倫理報告，認為既有產品責任原則同樣可適用於自駕系統。

※製造商及經營者應持續優化系統，並觀察其已交付之系統並於技術上可行且合理範圍內對其作出改進。

另一方面，2017年7月德國道路交通法修正，事故發生時車輛係由駕駛人操作時應由駕駛人負責，但若由自駕系統操作時應由製造商負責。但自駕車道路測試時，測試員或遠距監控員亦應負擔注意義務。



Photo by Bertrand Bouchez on Unsplash

12

## ● 以既有歸責原則為基礎進行檢討

### • 英國：

2018年7月生效之英國自動與電動汽車法案規定，就自駕車在道路或公共場所進行自動駕駛（driving itself）而生的事故視情形分別由保險人或所有人負責。

若該車輛於事故時已投保，且被保險人或其他人因該事故而遭受損害時，由保險人負初步賠償責任。

若該車輛於事故時未投保，且不適用1988年道路交通法第143條（使用者投保責任險義務），且有人因該事故而遭受損害時，由所有人負初步賠償責任。

保險人及所有人得再向對事故負有責任的第三人追償。



Photo by Bertrand Bouchez on Unsplash

13



## ● 以既有歸責原則為基礎進行檢討

### • 日本：

一般交通事故的民事責任包括駕駛人侵權責任及駕駛人僱主的僱主責任。此外就事故導致的人身損害，為保護受害人另有汽車損害賠償保障法上的運行供用者責任及汽車強制責任險。

※運行供用者係指為自己之利益將汽車供作運用途，通常係指汽車保有者，但汽車遭竊用時，竊賊方為運行供用者。亦即運行支配及運行利益之歸屬者。

運行供用者責任是相對於侵權責任及僱主責任的嚴格責任，一般認為在自駕車的情形亦無適用上的障礙。免責要件有三：

- (1) 自己及駕駛人就汽車駕駛無怠於注意
- (2) 被害人或駕駛人以外之第三人有故意或過失
- (3) 汽車無結構上陷缺或功能上障礙

另，尚可能涉及產品責任法之產品缺陷。

Photo by Bertrand Bouchez on Unsplash

14



## ● 以既有歸責原則為基礎進行檢討

### • 美國：

2017年9月交通部發布自動駕駛系統2.0：安全願景，其中建議各州評估自駕系統駕駛人是否應為自駕系統故障負責。

- (1) 評估事故發生時應如何在所有人、操作者、乘客、製造商及其他主體間分配責任。
- (2) 評估應由所有人、駕駛人、乘客、製造商及其他主體中的何者承擔投保責任。
- (3) 評估分配侵權責任的規則與法律。

以加州為例，加州汽車法要求製造商應投保美金500萬元之保險或提出同等金額保函或符合主管機關要求之自我保險。

Photo by Bertrand Bouchez on Unsplash

15



## ● 以既有歸責原則為基礎進行檢討

### • 歐盟：

2017年2月歐盟議會通過一份有關機器人民事法律規範的立法決議，提出為智能機器人重構責任規則並考慮賦予複雜的自主機器人法律地位的可能性，即所謂電子人（Electronic Person）的倡議。



Photo by Bertrand Bouchez on Unsplash

16

## ● 因應科技發展新的歸責原則

### • 補償基金

譬如我國的汽車交通事故特別補償基金。針對自駕車，由自駕系統所涉及的多方利害關係人投入作為資金來源，以填補無法由強制責任險所涵蓋的損害。



Photo by Bertrand Bouchez on Unsplash

17

## ● 我國現況

- 契約責任
  - 民法
    - 侵權責任（第184條）
    - 僱主責任（第188條）
  - 消費者保護法第7條
  - 強制汽車責任保險法
    - 強制汽車責任保險
    - 特別補償基金
  - 商業保險
- ※無人載具科技創新實驗條例草案第5條要求申請時應於創新實驗計畫中說明責任保險之規劃



Photo by Bertrand Bouchez on Unsplash



18

感謝各位的聆聽



Photo by Bertrand Bouchez on Unsplash



19

## 場次四：人工智慧於醫療領域之應用

人工智慧相關法規國際發展趨勢與因應研討會



## 人工智慧與醫療服務

報告人：莊郁沁初級合夥人  
理律法律事務所

### 目錄

人工智慧與醫療器材

人工智慧與健康個資

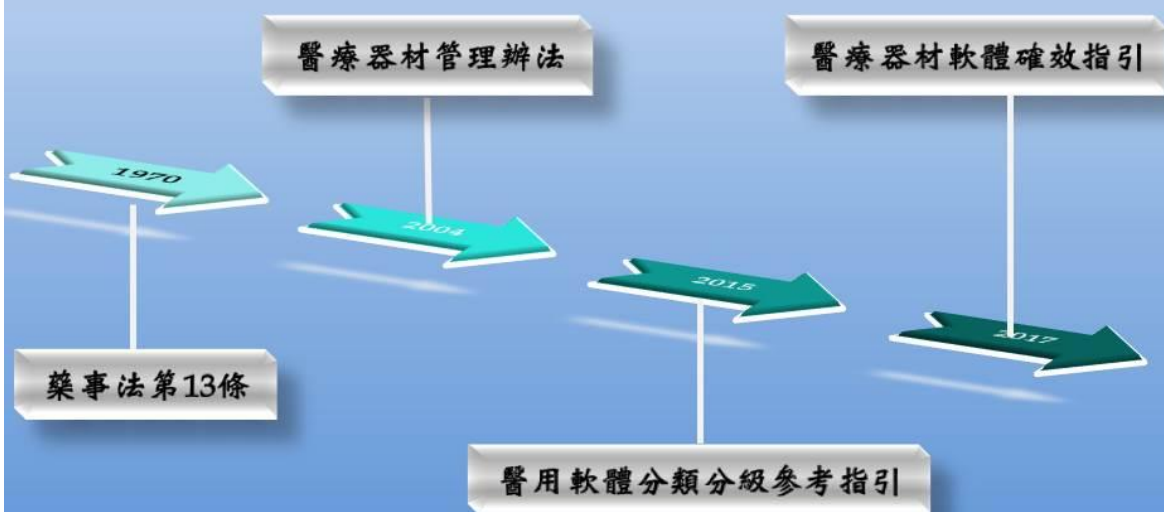
醫療AI與商品責任



## 規劃議題一

# 人工智慧與醫療器材

## 現行法架構



## 現行法架構

### 藥事法第13條第1項

所謂醫療器材，係用於診斷、治療、減輕、直接預防人類疾病、調節生育，或足以影響人類身體結構及機能，且非以藥理、免疫或代謝方法作用於人體，以達成其主要功能之儀器、器械、用具、物質、軟體、體外試劑及其相關物品。

### 醫用軟體分類分級參考指引

本指引所稱「醫用軟體」，泛指蒐集、儲存、分析、顯示、轉換人體健康狀態、生理參數、醫療相關紀錄等處理軟體，使用場所涵蓋醫療院所、個人居家使用及遠距醫療照護，而「醫用軟體」判定屬醫療器材管理者，在此則稱為「醫療器材軟體」。

(1) 醫療器材的附件 (2) 單獨的軟體 (3) 行動應用程式 (4) 儲存軟體的記錄媒體

## 歐盟 (European Union)

歐  
盟

2020年5月  
26日起取代

93/42/EEC指令

MEDDEV 2.1/6, July  
2016指令

醫療器材法 Medical  
Device Regulation

歐盟法院實務見解

### 醫療器材法

1. 針對軟體醫材制訂專門條款
2. 第2條第1項已將具有預後之預測 (prediction of prognosis) 目的的醫療軟體列為醫療器材，而受《醫療器材法》規範

### 歐盟法院—法國飛利浦案

軟體得否作為醫療器材應以製造商意圖使其用作醫療用途為斷，非因該軟體於醫療場合使用而使其成為醫療器材。該判決不僅為《93/42/EEC指令》及《2007/47/EC指令》背書，同時亦與《醫療器材法》觀點相同。

## 美國 (United States)

聯邦食品、藥品、化妝品法  
美國食品藥物管理局

### 指南

1. 行動醫療應用程式 (MMAs)
2. 醫療器材資料系統 (MDDS)
3. 軟體醫材 (SAMD)
4. 臨床決策支持系統 (CDSS)

21世紀醫療法案

釐清「器材」的概念，若軟體的功能為醫療機構的行政支援（例如：開具帳單等）、一般健康維護、電子病歷系統（例如：電子健康紀錄）或是傳輸、儲存、轉換臨床實驗室或其他器材的資料結果，則該軟體非為器材；部分MMAs、MDDS、SAMD、CDSS排除於醫療器材定義範圍外；第3060條更指出，部分CDSS，包含顯示、分析或列印病患醫療資訊或其他醫療資訊（例如：同儕審查臨床研究與臨床執行守則）之軟體、支援或提供醫療專業人員關於預防、診斷或疾病治療建議之軟體，均被認定為非醫療器材。

我國是否仍依藥事法第13條、醫療器材管理辦法，將與醫療有關之人工智慧技術列為醫療器材進行管理？

如是，主管機關查驗登記審查程序是否足以確保人工智慧技術的品質、安全性及有效性？

如否，是否應透過其他機制予以監督？

## 規劃議題二

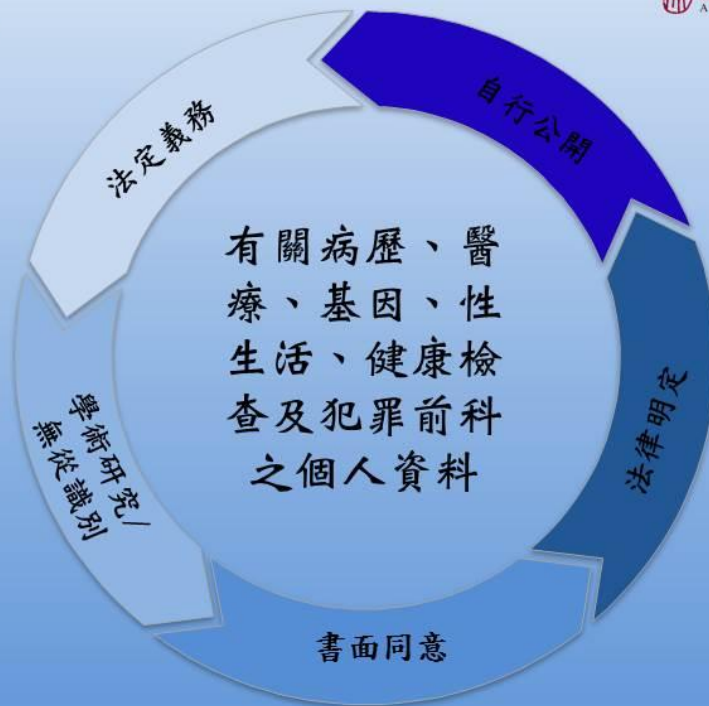
# 人工智慧與健康個資





## 現行法架構

- 個人資料保護法
- 衛福部衛生福利資料應用管理要點



## 一般資料保護規範 (GDPR)

基因資料、用以識別自然人之生物特徵識別資料、與健康相關或與自然人之性生活或性傾向有關個人資料之處理，應予禁止

明確同意

重大利益

自行公開

健康照護必要處理

公共衛生領域公益

研究目的

為使人工智慧技術在醫療領域蓬勃發展，有關病歷、醫療、基因、健康檢查等個人資料（健康個人資料）之蒐集、處理、保存與傳輸必不可免。

因此，如何在《一般資料保護規範》及我國《個人資料保護法》的施行下，適度放寬此等健康個人資料處理保護，以促進科技發展、提升醫療品質，並兼顧相關隱私權保障及防範個人資料侵害？

### 規劃議題三

## 醫療AI與商品責任



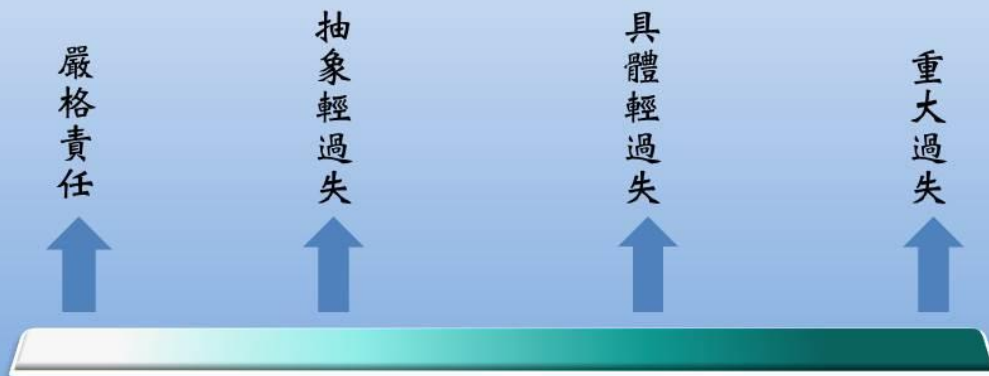
## 現行法架構

### 消費者保護法第7條

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

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。

企業經營者違反前二項規定，致生損害於消費者或第三人時，應負連帶賠償責任。但企業經營者能證明其無過失者，法院得減輕其賠償責任。



注意義務的光譜

是否放寬？

由於醫療人工智慧技術係由硬體與軟體組成，故是否應按消費者保護法第7條規定，逕將其視為純粹商品而有商品責任規範的適用，課予製造商或研發者嚴格的民事責任？



報告完畢，謝謝聆聽

## 肆、研討會會議紀錄

### 場次一：人工智慧發展下的著作權法制議題

(一) 主講人報告如會議簡報內容。

(二) 微軟全球助理法務長/台灣微軟公共暨法律事務部總經理施立成與談內容：

(一) AI 目前的發展已經到可以進行聽說讀寫的程度，惟目前法院判例多認為 AI 僅是將客觀的資料進行整理，並非個性的表達，故不具有可著作權性。

(二) 過去 AI 著重在 IQ 方面，主要是呈現其搜尋的資料。現在的 AI 除 IQ 方面外，更擴大到 EQ 面，如微軟開發的智慧機器人小冰，其回覆具有擬真性，回覆帶有情緒。

(三) 介紹各種市面上的 AI 軟體，包括 Microsoft Pix、Makeup Transfer、Time Lapse 等。

(三) 資策會科技法律研究所創意智財中心組長徐維佑與談內容：

(一) 自國際各國法制觀察，大部分國家均認為僅有人的精神創作才有可著作權性。僅英國法制較為特別。

(二) 如 AI 將某 A 及卡通圖結合產生卡通某 A 並製作周邊商品後行銷，此時應如何分配利益？

1. 美國法上有認為透過 hire doctrine 處理此一問題將能鼓勵 AI 的發展。

2. 歐洲有提出電子人格的看法。

(三) 英國、韓國都有 copyright hub 的制度，如利用 copyright hub 裡面的著作時，只要支付一定代價即可避免侵權。



(四) 因為進入資訊時代，網路上常出現不知著作權人為何之著作，如網路使用者加以利用後可能構成侵權。就此問題，國外有利用區塊鏈來紀錄創作歷程，再透過 smart contract 來處理授權金之分配。

(四) 國立交通大學科技法律研究所助理教授莊弘鈺與談內容：

(一) AI 創作是否具有可著作權性應區分情形而定

1. AI 僅作為工具、輔具：傳統著作權法可處理。
2. AI 為半自動/與人合作：傳統著作權法可處理。如為大公司開發供一般大眾使用的 AI，通常都會在使用條款中約定權利的歸屬。
3. AI 進行獨立創作：即有爭議。

(二) AI 獨立創作可否受著作權保護，目前仍有正面及反面的立論：

1. 反對理由：非人類創作者、美/歐/澳法院實務、人類創作受威脅、歸公共領域有助於公共利益、實際案例不多、舉證有困難、電腦僅是輔助工具。
2. 贊成理由：鼓勵創新、外國立法例(英國 PCDA、大英國協國家、1991 WIPO)、不限於文義、使 AI 具有電子人格、以職務發明原則解決此問題。

(三) AI 獨立創作之著作權歸屬，目前亦是存有不同的主張：

1. AI 本身：作為判斷作品本身之用，可以免去認定過程中，作者人格權的相關爭議。AI 只能以虛擬版權人的角色出現，真正的權利控制者還是其他創制人、開發人等等。
2. 公共領域：否定 AI 作為權利的主體，不給予 AI 創作任何權利。

3. 使用人：人類有參與的電腦創作才可討論著作權歸屬問題，應將權利給予觸發電腦創造產物的電腦使用人。
4. 所有人：所有人也會在所有的狀態中對 AI 注入自我意志，其所為之創作將含有所有人意志之呈現。可藉由將權利賦予所有人以達保護產業投資者利益的目的。
5. 創制人或所有人：重新對雇用作品原則中的「雇員」、「雇主」重新定義，讓 AI 創作的著作權議題可獲解決，並給予研發者依定的經濟誘因，以促進 AI 技術的發展。

(四) 就 AI 侵害他人著作權之問題，有認為需區分開發者與使用者之責任，如使用者是否下載其他軟體、使用者是否有依指示更新、使用者是否善意等。

(五) 臺灣大學法律學院教授謝銘洋與談內容：

(一) 目前發展出的各種 AI 僅為弱 AI，既有規範尚能處理。如未來因技術發展，AI 已變為強 AI 為主時，既有規範即有修正之必要，惟可能有兩種做法，第一是套用既有規範並加以修正，第二是設立新規範。

(二) AI 在著作權法上引發之問題：

1. AI 是否能為權利主體。
2. AI 創作是否能受著作權法之保護。
3. 以上兩個問題具有關聯性，但無必然關係，如即使 AI 不能為權利主體，其創作仍非必然不具有可著作權性。

(三) AI 是否能為權利主體？

1. 觀察法人制度從不被承認到被承認之歷史，其原因在於滿足社會所需，因此 AI 是否能為權利主體仍需視未來發展而定。如未來進入強 AI 時



代，AI 具有思考能力及情緒而與自然人並無太大的不同時，可考慮給予權利主體地位。

2. 然而，就現階段技術上僅發展至弱 AI 而言，尚無需要給予完整或限制的權利主體地位，否則將造成許多麻煩。如給予 AI 享有財產權後，侵權責任、債務不履行等問題如何處理？

#### (四) AI 創作是否能受著作權法之保護？

1. 大陸法系之著作權法要求著作權僅保護人類主體所為之創作，則 AI 既然不是人類，其所為創作似乎不具可著作權性。
2. 姑且不論上述問題，AI 所為創作尚有是否符合「精神創作」此一要件之問題。一般而言，著作須符合此一要件始能受保護。然而，有時縱使不具有此要件，只要對人類文化進步及傳播有相當貢獻，如表演，亦有給予鄰接權保護之立法例。
3. 因此思考重點應不在法律規範如何，而是「是否值得受保護」！如果 AI 的創作值得受保護，即可透過調整法律的方式加以解決，如給予鄰接權之保護。
4. AI 創作對人類文化進步應有貢獻，且如有商業交易價值時，更無理由不給予保護。如完全不給予保護，將使 AI 創作落入公領域之中。
5. 惟即便如此，AI 所為創作也不一定要用著作權之思維處理，因 AI 創作速度太快、太快，如保護期間太長，將形成對市場的壟斷，應考慮用保護較低度之鄰接權加以保護。
6. AI 所為之創作並非人格之展現，故不必給予人格權之保護，重點在於財產權之保護，惟其內容是否應包含排他權，即對於侵權人可主張權利侵害？考慮到 AI 之特性，恐值得再思考。如接續上述以鄰接權保護之看法，僅需賦予報酬請求權即可，亦即如有人使用 AI 所為之創作時，權利人可向該人請求報酬。

7. 有關權利歸屬之問題，應將權利歸屬給對產生「創作」在經濟上（而非精神上）貢獻程度較高的人。因為如果演算法寫的不好，則 AI 根本無法使用，故演算法之開發者最為重要，而提供資料給 AI 的人，其在經濟上之貢獻度可能沒那麼高，使用者對於「創作」之產生可能貢獻度最低。在權利歸屬上應考慮這些因素，亦不妨考慮讓這些在各個階段有經濟上貢獻的人可以共享這個權利。
8. 就是否要立法處理利益歸屬之問題，基本上只要透過契約約定即可解決利益歸屬的問題。倘若無契約約定時，智慧財產權法下亦有共有的概念，此時不妨視各參與者之經濟上貢獻程度來決定各自之應有部分比例。
9. 最後就 AI 在「創作」時所造成的侵權問題，如被侵權人欲依民法第 184 條告 AI 開發者須證明故意過失及因果關係，具有相當之難度。可考慮參考無人機或無人車對於侵權責任的處理方式用保險或基金加以處理。

## 場次二：人工智慧與個人資料

一、主講人報告如會議簡報內容。

二、中原大學法學院教授江耀國與談內容：

(一) GDPR 之所以會有這麼強的域外效力，遠因是歐盟作為一個強權，希望能夠對抗世界另一個強權美國，加上過去 20 年來個資保護已經逐漸與隱私脫離，本人認為在接納 GDPR 相關規定前，必須要先進行反省的論述，而非全盤接受。

(二) GDPR 第 22 條有兩個要件，沒有這兩個要件的話，適用範圍會過廣，第一個要件是該等決策僅只依賴自動化機器作成、沒有任何人為參與，第二個要件是對當事人將造成法律上或類似的重大影響。之所以要有第 22 條，是因為沒有人類參與的話，可能會有不正確的偏見，但自動化決策未必會造成法律上或類似的重大影響，例如使用自動化決策推播廣告給消費者。

(三) 識別性及去識別化其實是一個問題的兩面，兩者都是一個認知的過程，在判斷一個檔案是否具有識別性時，除了識別客體外，還涉及到識別主體及識別方法兩個要素，絕對主義主張只有世界上任何一個人能夠用任何方法識別出特定個人，這個檔案就是個人資料，如果往絕對主義的方向進行解釋，那麼去識別化將永遠不可能成功，但是往相對主義的方向進行解釋，那麼去識別化還有可能成功。GDPR 立法理由第 26 點便指出識別方法必須是合理的方法，不能是不計任何代價的方法。另一方面，英國則認為識別主體應排除具有先前知識的人。無論是識別性或去識別化，基本上都會涉及到識別主體、客體及方法這三個要素，但對於識別三要素，我國個資法目前只有規範識別客體而已，對於識別主體及方式的界線未作規範。

三、臺灣大學電機系暨電子所教授/優拓資訊共同創辦人黃鐘揚與談內容：

當人們愈投入人工智慧的領域，反而會發現人類的智慧相當值得崇敬，目前人工智慧能夠做的還是極其有限，即便人工智慧處理資料的速度比人類快速許多，

但基本上與人工處理資料並無實質差異，只要未涉及不公平競爭等問題，本人認為實際上無需過度恐慌，反而應該思考如何在資訊爆炸的時代下，運用人工智慧幫助我們篩選或消化資訊。

#### 四、輔仁大學財經法律學系助理教授翁清坤與談內容：

(一) 人工智慧運用大量的自動化決策，除了種族、性別等明顯可見的歧視外，還可能潛藏許多人類未察覺的歧視，但如果普遍賦予人們拒絕自動化決策的權利，可能反而會造成人工智慧無法發展的後果，所以是否要引進 GDPR 相關規定，本人認為可以再觀察。

(二) 在過去小數據的時代，資料的去識別化相當容易，但在大數據的時代，由於資料數量、種類及來源眾多，以往認為去識別化的資料有可能再識別，兩者在美國認為是一種武器競賽，在技術上已經無法百分之百地去識別化，因此可以透過法律或契約禁止資料擁有者進行再識別，違者須負契約或侵權責任。

#### 五、意藍資訊董事兼總經理楊立偉與談內容：

並非所有人工智慧及大數據應用都需要精準、不模糊地指向特定個人，除了去識別化或去連結化外，技術上還存在一種可能性是代碼化，譬如一個人可以有 multiple 多個虛擬身分，少數知道這些虛擬帳號與真實身分之間連結的業者需要控管，但對於只知道代碼、虛擬身分的外圍業者，其實已經足以形成一道防護牆。

### 場次三：智慧載具發展下責任與風險的分配

一、主講人報告如會議簡報內容。

二、景翊科技股份有限公司總經理陳奕廷與談內容：

#### (一) 針對自駕車上路測試

1. 自駕車的發展是一個全球趨勢，的確需要法律配套。但既然談到監理沙盒，就要從兩個觀點來看，一是鼓勵新創，給予其測試的空間；二是道路安全，思考如何規範使自駕車可以安全上路。這是兩個我觀察到國外在訂法規時的重點。
2. 全球發展自駕車最友善的國家，第一其實是芬蘭（Nokia 故鄉鼓勵新創），第二其實就是新加坡，相較於歐美可謂後發先至。美國 Waymo 自駕車進軍亞洲第一個落地的正是在新加坡。而新加坡無論在法規、封閉場域或實體場域測試都有很好發展，值得台灣未來推動自駕車產業借鏡。
3. 從法規面來看，透過我們參與新加坡計畫的夥伴，我們可以作一個比較。目前推動的無人載具科技創新實驗條例，要求車輛上路必須投保，這有助於事故發生時受害人迅速得到理賠；但並沒有要求車輛上路後的測試數據應該上傳公開，但新加坡有此要求。我們從經驗知道很多測試、驗證可能作假，若測試數據有上傳，政府才有可能去檢驗其真假。或譬如要求事故發生後十日內應該相關數據提供，有利政府分析檢驗。
4. 台灣目前作自駕車測試，主要作封閉場域或實體道路場域，從北到南計四個場域（士林、虎頭山、水楠及沙崙）都是作封閉場域。但國外都是先作模擬場域，先在系統上模擬所有的情境，譬如強逆光、強降雨或水漂現象。又像是台灣有非常多的摩托車，或行人突然竄出等情形也是封閉場域無法看到，應先經在模擬場域上作驗證。新加坡作得

很好，他們要求業者應先通過模擬場域驗證，作了約 500~1,000 種模擬情境，才進到封閉場域。但台灣目前是缺乏模擬場域驗證這一環節。

5. 新加坡為鼓勵新創，授權交通部長交通法規直接作修正，可配合新創發展及時因應修正。新加坡法令中我們可以參考的是，從模擬、從道路號誌適應、到封閉場域再到實體場域的順序。

## (二) 責任歸屬

1. 舊金山從 2014 年自駕車開始上路後，自駕車跟普通車發生事故的案件有 88 件，其中因自駕車而發生的只有 7 件。對照起來，自駕車還是比較安全。
2. 運用自駕車等於是演算法決定你的生命，若演算法不夠聰明，確實引人擔心。德國在提出自駕車的 22 條倫理規範中，第 7 條要求如果無法避免危險，則保護駕駛為其重要選擇。第 9 條要求不能因事故可能撞到對象的身分而有差別對待。在我們看來，自駕車遇到這些情境時該如何作出選擇是需要 rule based 的基礎，我們也看到國外有學者提出了窮舉法的作法，以完備選擇規則。但能否成功也取決於不同車廠是否願意採用同一套規則。
3. 至於針對現在推動的無人載具科技創新實驗管理條例，我覺得要到回歸到一個問題：你要不要鼓勵新創。若是鼓勵新創，希望引進國外技術，那應該思考怎麼營造友善的測試環境。

## 三、交通大學科技法律學院助理教授莊弘鈺與談內容：

### (一) 針對自駕車上路測試

1. 有關自駕車，從法制面來說，美國對於是否以聯邦法律管理目前尚在觀測階段（僅有草案於參議院送審），現行僅頒布了政策指引。目前

是交由各州以不同規範方式及內容來處理(譬如法律位階或行政辦法),而且呈現各州競相吸引產業測試(有的甚至開放無人在車內)。

2. 德國跟美國較不同,因基本上已有聯邦立法(道路交通安全法),且遵守維也納道路交通公約,允許有駕駛人在車內為前提的自駕車(Level 4)上路。該駕駛有隨時接管此車輛之義務,且車輛亦要求搭載黑盒子,有助於事故的釐清。
3. 台灣在自駕車的立法進度,不僅晚於歐美,也晚於日、韓、新加坡(2015年~2017年間)及中國(2017年~2018年間)等亞洲各國。若欲加速,我們或許可以考慮學習新加坡、中國,尤其新加坡等亞洲國家交通情形可能跟我們更相像。

## (二) 責任歸屬

德國要求設置黑盒子,其中主要係與行車相關的紀錄,不及駕駛人日常生活中開車的情況。同時車內也要求有一個人,這是有助於問題的釐清。也有人提到責任保險,目前業者提到最大的問題是他們不知如何計算保險,因此不敢承作。或許我們可參考美國、中國或新加坡,他們要求上路時車輛應滿足一定保險要求,譬如美國是要求500萬美金,中國或新加坡也有設定一個上限。

## 四、臺灣大學法律學院教授黃銘傑與談內容：

### (一) 針對自駕車上路測試

1. 我們知道自駕車可以減少事故,同時解決譬如身心障礙、老年人移動困難等社會問題,也會逐漸改變我們的生活型態。因此,自駕車的發展大家本身是沒有質疑的。
2. 然而在引進過程中,有許多人認為要像金融科技創新一樣,導入管制沙盒的工具,先試試,沒問題我們再讓它上路。但自駕車的測試究竟

與一般車有何不同？為何一般車出廠測試(安全審驗)不用監理沙盒，而自駕車需要？

3. 主管機關認為不待公路法及道路交通安全規則修正，自駕車就是該法令所稱汽車。也因此，也以行政辦法方式讓其上路測試。若是如此，我們又為何需要再通過一部無人載具科技創新實驗條例呢？而且，也不應該叫無人載具，上面肯定是要坐人才有意義。
4. 其次，我們要自駕車測試什麼？我認為真正要作的是安全性測試，譬如在台灣這種天候及交通環境是否可行。金融實驗需要監理沙盒是因為它是一種行為規則，要測試人們行動模式如何改變；但自駕車不一樣，是系統安全性測試，或車載軟體跟連線安全性的問題。德國法非常清楚告訴我們，自駕車不需要等什麼監理沙盒再修法。
5. 因此，若我們確認自駕車對我們是必要的，我們就直接修法，無需再制定什麼監理沙盒。
6. 剩下的唯一問題是現在道路交通管理處罰條例處罰的是駕駛人。針對這個，只要重新檢討駕駛人的概念，並思考要怎麼讓自駕車負責的問題解決就好。不宜讓監理沙盒阻礙我們產業的發展。
7. 另外，對參加沙盒的業者來說，也有一個問題是，為什麼我自己辛苦申請沙盒，通過決定修法後卻是由大家雨露均沾。這是有一個搭便車的問題，因此是否考慮賦與參加業者一定期間的獨占權。此外考慮到台灣修法速度，可能對業者更是折磨，假使花個三年，對新創也是嚴重拖延。

## (二) 責任歸屬

1. 未來若自駕車上路，我想我們很可能都不會買車。因持有成本遠高於租賃成本（含計程車）。未來保險業因事故的減少可能受到很大影響而蕭條。汽車業因車輛持有型態的轉變，譬如以大公司的租賃車隊型



態為主，個人無需買車，也不需要車位。若是如此，未來歸責的型態也可能需要相應作調整，由車隊負主要責任。

2. 我們目前在民事法律責任上是採故意跟過失為前提的過失責任。在自駕車方面的產品製造人責任我們採無過失責任，但存在所謂最高科技抗辯。換句話說，若自駕車其軟體、系統的設計是滿足最高科技抗辯，即可能存在一個責任真空狀態。若 AI 設計沒問題、AI 判斷的要素也比人還要周全，那我們究竟要怎麼究責？因此，若 AI 的引進真的對人類有益有必要時，我們勢必要共同負擔它的風險。也因此其他國家也在思考一些不同的概念，包括 BI(Basic Income)或對機器人課稅(Robot Tax)，為社會保障作共同承擔。
3. 另，自駕車未來不僅會遇到車外受害人選擇的倫理問題，也會遇到車內、車外應該優先保護誰的問題，這些倫理問題也是我們接下來需要開始思考的問題。

#### 場次四：人工智慧於醫療領域之應用

一、主講人報告如會議簡報內容。

二、宏達國際電子股份有限公司 Sr. Director 遊山逸先生與談內容：

(一) 「醫療 AI 與醫療器材規範」議題：

1. 關於人工智慧在醫療服務領域的發展，目前並無強人工智慧的產品，且美國亦暫無相關產品，其發展根本無法預期；至於弱人工智慧的產品，則為以資料導向的大數據分析，來協助檢出或診斷為主。另外，以機器學習來說，若其正確率能夠高達 95% 已是極佳，惟這 5% 的錯誤率不但無法解釋，技術也不易克服，也因為如此，目前人工智慧在醫療服務領域，仍是以輔助檢出或診斷為主。
2. 美國 FDA 係以臨床應用之使用目的 (Intended Use) 來決定產品的分類與分級。以個人角度來看，管理醫療器材的規範，目前應不需要有太大的調整，因為審查醫療器材時，仍然是以產品本身的有效性及安全性為標準，現行法律架構應已足夠適用目前的所研發的醫療器材。
3. 此外，若使用在機器學習過程中未曾訓練過的資料時，則產品錯誤率會大增。

(二) 「醫療 AI 與健康個人資料保護規範」議題

1. 歐盟 GDPR 對於個人資料保護越趨嚴格，亦是目前國際趨勢。
2. 如何兼顧人工智慧發展與個人資料保護，首先，由於書面同意將扼殺資料取得的效率，可考慮以其他不同方式行使同意；其次，針對去識別化，將個人資料擁有者匿名是必要；其三，建立回饋機制，例如若使用者願意開放個人資料，在全民健保上獲得補助，以提升人工智慧發展。

(三) 「醫療 AI 與商品責任規範」議題

依現行法規，醫療器材製造商仍有上市後監督責任，持續改善醫療器材的品質，以確保醫療器材製造商將產品的安全性及有效性盡可能做到最好。因此，即使是人工智慧的醫療器材製造商，仍應依該法規制度，審慎管制產品的安全性及有效性，以及上市後監督之責任。

### 三、宏達國際電子股份有限公司虛擬實境研發部門經理呂適任先生與談內容：

#### (一) 「醫療 AI 與醫療器材規範」議題

1. 當產品在系統上有任何更動時，即須進行軟體確效，甚至應申請醫療器材重新認證。對於人工智慧應更動至何程度始須行醫療器材重新認證，現行法規並無明確規定。
2. 對於人工智慧的資料庫，是否於第二次診療時能夠使用第一次診療所提供的資料，若是，則顯然違反第一次蒐集資料之目的；若否，則又需提供相同資料，顯然耗費資源，而現行法規對此並無任何規範。
3. 醫療器材係以使用目的為分類、分級，然人工智慧在應用上難以區分，造成審查時間延長。審查時間的延長即有可能造成病患生命殞落，或是有礙新創產業的發展。

#### (二) 「醫療 AI 與健康個人資料保護規範」議題

1. 人工智慧在擴展應用的同時，應取得資料所有者的同意，或可透過電子方式取得同意。但是去連結化後，應無法回復，故若欲取得同意，即代表可回復，而不符合去連結化的標準。
2. 個資法第 6 條可能會對醫療發展造成阻礙。且目前機器學習仰賴資料輸入，故若資料所有者能夠退出，勢必影響人工智慧準確性及技術發展。
3. 美國 FDA 公布資料使用「最小必要原則」，然此與人工智慧的發展方向完全相反，因為當資料越多時，人工智慧將越準確。

### (三) 「醫療 AI 與商品責任規範」議題

1. 人工智慧製造商的責任難以釐清，且當人工智慧涉及硬體，究竟應如何釐清製造商的責任，更加困難。在難以歸責的情況下，極有可能歸責診療判斷者—醫師。
2. 一般來說，營利與責任應一併觀之，惟若歸責於醫師，營利者卻為製造商，顯有疑問。

## 四、資策會科技法律研究所價值拓展中心副主任李昂杰先生與談內容：

### (一) 「醫療 AI 與醫療器材規範」議題

1. 現階段人工智慧與醫事人員協作的過程，對於人工智慧的不透明性，是否會影響目前的法律規定？值得深思。
2. 目前美國已經意識到軟體和傳統醫療器材硬體並不相同，應行區別其規範，並有類型化看法。而人工智慧在醫療服務運用上，更有如是之特徵。此外，人工智慧倘非醫療器材，則是否即無上述規範問題，亦宜考量。
3. 未來人工智慧若具備決策特徵，則是否應將其視為伙伴，歸為專業人員，而非產品，而不僅以醫療器材法規予以管理。

### (二) 「醫療 AI 與健康個人資料保護規範」議題

人工智慧在各不同面向對於個人資料的需求，如何適度調整相關個人資料保護規範，為目前的課題之一。英國目前以主管機關同意取代告知同意，立法者或可思考此制度；但宜注意其背後所代表「以立法者的（通案）決定取代當事人的（具體個案）決定」之意義。

### (三) 「醫療 AI 與商品責任規範」議題

有研究嘗試，以醫事人員參與程度為橫軸，人工智慧運作過程透明程度為縱軸，思考責任歸屬。當人工智慧運作過程透明時，得以傳統責任歸屬思考；惟當人工智慧運作過程不透明時，人為介入程度即會影響責任歸屬。

五、國立交通大學科技暨法律研究所副教授兼所長陳鈺雄先生與談內容：

(一) 「醫療 AI 與醫療器材規範」議題

1. 對於軟體是否為醫療器材的認定，歐盟法院係以「製造商是否意圖將其作為醫療器材」為判斷標準，該標準同美國的認定標準。
2. 美國 FDA 對於新創軟體的認定，基本上是盡可能擴大其管轄權，但在某些情形，例如風險小等，則 FDA 不予管轄。概念上同我國衛福部。美國亦透過「21 世紀醫療法案」將部分軟體排除在醫療器材範圍內。整體而言，「白箱」(white box) 因能夠揭露推論過程，故能由醫師檢測，而被排除在醫療器材認定範圍，但依然受到批評，因為與過去 FDA 以「風險」為標準進行認定，並不相同。
3. 對於新創軟體，基本上是創新與安全性的兩難，而 FDA 對於新創軟體的管理最大的不同在於，其上市的速度會比藥品上市的速度來得高。因為藥品生命週期較軟體長，且硬體、軟體雖不相同，但硬體壽命是否影響軟體，值得深思。
4. 由於現今人工智慧著重在「學習」(learning) 過程，故 FDA 管制的重心從產品本身移向生產軟體製造商，若生產軟體製造商能夠遵循 FDA 的指南，則不僅可加速該產品上市的速度，同時亦可降低製造商的責任義務。

(二) 「醫療 AI 與健康個人資料保護規範」議題

1. 個人資料保護難以在商業使用上放寬，因：全民健保訴訟，目前大法官正在審理中，由於病患在看病時同意提供資料，事後應有權選擇退

出，因此推測大法官應會認為有退出權，且世界各國均規定人民有退出權。

2. 對於告知問題，或許可在同意部分予以緩和，並取代書面同意。但若醫療機構欲提供資料與商業機構時，是否應在告知時，明確說明並指出。
3. 目前商業機構透過以下二種方法取得個人資料：(1)與學術機構合作，例如贊助醫學研究(2)技術上面改變，畢竟大數據分析不一定需要取得同意，因為人工智慧「學」好時，就不再需要資料了。這兩種方法目前是合法的。
4. 倫理方面來說，病患的個人資料，對於病患本身是有利的，但是對於非病患的其他病患來說，卻非如此，難以自圓其說，目前難有重大改變。

### (三) 「醫療 AI 與商品責任規範」議題

1. 個人認為要求人工智慧的產品責任是有難度的，因為即便是產品的無過失責任，均要求符合「可預見性」(foreseeability)，以判斷是否符合當前科技技術。但是人工智慧是「黑箱」(black box)，因此難以預測，進而課與製造商責任。
2. 或可考量藥害救濟法制度，由於因果關係難以證明，要求業者撥出一部分營收作為基金，以補償受害者。我國目前未將醫療器材列入，惟未來可考慮往此方向修法。
3. 在傳統消保法或商品責任法，如何證明產品設計瑕疵，必須先證明有更好的設計方式。但是在人工智慧中，因為有資料的獨佔特質(monopoly)且為市場上的唯一，致使難以證明對於該人工智慧有更佳的設計方式。

4. 對於業者或製造商，可透過產品標示，盡其對醫師的警示責任，滿足其義務。惟針對醫師端，醫師有告知同意的義務，但醫師有無義務告訴病人人工智慧診斷的過程及結果，充滿疑問。

六、 臺北醫學大學醫療暨生物科技法律研究所副教授李崇僖先生與談內容：

(一) 「醫療 AI 與醫療器材規範」議題

1. 由於 IMDRF，故美國、歐盟對於醫療器材的分類、分級均有較為一致的認定，而臺灣亦於去年加入該組織，國際上對於此亦有較一致的方向。
2. 醫療器材規範的典範轉移，像是物聯網 (IoT)、智慧醫療、遠距醫療、長照等，致使不能將醫材視為產品，而是一種服務、營運。因此，應用的場景亟需深思，且並無答案。不過，或可利用臺灣的優勢，例如全民健保制度，來提升臺灣在全球醫材的競爭力。
3. 針對目前醫療器材相關草案，已有幾項改變，例如對於個人資料，主管機關公告取代醫療器材使用者之書面同意等。

(二) 「醫療 AI 與健康個人資料保護規範」議題

歐盟 GDPR 的 G，即是 General 一般，亦即一般規範，因此可以完善規範特別法，使 GDPR 無法適用某些產業。特別法並得賦予資料使用者彈性取得資料，惟其責任亦相對應加重。

(三) 「醫療 AI 與商品責任規範」議題

現行法規例如消保法、醫療法規，並非不合理的規範標準，仍有臨床裁量空間，風險不高。較值得擔心者，在於醫療 AI 所改變的臨床決策模式，導致專業裁量空間是否存在的問題。亦即對於醫療應用、醫師培養養成、病患照顧等醫療情境，所造成的「Culture Shock」。

## 附錄五 參考資料

### 英文資料

#### 1. 專書

- (1) A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation, Mark.A. Geistfeld.
- (2) Abbott, Ryan Benjamin, Artificial Intelligence, Big Data and Intellectual Property: Protecting Computer-Generated Works in the United Kingdom (November 2, 2017). Research Handbook on Intellectual Property and Digital Technologies (Tanya Aplin, ed), Edward Elgar Publishing Ltd, Forthcoming.
- (3) Andres Guadamuz, Do Androids Dream of Electric Copyright? Comparative Analysis of Originality in Artificial Intelligence Generated Works, 2017:2 Intellectual Property Quarterly (2017).
- (4) Andrew Guthrie Ferguson (2015). Big Data and Predictive Reasonable Suspicion, 163 U. Pa. L. Rev.
- (5) Anne Fitzgerald & Tim Seidenspinner, Copyright and Consumer-Generated Materials - Is It Time to Reboot the Discussion about Authorship?, 3 Victoria U. L. & Just. J. 47 (2013).
- (6) Annemarie Bridy (2012). Coding Creativity: Copyright and the Artificially Intelligent Author. Stanford Technology Law Review, Vol. 5.
- (7) ARTIFICIAL INTELLIGENCE IN HEALTH CARE, 14 No. 1 ABA SciTech Law.
- (8) Automated Vehicle Lawsuits, How Will We Litigate the Auto Crash of the Future, Brett A. Ross.



- (9) Cameron Andrews (2011), Copyright in computer-generated work in Australia post-IceTV: Time for the Commonwealth to Act, 22(1) Australian Intellectual Property Journal.
- (10) Cameron Andrews, Copyright in computer-generated work in Australia post-IceTV: Time for the Commonwealth to Act, 22(1) Australian Intellectual Property Journal 29 (2011).
- (11) Commission of the European Communities Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area {SEC(2004)539} Brussels, 30.4.2004 COM (2004) 356 final,
- (12) Danielle Keats Citron and Frank A. Pasquale, The Scored Society: Due Process for Automated Predictions.
- (13) Danielle Kehl, Priscilla Guo, and Samuel Kessler (2017). Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing. Responsive Communities Initiative, Berkman Klein Center for Internet & Society, Harvard Law School.
- (14) European Civil Law Rules in Robotics.
- (15) Frank Pasquale (2015). The Black Box Society. Cambridge, Massachusetts; London, England: Harvard University Press.
- (16) Frank, Sharon. A new model for European Medical Device Regulation: a comparative analysis in the EU and the USA, Europa Law Pub, 2003
- (17) Hutchens, A., & Humble, E. (2017) Health care and the cloud – a prescription for complexity. Privacy Law Bulletin, 14(4).

- (18) Ira S. Rubinstein, Ronald D. Lee and Paul M. Schwartz (2008). Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches, 75 U. Chi. L. Rev.
- (19) Perfected in China, a threat in the West (June 2, 2018). The Economist.
- (20) Petra WILSON, Isabelle Andoulsi, Tony SOLOMONIDES, Vincent BRETON, Jean Herveg, Data protection and confidentiality in healthgrids: the SHARE project : a framework for developing a roadmap for the adoption of Grid technology in healthcare, Medizinische Informatik, Biometrie und Epidemiologie, 2006
- (21) Ryan Abbott (2016). I think, Therefore I Invent: Creative Computers and the Future of Patent Law. Boston College Law Review, Vol. 57.
- (22) Ryan Benjamin Abbott (November 2, 2017), Artificial Intelligence, Big Data and Intellectual Property: Protecting Computer-Generated Works in the United Kingdom. Research Handbook on Intellectual Property and Digital Technologies (Tanya Aplin, ed), Edward Elgar Publishing Ltd, Forthcoming.
- (23) Samuelson Pamela (1985). Allocating Ownership Rights in Computer-Generated Works, University of Pittsburgh Law Review.
- (24) Scott, M.D. (2008) Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?, Medical Law Review (67).
- (25) Solon Barocas and Andrew D. Selbst (2016). Big Data's Disparate Impact, 104 California Law Review.
- (26) Tsang L, Kracov D, Mulryne and others, The Impact of Artificial Intelligence on Medical Innovation in the European Union and United States, Intellectual Property & Technology Law Journal, August 2017.

- (27) UK House of Lords Artificial Intelligence Committee. 2018 AI in the UK: ready, willing and able? (HL Paper 100).
- (28) Webb, T., & Dayal S.(2018) Medical devices and the IoT: regulatory perspectives on cybersecurity risks in health care. *Internet Law Bulletin*, 20(8).
- (29) Viktor Mayer-Schönberger and Kenneth Cukier (2013). *Big Data: The Essential Guide to Work, Life and Learning in the Age of Insight*. London, England: John Murray.

## 2. 期刊

- (1) Alexandra George (2014), *Reforming Australia's Copyright Law: An Opportunity to Address the Issues of Authorship and Originality*, 37(3) *University of New South Wales Law Journal* (2014).
- (2) Christopher Bavitz (2018), *Morality in the Machines*. *Harvard Law Bulletin* - Summer 2018.
- (3) Darlin Glasser (2001). *Copyrights in Computer-Generated Works: if Anyone, Do We Rewarded*. *Duke L. & Tech. Review*.
- (4) HM Bøhler (2017). *EU copyright protection of works created by artificial intelligence systems*, JUS399 Master's thesis Faculty of Law of University of Law.
- (5) James Manyika et al. (2013). *Disruptive technologies: Advances that will transform life, business, and the global economy*. San Francisco, CA: McKinsey Global Institute.
- (6) Jennifer Krueckeberg (2018). *A Lawless Zone: Surveillance Technologies and the Police*. *Green European Journal*.
- (7) Kalin, Hristov (2017). *Artificial Intelligence and the Copyright Dilemma*. *IDEA: The IP Law Review*, 57(3).

- (8) Lincoln Tsang et al. (2017). The impact of artificial intelligence on medical innovation in the European Union and United States. *Intellectual Property & Technology Law Journal*, August 2017.
- (9) Michele C. Kirrane and Devinder S. Grewal (2016). Civil Liability Arising Out of the Commercial Ownership and Operation of Drones. *For the Defense*, 58(4).

### 3. 研究報告

- (1) Article 29 Data Protection Working Party (2007). Opinion 4/2007 on the concept of personal data.
- (2) Article 29 Data Protection Working Party (2014). Opinion 05/2014 on Anonymisation Techniques.
- (3) Article 29 Data Protection Working Party (2014). Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU.
- (4) Bill Siwicki (May 19, 2017). 86% of Healthcare Companies Use Some Form of AI. *Healthcare IT News*.
- (5) Changing driving laws to support automated vehicles Policy paper
- (6) Chung, Jason, Hey Watson, Can I Sue You for Malpractice? Examining the Liability of Artificial Intelligence in Medicine, Forthcoming, *Asia-Pacific Journal of Health Law, Policy and Ethics*, November 2017
- (7) Department for Digital, Culture Media & Sport (2018). Data Ethics Framework.
- (8) European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Single Market Strategy for Europe - COM(2015) 192 final European Parliament

- (9) European Civil Law Rules in Robotics.
- (10) European Parliament Committee on Legal Affairs (2016). Artificial Intelligence Potential Benefits and Ethical Considerations.
- (11) European Parliament Committee on Legal Affairs (2017). REPORT with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103/(INL)).
- (12) European Securities and Markets Authority, Final Report– Guidelines on certain aspects of the MiFID II suitability requirements
- (13) European Commission (2017). Report of the Working Group on mHealth assessment guidelines.
- (14) Executive Office of the President (2016). Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights.
- (15) Executive Office of the President (2016). Preparing for the Future of Artificial Intelligence.
- (16) Executive Office of the President (2016). Artificial Intelligence, Automation, and the Economy.
- (17) Federal Trade Commission (2012). Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers
- (18) Federal Trade Commission (2016). Big Data: A Tool for Inclusion or Exclusion?
- (19) Financial Conduct Authority (2015). Regulatory Sandbox.
- (20) Financial Conduct Authority (2017). Regulatory Sandbox Lessons Learned Report.
- (21) Financial Conduct Authority (2017). Regulatory sandbox - cohort 1.

- (22) Francesca Rossi (2016). Artificial Intelligence Potential Benefits and Ethical Considerations, European Parliament.
- (23) Fred H. Cate, Peter Cullen and Viktor Mayer-Schönberger (2013). Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines. Redmond, WA: Microsoft Corporation.
- (24) GAO (2018). Artificial Intelligence: Emerging Opportunities, Challenges, and Implications for Policy and Research.
- (25) Guidelines on the Qualification and Classification of Stand Alone Software used in Healthcare within the Regulatory Framework of Medical Devices, MEDDEV 2.1/6. (July 2016)
- (26) Government Office for Science (2016). Artificial intelligence: opportunities and implications for the future of decision making.
- (27) House of Commons, Science and Technology Committee (2016). Robotics and artificial intelligence: Fifth Report of Session 2016-17.
- (28) House of Lords. Select Committee on Artificial Intelligence (2018). Report of Session 2017-19: AI in UK: ready, willing and able?
- (29) IDC (2017). Data Age 2025: The Evolution of Data to Life-Critical.
- (30) Jani Ihalainen (2018), Computer creativity: artificial intelligence and copyright, 13(9) Journal of Intellectual Property Law & Practice.
- (31) Jani McCutcheon, Curing the Authorless Void: Protecting Computer-Generated Works Following IceTV and Phone Directories, 37 Melbourne University Law Review; UWA Faculty of Law Research Paper No. 28 (2013).
- (32) John McCarthy et al. (1956). A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence.

- (33) Jon Kleinberg et al. (2017). Human Decisions and Machine Predictions. National Bureau of Economic Research, Working Paper No. 23180.
- (34) Mariana Alpalhão Gonçalves, (Aug, 2018), Liability arising from the use of Artificial Intelligence for the purposes of medical diagnosis and choice of treatment: who should be held liable in the event of damage to health? (Tilburg Law School Tilburg University)
- (35) Mark Perry & Thomas Margoni (2010), From music tracks to Google maps: Who owns computer-generated works?, 26(6) Computer Law & Security Review.
- (36) Monetary Authority of Singapore (2016). Fintech Regulatory Sandbox Guidelines.
- (37) Monetary Authority of Singapore (2018). Experimenting in the Sandbox.
- (38) National Science and Technology Council (2016). The National Artificial Intelligence Research and Development Strategic Plan.
- (39) Official Journal of the European Union (L117) of May 5, 2017
- (40) Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), wp258 (29 November 2017).
- (41) Parasidis, E. (2018) Clinical Decision Support: Elements of a Sensible Legal Framework. Journal of Health Care Law & Policy, 20(183).
- (42) Parliament of Australia (1999), 'Simplification of the Copyright Act 1968 - Part 2: Categorisation of Subject Matter and Exclusive Rights, and Other Issues' (1999) 15 Research Note 1.
- (43) Peter Stone et al. (2016). Artificial Intelligence and Life in 2030. One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel, Stanford University, Stanford, CA.

- (44) President's Council of Advisors on Science and Technology (2014). Big Data and Privacy: A Technological Perspective.
- (45) Raso et al. (October 25, 2018). Artificial Intelligence & Human Rights: Opportunities and Risks, Berkman Klein Center Research Publication No. 2018-6.
- (46) Richard D. Arvey et al. (1994, December 13). Mainstream Science on Intelligence. The Wall Street Journal.
- (47) Robert Yu (2017). The Machine Author: What Level of Copyright Protection Is Appropriate for Fully Independent Computer-Generated Works? University of Pennsylvania Law Review, Vol. 165
- (48) Room document for the 38th International Conference of Data Protection and Privacy Commissioners (2016). Artificial Intelligence, Robotics, Privacy and Data Protection.
- (49) Standing Senate Committee on Social Affairs, Science and Technology (2017). Challenge Ahead: Integrating Robotics, Artificial Intelligence and 3D Printing Technologies into Canada's Healthcare System.
- (50) Andrew Guthrie Ferguson (2015). Big Data and Predictive Reasonable Suspicion, 163 U. Pa. L. Rev.
- (51) Swanson, A., & Khan, F. The legal challenge of incorporating artificial intelligence into medical practice. Journal of Health & Life Science Law, 6(90).
- (52) The Institute of Electrical and Electronics Engineers (2017). The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, Version 2.



- (53) Tuomas Sorjamaa (2016). I, Author: Authorship and Copyright in the Age of Artificial Intelligence, Department of Accounting and Commercial Law, Hanken School of Economics, Helsinki.
- (54) UK's Parliament, Select Committee on artificial intelligence collated written evidence volume - House of Lords (UK) - Statement of Cooley (UK) LLP (written evidence AIC0217)
- (55) United States Government Accountability Office (2017). Artificial Intelligence: Emerging Opportunities, Challenges, and Implications for Policy and Research.
- (56) France Cédric Villani & Marc Schoenauer & Yann Bonnet & Charly Berthet & Anne-Charlotte Cornut & François Levin & Bertrand Rondepierre. (2018). For a Meaningful Artificial Intelligence - towards a French and European Strategy.
- (57) Singapore Personal Data Protection Commission (2018). Discussion Paper: Artificial Intelligence (AI) and Personal Data – Fostering Responsible Development and Adoption of AI.
- (58) India NITI Aayog (2018). Discussion Paper: National Strategy for Artificial Intelligence #AIFORALL.

## 中文資料

### 1. 專書

- (1) 三津村直貴（著），陳子安（譯）（2018），《圖解AI人工智慧大未來》，臺北：旗標。
- (2) 松尾豐（著），江裕真（譯）（2016），《了解人工智慧的第一本書：機器人和人工智慧能否取代人類？》，臺北：經濟新潮社。
- (3) John Frank Weaver（著），鄭志峰（譯）（2018），《機器人也是人：人工智慧時代的法律》，臺北：元照。

(4) 李有專(2018)，《醫療大未來—臺灣第一本智慧醫療報告》，頁142，新北市：好人出版

(5) 裴有恆、陳玟錡(2018)，《AIoT人工智慧在物聯網的應用與商機》

## 2. 論文

(1) 陳昭妤(2017)，《論人工智慧創作與發明之法律保護：以著作權與專利權權利主體為中心》，國立政治大學科技管理與智慧財產研究所碩士論文。

## 3. 期刊

(1) 蔡毓華(2018)，〈英國因應自動駕駛車輛上路，提出新保險責任制度〉，《科技法律透析》，30卷3期。

(2) 鄭志峰(2018)，〈自動駕駛汽車的交通事故侵權責任〉，《法學》，2018年4期。

(3) 柯亦儒(2017)，〈澳洲國家交通委員會提出自駕車試驗指南〉，《科技法律透析》，29卷11期。

(4) 陶盈(2018)，〈自動駕駛車輛交通事故損害賠償責任探析〉，《湖南大學學報》，32卷3期。

(5) 林美鳳(2018)，〈產業創新與管制革新—日本國家戰略特區制度等之啟示〉，《科技法律透析》，30卷4期。

(6) 吳柏凭(2016)，〈人工智慧對於著作權概念的衝擊：日本著作權的新政策發展方向〉，《科技法律透析》，28卷12期。

(7) 王果(2016)，〈論計算機「創作作品」的著作權保護〉，《雲南大學學報法學版》，2016年第1期。

(8) 易繼明(2017)，〈人工智能創作物是作品嗎？〉，《法律科學(西北政法大學學報)》，2017年第5期。

- (9) 王遷（2017），〈論人工智能生成的內容在著作權法中的定性〉，《法律科學(西北政法大學學報)》，2017年第5期。
- (10) 石冠彬（2018），〈論智能機器人創作物的著作權保護：以只能機器人的主體資格為視角〉，《東方法學》，2018年第3期。
- (11) 李偉民（2018），〈人工智能智力成果在著作權法的正確定性：與王遷教授商榷〉，《東方法學》，2018年第3期。
- (12) 曹源（2016），〈人工智能創作物獲得反權保護的合理性〉，《科技與法律》，2016年第3期。
- (13) 梁志文（2017），〈論人工智能創造物的法律保護〉，《法律科學(西北政法大學學報)》，2017年第5期。
- (14) 陳忠五，在餐廳滑倒受傷與服務欠缺安全性—最高法院100年台上字第104號判決評釋，台灣法學雜誌第183期。
- (15) 熊琦（2017），〈人工智能生成內容的著作權認定〉，《知識產權》，2017年第3期。
- (16) 劉影（2017），〈人工智能生成物的著作權保護初探〉，《知識產權》，2017年第9期。
- (17) 黎其武（2008），〈計算機輔助量刑系統〉，《湖北警官學院學報》，總第103期。
- (18) 趙廷光（2007），〈論電腦量刑的基本原理〉，《湖北警官學院學報》，總第95期。
- (19) 羅祥、張國安（2017），〈著作權法視角下人工智能創作物保護〉，《河南財經政法大學學報》，2017年第6期。

#### 4. 研究報告

- (1) 論壇「健康醫療資訊科技發展政策建言」委員會（2018），《健康醫療資訊科技發展政策建言》，苗栗：財團法人國家衛生研究院。
- (2) 經建會人力規劃處（2013），〈全球人口老化之現況與趨勢〉，《人口老化專輯》，臺北：台灣經濟論衡。
- (3) 騰訊研究院法律研究中心，《2018年全球自動駕駛法律政策研究報告》，2018年5月。
- (4) 證券暨期貨市場發展基金會（2018），《我國發展機器人理財顧問之研究》。

## 日文資料

### 1. 專書

- (1) 內閣府，新しい經濟政策パッケージ。
- (2) 中山信弘（2014），《著作權法》，第2版，東京：有斐閣。
- (3) 自動運転に係る制度整備大綱。

### 2. 研究報告

- (1) 国土交通省自動車局，自動運転における損害賠償責任に関する研究会報告書。
- (2) 総務省，AIネットワーク社会推進会議報告書2018。
- (3) 山本隆司（2018），〈AI時代の著作權〉，《NBL》，1131期。
- (4) 出井甫（2016），〈AI 創作物に関する著作權法上の問題点とその対策案〉，《パテント》，69卷15期。
- (5) 金岡京子，自動運転と民事責任をめぐるドイツの状況，自動運転と民事責任 特集，2017年1月。

- (6) 泉 真樹子，ドイツにおける自動運転車の公道通行―第8次道路交通法改正―外国の立法275，2018年3月。
- (7) 島田里奈，自動運転者をめぐる法律問題，企業会計，69期，2017年。
- (8) 第2回自動運転における損害賠償責任に関する研究会，資料1-2自動運転と民事責任ドイツの状況。
- (9) 奥邨弘司（2017），〈人工知能が生み出したコンテンツと著作権〉，《パテント》，70巻2期。
- (10) 新たな情報財検討委員会（2017），《内閣府知的財産戦略推進事務局新たな情報財検討委員会報告書》，東京：自刊。
- (11) 福田弥夫，自動運転と損害賠償責任，最近の調査研究から，2016年2016巻。
- (12) 総務省情報通信政策研究所（2018），《AIネットワーク社会推進会議報告書2018》。
- (13) 藤田友敬，自動運転と運行供用者の責任，ジュリスト自動運転と民事責任。