導覽文獻標題原名：Taking AI Personally: How E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence
導覽文獻標題翻譯：歐盟如何學習衡量個資保護與人工智慧？
導覽文獻作者：Matthew Humerick
導覽文獻來源：Santa Clara High Technology Law Journal, 34 (4)
導覽評論人：法務部司法官學院犯罪防治研究中心專案研究人員林俐如
論文最後閱覽時間：110 年 07 月 29 日

**文獻導覽僅係本中心為提供研究或政策參考，簡單摘譯外國文獻；如欲完整理解文獻架構與內容，尚請讀者自行查找前述資料來源，為進一步研究。**

壹、本篇文獻簡介

本文主要討論人工智慧在《一般資料保護規範》(GDPR，General Data Protection Regulation ）的限制下會遭遇何種不利影響，並試圖提供解決方案，以協助歐盟能在個人資料保護與人工智慧推動間取得平衡。

貳、 本篇文獻之內容概要

一、何謂人工智慧

人工智慧可概略理解為人類替一個系統編寫初始演算法，讓系統得以利用其所蒐集的大數據，透過不斷地學習和自動產出演算法，以達到系統在無需額外的人為監督或互動下，解決新問題的工作模式。

二、歐盟對個人資料保護的監管

歐盟自成立初期即針對個人資料保護推動相關立法，將數據隱私的保護精神深植於各規範中，例如 1995 年實施的《個人資料保護指令》(DPD, Data Protection Directive)。惟在科技的快速發展下，DPD 已顯得相對過時；同時，由於歐盟頒布的指令需要經過會員國的國內立法程序才具有效力，導致 DPD 的執行成效不彰。因此該指令被 2016 年通過、2018 年全面實施的《個人資料保護規則》(General Data Protection Regulation, GDPR)取而代之，也因為 GDPR 屬於歐盟條例，可以讓各成員國直接適用，影響力所及甚廣，故而引起各國

高度重視。

另外，2010 年公布的歐洲聯盟基本權利憲章，亦對個人數據保護定有明文：

1.人人均有權享有個人資訊之保護。

2.此等資訊應僅得於特定明確目的，且於資訊所有人同意或其他法律規定之正當依據下，公平地被處理。人人均有權瞭解其個人資訊，並有權要求銷毀其個人資訊。

3.應由獨立之主管機關監督這些原則之確實遵守。[1]

## 三、《一般資料保護規範》(GDPR，General Data Protection Regulation )

GDPR 堪稱史上最嚴格的個資法，雖然 GDPR 並非特意針對人工智慧而設，但因為人工智能系統運行多涉及個人資料處理，該規範可謂強烈衝擊人工智能的發展。

首先，GDPR 對個人資料定義採相對寬鬆的解釋，認為「個人資料」係指有關識別或可得識別自然人（「資料主體」）之任何資訊；可得識別自然人係指得以直接或間接地識別該自然人，特別是參考諸如姓名、身分證統一編號、位置資料、網路識別碼或一個或多個該自然人之身體、生理、基因、心理、經濟、文化或社會認同等具體因素之識別工具。[2]另外，GPDR 也定義「處理」為對個人資料或個人資料檔案執行任何操作或系列操作，不問是否透過自動化方式，例如收集、記錄、組織、結構化、儲存、改編或變更、檢索、查閱、使用、傳輸揭露、傳播或以其他方式使之得以調整或組合、限制、刪除或銷毀。[3]其參考過去在 DPD 實施時期的案例，例如歐洲法院將 DPD 解釋為得保護某些 IP 地址，因為控制者可以將他們的數據與第三方的單獨系

[1] 「永久和平發展協會『歐洲聯盟基本權利憲章』」，https://www.lawlove.org/Top8/discovery.php?act=one&b=EU.001（造訪日期：2021 年 8 月 5 日）

[2] 「國家發展委員會『歐盟個人資料保護規則本文部分』」，https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3J1bGZpbGUvMC8xMTY5MS9iNGZiZTA0OS1jYWQ1LTQ3MGEtYjhlMy00ZGU0NjhmOWIxMGMucGRm&n=5q2Q55uf5YCL5Lq66LOH5paZ5L%2bd6K236KaP5YmH5pys5paH6YOo5YiGLnBkZg%3d%3d&icon=..pdf（造訪日期：2021 年 8 月 5 日）

[3] 同前註。

統進行比較，最終可推衍出某些私人資訊。據此應得合理推論在更嚴格的 GDPR 下，若前述 IP 地址被第三方使用會違反 GDPR。

再者，依據 GDPR 對領土適用範圍的解釋，可知 GDPR 不僅一體適用於在歐盟註冊登記的公司，任何要販售商品或服務到歐盟的企業，或是會蒐集歐盟公民個資的企業，都會受到 GDPR 的監督。且一旦違反 GDPR 情節嚴重，最高可能處以 2,000 萬歐元，或全球年營業額 4% 的罰鍰。

因此，在人工智慧開發模式與 GDPR 不符的困境下，將生許多問題，以下說明資料主體行使同意權、刪除權、資料可攜性權利和解釋權時，會對人工智慧產生何種影響。

(一)　同意權

控管者(controller)利用數據時，除須得資料主體(data subject)同意外，控管者也應證明資料主體已同意處理其個人資料。相對地，資料主體得撤回同意的權利。

然而，同意權的撤回會制約人工智慧系統對數據的學習。雖然同意權撤回前，系統對數據資料的應用為合法，然而後續任何進一步的學習都可能涉及原先撤回數據衍生物，故將生「如何同時使人工智慧停止從數據中學習，而不影響其先前之學習與開發」的難題。除非控制者設計出可以隔離的學習鏈，惟必須認知到人工智慧系統如神經網絡般複雜，如何區別各交織的數據，於實務運作上有極高難度。

(二)　刪除權（被遺忘權）

縱然刪除權的行使並不至於破壞人工智慧系統完整性，但一個刪除權的行使可能會影響多個人工智慧系統，此外，刪除數據也會降低人工智慧演算結果的準確度和可靠性。

再者，系統該如何刪除數據與避免非法保留個人數據，有兩條路徑可供參酌。其一是供公司使用修改後的人工智慧模型重新學習現有的數據，然因為人工智慧系統不得不重新訓練，恐生額外的研究成本和拖延開發進度，最終導致公司選擇直接停止與歐盟以及在歐盟內部的業務。另一方法為公司可以開發專門計算法

來消除某些數據輸入的問題，雖然此辦法無需再命人工智慧系統重新學習，但是公司不可避免地需支出額外的研發成本，並且系統在應用上仍可能會面臨 GDPR 適法問題。

（三） 資料可攜權

賦予資料主體擁有資料可攜權，將使個人資料得以透過有結構的、通常使用的、機器可讀的形式傳輸予其他控管者，雖然在某程度上會減輕控管者蒐集個人資料的難度，但也可能會對數據控管的競爭市場產生不良影響。

資料可攜權或許會降低公司對數據的取得成本，因而有助於整體人工智慧的發展，惟該權利隱藏著讓人工智慧系統產業垮台的巨大風險，一旦發生資安疑慮或同業間惡意競爭，大規模的資料轉移恐會造成人工智慧系統不可回復的損害。

（四） 解釋權

資料主體得要求控管者對其為解釋，然此解釋權的賦予限制了人工智慧自主性、自動化的特質，好比深度學習，有如在黑盒子內進行的過程，究竟如何決定數據的關聯性與權重以形成決策，向來是個難解的謎團。又從 GDPR 第 22 條可知，即使受自動化決策，個人仍然有權知道它的存在，且得要求控管者提供所涉邏輯的有意義信息，以及此類處理對資料主體的重要性和預期後果。

尤其是商業面向的人工智慧系統，以個人的廣告投放為例，其善於分析、預測消費者的個人特質，然而在 GDPR 下，資料主體可能會拒絕人工智慧為前述的分析和預測行為；另外，規範中不存在例外允許的情況，將使人工智慧系統無法對數據為廣泛學習。

四、歐盟對人工智慧的監管立場

根據歐洲議會下法規事務委員會(Legal Affairs，JURI)過去報告顯示，議會曾有倡議建立專門管理人工智慧的獨立機構，由機構提供技術、道德、監管等專業知識，惟機構的建置目的著重在解決數據隱私保護問題，而非以協助人工智慧發展為設立宗旨。

此外，英國資訊專員辦公室（ICO，Information Commissioner's Office）雖曾提及當前立法中的數據保護概念不適合目前數據分析環境，會對人工智慧發展產生威脅，但並未提出任何修法建議，反而強化支持 GDPR 的立場。故參酌以上聲明，應可推測即使歐盟未來頒布新法也不太可能處理人工智慧在 GDPR 上的適用爭議，進而可能扼殺歐盟尋求方案解決數據隱私對人工智慧衝擊的機會。

## 五、在 GDPR 下的人工智慧發展解決方案

如何解決數據隱私保護對人工智慧的威脅，文獻作者提供兩種解決方案，分述如下：

### （一） 將人工智慧排除於 GDPR 外，另設管理規範

鑒於 GDPR 下對領土適用範圍的解釋，可謂歐盟有廣泛的領土管轄權，故在嚴厲的管制下，相關企業都有可能因領土適用範圍被訴，造成跨國企業選擇轉往歐盟以外地區發展。

歐盟應如多數國家一樣意識到資料保護規範造成的潛在不利影響，而不是利用 GDPR 保留其國際管轄權，並推動人工智慧配合 GDPR。以資訊遺忘權為例，應不強調完全刪除資訊，而是思考如何保留部分資訊，確保資訊在未來不會被學習，使人工智慧系統不需要重新學習和建構，並在個人隱私與數據發展間取得平衡。另外，需要將人工智慧系統視為一般的人類信息，而非僅是資料蒐集的觀念，故不應要求人工智慧系統如何遺忘與不學習，而是如何將學習行為與學習中所取得的數據分開。綜上所述，在了解人工智慧系統與一般系統對數據應用上的差距後，建議將人工智慧獨立於 GDPR 外，另設管理規範。

### （二） 支持合於 GDPR 的人工智慧系統發展

歐盟得仿效中國政府資助企業對人工智慧發展的作法，鼓勵企業設計符合 GDPR 的人工智慧系統。現今的人工智慧系統得反向追溯到特定人的個人資料，而 Google 跟 OpenAI 建立了一個追溯性較低的演算法，可以讓人工智慧系統學習但又彷彿未看過那些數據，雖然該方法的準確度會較傳統人工智慧系統為低，但可以符合 GDPR，值得企業進一步發展。又政府支持合於 GDPR 的人

工智慧系統發展的同時，也可能會放寬對 GDPR 的執行，對人工智慧發展可謂利大於弊。

## 六、結語－與我國實務的連結

目前我國政府正積極向歐盟爭取 GDPR 適足性認定（adequacy decision），以便個人資料能夠在我國及歐盟間自由傳輸。惟在取得適足性認定前，從事跨境個資傳輸的企業僅得選擇遵循標準個資保護契約條款（Standard Contractual Clauses）、拘束性企業規則（Binding Corporate Rules）、行為守則（Codes of Conduct）或取得特定認證（Certification）及符合其他例外情形下，企業位於歐盟分支機構的資料才能回傳我國。[4]

無論如何我國政府必須意識到，適逢智能革命時代，該如何迎接人工智慧發展，並緩解科技應用對個資維護帶來的衝擊，以及思考在我國個人資料保護相關法規調適與鬆綁的同時，如何將 GDPR 的要求納入考量。易言之，須在「促進個人資料之合理使用」與「避免人格權受侵害」間取得平衡，始堪完備。

[4] 「國家發展委員會『歐盟「一般資料保護規則」(General Data Protection Regulation, GDPR）簡介』」，
https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3J1bGZpbGUvMC8xMTY4Ny81Y2M4ZjAyNy0wMGFhLTQxOGQtYTBjZi0zMDRkZDE1YTc5NmIucGRm&n=R0RQUuewoeWgsS5wZGY%3d&icon=..pdf（造訪日期：2021 年 8 月 5 日）