人工智慧時代的個人資料與疾病控制

劉靜怡*

人工智慧可以基於資料進行運算，從人類的行為中推測出其健康情形，即使該等人類行為與健康情形不盡然有直接關係，亦然。同樣地，人工智慧時代中各種數位科技的運用，可以監控特定個人的位置並據以追蹤傳染性疾病，也可以從個人消費紀錄中辨識出懷孕的顧客，甚至可以從社群網站的資料辨別出潛在自殺者。換言之，現代人的網路生活特性，使得上述推測、監控與追蹤成真，無論是社群網站、智慧型手機、穿戴裝置，以及其他各種主動提供個人資料或被動繳出個人資料紀錄的行為模式，都因此製造了「潛力無窮」的數位足跡。

在其原始型態下，上述數位足跡並無特殊的作用可言，然而，透過演算法，人工智慧科技卻可以把這些資料轉化成所謂的「緊急醫療資料」（Emergent Medical Data，簡稱 EMD），發揮一定程度的監測疾病功能、達到某些公共衛生目的[1]。換言之，「緊急醫療資料」可以簡單定義為：透過人工智慧或機器學習，從與健康情形沒有直接關聯的各種細瑣零散（trivial）行為中所推論（infer）或推測出來的健康資料（health information）或醫療資料。

究其實際，EMD 在本質上其實不同於一般傳統的醫療資料，尤其從傳統的醫療照護脈絡來看，醫療資料通常都是個人自願分享的結果，而且在現狀下也受到醫療相關法令的保護，以確保個人醫療或健康隱私不至於陷入遭受侵害的局面。相對地，EMD 到底是如何蒐集、處理和運用，以及 EMD 何以應該被當成一種新興型態的健康或醫療資訊予以管制，以便適當地處理 EMD 的取得——無論是基於商業、醫學或者公共衛生目的而取得——所帶來的種種法律、倫理和社會層面的影響。

* 國立臺灣大學國家發展研究所專任教授、中央研究院法律學研究所合聘研究員、中央研究院資訊科技創新中心合聘研究員

[1] See generally *Mason Marks, The Right Question to Ask About Google's Project Nightingale*, Slate (Nov. 20, 2019), available online at https://slate.com/technology/2019/11/google-ascension-project-nightingale-emergent-medical-data.html

如前所述，傳統的醫療資料通常是在醫療環境下由患者自願提供，其目的在於接受精確有效的診斷和醫療，而患者通常是在信任取得資料者的醫病關係脈絡下提供之。相對地，EMD 則是透過各種數位科技手段從人類日常生活中以隱密的方式取得。同時，由於目前關於 EMD 的蒐集處理利用過程，通常並未有如前述醫病脈絡下一樣具有嚴格的專業準則作為控制基礎，因此比較容易出現隱私侵害和歧視風險。至於為何要取得 EMD，則有可能是基於流行病學研究、公共衛生監控、甚至對於自殘自傷等行為進行監控的公共利益的目的。也曾有研究者針對 Facebook 使用者的線上行為進行研究之後，發現某些字眼的使用與特定的健康或醫療情況有相關。像是一定的宗教語言與糖尿病有關、敵意字眼與藥物濫用有關等等。[2] 而 EMD 的取得和運用，則在人工智慧和機器學習的演算法加持下，變得更加具有吸引力。因為，EMD 不但可以協助非醫療機構從非醫療資料中推論出醫療資料，而且不必遵守關於醫療法規對醫療資料的規範。換言之，幾乎任何人均可能在人工智慧與機器學習的協助下，取得本質上相當敏感的 EMD，並且基於各種的目的加以利用。

然而，由於 EMD 往往是透過網路使用者或消費者行為而取得，而且通常是暗中取得、違反當事人預期的倫理爭議，甚至，EMD 的取得是透過分析社群媒體上的貼文、電子郵件中的訊息、拍賣網站上的瀏覽記錄所得，對身為資料主體的個人而言，EMD 完全不是在其所得掌控或預期的資料脈絡下所形成的，也就是完全沒有預料到其與自身健康毫無關聯的行為資料，會變成另一種新型態的醫療資料，使用在各種紓解緊急狀態或疾病控制的脈絡下，甚至也可以大量使用在各種商業用途上。更有甚者，與醫病脈絡下的診斷不同的是，EMD 這種偏重特徵描述的資料乃是基於「可能性」而生，而且，病患去找醫生的目的是為了接受診斷，但是，個人上網的目的則不在於接受診斷，更未同意基於醫療目的使用其個人資料，尤其許多 EMD 的取得與處理利用，是透過智慧型手機中的應用程式暗中蒐集資料，未取得用戶的真正同意，甚至這類針對網路平臺、穿戴裝置、定向行為廣告受眾進行分類，進而透過投放不同資訊並觀察其反應，以達到特定研究目標的研究，往往欠缺制度性的倫理審查機制（Institutional Review Board，簡稱 IRB）把關受測者或個資主體的權利，也是不該忽視的個資風險。諸如此類的研究，研究者對於受測者應該負擔注意、保密和忠誠義務，但是，在 EMD 目前的發展過程中，不但忽略上述義務，也未透過 IRB 的審查來確保這些義務的落實，則是另一個有待建構的規範面向。換言之，如何確保

[2] Raina M. Merchant et al. (June 17, 2019). *Evaluating the predictability of medical conditions from social media posts*, *PLoS ONE*, 14(6): e0215476. https://doi.org/10.1371/journal.pone.0215476

使用 EMD 的公司與研究者落實對資料主體的受託責任，而且基於 EMD 的準醫療資料性質，應該必須負擔比較高的受託責任，或許是應該採行的法律與倫理規範方向。

就法律規範層面而言，是否應該對特定情境下的數位足跡蒐集處理利用，予以一定程度的限制，並且規範其使用方式，例如在目的上必須限於公共衛生領域的需求，或者禁止涉及醫病關係或自殺專線的資訊被蒐集，甚至在資訊類型上限於公開可取得且不具有任何隱私期待的資訊，均是應該考慮的方向。接著，就 EMD 的演算法而言，管制 EMD 的演算法，針對演算法可能對社會帶來的風險和效益予以規範，並且要求這類演算法必須滿足一定的安全測試標準，若未能通過上述檢視並獲得政府許可，即使取得當事人同意也不得從事 EMD 演算，固然是可能治理模式之一，但通過的標準應如何設計，以及管制者應該如何規劃其風險評估架構，包括 EMD 隱含的標籤化、歧視和操縱等風險，都有待深入探討。相對地，其他治理模式，則可能包括強調不符合公共利益要求的使用即應禁止，或者修改「告知後同意」原則內涵並強化資料受託人義務的管制等等。

總之，EMD 這種因為人工智慧出現後的新類型醫療資料，雖然有其益處，但也可能帶來不少社會風險，而且目前仍有許多規範漏洞，尤其 EMD 潛藏的不符社會規範、違背個人隱私期待、違反道德標準而造成權益侵害甚或危及醫病關係的爭議，將是人工智慧時代難以迴避的課題。