提高科技信任，堅實新興科技發展基礎

陳宗胤/工研院產科國際所

近年來，由於運算速度大幅提升與晶片製程演進，加上全球產生的資料量迅速增長，讓結合大數據與機器學習的人工智慧掀起創新巨浪，除了業者積極布局外，各國政府都將 AI 視為重要的科技發展項目，深怕錯過了這項科技帶來的改變與機會。因此，可以看到許多國家推出國家級策略，如美國的人工智慧倡議、歐盟的資料戰略與人工智慧白皮書、法國的 AI For Humanity、日本的 AI 戰略、韓國的人工智慧國家戰略、新加坡的 AI Singapore 等，都以政府力量與資源推動人工智慧發展。

在歐盟的部分，政策推行重點放在創建數個歐洲資料空間(European data space)，建立資料與數據自由流通的規則與執行機制，同時保障個人權益，並明確列出高風險 AI 與建立強制性的監管框架，控管 AI 應用可能帶來的風險，這兩點與本次全科會子題 2-4「科技風險評估與資料管理」不謀而合。

除了國家級策略以外，今年成立的全球人工智慧夥伴關係(GPAI)，也宣布將以符合人權、基本自由和共同民主價值觀的方式，負責任且以人為本的支持 AI 的開發和使用，可以看到這些由大數據驅動的新興科技，未來發展重點不再僅僅只是技術突破，而是逐漸轉移到了民眾是否信任這些科技的安全性。各國政府之所以採取這些措施，是由於人工智慧雖然帶來許多創新可能，但其不透明的黑盒子特性，加上需要使用個人資料的敏感性，造成社會大眾對人工智慧可能產生歧視與侵犯隱私的疑慮日漸提高，所產生的不信任感可能造成不願意接受這類新興技術。

因此，為了順利推動這類新興技術的發展，除了技術面的解決方案，例如可供檢視決策過程的可解釋性 AI(Explainable AI)，與避免個資隱私外洩的聯盟式學習(Federated learning)之外，政府更必須致力於良好基礎環境，特別是軟性環境的建置，包括法制框架、倫理論述與資料共享與治理機制，讓社會大眾願意相信在享受人工智慧所帶來的利益同時，不會被其負面特質所傷害。