韓國人工智慧風險管理趨勢研析

韓國人工智慧風險管理趨勢研析

資訊工業策進會科技法律研究所
2020年6月25日

人工智慧技術正不斷地突飛猛進，後更因深度學習應用帶來令人難以置信的進步，迅速成為眾多產業轉型的重要推手。然而，當眾人專注於追求人工智慧的逐利時，也隱然意識到人工智慧與現實世界的互動，似已超越人類認知能力，或依當下技術知識經驗仍難加以掌握。以自駕車為例，其利用感測器感知外界進行影像辨識、理解預測進而做出決策的整體流程上，不論是在路人、車輛等圖像辨識、現場就路人及車輛行動之預測，乃至後端根據前階段路人、車輛行動預測與現在位置判斷最佳路徑的過程，處處是不可測的風險。申言之，從辨識正確率、現場狀況理解度至演算法決策來說，吾人所得掌控者有限。主因在於人工智慧的複雜與靈活性特色，實難通過統一概念加以界定。次者是人工智慧的自動化決策本身，事實上難以被確實地預見。甚至，就人工智慧可控性上，亦充斥各類不確定要素，特別是訓練資料偏差、又或設計者主觀意識之偏頗都可能造成預想之外的結果。

截至目前為止，人工智慧應用已然帶來已引發諸多風險議題，包含於開發、設計及製造端所論及之風險議題涵蓋歧視與偏見，如資料偏差、樣本資料結構性不平等[1]致使機器學習或有偏誤，進而影響判斷，產出具有歧視或偏見之結果[2]；個人資料及隱私保護上，則係因人工智慧訓練對資料具有大量需求，涉及個人資料部分，將面臨蒐集（踐行告知程序）、處理和利用（於當事人同意之範圍內處理、利用）是否善盡保護義務與合乎法規要求；演算法黑箱帶來不透明的決策，難以預測與檢驗決策流程、判準是否有誤[3]。就此，考慮到人工智慧之重要性與風險，或有必要立基於風險預防理念進行相關風險控管，甚或以風險責任分擔角度，討論相關權責分配，以應對未來可能衍生的危害或重大風險。

人工智慧風險控管之法律基礎無法悖於倫理道德基礎。觀諸國際間討論，韓國早在2007年即已倡議機器人道德理念，並在2008年起接連有相關立法舉措。本文將以之為中心，探究其人工智慧在風險控管之相關立法政策措施，盼可從韓國做法中反思我國推行人工智慧風險管理之方向。

壹、事件摘要

一、韓國智慧機器人相關法制措施

（一）《智慧機器人發展和促進法》風險管控介紹

2008年9月韓國《智慧機器人發展和促進法》（지능형 로봇 개발 및 보급 촉진법）正式生效。該法旨在鋪設智慧機器人產業發展之法律基礎，包含在法律中嘗試引入智慧機器人定義（指通過識別外部環境並判斷狀況後自動運行之機器設備，包含機器設備運行所必要軟體），以此作為後續促進產業發展、規劃機器人責任歸屬或保險等討論之開展基礎；另外也以促進產業發展觀點，訂定產品安全開發與布建之支持法源依據；挹注國家科研能量確保技術穩定；建置智慧機器人產業分類系統，依此做為機器人產業統計基礎，為國家在機器人管理及政策提供相關數據。

其中，特別的是除了促進性規範外，亦首度於法律提出機器人倫理道德的概念，賦予主管機關訂定與「機器人倫理道德憲章」（로봇윤리헌장）相關內容之義務。

所謂「機器人倫理道德憲章」，係指針對智慧機器人功能及其智慧化發展，規範製造和使用人員之指導方針，以防杜危險發生並避免機器人不利於人類生活品質。換言之，機器人倫理道德憲章可認為是針對智慧機器人開發、製造、使用上的準則，盼可用以防止因智慧機器人功能而衍生之社會損害。就此，韓國工商部曾擬定《機器人倫理道德憲章草案》，可參考如下：

第一條（目標）機器人倫理道德憲章目標係為人類和機器人共存共榮，並確認以人類爲中心的倫理規範。
第二條（人與機器人的共同原則）人類和機器人應當維護相互之間生命的尊嚴、資訊和工程倫理。
第三條（人類倫理）人類在製造和使用機器人時，必須使用良好的方法判斷和決定。
第四條（機器人倫理）機器人是順從人類命令的朋友或是協助者、夥伴，不得傷害人類。

第五條（製造商倫理規範）機器人製造商有義務製造維護人類尊嚴之機器人，同時，必須承擔回收機器人、資訊保護義務。
第六條（使用者倫理）機器人使用者應當尊重機器人爲人類的朋友，禁止非法改造和濫用機器人。
第七條（實施的承諾）政府和地方政府應實施有效措施，以體現《憲章》的精神[4]。

觀察《智慧機器人發展和促進法》內涵，富有藉重法律效果與效能引領智慧機器人產業發展之精神，企圖形成政府政策借助立法促成經濟層面活動向上發展。然而，隨智慧機器人技術逐漸深入社會，韓國旋即意識到人工智慧在權益維護、風險管控上仍有進一步補強之必要，進而提出《機器人基本法草案》，並開展韓國在機器人倫理道德、歸責原則之相關討論，以順應社會整體的變革。

（二）《機器人基本法草案》

如前所述，意識到人工智慧發展已然滲入日常生活，有必要在機器人普及化的社會接受過程中，應對各類問題預先防範。韓國國會議員遂於2017年7月19日提出《機器人基本法草案》（로봇기본법）以反映機器人發展趨勢與問題。

《機器人基本法草案》主要目的是為機器人融入社會過程中的政策方向、原則進行引導，以有助於機器人產業健全發展。是以，該法在風險控管部分，通過二類做法予以調控，一是建立倫理道德準則之原則、二是嘗試提出歸責原則以釐清相關應用所生之爭議。

一者，藉道德倫理界線之提出使產業更為允當運用人工智慧。借用產品生命週期之概念，分就設計、製造以及使用者責任三階段規範。在設計階段，著重於產品內部構造、軟體介面設計的安全性，另就不侵犯人權及社會利益上，強調預先從設計確保產品永續性、倫理性及使用上的安全性；在製造階段，則從遵法性、說明義務及產品維護修繕責任等，揭示製造商在產品製造、銷售應行之事項；最後，則從使用者角度，以應用階段各項自律、他律規範，明示遵法義務與道德倫理原則，並特別指明宜避免過度成癮。

次者，在責任分配與歸屬上，於現行法令無以適用情況下，允許受損害者得向機器人之銷售者或提供者求償。然而，為免製造商或銷售者過度承擔賠償責任之風險，亦設置免責條款，規定當產品因缺陷致使損害發生，而該缺陷係以當時技術水準所無法發現之情況，或是該缺陷是製造商遵守當時機器人法令所規定標準所肇致，則將免除製造商之損害賠償責任。

綜合前述，《機器人基本法草案》在倫理道德及責任分配歸屬的風險管控上，提出諸多可資參考之方式，然而在基本法審議過程中，韓國政府認為雖有必要管制風險，卻不宜過早以立法手段介入遏止創新，而未能通過韓國國民議會。

（三）韓國人工智慧國家戰略

雖然《機器人基本法草案》未能立法通過，然而韓國相關立法脈絡已展現除關注於促進智慧機器人產業發展外，在倫理道德、責任上的風險調控亦不可偏廢態勢，且從智慧機器人進一步聚焦於人工智慧。

2019年12月第53屆總理會議（국무회의）[5]，韓國擬定涵蓋科學資通訊技術部在內所有部會共同推動之「人工智慧國家戰略」（AI 국가전략）作為橫跨經濟和社會的創新專案[6]，以攻守兼備方式發展人工智慧。分從技術、產業、社會三方面著手，為韓國發展人工智慧半導體產業取得先機，進而拔得在相關領域的頭籌；次者，完備先進資通訊技術基礎設施，借力人工智慧積極轉型為新世代數位政府；其三，從教育扎根，建設人工智慧教育體系以培植相關領域專業人才；第四，秉持「以人為本」精神發展人工智慧，建立人工智慧倫理原則、擴張就業安全網保障勞工，使人工智慧所產生之效益可散發至社會各個角落。預計通過該戰略，將可在2030年壯大韓國之數位競爭力，使人工智慧經濟產值增長至4550000億韓圜（約3800億美元），提升國民生活品質[7]。

整體而言，該戰略建立基於技術的立法、以人為本的道德以及改善整體社會法律體系三者為核心。基於技術的立法，如《信用資訊法》修訂，允許假名化資料利用，以鬆綁人工智慧資料應用需求，並平衡隱私保障；以人為本的道德，像是參考國際間道德倫理之標準，推行「人工智慧道德標準行動計畫」（AI 윤리기준 및 실천방안 마련），加速研擬建立在安全、責任或是擔保上的規範[8]；改善整體社會法律體系，包含修正《國民就業援助法》擴大就業安全網，透過保險、教育、就業支援等方式協助受人工智慧衝擊影響之勞工、《就業政策基本法》中研擬為人工智慧業務建立相應人才教育。三者之推動，除帶動人工智慧產業蓬勃發展外，也兼顧社會層面道德、權益保障。

貳、重點說明

一、以剛性立法手段推進產業發展

觀察韓國，其人工智慧發展態度係以鼓勵為重。主因在於對企業來說，採用新興科技應用或可能囿於法遵成本、研發投資耗費過鉅、相關領域人才稀缺等多重因素而有所疑慮。有鑑於前開問題，韓國以正面態度，在風險控管措施上，嘗試藉由法規手段解消人工智慧發展所面臨之問題，即在賦予政府確實制訂與推進人工智慧發展政策責任，使業者可預期政府態度；次者，設置法律作為行政機關提供產品安全開發與布建支援依據，確保科研能量技術的穩定；再者，藉由智慧機器人分類系統建立產業管理與統計基礎，俾利後續依統計數據進行決策。

至於權益保障、風險如何評價及規範，雖有論者倡議另制定《機器人基本法草案》彌補《智慧機器人發展和促進法》於法律內部體系權利價值詮釋上的缺陷，然經立法成本與當時技術成熟度之衡量，並未過早規範技術之發展。

二、借軟性規範措施型塑兼容並顧之環境

另方面，觀察韓國在面對人工智慧機器人時的應對方式，發現在促進發展上，韓國無不餘力地大力採用剛性立法手段，以鋪設技術、投資所需之基礎建設及支援。而就尚難定論之技術風險管控，像是倫理道德、歸責原則調控等，考量技術尚未臻成熟，實難以剛性立法方式加之管理，而有以政策方式先試先行之傾向，形塑具有包容彈性之環境，鼓勵人工智慧機器人產業之投入，並依此作為後續法規調適之基礎。

鑒於人工智慧機器人所涉領域之多元，誠然有必要以宏觀角度全盤檢視與調適相應之規範及措施。故而，韓國2019年底提出富含權益保障與經濟逐利精神之「人工智慧國家戰略」，並鏈結不同部會共司建立彈性包容人工智慧機器人產業之環境。

參、事件評析

綜觀上述，韓國面對人工智慧及機器人，對內，以剛性立法手段，先行鋪設智慧機器人產業發展之基礎，包含界定智慧機器人範圍、賦予行政機關訂定倫理規範等一定義務、設置行政支持法源依據、以分類系統規劃作為數據統計基礎進行決策等，以拉抬、激勵企業投入研發，促

成經濟層面活動之擴散與發酵；對外，以軟性規範宣示韓國政府發展智慧機器人產業態度、吸引國際間產學研能量挹注，並同步促成內部社會法體制之調整，不難看出韓國政府的企圖與決心，且整體上已約略有鼓勵、促進逐漸轉變為管理層面意味。

在我國方面，亦已意識到人工智慧風險管理之重要性，立法委員並在2019年5月倡議《人工智慧發展基本法草案》希望以制定基本法之方式，從研究、開發乃至整合等，厚植我國人工智慧實力，並嘗試建立人工智慧開發準則與倫理原則。韓國前述有關人工智慧之規範作法，或許可茲我國借鏡，就促進人工智慧技術經濟層面效益之面向，可由政府擬定具實質效力之法規範推動之；就現尚難明確定位之倫理準則及風險控管，採用軟性規範方式，先行以具包容性之政策、指引等作法試行，以待日後技術臻至成熟穩定，再行考量轉化為立法管理之必要。

[1] Crawford, K. et al. *The AI Now Report: The Social and Economic Implications of Artificial Intelligence Technologies in the Near-Term,* AI Now, 2016, https://ainowinstitute.org/AI_Now_2016_Report.pdf（last visited May. 22, 2019）

[2] Cassie Kozyrkov, *What is AI bias?*, https://towardsdatascience.com/what-is-ai-bias-6606a3bcb814（last visited May. 22, 2019）

[3] BBC, The real risks of Artificial Intelligence, http://www.bbc.com/future/story/20161110-the-real-risks-of-artificial-intelligence（last visited May. 22, 2019）.

[4] 김성원 선임,지능정보사회의 도래와 법·윤리적 과제- 인공지능기술의 발달을 중심으로 -, National Industry Promotion Agency（2017/11/15）, p10.

[5] 總理會議係韓國特有的系統，主要由總統、總理以及15位至30位不等之國務院成員共同組成，成員包含各部會之首長。主要職能是做為國家決策的機構，並協調政策或行政事務。詳細資料可參見：http://theme.archives.go.kr/next/cabinet/viewIntro.do。

[6] 〈정부, AI 국가전략 발표…"AI 반도체 세계 1위 목표"〉，Bloter，2019/12/17，http://www.bloter.net/archives/364678 （最後瀏覽日：2020/2/1）。

[7] 〈인공지능（AI） 국가전략 발표〉，과학기술정보통신부，2019/12/17，https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=_policycom2&artId=2405727（最後瀏覽日：2020/2/1）。

[8]〈인공지능 국가전략〉，관계부처 합동，2019/12，頁36-38。

本文為「經濟部產業技術司科技專案成果」

相關連結

What is AI bias?

The real risks of Artificial Intelligence

總理會議係韓國特有的系統，主要由總統、總理以及15位至30位不等之國務院成員共同組成，成員包含各部會之首長。主要職能是做為國家決策的機構，並協調政策或行政事務

정부, AI 국가전략 발표…"AI 반도체 세계 1위 목표"

인공지능（AI）국가전략 발표

相關附件

The AI Now Report: The Social and Economic Implications of Artificial Intelligence Technologies in the Near-Term [pdf]

你可能會想參加

→ 製程工業AI應用與規範研討會

蔡毓華
法律研究員 編譯整理

上稿時間：2020年09月

文章標籤

人工智慧

推薦文章