科技人權觀察：無縫雙面刃的國際輸出

翁逸泓*

摘要

中國在高端科技研發方面飛速發展，人民於近用資訊科技的機會大增，就中國境內對新興科技於經濟上加值應用深化與廣化來說，相當程度上對於包括財產權、智慧財產權等享有科技進步的成果的權利，有長足進步，亦可視為履行國際人權公約之進展。

不過，高端科技之應用不見得僅只帶來對於人權面向之益處，而通常會是一個雙面刃。就 2019 年度最嚴重與急迫之科技人權受侵害態樣言，本年度觀察重心在於中國之 ICT 相對提升而供做大眾應用後，人權與基本權利保障事項，尤其在政治與公民權利部分，可能因此發生一定程度之潰縮；甚至於在科技發展帶來之生活便利與經濟支持下，民眾對於該等侵害欣然、無感或是予以最大程度之容忍。本觀察評價中國科技人權領域相關指標包括：（一）線上：以科技方法阻礙資訊自由流通及監控；（二）線下：日常生活各面向之科技控制；以及（三）溢出：科技威權輸出。

就本年度觀察與去年度相較，在應用新興發展之科技於生活與政府監控上，似乎有進一步更趨緊縮之問題，並以增加打擊面之方式，持續墊高投入監控審查之成本，但基本上仍不脫相近似之手段：實名制、加重落地服務之 ISP 業者責任、備案、嚴懲。此外，監視之物理空間從重要交通渠道據點擴張至包括公園與校園等一般公共空間，甚至已然進入私人親密之

* 翁逸泓，世新大學法律學院副教授、英國德倫(Durham)大學法學院法學博士。本文感謝與談人與匿名審稿人給予的積極建議與幫助。

住居場域。不過，為反應輿情，政府提出了對「守法者」不擾民之政策，但是否能真正落實，尚有待觀察。又，在中國對於資訊不對稱與不實訊息之利用逐漸成熟之際，除對內利用諸如「學習強國」與「AI 謠言粉碎機」等應用程式進行洗腦與言論逆向追尋咎責外，中國並向外輸出或是利用該等技術。

綜言之，對於全方面應用科技以施行完美控制之模式言，今年度更加成熟，甚至可供輸出，並仍持續強化中。

關鍵詞：科技人權、信用評價、大數據、資訊自由、個資保護

壹、前言

科技人權之廣度包含了聯合國所肯認的所有關於「享有科技進步及其應用所得利益之權利（the right to enjoy the benefits of scientific progress and its applications）」（UNESCO, 2009）。由 ICCPR 來看，關於第 17 條私生活權利以及第 19 條表意自由權，乃至第 18 條的思想、信仰與宗教權利、第 26 條不受歧視與第 27 條少數民族之語言與宗教權利保障等其權利內涵也包括了至少有（資訊）隱私權、言論自由、（智慧）財產權以及不受歧視或不平等對待而近用科技之權利。另外，ICESCR 第 15 條第 1 項第 1 款關於享有科技進步的成果的權利、第 5 款對於智慧財產權之保障等，均應在網路空間中有所適用。從國際人權法之角度來看，個人對於資訊與通訊技術 (Information and Communication Technology, ICT) 之接近使用係較為晚近之保障事項，自歐洲理事會於 2009 年通過正式文件起，聯合國人權委員會（OHCHR, 2013）、歐洲人權法院、美洲人權法院以及歐盟執委會才以相對較為緩慢之速度加以承認（McDonagh, 2013）。

就網路普及與數位應用言，在統計上截至 2019 年 6 月為止，中國網民 (netizen) 規模為 8 億 5,400 萬，上半年新增網民 2,598 萬人，網路普及率達 61.2%，較 2018 年末增加 1.6%；中國手機網民規模達 8 億 4,700 萬，上半年新增手機網民 2,984 萬人，較 2017 年末增加 0.5%，網民中使用手機上網人群的佔比達 99.1%（中國互聯網絡信息中心，2019）。就該報告總結趨勢看來，中國之網路基礎設施建設的確優化升級。然而，卻仍有四成左右之人口仍未享有該項權利所帶來之利益，形成數位落差，相當地可惜。中國在高端科技研發方面飛速發展，人民於近用資訊科技的機會大增，就中國境內對新興科技於經濟上加值應用深化與廣化來說，相當程度上對於包括財產權、智慧財產權等享有科技進步的成果的權利，有長足進步，亦可視為履行國際人權公約之進展。

不過，高端科技之應用不見得僅只帶來對於人權面向之益處，而通常會是一個雙面刃。就 2019 年度最嚴重與急迫之科技人權受侵害態樣言，本年度觀察重心在於中國之 ICT 相對提升而供做大眾應用後，人權與基本權利保障事項，尤其在政治與公民權利部分，可能因此發生一定程度之潰縮；甚至於在科技發展帶來之生活便利與經濟支持下，民眾對於該等侵害欣然、無感或是予以最大程度之容忍。

就此而言，在中國近期對於使用資通科技對於民眾的監控以及人權侵害的問題上，所主要深刻影響的除了全民電子監控對於個人資料保護與隱私權之直接侵害，阻斷資訊對於人民資訊權以及其他權利事項如健康權之侵害外，較為特殊者也包括利用新興科技帶來的生活便利與經濟發展，使得人民樂於「自律」而對於人權之侵擾與社會控制。而此等社會控制方式也相當程度地反應了中共十九屆四中全會通過《中共中央關於堅持和完善中國特色社會主義制度、推進國家治理體系和治理能力現代化若干重大問題的決定》中，與過往不同而特別新增的「科技支撐的社會治理體系」。另外，此等以科技應用而全方面影響人民私生活面向與各項公民政治權利，甚至經濟、社會與文化面向權利之模式與技術設備，有外溢於領域外之現象。

準此，本觀察評價中國科技人權領域相關指標包括：（一）線上：以科技方法阻礙資訊自由流通及監控；（二）線下：日常生活各面向之科技控制；以及（三）溢出：科技威權輸出。

貳、線上：以科技方法阻礙資訊自由流通及監控

一、阻礙資訊自由流通

在意見、言論與新聞自由流通等人權保障事項之侵害中，原初之階段

乃為阻斷該等訊息的自由流通。中國於 2016 年頒布《中華人民共和國網絡安全法》作為網路管制之法律基礎，包含總則、網路安全支持與促進、網路運行安全、網絡信息安全、監測預警與應急處置、法律責任與附則等篇章，其中與網路監控較有直接關係者，仍依照人大常委會決定，[1] 為規範一般網路營運者義務，及關鍵資訊基礎設施營運者之義務而在網絡信息安全章中規範個人資訊保密，及對於網路資訊監控之相關規定；另在監測預警與應急處置章節中，規範網路安全事件之預警通報機制之建立，以及網路安全事件風險增加或發生後，各級政府應變措施與營運者應為之措施。

時至 2019 年，中國在審查網路訊息而阻斷資訊流通方面，已逐漸應用新興科技而試圖使審查更有效率與效果，而該等技術當然仍對於其國內發生影響。在本年度的觀察中，首先注意到的是中國仍相當地強調對線上資訊流之「導正」，而採取多面向之方式。另方面在阻斷對象上，其內容類型除了政權底線本身之防衛，亦即不准煽動任何對共產黨統治有影響的言論政治意識外，其餘社會生活面向之意識檢查也逐漸開展。

準此，先就科技阻斷資訊與言論流通言，本年度中國阻斷公民資訊權之方式約略如下：

(一)逐步增加防火牆的高度與翻牆的難度

中國亦以違反資訊隱私權及個資保護權利之保障，蒐集並分析翻牆工具（網路代理伺服器，Virtual Private Network, VPN）使用者瀏覽違禁網站的各種模式，諸如網站種類、內容、瀏覽時間等，並連結使用者身分，便可建立巨量資料（大數據，Big Data）加以分析，作為制訂網路查禁措施的依據。即便想翻牆脫離言論阻斷，中國許多透過手機 VPN 瀏覽國外網站的網友，只要被公安查到手機內裝有「翻牆」程式，皆會遭到行政

[1] 在2000年中國人大常委會即發佈《全國人民代表大會常務委員會關於維護互聯網安全的決定》。

處罰。例如，蘇州市廣播電視總台一位高官因使用 Twitter 和瀏覽境外網站，遭當地警方傳喚並被撤職降調（王兆陽，2019）。

更有甚者，原本的翻牆工具，其自身已然成為阻斷資訊與監控之工具乃至於除阻斷外尚以此揪出瀏覽群，進而對 VPN 使用者採取監控或其他線下強制措施。另外，中國之相對應策略包括斥資收購海外的 VPN 公司，以強化翻牆難度（VPN Pro, 2019）。[2]

（二）擴大審查工廠規模

中國在審查網路訊息方面，雖已逐漸應用新興科技而試圖使審查更有效率與效果，然而因為演算法技術仍未臻完美、敏感字詞的資料庫需不斷更新以外，[3] 人（網）民經常很有「智慧」地試圖繞過敏感字詞，因此人工審查仍不可少。非但如此，人工審查之投入甚至形成特殊新興行業。紐約時報 2019 年初報導揭露了網路審查工廠，該等審查工廠不僅對於言論形式，也對於言論之實質內容以人工方式進行審查，以博彥科技為例，其係總部在北京的一家科技服務公司，在其內容審查工廠僱用了 4,000 多名員工，日夜瀏覽和審查網絡內容（袁莉，2019）；對比 2016 年，這家公司僅有 200 名左右的審查員。值得特別注意的是，關於該等人工審查的人力，卻需要先透過教導何種實質內容被歸屬為「敏感」的培訓，而讓人玩味的地方在於這些原本對於政治毫無興趣之審查員，反而因此必須補充地盡力知道部分歷史與敏感字詞。

---

[2] 美國資安機構一項最新調查顯示，全球97家主要VPN業者中，至少有29家的母公司是中資公司，幾乎達三成。

[3] 在人工智慧的科技角力當中，如果比較中國與美國各自強項，則美國在運算的硬體芯片上具領先優勢，但是基於中國對於隱私權與個資保護之忽視，因此在個資取得上，中國相對保持優勢。而在此種科技發展之下，在中國AI領域最有「錢途」的行業應用，就是中共對民眾的監控，這種應用很多時候也被叫做安防、公共安全，或智慧城市。換言之，中國不但耗費中國納稅人的巨額資金用於「維穩」，為AI監控提供了龐大規模的市場需求；同時還為相關的AI研發提供從政策到資金、大數據的全方位支持。

關於該等敏感字詞，中國網絡視聽節目服務協會在官網發布《網絡短視頻內容審核標準細則》100 條規則，覆蓋範圍大到國家民族，小到私生活（人民網，2019d）。這些敏感字詞不僅止包含境內，即便是國際事件如委內瑞拉政變等，亦在禁止之列。相關字詞由於不確定性高，且打擊範圍面除政治言論等高審查密度言論以外，尚及於較低密度的商業言論如廣告以及卡通、動漫等，因此引起較大反彈。然而事實上，中國中央高層對此等反彈未嘗不識，早有提出「雙隨機、一公開」以為對應之道（人民網，2019b）。該概念主要是解決日常監管的問題，內涵主要包括兩點：一是切實解決一些領域存在「檢查任性」、「執法擾民」的問題，減少企業的負擔，對守法守信者無事就不打擾別人，沒事就不要檢查別人。二是實行政府部門有限監管資源最優配置，提升監管執法的效能和法律法規的震懾力，對違法失信者「利劍高懸」。

對此，在 2019 年中國第 13 屆全國人大二次會議中，國務院總理李克強在報告中表示將推行信用監管和「互聯網 + 監管」改革，以「優化環保、消防、稅務、市場監管等執法方式，對違法者依法嚴懲、對守法者無事不擾。深化綜合行政執法改革，清理規範行政處罰事項，堅決治理多頭檢查、重複檢查。對監管者也要強監管、立規矩，決不允許搞選擇性執法、任性執法，決不允許刁難企業和群眾。依法打擊制售假冒偽劣商品等違法行為，讓違法者付出付不起的代價」（人民網，2019c）。這在實務上後續是否真的將落實第一點內容，以及倘若未見具體落實，其可能激起之政治與社會效應又如何，仍待進一步觀察。

（三）阻斷工具進化：非結構式圖像審查

加拿大多倫多大學公民實驗室（Citizen Lab）發表研究報告，發現微信系統針對使用者所傳送的圖像建立龐大且不斷更新的資料庫，系統會自

動監測、辨認出「敏感」非結構式圖片，將之加入黑名單並刪除（Knockel and Xiong, 2019）。對使用者對話中發送的圖片進行實時自動檢測和審查時是基於圖片中包含的文字以及目標圖片與系統資料庫中的敏感圖片的相似度匹配。另外，微信主要審查政治敏感的圖片，這些圖片大多與政府和社會反抗等高密度品質之言論有關。

(四)內容風險控制師

人民網發放了首批共 67 張「互聯網內容風控師（初級）證書」（人民網，2019a），這也是中國對網際網路內容風控領域首次發放風控師證書。其宣稱內容風控培訓契合了互聯網發展的瓶頸和命脈，發揮黨報黨網在內容生產、質量管控、意識形態安全等方面的政策水平、豐富經驗，可以為所有借助網路進行形象傳播的政府部門、企業、NGO 和公眾人物，提供內容風控的諮詢顧問服務。而此種將線上言論審查予以證照化之情況，除有妨害表意自由之問題外，另涉及以經濟鼓勵之作為，扭曲民眾對言論自由與資訊權等基本權利之理解。

又，本觀察歸納對資訊流之障礙阻斷內容類型如下：

1. 公序良俗類型

例如微信平台發生公眾號持有者網紅「咪蒙」親上火線發道歉信，將自己的微博永久關閉，內容全部刪除。而其所謂「內容違規」，係指文中飽含的負能量與厭世感：在中國，勵志的文章被稱為「雞湯」，而渠等辛辣厭世的文章被稱為「毒雞湯」，該等文章雖無國家意識之問題，但仍踩到「販賣焦慮」的紅線而成為禁區（蕭歆諺，2019）。

2. 災難維穩類型

在災難現場，為了「維穩」緣故，常以科技方式干擾新聞自由（蘋果

日報，2019a）。又，中國在 2019 年初有豬瘟、年底有鼠疫之疫情，在網路上對該等疫情之正確資訊均受到一定程度之阻斷或干擾，則除資訊權等基本權利受到侵擾，對於健康權來說，亦有重大之影響（自由時報，2019b）。

3. 特定企業保護類型

就在華為 5G 技術正受到海外普遍抵制之際，去年剛剛上市的 Nova3 手機突然爆炸，炸傷使用者大腿。但該消息見諸報端後，疑華為已啟動公關，中國社交媒體及網媒也開始大規模刪除這則華為手機爆炸的訊息（看中國，2019）。

4. 敏感事件排除類型

在六四的卅週年到來，中國全面強化線上與線下的資訊阻斷。據路透社 5 月 26 日報導，隨著六四臨近，中國廣泛應用網路機器人以加班加點的方式來審查網絡上與六四相關話題，就演算法之精進言，相關審查的精準程度也前所未有。其引述北京「字節跳動科技公司」匿名員工的話形容，人工智能就像手術刀，而人工審查像大砍刀。除了六四天安門事件外，臺灣和西藏等敏感詞也被大量偵測，在社群媒體平台上的貼文如果包含能讓人聯想到這些敏感事件的日期、圖像和名稱，就會被自動拒絕。在中國境內之社交平台微博、QQ、微信、貼吧、知乎、豆瓣、嗶站、淘寶、網易雲都不能換頭像，對於境外媒體的 Twitter 則顯示有封鎖狀況，也開始無法連結維基百科等大眾資訊查詢常用網站（中央通訊社，2019）。

第二個重大敏感事件則是香港特首林鄭月娥於 7 月宣布《逃犯條例》修例工作完全失敗，修訂草案已經「壽終正寢」後，中國關於其科技上阻斷，於香港發生之在香港人民反對修訂《逃犯條例》的抗爭當中，也扮演了相當重要的角色：群眾與政府在此進行激烈的攻防，隱私通訊軟體

Telegram 和智慧型手機小米 6 也都分別在網路戰場上亮相。另外在對中國內地方面，中國對此全面封鎖新聞，社群媒體微博、微信與百度相關的外媒報導均遭下架。同月，四川省宜賓市敘州區政府召開微信群主網路安全教育培訓會，重申微信群「九不發」原則，包括不發未核實的港、澳新聞等，並再提群員若因言獲罪，群主將可能連坐（LEE，孟寶勒，2019）。而自 6 月以來，微信系統申請新帳號非常困難，這是因為申請新帳號必須被另一個帳號批准，而另一個帳號必須存在六個月、「信譽良好」、一個月內未批准其他帳號成立。

二、利用科技方式線上監控

本年度對於利用科技方式而為網路上之監控作為，致使侵害人民私生活權利與資訊隱私權等，觀察如下：

(一)一體化聯合作戰平台

中國之監控已然發展出「一體化聯合作戰平台」之個資統合平台（聯合新聞網，2019a），用以將各類個人資料與其他關聯性資料整合後，對大規模之被監控者加以剖析（profiling）。例如就新疆言，報告顯示新疆政府透過一體化作戰平台，將民眾關於身高、宗教信仰到政治傾向等各類型信息，具體根據不與鄰居往來、拒用智能手機或積極替清真寺募款或募集物資等 36 種行為來鎖定可疑人物。然而，雖然蒐集大量人民個資，然而其資料庫的資訊安全卻可能因為法規環境的特殊性以及管制真空，反而造成除了國家監控以外的個人基本權利事項受侵害風險升高。

(二)各式官方與民間APP之監控：華為警務通

新款「警務通」是中國公安部第一研究所與華為合作，專為

MATE10/10Pro 手機所研發的雙系統，一是警務人員日常使用的系統，另一個則是可切換至公安內部數據庫的系統。根據報導，這兩個系統不僅可以安全獨立運行，還可以一鍵切換，更因為這款手機配有超強的人臉識別和生物識別功能，中國警察透過拍照或採集指紋，便可以從數據庫查到民眾的任何訊息（楊向文，2019）。

在監控社群平台方面，今年開始發現中國或中資的 APP 均可能有被監控可能，且其可能以掩飾之方式，使使用者放鬆警戒。例如，短片平台「抖音（TikTok）」近來十分地熱門，在全球每月活躍使用者數字達到 5 億，但美國智庫研究指出，抖音可能已成為西方國家的安全隱患，將使用者資料傳回中國，成為中國蒐集情報的工具之一（李台源，2019）。對此，美國加州一名女大學生更在一場集體訴訟控告抖音把私人使用者個人資料轉移到位於中國的伺服器（Paul, 2019）。

(三)香港612反送中事件個資監控等

香港 612 警民衝突後，有示威者在現場受傷到公立醫院求診時卻被警方拘捕，引發醫護人員洩露病人隱私與敏感性個資侵害的疑慮。有醫護人員揭發醫管局要求對求醫者進行標籤，以分辨病患是否參與衝突，以及分辨病患身份是「警察」、「記者」、「市民」或「其他」。

又，為了打壓如火如荼的反送中運動，香港政府利用數位足跡找出抗議者的真實身分，類似於中國的網路監控手法。為逃避政府的監控，香港的抗議人士選擇以隱私保護著稱的通訊軟體 Telegram 作為聯絡管道。然而在 6 月 12 日 Telegram 在官方 Twitter 發文表示遭受 DDoS 網路攻擊，其創辦人 Pavel Durov 更指出攻擊 IP 來自中國（楊安琪，2019）。

參、線下：日常生活各面向之科技控制

隨著資通訊（ICT）科技之長足進步以及法規範管制的短缺，中國近兩年的監控越來越嚴密，監控的手段越來越多。中國近年以維穩為理由持續加強社會控制，不斷發展各種監控技術，並利用生物識別系統等新興科技進行威權式社會控制。

一、私生活：手機、住居內智慧生活家電與身分證

據衛報、紐約時報和南德意志報的調查，中國對從接壤中國的吉爾吉斯共和國（Kyrgyzstan）入境，尤其是在偏遠邊境伊爾克什坦山口（Irkeshtam）進入新疆旅客，邊境職員會取去他們的手機，暗中裝上流動應用程式進行監控。另外，中國邊境官員已開始對香港進入中國旅客的手機進行例行搜查。

不僅在公開場合有空間監視之存在，中國為加強對居民的全面控制，此前已採用「天網」、「雪亮」等一系列高科技監控系統的相關工程，如今更全面要求屋主在出租房內安裝監視器。據報導指出，中國眾多省份的民眾從去年底紛紛反映，被警方告知若欲出租房舍，必須在室內安裝監視攝影機，並長期接受警方不定期檢查。警方表示，這一切都是為了防盜，一旦發現房內未安裝監視器，甚或是監視器無法正常運作，房東就會被開罰人民幣 500 元的罰金並強制改善狀況。

另外，安全公司 vpnMentor 研究人員在公開網路上發現一個內容豐富的資料庫，屬於 Orvibo（歐瑞博）的智慧家庭產品。其係總部位於深圳的智慧家庭製造商，公開的資料庫包含超過 20 億筆紀錄，涵括使用者姓名、ID、電子郵件、IP、密碼、家人姓名、家人 ID、連網裝置、重設密碼、及精確定位座標等。

在身分證方面，香港也計劃明年以免費方式為所有居民建立包含人臉

辨識在內的「數位個人身分」（eID），相關服務近日已確定由中國保險業巨擘「中國平安」旗下的平安科技，以 4,400 萬港元（約 1 億 7,200 萬元台幣）得標。

二、面部辨識

生物特徵之監控種類繁多，諸如最簡單的指紋，乃至虹膜、聲紋或是複雜的 DNA 等，在蒐集樣本後為了要發揮其功能，最重要者還是在於需有快速比對樣本之可能與普及性。其中，面部辨識因為面部之外露性、頻繁性以及採樣比對時可以依靠鏡頭主動採集因此具有比對上之簡便性，因而特別地容易侵害當事人之資訊隱私權以及個資保護權利等基本權利與自由保障事項。

在比對採集相關樣本上，中國不斷地強化其硬體設備，並大量廣布監視鏡頭。例如相關研究人員發表一個 500 萬像素的雲攝像系統，稱這個新型「超級相機」系統能夠在成千上萬的街頭人群中即時捕捉到每個人的面部細節，並精確定位特定目標，其分辨率是人眼的五倍，而且還配備了人工智慧（AI）、面部識別、即時監控和雲計算技術（自由時報，2019a）。

並且，在盡可能地擴充應用，使得人民不自覺地，或即便知道被蒐集也無法抗拒的層面上，獲得最多的面部對比。例如基於便利性，中國正迎向刷臉支付時代，以簡便之方式便可大量而較無感地蒐集面部特徵與對比樣本。當然這有很大的個資侵害風險與疑慮，事實上中國政府對此可以目的外使用，為了監控目的而利用該等個資，例如監視、監控、追蹤政治異議人士、控制社會和訊息等目的，出現如同針對新疆維吾爾人進行種族剖析的情形，甚至是預測性警務（predictive policing）（AFP, 2019）。

另外在各交通要道如機場、鐵路、口岸等，也開始進行面部辨識。繼廣州 4 個地鐵站試行「刷臉」進出閘口後，9 月 20 日深圳地鐵 11 號線也

開始試行人臉識別技術系統。年滿 60 歲的老人、身心障礙人士等免票人士實名註冊後，可「刷臉」免費進出站。新政策引發民眾擔憂個人隱私受到威脅，可能遭到當局監控，尤其是該處位於香港鄰近，對目前反送中運動來說，十分不利。

除實體空間的世界充滿面部辨識之外，甚至擴張至虛擬世界當中：中國工業和信息化部公布《關於進一步做好電話使用者實名登記管理有關工作的通知》，要求電信企業辦理民眾申請新門號服務時，除了要進行身分證實名制登記外，自 12 月 1 日起在實體通路全面實施人臉辨識比對措施，以確保「人證一致」。

三、步態辨識

繼人臉識別後，中國人工智能（AI）公司銀河水滴在北京宣布開發出全球第一個步態識別系統「水滴慧眼」：即使目標人物遮著臉，系統也可以依靠走路姿態辨認出來。步態識別擁有遠距離，全視角等諸多「獨特」優勢（自由時報，2019c），除供上萬部監視器實況同時運作，並支援巨量歷史鏡頭畫面與實況畫面的交互即刻檢索與定位。

四、腦波監控頭環

在中國，越來越多學校在教室配備人工智慧攝影鏡頭，讓學生戴上所謂的 AI 頭環。華爾街日報記者走訪上海一所小學，實地觀察小學生的生活如何被 AI 改變：雖然老師和家長認為，AI 頭環能讓學生更專心用功，提高成績，但是，加州大學舊金山分校神經科學家札托（Theodore Zanto），對於尚未成熟的腦電圖技術（Electroencephalography, EEG），大規模在小學生身上使用，卻沒有任何隱私權保護，感到相當驚訝（華爾街日報，2019）。

五、生物特徵樣本採集之全面化

關於行為式生物特徵，目前中國各大城市已建置步態辨識系統與面部辨識系統，其所獲得的監控資料，再經過後端資料庫的比對，可立即掌握特定人物的行蹤，並持續追蹤其後續活動狀況。過去幾個月來關於大規模生物特徵之蒐集大多發生在敏感區域如新疆，但這種狀況似乎已逐漸向其領土內部延伸。例如，廣東佛山丹灶公安於車站收集旅客的「口水樣本」，中國大數據收集從早前採集血液、聲紋、指紋等，現進階到採集公民「口水樣本」，顯示「新疆模式」正推廣至全中國（蘋果日報，2019b）。

中國公安部近期部署了在全國範圍內採集 DNA 數據，尤其是男性 DNA。例如鄞州警方在線（鄞州公安分局雲龍派出所）9 月 9 日回覆明確表明，是根據「公安部部署」要求，「近期將在全國範圍內開展國家 DNA 數據庫數據採集工作。近日，雲龍派出所已與鎮、村政府相關部門對接，在全鎮逐村開展男性家族 DNA 數據採集工作。」而安徽省肥東縣公安局的招標公告強調，該「男性家族排查系統建設項目」是公安部、省公安廳 2018 至 2019 年度部署的重點工作，用於將該縣男性家族排查系統建設所採集的人員樣本進行檢測，並記錄載入國家 DNA 資料庫，以建立覆蓋全縣的 Y-STR DNA 資料庫。[4]

六、信用評價系統

所謂失信被執行人在中國法律上的定義是經中華人民共和國各級人民法院認定的「被執行人具有履行能力而不履行生效法律文書確定的義務」，他們被中國法律規定不能買不動產、搭飛機、火車時不能坐二等以上艙位、也不能住星級旅館，甚至不能旅遊度假。

透過特徵剖析與信用評價之實際應用，中國河北省高級人民法院 1 月 14 日上線微信小程式「老賴地圖」測試版，可以偵測使用者 500 公尺內俗

[4] 第23對之Y染色體上，此Y-STR基因被作為鑑定男性身分的專屬系統。

稱「老賴」（未繳交欠債與罰款等失信被執行人）的失信[5]被執行人相關資訊，包括本名、違反了什麼規定，甚至還設計了分享機制，「方便」讓使用者隨時隨地分享身邊有多少老賴給朋友圈。然而，人權倡議者擔心，專斷的評量體系並為將個人因素列入考量，經常發生個人和企業在有失公允的狀況下，被評為不值得信賴。這尤其是在信用評價之評價標準不透明與不穩定的情況之下，非常容易發生（BBC 中文網，2019）。

在積極促進信用評價積分方面，中國官方宣傳國家主席習近平個人形象不遺餘力，近來配合高度發展的智慧型手機科技，推出一款名為「學習強國」的習語錄 APP，官方強迫近 9,000 萬黨員下載使用，並透過積分制變相強迫黨員每天使用，成效較低者還會被通報檢討。該「學習強國」應用程序的創建者為阿里巴巴。安裝「學習強國」，需要向該 APP 授予包括真實姓名、位置等多達 19 項具隱私性質的權限，如同移動監控設備。

七、新聞自由之保障：學習強國與AI謠言粉碎機

關於學習強國 APP，除前述關於監控問題外，尚因為中國中宣部傳媒監管局 8 月 23 日發出「關於在『學習強國』學習平台創建和認證新聞採編學習組織的通知」。根據通知，申領者須通過「學習強國」平台手機使用者端的培訓考試，之後才能申領新版記者證，而有妨礙新聞自由之疑慮。

另方面，阿里巴巴發布了一款旨在粉碎網路謠言和假新聞的「AI 謠言粉碎機」，分析表示「AI 謠言粉碎機」是中共藉高科技維護專制集權的維穩工具。然而，問題在於該等作為判斷標準之「訊息」，卻往往是中國政府「希望被聽到的」訊息，而無論其真偽。從而，該等「澄清」反而往往成為洗腦工具。

[5] 所謂失信被執行人在中國法律上的定義是經中華人民共和國各級人民法院認定的「被執行人具有履行能力而不履行生效法律文書確定的義務」。

肆、溢出：科技威權輸出

中國以科技控制作為手段而邁向威權之路，在達到一定的效果以後，開始向外輸出其數位監控技術與模式。

一、數位監控技術與設備之輸出

在被動受「裝置」中國數位監控技術的問題上，例如在 5 月初，美國國土安全部發布警報警告美國國家電視公司，中國製造的無人機可能會向其在中國的製造商發送敏感的飛行資料。該消息再度引發人們對來自共產黨統治的中國生產的智能設備的安全擔憂。據此，彭博社在 5 月的報導表示，有兩位知情人士透露，美國政府正考慮將五家中國監控設備公司列入與華為類似的「黑名單」，限制他們採購美國的技術和設備。這五家公司分別是海康威視（Hangzhou Hikvision Digital Technology Co.）、浙江大華（Zhejiang Dahua）、曠視科技（Megvii）、美亞柏科（Meiya Pico）和科大訊飛（Iflytek Co. Ltd）（聯合新聞網，2019b）。

此外，事實上也有國家主動地願意裝置數位監控設備，例如中國耗費鉅資打造的「AI 監控系統」甚至是數位威權主義引起許多國家的關注和興趣，在中國擴大監控範圍至全國之後，AI 監控技術的價格也隨之壓低並「外銷」到世界上其他國家。例如，自由之家去年發佈的一份報告指出，如今已有包括辛巴威、烏茲別克、巴基斯坦、肯亞、阿拉伯聯合大公國以及德國等 18 個國家使用中國製造的 AI 監控系統，還有 36 個國家接受中國進行「言論審查」的培訓（賴昀，2019）。

近來尤其是因為中國一帶一路政策的連結，據紐約時報報導，加入中國「一帶一路」計畫的南美洲國家厄瓜多以石油儲備為代價，向中國貸款 190 億美元建設水壩和煉油廠等基礎建設，同時購入中國的影像監控系統 ECU-911，在過去四年內在全國範圍安置了無數監視器鏡頭，並請中國

工程師前往厄瓜多進行使用技術指導。該系統主要由兩家中國公司製造，一家是國有企業—中國電子進出口有限公司，一家是有解放軍背景的公司華為。其後，委內瑞拉也購入了該系統，目標是在國內裝設三萬個監視鏡頭，玻利維亞和非洲國家安哥拉則緊隨其後。

二、境外監控與資訊戰主力：微信

由於微信不但是中國境內最多人使用的通訊軟體，在境外之華人也大多使用該通訊軟體，但微信有一個由公安部派出的駐地互聯網警察局時時刻刻都監管該平台執行中國法律。[6] 因此，相關研究者指出該大多人使用的便利性要付出浮士德式的代價（Thayer and Han, 2019）。此際，無論是在中國境內或是境外，華人或非華人，只要是該 APP 之使用者，在微信上流通的大量個人資料與言論分別受到中國法律規定之封鎖與監控；成為中國大外宣戰略重要武器，投放各種不實訊息。

三、境外蒐集個資之其他途徑

中國在境外蒐集個資並建立資料庫，而侵害外國人基本權利事項之問題已然成形。例如，8 月 29 日，中共內蒙古赤峰市委統戰部發布《關於在全市範圍內開展僑情台情調查統計的通知》，要求向該市國外華僑、外籍華人、歸僑、僑眷、港澳臺居民、留學生、歸國留學人員、港澳臺屬、僑資企業、臺資企業，了解基本情況，建立該地區僑情台情基本情況資料庫。

[6] 依據《中華人民共和國國家情報法》第7條：「任何組織和公民都應當依法支持、協助和配合國家情報工作，保守所知悉的國家情報工作秘密。」14條：「國家情報工作機構依法開展情報工作，可以要求有關機關、組織和公民提供必要的支持、協助和配合。」，而國家對支持、協助和配合國家情報工作的個人和組織，亦給予保護。另外，《中國共產黨章程》第30條規定，包括企業、農村、機關、學校、科研院所、街道社區、社會組織、人民解放軍連隊和其他基層單位，凡是有正式黨員三人以上的，都應當成立黨的基層組織。而其《公司法》第19條則規定在公司中，根據《中國共產黨章程》的規定，設立中國共產黨的組織，開展黨的活動，並為黨組織的活動提供必要條件。

境外的個資蒐集還包括文化語言類型，以隸屬於中共中央宣傳部的中譯語通科技有限公司為例，其整合中國國企、私營科技企業、境外高校等多方面的資源透過先進的自然語言處理與語義計算技術對全球巨量數據進行挖掘與分析。該公司蒐集全球 65 種語言的資料，並且將分析結果提供給政府以及企業客戶。

四、收購技術以達到威權監控

俄羅斯《消息報》在 6 月 3 日報導稱，華為已完成收購 Vocord 臉部辨識技術專利及開發團隊，而其部分員工正陸續調往華為（科技新報，2019c）。創建於 1999 年的 Vocord，是俄羅斯基於人工智慧生物辨識技術的專業視訊監控系統開發製造公司，而華為透過本次收購，能在最短時間獲得可應用的全球頂尖 AI 安防技術。

另方面，12 月紐約時報報導，新疆圖木舒克市採集了當地數百名維吾爾人的血液樣本，並據此建立基因資料庫，分析基因型與個人外觀特徵和家族血統的相對關係，以產出相應的人臉圖像。雖然相關技術在中國仍處於早期發展階段，所產出面部圖像的品質僅能用於縮小「肉搜」範圍和排除特徵不合的犯嫌，但專家憂心的是其真正意圖是打造有效工具，以強化對維吾爾族的歧視性政策，且未來甚至可將根據基因資料庫建立的人臉圖像輸入遍布新疆的人臉辨識和大規模監控系統，以加強偵測異議份子和罪犯，提升社會控制強度。而這項技術則似乎分別與德國頂級科學研究機構馬普學會（Max Planck Society）及荷蘭伊拉斯莫斯大學醫學中心（Erasmus University Medical Center）有一定程度之關聯性（Wee and Mozur, 2019）。

五、資訊戰之境外輸出

關於不實訊息（假新聞）與資訊戰之境外輸出，中國政治、經濟學者

何清漣的新書《紅色滲透》在 3 月出版，她認為，部分臺灣假新聞是出自中共的操作，有必要立法因應，她也表示，臺灣因為被中國視為核心利益，而無法避免這股「紅色滲透」。其中，透過購買社群媒體粉絲專頁之手法，企圖基於原信任關係而踐行不實訊息或洗腦資訊之投放。[7]

Facebook 與 Twitter 在 8 月底的網頁公告中表示已發現中國企圖挑撥離間的證據。Twitter 在公告中寫道：「這些帳號蓄意且明確企圖在香港製造政治矛盾，包括削弱示威運動合法性與政治立場。」因此宣布 936 個可疑帳號停權，也將禁止中國國營媒體發表具宣傳性質的推文（Twitter Safety, 2019）。另外，Facebook 從 Twitter 獲知相關訊息後，宣布移除 7 個專頁、3 個社團和 5 個帳號，並指這些專頁、社團與帳號「配合從事造假行為」，而移除理由是「我們不希望我們的服務被用來操弄人群」（Facebook, 2019）。

緊接著在 8 月 22 日，Google 以反間諜威脅分析小組（Threat Analysis Group）主任 Shane Huntley 的名義，在其網站上發出聲明指出其在打擊網路干預活動時，發現 210 個 YouTube 頻道上有關香港反送中抗爭的訊息，以一種「協調方式」的運作。Google 並指出這一發現與最近臉書和推特宣布與中國有關的觀察和行動一致：這些 YouTube 頻道使用 VPN（翻牆）和其他方法，來掩蓋這些帳號的來源，以及其他相關的協調式干預活動（Huntley, 2019）。

對此，中國外交部發言人則稱海外中國公民、留學生應當有權可以表達觀點和看法。然而，該等所謂言論之表達，仍似為中國 2009 年決定投入 450 億元人民幣鉅資在全球推廣「中國對外宣傳大布局（大外宣）計畫」之一環。

[7] 例如台灣之粉絲專頁「中肯小兔 動画映像收藏區」原管理員PO出對話紀錄證實粉絲專頁已經易主，新管理員還要求要他對外澄清「不是賣給中國人」，但今日粉絲專頁的封面竟真的換成習近平的照片，上面還寫著「必然統一」之字樣。而台灣政治人物或政治社團之網路聲量，亦經常發現簡體文字之特定支持與出沒。

伍、結論

科技之發展以及其所帶來之生活加值，本係對於國際人權上經濟社會文化面向保障之積極事項，而中國近來之科技以及應用科技所帶來之經濟上利益，確實在強化 ICESCR 關於享有科技進步的成果的權利上，有所進展。

但，在科技發展之同時，如果未能注意到其具有雙面刃之特質，而可能造成侵害人權之結果，則未免可惜。就本年度觀察與去年度相較，在應用新興發展之科技於生活與政府監控上，似乎有進一步更趨緊縮之問題。

今年度不僅科技監控之手段更趨多元且密集，從線上與線下電子監控，擴張至一切可能的生物特徵個資特徵剖析，包含面部辨識、步態辨識，乃至 DNA 等。本次觀察發現了中國用以上增加打擊面之方式，持續墊高投入監控審查之成本，但基本上仍不脫相近似之手段：實名制、加重落地服務之 ISP 業者責任、備案、嚴懲。此外，監視之物理空間從重要交通渠道據點擴張至包括公園與校園等一般公共空間，甚至已然進入私人親密之住居場域。除了較為直觀的個資侵害方式例如以監控攝影機方式蒐集公民行動等，在中國逐漸地以日常生活便利與享受科技發展成果之利益等個資當事人自願「同意」的方式，對個資上權利與資訊隱私權等加以侵害。

雖然如此，不過因為增加投入監控與信用評價成本持續墊高，但是手段卻具同質性，故應持續觀察其後續效率與效果問題。再者，面對可能的反彈，雖然中國政府提出了對「守法者」不擾民之政策，但一來「守法」之定義與標準浮動，二來監控與評價範圍包含政治與日常民生經濟與娛樂活動，三來是否能真正落實，尚有待觀察。又，在中國對於資訊不對稱與不實訊息之利用逐漸成熟之際，除對內利用諸如「學習強國」與「AI 謠言粉碎機」等應用程式進行洗腦與言論逆向追尋咎責外，中國並向外輸出或

是利用該等技術。

綜言之，對於全方面應用科技以施行完美控制之模式言，今年度更加成熟，甚至可供輸出，並仍持續強化中。特別之處在於不但使得人民無感，溫水中大多數青蛙還樂意自行進入鍋釜之中，乃至於強迫鍋外的青蛙一起跳入。雖然因為影響部分常民生活而有寥寥自救之聲，然多數情況下對於包括資訊權、隱私權、表意自由權，甚至健康權、財產權等，仍迭有侵害。

參考資料

人民網（2019a）。〈人民網發放首批互聯網內容風控師証書〉，人民網，2019年7月25日，http://media.people.com.cn/BIG5/n1/2019/0725/c40606-31254458.html。2019/11/29。

人民網（2019b）。〈安徽：全面推行部門聯合「雙隨機、一公開」監管〉，人民網，2019年6月25日，http://ah.people.com.cn/BIG5/n2/2019/0625/c358266-33074685.html。2019/11/29。

人民網（2019c）。〈李克強：讓制售假冒偽劣商品的違法者付出付不起的代價〉，人民網，2019年3月5日，http://lianghui.people.com.cn/2019npc/BIG5/n1/2019/0305/c425476-30958520.html。2019/11/29。

人民網（2019d）。〈短視頻內容審核標準發布 百條內容紅線勒緊風口〉，人民網，2019年1月10日，http://media.people.com.cn/n1/2019/0110/c40606-30513430.html。2019/11/29。

中央通訊社（2019）。〈六四30週年中國加強網路審查 人工智慧扮要角〉，中央通訊社，2019年5月26日，https://www.cna.com.tw/news/acn/201905260157.aspx。2019/11/29。

中國互聯網絡信息中心（2019）。〈第44次中國互聯網絡發展狀況統計報告〉，中國互聯網絡信息中心，2019年8月30日，https://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201908/t20190830_70800.htm。2019/11/29。

王兆陽（2019）。〈蘇州電視台高管使用Twitter瀏覽境外網站　遭警方傳喚並被撤職〉，香港01網，2019年4月11日，https://reurl.cc/9zQ04j。2019/11/29。

自由時報（2019a）。〈不「刷臉」無法回家！「新疆式」高壓監控蔓延全中國〉，自由時報，2019年9月1日，https://news.ltn.com.tw/news/world/breakingnews/2902627。2019/12/5。

自由時報（2019b）。〈中國鼠疫消息遭封鎖 蔡依橙：搞不清狀況易釀大規模流行〉，自由時報，2019年11月18日，https://news.ltn.com.tw/news/world/breakingnews/2981338。2019/11/29。

自由時報（2019c）。〈在中國步步驚心！「步態識別」系統緊盯這些人...〉，自由時報，2019年7月14日，https://news.ltn.com.tw/news/world/breakingnews/2842154。2019/11/29。

李台源（2019）。〈下一個華為？美智庫：「抖音」恐成安全隱憂〉，Newtalk，2019年1月14日，https://newtalk.tw/news/view/2019-01-14/194228。2019/11/29。

看中國（2019）。〈華為手機爆炸致使用者重傷 被公關刪帖〉，看中國，2019年4月10日，https://www.secretchina.com/news/b5/2019/04/10/890109.html。2019/11/29。

科技新報（2019c）。〈華為以 5,000 萬美元收購俄羅斯老牌 AI 安防廠商 Vokord〉，科技新報，2019年6月5日，https://technews.tw/2019/06/05/huawei-buy-ai-vokord/。2019/11/29。

袁莉（2019）。〈互聯網審查工廠：一個有中國特色的新生行業〉，紐約時報中文網，2019年1月2日，https://cn.nytimes.com/technology/20190102/china-internet-censor/zh-hant/。2019/11/29。

華爾街日報（2019）。〈AI監控走進中國小學課堂，頭戴腦波儀能提高孩子成績？〉，華爾街日報，2019年9月20日，https://www.wsj.com/video/china/1ED1BF37-1C78-4D7C-96D0-C8C1ED75D6F8.html。2019/11/1。

楊向文（2019）。〈華為警務通：超強識別功能、數據庫成迫害宗教助力〉，寒冬，2019年6月1日，https://zh.bitterwinter.org/huawei-smartphones-to-maintain-stability/。2019/11/29。

楊安琪（2019）。〈巧合不是第一次！Telegram 創辦人：DDoS 攻擊 IP 大多來自中國〉，科技新報，2019年6月13日，https://technews.

tw/2019/06/13/telegram-says-powerful-ddos-attack-was-mostly-from-china-again/。2019/11/29。

賴昀（2019）。〈「用智慧手機被監控，非智慧手機被通報」中國 AI 高科技監控下，新疆成露天監獄〉，沃草，2019年5月9日，https://musou.watchout.tw/read/JILHbFIbGRRKAcY9zrEf。2019/11/29。

蕭歆諺（2019）。〈「毒雞湯」讓她從天堂跌入地獄，1,000 萬粉絲瞬間蒸發〉，遠見雜誌，2019年3月5日，https://www.gvm.com.tw/article/56422。2019/11/29。

聯合新聞網（2019a）。〈中國「作戰App」：新疆官民全面監控的天網牢籠〉，聯合新聞網，2019年5月2日， https://global.udn.com/global_vision/story/8662/3788950。2019/11/29。

聯合新聞網（2019b）。〈不只華為！美國考慮列5家中國企業入黑名單〉，聯合新聞網，2019年5月22日，https://udn.com/news/story/12639/3828075 。2019/11/29。

蘋果日報（2019a）。〈【江蘇化工廠爆炸】政府佈置反無人機干擾器 曾派人色誘記者阻採訪〉，蘋果日報，2019年3月22日，https://hk.news.appledaily.com/china/realtime/article/20190322/59397840。2019/11/29。

蘋果日報（2019b）。〈新疆式監控　粵強採民眾口水建數據庫〉，蘋果日報，2019年8月9日，https://hk.appledaily.com/china/20190808/4CVBFTDVYODLRSOALEVTPOHT5E/。2019/11/29。

BBC中文網（2019）。〈微信「老賴地圖」：中國用新技術追債與隱私爭議〉，BBC中文網，2019年1月25日，https://www.bbc.com/zhongwen/trad/chinese-news-47004328 。2019/11/29。

LEE, STEVEN MYERS，孟寶勒（2019）。〈中共如何對香港抗議者展開資訊戰〉，紐約時報中文網，2019年8月14日，https://cn.nytimes.com/china/20190814/hong-kong-protests-china/zh-hant/。2019/11/29。

AFP (2019). “Chinese Shoppers Adopt Facial Payments in Cashless Drive.” Yahoo. 2019/9/4. https://news.yahoo.com/chinese-shoppers-adopt-facial-payments-cashless-drive-152444476.html. (accessed December 6, 2019).

Facebook (2019). “Removing Coordinated Inauthentic Behavior from China.” Facebook. 2019/8/19. https://newsroom.fb.com/news/2019/08/removing-cib-china/. (accessed August 21, 2019).

Huntley, Shane (2019). “Maintaining the Integrity of Our Platforms.” Google. 2019/8/22. https://blog.google/outreach-initiatives/public-policy/maintaining-integrity-our-platforms/. (accessed August 22, 2019).

Knockel, Jeffrey and Ruohan Xiong (2019). “An Analysis of WeChat’s Realtime Image Filtering in Chats.” the Citizen Lab. 2019/6/15. https://citizenlab.ca/2019/07/cant-picture-this-2-an-analysis-of-wechats-realtime-image-filtering-in-chats/. (accessed August 21, 2019).

McDonagh, Maeve (2013). “The Right to Information in International Human Rights Law.” Human Rights Law Review, Vol. 13, No. 1:25-55.

OHCHR. “The Right to Privacy in the Digital Age.” https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx.(accessed November 24, 2019).

Paul, Katie (2019). “TikTok Accused in California Lawsuit of Sending User Data to China Reuters.” REUTERS. 2019/12/3. https://www.reuters.com/article/us-usa-tiktok-lawsuit/tiktok-accused-in-california-lawsuit-of-sending-user-data-to-china-idUSKBN1Y708Q. (accessed December 6, 2019).

Thayer, Bradley A. and Luamchao Han (2019). “The Faustian Bargain of WeChat: China Shackles the World.” The Hill. 2019/7/31. https://thehill.com/opinion/technology/454747-the-faustian-bargain-of-wechat-china-shackles-the-world. (accessed August 21, 2019).

Twitter Safety (2019). “Information Operations Directed at Hong Kong.” Twitter. 2019/8/19. https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html. (accessed August 21, 2019).

UNESCO (2009). “The Right to Enjoy the Benefits of Scientific Progressand Its Applications.” Paper presented at The Right to Enjoy the Benefits of Scientific Progress and its Applications, Italy, July 16-17.

VPN Pro (2019). “The Few behind the Many: Hidden VPN Owners Unveiled.” VPN Pro. 2019/6/2. https://vpnpro.com/wp-content/uploads/Infographic-VPNpro-97-VPN-products-run-by-just-23-companies.pdf. (accessed November 29, 2019).

Wee, Sui-lee and Paul Mozur (2019). “China Uses DNA to Map Faces, With Help from the West.” The New York Time. 2019/12/3. https://www.nytimes.com/2019/12/03/business/china-dna-uighurs-xinjiang.html. (accessed December 6, 2019).