

大數據、治安與提升免疫力

吳斯茜¹、黃家珍²

摘要

各國積極推動數位政府並開發大數據的應用，治安是重要的應用領域，本文介紹目前國內警政機關大數據分析的發展現況，並以打擊詐騙犯罪為例，介紹國外運用大數據在犯罪偵查工作的協助；面對新興犯罪型態，另提出未來的情境模擬及犯罪預防的相關建議，期盼警民共同努力營造更安全與互相信任的社會。

壹、前言

「我們的數位宇宙正在不斷擴張。」

這是《大數據》作者麥爾荀伯格（Viktor Mayer-Schonberger）與庫基耶（Kenneth Cukier）的貼切形容，書中以奈米科技為例，技術重點是縮小，只要夠小就能做出過去做不到的事；大數據的重點則是放大，資料量夠巨大就能做出過去做不到的事（Mayer-Schönberger & Cukier, 2013/2013）。以現今生

¹ 中央警察大學行政管理學系副教授。

² 中央警察大學犯罪防治學系講師。

活每個人留下的數位足跡，大數據的商機驚人，資料將一再被拆解、販售，交給演算法模型無限次使用；且一旦數位化、放上網的資料就可能會被挖出來，無法永除後患，資料量註定有增無減，也因為這些源源不絕的豐沛資料，令各行各業紛紛投入大數據淘金潮。

然而，惡意使用大數據的狀況，最具破壞性的實例是「劍橋分析公司」（Cambridge Analytica）利用大數據作為 2016 年美國總統選戰武器，資料來源包括臉書（FaceBook）用戶的發文、每次按「讚」、消費紀錄……等，用來分析選民的政治偏好，再精準投放個人化訊息，尤其針對中間選民下手，進一步操弄選情。該公司也坦承在英國脫歐事件（Brexit）扮演關鍵角色，定義脫歐公投為情緒的戰爭，試圖對選民渲染恐懼的情緒，把政治慣用伎倆套用在網路社群的同溫層，最後恐懼心理奏效（Kaiser, 2019/2020），可見大數據的強大威力，在民主政治發展中，這真的是過去做不到的事。

政府內部蘊涵著非常大量資料，不必要外求，且相對於外部資料，多數是結構化較佳的資料，故可善用大數據分析提升政府治理能力（蕭乃沂、廖洲棚、陳敦源，2015）。例如新型冠狀病毒肺炎防疫期間推動的「口罩實名制」，就仰賴健保資料庫的大數據分析，進而動態調整全國特約藥局（2020 年 3 月 19 日公告計 6,278 家）的口罩配售，這是造福人群的例子。另從跨域治理的觀點，政府與民間應讓資料在特定協力合作機制上互補互惠，以取得資料驅動公共治理創新（data-driven innovation）的效益與價值（蕭乃沂、朱斌好，

2018)。

科技讓生活更便利且愈來愈不可或缺，亦衍生出新興犯罪型態，大數據分析是警方的重要利器，對內就警察機關而言，大數據分析改變勤務派遣方式，特別是預測犯罪熱點的巡邏勤務，在打擊詐騙犯罪已有成功經驗；對外在為民服務也陸續推出以智慧型手機為主的應用程式。本文介紹目前的進展，供其他機關擴大公共服務之參考；而後進一步就人工智慧的趨勢發展，挑選幾個專家設定的情境模擬，供大家想像未來生活可能的影響，強化犯罪預防的意識。

貳、大數據分析協助打造更安全的社會

治安狀況對於社會福祉的影響不言可喻，大數據分析如何幫上忙？

你晚上正要出門提款，想到了一台你常去的 ATM，那一區你認為滿安全的，你查手機看看如果走路而不開車，被搶的可能性有多少。這個分數比幾天前升高了，你看見了你的未來，令人發抖。你的社區不再像你以為的那麼安全，所以你改為白天去提款，並且參加下一場社區會議。

資料來源：Tucker (2014：304)。

這是引用《未來學人》科技雜誌副總編輯派區克·塔克（Patrick Tucker）所提出的情境模擬，從中可發現民眾如何使用大數據分析結果，降低個人受害機率，目前國內的犯罪統計資料還沒有研發這類 APP，但警方已運用大數據分析強力打擊詐騙犯罪。犯罪集團的主要手法是在國外設置詐騙機房，在國內招募員工擔任話務機手並訓練詐騙話術，再透過網路電話向被害人詐騙，得逞後約定面交金錢或匯款，隨即由國內的車手提領贓款，警方於是針對末端的提領行為，推出「斬手行動」；運用大數據分析詐騙帳戶、ATM 提款熱點、提領時間、車手影像……等，再部署警力逮捕車手，屏東縣的成效尤其卓著，統計遭車手提領次數從 2018 年 7 月的 731 次，至 2019 年 7 月降到只有 3 次（翁禎霞，2019 年 10 月 17 日）。然而，令人遺憾的是犯罪集團會吸收懵懂的青少年，例如以出國打工名義招募機手，或以高報酬、低風險誘惑擔任車手，他們可能只是為滿足物質欲望而誤入歧途，使詐騙行為難以根除。

內政部警政署推出的「警政服務 APP」，重點不是犯罪偵查而是犯罪預防，策略上是「智慧警政、行動警察」，自 2012 年 8 月啟用後，陸續改版與擴增功能，並榮獲 2017 年「政府服務品質獎」，統計至 2018 年底累計下載量突破 203 萬次；以打擊詐騙犯罪為例，功能包含反詐騙宣導、查詢詐騙來電排名、高風險賣場等資訊，並可即時向警方檢舉或報案（內政部警政署，2019）。此類工具背後運作思維有兩種方向：一是警察走向民眾；二是民眾走

向警察，檢視目前「警政服務 APP」項目，多屬於民眾報案、資料查詢為主，效益上是縮短民眾走向警察的距離（實體空間）與時間；未來服務要更升級，系統開發思維建議設計警察主動走向民眾的機制，其中關鍵條件是「適地性服務」（location-based services）。

廣告行銷界很善用「適地性」，運作方式是智慧型手機再搭配 GPS 定位資訊後，馬上進化為「行動促銷」（mobile promotions），等於是瞄準對的人，在對的時間、對的地點作行銷出擊。為什麼它會知道誰是對的人呢？別忘了數位足跡是非常有價值的，甚至有些人一天裡待在虛擬世界的時間比真實世界還要長，所以公司可以買進各種資料，進一步掌握消費習慣（還能再轉賣），這種作法不再只是網路瀏覽時附帶出現的廣告，而是以消費者進入特定區域或特定行為作觸發點，立即透過手機呈現為消費者量身訂作的促銷方案（Andrews, Goehring, Hui, Pancras, & Thornswood, 2016）。

不久的將來，你逛街時可能覺得自己很幸運，因為手機常會傳來「限時優惠」，而且剛好都是你喜歡吃的食物或預計要買的商品。也有未來學家模擬當計程車由自駕車營運的情境，因為系統已經掌握乘客個資，搭車的體驗就有很大的差別，高社經地位乘客派去的車種比較高級，會貼心的設定舒適溫度和偏好音樂，更可能整趟車程都被廣告包圍。這個情境可以讓人理解到大數據進入日常，以及隨之成形的「數位種姓制度」（Webb, 2019/2020）。

我偶爾會收到警察機關發送的關心簡訊，提醒我小心詐騙，問題是它出現的時間似乎很隨機，並沒有在通話、網路購物使用 ATM 提款時出現，這些訊息就浪費掉了。希望官方發送訊息時能夠考量到適地性服務原則，讓這些提醒來得正是時候，或者針對特定對象，就如同業者藉大數據分析更精準地投放廣告一樣。例如英國有項研究針對汽車竊盜案件，運用「輕推理論」(Nudge Theory) 製發犯罪預防宣導單，建議車輛停放在高犯罪率地區的車主，建議提高警覺，尤其要停隔夜的車輛，研究結果證實可降低汽車竊盜率 (Roach, Weir, Phillips, Gaskell & Walton, 2017)。對民眾而言，「事前」、「即時」的提醒才更能感受到「警察關心您」。

參、萬一過了頭？

前述的情境模擬，國外推出一個 App，讓使用者在地圖上標示暴力事件、毒品交易、鬧事者聚集……等好發地點，目的希望幫助孩童安全返家，可以想見家長們的愛用。國內運用官方犯罪統計資料的成果，例如 2015 年臺北市推出的「市民安心地圖」，目前可查詢住宅、汽車、機車、自行車竊盜、強盜及搶奪案等 6 種案類犯罪資料庫。如果未來希望建立預測模型，更深層的思考是如何計算「安全」？又由誰來定義？

倫敦大學學院（University College London）城市數學教授漢娜·弗萊（Hannah Fry）在《打開演算法黑箱》（Hello World: How to be Human in the Age of the Machine）書中發出急切的警告，面對演算法蔓延到現代生活的每個層面之際，「究竟我們讓出多少權力，以及是否已經讓事態演變到過了頭。」（Fry, 2018/2019）會過了頭的原因之一是「可解釋性」（explainability）問題，假設大數據的演算法納入上百項跟地區治安狀況有關的指標，分開來個別的比重雖然低，但整合起來就能建立預測模型，最後會產生分析結果，但它可能複雜到難以理解答案究竟是如何得出。換言之，未來如果警方運用大數據分析結果，如何確保執法的「程序正義」？

警方對大數據最具前瞻性且寄予厚望的是超前部署，提供犯罪預測功能，如果能夠事前預防犯罪的發生而非事後，就可以避免更多人受害；然而，系統是以過去的犯罪統計資料為基礎進行預測，過去發生的就表示未來一定會如此嗎？例如有發生過謀殺案，22 歲兇手殺害 20 歲的前女友，他曾在三週前上網搜尋如何殺人的資訊，那麼警方要不要從關鍵字搜尋來防範呢？通常人們對 Google 很誠實（對臉書卻不是），根據 Google 統計 2014 年「如何殺死你的女友」的關鍵字搜尋約有 6 千筆，當年實際發生女友謀殺案約 4 百件，比例是 15 分之 1，且不能排除沒有先上網查資料，一時氣憤痛下毒手的情況，所以要用大數據預測某人可能的犯罪行為，並沒有電影演的那麼神奇（Stephens-Davidowitz, 2017/2017）。此外，如果資料本身帶有偏見呢？美國

已發生有色族群被列入犯罪人的機率更高，演算法可能設定某些區域警察要密集巡邏，導致過多盤查、過度執法。

此外，目前犯罪偵查非常倚重監視器影像，搭配的人臉辨識技術亦不斷提升，美國華盛頓大學舉辦人臉辨識全球挑戰賽，2015 年 Google 公司以 FaceNet 演算法奪冠，辨識正確率約 75%；至 2018 年已有多家科技公司的技術辨識率高達 99% (MagaFace, 2018)。雖辨識的正確率已接近百分之百，亦代表著如果系統版本較舊，以及天候、光線、角度等因素影響，人臉辨識結果並不可靠，仍需輔以人工比對；除非再加入其他辨識技術，例如步態、聲紋……等綜合判斷，否則就會發生指認錯誤的問題。

讓情況更惡化的是「深度偽裝」(Deepfake) 技術，這個人工智慧有高超的「換臉」技術，已有許多名人受害，一旦假影像散播出去，要洗刷自己的清白就非常困難了。假設你接到外國總公司高層要求，緊急匯款給供應商，應該會馬上辦理；但這不是情境模擬，而是已發生的詐騙手法，有員工接到一通執行長的來電，要求處理 22 萬歐元的轉帳，因為聲音聽起來很像執行長的德國口音，因為不疑有他結果受騙。這種詐騙集團的技術水準很高，詐騙話術是量身訂作，旗下員工不一定是人，可能是「聊天機器人」，它們不眠不休、不吃不喝專心工作，還會自我精進（很遺憾這也已經發生了），未來如果詐騙集團再升級，使用深度偽裝技術，尤其正在推廣遠距辦公，那問題就嚴重多了（吳斯茜，2018）。資訊安全權威、國際刑警組織（Interpol）資深顧問

馬克·古德曼（Marc Goodman）就警告：「現在的威脅是不對稱的，攻擊者只需要找到一個弱點，就能揮軍向前，防禦者得守住所有據點，但事實上不可能全部守住。」可以預見未來警方所要面臨的嚴峻挑戰（Goodman, 2015/2016）。

然而，詐騙犯罪付出最大代價的是人際之間的信任被破壞了，人類能夠擴大信任網絡可是經過漫長歲月，高信任的社會具備經濟發展優勢，讓人安居樂業，故信任度也可以作為治安狀況的觀察指標。根據「2019 臺灣社會信任」調查結果，從 2001 年至 2019 年社會上 14 項角色中，有 10 項角色的信任度評分上升，代表整體社會的信任程度提高；其中，以民眾對警察的信任度上升最多，2001 年調查結果為 46.4%，2019 年增加至 76.5%（遠見研究調查，2019），這要歸功於警民共同的努力，成果得來不易，信任一旦被破壞很難修復。

基因資料是另一個高潛力的大數據資料，美國聯邦調查局（FBI）近期利用 GEDmatch.com 網站的基因資料庫，於 2018 年 4 月偵破被稱為「金州殺手」（Golden State Killer）的懸案，1970 至 1980 年代這位殺手犯下 12 件謀殺、50 多件性侵和上百件盜竊案，遲未破案造成人心惶惶。該網站蒐集約 1,700 萬份個人自願提供的 DNA 資料，而警方把在犯罪現場採到的 DNA 資料上傳作比對，才得以持續縮減嫌犯對象，不斷過濾到最後，終於鎖定一名嫌犯，將他逮捕後進行 DNA 鑑定，結果吻合、鐵證如山。雖然警方已有建置犯罪人

DNA 資料庫，卻要拜大數據之賜才能在 40 年後破案。

然而，同時這個案件亦引發倫理的疑慮，因為該網站採用的基因族譜技術主要目的是供大家尋親，所蒐集的 DNA 個資並非作為偵查犯罪之用；即使是想協助打擊犯罪的好公民，同意分享個人 DNA，一旦分享就等於揭露整個家族和後代的基因遺傳資料 (Nature, 2018)。有個求職的模擬情境，想像有一天你的孫子去公司面試，該公司面試人員可能已經清楚關於他的一切，因為手上有求職者的基因資料 (Minkel, 2019)。還有情境模擬醫院的資料庫被駭客入侵，如果將特定資料傳送給雇主，例如憂鬱症、酒癮、暴力基因的高危險群，員工是否因此被解雇？可以想見未來基因隱私也會成為關注議題。

NATIONAL ACADEMY OF CIVIL SERVICE

肆、建議：提升免疫力

新科技的飛快進展總讓人對未來智慧化的生活充滿美好的想像，我們期望政府治理持續有新意，擴大公共服務，但新科技本身尚在試誤期，愈來愈多隱憂值得注意，尤其人工智慧領域使用機器學習技術，會不斷優化，它是怎麼學成出師的，也很重要。史登商學院策略遠見教授艾美·韋伯 (Amy Webb) 在《AI 未來賽局》書中建議系統要具備可解釋性，仿照食品營養標籤的概念，系統要說明所使用的學習資料、學習過程，實際應用的資料及預期結果，而且要有公證機構可以驗證系統的透明度 (Webb, 2019/2020)。萬一系統出錯，

總要有人知道它錯在哪裡。

另一個構想是幫系統增加免疫力，在 AI 的學習階段，先把會影響表現的攻擊樣本當成疫苗，讓 AI 學習去辨識這些危險資料，以免實際運作後資料庫遭到污染或惡意欺騙演算法；所以請研發人員在 AI 學生的課表上，把犯罪心理學、被害者學、犯罪預防……等列入必修課程。不過，更優先要務是培養人們的資安意識與警覺心，提升免疫力的作法包括：對可疑訊息保持戒心、定時更新軟體、強化密碼管理……等（毛敬豪，2020）。如果不小心成為犯罪的被害人，可能因為有損個人聲譽而未向警方報案，但自動化科技的犯罪要追查犯罪模式，有賴於被害人勇於揭露不法，才能更快偵破、阻止更多人受害。

NATIONAL ACADEMY OF CIVIL SERVICE

研發人員自己也有必修課程，是倫理道德課。2017 年 1 月有近千名的人工智慧專家聯合簽署「阿西洛馬人工智慧原則」(Asilomar AI Principles)，其中，第 9 條職責原則 (Responsibility) 內容：「高階人工智慧系統的設計者和建造者，在道德影響上係人工智慧使用、誤用和行動的利害關係人，有責任和機會去形塑後續的影響。」第 10 條價值觀一致原則 (Value Alignment) 內容：「設計高自主性人工智慧系統時，應確保在整體運作下之目標和行為與人類價值觀一致。」專家們大聲疾呼在系統設計階段就要注意倫理道德議題 (Future of Life Institute, 2017)。2017 年美國麻省理工學院畢業典禮邀請蘋果公司執行長提姆·庫克 (Tim Cook) 演講，他说不擔心人工智慧會讓電腦像

人類的思考，擔心的是人類像電腦那樣思考，摒棄同理心和價值觀，並且不計後果。

推動大數據、人工智慧就需不斷蒐集大量資料，隱私權議題也日益急迫，如果要追求更安全的社會，系統監控的紅線在哪裡？科技的突飛猛進提供數據科學家大顯身手的舞台，但需要向他們課責，避免瘋狂科學家釀成難以收拾的災難。願他們是利他主義者，承諾研發的系統來自良善意圖，能發揮正向作用，並且要回答得出艾美·韋伯的提問：「如何教 AI 人類的同理心？如何平衡 AI 的商業化與人類的的基本願望（隱私、安全、歸屬感、自尊）？」

伍、結語

「擁有大數據並不會自動產生精闢見解。」

這是數據科學家賽斯·史蒂芬斯—大衛德維茲 (Seth Stephens-Davidowitz) 在《數據、謊言與真相》書中的忠告，雖然我們認為大數據的潛力無窮，但關鍵是要問正確的問題，以及參考有豐富經驗者的決策，相輔相成才會發揮更好的作用。對維護社會治安而言，大數據可以協助釐清案情，加快抽絲剝繭的進度；但就案件偵辦方向、蒐集哪些證據、突破嫌犯心房……等工作，需要靠警察的經驗、智慧判斷與隨機應變。然而，改善治安真正需要的，並不是更強大的科技或更高明的警察，而是更善良的人心。

參考文獻

一、中文部分

Minkel, E. (2019 年 1 月 11 日)。基因檢測會暴露我們的隱私嗎？【國家地理中文網】。取自 [https://www.natgeomedia.com/science/article/content-](https://www.natgeomedia.com/science/article/content-8373.html)

8373.html

內政部警政署 (2019)。警政服務 APP，警察服務一指通！取自 <https://www.npa.gov.tw/NPAGip/wSite/ct?xItem=92472&ctNode=12958&mp=1>

毛敬豪 (2020)。新科技、新時代：人工智慧如何改變我們的世界。T&D 飛訊，264，1-13。

王怡文 (譯) (2014)。遙測個人時代：如何運用大數據算出未來，全面改變你的人生 (原作者：Tucker, P.)。臺北市：遠流。(原著出版於 2014 年)

林志懋 (譯) (2019)。打開演算法黑箱：反噬的 AI、走鐘的運算，當演算法出了錯，人類還能控制它嗎？(原作者：Fry, H.)。臺北市：臉譜。(原著出版於 2018 年)

林俊宏 (譯) (2013)。大數據 (原作者：Mayer-Schönberger, V., & Cukier, K.)。臺北市：天下遠見。(原著出版於 2013 年)

林俊宏 (譯) (2016)。未來的犯罪：當萬物都可駭，我們該如何面對 (原作

者：Goodman, M.)。新北：木馬文化出版。(原著出版於 2015 年)。

翁禎霞 (2019 年 10 月 17 日)。大數據抓車手 屏詐騙提領 731 變 3 次【聯合報】。取自 <https://udn.com/news/story/7320/4108721>

陳琇玲 (譯) (2017)。數據、謊言與真相：Google 資料分析師用大數據揭露人們的真面目 (原作者：Stephens-Davidowitz, D.)。臺北市：商周。(原著出版於 2017 年)

黃庭敏 (譯) (2020)。AI 未來賽局：中美競合框架下，科技 9 巨頭建構的未來 (原作者：Webb, A.)。新北市：八旗文化。(原著出版於 2019 年)

楊理然、盧靜 (譯) (2020)。操弄【劍橋分析事件大揭祕】：幫川普當選、讓英國脫歐，看大數據、Facebook 如何洩露你的個資來操弄你的選擇？(原作者：Kaiser, B.)。臺北市：野人。(原著出版於 2019 年)

遠見研究調查 (2019)。「2019 臺灣社會信任」調查結果出爐。取自 <https://gvsr.cwgv.com.tw/articles/index/14810/1>

蕭乃沂、朱斌好 (2018)。資料驅動創新的跨域公共治理。國土及公共治理季刊，6 (4)，74-85。

蕭乃沂、廖洲棚、陳敦源 (2015)。政府應用巨量資料精進公共服務與政策分析之可行性研究。國家發展委員會委託臺灣電子治理研究中心研究報告。

二、英文部分

Andrews, M., Goehring, J., Hui, S., Pancras, J., & Thornswood, L. (2016). Mobile promotions: A framework and research priorities. *Journal of Interactive Marketing*, 34, 15-24.

Future of Life Institute (2017). *Asilomar AI Principles*. Retrieve from <https://futureoflife.org/ai-principles-chinese/>

MagaFace (2018). *FaceScrub Result*. Retrieve from <https://megaface.cs.washington.edu/results/facescrub.html>

Nature (2018). *The ethics of catching criminals using their family's DNA*. Retrieve from <https://www.nature.com/articles/d41586-018-05029-9>

Roach, J., Weir, K., Phillips, P., Gaskell, K., & Walton, M. (2017). Nudging down theft from insecure vehicles: A pilot study. *International Journal of Police Science & Management*, 19(1), 31-38.

國家文官學院