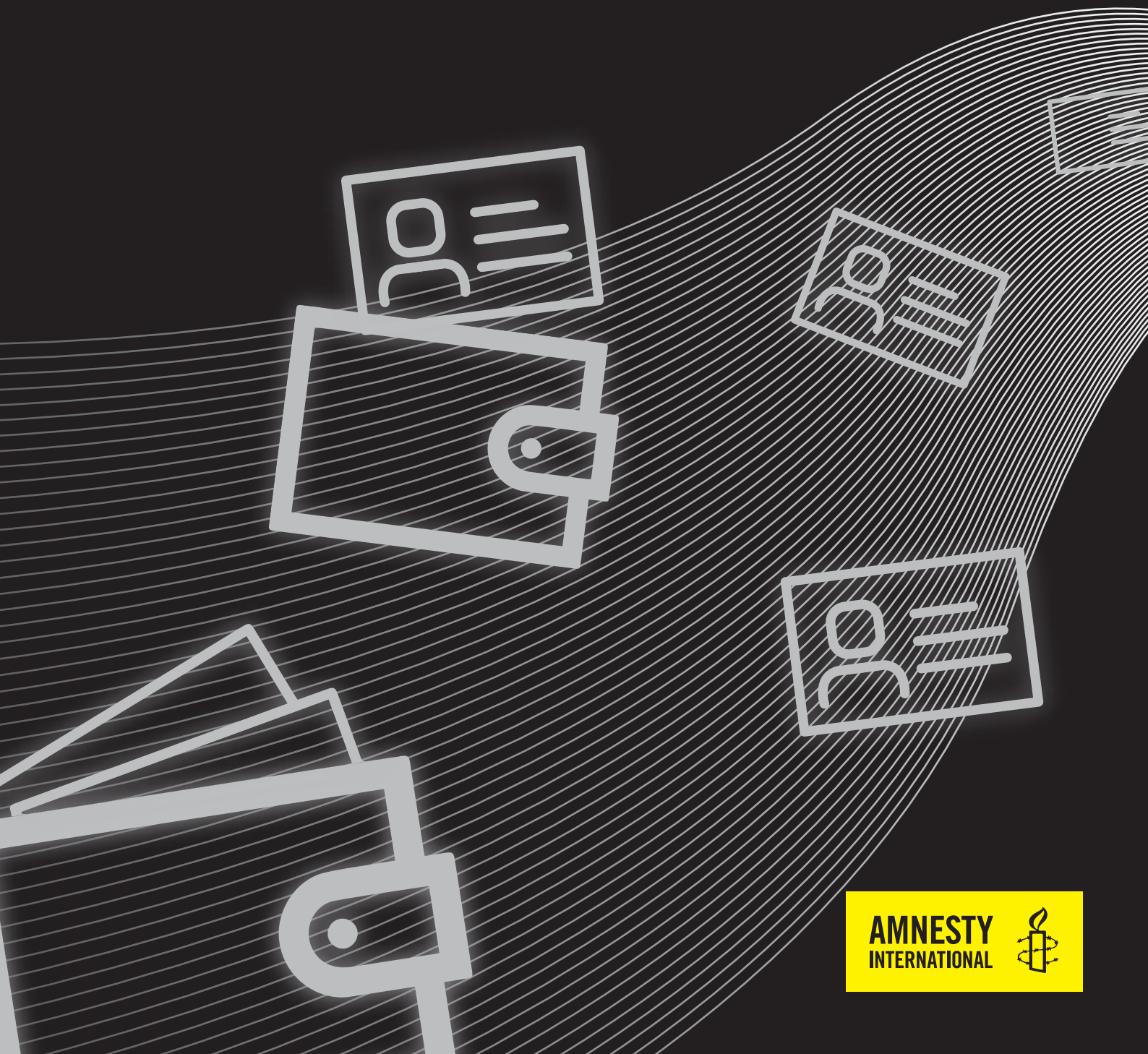
國際特赦組織台灣分會

台灣數位身分證之人權風險

2021



AMNESTY INTERNATIONAL

國際特赦組織是一個在全球有一千多萬人參與的運動，致力於締造一個人人均享有人權的世界。我們的理想是使每個人都享有《世界人權宣言》和其他國際人權標準中列載的所有權利。我們獨立於任何政府、政治意識形態、經濟利益或宗教，資金主要來自成員會費和大眾捐款。

目錄

1. 引文

資料驅動（data-driven）科技對隱私權帶來的挑戰是人權議題中最迫切的新興領域。雖然是私部門促成了許多大數據及人工智慧相關的技術突破，如今政府部門也亦步亦趨，設法借助這些創新科技的力量。資料驅動科技若被使用正確有可能為社會帶來許多益處，但卻也對人權構成不可忽略的風險。

其中科技如何幫助政府提供更好的公共服務特別受到關注。所謂「智慧政府」計畫承諾以更有效率、更平易近人的方式提供服務，也許看似無害，但大量資料蒐集和集中化卻也可能讓政府或商業實體有機會透過分析數位足跡（digital footprints）追蹤及進行其他目的外利用。

台灣政府正試圖善加利用數位友善的環境建立其「智慧政府」系統。[1]2020 年 10 月 5 日，台灣內政部公布，政府將於 2021 年 7 月啟用全新的「數位身分識別（electronic identification, eID）」系統。[2]新的數位身分證將結合身分識別與驗證功能和個人資訊存取，承諾提供使用者一系列能透過單一線上平台操作及管理的服務。

這則消息在台灣社會引起廣泛關注，對如此包羅萬象的系統將如何衝擊 / 影響隱私權及經濟與社會權產生疑慮。作為回應，政府暫緩數位身分證上路，並承諾繼續推行該政策前，會針對是否有制定額外法規之必要進行更多意見蒐集。[3]

---

[1] '數位身分識別證打開智慧政府的關鍵鑰匙' (E-identification is the Key to Fulfill Smart Government), Ministry of the Interior, 22 August 2019, bit.ly/2GF73xF, p. 9.

[2] '立法院第 10 屆第 2 會期內政委員會-內政部業務報告' (The Ministry of the Interior submitted to the Legislator Yuan in the 10th term, second session), Ministry of the Interior, 5 October 2020, reurl.cc/VXQxG6, p4.

[3] '暫緩數位身分證發行計畫 蘇揆:完善法制後再推動', 行政院, 21 January 2021, https://www.ey.gov.tw/Page/9277F759E41CCD91/e80e55a2-0102-4031-b6d3-a7c40f4cac6a.

這份報告將試圖聚焦於台灣數位身分證計畫中可能涉及人權問題提供資訊。透過分析政府官方文件、學術研究及相關政府報告，國際特赦組織認為台灣現存法律及體制不足以防範數位身分識別系統可能對人權造成的風險。我們能在台灣現存的傳統非數位國家身分識別系統中指出許多可能因新的數位身分識別系統上路而產生或加劇的潛在風險，若該系統在相關法規制度沒有實質改變的前提下推行更是如此。

為保護個人隱私權及其他相關權利，台灣新的數位身分識別系統應於詳盡的法規、獨立管理、公開透明等前提下啟用，因為集中化管理任何個人資料皆有導致資料濫用的風險。政府能透過特定方式分析集中管理的個人資料，進行大規模監控等危及人權行為。因此，台灣應在數位身分相關的所有面向中，制訂完善的法規，以避免個人資料遭公私部門濫用，包括明確限制資料的範圍、使用方式、使用途徑及存取，以及建立有效的資料保障機制。政府也應有效監督公私部門如何遵守隱私權相關法律、是否得調查違反隱私權潛在案例。最後，數位身分識別系統的過程可能邊緣化特定族群，造成其使用公共服務的障礙。此潛在風險將危及人權，尤其是經濟、社會權及資訊自主[4]，故政府應保留非晶片身分證作為身分識別的選項之一。

2. 台灣的國民身分證系統

2.1 台灣現存身分識別系統

台灣數位身分識別系統將建立於現存國家身分識別系統之上，而國家身分識別系統之悠久歷史甚至可回溯至日治時期（1895–1949）。在現今台灣，人自出生一刻起，便獲得一組特定且固定的身分證字

[4] 資料自主意旨人應擁有控管個人資料的權利，聯合國人權理事會（United Nations Human Rights Council, UNHRC）亦指出自主的概念難以與隱私分離。（Report of the Special Rapporteur on the right to privacy, Human Rights Council, Un doc. A/HRC/31/64, 24 November 2016, para. 25.）

號，將一生跟隨其人，並連結其個人資訊。身分證字號已深植台灣人日常生活的許多面向正是眾人擔憂隨數位身分證啟用，個人資料將進一步數位化的主因之一。

台灣現存身分證可追溯至戶政系統，故身分證上早已較其他管理系統證件印有更多個人資訊：姓名、出生年月日、性別、身分證字號、家長姓名、配偶姓名、住址。正面更附上包含頭至肩膀之標準正面半身照，背面則有身分證字號條碼供光學條碼掃描器識別。

圖 1 台灣身分證背面

近乎所有公私部門機關目前皆使用身分證字號進行身分識別。舉例而言，申請或使用醫療照護或健康保險、繳稅、車輛登記或是進行某些商務交易皆須出示身分證。COVID-19 疫情期間，個人進入各政府機關時經常被要求掃描國民身分證。

現存身分證是為親自到場進行身分識別及驗證而設計，一般來說不足以於線上使用，因為身分證無法透過網路驗證或證實身分虛實，而多數政府機構在過去也不提供線上服務。

政府了解這些限制後，於 2013 年啟用「自然人憑證」。數位憑證存於和身分證完全不同的晶片卡，包含個人基本資訊，如姓名和身分證字號，並以雜湊運算演算法及非對稱式加密加以保護。個人可以使用數位憑證於線上驗證身分、簽署電子文件及遠距使用政府服務。和強制性的國民身分證不同，數位憑證可選擇性辦理。

2.2 政府推行數位身分證的目的

政府為推行數位身分識別系統提出了四大理由：首先，為實施「智慧政府」的服務項目，政府欲普及數位身分識別的使用。其次，數位化將幫助政府透過網路提供更多線上服務，藉此促進「智慧政府」

發展。[5]再者，數位身分證可簡化防偽機制，避免偽造文書並降低卡內儲存之個人資料遭更動的風險。[6]最後，政府欲透過推行數位身分識別系統進一步推廣在台灣經濟已佔有一席之地的高科技產業所研發的創新科技。[7]

除了數位身分辨識系統，台灣「智慧政府」服務計畫中另一主要項目為政府資料傳輸平臺 T-Road。該平台的設計奠基於現存的政府網際服務網（Government Service Network），並取經愛沙尼亞的 X-Road 和新加坡的 CODEX[8]，欲連結不同政府資料庫，並將其中資料標準化，讓使用者能透過登入單一平台，使用多項政府服務。

過去，內政部及為計畫國家發展策略及資源分配而負責協調不同政府單位的國家發展委員會（National Development Council, NDC）[9]一再聲稱新式數位身分證其數位辨識功能是構成 T-Road 平台不可或缺的一步。[10]然而，國家發展委員會卻也曾承認現存分開的數位憑

[5] 「智慧政府」是由國發會提出，目的在於透過數位化身分識別與跨部門資訊共享機制提升政府服務品質。見 National Development Council "Smart Government Action Plan (since 2019 to 2020)", https://www.ndc.gov.tw/en/Content_List.aspx?n=C8A462AE07F6F3C5.

[6] '數位身分識別證(New eID)簡易問答集' (Q&A for the New eID), Ministry of the Interior, September 2019, www.ris.gov.tw/documents/data/5/6/ca2b5d37-d0e0-4b18-83be-fae54ea6ee34.pdf, p. 2.

[7] '數位身分識別證（New eID）-新一代國民身分證換發計畫' (The plan for issuing the New eID), Ministry of the Interior, August 2020, https://www.ris.gov.tw/documents/data/5/6/79ba9c21-5c4c-4ab7-a2da-3aa5c0a3d7d0.pdf, p. 4.

[8] '智慧政府推動策略計畫' (The Smart Gov strategy action plan), National Development Council, 10 January 2019, tinyurl.com/y7op9sh6, pp. 2-6.

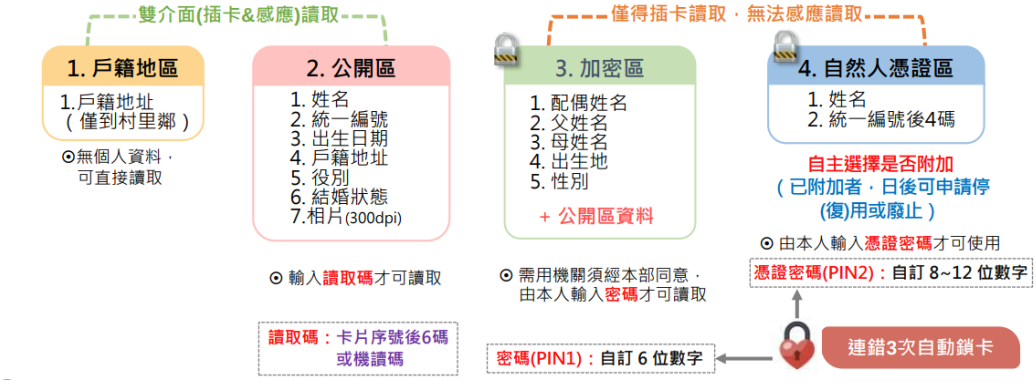
[9] 根據〈國家發展委員會組織法〉，國家發展委員會職責圍在不同政府單位間協調，以計劃國家發展策略與分配資源。〈國家發展委員會組織法〉第 1 條。

[10] 邁入數位身分新紀元 ── 數位身分識別證 (Toward the New Digital Identity Era: The New eID), Ministry of the Interior, March 2019, https://bit.ly/2IODeLv, pp 58-59.

證系統足以供民眾使用 T-Road。[11]而這項聲明也引來眾人對結合國民身分證與數位憑證系統之必要性的質疑。

2.3 新身分證運作方式與使用時機

新身分證將於卡上晶片結合目前存於身分證及數位憑證的資訊。印於現存身分證上的個人資訊將改以晶片存取，並同時整合數位憑證的功能。



表一 計畫存於新身分證的個人資訊

根據最新設計，數位身分證上儲存的資訊將分為四區，分別存放以下資料：戶政資訊、開放個人資料、受密碼保護的個人資料及數位憑證。不同程度的使用限制會決定各類資料將如何被使用。(請見表一) 親自到場進行身分識別依賴存於開放個人資料與受密碼保護的個人資料。線上服務則需要透過數位憑證驗證身分。[12]

---

11 國家發展委員會最新釋出的新聞稿指出，新的數位身分識別系統已不再是線上公共服務身分認證時的必要手段。國家發展委員會，'智慧政府 2.0 啟動資料治理新三箭' (Smart Government 2.0 The three key of launching the data governance), 28 January 2021.

12 '國民身分證及戶口名簿格式內容製發相片影像檔建置管理辦法' (Measures for the Administration of the Establishment and Distribution of Photo and Image Files in the Formats and Contents of National ID Cards and Household Registers), 25 December 2020, https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=D0030030.

政府單位將得以使用新身分證上儲存之戶政資訊及開放個人資料，但要使用受密碼保護的個人資料及數位憑證，各機關必須向內政部提出授權申請。[13]然而，其中隱憂之一為目前現存法律尚無以管制內政部得如何授權存於數位身分證上的加密資料及數位憑證的使用。

考慮到台灣現存身分證於身分識別方面用途之廣，專家擔憂進一步數位化會導致數位身分證使用更為頻繁，尤其是用於私部門電子商務或會員註冊。這些使用方式將留下能提供分析的數位記錄，而進一步剖析能獲得大量的個人資訊將超乎個人想像。某些線上串流平台早已會蒐集個人資訊如每日行程及瀏覽偏好，數位身分識別則可能透過提供私部門高可用性的個人資訊加劇資訊被蒐集的情況。[14]除非數位身分證上資料的範圍與應用被嚴加控管與限制，不然這類「功能蠕變」(function creep）是可預見且必須被處理的。[15]

2.4 現存法律架構

目前台灣並無特定法律可管制新式數位身分證。政府曾反覆聲明數位身分證無須特定法律管制，現存戶籍法、個人資料保護法、資通安全管理法及電子簽章法便足以因應，以及提供全面推行數位身分辨識系統的法律基礎，並保護個人隱私。

公民團體和學界皆對這樣的立場產生質疑，表示現存法律框架內有過多尚待詮釋與決議的空間，會對個人隱私造成風險。

目前台灣現存法規仍無法在數位身分識別系統下提供個人隱私足夠的保護。例如，個人資料保護法為目前台灣和隱私權相關最重要的法規之一，但該法及其他相關法規卻都沒有明確的管理規範，包含

---

[13] '數位身分識別證（New eID） -新一代國民身分證換發計畫' (The plan for issuing the New eID), Ministry of the Interior, August 2020, www.ris.gov.tw/documents/data/5/6/79ba9c21-5c4c-4ab7-a2da-3aa5c0a3d7d0.pdf, p. 22.

[14] 中研院法律學研究所資訊法中心, '數位時代下的國民身分證與身分識別政策建議書' (The recommendation on the e-identification in the digital era), 2 November 2020, p23.

[15] 中研院法律學研究所資訊法中心, '數位時代下的國民身分證與身分識別政策建議書' (The recommendation on the e-identification in the digital era), 2 November 2020, p. 5, p.175, p. 217, p. 219.

任何限制蒐集、存取、處理及使用數位足跡的法條。[16]缺乏管理及規範數位足跡的法規將令有心人士有機可趁，濫用此項個人資訊。

政府服務數位化及新興科技快速發展將導致保護隱私變得更為艱難。然而，台灣並無專門的政府單位負責保護隱私與個人資料。目前為止，隱私相關問題仍交由不同單位，如國家發展委員會等。[17]在這種狀況下，台灣政府將難以處理不成熟的數位身分識別系統可能引發的人權問題。

很重要的是，台灣現存法律並未提供任何「逆向監視」的機能，或授權個人追蹤誰有權使用自己的個人資料，以避免資料被政府或企業作為監控或監視的手段任意使用。與之相對，擁有完善的數位身分識別系統及「智慧政府」系統的愛沙尼亞，其相關法律明確要求政府應保障本人得追蹤個人資料的使用情況，使數位資訊公開透明。

在缺乏法律監督的前提下，獨立運作或逆向監視的機能是台灣數位身分證政策中最關鍵的爭論點。經過一連串針對數位身分識別系統的抗議，政府現在已暫緩政策執行，並宣告會考慮制定特殊法律予以規範。

3. 身分制度下的人權風險

3.1 既存的身份制度可能引發的人權風險

台灣現存身分識別系統的許多特徵也有危害個人隱私的風險。首先，強制的身分制度，本質上就是對隱私權的一種侵擾，同時也妨礙其

[16] 中研院法律學研究所資訊法中心，‘數位時代下的國民身分證與身分識別政策建議書’ (The recommendation on the e-identification in the digital era), 2 November 2020, p. 35.

[17] 中研院法律學研究所資訊法中心，‘數位時代下的國民身分證與身分識別政策建議書’ (The recommendation on the e-identification in the digital era), 2 November 2020, p. 35.

自主性與選擇自由。[18]身分證字號的特殊性使政府與商業實體得相對輕鬆地透過不同資料庫鎖定個人，導致個人難以維持匿名。

數位身分識別系統將進一步提升國家系統性監控與追蹤個人的能力，對隱私權造成不符比例原則的干涉。

集中管理身分資訊亦有資料遭未授權使用的隱憂。透過單一身分證字號便可連結至不同類型的資訊會使被授權使用大量資訊的人員有機會得針對單一個人匯集資料，掌握其一生的輪廓，故限制可使用的資訊必須是為達成某一特定、合法目的所必要的相當重要。

2020 年初 COVID-19 疫情爆發後，政府建議民眾於便利商店使用健保卡領取口罩，卻因便利商店可能得蒐集個人資料或身分證字號違法連結至其他資料庫而引發疑慮。

大量資料集中管理亦令人擔憂資料外洩的後果將不堪設想。2020 年 5 月，一家國際網路安全公司揭露，台灣有 2 千萬筆個人資訊，包含身分證字號，在線上黑市流通。[19]鑒於台灣總人口約 2 千 4 百萬人，該調查結果引發社會大眾廣泛憂慮，因為這些個人資料在日常生活中不可或缺。然而，政府並未對這項問題有實質作為。

3.2 數位身分系統的隱憂

雖然數位化個人資料能在提供服務前更容易蒐集與傳送驗證身分所需的資料，但正是這份便利使資料數位化後，人們要追蹤個人資料的使用情況變得極為困難。

在沒有法律規範下，大量蒐集與數位身分證有關的數位足跡資料有可能被用來分析個人興趣、習慣或生活方式，一如線上商業科技巨擘追蹤消費者在網路上的瀏覽或購物習慣。

內政部幾次聲稱公部門不會藉由數位身分證的使用蒐集這類與個人活動和位置相關的資料，但沒有將數位足跡資料的處理及儲存納入法律規範範圍，台灣私部門蒐集與使用這類資訊將完全不受管制。

---

[18] Privacy International, A Guide to Litigating Identity Systems, September 2020, paras, 33-34.

[19] '2000 萬筆台人個資流暗網 內政部：非官方外洩', 公視新聞網, 31 May 2020, https://news.pts.org.tw/article/480978.

更重要的是，在沒有明確的法律架構前提下，未來若政府或政策方向更替，個人資料蒐集的相關政策會有遭更動的風險。

使用數位身分證的服務擴大將無可避免地使更多政府單位持有個人資料和數位足跡。因可能受駭客鎖定與攻擊的目標增加，敏感性個人資料外洩的風險也隨之提升。

資料傳送的效率和保護隱私完全無關：根據政府幾份公開文件，數位身分證一部份是為了讓個人能使用 T-Road 入口網絡，2019 年起，國家發展委員會開始推動 T-Road 計畫，其主要目的有二，一是使政府部門間資料傳送標準化；二是發展 MyData 個人化資料自主運用平台。

生物辨識特徵如臉部特徵、指紋及虹膜圖樣經常被世界各地的政府用來作為驗證身分的手段。每個人的生物辨識特徵皆獨一無二，無法更改，為敏感性個人資料。以身分辨識為目的的人臉辨識科技（facial recognition technology, FRT）可被視為無差別大規模監控，會侵害隱私權及其他人權。以台灣的新式數位身分證為例，台灣政府表示其中不會儲存生物辨識特徵資料，但數位身分證中存有 300dpi 的證件照，有被政府用來進行人臉辨識與監控的疑慮。將人臉辨識科技應用於集中管理的影像資料庫可於個人不知情或未同意下取得生物特徵檔案。[20]紐約的案例顯示，即使是蒐集自社交平台的影像也能成為優秀的人臉辨識資料庫。[21]儲存於戶政系統中形式統一的高解析度證件照可說是相當有利於訓練人臉辨識科技的材料。經過幾百萬張人臉影像的訓練，人臉辨識科技的能力近年大幅提升

[20] Drew Harwell, FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches, 8 July 2019, https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/.

[21] Amnesty International, Ban dangerous facial recognition technology that amplifies racist policing, 26 January 2021, https://www.amnesty.org/en/latest/news/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/.

[22]，即使是低解析度影像也可以在幾公尺外被正確識別。[23]但這些科技無可避免地為大規模監控的發展提供強力基礎，對隱私權、集會權及其他權利造成巨大風險。[24]因此，中央研究院專家擔憂未來數位身分證的大頭照有可能遭不當使用。台灣司法院也強調生物識別資料不應儲存於國家身分證。

德國經驗

德國和台灣一樣，發行與使用國家身分證已有相當長的歷史，如今已經數位化成為數位身分辨識系統。[25]2009 年，為面對處理大量資訊的需求及資訊安全的挑戰，德國通過〈身分證及電子識別法〉（Act on Identity Cards and Electronic Identification），定義哪些行政機關得使用數位身分識別系統確認身分，並限制其使用範圍與目的。[26]

德國數位身分證儲存敏感性生物辨識資料，如指紋、眼睛色彩及身高。但政府並不強制蒐集這類資料[27]，因為生物辨識資料極為敏感，

[22] Li et al., 'Face Recognition in Low Quality Images: A Survey', 2018, p1.

[23] Marciniak, T., Chmielewska, A., Weychan, R., Parzych, M. and Dabrowski, A., Influence of low resolution of images on reliability of face detection and recognition. Multimedia Tools and Applications, 2013, pp.4329-4349.

[24] Amnesty International, EUROPE: Proposed legislation too weak to protect us from dangerous AI systems, 21 April 2021, https://www.amnesty.org/en/latest/news/2021/04/eu-legislation-to-ban-dangerous-ai-may-not-stop-law-enforcement-abuse/.

[25] Bundesamt für Sicherheit in der Informationstechnik, German eID, https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/German-eID/german-eID_node.html. (Last accessed: 25 January 2021)

[26] '身分證數位化的表象與實際：一個歷史與比較法的考察' (The appearance and the reality of digitalized ID: An investigation on history and comparative law), Wen-Tsong Chiou et al., August 2020, pp. 109.

[27] 見§23 [PAuswG], Act on Identity Cards of 18 June 2009 (Federal Law Gazette I, p. 1346), amended by Article 4 of the Act of 22 December 2011 (Federal Law Gazette I, p. 2959),

蒐集之可能嚴重影響個人權利。[28]為避免生物辨識資料遭濫用，德國立法禁止該資料集中管理，而該資料僅供相關主管機關，如邊境控制與警察使用。[29]

德國經驗顯示，為保障個人隱私權，政府蒐集敏感性資料須要配套法規，包含資料蒐集相關法律，以及得授權使用數位身分證的政府單位。

愛沙尼亞經驗

愛沙尼亞是世界上最早採取數位身分辨識系統的國家之一，其系統經常被其他國家作為參考案例，為了建立政府與民眾之間的信任，並且民眾對數位身分辨識系統的信心，在 2017 年，愛沙尼亞政府建置逆向監視系統 Data-Tracker，向民眾揭露個人資料如何被政府單位使用，這個系統同時也會顯示政府使用個人資料的原因。[30]

然而，愛沙尼亞的數位化之路也並非一帆風順。在 2017 年 8 月，愛沙尼亞政府因數位身分證系統的安全缺陷，停用約 80 萬張數位身分證，近半數民眾受到影響。[31]從愛沙尼亞經驗來看，任何國家身分證計畫，都應有周全的安全性及隱私評估。

在我們的觀察中，德國及愛沙尼亞的應用案例僅屬少數，數位身分證在許多國家的案例中依舊充滿爭議。

---

[28] OHCHR, The right to privacy in the digital age (3 August 2018), UN doc. A/HRC/39/29, para. 14.

[29] German Missions in the United States, Important Information on the new electronic German ID Card, https://www.germany.info/us-en/service/02-PassportsandIDCards/id-card-important-information/917866.

[30] Federico Plantera, Data tracker – tool that builds trust in institutions, September 2019, https://e-estonia.com/data-tracker-build-citizen-trust/.

[31] Estonian Information System Authority, Estonia resolves its ID-card crisis, 8 December 2017, https://www.ria.ee/en/news/estonia-resolves-its-id-card-crisis.html.

4. 國際人權規範

4.1 相關人權標準與台灣實際執行之落差

隱私權受到《公民權利及政治權利國際公約》第 17 條明文保障，「不得無理或非法侵擾」個人隱私、家庭、住宅或通信，並應立法提供保障。[32]隱私權包含三種彼此關聯之概念：私生活不受干預、掌控個人資訊之自由，及得以自由表達自我之空間。人權事務委員會長期以來認同隱私權保障，包含須立法規範「以電腦、資料庫及其他儀器收集或儲存私人資料–不管是由政府機關或民間個人或機構」之情形。[33]

干涉個人隱私只有在符合國際人權法中非恣意或違法的條件下才得以進行。國際人權法與標準設立了三階段檢測來檢驗干涉隱私權的行為屬合法或違反規定。首先，干涉行為須符合法律規範且有法源依據（合法性）；其次，干涉行為須出於合法意圖；最後，行為須嚴格符合該合法意圖—例如行為是出於維護國家安全或公共秩序而為之（必要性）—且須符合比例、不帶歧視，這表示必須在干涉行為本身，與為干涉而干涉的行為程度間達成平衡（適當性）。

各國有責任積極保障隱私權並應立法或採取相關措施。[34]大量收集及儲存與個人身分及生活習慣有關之資訊會對隱私權形成風險，降低個人對自身資訊的控制。[35]大環境之下，數位工具提升了政府收

[32] Universal Declaration of Human Rights, Article 12; International Covenant on Civil and Political Rights, Article 17.

[33] Human Rights Committee, General comment No. 16: Article 17 (Right to privacy) (1988), UN Doc. HRI/GEN/1/Rev.1 at 21 (1994), para. 10.

[34] OHCHR, The right to privacy in the digital age (3 August 2018), UN doc. A/HRC/39/29, para. 23.

[35] OHCHR, The right to privacy in the digital age (3 August 2018), UN doc. A/HRC/39/29, para. 7.

集與取得個人資訊的能力，這表示必須有效規範並採取其他措施限制當局權力才能有效保障隱私權。[36]

人權事務委員會曾提到，收集與儲存個人資料應受到法律限制。[37]留存於數位身分證之個人資料也可能被其他以認證身分為由，使用數位身證之行為人取用。因此對取用數位身分證施加限制之餘，明定個人資訊合法使用範圍也非常重要。

各國政府須積極主動展現收集、儲存與使用數位身分證內的資料符合特定正當需求，方符合人權原則並正當化隱私權之干涉行為，並須對收集、儲存及使用行為設下清楚限制。若要在數位身分證系統所謂的益處，及其對隱私權造成之衝擊間取得平衡，就必須要有充分的資訊保障。[38]

法律架構須針對處理個人資訊提供標準，讓整體程序更加透明。這代表政府或私人單位在處理個人資訊時應事先知會當事人，而任何會處理個人資訊的行為單位應建立隱私保護機制，例如隱私衝擊補償評估、人權評估等等。也須有明確機制調查人權侵害情形，給予適當補償，做為有效保障補償權的一環。

各國有義務確保包含個人資訊在內的資訊傳輸不會構成或助長不當隱私權干涉。面對大量處理個人資訊帶來的人權問題，其中一種保障機制是由政府成立獨立監督單位，監控政府或商業單位的資訊處理過程。要有效發揮角色功能，必須從法律清楚授權，明訂其職責、權力範圍與獨立性。監督單位也須獲得足夠的技術、財力與人力資源，以調查任何公私部門犯下地濫用資訊行為；另也須授與充分法律權力以回應任何侵害或濫權行為，包含適當實施制裁的權力。[39]

---

[36] OHCHR, The right to privacy in the digital age (3 August 2018), UN doc. A/HRC/39/29, para. 26.

[37] Human Rights Committee, General comment No. 16: Article 17 (Right to privacy) (1988), UN Doc. HRI/GEN/1/Rev.1 at 21 (1994), para. 10.

[38] Privacy International, A Guide to Litigating Identity Systems, September 2020, para. 44.

[39] OHCHR, The right to privacy in the digital age (3 August 2018), UN doc. A/HRC/39/29, para. 33.

台灣目前的法規並無清楚限制那些政府單位有權取得、收集及使用數位身分證之個人資訊。當前法規也未規範資料存儲的範圍與時機。[40]

另外，台灣目前也無任一政府單位在隱私權的領域上有任何權威或職責，因此各單位都能再個人資訊和隱私保障上發展自己的制度，讓整體隱私保障體制變得十分薄弱，既不獨立也不有效。

5. 結論與建議

國家身分證系統本身即須大量收集個人資訊。為了「智慧政府」數位化相關個人身分資料，可能會擴大個人資訊收集範圍，對隱私權進一步形成風險。

我們呼籲台灣政府在尚未完整規劃與建立監督機制保障個人資訊前，不應採用新的數位身分證制度。我們也呼籲台灣政府將國際對人權的認知，應用在檢驗數位身分證相關之法律架構、機構與政策上，且檢驗須符合合法、必要與適當原則，並納入《世界人權宣言》第 12 條、《國際公民與政治權利公約》第 17 條及其他相關國際法與標準。

5.1 建議

國際特赦組織台灣分會呼籲台灣政府：

- 全面規範與新興數位身分證有關之內容，以免公、私部門濫用個人資訊，並應明確詳細指出數位身分證得於何種情況使用，例如資料範圍、性質、取用及存儲，並明訂有效保障措施；

[40] Amnesty International, TAIWAN: SUBMISSION TO THE INTERNATIONAL REVIEW COMMITTEE ON THE DOMESTIC IMPLEMENTATION OF THE ICCPR AND THE ICESCR: 3RD REPORTS, 22-26 MARCH 2021 (22 October 2020), ASA 38/3212/2020, p. 12.

- 建立獨立機構以確保有效監督公、私部門是否依循隱私相關規範，並調查可能發生隱私權侵害之情形；
- 保留非晶片身分證作為確認身分的選項；
- 建立機制揭露個人資料使用情形，提供透明的政府取用資料程序；
- 規劃並進行數位身分證計畫的隱私影響評估。

國際特赦組織是一個全球性的人權運動。

當一個人遭遇不公義的事情，都與我們所有人息息相關。

info@amnesty.tw

+886(2) 2503-9301

@AITW0528 @AmnestyTaiwan @Amnestytw Amnesty International Taiwan