元照出版提供　請勿公開散布

面部自動辨識監控系統與個資保護問題研究
——Bridges案之啟示

翁　逸　泓*

要　目

壹、前　言
　一、準確度之質疑
　二、歧視性之問題
　三、國家監控之威權問題
貳、Bridges案作為觀察起點
　一、案件事實
　二、法院判決
　三、資訊委員意見
參、Bridges案的啟發：警用密錄器與規模化面部辨識系統
　一、監視器之個資爭議：警用密錄器
　　㈠未有明確之特定法規
　　㈡個資法上的問題：適用與否
　　㈢警用密錄器在個資保護與資訊透明之衡平
　二、科技時代下公共空間與隱私的合理期待：大規模面部辨識

DOI：10.53106/102398202022030168005

* 世新大學法律學院副教授，英國德倫大學法學院法學博士。本文為作者執行科技部研究計畫（MOST-109-2410-H-128-019-）之研究成果。作者衷心地感謝諸位審稿人之具體評論、建議與提點，這些寶貴的意見對本文以及對於作者本身都有極大幫助與鼓勵，惟文責當由作者自負。

投稿日期：一一〇年一月十三日；接受刊登日期：一一〇年九月十七日

責任校對：鍾淑婷

元照出版提供 請勿公開散布

㈠在科技新穎化時代下，於公共空間中的個人仍應有隱私之期待
㈡大規模面部辨識與公共場域的合理隱私期待：程序與組織保障
肆、以人工智慧／自動化系統結合面部辨識之監控
一、科技治理與信任基礎
㈠平等原則
㈡透明原則
㈢課責原則
二、以人工智慧／自動化系統作為治理方法？
㈠從體系解釋之角度，應採禁止說
㈡GDPR之有權解釋機關，亦採禁止說
㈢從目的解釋之角度，應採禁止說
伍、結　論

元照出版提供　請勿公開散布

摘　要

本文探索自動面部識別技術（Automated Facial Recognition technology, AFR）作為政府監控所可能發生之個資保護爭議，並以世界首例之英國Bridges v CCSWP and SSHD案判決為起點，分析我國推動AFR於打擊犯罪防止等目的時，所須滿足之個資保護要件與實際治理策略。

本文研究之問題依序為：Bridges案所能帶來的啟發為何？AFR在個資保護法制架構的概念上，所引起之爭點為何？又應當如何應對？

本文認為思考任何以科技方式治理決策時，無論是十餘年前全民指紋錄存釋憲案，乃至大規模AFR，於進行系爭權利辨識以及衡平之前，都應先考量降低權利間競合之風險。如就資料治理言，當政府要將人民對其基於民主之相互信任關係移轉至由自動化系統或人工智慧進行決策時，因為難以具體地對於該等非人類決策進行課責，因此若期待重塑整體資料治理之信任基礎，本文認為更需要有個資權利在法制、程序以及組織上之強化保護與作為。

關鍵詞：面部辨識、人工智慧、資料治理、個資保護、GDPR、隱私權、科技治理、自動面部辨識

元照出版提供 請勿公開散布

壹、前 言

本文所討論之主題為探索應用自動面部識別技術（Automated Facial Recognition technology, AFR）而蒐集、處理與利用特定或不特定之個人活動與位置資料，以作為政府監控情境的情況下，所可能發生之個資保護爭議問題。本文對此以世界首例於二〇一九年九月之英國相關案件Edward Bridges v The Chief Constable of South Wales and Secretary of State for the Home Department（R (bridges) v CCSWP and SSHD）[1]案之法院判決為觀察對照，試圖分析在我國推動AFR加值應用於政府打擊犯罪防止等目的監控時，所必須滿足之個資保護要件與實際執行上的個資治理策略。

無獨有偶地，在二〇一九年十一月臺灣鐵路局亦準備完成類似之自動面部辨識監控系統。依據交通部新聞稿，雖然長久以來臺鐵在各車站均建置有CCTV系統將車站各重要區域予以完整監控來處理發生緊急或意外狀況之調閱畫面，但是該等「被動式」之管理被其認為猶有不足，因此鐵道局（前鐵工局）在辦理鐵路工程計畫時，即持續考量如何利用攝影機先進技術，參考國外先進車站及高鐵局和中科院合作於高鐵臺中站建置「智慧影像監控系統」辦理經驗，[2]選定於臺鐵豐原站試辦「智慧型影像監控系統工程」。[3]該案

1 Edward Bridges v The Chief Constable of South Wales and Secretary of State for the Home Department, [2019] EWHC 2341 (Admin), 4 September 2019.

2 需注意者，時任高鐵局長說明在2015年12月已在高鐵臺中站試用，系統偵測異常行為包括月臺黃線區域有人無故滯留、車廂月臺有人急速奔跑，人員闖入禁止區域、平交道；其表示「原想在車站及車廂推『人臉辨識系統』，但涉及隱私，將改為『特徵辨識』，以穿著、身高類似為對象過濾。未來將優先推廣到台鐵豐原站，期能降低台鐵平交道死亡率」。黃立翔，高鐵防鄭捷們　整合沿線監視器動態偵測，自由時報，2016年2月25日，https://news.ltn.com.tw/news/life/paper/961770，最後瀏覽日：2020年11月13日。

元照出版提供　請勿公開散布

承攬廠商結合監視系統與物聯網（internet of things, IOT）設備，**打破單一監控設備**的限制，其影像辨識系統能在發現潛在風險時立即發出警訊，並利用運算科技而使終端設備能**截取旅客特徵**，並**透過人工智慧分析**，即時通知站務或警務人員前往處理，且後續即可於其他臺鐵車站陸續推廣，甚至加以**普及化**。[4]不過，因為其人工智慧運算標的包含**警務用安全**（觀察）名單，甚至包括**身障**人士之白名單以方便其進出車站，因此引起隱私疑慮與新聞報導。為此，交通部於隔日再以新聞稿指出「本系統目前仍由鐵道局建置測試中，惟基於各界對於人臉辨識功能及適法性仍有疑慮，臺鐵局將不使用該項功能，並已協調鐵道局及鐵警局取消其中人臉辨識功能及安全特殊名單（警務用），**以確保民眾隱私權不受侵害**」。[5]準此，交通部主要係基於考量了隱私權保障之爭議，而予以暫緩應用AFR之功能。

然而相對於交通部主要考量的隱私問題，在關於AFR於國際的應用實例上，所可能遭遇的疑難並非僅限於隱私與個資保護之單一

3 黃育仁，豐原站智慧監視恐侵隱私　台鐵決定不用人臉辨識功能，華視新聞，2019年11月6日，https://news.cts.com.tw/cts/life/201911/201911061980187.html，最後瀏覽日：2021年5月24日。

4 中華民國交通部，交通新聞稿，臺鐵豐原站智慧型影像監控系統試辦案，2019年11月5日，https://www.motc.gov.tw/ch/home.jsp?id=14&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201911050001&aplistdn=ou=data,ou=news,ou=chinese,ou=ap_root,o=motc,c=tw&toolsflag=Y&imgfolder=img%2526amp%253B%2526%2523x23%253Bx2f%2526%2523x3b%253Bstandard，最後瀏覽日：2019年11月8日。

5 中華民國交通部，交通新聞稿，有關報載「火車站人臉辨識恐侵人隱私」臺鐵局回應說明，2019年11月6日，https://www.motc.gov.tw/ch/home.jsp?id=14&parentpath=0%2C2&mcustomize=news_view.jsp&dataserno=201911060002&aplistdn=ou=data,ou=news,ou=chinese,ou=ap_root,o=motc,c=tw&toolsflag=Y&imgfolder=img%2Fstandard，最後瀏覽日：2019年11月8日。

元照出版提供 請勿公開散布

問題，而至少包含了對於該等技術之準確度、歧視性，以及監控威權主義等風險問題：

一、準確度之質疑

雖然AFR比對之準確率在科技進展之下大幅地提高，但是仍有發生比對錯誤之風險存在，即便是AFR在國際應用上相對成熟的美國，美國政府責任署（Government Accountability Office, GAO）在其二〇一九年相關報告[6]發現FBI在接受和部署其面部識別系統之前，對面部識別搜索的準確性僅進行了有限的評估，且FBI尚未評估由外部合作夥伴（例如州或聯邦機構）管控的面部識別系統的準確性，並建議採取措施確定外部合作夥伴系統對於FBI的使用是否足夠準確。GAO也發現FBI並未進行年度審查來確定面部識別搜索的準確性是否滿足使用者需求。[7]

二、歧視性之問題

在面部辨識的爭議中，美國因為佛洛伊德案件所引起的平權運動，使IBM與AMAZON等基於面部辨識技術對某些族群的準確率比其他低，一直被認為有種族歧視之緣故，而對警方暫停提供技術與應用；[8]美國電腦協會（Association for Computing Machinery,

6 GAO, Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains, GAO-19-579T, June 4, 2019, *available at* https://www.gao.gov/assets/700/699489.pdf (last visited: 2020.11.13). 需注意者，至2019年5月止司法部和聯邦調查局已採取了部分行動來解決三項建議，卻未對其他三項採取任何行動。

7 *Id.* at 1.

8 Asa Fitch, Amazon Suspends Police Use of Its Facial-Recognition Technology, The Wall Street Journal, June 10, 2020, *available at* https://www.wsj.com/articles/

元照出版提供　請勿公開散布

ACM）也向國會發出公開信，同樣地基於考量面部辨識技術存在民族、種族以及性別偏見，應該立刻禁止企業和政府使用臉部辨識技術。[9]

三、國家監控之威權問題

由於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，面部辨識在實際應用上的功能大致上可分為三個類型：一對一對照獲得之確認功能；一對多對照之辨識功能；以及比對後符合一般特徵之分類功能，[10]此間因為面部之**外露性、頻繁性**以及採樣比對時可以依靠鏡頭**主動蒐集**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權利等基本權利與自由保障事項，而造成之結果不但對於個資侵害風險顯著升高，且風險實現之可能性也隨之升高。倘國家不斷地強化其關於生物特徵監控之硬體設備，例如大量廣布應用AFR功能之監視鏡頭，且串接其他公、私部門資料庫，例如警政、戶政、健保甚至金流資料庫，則對隱私之破壞性

---

amazon-suspends-police-use-of-its-facial-recognition-technology-11591826559?mod=tech_lead_pos1 (last visited: 2020.11.13).

9 ACM U.S. Technology Policy Committee, Statement on Principles, and Prerequisites for the Development, Evaluation and Use of Unbiased Facial Recognition Technologies, June 30, 2020, *available at* https://www.acm.org/binaries/content/assets/public-policy/ustpc-facial-recognition-tech-statement.pdf (last visited: 2020.11.13).

10 European Union Agency for Fundamental Rights, Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement, pp. 7-8, *available at* https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf (last visited: 2020.11.13).

元照出版提供 請勿公開散布

侵害更有明顯妨害人格自由發展之疑慮。再，如果國家運用資訊與通訊科技（Information and Communication Technologies, ICTs）進一步地透過極端面部特徵辨識之身分實名制以對於社會管理與控制，甚至引導民意而鞏固政權，則可能為學者所稱「科技威權主義」（technological authoritarianism）之實現，[11]帶來充沛可行之機會。

不過如果企圖對以上列舉之問題癥結作出關於AFR應用在法律上之全面分析，就廣度言顯非本文的單一研究篇幅限制所能及，因此本文僅將主要的焦點集中在個資保護之層面。由於個資保護之概念、體系建構以及具體實踐等，都以歐洲較具有國際上影響力，且我國個資法係移植自歐盟個資保護相關法制，而英國在脫歐前已於二〇一八年公布資料保護法（Data Protection Act 2018, DPA 2018）[12]以對應歐盟一般資料保護規則（General Data Protection Regulation, GDPR），[13]因此本文以歐洲相關立法與研究以及實踐作為借鏡對象。至目前為止就整個歐盟（包含脫歐前的英國）來看，歐盟之官方文件指出以英國警方在執行法律時最積極地應用AFR。[14]相對於

11 王信賢，科技威權主義：習近平「新時代」中國大陸國家社會關係，展望與探索，16卷5期，頁113-117，2018年5月。

12 英國的2018年資料保護法係其關於個人資料保護的第三版本法規範，承繼英國1998年資料保護法（Data Protection Act 1998, DPA 1998），而英國早在1984年便有資料保護法（Data Protection Act 1984）。第二版本之DPA 1998係爲對應歐盟個資保護指令（Directive 95/46/EC），而第三版本之DPA 2018乃是對應歐盟之一般資料保護規則（GDPR）。

13 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, *OJ L 119, 4.5.2016, pp. 1-88*.

14 European Union Agency for Fundamental Rights, 11.

元照出版提供　請勿公開散布

英國警方的積極應用，歐盟指出雖然德國也在二〇一七年至二〇一八年間在柏林的火車站試辦AFR，而法國也在尼斯二〇一八年的嘉年華應用AFR，但是德國與法國對於AFR之應用均是小規模試點，且都有經過當事人之自願同意，而非如英國一般大規模地用於監控。[15]不過也正因為如此，導致英國發生了世界上第一個相關訴訟案件。基於本案係為全世界關於第一件AFR與政府為打擊犯罪、維護治安等「公共利益」而對不特定人民監控之判決，對於我國當前相關實務爭議之解決或許帶來些許線索。是以，本文以其相關事實與判決結果作為引線，嘗試釐清問題之癥結。綜上，本文將焦點集中於AFR之應用在個資保護上的爭議，提出以下研究之問題：

㈠Bridges案所能帶來的啟發為何？

㈡AFR在我國個資保護法制架構的概念上，所引起之爭點為何？如何應對？

為此，本文在架構上首先簡要敘述Bridges案內容始末，分析判決理由以及英國個資保護獨立專責機關之意見。在回顧與分析比較法上之狀態後，本文分別從國家對人民[16]以監視器攝錄影面部、各類結合面部辨識功能科技，以及以自動化系統乃至人工智慧方式將蒐集而得之個資結合面部辨識應用等不同視角與爭議問題，[17]來分析各自對個資風險之升高與侵害可能。在本文架構上基於整體

15 德國事實上曾在2017年的G20高峰會上為了維安而應用AFR，但漢堡個資保護委員提出報告指出該等應用缺乏法律保留，不合個資法規定；*id.* at 12.

16 關於國家監控與法規範之整體研究，可參MARIA HELEN MURPHY, SURVEILLANCE AND THE LAW: LANGUAGE, POWER AND PRIVACY (2019).

17 事實上本案牽涉範圍以更宏觀之角度來看，亦涉以人工智慧為資訊治理乃至法律治理之層次，其中除法律面向外，亦涉及倫理與社會面向，而甚至足以自成一格形成人工智慧之倫理、法律與社會應用（Ethical, Legal and Social Implications, ELSI）領域。

元照出版提供 請勿公開散布
面部自動化辨識之應用在結構上大致可以區隔成兩個面向來分析相關個資保護問題，也就是「面部辨識」（Facial Recognition）在應用上本身關於個資保護之爭議問題，以及自動化決策系統（Automated）結合了面部辨識這個科技治理方式上出現的個資保護問題。簡言之，前者本文討論的是FR本身之問題，後者則分析AFR之整體科技治理問題。關於前者，本文以我國法律規範幾近空缺之警用密錄器所得資訊進行面部特徵辨識行為作為研究標的，分析其在個資保護上發生之可能爭議問題；復次，在Bridges案中重要爭點之一即在於大規模地在公共空間中實行AFR時必須特別對於何人被置於監控名單以及在何地施行AFR監控等問題予以特別規範，以保護全民之個資權利及合理隱私期待，本文以臺灣之現狀為對象加以比較評析。而關於後者，即在分析基於在比對資料庫之監控名單與即時面部監視辨識所得之資料，而為包括自動刪除比對資料等之自動化決策問題，討論何種態樣之法律規範在AFR應用之時足以保障人民個資權利。

貳、Bridges案作為觀察起點

二〇一九年九月，英國新南威爾斯地方法院之R (bridges) v CCSWP and SSHD案之判決書上開宗明義地點出：（規範）演算法之法律必須跟上新興的技術，[18]而本案之判決提出關於員警部隊使用AFR之科技與法律問題，其核心關鍵爭點在於英國當前法律制度，是否足以確保在自由和文明的社會中適當及非任意地應用AFR，尤其是必須釐清關於AFR的隱私和個資保護影響爭議。準此，本文就該案之基礎事實、法律規範與法院判決之重要之處加以

18 R (bridges) v CCSWP and SSHD, para. 1.

元照出版提供　請勿公開散布

說明，以為其後論述之起點。

一、案件事實

本件事實發生地為英國南威爾斯的卡爾地夫，原告Edward Bridges為英國人權團體之一員，而南威爾斯警方（South-Wales Police, SWP） 警方利用AFR拍攝到他外出買三明治及參加和平示威。為此，Bridges質疑SWP使用AFR定位（面部識別技術的特殊應用）的**合法性**，理由是使用AFR定位系統違反了一九九八年人權法（Human Rights Act 1998, HRA 1998）、DPA 2018，以及SWP實際執行時並未依二〇一〇年平等法（Equality Act 2010）所載公共部門平等義務為之。另方面，法院也注意到了英國執法機關不僅使用AFR，在科技發展的進步之下，歷有使用生物特徵辨識技術包括去氧核糖核酸（DNA）證據的刑事案件法醫學使用、[19]閉路電視（CCTV）證據、[20]自動車牌識別技術（automatic number-plate recognition technology, ANPR）被全國員警廣泛使用、細胞現場證據等相關訴訟。[21]

---

19 關於DNA與資料庫監控問題，在英國與歐洲人權法院之著名案例即為S. and Marper v the United Kingdom App no 30562/04 (ECtHR, 4 December 2008)。中文相關文獻，參翁逸泓、廖福特，私生活權利：探索歐洲，反思台灣，頁81-108，2014年12月。

20 相關中文文獻之探討，參李寧修，警察存取預防性資料之職權與個人資料保護：以監視器之運作模式為例，國立臺灣大學法學論叢，48卷2期，頁391-437，2019年6月。

21 此外，關於電子通訊（包括網路）監察，在英國前亦有關於「資料留存與調查權力法」（Data Retention and Investigatory Power Act 2014, DRIPA）及其後「2016調查權力法」（Investigatory Powers Act 2016）所引起之關於打擊犯罪或反恐之警察調查權之個資保護與隱私訴訟。

元照出版提供 請勿公開散布

二、法院判決

本案英國地方法院判決警方勝訴，也不認為應對警察相關調查權進行全面司法審查。其理由略為：

㈠SWP使用AFR與位置資訊符合一九九八年人權法的相關要求，而使用AFR與位置資訊也確實涉及**被拍攝和處理圖像**社會大眾關於歐洲人權公約第8條所保障的私生活權利。[22]

㈡AFR雖然與隱私及個資有關，但是此等行動受到政府之相關基本規範（包括資料保護法）、法定行為守則（codes of practice）和SWP自行公布的個資保護政策中，所包含之充分法律控制的約束與限制，[23]並且均具法律正當性，因此合於合法性原則之要求。[24]細究之，在**每次**AFR使用之時，均有使用上時間以及針對特定與限制性目的之限制；又，除非**被拍攝和處理圖像而辨識出**之社會大眾與監控名單上的人相符，否則與監控名單無關的所有資料和個資均在得到比對處理後，**立即地被刪除**。需注意者，法院認為即使不能在公眾之間辨識出監控名單上之特定人，該等AFR之行為仍然是在處理個資。[25]

㈢法院指出在進行本AFR訴訟前，SWP均符合公部門關於國家平等對待義務之要求。[26]

㈣法院進一步得出結論，SWP利用AFR對個資的處理係合法，且完全符合法律規定的條件，尤其是DPA 2018中適用於SWP等執法者的條件。[27]

---

22 R (bridges) v CCSWP and SSHD, paras. 47-62.
23 *Id.* paras. 63-97.
24 *Id.* paras. 98-108.
25 *Id.* paras. 110-27.
26 *Id.* paras. 149-58.
27 *Id.* paras. 128-47.

元照出版提供　請勿公開散布

其中DPA 2018關於特種個資例外得為個資處理之條件，原告聲明中認為SWP對AFR利用違反DPA 2018之理由有二：第一，AFR在公共領域擷取不特定大眾之面部特徵，分析後與資料庫上監控名單相比對，係為DPA 2018第35(8)條所謂處理**敏感性特種資料**，因此除有例外情狀，均應禁止；第二，SWP對AFR之應用不符合DPA 2018第35(5)條之要求，包括以執行法律為目的而處理個資之「嚴格必要性」（strictly necessary）要求、DPA 2018附件8對處理敏感性特種個資之前提條件要求，以及並無符合DPA 2018第42(2)條標準所規定之公布與存放個資保護政策文件。法院對第一個原告聲明採肯定之見解，認定本案AFR所處理者確為生物特徵（biometrics）個資，且為敏感性／特種資料，與GDPR第9條及歐盟法律執行指令（Law Enforcement Directive, LED）[28]第10條規範解釋上一致。[29]但即便如是，法院審酌各項法規與警方內部規則及個資保護政策後，認為警方的確滿足各項條件要求，因此係合法地處理該等敏感性個資。

在此必須說明關於歐盟層級之GDPR、LED及英國國內法層級之DPA 2018之規範中，例外得**以執行法律為公共利益目的而處理敏感性個資**之條件，方能更體系性地解釋為何地方法院允准該等個資

28 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA *OJ L 119, 4.5.2016, pp. 89-131.* 在此基於該等刑事或公共安全維護目的執行法律而干預個資之行為，在歐盟層級乃係LED之規範，而非GDPR所企圖全部涵攝者。

29 R (bridges) v CCSWP and SSHD, para. 132.

元照出版提供 請勿公開散布

處理。[30]先就個資保護領域言，英國甚至早於歐盟相關規範而在一九八四年便制定資料保護法（Data Protection Act 1984），並成立資料保護登記官（Data Protection Registrar），此即為英國資訊委員（Information Commissioner, IC）之前身。其後身為歐盟會員國之一員，英國在歐盟一九九五年個資保護指令（95/46/EC）[31]後將其轉換至國內法而有一九九八年資料保護法（Data Protection Act 1998, DPA 1998）與一九九八年人權法（Human Right Act, HRA）[32]分別落實個資保護與人權保障之規範。其中，個資保護指令與英國國內法之DPA 1998分別可被視作是歐盟法與英國法層級之個資保護基本法，而歐盟就個資之保護相關之特別領域陸續規範有「電信事業個人資料處理及隱私保護指令」、[33]「隱私及電子通訊個人資料保護指令」（ePrivacy Directive, ePD）[34]及「共同體機構及部門間個人資料自由流通之規則」[35]等特別規定。[36]

---

30 關於系統性地分析GDPR如何施行於英國準據法體系中，以及在實際執行層面上如何將其化爲簡單文字的規範具體落實，詳參翁逸泓、李寧修，「歐盟國家個人資料保護法制因應GDPR施行之調適——以德國與英國爲例」委託研究計畫結案報告，國家發展委員會，2020年5月。

31 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ L 281, 23.11.1995, pp. 31-50.*

32 「歐洲聯盟基本權利憲章」（Charter of Fundamental Rights of the European Union）第8條中亦明文規範有對個資保護之規定。

33 Directive 97/66/EC of 30 January 1998 the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector [1998] OJ L24/1.

34 Directive 2002/58/EC of 31 July 2002 the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37.

35 Regulation (EC) 45/2001 of 12 January 2001 the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the

元照出版提供　請勿公開散布

及至二〇一八年正式施行GDPR，由於GDPR除了具有歐盟法上「規則」（Regulation）層級一體適用之效力，而僅在部分之規範令會員國有以國內法選擇是否調和，也就是會員國可基於本國法律體系或國情而對某些特定之條文規範而「排除」（derogation）GDPR之空間外，GDPR本身也具有「一般性」（general）之基本法特質。[37]也因此在歐盟層級的資料保護法體系上，除了GDPR以外，尚有包括LED[38]乃至研議中的「電子通訊隱私規則提案」（ePrivacy Regulation, ePR）[39]等特別領域規定，完整而交錯地保護個資權利。為此，英國在一般個資保護基本法上，乃更新至第三版本的DPA 2018。在內容上比較GDPR與英國DPA 2018，由於制定後者當時英國仍為歐盟會員國，因此除可排除之彈性立法部分，大致上與GDPR規範一致以求減少脫歐之法規陣痛機會成本。而前述所謂會員國得彈性立法之部分，即包括GDPR之補充、於特殊案件之調整、法律執行機關以及國安情報之例外，也因此英國除了在DPA 2018安置了一般領域之個資保護規範以及包括LED與ePD之歐盟指令之一般性個資保護原則外，在法律執行與國安情報之特別領

processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L8/1.

36 翁逸泓、廖福特，同註19，頁48-53。

37 翁逸泓、李寧修，同註30，頁42-44。

38 由於LED係爲歐盟法上指令之層級，因此會員國須轉換爲本國法。另方面，雖然GDPR爲規則層級本有會員國一體適用之效果，但是因爲GDPR本身仍有使會員國能在部分排除規定有立法裁量適用之餘地，因此DPA 2018同時依循了GDPR與LED之立法原則。

39 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final - 2017/03 (COD).

元照出版提供 請勿公開散布

域，另有「資料留存與調查權力法」（Data Retention and Investigatory Power Act 2014, DRIPA）即其後之「2016年調查權力法」（Investigatory Powers Act 2016）。

另方面，英國亦為歐洲理事會（Council of Europe）之會員國[40]並同受歐洲人權公約（European Convention of Human Rights, ECHR）拘束，而歐洲理事會乃至歐洲人權法院（European Court of Human Rights, ECtHR）對於國家蒐集個資之行為相對於歐盟法院（Court of Justice of the European Union, CJEU）採取較為謹慎之態度，除有「關於個人資料自動化處理保護個人公約」（Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data）對於個資之蒐集與處理為依歸外，在實際案例之判決上通常以歐洲人權公約第8條作為判決基礎。[41]

在說明本案所涉及的GDPR相關規定與英國DPA之連動體系關係後，本文認為可以從以下之面向分析該地方法院之判決：

1. 比例原則與公共利益之連動性面向

由於面部特徵為生物特徵的一種，因此為特種個資，原則上禁止處理，而例外得處理特種個資的第一個條件規範在DPA 2018第35(5)條，即前述所謂「嚴格必要性」（strictly necessary）要求。惟需注意者，DPA 2018此處的概念係來自為執法目的之LED第10條，而其內涵依據歐盟個資保護指令第29條工作小組（WP 29）在其對LED之意見[42]中指出「嚴格必要性」必須理解為要求「在處理特種敏感資料時特別注意必要性原則，並預見處理此類資料的確切

40 需注意者，由於歐盟與歐洲理事會爲兩個不同之國際組織，因此即便目前英國退出歐盟，也仍爲歐洲理事會之會員國，不可混淆。

41 翁逸泓、廖福特，同註19，頁47-48。

42 Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP 258, 29 November 2017.

元照出版提供　請勿公開散布

和特別堅實之合理化事由」（foresee precise and particularly solid justifications），換言之，此種以「公共利益」作為處理特種個資例外允許之事由，對該等「公共利益」即必須特別注意所謂的「公共利益」當然不能以概括的規定方式為之，而是必須具有可預見性、正當化之事由需明確、特定且具不易變動性等。而這個所謂的「公共利益」，更不是在應用AFR時可以任由執法機關任意指稱其執法行為均是在追求包括維護社會治安等鬆散、模糊而概括之公共利益可以輕輕帶過的。本文認為，或許如同英國DPA 2018第35(5)條所對應之DPA 2018附件1第2部分，特別針對特種個資與犯罪偵查資料中的實質公共利益作出詳細描述，也就是在何種情狀下之何種特定公共利益為細緻的說明，是一個可能的選擇。不過，這種規範之態樣當然也可能招致法律之規範本就難以對於各種實際執法情狀完整預測之議。對於此，本文認為即便規範的態樣無法如此細緻，但是至少執法機關具體的個資保護政策說明文件乃是不可或缺，且可以預先將隱私與個資保護機制預先安置，而得隨時調整的。

除了前述DPA 2018第35(5)條外，對特種個資處理之其他條件、則更詳細地規範在DPA 2018附件8。需要特別注意的是在比例原則之檢驗上，因為英國係歐洲理事會之會員國並受歐洲人權法院管轄，因此對於該等干預個資保護與隱私權之檢驗，同時仍須合於歐洲人權公約第8條對個人私生活權利保障所要求，必須有「民主社會之所需」，且其理由是「相關及充分的」。[43]

2. 個資保護政策文件之面向

在DPA 2018第35(5)(c)條中，明確要求個資控管人必須具備合於同法第42(2)條所規範之個資保護政策：該政策需解釋個資控管

43 S. and Marper v the United Kingdom (2009) 48 EHRR 50, para. 112.

元照出版提供 請勿公開散布

人確保遵守資料保護原則的程序（參見同法第34(1)條），如有關敏感性特種個資之處理，需有資料當事人的同意或（視情況而定）其他例外情狀條件之滿足；以及解釋個資控管人關於依據資料主體的同意或（視情況而定）其他例外情狀條件之滿足而保留和刪除個資的政策，並具體指明此類個資可能被留存的期限。

然而，關於此處個資保護（或隱私權）政策，因為DPA 2018第42(2)條僅係為對於敏感性個資處理之一般性要求，而缺乏對於「系統性對不特定大眾辨識」此種經常性對敏感性資料處理而升高隱私與個資風險之特別說明，且該政策並未公開於大眾周知，因此在本案中法院對此存有疑問。不過，法院將此處未有具體細部指引（guidelines）之問題歸諸於資訊委員，因為法院認定依照DPA 2018附件13，則該等具體指引之頒布而使個資控制人能夠有所遵從，乃係為資訊委員之職責所在，因此並不認為SWP未盡其法律上義務。[44]再者，同樣地對於該等系統性對不特定大眾辨識特種個資之行為的特別隱私權政策內容指引乃是資訊委員之權責，因此法院也無意進一步地認定與說明該政策內容應包含之詳細要點為何，而留待給資訊委員認定。[45]本文認為，在此處也一併地使得個資保護專責機關在組織架構上對於個資保護之重要性更特別地被凸顯。

然而，這樣的判決認定警方得大規模地應用AFR之結果毫無意外地引起一陣譁然，甚至就連英國的資訊委員也為此表達一定程度之遺憾。因而，本案敗訴方即原告為此依據歐洲人權公約第8條、英國DPA 2018以及平等法提起上訴，上訴法院[46]於二〇二〇年八月

44 R (bridges) v CCSWP and SSHD, paras. 139-40.

45 *Id.* para. 141.

46 Court of Appeal judgment in R (Bridges) v Chief Constable of South Wales Police & Others, [2020] EWCA Civ 1058.

元照出版提供　請勿公開散布

以判決分別對原告的五個聲明為認定：

⑴SWP相關作為不符合歐洲人權公約第8條第2項之「依法」得限制基本權利與自由之要件：該作為雖符合DPA 2018以及授權命令的錄影監控行為準則（Surveillance Camera Code of Practice），但是對於**誰**將會被納入對比名單，以及將會在**何處**實施AFR並**未有明確之指引**規範。[47]

⑵上訴法院部分地同意地方法院的判決，認定SWP使用AFR是基於對歐洲人權公約第8條第2項規定而對私生活權利為一定程度的干涉：上訴法院認為地方法院對此已經正確地進行衡平AFR之使用所帶來之公共利益以及原告之私生活權利，且前者較後者更具強烈之應受保護性。[48]

⑶上訴法院認為SWP認為其依據DPA 2018第64條的規定而提供足夠的個資保護影響評估（Data Protection Impact Assessments, DPIAs）是錯誤的：基於DPIA係建立在歐洲人權公約第8條關於私生活權利之基礎上，但在第一聲明中，上訴法院認為SWP違反歐洲人權公約第8條的規定，因此在邏輯上連帶地使得該DPIA也存在缺陷：[49]DPIA沒有適當評估個人權利和自由的風險，也沒有採取為應對法律框架缺陷所引起風險而生之措施。

⑷上訴法院認為地方法院認定SWP未依DPA 2018第42條所指而制定「適當政策文件」是錯誤的：這是因為原告所主張之法律基礎，均發生在DPA 2018生效之前，因此不需為之。[50]

---

47 *Id.* para. 152.
48 *Id.* para. 143.
49 *Id.* para. 153.
50 *Id.* paras. 155-57.

元照出版提供 請勿公開散布

在此需注意者，上訴法院並非認為不需制定「（個資保護）適當政策文件」，而僅只是因為彼時DPA 2018尚未生效，故不應溯及地要求SWP在當時便有「（個資保護）適當政策文件」。

⑸就避免歧視之面向言，上訴法院認為地方法院認定SWP之作為合於公務部門之「平等對待義務」（public sector equality duty, PSED）有所違誤。英國之平等對待義務係基於二〇一〇年英國平等法而來，要求其政府公共部門在開展活動時應充分考慮消除歧視，促進機會均等以及在不同人群之間建立良好關係的必要性。[51]與本案相關的兩個平等法上特質為種族與性別，上訴法院認定PSED之目的是確保公務部門考慮政策是否會產生歧視性的潛在影響，而即便沒有明確的證據表明AFR之演算法實際上是基於種族和／或性別的偏見，但SWP也未能採取合理程序來確認AFR之演算法是否出於種族或性別歧視。[52]

在上訴法院宣判之後，SWP隨即表示不再上訴，使得本案至此確定。

---

51 英國平等法之主要目的在於規範保護人民免受服務和公共職能、工作、教育、結社和運輸中直接和間接歧視，騷擾和傷害的基本框架，透過取消醫療監督的要求來改變性別分配的定義，爲因被認爲擁有或與某人具有受保護特徵相關的歧視而提供保護，爲母乳餵養的母親提供更明確的保護，將間接歧視的統一定義應用於所有受保護的特徵，及統一允許自願採取積極行動的規定等。

52 Court of Appeal judgment in R (Bridges) v Chief Constable of South Wales Police & Others, [2020] EWCA Civ 1058, paras. 163-202.

元照出版提供　請勿公開散布

三、資訊委員意見

相較於歐盟層級關於GDPR本身之解釋落在歐盟的個資保護委員會（European Data Protection Board, EDPB），[53]在GDPR之國內執行以及英國國內法DPA 2018之落實上，有兩個組織上機關分別執行不同職責。其一是係為英國文化、媒體與運動部（Department for Digital, Culture, Media and Sport, DCMS），乃是確保GDPR於英國要求之適足性的部會，也負責制定英國資料保護法之立法，但並不為DPA 2018之實際施行；至於GDPR及DPA 2018實際執行則交由英國資訊委員，其權力包括（關於個資）犯罪調查與罰鍰等，並提供企業與人民團體與政府機關（包含地方政府）對於如何適應GDPR之指引，換言之，資訊委員對於DPA 2018以及GDPR之在地落實詮釋，自有其權威性。

基於GDPR以及DPA 2018之相互關係，DPA 2018也對於資訊委員賦予國際合作職權，如與其他國家個資保護專責機關之合作、履行國際個資保護規範框架之義務，以及與歐盟會員國互助合作執行個資保護規範之履行等，與本文直接相關聯者，便是在DPA 2018附件13的第1條第i款特別提出，資訊委員須與EDPB尤其是關於LED之層次上相互合作。

關於Bridges案，英國資訊委員在第一審法院尚未宣判之前，即表達目前面部辨識之應用尤其是在關於執法目的之監控上，有違背比例原則與不必要介入之處。在該判決後，資訊委員便發布意見書，[54]表明在公共場域空間中執法單位應用面部識別技術時，應有

53　其前身即WP 29。

54　ICO, Information Commissioner's Opinion: The Use of Live Facial Recognition Technology by Law Enforcement in Public Places, October 31, 2019, *available at* https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-

元照出版提供 請勿公開散布

相關治理之指導。資訊委員更進一步表示雖然（一審）法院並不同意資訊委員部分見解，但資訊委員尊重判決並將注意上訴進度，並指出一審法院之判決並不能被視為是AFR應用在所有的情狀均應被准許的空白支票。[55]

相關之英國國內法規範除了資料保護法以外，另外也包括警察與犯罪證據法（Police and Criminal Evidence Act, PACE）以及監視攝影實踐準則（Surveillance Camera Code of Practice）。[56]在該意見中首先將本案關於面部辨識之應用認定為涉及個資保護之事件，此外執法機關為執法目的而處理該等面部辨識個資因為包含生物特徵資料，故係屬於DPA 2018第35(8)(b)條之特種處理行為。職是之故，必須注意的是此種敏感性個資處理行為包含**所有類型**之面部特徵辨識，且無論圖像是否與監視列表中的某個人配對，或者隨後在短時間內刪除未配對者的生物特徵資料，都是進行敏感個資之處理。

在個資保護核心原則方面，本案就合法與公平性原則來看，除了必須注意公平性以外，依照DPA 2018第35(1)與(2)條法律保留之規定，必須依照清楚、確定與可預見之法律，以及個資當事人之同意**或**履行法律義務之必要，而這個所謂之「必要」，在比例原則之操作上須符合嚴格之必要性，並且需有個資保護影響評估以及符合

opinion-20191031.pdf (last visited: 2020.11.13).

55 *Id.* at 5.

56 監視攝影實踐準則是於英國專門針對CCTV系統操作的守則，其法律授權來源是英國2012年自由保障法（Protection of Freedoms Act）第30(1)(a)條規範，而此下設有監視攝影委員辦公室（Surveillance Camera Commissioner）之機關。相關規範參Home Office, Surveillance Camera Code of Practice, June 2013, *available at* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf (last visited: 2020.11.15).

元照出版提供　請勿公開散布

DPA 2018第35(4)條或第35(5)(c)條之適當個資保護政策文件。[57]

詳言之，就獲得個資當事人之同意來看，至少須符合GDPR第4(11)條之定義與要件，諸如當事人自主、特定、經告知後知情、明確而透過聲明或明確之行動（意思表示）為之等。不過，不清楚自己為何被放入比對名單資料庫之個資當事人根本難以發動同意之行為，[58]故在實務上此等程序難以全面達成，也因此在對應機關履行法律任務所必要之相關規範來看，更為關鍵。另就適當個資保護政策文件言，DPA 2018第42條指出該等政策文件應至少包括說明處理如何符合相關的個資保護原則之內容以及解釋個資控管者有關留存時期和刪除個資的策略。

資訊委員並就在治理AFR時須考量之點，提出對以下不同層面之建議：[59]

㈠就個資保護為預先設計與內置（data protection by design and by default）：於歐盟LED以及英國DPA 2018中均有此原則之要求，資訊委員認為對於AFR來說更為重要，基於這個原則，在AFR之應用上應確保個資控管人僅出於特定且必要的目的處理個資，且必須從設計初始階段直到完成應用（刪除個資）為止全程均加以遵循。

㈡個資影響評估（DPIAs）：基於AFR之應用涉及敏感個資，因此該等技術之應用時，相關影響評估應注意在每次裝置AFR[60]之

57 ICO, *supra* note 54, at 7-8.

58 *Id.* at 10-11.

59 *Id.* at 13-20. 在此，除了本文轉引資訊委員之下列建議外，資訊委員也提出針對面部辨識演算法可能有歧視或偏見之問題，提出關於消除偏見（eliminating bias）之建議，惟基於本文僅就個資保護爭點論證，故不摘述。

60 雖然資訊委員相關意見中對於所謂應該對於每個AFR/LFR在裝置前應有DPIA（…is required in Data Protection Impact Assessments (DPIAs) that controllers

元照出版提供 請勿公開散布

前完成或予以更新，以便主管機關或個資控管者能夠證明其已經完整考量個人權利和自由在應用AFR時的風險，以及該等應用是否在科學技術上真的能夠有效達成原本預期之目標，例如對於偽陽性（false positive）、偽陰性（false negative）驗出與演算法偏誤等問題，是否能有效緩解。另外，對於AFR之影響評估必須明確、全面、持續至結束應用為止，且符合比例原則之檢驗，以解釋為何一定需要應用AFR已完成相關目的，以及為何排除了侵入性較小的選項。

㈢符合嚴格之必要性與比例原則檢驗：關於嚴格必要性之實際操作，資訊委員認為必須符合AFR之應用係基於特定標的或小範圍應用，以及應用時所欲達成之目的須採狹義解釋。例如應用AFR如係為警用目的，則需實際上有相關情報佐證嫌疑人將於特定地點與特定時間出現。

㈣有效性：基於前揭關於嚴格必要性之要求，因此資訊委員認為個資控管者必須能明確地解釋為何該等科技能有效助於達成特定執法目的。需注意者，這並不表示該等有效性之判準即僅為正確與錯誤比對之比率，或是實際上基於應用AFR而逮捕嫌疑人之數量，而必須是可表現促進公益，例如真正有效地減緩嚴重之犯罪，並使大眾能近用足夠之相關資訊。

㈤監控名單：同樣地基於前揭關於嚴格必要性之要求，資訊委員認為該等監控名單基於比例原則，不應包含非嚴重之犯罪嫌疑人，且監控名單之對象應依據對於預期的執法目的來說係合比例原則，而有合理之理據及符合一定之程序。再者，在監控名單之比對

must ensure are in place prior to each LFR deployment.）中所謂的每次裝置AFR/LFR具體意指爲何並未明確說明，但本文認爲因爲每個辨識比對監視器之裝置都是對於個資蒐集與處理的新增行爲，因此此處應指的是每次的個別面部辨識比對監視鏡頭以及整體AFR系統裝置前都應該要經過DPIA。

元照出版提供　請勿公開散布

影像僅應包含準確而可驗證的圖像，並在使用時由個資控管者或處理者合法持有；而在比對時，如不符合監控名單而被蒐集之圖像應儘速刪除，且不將監控與比對之圖像用於其他目的或未依程序任意串聯其他資料庫。最後，資料控管者與處理人須有足夠之個資保護教育與訓練。

㈥協尋失蹤人口：再次基於前揭關於嚴格必要性之要求，如果企圖以AFR尋查該等人口，則需該等人口達到能被考慮為易受傷害之人，或是有情報指出該特定之人將在特定時間於特定區域出現。

㈦最後，資訊委員也認為AFR管理機關之個資保護長（Data Protection Officer, DPO）應要能有效行使其職權，包括監控內部個資保護之實踐、告知機關個資保護相關義務、對DPIA提出建議，以及與資訊委員保持聯絡等。

基於以上各種考量，資訊委員認為其必須與相關機關合作，以期通過具有約束力的法定行為守則來強化法律框架。資訊委員認為，該等規範植基於在監視攝影實踐準則中建立的標準，並與DPA 2018並列，但該守則需明確地聚焦於執法使用AFR和其他現存或預計將可發展之生物識別技術上。而在上訴法院判決之後，資訊委員也表達欣見之意。

另方面就本案高等法院判決言，英國監視攝影委員（Surveillance Camera Commissioner）也特別注意到判決中可能存在關於面部識別算法固有偏差的問題。他認為如果警方不能證明使用該技術具公正和非歧視性，則警方不會也不應該使用該技術。[61]監視攝影委員

61 SCC, Surveillance Camera Commissioner's statement: Court of Appeal judgment (R) Bridges v South Wales Police—Automated Facial Recognition, August 11, 2020, *available at* https://www.gov.uk/government/speeches/surveillance-camera-commissioners-statement-court-of-appeal-judgment-r-bridges-v-south-wales-police-automated-facial-recognition (last visited: 2021.05.24).

元照出版提供 請勿公開散布

也據此修改相關指引，以確保警察意識到系統中的潛在偏見，並考慮如何與該技術的製造商合作以消除該等偏見。[62]

參、Bridges案的啟發：警用密錄器與規模化面部辨識系統

一、監視器之個資爭議：警用密錄器

在英國Bridges案中，其面部特徵辨識比對之錄影畫面資料來源除了街頭巷尾的錄影監視器以外，亦包括在警車上裝設或由警察人員隨身攜帶之的行動式錄影器材（警用密錄器），[63]以取得各種場所進出的每一個人的即時影像，再透過AFR技術，將監視錄影機所蒐集的面部影像（Face Image）與目標人物資料庫（Image Database）進行比對，一旦系統判斷臉部特徵吻合，將立即警示執法人員，讓執法人員判斷該人物是否為調查對象。

62 SCC, Facing the camera: Good practice and guidance for the police use of overt surveillance camera systems incorporating facial recognition technology to locate persons on a watchlist, November 2020, *available at* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf (last visited: 2021.05.24).

63 不過事實上，警用密錄器與街頭監視器在關於空間隱私概念上的干預狀態仍有其差異，前者的空間隱私問題在於人民難以瞭解監視器設置之確切處所以及如何運作；而後者則是動態地將許多原本的私密場合，在一定程度下轉換爲公共空間。Tjerk Timan & Nelly Oudshoorn, *Mobile Cameras as New Technologies of Article Surveillance? How Citizens Experience the Use of Mobile Cameras in Public Nightscapes*, 10 SURVEILLANCE & SOCIETY 167, 167-81 (2012), *cited from* Tjerk Timan, Bryce Clayton Newell & Bert-Jaap Koops, *Introduction: Conceptual Directions for Privacy in Public Space*, *in* PRIVACY IN PUBLIC SPACE: CONCEPTUAL AND REGULATORY CHALLENGES 1, 4-5 (Tjerk Timan, Bryce C. Newell & Bert-Jaap Koops eds., 2017).

元照出版提供　請勿公開散布

本文在此部分先就如果警用密錄器所錄存之畫面為面部辨識之個資保護爭議問題，帶出我國不僅在該面向之規範有對於個資保護不足之處，也點出雖然依照社會情狀容有不同權利間衡平個案不同之情狀，但是缺乏一個規範密度足夠的法律實體與程序規範，以及一個組織上的監督機關，或許對於科技治理之層面來說，有其害處。其後，則就整體公共空間之大規模面部辨識，提出個資保護相關爭點之析論。就本節而言，架構上將先點出警用密錄器相關特別法規之規範問題，其後在就個資法之相關問題，區分個資法適用與否以及相關規定之分析二個層次，分別提出論述。

㈠未有明確之特定法規

我國對於在**公共空間之監控、跟追與辨識特定個人**之問題，在大法官釋字第689號解釋[64]肯認個人即便在公共場域亦有不受侵擾自由與個資資料自主與自決之權利後，當然同時地表明通訊監察或檢（偵查）、警、調跟監或任何國家監控過程中蒐集、處理與利用公共場域之一般民眾活動與位置資訊的手段，屬於對於基本權利與自由之干預。然，國家監控如果僅是**純粹觀察或蒐集、處理特定或不特定之人之活動與位置**，並不在通訊保障及監察法第5條至第6條之射程範圍，也因為可能並無物理性侵入行為而不適用刑事訴訟法關於搜索之相關規範。又，無調取通訊資料與內容之作為也並未被規範在通保法第11條之1；而近來熱烈討論的GPS偵查與個資或隱私保護爭議問題，雖亦為國家監控須受法律保留之拘束，使得學者

64 需注意者，英國Bridges案與我國之警用密錄器在性質上乃係公部門於公共空間對不特定之人進行監聽、監視與辨識，與釋字第689號解釋之情境爲新聞記者的跟追、監視、監聽情境不同，然均有在公共空間對不特定之人進行監聽、監視與辨識之同質性，而本文在此所主要要處理之爭點，即爲在**公共空間蒐集不特定人面部特徵而予以辨識**之問題。

元照出版提供 請勿公開散布

多倡議需有明確規範，[65]但仍未見我國法規範對此有明確處理，僅見於實務判決如最高法院106年度臺上字第3788號刑事判決，並進而引起修法之芻議討論。不惟如此，對於單純蒐集、處理或利用不特定之人個資的監視攝影機相關監督機制來說，學者指出即便是在道路交通管理處罰條例、警察職權行使法以及部分地方政府之自治法規（如臺北市錄影監視系統設置管理自治條例）交錯的當下，仍有「未必建構有完整的個資保護規範架構，而恐導致個資保護之疏漏」之虞。[66]

就隨身攜帶之的行動式錄影器材（密錄器）之監控與資料保存問題來看，實務上警政署頒有「警察機關執勤使用微型攝影機及影音資料保存管理要點」以及「警察機關警用車輛使用行車紀錄器及影音資料保存管理要點」，目的係為規範警用車輛使用行車紀錄器及影音資料之保存管理，以維護員警執勤安全及保障人民權益。依據警政署相關新聞稿，員警執勤使用密錄器，是為**保障民眾權益及員警執勤安全**，避免事後**舉證**困難而無法還原真相，[67]而其使用時機以及檔案之保管、調閱、複製，均依內政部警政署前述管理要點

65 薛智仁，GPS跟監、隱私權與刑事法——評最高法院106年度台上字第3788號刑事判決，裁判時報，70期，頁42-60，2018年4月；范耕維，現行法下GPS追蹤定位偵查行爲之合法性與立法方向——比較法觀點與最高法院106年度臺上字第3788號判決之考察，政大法學評論，157期，頁109-197，2019年6月；蔡聖偉，再論私裝GPS跟監與「竊錄非公開活動」——評最高法院106年度台上字第3788號刑事判決，裁判時報，76期，頁27-40，2018年10月；溫祖德，從Jones案論使用GPS定位追蹤器之合憲性——兼評馬賽克理論，東吳法律學報，30卷1期，頁121-167，2018年7月。

66 李寧修，同註20，頁408-409。

67 警政署，108年4月16日報載「你知道嗎、警察正對你錄影　有侵犯隱私的疑慮」？　真相報你知，2019年4月16日，https://www.npa.gov.tw/NPAGip/wSite/fp?xItem=91653&ctNode=11436&mp=1，最後瀏覽日：2019年11月20日。

元照出版提供　請勿公開散布

為之。此二類型之攝影器材非但員警會自行購置，警方亦曾以公務預算購置配給員警供執勤使用，並且經常地於法庭訴訟上作為證據使用。雖然，無論影音資料之建檔、保存流程及期限，在該等要點中均指定專人處理，且資料保存與銷毀均有明確規範；申請調閱或複製，均須提出書面申請，由分局長或相關職務以上長官或其授權人核准後始得辦理，並不得擅自複製或洩漏；員警執行公務與民眾接觸前或依個案研判有開啟必要時，便應開啟並完整連續攝錄處理事件經過，看起來在相當程度上尚稱「管理嚴格」。然而，該等可能干預人民基本權重大之作為，僅係以行政程序法第159條第1項依機關權限或職權為規範機關內部秩序及運作所為，非直接對外發生法規範效力之一般、抽象之規定，更何況在實務的運作上違反此要點僅有行政懲處之效果，而可能發生損害結果與責任間之不符比例情事。

㈡個資法上的問題：適用與否

對於警察實務上密錄器**所蒐集而得個資**之應用[68]類型與策略，論者有將其區分為四類者：[69]

1. 監視性應用

應用重點在於對人、事與地等之詳細觀察。在此，與街頭監視

---

68 至於密錄器在技術上可結合之相關應用，如結合CCTV等，參Marc J. Blitz, *Local Law Enforcement Video Surveillance: Rules, Technology, and Legal Implications*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 263, 283-85 (David Gray & Stephen E. Henderson eds., 2017).

69 Ben Bowling & Shruti Iyer, *Automated Policing: The Case of Body-Worn Video*, 15 INTERNATIONAL JOURNAL OF LAW IN CONTEXT 140, 143 (2019). *Also see* Metropolitan Police, Body Worn Video (BWV) Policy Statement, September 27, 2016, *available at* https://www.met.police.uk/SysSiteAssets/foi-media/metropolitan-police/policies/bwv_policy_statement_february2017.pdf (last visited: 2020.03.14).

元照出版提供 請勿公開散布

器相較，最大之問題在於密錄器伴隨著警察之移動範圍與勤務期間，有可能比傳統之監視手段具有更嚴重的空間侵入性，使得原有之私密空間可能被動地遭到轉換為公共空間，而造成一定程度的空間隱私權利退縮。再者，例如在英國實務上警方密錄器之影像可以自動即時上傳至警方資料庫，並在留存影像達三十日後刪除，則此部分有可能留存無辜第三人之影像，並成為比對辨識之樣本。

2. 調查性應用

將密錄器應用在對於犯罪事件與人物相關記錄、觀察資料與物理跡證之**資訊蒐集與分析**。此部分影像除供蒐集與分析物證以外，在實務上已可在廣度上結合面部辨識，[70]甚至更進一步地在深度上結合人工智慧[71]用來預測犯罪熱點與嫌犯足跡，只是實際之應用範圍仍有侷限罷了。

3. 證明性應用

側重於檢查與評估證據之用。須注意者，由於該等影像作為證據之用時，雖然俗語「畫面會說話」，但是事實上所謂畫面說出來的話都是經過結合其他跡證之「轉譯」，仍有可能基於錯譯而發生誤導；而過度地依賴該等畫面，也可能排擠或排除了其他證據之適用。

4. 規範性應用

將密錄器應用在管制警方勤務，使其更加透明化、合法化以及具有責任性，而同時也因為員警與民眾因為知悉警用密錄器之存

70 結合面部辨識爲本文下節討論重點。*Also* Bowling & Iyer, *id.* at 146-47.

71 結合人工智慧部分，亦爲後文討論對象。Pasternack Alex, Taser Acquires a Computer Vision Startup to Bring AI to Police Body Cameras, FastCompany, September 2, 2017, *available at* https://www.fastcompany.com/4030358/taser-acquires-computer-vision-startup-dextro-to-bring-ai-to-police-body-cameras (last visited: 2020.03.14), *cited from* Bowling & Iyer, *id.* at 147.

元照出版提供　請勿公開散布

在，而可能改變了彼此互動之行為。

另方面，如果就如何應用密錄器所得個資之處理程序來看，在政策上可以區分為關於其近用與儲存之面向、開啟密錄器紀錄裁量權之面向、在警方作成相關聲明或相關報告前之近用，以及公眾對之近用等不同層次問題。[72]然就整體資料治理之層面上，觀諸現有之前述「警察機關執勤使用微型攝影機及影音資料保存管理要點」以及「警察機關警用車輛使用行車紀錄器及影音資料保存管理要點」，僅有關於機關、警察人員甚至新聞媒體之調閱或提供程序，並無受錄影之個資當事人或第三人之申請程序規範。員警隨身密錄器或警用車輛行車紀錄器透過鏡頭所蒐集者，當然可能直接或間接識別特定當事人，依學者見解雖其係在公共場域所為，但因其攝、錄之目的係為將來識別特定人，故應不認合於個資法第51條第1項第2款所謂於公開場所或公開活動中所蒐集、處理或利用之未與其他個資結合之影音資料而不適用個資法之情況；[73]尤其在員警依警察職權行使法第6條至第16條查證當事人後，更已無個資法前述該例外條款之適用餘地，而**仍應為個資法適用範圍**。

㈢警用密錄器在個資保護與資訊透明之衡平

無論是就警用密錄器前揭何種區分之類型來看，都可能會發生關於個資保護以及資訊透明公開的競合問題。此爭點雖相當程度地反映在我國「警察機關警用車輛使用行車紀錄器及影音資料保存管

72 Blitz, *supra* note 68, at 286-89.

73 劉定基，個人資料保護法講座：第一講個人資料的定義、保護原則與個人資料保護法適用的例外——以監視錄影爲例（上），月旦法學教室，115期，頁42-54，2012年5月；劉定基，個人資料保護法講座：第一講個人資料的定義、保護原則與個人資料保護法適用的例外——以監視錄影爲例（下），月旦法學教室，119期，頁39-54，2012年9月。

元照出版提供 請勿公開散布

理要點」第6條第1項前段之「影音資料之調閱、複製，應恪遵警察職權行使法、個人資料保護法等相關規定」，然似乎未顧及政府資訊公開法付之闕如，遑論不同權利衝突時競合之問題。

其中，關於該等個資當事人之個資是否能由個資當事人依照個資法第10條「就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本」，或依照政府資訊公開法第9條申請資訊公開，而無同法第18條之限制，不無疑問。細言之，根據個資法第10條之規範，「公務機關或非公務機關應依當事人之請求，就其蒐集之個資，答覆查詢、提供閱覽或製給複製本」，則個資當事人應認有權查閱含有其個人影像的隨身攝錄機錄影紀錄。此時，基於警方可能需先行把錄影紀錄中不相關的影像遮蓋以維護其他人之隱私、個資上權利，甚至是第10條但書所稱妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益；妨害公務機關執行法定職務；或妨害該蒐集機關或第三人之重大利益之情狀下，[74]需遮蔽或不提供，則此時警方似仍有操作上之模糊空間。大多數的情況下之所以警用隨身或車用行車紀錄器會使輿論關心之重大原因在於該等無差別側錄之主要實務上用途與目的均在於過度地側重在對警方之「自保」而成為訴訟證據；[75]但相對地，有利於當事人之畫面，往往在調閱上出現如困難。甚至，是否員警應於執勤時強制配戴且始末錄影，在實務運作上也有爭議：如僅依前述相關要點，似可解為微型攝影機無強制性要求員警執勤須配戴，僅鼓勵員警自行主動攜帶錄影（音）設備，因此不得以員警未攜帶或未錄影而予以懲處；但在監察院之糾

74 解釋上此等但書之例外情狀係限制當事人權利，故須採嚴格之限縮解釋。例如，妨害公務機關執行法定職務，解釋上須對公務機關執行職務有重大影響，非不提供無法達成該個案職務之達成等，方為但書條件之滿足。

75 警用微型攝影機之影音資料作為證據者，如臺中地方法院108年度交字第121號交通裁決。

元照出版提供　請勿公開散布

正案文中，卻清楚載明依據警政署回覆監察院函詢等，稱依「員警執勤之應勤裝備攜行原則」與「警察機關執勤使用微型攝影機及影音資料保存管理要點」之精神，員警在執勤時**必須要**攜帶微型攝影機（密錄器）並適時開啟。[76]相反地，於刑事案件中也經常可見員警[77]稱其查緝為避免犯嫌發覺，均著便衣及駕駛偵防車執行勤務，又因配發之微型攝影機印有明顯之警察徽章，且機型過大，配戴身上使用易遭查緝對象識破，故執行埋伏逮捕通緝犯勤務時，**均未配戴**使用微型攝影機，故礙難提供查緝過程錄影畫面供參。甚至，有「考量當時查緝對象狀況不明，故先行埋伏伺機而動，如配戴微型攝影機值勤將暴露警察身分而驚動查緝對象，恐錯失緝捕先機，故未配戴」等辯駁，而法院均為接受採納之情狀。[78]由此可見該等對內生效之行政規則，在實際操作上仍具有模糊性。

需注意者，該等競合之衡平考量往往依照當地不同社會情狀，而有所偏好。究其原因，乃是人民不滿警方在利用該等個資時的單向性利益：僅於警方有利時提供使用。[79]然而，打擊與防止「犯

---

76 監察院，糾正案文107內調0042號，陳慶財委員、李月德委員、章仁香委員、楊美鈴委員調查，新竹縣政府警察局竹北分局鳳岡派出所員警於106年8月31日查緝竊盜案時，近距離朝涉案之越南籍逃逸外勞連開9槍，致該外勞傷重斃命，警方涉有執法過當等情乙案之調查報告，2019年5月29日。

77 例如：臺灣新北地方法院107年度訴字第1240號刑事判決。

78 臺灣新北地方法院107年度訴字第1240號刑事判決。

79 例如在美國部分的州，因爲顧及公眾信任與促進透明與責信原則，較傾向於將該等影音資料向大眾揭露，並將揭露之限制予以緊縮，但卻可能因此造成隱私風險之升高。另一方面，同樣地在美國某些州，則將公眾對該等影音個資之近用予以限縮，例如德州僅准許以之作爲刑事追訴之證據，同時也禁止警察部門要求執勤員警執勤時連續錄影；奧勒岡州則要求警方僅在具有公共利益的條件下得揭露，且揭露時必須對個人予以去識別化。亦有部分的州在衡平時採較折衷之過濾式揭露（filtered disclosure）方法，就該等影音個資之利用、攜帶密錄器所得進入之處所、所得錄影之情狀等，分別予以過濾。*See*

元照出版提供 請勿公開散布

罪」及「恐怖主義」的興起與其對社會秩序破壞，一直都是國家強制力施作之重要公共利益憑藉，而以防微杜漸之心態將國家干預人民權利之權限提前擴張，亦即警調干預人民基本權利之基準，從懲罰犯罪、危害防止之角度前展至為風險預防之觀點。[80]警用之隨身密錄器在應用上除了辨識個人身分以外，如串連資料而為資料導向之警用，甚至可以預測犯罪發生而生先發制人之效果。[81]然而，在**無明確特定之證據**能突出何種權利居於較優勢被保障地位之際，倘損害某一權利所帶來之結果將劣於另一權利，將發生嚴重或無法回復之損害發生之虞的話，則以預防原則（precautionary principle）[82]

MARY D. FAN, CAMERA POWER: PROOF, POLICING, PRIVACY, AND AUDIOVISUAL BIG DATA 164-67 (2019).

80 Malcolm M. Feeley & Jonathan Simon, *Actuarial Justice: The Emerging New Criminal Law*, *in* THE FUTURES OF CRIMINOLOGY 173, 185 (David Nelken ed., 1994). 另參李寧修，同註20，頁394-395；李震山，公權力運用定位科技措施與基本權利保障，載：人性尊嚴與人權保障，頁299，2011年10月，4版；林明鏘，由防止危害到危險預防：由德國警察任務與權限之嬗變檢討我國之警察法制，國立臺灣大學法學論叢，39卷4期，頁174-175，2010年12月。

81 Mark Andrejevic, *Data Collection Without Limits: Automated Policing and the Politics of Framelessness*, *in* BIG DATA, CRIME AND SOCIAL CONTROL 93, 95 (Aleš Završnik ed., 2018).

82 所謂「預防原則」，學者程明修認爲係一先於危險發生前的保護思考，其特徵在於雖然想像中存在有發生危險的可能性，卻因受限於現有的科學知識，而無法完整地預設未知事物發生的蓋然性。在此，因爲在科學證據尚無法完整確知究竟該等安全問題之發生可能性，也無法確知如果採危險防護的強制性強烈法律效果究竟對於個人權利侵害之程度是否爲容忍之必要的時候，依據Beyleveld及Brownsword教授之見解，如果無法由任何方法得知X是否含有P特質，錯誤地預設X沒有P特質所產生之結果將會比錯誤地預設X有P特質所產生之結果更壞時，則在可能之範圍內，應當將X假定爲具有P特質；相反地，如果將X與P交換來看，也會是如此。程明修，行政法上之預防原則（Vorsorgeprinzip）食品安全風險管理手段之擴張，月旦法學雜誌，167期，頁127-136，2009年4月。DERYCK BEYLEVELD & ROGER BROWNSWORD, HUMAN

元照出版提供　請勿公開散布

之角度思考應當儘量地予以避免。也正因如此，該等限制人民基本權利與自由之國家干預行為，必須通過嚴格的權利衡平檢視，尤其是比例原則之操作。因此在國際上，民主國家莫不對於以國家力量監控不特定大眾之作為，予以適當並符合預防原則與比例原則之衡平監督機制。[83]而純然地以科技管理之方式進行犯罪之預防，也可能使法律規範追求之目標與科技管理本身發生脫節。換言之，科技管理之方式作為預防犯罪之手段，雖然在比較法上可以參考國際相關規範與實踐，但仍必須與整體社會之道德觀相符合，[84]而這也正是前所提及所謂依照當地不同情狀偏好而調整衡平之理據所在。

而本節所評論核心之監視設備，包括密錄器係單純紀錄與留存影像之犯罪偵查（crime detection）手段，即係面對無明確特定證據之風險預防（precaution）。然而，此等警用隨身之密錄器隨著科技之進展，次世代的警用密錄器搭載即時連線之面部辨識之應用功能，或許即將普及。[85]那麼，接下來的問題便在於即時面部辨識與個資保護之關聯，究竟為何。

DIGNITY IN BIOETHICS AND BIOLAW 85 (2001).

83 例如在英國爲此甚至有獨立之攝影監視委員（Surveillance Camera Commissioner, SCC），並與資訊委員一同作爲本文前述R (bridges) v CCSWP and SSHD案之訴訟參加人。SCC並基於職權發布監控規則指引（Guide to the Regulation of Surveillance）。Surveillance Camera Commissioner, Guide to the Regulation of Surveillance, February 27, 2019, *available at* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786444/Guide_to_the_Regulation_of_Surveillance.pdf (last visited: 2020.11.30).

84 BEYLEVELD & BROWNSWORD, *supra* note 82, at 216.

85 ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT 89-90 (2017). Bowling & Iyer, *supra* note 69, at 145.

元照出版提供 請勿公開散布

二、科技時代下公共空間與隱私的合理期待：大規模面部辨識

前已說明AFR係為即時且針對性地對於**監控名單**（watchlist）上之人進行犯罪防止（crime prevention）之手段，此時包括比例原則以及透明原則等個資保護與對人權限制的衡平原則，較側重之處則在該等名單需有一定程度之證據，證明該等特定對象之高度犯罪可能，而導致標的對象被列入監控名單以工作比對。在Bridges案確定判決中，法院對第一個聲明雖然認定SWP之作為符合個資法與錄影監控行為準則，但卻也認定SWP對**誰**將會被納入對比名單，以及將會在**何處**實施AFR並**未有明確之指引**規範。而這個爭點討論之核心即在於在公共空間或是公眾得出入之場所究竟是否仍有隱私之期待，以及如果有隱私之期待，如何評量其強度。

在Bridges案第一聲明中，判決引述Laws法官在R (Wood) v Metropolitan Police Commissioner案之意見，指出「對於干預基本權利越強烈之措施，便需要有更明確與特定之法律規範以正當化該等干預」。[86]而判決隨後分析面部辨識應用干預基本權利在比例原則上之考量基礎，並將重點放在對於監控名單中的「誰」（Who）在「何處」（Where）被列入監控名單之明確與透明性需要達到具體精細規範之程度。[87]從邏輯上來看，既然法院高度地要求規範須具明確與特定程度，則必須溯及地先探究到底面部辨識在對於基本權利的干預程度上有多劇烈。

細言之，無論是個資保護之權利乃至私生活之權利，均非為絕

86 Court of Appeal judgment in R (Bridges) v Chief Constable of South Wales Police & Others, [2020] EWCA Civ 1058, para. 82; R (Wood) v Metropolitan Police Commissioner [2009] EWCA Civ 414, [2009] 4 All ER 951, para. 53.

87 Court of Appeal judgment in R (Bridges) v Chief Constable of South Wales Police & Others, [2020] EWCA Civ 1058, para. 91.

元照出版提供　請勿公開散布

對權之態樣，因此在有相對的公共利益時，例如對於犯罪偵查與防免，甚至國家安全之維護需求時，均可能有一定程度之干預。然，基於此等對基本權利與自由之潛在強烈干預，則相對地必須把干預的界線加以特定而明確地釐清。英國上訴法院即基於此考量，認為該等以AFR為干預之方式，必須在「人」與「處所」，也就是「誰會被放在監控名單上」，以及「如何決定將在何處施行AFR」這兩個原本模糊不清的操作上加以釐清。至於在順序上，如果能先釐清「誰」的問題，則對於施行AFR的「處所」問題便能給予明確之準則，因此對於「誰」會被放在監控名單上之明確與特定，將是先決之問題。[88]不過事實上也有不同之論點，認為空間處所在預測犯罪風險時，較預測特定「個人」之行為為重要者。例如以近年熱門的資料導向的預測性警察活動（predictive policing）理論[89]來看，對於犯罪熱點的資料應用預測，使得警察活動針對相對較小區域能夠準確的預測，並且在合理的時間內確保警方部署，並衍生出近乎重複理論（Near Repeat Theory）與風險區域理論（the Risk Terrain Theory）等不同的發展。[90]然而，基於在公共空間上往來之人係為不特定，如果以環境監控作為主軸，則非常容易造成毫無框架限制的人別監控，[91]且個資之權利保護又以對於「個人」之識別為主要

88 *Id*. para. 96.

89 所謂預測性警察活動係指預測將來的犯罪會發生在何人、何時與何地，進入現今的資料應用時代，多藉該等資料科技為之。詳細的評論，參王正嘉，預測性警察活動在犯罪偵防運用與問題，刑事政策與犯罪防治研究專刊，25期，頁5，2020年8月。

90 所謂近乎重複理論指的是如某地點發生犯罪後，從資料上來看可以發現短時間內鄰近的區域可能出現類似犯罪。而風險區域理論則將不同的犯罪因素相關的資料標誌在地圖上，成為犯罪風險地形圖，此時在越多犯罪因素加乘的區域，便越有可能再次發生犯罪而成為熱點。參王正嘉，同前註，頁23-27。

91 Andrejevic, *supra* note 81, at 100-01.

元照出版提供 請勿公開散布

判斷，因此本文認為採前說為妥。

然而就關於比例原則之操作而言，基於隱私權在內涵上之複雜而模糊特性，因此學者認為如有涉及隱私權之競合問題，不可一概而論地立即進入以權利為基礎操作比例原則公式的衡平審查，而必須依個案之脈絡，對涉及隱私進行動態之空間辯證。[92]故而，在判斷何人得列入AFR之監控名單以及為了監控人而決定在何處實施AFR時，究應如何操作此處所謂的嚴格必要性的比例原則，便應當回歸大規模進行面部辨識監控之在事實上的本質脈絡處理。

就事實言，必須先認知的是面部辨識本身雖然不再算是非常新穎的技術，不過時至今日其科學技術之應用已然發生了在量與質上的變化。在量的部分，面部辨識在現今的應用上可以分為實體的線下部分以及虛擬網路的線上部分，而無論是線上或是線下，其流程都是先根據所需將包含面部生物特徵的個人照（影）片予以數位化（digitised）後，形成依照監控名單集成之資料庫，然後透過監視攝影機或軟體程式等畫面擷取工具，完全自動化或以人工介入之方式比對是否有符合資料庫數位化照片特徵。其中在線下的實體部分，主要透過監視攝錄影機器擷取畫面以供比對，而基於現代相關硬體成本的明顯降低，鏡頭廣布的社會景象已經幾乎不足為奇。在虛擬世界的線上部分，由於社群媒體與智慧型通訊器材（手機等）興起，因此現今流行的社群媒體大多已包含畫面與影片，甚至以其為青少年世代主流（如Instagram、TikTok等），而其上含有面部之照片早已可透過軟體大量蒐集與分析。另外在質的部分，除了對辨識的正確性大幅提升以外，自動化比對的精準度與速度都大幅度地提升，並且可以交錯比對線上與線下所擷取畫面，再透過其他技術

92 葉俊榮，探尋隱私權的空間意涵：大法官對基本權利的脈絡論證，中研院法學期刊，18期，頁26-34，2016年3月。

元照出版提供　請勿公開散布

之連結，而有其他諸如即時定位、軌跡追蹤、作息定序、人際（社群）網路關係剖析、個人人格剖析、親族與疾病、生理狀態分析，甚至預測位置與各類型活動等潛在的延伸功能，使得目前的面部辨識科技成為一個與之前已知原有技術截然不同的「新穎科技」（novel technology）[93]。

而大規模的面部辨識監控也因為這些新穎的科技功能而發生對於個人私生活權利的全面性干預。在關於大規模生物特徵辨識監控之目的層次問題上，論者指出目的有二：第一，使得人民之身分更加地透明；第二，可以對人民進行類型化與評估。[94]也正因為該等目的之達至，加上現今新穎科技應用上成本降低而大量布建的高密度面部辨識監視器，便發生強制凝視（compulsory visibility）的效果，[95]使得不但物理上具有邊沁所指圓形監獄（panopticon）的監控效應，更可能基於其線上與線下複合實體與虛擬空間，造成之實踐使不特定大眾感受無所不在的（被）凝視效果，而出現傅科所指無形凝視的全景式[96]監獄規訓結果。[97]

---

93 Court of Appeal judgment in R (Bridges) v Chief Constable of South Wales Police & Others, [2020] EWCA Civ 1058, para. 86.

94 Margaret Hu, *Biometric Surveillance and Big Data Governance*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 121, 132-33 (David Gray & Stephen E. Henderson eds., 2017).

95 IAN BERLE, FACE RECOGNITION TECHNOLOGY: COMPULSORY VISIBILITY AND ITS IMPACT ON PRIVACY AND THE CONFIDENTIALITY OF PERSONAL IDENTIFIABLE IMAGES 75-85 (2020).

96 所謂Panopticon係爲英國法哲邊沁所提出，通常翻譯爲全景式監獄或圓形監獄。該監獄之建築由一個圓形大廳作爲主體，其中間設有孔洞之檢查室，而使一個警衛就可以監視該監獄的所有囚犯，且囚犯將不知道自己是否受到監視。基於該單一警衛不可能在同一時刻觀察所有囚犯的牢房，但囚犯卻因爲不知何時會受到監視與檢查，因此其只有假設自己無時無刻不被監視，而被有效地強迫自己規範自己的行爲。法國哲學家傅柯據此認爲，因爲永遠有人

元照出版提供 請勿公開散布

據此，如大規模地以面部辨識為科技治理，則對於「每個人」來說，帶來了無論何時何地，特別是在公共之場域時，都會在無感知的情形下遭到類似搜索，或甚至比被搜索更一覽無遺之全觀透視效果。[98]然而，公共場域是否個人即完全無隱私之期待，並非無疑。

㈠在科技新穎化時代下，於公共空間中的個人仍應有隱私之期待

隱私權乃係一逐漸開展之權利，[99]因而在個人的私密空間之中的獨處權利，亦即個人得獨立於群體之外而不受任何人的監視成為最早之隱私開展點。[100]然而隨著科技之「新穎化」，雖然某種科技已然在生活中應用一段時日，但是因為科技之發展，該項科技得以結合其他科技為「質」之變化，或因為成本之降低而可以大量應用為「量」之變化，使得原本之科技期應用之效能影響之程度超過原有之預測，所伴隨的科技與法律風險也隨時發生質與量之變化，而在釋字第603號解釋林子儀大法官之協同意見書也指出：

……蓋隨電腦處理資訊技術的發達，過去所無法處理之零

「凝視」著該囚犯，因爲永遠被人看著，所以能夠使人保持紀律，而永遠順服。MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 187 (1977).

97 Maria Brincker, *Privacy in Public and the Contextual Conditions of Agency*, *in* PRIVACY IN PUBLIC SPACE: CONCEPTUAL AND REGULATORY CHALLENGES 64, 76-78 (Tjerk Timan, Bryce C. Newell & Bert-Jaap Koops eds., 2017).

98 BERLE, *supra* note 95, at 122.

99 關於隱私權，尤其是資訊隱私權隨著時間而逐漸擴大開展其內涵與範圍之敘述，可參 DANIEL J. SOLOVE, MARC ROTENBERG & PAUL M. SCHWARZ, INFORMATION PRIVACY LAW 2 (2d ed. 2006).

100 Samuel D. Warren & Louis D. Brandies, *The Right to Privacy*, 4 HARV. L. REV. 193, 193-220 (1890).

元照出版提供　請勿公開散布

碎、片段、無意義的個人資料，在現今即能快速地彼此串連、比對歸檔與系統化。當大量關乎個人但看似中性無害的資訊累積在一起時，個人長期的行動軌跡便呼之欲出。誰掌握了這些技術與資訊，便掌握了監看他人的權力。故為因應國家和私人握有建立並解讀個人資訊檔案的能力，避免人時時處於透明與被監視的隱憂之中，隱私權保障的範圍也應該隨之擴張到非私密或非敏感性質的個人資料保護。……

相對地，如果將隱私之概念過度之限縮拘泥，則或許會認為在公開的場域，有監視其實是不妨害隱私的：因為同意進入該公開場合即視為已經自願將部分隱私權放棄，且在公開場合除非意圖犯罪，否則無不可告人之事。事實上，對公共空間隱私予以限縮之解釋方式仍見諸於立法設計之中。例如，法務部科技偵查法草案[101]即於第2條第3款將隱私空間，將具有「隱私或秘密之合理期待者」以外之空間定義為「非隱私空間」，並在立法說明中表明：

……無圍牆之庭院及房屋附連圍繞之土地，平視即可合法觀看之，均不具有隱私或秘密之合理期待；公共空間或公眾得出入之場所，例如百貨公司、公共汽車等均無隱私或秘密之合理期待，均屬「非隱私空間」。

但如若法制上或實務上允許大規模地在實體物理空間之公共場所進行面部特徵辨識，則可能因為全景式強制凝視之結果使得被凝視者無法「協商」社會關係之公共與私密空間界線，[102]更大幅地降低了對於該等公共場域中個人仍可能保有隱私的合理期待程度，甚至誤認為在開放的公共空間中，即完全毫無隱私保障之存在可

101 法務部法檢字第10904527940號函參照。
102 葉俊榮，同註92，頁22。

元照出版提供 請勿公開散布
能。並且，在公共場域中在我國應認為仍有一定程度之合理期待，已獲大法官釋字第689號肯認：

> **……是個人縱於公共場域中，亦應享有依社會通念得不受他人持續注視、監看、監聽、接近等侵擾之私人活動領域及個人資料自主，而受法律所保護。惟在公共場域中個人所得主張不受此等侵擾之自由，以得合理期待於他人者為限，亦即不僅其不受侵擾之期待已表現於外，且該期待須依社會通念認為合理者。**

而這個類似的見解其實也曾出現在歐洲人權法院的Antović and Mirković v. Montenegro案中，[103]法院依照其向來之見解[104]認為對於私生活之權利應採取較寬廣之解釋而將其範圍擴大，也因此即便該案系爭事實是在大學的開放劇場空間為了安全目的架設攝影機，但是因為同時拍攝到教師之上課畫面並包含教師與學生與互動，從而法院認為影響該教師關於發展相互關係並建立其社會身分之私生活態樣。[105]即便是在工作場所當中，歐洲人權法院也在Bărbulescu v. Romania案認定工作場所之錄影監視畫面屬於私生活權利之範圍，即使雇主對員工在工作場所的私人社交生活之內部工作守則具限制性，也不能將其減縮至零，而必須在該等公共場合或工作處所

103 Antović and Mirković v. Montenegro (application no. 70838/13, 28 November 2017), ECHR.

104 *E.g.*, Niemietz v. Germany (16 December 1992, §§ 29-31, Series A no. 251-B); Peck v. the United Kingdom (no. 44647/98, §§ 57-58, ECHR 2003-I); Halford v. the United Kingdom (25 June 1997, §§ 44-46, Reports of Judgments and Decisions 1997-III); Fernández Martínez v. Spain [GC] (no. 56030/07, §§ 109-110, ECHR 2014 (extracts)); and Bărbulescu v. Romania [GC] (no. 61496/08, §§ 70-73, 5 September 2017).

105 Antović and Mirković v. Montenegro, paras. 44-45.

元照出版提供　請勿公開散布

使得當事人有一定之合理隱私期待。[106]而這種空間上對隱私的合理期待程度，在虛擬網路空間中也因為同畫面中經常包含不同個資當事人之接觸、線上與線下不同面部資料庫之串連，造成對潛在的社交關係關聯性剖析，甚至無法避免地形成對於個資之蒐集目的外之氾濫使用。

然而，在新穎科技大量應用的情境之下，似乎個人在公共空間有越來越難以期待隱私之趨勢。以辨識之精準程度而言，現今面部辨識科技此等利用生物特徵之不易變換，獨一無二特性已然足以應用於生物特徵為導向之執法監控，而得以在實體與虛擬空間幾乎毫無遺漏地監控在公共場域出現的每一個行動者。並且，在現今的新穎科技應用之下，也應認為有足夠之知識普及使得社會中的成員都**認知**到在公共空間有極大之機率受科技之清楚辨識的**社會通念**，也因此，似乎應該認為在開放之虛、實空間監控科技匯流之現實中，認定公共空間的隱私權期待應萎縮至極低，甚至歸零。另方面，不對稱的科技監控之打擊犯罪目的不僅在於公共空間的人身安全之維護，而是包含許多層面之犯罪防止與制裁，例如在金融與稅捐領域之監控與抓漏行為，便可能查察以往隱晦的白領精英金融犯罪。[107]從這點來看，公共空間之隱私權內涵或許可以被認為已經被現今的社會通念更加地淡化了。

但即便如此，本文認為從隱私權內涵之視角來看，仍應採取較為舒展擴大的隱私概念，使個人即便身處公共場合或是在公共場合中所做的舉動，其身分仍有得不被辨識出來或是受到監視之權利，而因此可以獲得行動自由以及對私生活權利之控制。這是因為雖然

106 Bărbulescu v. Romania, para. 80.

107 Frank Pasquale, *Paradoxes of Privacy in an Era of Asymmetrical Social Control*, *in* BIG DATA, CRIME AND SOCIAL CONTROL 31, 47-51 (Aleš Završnik ed., 2018).

元照出版提供 請勿公開散布
在個人已知受監控之情況下或許並未直接阻止個人出現在某個場合或是作出某種行止，但是受到辨識的個人卻會因為社會壓力或是其他原因而不敢或是不願出現在特定場合或是為特定的舉動。學者甚至進一步地認為「公共空間與私密空間的界線便是在不同人或群體之間，透過暗示或明示的互動與協調而逐漸建構」，並且「對於界限的侵入或者協調過程的強制，便是對於互動規則的違犯」。[108]

至此，在特定情況下對於實體與虛擬公共空間隱私合理期待之降低甚至歸零之見解，明顯地有非常高的機會是因為該等情況不夠「特定而明確」，導致建構已久的公共空間合理隱私期待制度與論理空虛化，更形成對空間隱私過於劇烈之縮減甚至滌除。基於此，本文認為由於面部辨識技術之新穎性應用與傳統未有面部辨識功能之監視器在應用上之法律規範強度應有不同之處理，如若監視之識別方式具有新穎性的面部辨識功能而在公共空間裝置，則需要預先有更明確之裝設與蒐集面部特徵與比對理由，以及更完備的DPIAs。也因此，為檢視基於適法之機關[109]為預防、調查、偵查與追訴刑事犯罪或執行包括為維護及預防對公共安全形成威脅之刑罰目的，而執行法律之所需的干預行為是否符合比例原則，焦點便在於將「人」放在監控名單之判準，必須依據干預之行為而符合不同層級強度之保護要求。

㈡大規模面部辨識與公共場域的合理隱私期待：程序與組織保障

本文認為為保障資訊隱私之權利，以符合當代科技之方式治理本為大法官期待之誡命，然治理之核心所應關懷者，毋寧在必須於法律制度上、程序上以及組織上的三維面向，謹守分寸。既然除了

108 葉俊榮，同註92，頁22。

109 依據DPA 2018第30(2)條，情報機關（intelligence service）並非在此所指的適法機關，而適法機關則被詳細地規範在DPA 2018的附件7。

元照出版提供　請勿公開散布

法律制度保障以外，在以科技治理上所謂的「合理」隱私期待如考量Bridges案之經驗，也需要具備程序上與組織上之保障，那麼本文即必須接著分析的是在比較法觀察上有如此要件的情況下，則臺灣本土的科技治理是否也應如此地要求？

本文認為如果仔細地分析釋字第603號解釋，則應當作出至少與Bridges案同等強度之解釋。在我國該指紋釋憲案的解釋理由書中，可以歸納出大法官們認為倘國家有大規模蒐集、錄存人民之生物特徵（無論是指紋，抑或本文討論之面部特徵），並有建立資料庫儲存之必要以供比對者，在法律制度上必須至少符合下列要件：

1. 該等治理行為係基於特定重大公益之目的，且以法律明定其蒐集之目的，並應明文禁止法定目的外之使用；以及

2. 其蒐集行為應與重大公益目的之達成，具有密切之必要性與關聯性。

除了這個法律本身之要件以外，另方面，基於憲法保障人民資訊隱私權之本旨，大法官們同時也在理由書與意見書[110]中指明主管機關應以**配合當代科技發展**之方式，確保資訊安全以及資訊之正確性，並且對所蒐集之生物特徵檔案採取**組織上**與**程序上**必要之防護措施。[111]既如此，本文必須接續分析之問題厥為所謂組織與程

110 釋字第603號解釋中，許宗力大法官與曾有田大法官所提出之共同協同意見書，即指出：「……是基於基本權的保護義務功能，國家有義務採取適當之組織與程序上保護措施，使個人資訊隱私權免於遭受第三人之侵害。同時基於當代資訊科技發展之開放性，國家並有義務不斷配合資訊科技發展的腳步，採取隨科技進步而升級之動態性的權利保護措施，以有效保護人民之資訊隱私權。……」

111 前揭的許宗力大法官與曾有田大法官共同協同意見書中，爲此甚至疾呼曰：「……在這種欠缺組織與程序上保護措施規定所導致之違憲瑕疵，單靠『信賴政府保護資訊之能力』的信心喊話，或『不能因資訊外流的風險而因噎廢食』的道德呼籲，是無法獲得治癒的……」。

元照出版提供 請勿公開散布
序上之措施，其具體內涵可能為何。

首先在程序上，在釋字第603號解釋中所稱的人格發展自由，其內涵應當是可以依照其自由意志決定其發展之方向、方法、程度與所有的可能性，也就是解釋文所謂「其中就個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權」。如果從這點來看，人格發展自由除了有實質上「應該發展成怎樣的人格」的面向外，更有程序上「自由選擇如何發展而能夠具體地實現所想要發展成的人格」的面向，而後者即在確保達成「具有實質性價值內涵之要求」之目標。[112]而這個程序上之人格自我發展決定之保障，反映在個資當事人之同意其個資的相關蒐集、處理與利用之行為上，在一般個資即須**獲得個資當事人之同意**或**符合明確之法律規範**；至於敏感性個資的面部特徵個資，除邏輯上當然仍須符合一般個資之保護要件，另方面對於將何人放入追蹤名單之問題，在程序上亦應當具有一定之程序上保障機制而不應恣意。[113]

但是以國家機關在公共空間發動AFR之行為來看，要求所有個資當事人，也就是進入被監視之公共空間的所有人，均同意該等個資處理行為，顯有實務上困難，則對應機關的**個資保護政策文件顯然地必須明確訂立且嚴謹地執行**，以填補這個實務的困難。換言之，基於犯罪偵查等治安或國家安全之需要而蒐集人民之各類生物

112 邱文聰，從資訊自決與資訊隱私的概念區分——評「電腦處理個人資料保護法修正草案」的結構性問題，月旦法學雜誌，168期，頁179，2009年5月。

113 例如美國法院在Terry v. Ohio案中，法院便明白地宣示法院有確認追蹤名單之權，且如若因爲該等程序恣意而達成之查獲，將排除於證據之外。Terry v. Ohio (1968), 392 U.S. at 15.

元照出版提供　請勿公開散布

特徵資料並非絕對地不允許，不過相對嚴謹地控制程序[114]以圖填補前述困境，則必須加以正視。又，在此所謂的「嚴謹地」落實個資保護政策，本文認為基於在公共空間面部辨識基於面部之外露性、頻繁性與比對上的即時性與簡便性而特別容易侵害當事人個資上權利，因此本文依循林子儀大法官之見解，認為應在關於此等生物特徵之大規模蒐集與辨識上，採取嚴格之審查標準予以審查，也就是說公務機關在進行公共空間的面部辨識時，必須是為了「非常具體且重大之公益目的，且沒有其他更小侵害之替代手段足以達成目的時」，方准予為之。[115]如果借鏡Bridges案，DPA 2018第35條亦特別要求須符合嚴格之必要性、符合英國DPA 2018附件8所規定之各類型干預之詳細要件，以及依法揭露合適的個資保護政策文件。而就所謂的合適個資保護政策文件，英國資訊委員認為必須能適切地反應干預行為關於嚴格之必要性之要求，也就是至少須滿足有足夠之明確性與可預見性之要求，並需有合適之個資風險影響評估。[116]

然而，面對現在新穎科技之應用於監控名單之追蹤，顯然被動

114 釋字第603號解釋中，林子儀大法官所提出之協同意見書，指出：「……基於刑事偵查需要而蒐集人民之指紋資料，並非一概不可，但就對象與事由仍須事先嚴加規範，並須有嚴謹的程序控制。例如刑事訴訟法第二百零五條之二規定：檢察事務官、司法警察官或司法警察因調查犯罪情形及蒐集證據之必要，得對經拘提或逮捕到案之犯罪嫌疑人或被告，強制採取其生物特徵資訊，如指紋、掌紋、腳印、相片、身高等，如有相當理由認爲毛髮、唾液、尿液、聲調或吐氣得作爲犯罪證據時，並得採取之。其爲犯罪偵查而蒐集別辨識或犯罪證據有關之個人資訊，尚有較爲嚴謹之目的及程序規定，則爲有助於犯罪偵防與改善治安，而向全民蒐集指紋資訊，更不能以法律籠統之授權而爲之。……」

115 釋字第603號解釋林子儀大法官提出之協同意見書參照。

116 ICO, *supra* note 54, at 11.

元照出版提供 請勿公開散布
地僅在程序上賦予個資當事人權利侵害救濟已然不足，學者也認為應有正當程序保障以使合理懷疑標準（reasonable suspicion standard）更加清晰，並以外部之監督機制來確保權力分立原則之踐行。[117]換言之，為了確保人民也就是個資當事人之基本權利與自由不致遭受過度之干預，國家應採取合適之組織保護措施。如果以Bridges案的英國來看，英國對於AFR相關技術之監督共有四個獨立機關，分別為對應監視攝影系統執行準則的監視攝影委員（Surveillance Camera Commissioner, SCC）、對於偵查程序生物特徵個資留存與利用加以監督的生物特徵委員（Biometrics Commissioner, BC）以及專責鑑識品保的鑑識科學管控官（Forensic Science Regulator, FSR），另一個獨立專責機關即為資訊委員。[118]

如單就個資的組織上保障措施來看，顯然地從GDPR第51(3)條與我國目前現行個資法回歸由各該中央目的事業主管機關之分散式監管模式不同，這是因為該GDPR之規範規定會員國應「指定其一於委員會代表各監管機關，並應建立機制，以確保其他機關遵循與第63條所稱之一致性機制有關之規範」，以此來看，應可推定為較鼓勵會員國採取集中式之專責型態，[119]並受GDPR第52條之獨立性保障，而其相關之組織功能，論著也以其具備對於個資保護之多功能面向，並可以快速應變新興科技與當前緊急局勢，而有對應、專業且具有能量之保護。

又，或許有論者會認為個資保護之法制架構及規範內涵如果過

117 Jeffrey Kahn, *Terrorist Watchlists*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 71, 93-99 (David Gray & Stephen E. Henderson eds., 2017).

118 關於英國資訊委員在組織上之保障功能分析，參翁逸泓，資訊委員的時代角色——以GDPR及英國2018年資料保護法爲中心，月旦法學雜誌，286期，頁32-50，2019年3月。

119 翁逸泓、李寧修，同註30，頁16。

元照出版提供　請勿公開散布

於「嚴謹」而不「鬆綁／適度調整」，[120]則將可能因為無法更自由地串接資料而阻礙資訊之流通乃至於更大公共利益之追求。然從立法目的上無論從GDPR、DPA 2018或是臺灣之個資法來看，「促進個人資料之合理利用」與流通本身即為個資保護整體架構的追求目的。而這個尋求以負責任之方式合理地利用個資而促進資訊流通以達成AFR追求之打擊犯罪與維護國家安全等目的，其實亦可以該等組織上之監督管理，以及教育宣導、法律解釋、執法制裁等功能為之。綜言之，本文認為一個有效能的個資保護專責機關除了可以反映憲法解釋上關於個人人格自主發展自由的組織保護要求，也可因為其多樣之功能而成為推動資訊流通與應用之助力。據此，本文認為在組織上，這個**外部**之監督機制，至少在AFR關於個資保護之判斷上，可由專責之獨立個資保護機關為之。

肆、以人工智慧／自動化系統結合面部辨識之監控

由AFR技術之應用於監控來看，可以發現在資料科學與人工智慧高度快速發展的現代，新穎科技相當程度上出現了兩個較以往科技應用於法律執行不同之處：其一，科技之應用可能造成對於基本權利更高效率之保障，卻也同時帶來了更大的侵害風險；復次，法治國下以法律作為治理基礎之原則，似乎漸有移轉至以科技應用作為治理方法之趨勢。前者在前節中已然討論，本文接續分析後者對於應用科技治理在公部門領域中最為敏感的犯罪防免與監控之問題。

120 「適度地」將原有個資法規調整以求更強化之應用效能者，例如去識別化後的健保資料，健保署期待能讓業界企業與學術單位聯合申請，因此鬆綁以往只開放學術單位使用的規定。然亦有學者採取相對質疑之態度。參廖緯民，健保資料庫不應擴大鬆綁，聯合報，2019年4月7日。

元照出版提供 請勿公開散布

一、科技治理與信任基礎

以科技應用之方式為治理決策依據，文獻上已有相當之討論，尤其是對於聚焦於資料科學之應用為中心以提升政府效能，已然成為科技法律之研究者無法忽視之領域。[121]之所以以科技方式作為現今多方倡議之治理決策方法，學者指出原因約略有二：追逐成本效益之提升，並嘗試以科學之客觀性格來移除人類決策在人性部分可能出現之偏見與歧視。[122]此二吸引政府以資料科學為導向而應用科技方法為治理決策依歸的誘因，也在AFR監控作為犯罪預防與打擊中成為主要爭議焦點，而無論對於前者或是後者而言，都必須要一併地考量對基本人權之干預問題。對此，有許多國際上之文獻均聚焦在演算法治理、歧視問題之解決乃至於法律與倫理上之衝突問題解決等，而（以機器）對個人自動化作成決策之應用研究，尤其是其加值應用與整體社會面向之交錯競合衝擊研究或是報告，事實上亦所在多有。

不惟如此，我國近來在實務上也逐漸有關於科技方式為治理行為，尤其是關於科技偵查之重要影響裁判。以具有指標意義的關於GPS追蹤器之最高法院106年度臺上字第3788號刑事判決為例，該判決指出：

> **……倘有壓制或違反個人之意思，而侵害憲法所保障重要之法律利益時，即屬「強制偵查」，不以使用有形之強制力者為限，亦即縱使無使用有形之強制手段，仍可能實質侵害或危害他**

121 *E.g.*, Han-Wei Liu, Ching-Fu Lin & Yu-Jie Chen, *Beyond State v Loomis: Artificial Intelligence, Government Algorithmization and Accountability*, 27 INT. J. LAW INFO. TECH. 122, 122-41 (2019); JAKE GOLDENFEIN, MONITORING LAWS: PROFILING AND IDENTITY IN THE WORLD STATE (2019).

122 Liu, Lin & Chen, *id.* at 124.

元照出版提供　請勿公開散布

人之權利或利益，而屬於強制偵查。又依強制處分法定原則，強制偵查必須現行法律有明文規定者，始得為之，倘若法無明文，自不得假借偵查之名，而行侵權之實。……

……是個人縱於公共場域中，亦應享有依社會通念得不受他人持續注視、監看、監聽、接近等侵擾之私人活動領域及個人資料自主，而受法律所保護，此觀司法院釋字第603號、第689號解釋意旨自明。故而隱私權屬於憲法所保障之權利，殆無疑義。……

……即使個人身處公共場域中，仍享有私領域不被使用科技設備非法掌握行蹤或活動之合理隱私期待。……

在這則具指標意義的判決中，暫且不論後續所引起關於法務部嘗試推動科技偵查法立法之系列討論，[123]至少可以歸納出一個基本之觀察，亦即使用科技設備為治理行為，包含對犯罪之防免、偵查與制裁時，通常伴隨著如本文所指的權利衡平問題。然，在進入利益衡平以決定是否在比例上所求利益為可能選項之前，本文認為與其直接對於比例原則之適用進行分析，毋寧應當優先反思科技治理在本質上之基礎為何，以作為後續論理之憑恃。

本文認為政府在治理決策時，都必須先在一定的程度上建立起

123 法務部109年9月8日在官網上，公告「科技偵查法」草案，共有7章28條之條文，然其立即引起相當之回應。爲此，律師公會與司法院亦有部分歧異之意見，而學界亦有發表聲明，表示科技偵查立法有必要性，但草案應加強程序保障規定，尤其是大幅提高法官保留密度者。林育瑄，科技偵查法草案涉隱私權 法務部司法院不同調，中央通訊社，2020年9月25日，https://www.cna.com.tw/news/aipl/202009250234.aspx，最後瀏覽日：2020年11月30日；林長順，科技偵查法草案　法界籲提高法官保留密度，中央通訊社，2020年10月7日，https://www.cna.com.tw/news/asoc/202010070230.aspx，最後瀏覽日：2020年11月30日。

元照出版提供 請勿公開散布

與社會成員之信任關係。這是因為在進行公部門治理時，難免有干預社會成員基本權利，尤其是私生活權利之可能，而此種特性亦更見於以科技方式，例如以資料分析或人工智慧進行的政策治理之中。[124]此際權利發生競合之時往往難以期待一致且穩定的衡平方式，因此如果能建立起社會整體對於該等治理方式之信任關係，則論理上能有效地降低權利間彼此衝突競合的機會，而減緩必須要進入這個不穩定衡平考量之次數。[125]

就本文參考點的Bridges案來看，歐盟與英國之個資保護架構乃是整體涉為經濟發展與科技在各層次應用之基礎前導工程，例如歐盟在二〇二〇年第四季提出「共同歐洲資料空間」（common European data spaces）的治理立法框架以強化共同資料空間及其他跨公私部門資料利用方式的治理機制之時，便在其政策中說明因為整個歐盟已然熟悉GDPR之個資保護秩序，因此在GDPR基礎下能在因為科學研究目的利用敏感個資時，決定「何人」可以「如何」利用「何種」資料，令個人更容易同意其個資的公益目的利用。[126]例如基於二〇二〇年之COVID-19疫情，因為需要相當數量的疫情相關個人特種健康個資而為疫苗以及相關症狀醫療之研究基礎，對於科學研究之面向有所影響，因此有關依據GDPR第4(15)條將健康

124 Liu, Lin & Chen, *supra* note 121, at 122.

125 相關之論證，*See* Deryck Beyleveld, *Conceptualising Privacy in Relation to Medical Research Values*, *in* FIRST DO NO HARM: LAW, ETHICS AND HEALTHCARE 151, 156-59 (Sheila A. M. McLean ed., 2006); 翁逸泓，開放政府資料於數位匯流加值應用的個人資料保護問題：對於「合作模式」之證成，載：施茂林教授七秩華誕祝壽論文集（上冊），頁813-821，2020年7月。

126 European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS "Towards a common European data space", COM/2018/232 final.

元照出版提供　請勿公開散布

資料用於此類研究目的的法律問題不斷出現時，歐盟能迅速地透過指引闡明其中最緊迫的問題，包括法律依據、對此類健康資料處理的充分保障措施的實施以及對個資當事人權利的行使等，[127]使得個資當事人能理解權利行使而提高獲得其同意之機會。

須知，努力走向值得信任的科技治理在概念上不僅要考慮科技應用系統本身的可信賴性，基於治理之對象和過程是系統整個生命週期中社會技術環境的一部分，因此該等治理是否值得信任，還需要在實際操作前考量整體系統，包含其所有的參與者和治理之過程。而這個概念亦反映於歐盟GDPR第35(1)條[128]所明文規範指出此種「使用新科技之處理方式」，應當考量該處理之本質、範圍、使用情形及目的，且在時間點上，倘若可能導致自然人之權利及自由的高度風險時，個資控制人應於處理**前**，實行該處理對於個資保護之影響評估。再者，個資保護之核心原則「公正資訊處理原則」（fair information practice principles, FIPPs），更應在司法審查之範圍。[129]至於具體的**判斷標準**，以英國實踐GDPR為例，其資訊委員及著名的圖靈研究所（The Alan Turing Institute）在管制上要求人

127 EDPB, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, *available at* https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf (last visited: 2021.09.17).

128 GDPR第35(1)條：「於特別使用新科技之處理方式，且考量該處理之本質、範圍、使用情形及目的後，認為該處理可能導致自然人之權利及自由的高度風險時，控管者應於處理前，實行該處理對於個人資料保護之影響評估。單一評估得針對一系列呈現相似高風險之類似處理。」

129 該原則其下尚有五個子原則，包括知情原則、同意原則、參與原則、資安原則，以及救濟原則等。詳參翁清坤，大數據對於個人資料保護之挑戰與因應之道，東吳法律學報，31卷3期，頁79-159，2020年1月。

元照出版提供 請勿公開散布

工智慧之決策作為需注意：[130]

㈠平等原則

核心重點在於避免AI系統的輸出是否具有歧視性影響，此時必須將防止歧視和減輕偏見的目標充分安置到系統的設計和實施中，且需確定結果分配到系統中之公平標準納入其中，並預先將這些結果明確告知使用者，以確保該模型是否防止了因為歧視造成之損害結果。

㈡透明原則

在此應審視個資保護模型輸出背後的技術邏輯或推理為何，也就是必須說明哪些輸入特徵、參數和相關性在模型結果的計算中有較重要之作用，以及如何發揮該等作用。而該等解釋必須以易於理解是方式說明相關原理，使而受決策結果影響之個人或其代表能有能力對其進行理性之評估。另外就個資之流動，必須揭露個資控管者使用了何種個資來訓練模型，該等個資從何而來，以及如何確保個資品質。

㈢課責原則

此處之判斷標準最重要者厥為確認從定義結果的初始階段到提供解釋的總結階段，究竟由誰來負責AI系統設計和部署的每個階段？哪些機制是課責之標的？以及整個治理機制中，應如何使確保該設計和實施過程的可追溯和可審核性。

---

130 ICO and The Alan Turing Institute, Explaining Decisions Made with AI, pp. 38-44, *available at* https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-artificial-intelligence-1-0.pdf (last visited: 2021.04.24).

元照出版提供　請勿公開散布

本文認為如果觀察以上三個原則，其共通之處均在於建立一定之信任關係。既然促進社會成員的人民對政府治理之信任為治理行為之基礎，那麼如果希冀以自動化科技帶來的最大便利與科學正確性方式，串連各類個資以為犯罪防免的治理行為，當然也需要以此為出發點。基於此，本文以下分析AFR的最後一個特性：自動化／人工智慧處理個資，以及以該處理結果為決策之問題。

二、以人工智慧／自動化系統作為治理方法？

基於人工智慧與面部辨識之經濟發展與監控有效性，臺灣許多研發團隊均以此之相關應用發展，而有一定科學技術上之成果。以本文前揭所舉之臺鐵豐原站之「智慧型影像監控系統工程」，就是一個較為明確的人工智慧分析之AFR應用於即時監控。其他在經濟民生之相關應用上，例如有研究團隊發想廣告企劃，運用AI**技術**結合一萬個臺灣人**臉孔**（**面部特徵**），創造出AI臺灣人「戴怡宛」。[131] 然，其在個資之獲取上是否經同意，如否，得合法蒐集、處理與利用之預先同意且免告知事由為何？當事人是否有退出可能？等等法學上問題，均有待回答。

另方面，在我國新創業者能在美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）二〇一九年公布面部辨識比賽（Face Recognition Vendor Test, FRVT）最新報告中多項測試跑分均位居第一，在大頭照（Mugshot）測試中甚至高於中國某AI獨角獸（估值超過10億美元）的1.3GB模型的國際研

131 吳家豪，一萬張臉綜合體　AI台灣人戴怡宛找工作玩臉書，中央通訊社，2019年12月16日，https://www.cna.com.tw/news/firstnews/201912160283.aspx，最後瀏覽日：2019年12月21日。

元照出版提供 請勿公開散布

發有領先成就之時，[132]即便面對科學界已然承認AI具有偏見之當下，[133]我國在對應的規範上卻仍相對地未臻足夠。我國之個資法雖有將個人資料檔案定義為「指依系統建立而得以**自動化機器**或其他非自動化方式檢索、整理之個人資料之集合」[134]之關於自動化機器之文字敘述，然所規範之單純得以自動化方式檢索與整理之機器事實上與得作成自動化決策或甚至人工智慧決策之當代資料科技應用方式頗有區別，在適用上仍有落差，故我國個資法在未經「現代化」之變更之前，難謂有**任何個資法上對於該等自動化機器作成之決策與評價作出明文規範、保護乃至於例外情狀之判準**，甚至與歐盟提案中「**關於電子通訊面向保障個人私生活與個人資料保護規則**」（Regulation on Privacy and Electronic Communication, PECR）[135]之個人特徵剖析概念相銜接而獲得歐盟就GDPR適足性之認證。[136]那

---

132 林宏翰，耐能AI人臉辨識全球第一　擊敗中國億元獨角獸，中央通訊社，2019年7月13日，https://www.cna.com.tw/news/aopl/201907130086.aspx，最後瀏覽日：2019年12月21日。

133 中央通訊社，AI學習人類偏見　出乎開發者意料，2019年11月13日，https://www.cna.com.tw/news/firstnews/201911120380.aspx，最後瀏覽日：2019年12月21日。

134 個資法第2條第2款參照。

135 European Commission, Proposal for a Regulation of the European Parliament and of the Council: Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final, 2017/0003 (COD) (Brussels, 10.1.2017), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN (last visited: 2019.11.23).

136 我國在研發方面之人工智慧發展，科技部有以較為軟性概略「人工智慧科研發展指引」對應。其中關於個資保護，僅有「個人資料隱私侵害的預防，必須建立有效的數據治理，在AI研發與應用上，AI科研人員應致力注意個人資料蒐集、處理及利用**符合相關法令規範**，以保障人性尊嚴與基本人權，並針

元照出版提供　請勿公開散布

麼，在法規範接近真空之狀態下，政府邇近大力推行之科學技術發展重點領域如人工智慧之研發與加值應用等，又該如何真正地面對來自於個資法之潛在挑戰呢？又，即便是主張對於犯罪之防免與偵查應以人工智慧或其他機器自動化處理之科技方式加以治理，但於其所必然包含的個資處理概念如果因為法律真空而無所適從時，難道真的能有一個完全不理會法律規範的人工智慧管制模式嗎？[137]既然我國無相關規範，則本文認為不妨於我國刻正嘗試通過歐盟GDPR適足性認證之同時，適度地借鏡歐盟相關經驗：如果治理之決策與行為均建基於本文前述所指信任關係上，將有較大的機會如同歐盟執委會成立的高階人工智慧專家團（High-Level Expert Group on Artificial Intelligence, HLEG）所指，在信任的架構下，透過民主、法制及基本權利的支持，AI之應用可在此環境下持續精進及保衛民主文化，並促使創新及負責之競爭得以實現。[138]再者，該份「值得信任的AI倫理指引」也認為因為如果沒有值得信賴的AI系統以及「（系統）其後之人類」，那麼可能會導致不必要的後果，並且可能會阻礙其應用，以致無法實現AI應用可能帶來的巨大

對AI系統內部之個人資料架構有適當的管理措施，以維護資料當事人權益。」然在相關法令缺乏對應之狀態下，該等指引似難有真的「指引」效果。

137 關於智慧科技管理時代，不以法律規範而替代以科技管理方式為之，則對傳統法律概念如法治、人權保障與人性尊嚴等，應如何面對之論理與反思法律本身的價值與法律如何規範，可參Roger Brownsword, *Regulating the Information Society: The Future of Privacy, Data Protection, Law, and Consent*, *in* LAW, TECHNOLOGY AND SOCIETY: RE-IMAGINING THE REGULATORY ENVIRONMENT 300-02 (Roger Brownsword ed., 2019).

138 European Commission, High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, April 8, 2019, *available at* https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419 (last visited: 2020.11.30).

元照出版提供 請勿公開散布
社會和經濟利益，因此，信任感是人們和社會開發，部署和使用AI系統的先決條件。[139]

在以人工智慧或其他機器自動化處理之科技方式治理關於犯罪之防免與偵查之決策上，並非所有自動化治理的作法，都能被視為一種自動化決策，此間相關之治理之模式，可以分為三類型：[140]

⑴規則為本（rule-based）之方式

根據少量經過先驗選擇的上、下文相關指標，將調節因素置於優先級分組中而為決策。

⑵資料—通知（data-inform based）為基礎之方式

預先呈現、匯總眾多優先選擇的廣泛指標，以告知一個或多個專家組成之上位決策，依據決策結果加以治理。

⑶演算法為基礎之方式

以智慧學習技術從可得知資料中決定最正確之優先模式。

而只有在自動化治理之實際作為上，各項以人工智慧之治理作為在符合僅基於自動化處理（包含剖析）所作成而對其產生法律效果，或類似之重大影響之決策時，而無前述例外情狀後，即屬以機器自動化作成決策之行為。換句話說，其中是否有人為之介入的構成要件，係區辨是否為純以人工智慧治理之關鍵差異。故，應認只有類型⑶，且發生如本文前述具有歧視與壟斷性結果，而成為類似之重大影響決策時，方為討論標的。

關於此處之（以機器）對個人自動化作成決策與個資保護之問題，歐盟個資保護指令早在一九九五年即明文規範有**個資當事人應**

139 *Id.* at 4.

140 Alex Griffiths, *The Practical Challenges of Implementing Algorithmic Regulation for Public Services*, *in* ALGORITHMIC REGULATION 150, 153-58 (Karen Yeung & Martin Lodge eds., 2019).

元照出版提供　請勿公開散布

有權不受自動化決策之拘束（not to be subject to a decision）[141]，而該決策需對個資當事人產生法律效果或類似之重大影響，並僅以自動化處理來評估其個人特徵之措施。例如：網路簽證申請之自動否准，或不包括任何人為介入之電子化人力招募等。依指令及其解釋，即便為締結或履行資料主體與控管者間之契約所必須，或個資主體已明確同意，資料控管者仍應執行歐盟或會員國規範之適當措施，以保護個資主體之權利及自由及正當利益，並至少應確保得以部分之人為參與（human intervention）、表達意見（to express his or her point of view）及獲得挑戰該決定（contest the decision）之機會[142]，此項權利亦繼續被承繼在GDPR第22(1)條拒絕機器自動化決策權。不過，GDPR與原有個資保護指令最大之差異在於GDPR個資當事人有權利發出通知，請求個資控管者不要使用其個資作出任何自動化決策，並要求個資控管者重新考慮通過自動方式作出的決定。

行文至此，必須處理的一個論理上問題，即在於為何在講求人工智慧發展與應用的資料科學時代，原則上不能以機器自動化決策之方式，以預設之方式**完全**替代資料主體本身之意志，亦即資料當事人為何「（有權利）能拒絕受機器自動化決策之拘束」？這個法理上問題的根本回應當然還是回到資料當事人作為個資權利主體本即有其資訊自主權，亦即個資當事人對其「自身相關之資訊，擁有決定在何種範圍內、**於何時**、向誰及以何種方式加以揭露、處分使用之自主權」。[143]就第22(1)條來看，其文字為「個資當事人應有

141 歐盟個資保護指令第15條參照。

142 Lee A. Bygrave, *Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, 17 COMPUT. LAW SECUR. REV. 17, 18-21 (2001).

143 司法院釋字第689號解釋林子儀、徐璧湖大法官部分協同部分不同意見書，頁5。

元照出版提供 請勿公開散布
權不受僅基於自動化處理，包括剖析所作成而對於該個資當事人產生法律效果或類似重大影響之決策所拘束」（The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.），不過這邊所生的爭議問題乃是雖然條文本身「看起來」像是第22條賦予的是個資當事人在個資控制人僅為自動化處理並決策時，得予拒絕之拒絕權，但是對應的GDPR前言第71點卻也明文「然而，在歐盟法或會員國法明確授權受該等法所從之個資控管人時，該等基於（個資自動化）處理，包括剖析則**應予允許**」（However, decision-making based on such processing, including profiling, **should be allowed** where expressly authorised by Union or Member State law to which the controller is subject, including for…）（emphasis added），以及在最末段稱「對於特種個資所為之自動決策與剖析僅可在特定條件下**被允許**」（Automated decision-making and profiling based on special categories of personal data **should be allowed** only under specific conditions.）（emphasis added）等文字看來，又像是可以解釋為除非有例如第22(2)條之例外情況，否則原則上禁止個資控制人僅為自動化處理並決策之行為。

這兩個不同解釋之區別實益在於如果為「拒絕權」之解釋，則個資控管人（亦即本文所討論之施行AFR應用之公務機關）原則上可為僅由機器自動化決策而對於該個資當事人產生法律效果或類似重大影響與剖析之行為（例如應用AFR），而個資當事人則在其行為後如未有例外情狀下，有權拒絕；相反地如果為禁止說之解釋，則原則上該等行為是被禁止的，除非有例外之形狀出現，個資控管人才可以為之。此時，基於例外情狀在解釋上應予以嚴格限縮，則如果採取後者的解釋，明顯地對於個資控管者，也就是AFR之應用

元照出版提供　請勿公開散布

者較為不利，因為其例外之情狀應當相對地有限。也因此，學者認為未來對於GDPR第22條其在解釋適用上，應該就其性質應該屬於「禁止說」或是「有權反對／拒絕權說」說作出判斷，係為相關爭議問題之關鍵研究重點。[144]

就此問題，**本文認為應採前者「禁止說」為妥**，理由如下：

㈠從體系解釋之角度，應採禁止說

在對該爭點作出細部分析之前，[145]必須先將GDPR作出體系化之觀察。首先，「以機器自動化作成決策」之概念必須與「以機器自動化處理（個資）」加以區別。前者所謂係指於利用個資所達成之決定之作成能力由科學技術之工具完成，而未必有自然人意志之介入、參與；而後者之自動化僅至處理個資之階段。故以階段言，前者之實現必須是以後者已然實現為條件。再者，「（以機器）對個人自動化作成決策」之概念必須與「特徵剖析」（profiling）之概念區分：GDPR第4條將個人特徵剖析定義為：「為評估與自然人相關的某些個人情況，對個資進行任何自動化處理與利用的方式，特別是針對與自然人的工作表現、經濟狀況、健康狀況、個人偏好、興趣、信度、習性、位置或行蹤相關的分析和預測。」

基於此，特徵剖析僅為以機器自動化處理、利用個資後所作成之評價，而該等評價可以作為至少三種不同功能之利用：找出個資當事人偏好、預測個資當事人行為，以及可作為進一步決策之依

144 參劉靜怡，人工智慧潛在倫理與法律議題鳥瞰與初步分析——從責任分配到市場競爭，載：人工智慧相關法律議題芻議，頁42-43，2018年11月。

145 相關詳細的分析也可參見Lee A. Bygrave, *Article 22 Automated Individual Decision-Making, Including Profiling*, *in* THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 522, 530-32 (Christopher Kuner, Lee A. Bygrave & Christopher Docksey eds., 2020).

元照出版提供 請勿公開散布

據，其中，只有第三種作為決策之依據的態樣，會使得特徵剖析成為自動化作成決策之一部分。須注意者，此二者於決定之作成係由一系列之機器對於個資作出處理、利用而後逕為決定之時，可能有所重疊，而非必為絕對分離之概念。例如，在某些情況下，人為介入可能只是簡單地對系統的所有結果進行「簽到」（sign off），從而使其產生幾乎自動化決策之結果。[146]

至於GDPR第22條，[147]在體系上是位於關於第三章資料當事人權利保障體系下的第四節「拒絕權及對個人之自動化決策，包含剖

[146] Michael Veale & Lilian Edwards, *Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling*, 34 COMPUT. LAW SECUR. REV. 398, 398-404 (2018).

[147] Art. 22 of the GDPR:

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph 1 shall not apply if the decision:
   a. is necessary for entering into, or performance of, a contract between the data subject and a data controller;
   b. is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
   c. is based on the data subject's explicit consent.
3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

元照出版提供　請勿公開散布

析」（Automated individual decision-making, including profiling），而該小節涵括了兩個重要規範：其一是第21條的拒絕權；其二是第22條對個人自動化決策，包含剖析之相關規範。本文認為這二者被放在同一小節之內，顯見其在體系上應為一致（consistent）而不相互排斥（消極的一致性），且彼此支持（積極的一致性）之解釋。據此，一個立即的觀察便是在第21(5)條即出現在使用資訊社會服務（Information Social Service, ISS）[148]之過程中，資料當事人得拒絕「以使用技術規範／標準的自動化處理（個資）」，此時當個資當事人拒絕了該種處理個資之方式，則其後自然難以產生以該種處理方式而導致之「（以機器）自動化作成決策」，並進入第22條之包攝範圍。因此，本文認為在本質上第22(1)條[149]是一個在個資當

148 Article 21(5) of the GDPR: In the context of the use of **information society services**, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications. 其中，ISS此名詞係來自於歐盟關於技術規則與資訊社會服務領域相關資訊之程序指令（Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.）第1(1)(b)條之定義：通常以一定距離，通過電子方式並應服務接受者的個人要求提供有償服務的任何服務。此時所指「一定距離」，即提供服務時各方沒有同時出席；透過「電子方式」，指該服務最初是通過電子設備發送和接收之用於處理（包括數字壓縮）和資料的電子設備，並且通過有線、無線電、光學手段或其他電磁手段完全傳輸，傳送和接收；「應服務接受者的個人要求提供有償服務」則指通過根據個人要求傳輸資料來提供服務。據此，從本質上來說大多數**線上服務**都會落在ISS的定義範圍內，即便該服務的「報酬」或資金並非直接來自最終用戶，也會被認定爲ISS。此時，向最終用戶**免費提供但通過廣告資助**的線上遊戲應用程序或搜索引擎，仍解釋爲屬於ISS的定義範疇內。

149 Article 21(1) of the GDPR: The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of

元照出版提供 請勿公開散布

事人未行使第21(5)條拒絕權後，對於未行使權利所生之事實（自動化處理／剖析之結果），基於該事實的另一個法律行為（決策）而生法律效果或類似之重大影響結果的下一個階段的問題。而相對地，如果個資當事人在一開始便選擇了第21(5)條拒絕個資控管者「以使用技術規範／標準的自動化處理（個資）」，則邏輯上其結果當然就一併禁止了個資控管者進行並實現後續的「（以機器）自動化作成決策」。

㈡GDPR之有權解釋機關，亦採禁止說

除了本文以上以體系解釋之方法論證GDPR第22條並非為拒絕權以外，事實上歐盟WP 29也對此其他之理由，同樣地認為第22條不應解釋為個資當事人之拒絕權：[150]

1. 雖然GDPR第三章之標題為關於個資當事人之權利，但是其中第12條至第22條並非全部都是主動權，例如，雖然第15條至第18條和第20條至第21條是關於個資當事人積極行使其權利之事項，但是第13條與第14條涉及個資控制者必須履行的職責，而個資當事人並未主動地參與該等事項。據此在該章中包含第22條本身並非立即表示其乃為個資當事人主動拒絕之權利；反之，亦然。

2. GDPR第三章第四節之標題為「拒絕權及對個人之自動化決策，包含剖析」，而該小節涵括了兩個規範：其一是第21條的拒絕

---

personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. 2The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

150 WP 29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, adopted on 3 October 2017, last revised and adopted on 6 February 2018, 34-35.

元照出版提供　請勿公開散布

權；其二是第22條對個人自動化決策。如此一來，如果把第22條也解釋為拒絕權，則並無在第四節標題使用拒絕權「**及**」對個人之自動化決策，包含剖析而聯立並行置於標題上之必要性。

3. 如果將第22條解釋為一拒絕權，則第22(2)(c)條之例外規定將毫無意義。這是因為第22(2)(c)條之例外是基於個資當事人之同意而能使自動化決策仍能被施行，但是在此時如果將其解釋為拒絕權，則會出現個資當事人便在**同一個程序中同時行使拒絕權以及同意權**之矛盾。

4. 如果將第22條解釋為拒絕權，則行使拒絕即在表示必須進行隨後之人為參與。雖然第22(2)(a)條和第22(2)(c)條的例外規定推翻了第22(1)條的主要規則，但其前提乃是只有對第22(3)條規定之個資當事人可以進行人為參與。既然個資當事人藉由提出拒絕已經請求人為參與，因此在每種情況下都將自動規避第22(2)(a)條和第22(2)(c)條，從而使該等規定實際上失去任何意義。

也因為如上之理由，WP 29認為GDPR第22(1)條中的「權利」一詞，並不即指其僅在個資當事人主動援引其「權利」時方有適用，而是規定了**對僅基於自動化處理的決策的普遍禁止**（a general prohibition for decision-making based solely on automated processing）。[151]

㈢從目的解釋之角度，應採禁止說

本文認為另外一個更重要之原因則或許是在巨量資料時代一旦機器透過個資處理而能比個資當事人更瞭解該當事人本身，則真正的個資控制實力已經由個資當事人或其他個資控管者等自然人手中

151 *Id.* at 19.

元照出版提供 請勿公開散布

移轉至演算法，[152]而該等演算法如果缺乏了完整的人類意志（例如自然人同意給予決策權），則可能對當代民主與個人基本權利與自由之保護，造成一定程度之威脅。質言之，關於智慧學習後資料經演算法處理所連結之實際利用，也就是此處自動化決策之威脅，學者提出至少包括：*1.*隱匿基於可以分類而為之差別對待；*2.*偏誤複製陷阱可能使其延續社會既有的系統性偏見；*3.*僅生產關聯性知識而無力提出因果說明，則雖用在提供更廣泛預測可能性，造成反歧視法律適用之困境；以及*4.*因為抽離社會意義脈絡所帶來無法課責之問題。[153]而英國資訊委員也在報告中提出以智慧學習而生之演算法，可能作出具有歧視性、錯誤與不當之決策，因此，應以釐清演算法決策之背景理由與因素，及確認是否有歧視性、錯誤與不正當的決策。[154]從而，人為之適時介入仍有助於調整前述偏誤。由於個人基本權利與自由保障本即為GDPR之立法目的，且在闡明立法目的的GDPR前言第77點在解釋上亦較偏向禁止說，因此綜合前述理由，本文認為以禁止說為妥。

基於此，在現今的GDPR規範下關於自動化作成決策之個資保護所謂的適當保護措施，英國資訊委員認為必須至少符合幾個要件：告知個資當事人關於其個資處理之相關資訊、導入易於人類介

152 Stephanie Hankey, Julianne Kerr Morrison & Ravi Naik, Data and Democracy in the Digital Age, The Constitution Society, *available at* https://consoc.org.uk/wp-content/uploads/2018/07/Stephanie-Hankey-Julianne-Kerr-Morrison-Ravi-Naik-Data-and-Democracy-in-the-Digital-Age.pdf (last visited: 2019.11.23).

153 邱文聰，初探人工智慧中的個資保護發展趨勢與潛在的反歧視難題，載：人工智慧相關法律議題芻議，頁164-168，2018年11月。

154 ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection (20170904 Version: 2.2), pp. 10, 51, 86, 88, 98, *available at* https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (last visited: 2020.04.24).

元照出版提供　請勿公開散布

入或挑戰決策過程之機制，以及持續確保該系統如預期目的運作。[155]此時，如果以自動化（包括人工智慧）方式影響個資當事人法律上權利，則在GDPR第22條下一般之個資僅有三種情狀可例外地被允許，也就是在**符合個資保護的基本原則後**：締結或履行控管者與個人之契約所必要、控管者受拘束之會員國或歐盟法律有明文授權，且定有適當保護個資主體權利及自由與正當利益之措施、或基於資料主體明確同意者。但如果自動化作成之決策**含有特種個資**，則僅限於必須個資當事人明確同意或是個資之處理（自動化作成決策）係為實質公共利益必要之所需，並且遵從個資保護核心且以適當及特定之措施保障個資當事人基本權利與利益。

在此必須特別注意的是，通常理解GDPR最常出現的問題之一在於解讀例外豁免得對個資當事人之個資處理條件時，僅考量該等例外豁免得處理個資之特別要件，例如GDPR第9(2)條或第22(2)條之規定等，而忽略了GDPR之規範在處理**所有的**個資時，均需要符合第5條之個資保護之核心原則（如個資目的性原則、最小化原則、合法、公平、透明、正確、限期原則等），並有第6條適法之基礎等一般要件。細言之，基於個資保護必須先滿足核心原則，**所有的**個資處理都須符合各項原則方得為處理。[156]但在特種資料範疇內為個資處理時，除了在**邏輯上特種個資之處理當然要先符合所有個資處理之核心原則**外，又區分為特種個資之一般處理以及特種個

155 ICO, Rights Related to Automated Decision Making Including Profiling, *available at* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/ (last visited: 2020.05.20).

156 由於GDPR將「處理」（processing）定義爲包括我國個資法上對於個資之「蒐集、處理與利用」等所有階段，本文之論述亦同。

元照出版提供 請勿公開散布

資之自動化作成決策而各有例外豁免要件。[157]於特種個資之一般處理情況時，須符合GDPR第22(2)(a)至(i)條之豁免要件其一，方得例外地進行一般處理；至於特種個資之自動化作成決策之情狀，則依GDPR第22(4)條之規定，更嚴格限縮至僅在第9(2)(a)條與第9(2)(g)條的兩種例外豁免條件滿足之時，方得為之。

伍、結　論

綜合本文以上之分析，本文認為在考量任何以科技方式治理決策時，無論是十餘年前爭執的我國全民指紋錄存釋憲案（即釋字第603號解釋），乃至於本文所研究之大規模自動化面部辨識，於進行系爭權利辨識以及衡平之**前**，或許都必須採取一定方法，來降低權利間彼此競合之風險。本文認為，這個事前預先所必須要採取之方法，包括早在當年釋憲案的理由書中指出的，「主管機關尤應配合當代科技發展，運用足以確保資訊正確及安全之方式為之，並對所蒐集之指紋檔案採取組織上與程序上必要之防護措施」等等相關措施，核心主旨都是在於以各種可能的策略，建立政府與人民之間的信任關係。

在關於Bridges案所能帶來的啟發之問題上，可以總結面部辨識技術之應用必然地與個資相關並涉及私生活權利之保障，而為基本權利與自由事項。此際，明確的規範以及對於可能帶來之基本權利侵害風險的防禦，是在比例原則判斷時的重要關鍵所在。這點也早在前述我國的憲法解釋理由書中所指「國家基於特定重大公益之

157 WP 29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01), *available at* https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826 (last visited: 2020.04.24).

元照出版提供　請勿公開散布
目的而有大規模蒐集、錄存人民指紋、並有建立資料庫儲存之必要者，則應以法律明定其蒐集之目的，其蒐集應與重大公益目的之達成，具有密切之必要性與關聯性，並應明文禁止法定目的外之使用」之論點能尋得脈絡。然而，時至今日，公務機關在應用更加進化而更可能干涉個人基本權利之新穎科技，卻似乎總是遺忘這些曾經被糾正過的回憶。

AFR這個新穎科技所帶來的除了將例如警用隨身密錄器、實體與虛擬空間的面部辨識應用帶來（持續一段不算短時間的）新的爭議問題，例如未有明確規範與組織上及程序上的合適保障以外以自動化系統或人工智慧方式結合該技術之應用更帶來科技治理的新時代難題：科技決策是否能成為一個在法律制度上能完全地被接受的治理方式？本文認為，如就資料治理考量AFR之個資保護問題，當政府機關要將人民對其基於民主之相互信任關係移轉至由自動化系統或人工智慧等非人類而進行決策之時，因為難以具體地對於該等非人類決策進行課責，因此人民與政府之信任之關係在此相對地轉趨弱化。此際如期待重塑整體資料治理之信任基礎，本文便認為更需要有個資保護在法制、程序以及組織上之強化，方得為之。

基於此，本文綜整所觀察之Bridges案分析所得，認為我國在保障人民基本權利與自由之前提下施行AFR並非絕對不允，而是在目前法制環境之狀態下，於法制與程序上應預先地考量有一特別、明確之指引與包括DPIAs之措施，尤其是對於何人應被放入AFR監控之名單，以及在何處實施AFR等要件與解除條件必須特別注意。另外，該等規範必須特別地注重平等（不歧視）、透明以及比例原則，以及對於自動化決策之課責可能，而使人民能有效地獲知該等政策，使法律規範具有預測性與安定性，以維持人民與政府之間的信任關係。最後，在組織上，則本文認為遲至今日未有之獨立個資專責監管機關的儘速建立，應為放行AFR的重要前提要件。

元照出版提供 請勿公開散布

參考文獻

一、中 文

1. 王正嘉，預測性警察活動在犯罪偵防運用與問題，刑事政策與犯罪防治研究專刊，25期，頁1-47，2020年8月。
2. 王信賢，科技威權主義：習近平「新時代」中國大陸國家社會關係，展望與探索，16卷5期，頁111-127，2018年5月。
3. 李寧修，警察存取預防性資料之職權與個人資料保護：以監視器之運作模式為例，國立臺灣大學法學論叢，48卷2期，頁391-437，2019年6月。
4. 李震山，公權力運用定位科技措施與基本權利保障，載：人性尊嚴與人權保障，4版，頁273-314，2011年10月。
5. 林明鏘，由防止危害到危險預防：由德國警察任務與權限之嬗變檢討我國之警察法制，國立臺灣大學法學論叢，39卷4期，頁167-212，2010年12月。
6. 邱文聰，從資訊自決與資訊隱私的概念區分——評「電腦處理個人資料保護法修正草案」的結構性問題，月旦法學雜誌，168期，頁172-189，2009年5月。
7. 邱文聰，初探人工智慧中的個資保護發展趨勢與潛在的反歧視難題，載：人工智慧相關法律議題芻議，頁152-180，2018年11月。
8. 范耕維，現行法下GPS追蹤定位偵查行為之合法性與立法方向——比較法觀點與最高法院106年度臺上字第3788號判決之考察，政大法學評論，157期，頁109-197，2019年6月。
9. 翁清坤，大數據對於個人資料保護之挑戰與因應之道，東吳法律學報，31卷3期，頁79-159，2020年1月。
10. 翁逸泓，資訊委員的時代角色——以GDPR及英國2018年資料保護法為中心，月旦法學雜誌，286期，頁32-50，2019年3月。
11. 翁逸泓，開放政府資料於數位匯流加值應用的個人資料保護問題：對於「合作模式」之證成，載：施茂林教授七秩華誕祝壽論文集（上冊），頁801-830，2020年7月。
12. 翁逸泓、廖福特，私生活權利：探索歐洲，反思台灣，2014年12月。

元照出版提供　請勿公開散布
13. 翁逸泓、李寧修，「歐盟國家個人資料保護法制因應GDPR施行之調適——以德國與英國為例」委託研究計畫結案報告，國家發展委員會，2020年5月。
14. 程明修，行政法上之預防原則（Vorsorgeprinzip）食品安全風險管理手段之擴張，月旦法學雜誌，167期，頁127-136，2009年4月。
15. 溫祖德，從Jones案論使用GPS定位追蹤器之合憲性——兼評馬賽克理論，東吳法律學報，30卷1期，頁121-167，2018年7月。
16. 葉俊榮，探尋隱私權的空間意涵：大法官對基本權利的脈絡論證，中研院法學期刊，18期，頁1-40，2016年3月。
17. 劉定基，個人資料保護法講座：第一講個人資料的定義、保護原則與個人資料保護法適用的例外——以監視錄影為例（上），月旦法學教室，115期，頁42-54，2012年5月。
18. 劉定基，個人資料保護法講座：第一講個人資料的定義、保護原則與個人資料保護法適用的例外——以監視錄影為例（下），月旦法學教室，119期，頁39-54，2012年9月。
19. 劉靜怡，人工智慧潛在倫理與法律議題鳥瞰與初步分析——從責任分配到市場競爭，載：人工智慧相關法律議題芻議，頁1-45，2018年11月。
20. 蔡聖偉，再論私裝GPS跟監與「竊錄非公開活動」——評最高法院106年度台上字第3788號刑事判決，裁判時報，76期，頁27-40，2018年10月。
21. 薛智仁，GPS跟監、隱私權與刑事法——評最高法院106年度台上字第3788號刑事判決，裁判時報，70期，頁42-60，2018年4月。

二、外　文

1. Andrejevic, Mark (2018), *Data Collection Without Limits: Automated Policing and the Politics of Framelessness*, *in* Aleš Završnik ed., BIG DATA, CRIME AND SOCIAL CONTROL. (Oxon: Routledge).
2. Berle, Ian (2020), FACE RECOGNITION TECHNOLOGY: COMPULSORY VISIBILITY AND ITS IMPACT ON PRIVACY AND THE CONFIDENTIALITY OF PERSONAL IDENTIFIABLE IMAGES, Cham: Springer.

元照出版提供 請勿公開散布
3. Beyleveld, Deryck (2006), *Conceptualising Privacy in Relation to Medical Research Values*, *in* Sheila A. M. McLean ed., FIRST DO NO HARM: LAW, ETHICS AND HEALTHCARE. (Oxon: Routledge).
4. Beyleveld, Deryck & Brownsword, Roger (2001), HUMAN DIGNITY IN BIOETHICS AND BIOLAW, Oxford: Oxford University Press.
5. Blitz, Marc J. (2017), *Local Law Enforcement Video Surveillance: Rules, Technology, and Legal Implications*, *in* David Gray & Stephen E. Henderson eds., THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW. (New York, NY: Cambridge University Press).
6. Bowling, Ben & Iyer, Shruti, *Automated Policing: The Case of Body-Worn Video*, 15 INTERNATIONAL JOURNAL OF LAW IN CONTEXT 140 (2019).
7. Brincker, Maria (2017), *Privacy in Public and the Contextual Conditions of Agency*, *in* Tjerk Timan, Bryce C. Newell & Bert-Jaap Koops eds., PRIVACY IN PUBLIC SPACE: CONCEPTUAL AND REGULATORY CHALLENGES. (Cheltenham: Edward Elgar).
8. Brownsword, Roger (2019), *Regulating the Information Society: The Future of Privacy, Data Protection, Law, and Consent*, *in* Roger Brownsword ed., LAW, TECHNOLOGY AND SOCIETY: RE-IMAGINING THE REGULATORY ENVIRONMENT. (Oxon: Routledge).
9. Bygrave, Lee A., *Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, 17 COMPUT. LAW SECUR. REV. 17 (2001).
10. Bygrave, Lee A. (2020), *Article 22 Automated Individual Decision-Making, Including Profiling*, *in* Christopher Kuner, Lee A. Bygrave & Christopher Docksey eds., THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY. (Oxford: Oxford University Press).
11. Fan, Mary D. (2019), CAMERA POWER: PROOF, POLICING, PRIVACY, AND AUDIOVISUAL BIG DATA, Cambridge: Cambridge University Press.
12. Feeley, Malcolm M. & Simon, Jonathan (1994), *Actuarial Justice: The Emerging New Criminal Law*, *in* David Nelken ed., THE FUTURES OF CRIMINOLOGY.

元照出版提供　請勿公開散布
(London: Sage).

13. Ferguson, Andrew Guthrie (2017), THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT, New York, NY: New York University Press.

14. Foucault, Michel (1977), DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON, New York, NY: Pantheon Books.

15. Goldenfein, Jake (2019), MONITORING LAWS: PROFILING AND IDENTITY IN THE WORLD STATE, Cambridge: Cambridge University Press.

16. Griffiths, Alex (2019), *The Practical Challenges of Implementing Algorithmic Regulation for Public Services*, *in* Karen Yeung & Martin Lodge eds., ALGORITHMIC REGULATION. (Oxford: Oxford University Press).

17. Hu, Margaret (2017), *Biometric Surveillance and Big Data Governance*, *in* David Gray & Stephen E. Henderson eds., THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW. (New York, NY: Cambridge University Press).

18. Kahn, Jeffrey (2017), *Terrorist Watchlists*, *in* David Gray & Stephen E. Henderson eds., THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW. (New York, NY: Cambridge University Press).

19. Liu, Han-Wei, Lin, Ching-Fu & Chen, Yu-Jie, *Beyond State v Loomis: Artificial Intelligence, Government Algorithmization and Accountability*, 27 INT. J. LAW INFO. TECH. 122 (2019).

20. Murphy, Maria Helen (2019), SURVEILLANCE AND THE LAW: LANGUAGE, POWER AND PRIVACY, Oxon: Routledge.

21. Pasquale, Frank (2018), *Paradoxes of Privacy in an Era of Asymmetrical Social Control*, *in* Aleš Završnik ed., BIG DATA, CRIME AND SOCIAL CONTROL. (Oxon: Routledge).

22. Solove, Daniel J., Rotenberg, Marc & Schwarz, Paul M. (2006), INFORMATION PRIVACY LAW (2d ed.), New York, NY: Aspen Publishers.

23. Timan, Tjerk & Oudshoorn, Nelly, *Mobile Cameras as New Technologies of Article Surveillance? How Citizens Experience the Use of Mobile Cameras in Public Nightscapes*, 10 SURVEILLANCE & SOCIETY 167 (2012).

元照出版提供 請勿公開散布
24. Timan, Tjerk, Newell, Bryce Clayton & Koops, Bert-Jaap (2017), *Introduction: Conceptual Directions for Privacy in Public Space*, *in* Tjerk Timan, Bryce C. Newell & Bert-Jaap Koops eds., PRIVACY IN PUBLIC SPACE: CONCEPTUAL AND REGULATORY CHALLENGES. (Cheltenham: Edward Elgar).

25. Veale, Michael & Edwards, Lilian, *Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling*, 34 COMPUT. LAW SECUR. REV. 398 (2018).

26. Warren, Samuel D. & Brandies, Louis D., *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

元照出版提供　請勿公開散布

Research on Automated Facial Recognition Technology System and Personal Data Protection: Lessons from Bridges v CCSWP and SSHD

Yi-Hung Weng*

Abstract

This article aims to explore possible personal data protection disputes in relation to the governmental application of the Automated Facial Recognition technology (AFR) in large-scale surveillance. To deal with this, the essay takes the world's first relevant case *Bridges v CCSWP and SSHD* decision of the UK as a departing point to analyze the requirements and actual implementation of legal governance strategies in the data protection regime when Taiwan promotes the application of AFR to the government's anti-crime prevention and other purposes.

With this in mind, the issues studied in this article are as follows: First, what inspiration can the *Bridges* case bring? Secondly, what are the disputes caused by AFR in the concept of the legal framework for

* Associate Professor, College of Law, Shih Hsin University; Ph.D. in Law, School of Law, Durham University, UK.

Received: January 13, 2021; accepted: September 17, 2021

元照出版提供 請勿公開散布
personal data protection? How should we respond?

This article believes that when thinking about any decision-making by scientific and technological methods, it is necessary to adopt certain methods to reduce the risk of competing rights BEFORE balancing the competing rights. Moreover, when government agencies want to transfer the people's trust relationship based on democratic procedures, even if the transferred objects are non-humans such as automated systems or AI, they still transform the trust relationship. In this regard, there is a need for stronger consolidation and supervision of the legal system, procedures, as well as an appropriate institutional framework.

Keywords: Facial Recognition, AI, Data Governance, Data Protection, GDPR, the Right to Privacy, Tech Governance, AFR