

國立臺灣大學進修推廣學院事業經營法務碩士在職學位學程

碩士論文



Professional Master's Program of Law in Business Administration

School of Professional Education and Continuing Studies

National Taiwan University

Master Thesis

人工智慧發展下資料運用與個人資料保護之研究

-以自駕車為例

A Study on Data Application and Personal Data
Protection in Artificial Intelligence Application

-Take the Automated Vehicles as the example

黃國忠

Kuo-Chung Huang

指導教授：黃銘傑 博士

Advisor: Ming-Jye Huang, Ph.D.

中華民國 111 年 4 月

April 2022



國立臺灣大學碩士學位論文
口試委員會審定書

人工智慧發展下資料運用與個人資料保護之研究
-以自駕車為例

A Study on Data Application and Personal Data Protection
in Artificial Intelligence Application
-Take the Automated Vehicles as the example

本論文係黃國忠君(P08E42023)在國立臺灣大學事業經營法務碩士在職學位學程完成之碩士學位論文，於民國 111 年 04 月 29 日承下列考試委員審查通過及口試及格，特此證明。

口試委員：

黃錦傑

(指導教授)

王偉霖

莊弘鈺

李若凡

所 長：

中華民國 111 年 4 月 29 日

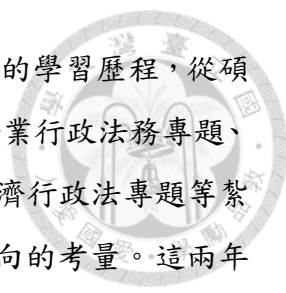
誌謝



從台大電資學院博士畢業後，沒想到我再次回到母校不同學院修讀法律專業。此論文研究主題在我腦中已浮現多年，人工智慧自駕車之個資議題牽涉廣泛且深入，為了能更瞭解這題目的細節，並克服不同領域的鴻溝，研究期間除了研讀文章及判例、訪談許多相關的研究或從業人員，個人並通過考核成為國際大廠探索機械學習課程(GwG – Explore ML)種子講師，在教學相長之間更深入瞭解人工智慧/機械學習的進展與限制；為了最後章節之完備，亦在論文撰寫最後階段同時間完成由人工智慧學校舉辦，中研院孔祥重院士親自講授的人工智慧加速器課程，透過課程確認本文在現階段結論之嚴謹。期待如此耕耘下，這篇論文內容能奠基學理並貼合產業發展趨勢。

論文能從一步一步寫作到完成，非常感謝指導老師黃銘傑特聘教授。謝謝黃老師在這兩年多來寫作指導與論文方向的提點，讓論文能有更加明確的框架。從構想、大綱、撰寫到最後論文修改，黃老師的指點常常能令人茅舍頓開，最後論文論述收斂之提點，更是有畫龍點睛之效。黃老師在科技法律上學有專精，親切誠懇且思想開明，給予學生自由發揮的空間。每次請教黃老師總是給我滿滿的收穫，令人如沐春風。兩年多課業的薰陶與論文撰寫磨練，對我個人法律素養之奠基有非常大的幫助，學生國忠銘感在心。另外也要感謝兩位論文的口試委員，資策會科法所王偉霖所長及陽明交大科所法莊弘鈺副教授百忙中審閱本論文，兩位委員都是國內科技法律界的翹楚，在科法研究上成就卓著。資策會科法所亦為我國科技法律領域重要幕僚單位，曾經承接經濟部「無人載具科技創新實驗推動計畫」並協助無人載具實驗之推動，對於本文所涉及之政策法規知之甚詳。兩位委員的審查更是讓本人如履薄冰，委員所提之問題都能直指問題核心，感謝兩位委員的指教與提點讓本文論點更完整。

台大 PM 學程「有名的是老師」、「豐富的是課程」、「精彩的是同儕」。學程入選之同學們皆為各行各業一時之選，術有專攻。跨行業間實務經驗的相互學習，截長補短，除能瞭解不同領域的產業、開拓自己的人生視野高度與廣度，也讓本文能



夠以更高、更廣與更前瞻的視野來探索。回首這兩年多法務碩士的學習歷程，從碩一暑期基礎的財務報表分析、管理概論、企業相關民刑法專題、企業行政法務專題、企業商事法律專題到碩二的經營策略與法律、智財產業專題、經濟行政法專題等紮實的課程訓練，一步一腳印；跨學門的激盪，也讓本文有更多面向的考量。這兩年多來在學程所有的老師的教導與同學的關愛讓我感受學業上的充實與人際互動上的幸福。另外，特別感謝同門的同學們，這兩年多求學與撰寫論文一路上，對我的照顧與關心。感謝同門優秀的明志、威汎、瑞鴻及志瑋同學，在成立群組中互相分享訊息、資料交流，相互學習成長。在碩士論文撰寫之外，學程中同組並肩作戰的108級懋億、委正、佳惠、翰選、雨潔及麒真；109級的儒霖、咸明、武諺、大為、伊莉及穎楨；110級的順彬、展鵬、康偉、育菁、其翰及耕燦，同組同儕間群策群力，和衷共濟一同完成作業，在不同背景的同學激發下文思泉湧，綵筆生花。感謝這些同學在這段日以繼夜、焚膏繼晷、逐字逐句撰寫，反覆修改論文的艱困時光互相鼓勵，共同攜手熬過這段紮實的學習旅程。

最後謝謝我太太瓊玉與女兒，在這兩年多的台大忙碌學業期間給予我的陪伴與支持，是我學習過程背後最大的支撐。

黃國忠 謹識

於 台灣大學

中華民國 111 年 4 月

中文摘要



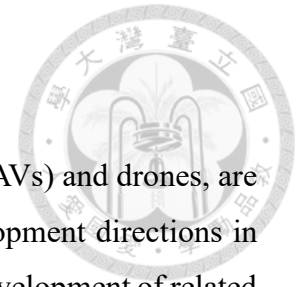
無人載具，包含自動駕駛車輛及無人機等是已商品化的科技產品，並為各國及眾多廠商重要的發展方向，然而因為技術發展快速、影響層面不斷擴大及牽涉到生命安全，無人載具的資料法規研究有相當大的探索空間，特別有關載具科技、資料、個資及隱私間的研究。本文以個人資料保護角度探討自動駕駛車輛之資料運用。

自駕車被市場廣泛看好，並且已有多款商品化產品。自駕車集先進軟硬體技術於一身，被視為一台「移動的超級電腦」，近年來在快速成熟人工智慧技術推波助瀾下，更是如虎添翼，百花齊放的先進技術再再挑戰現行法規。自駕車資料法規研究的重要性在於：(一).自駕車深入生活，影響深遠；(二).巨量資料且更加以聯網車輛間資料之結合；(三).隱密不易被察覺；(四).事關安全，管理須謹慎；(五).人工智慧技術採用之必要；(六).法律上之「蒐集」、「處理」到「利用」行為難切割；(七).人工智慧模型資料須更新，監管困難；(八).人工智慧運用下資料與模型在地化；(九).少有對車外的資料或個資之探討；(十).自駕車目前以企業為主導，若為追求商業利益而運用個人資料者，將與個人權益有所衝突；(十一).國際已有自駕車個資之規範，相關法制亦應與時俱進，才能行穩致遠。

有鑒於自駕車發展是全球性的競爭，我國雖已於 2018 年通過《無人載具科技創新實驗條例》，目前台灣自駕車開發已進入測試階段，然而台灣現行《個資法》之相關規範是否足以涵蓋現有全球自駕車技術之快速發展與個資保護之趨勢？本文最後從企業責任與自我要求角度，以設計隱私 (privacy by design) 的概念應用到自駕車開發商或營運商應該要有的企業內部管理與企業責任。本文擬透過相關文獻先行定義出自駕車資料涵蓋之個資議題，其後透過分析與各國法規之比較，針對自駕車資料及個資議題提出管制之利與弊整理分析，以期未來在我國自駕車資料蒐集、處理及應用等議題之規範能夠貢獻出綿薄之力，並期待能夠提出實質有效的結論與建議。

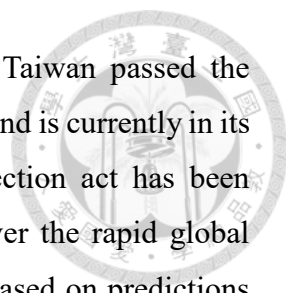
關鍵字：人工智慧、機械學習、無人載具、自駕車、個人資料、個資法、隱私

ABSTRACT



Nowadays, unmanned vehicles, such as Automated Vehicles (AVs) and drones, are commercialized technological products, which are important development directions in various countries and for many manufacturers. However, the rapid development of related technology and its expanded influence can threaten personal safety and privacy. Considerable research can be done on the data regulations of unmanned vehicles, especially regarding personal data and privacy. This study discusses the data usage for AVs from the personal data protection perspective.

Automated Vehicle has a bright future in the market. Many major manufacturers and countries regard the development of AVs as an important direction of development, and many commercialized products already exist. Automated vehicles integrate advanced software and hardware and can be viewed as a “mobile supercomputer,” and such flourishing technology can challenge current laws and regulations. Self-driving technology can be divided into six levels, from zero to five, according to its degree of automation, ranging from the ubiquitous collision warning system to fully automatic driving similar to scenes depicted in the science fiction series Knight Rider. Behind all these self-driving technologies are a huge amount of raw data and calculations. Research on AVs data regulations should be done for several reasons: 1) Automated vehicles may become an integrated part of our lives and cause a far-reaching impact; by 2025, AVs in the automotive market are predicted to reach a penetration rate of 13%, and will continue to rapidly increase each year. Automated vehicles will roam the streets collecting and processing huge amounts of data, and will impact the country, society, and people; we have to be cautious when discussing the impact. 2) The sheer amount of data. 3) Data gathering can be secretive and difficult to detect. 4) It is a matter of safety. 5) Reliance on artificial intelligence. 6) Laws do not differentiate well enough between capturing, processing, and utilizing data. 7) Data need to be updated and is hard to regulate. 8) The localization of data and the models. 9) only a few discussions on the personal data collected outside of the car. 10) The development of AVs is mainly led by companies, and they could have different ideas that could cause disagreements on how personal data should be used. 11) There are relevant international AVs Data Protection regulation.



The development of AVs is a global competition. In 2018, Taiwan passed the “Unmanned Vehicles Technology Innovative Experimentation Act”, and is currently in its testing phase for AVs. However, although the personal data protection act has been revised twice in 2010 and 2015, are the regulations enough to cover the rapid global development of AVs? Currently, Taiwanese laws on AVs are made based on predictions of what the technology may look like in the future. Is it necessary to do a rolling review of the development of self-driving technology and change the regulations accordingly? In addition, from the perspective of corporate responsibility and self-discipline, the concept of “privacy by design” can be applied to the companies that develop and operate AVs. This study first identifies the problem surrounding the discussion on data collected by AVs in the relevant literature, then analyzes and compares the relevant discussions, guidelines, regulations, and drafts of various countries on AVs data and personal data. We analyze the pros and cons in the hopes that this study can provide a helpful conclusion and effective suggestions in the future regarding how AVs can collect, processing and use data in our country.

Keywords: Artificial Intelligence, Machine Learning, Unmanned Vehicles, Automated vehicles, personal data, personal data protection act, privacy

目 錄



口試委員審定書.....	I
誌謝.....	II
中文摘要.....	IV
ABSTRACT.....	V
目 錄.....	VII
圖目錄.....	XVI
表目錄.....	XXI
第壹章 緒論.....	1
第一節 研究動機與目的	1
第一項 智慧自駕車是未來趨勢，具有多重的價值與意義	1
第二項 生命法益為優先考量，個資保護與利用間平衡更複雜	2
第三項 人工智慧應用於自駕車	4
第四項 自駕車亦是智慧城市的一環，集合先進科技與匯集多元資料的移動電腦	5
第五項 智慧自駕車再次衝擊個資保護規範	7
第六項 國際已有自駕車個資管理規範	8



第七項 本文研究目的	9
第二節 研究方法	10
第三節 研究範圍與限制	12
第四節 研究架構及章節順序	13
第五節 專有名詞、術語、法律用語與標準符號使用說明	18
第貳章 人工智慧與自駕車概觀.....	21
第一節 前言	21
第二節 人工智慧、自駕車與個資法	24
第一項 人工智慧技術簡介	24
第二項 無人載具的定義與自駕車發展	36
第三項 資料是石油	70
第四項 個資與隱私	83
第三節 各國自駕車政策與法規規範	103
第一項 美國自駕車政策	103
第二項 德國自駕車政策	113
第三項 日本自駕車政策	124
第四項 英國自駕車政策	126
第五項 新加坡自駕車政策	128



第六項	中國大陸自駕車政策	134
第七項	聯合國 UN-R157	136
第八項	台灣自駕車主要政策與實驗條例	137
第九項	自動駕駛測試計畫與場域發展案例	142
第十項	不同國家地區自駕車政策法律比較	145
第參章 個人資料保護相關法規.....		149
第一節 中華民國個人資料保護法簡介		149
第一項	立法歷史	149
第二項	個人資料保護法立法目的	154
第三項	敏感性個資定義	154
第四項	資料自決權	155
第五項	「資料可識別性」與「個資去識別化」概念之區分	156
第六項	「資料可識別性」的判斷標準	157
第七項	個資法排除適用情形	158
第八項	現行個資法重點	160
第九項	我國個資法與聯網車	160
第二節 歐盟《一般資料保護規範》(GDPR)		162
第一項	《一般資料保護規範》(GDPR)簡介	162

第二項	GDPR 與我國個資法之比較	168
第三項	GDPR 針對聯網車之規範	172
第三節 中華人民共和國《民法典》與《個人信息保護法》		177
第一項	背景介紹	177
第二項	中國個資法重點	181
第四節 中華人民共和國汽車數據安全管理若干規定（試行）		188
第一項	更廣泛的適用範圍和對象	188
第二項	個人信息的界定	189
第三項	敏感個人資料	189
第四項	重要資料的範圍	190
第五項	車輛資料處理基本原則	191
第六項	汽車行業特殊資料蒐集規定	192
第五節 《數據出境安全評估辦法》		197
第六節 敏感性個資比較		198
第一項	敏感性個資規範差異	198
第二項	例外得蒐集之合法事由	199
第七節 境外傳輸比較		202
第肆章 人工智慧自駕車無人載具與個資權益影響.....		204



第一節 人工智慧、自駕車發展與個人資料總覽	209
第一項 人工智慧應用於自駕車	210
第二項 人工智慧與個人資料之關聯探討	216
第三項 自駕車與個人資料之關聯探討	222
第四項 人工智慧自駕車的個資問題小結	223
第二節 對車內駕駛及乘客個資保護之規範	225
第一項 對駕駛或者乘客的個資蒐集是否有公眾利益與保護生命法益之目的?	228
第二項 資料是否等同於個資?人工智慧與大數據下的挑戰	229
第三節 公開場合個資保護近似案例探討	229
第一項 Google 街景圖	231
第二項 街口傳統監視器	235
第三項 影像式行車紀錄系統	239
第四項 聯網車所拍攝之車牌	240
第五項 防疫足跡	241
第六項 以當事人權益無侵害作為合法事由之判斷依據	242
第四節 自駕車與個資保護之探討	242
第一項 生命法益之保護	243
第二項 個資保護、社會公益與生命法益	247

第五章 個人資料保護法與人工智慧機械學習驅動自駕車之 調和探討..... 248

第一節 技術與產業發展對個資法之挑戰 248

- 第一項 資料與資訊(Data and Information) 249
- 第二項 數據或資料 253
- 第三項 「個人資料」是否真實無誤(True or Proved)? 255
- 第四項 「個人資料」中資料與個人關聯性探討(Relating to) 256
- 第五項 明文例示的個資是否就屬於直接識別性個資 261
- 第六項 已識別或足資識別(identified or identifiable) 261
- 第七項 辨識的主體 262
- 第八項 個人資料分類 265
- 第九項 個資法排除適用討論 268
- 第十項 人工智慧機械學習驅動之自駕車再次挑戰個資法 270
- 第十一項 資料、個資與個資法適用說明 279

第二節 社會公益與私人個資權益取捨 280

- 第一項 個資保護與個資法保障 281
- 第二項 公益性的討論 281

第三節 法令遵循與風險管控 282



第一項	智慧自駕車個資風險	282
第二項	自駕車個資法令遵循原則	285
第三項	生物特徵辨識之監管	291
第四項	跨境規範	292
第四節 隱私設計(Privacy By Design)理念的導入		295
第一項	個人資料保護、合理利用與隱私權保護	295
第二項	隱私設計(Privacy By Design)介紹	296
第陸章 結論與未來展望		300
第一節 自駕車趨勢不可擋，回首電腦網路發展時刻		301
第一項	自駕車的發展不但是現在進行式，亦是共識的未來趨勢	301
第二項	回首電腦資料處理保護法，移動電腦的個資法規再次審視	302
第三項	生命法益的保護	303
第四項	過分強調資料管控，可能阻礙科技發展	305
第二節 自駕車的議題錯綜複雜，資料管理需要更重視		306
第三節 國際已看到自駕車個資議題，值得台灣借鏡		309
第四節 本文之建議		310
第一項	非公務機關的建議-隱私設計為核心	310
第二項	本文對公務機關的建議	315

第五節 其他展望

- 第一項 個資定義更廣泛 319
- 第二項 生物特徵辨識為敏感性個資，各國有更嚴格管制趨勢 320
- 第三項 超越隱私，資料已被列為國家資產，甚至攸關國家安全 321



參考資料.....	325
期刊	325
研討會論文	328
學位論文	329
專書	330
網路資源與媒體報導	332
研究報告	341
研討會	344
專利	345
紀錄片	346
附錄(I)：符號與標註說明.....	347
附錄(II)：汽車數據安全管理若干規定(試行).....	349
附錄(III)：雙語詞彙(依英文字母排序)	355

附錄(IV)：法務部函釋整理..... 360

索引..... 364



圖目錄



- 圖 1. 自駕車為新興科技的結合，並會形成一個自駕車網絡，運作巨量且多元的資料。資料來源：《自動化和網聯化車輛交通倫理準則》.....6
- 圖 2. Smart Intersection 技術。資料來源：Honda 7
- 圖 3. 本論文主題圍繞在自駕車-人工智慧/機械學習(AI/ML)-個資/隱私三大區塊。資料來源：本文整理..... 10
- 圖 4. 人工智慧應用於自駕車市場預測。資料來源：Mind Commerce(2019);工研院產科國際所(2020/12)..... 23
- 圖 5. 人工智慧(AI)的三波演進，目前第三波是以機械學習(ML)演算法為基礎。資料來源：Business Science..... 27
- 圖 6. 人眼與電腦視覺在影像分類上的競賽，人工智慧在 2014~2015 間後就擊敗了人類。資料來源：ImagNet;本文整理 29
- 圖 7. 人工智慧(AI)、機械學習(ML)與深度學習(DL)的發展年代與定義。資料來源：Oracle;本文整理 30
- 圖 8. 傳統規則性(Rule-based)與機器學習(ML)演算法的差異，在於機器學習(ML)利用數據來訓練模式(Model)，而非由程式設計人員預先給定規則。資料來源：Google;本文整理 31
- 圖 9. 深度學習的運作方式。資料來源：Simplilearn;本文整理..... 33
- 圖 10. 機械學習(ML)運作需要三個步驟：包含蒐集資料、訓練模式(Training Model)及實際運用;圖右為傳統統計方式。資料來源：本文整理 34
- 圖 11. 感測器特性、應用距離、價格及網路速度之比較。資料來源：STPI;科技發展觀測平臺。 43
- 圖 12. 每 100 萬英里的行駛里程數出現事故次數，數據顯示自駕車(<1)相較人為操作(>2)可大幅降低車輛事故。資料來源：Tesla(2020) 44
- 圖 13. 自駕車所創造消費者與社會利益，2050 年預估可達 800 Billion

美元。資料來源：SAFE; David Montgomery	45
圖 14. 自駕車的理念發展已超過 60 年。資料來源：VeloceToday.com	47
圖 15. 宣稱擁有 SAE L3-L5 自駕車(AV)廠商，至 2021 年有超過 10 家 車商擁有 L3 以上車輛	51
圖 16. 人工智慧/機械學習運用於自駕車法的流程架構。資料來源： Mind Commerce(2019)；工研院產科國際所(2020/12).....	52
圖 17. SAE 定義的自駕車(AV)自動化程度程度與責任分工。L3-L5 被 稱為高自動化自駕車，也代表著越仰賴智慧化技術。資料來源：SAE International;科技發展觀測平臺	55
圖 18. 車聯網技術示意圖。資料來源：工研院.....	63
圖 19. 自駕車感應器與涵蓋範圍。資料來源：WEVOLVER	65
圖 20. 自駕車會遇到不同的緊急狀況，對於單一物件的警示須透過不 同感測器並將影像融合以作為後續動作判斷。資料來源：Intellias Global; 本文整理	66
圖 21. 高精地圖態樣，不論解析度或維度上遠高於 Google 地圖。資料 來源：科技新報.....	68
圖 22. 資料處理流程。不同原始資料、不同模型與不同任務目標都直 接影響結果。資料來源：本文整理.....	75
圖 23. 統計與人工智慧的結合，成為統計學習，能處理更多變量且達 成更多目的。資料來源：本文整理.....	76
圖 24. 深度學習(DL)可輸入多變量/不同特徵之資料。資料來源： Playground.Tensorflow;本文整理	77
圖 25. ML/DL 在商業上應用。資料來源：Carlos Martinez;本文整理	78
圖 26. 資料與個資管理，圍繞在個資保護-資料運用及生命法益保護三 者。資料來源：本文整理.....	83
圖 27. 「個人資料」、「資訊隱私權」及「隱私權」三者性質與關係。	

資料來源：本文整理.....	101
圖 28. 美國官方指定測試區。資料來源：ARTC.....	105
圖 29. AVCP 的架構。資料來源：DOT.....	111
圖 30. 日本 SIP-adus 計畫。資料來源：車輛中心.....	125
圖 31. 東南亞地區第一個自動駕駛測試中心 CETRAN。資料來源：CETRAN.....	131
圖 32. 新加坡的緯壹(One-North)園區的自駕車服務測試計畫。資料來源：iThome.....	133
圖 33. 台灣自駕車政策之中央與地方跨部會配套規劃。資料來源：經濟部(2019/5).....	138
圖 34. 2021 年各國自駕車最高測試等級概況。資料來源：科技發展觀測平臺.....	144
圖 35. 主要國家自駕車規範比較。資料來源：科技發展觀測平臺;本文整理.....	147
圖 36. 個人資料保護法立法歷程與重要大法官釋字。資料來源：立法院法律系統;司法院判決書查詢系統;本文整理.....	153
圖 37. 個資法三讀時加入該法第 51 條第一項第 2 款。資料來源：立法院公報第 99 卷第 29 期院會紀錄，立法院法律系統.....	159
圖 38. 我國現行個資法、重要判例與 GDPR 施行之時間。資料來源：本文整理.....	169
圖 39. 聯網車擁有許多資料，其中包含許多個人資料。資料來源：EDPB;本文整理.....	173
圖 40. 生活中不同 STOP 警示，這些不同的單一警示牌告對人類容易辨識，但對於傳統規則式演算法卻是難以駕馭。資料來源：Grow with Google, Google.....	212
圖 41. 自駕車基本要具有可以辨識交通號誌、車輛及用路人之障礙物偵測系統.....	214

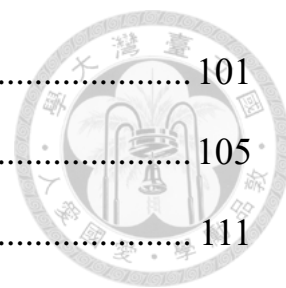



圖 42. Tesla 增強版自動輔助駕駛。資料來源：Tesla 網站.....	215
圖 43. 駕駛生物特徵偵測，包含人臉、聲音、心跳等一般及敏感個資。 資料來源：IEEE;本文整理.....	221
圖 44. 自駕車-人工智慧-個資三者間關聯與必要性表示圖。圖中紫色 字體為先前文獻已有初步探討，本文補充;紅色字體為本文提出。資料 來源：本文整理.....	224
圖 45. Google 街景圖爭議圖片。資料來源：Privacy Rights in the Age of Street View	233
圖 46. 全球 2020 年行車紀錄器使用概況。資料來源：VIA	240
圖 47. 對於複雜的路況，首先要標示出車輛及用路人等重要物件。資 料來源：Nvidia.....	244
圖 48. 自駕車偵測到用路人後(圖左)，再以偵測人眼以判斷行為是否 有注意到車輛(圖右)，資料來源：US10082796B2	245
圖 49. 用路人人臉偵測與自駕車動作判斷，資料來源：US10082796B2	245
圖 50. 自駕車除偵測用路人外，並依據人臉與步態辨識判斷 1.行為對 車輛的警覺程度(Awareness)及 2.過馬路的意願(Intention)。資料來源： Hyundai	246
圖 51. 在本文智慧自駕車的應用環境下，是權衡個資保護-社會公益- 生命法益三者。資料來源：本文整理.....	247
圖 52. 原始資料、資料、資訊到知識。資料與資料以知識管理、人工 智慧/機械學習、大數據觀點都具不同意涵。資料來源：本文整理...	252
圖 53. 真實的笑容判斷。特徵為 1. 眼角皺紋;2.臉頰鼓起及 3.眼睛周圍 肌肉運動。資料來源：《每日頭條》;本文整理.....	255
圖 54. 我國個資法實施細則修正草案對照表，黃底部分但書並沒有被 列入最後版本。資料來源：法務部.....	258
圖 55. 重要技術發展、個資法及重要判例以時間軸展開。資料來源：	

本文整理.....	271
圖 56. 資料、個資與個資法適用流程圖。資料來源：本文整理.....	280
圖 57. 「隱私」、「個資」、「個資法所謂之個資」及「資料」間關係。資料來源：本文整理.....	296
圖 58. 隱私、個資保護與重要科技發展歷史回顧。資料來源：本文整理.....	303
圖 59. 人工智慧自駕車個資討論，在個資保障-個資合理利用-生命法益三者間所衍生的議題。資料來源：本文整理.....	305
圖 60. Facebook 刊登在多家報社的聲明。資料來源：Facebook.....	312
圖 61. 在現今國際局勢的演變下，資料/個資的保護與運用更形複雜。資料來源：本文整理.....	324

表目錄



表 1. 人工智慧大事記。資料來源：數位時代;本文整理	35
表 2. 各種感測器之優缺點比較。資料來源：工研院資通所	42
表 3. 具各種感測器之自駕車至 2050 年產生的公眾與消費者利益預估 達美元 796B。資料來源：SAFE;本文整理	46
表 4. SAE 所定義之自駕車等級。資料來源：SAE	54
表 5. 自駕車邊緣運算需求。資料來源：陳右怡，IEK(2018);本文整理	64
表 6. 不同格式與儲存容量。資料來源：本文整理.....	71
表 7. 不同國家地區對個人資料/資訊的規定。資料來源：各國法規資料 庫;本文整理.....	84
表 8. 四種隱私基本侵害態樣及展開的 16 種隱私問題。資料來源： 《Understanding Privacy》，本文翻譯/整理.....	90
表 9. 美國交通部(DOT)公告的自動駕駛政策。資料來源：DOT;NHTSA; 本文整理更新.....	106
表 10. FAVP 與 ADS 2.0 比較。資料來源：FAVP;ADS;資策會 MIC;本文 整理更新.....	107
表 11. 德國自駕車《倫理指南》之 20 項倫理準則。資料來源：科技法 律透析，本文整理更新 2017 年版本.....	115
表 12. 無人載具科技創新實驗條例內容綱要。資料來源：立法院法律系 統;行政院;本文整理.....	140
表 13. 一般個資與敏感個資依據《個資法》處理方式.....	155
表 14. GDPR、我國個資法與本文名詞使用。資料來源：GDPR;我國《個 資法》;本文整理.....	169
表 15. GDPR 與我國現行《個資法》之基本項目比較。資料來源：GDPR;	



《個資法》;我國法院判決;本文整理	171
表 16. Guidelines 01/2020 版本歷史	173
表 17. 《汽資安全規定 (試行)》個資保護整理。資料來源：本文整理	195
表 18. 例外得蒐集之合法事由。資料來源：本文整理.....	199
表 19. 中國個資法及 GDPR 對於境外傳輸規定之比較。資料來源：各 國個資主管單位網站;本文整理.....	203
表 20. 不同演算法比較。資料來源：本文整理.....	211
表 21. 安全必要性觀點探討技術對個資資料處理原則可能衝擊。資料 來源：本文整理	225
表 22. Data 與 Information 意涵與關係整理。資料來源：Anthony Liew; 本文整理	250

第壹章 緒論



第一節 研究動機與目的

第一項 智慧自駕車是未來趨勢，具有多重的價值與意義

以人工智慧(Artificial Intelligence, AI)驅動之自動駕駛車(Automated Vehicle, AV。以下簡稱自駕車)，又被稱為電腦駕駛車或者無人車。自駕車集合最頂尖、最新穎的軟硬體技術，配合人工智慧的大腦操控，顛覆過去的交通運輸型態，逐步落實在現實生活中交通運輸¹。也因為集合先進技術於一身，被稱為「移動的超級電腦」²。自駕車能夠讓道路的利用率大幅提高 200%，也能夠降低 90%的人為交通事故³，對於未來交通及社會有重大的影響。自駕車的出現和廣泛的應用將是本世紀的一個重大革命，不僅引發新的產業革新和社會變革，而且會改變許多傳統社會生活型態和顛覆人們對於交通運輸的觀念。近年來，自動駕駛技術成為各傳統汽車大廠、科技巨頭甚至是各國家競逐的領域，各國公務機關並因應自駕車之推動而制定許多自駕車政策及法案；在技術上，包含先進輔助駕駛系統(Advanced Driver Assistance Systems, ADAS)到高度自駕車系統(Automated Drive System, ADS)，應用的科技包括物聯網(Internet of Thing, IoT)、5G 高速傳輸、感測技術、大數據(Big Data)、雲端計算(Cloud Computing)、邊緣運算(Edge Computing)、人工智慧(Artificial Intelligence, AI)和智慧型運輸系統等，並連結已有的智慧城市提升整體都市運作效率，社會發展與經濟成長之誘因將原本在研究學術領域的知識，結合快速發展的先進技術逐漸將自駕車，特別是高度自駕車推向商業化。自駕車目前除了已在公路道

¹ CBInsights (2021/09/09). *Tech Market Map Report — Autonomous Driving Tech In Auto & Mobility*. <https://www.cbinsights.com/research/report/tech-market-map-report-autonomous-driving-tech-auto-mobility/>

²陳達誠 (2018)，一文看懂自駕車：在路上跑的超級電腦，鉅亨網編譯，載於：
<https://news.cnyes.com/news/id/4249673> (最後瀏覽日：2021/04/13)。

³ The Economist (2012/08/30). *Look, No hands*. <https://www.economist.com/technology-quarterly/2012/08/30/look-no-hands>

路上運行外，還有已經廣泛使用在工廠運輸、採礦、倉庫物流和港口等工業環境中。從提供人類駕駛自動車道維持系統(Automated Lane Keeping System, ALKS)、防撞預警(Pre-crash system, PCS)等不同功能的半自駕車，到沒有方向盤、油門與煞車的全自駕車等，自駕車透過百花齊放的智慧自駕系統之運行，引領相關產業鏈發展和提升社會經濟體系運作效率，也讓交通成為一種更安全、更便利的服務，顛覆現有移動的方式及提升社會整體之運輸效率。自駕車具有廣泛的公益特性，除了能節能減碳，還有減少車禍、避免塞車、降低空氣汙染。除此，老人、未成年人與身障者也能獲得突破性的移動能力⁴，改變弱勢族群生活且更適應未來老化社會之運作。但是，任何的創新科技都有可能造成負面效果，自駕車也不例外，像是造成職業駕駛失業、自駕車交通法規衝擊、新型態車輛安全問題，及本文所要探討的資料濫用與可能侵犯個人隱私等問題⁵。

綜上所述，智慧自駕車具有三大特點：1.生命法益保護優先;2.人工智慧等新興技術導入之必須;3.自駕車也是智慧城市的一環。三大特點使得自駕車的個資問題討論有其複雜性，亦更顯得其研究的重要。以下就此三點做一簡要之概述，若深入探討這些議題對智慧自駕車個資研究的重要性與必要性，需待第二、三章作更清楚背景知識說明之後，一併於本文第四章以後探討。

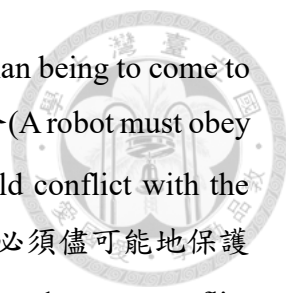
第二項 生命法益為優先考量，個資保護與利用間平衡更複雜

理想的自駕車如同一個有智慧的移動機器人⁶，回顧 1942 年著名科幻小說家愛莎克希莫夫(Isaac Asimov)在其科幻小說《環舞 (Run around) 》中提出了著名的機器人三大原則：第一，機器人不得傷害人類，或坐視人類受到傷害而袖手旁觀(A

⁴ Jenny Cusack (2021/11/30). *How driverless cars will change our world*. BBC News. <https://www.bbc.com/future/article/20211126-how-driverless-cars-will-change-our-world?xtor=AL-73-%5Bpartner%5D-%5Btw.yahoo.com%5D-%5Blink%5D-%5Bchinese%5D-%5Bbizdev%5D-%5Bisapi%5D>

⁵ Hod Lipson & Melba Kurman (著)，徐立妍 (譯) (2019)，《自駕車革命：改變人類生活、顛覆社會樣貌的科技創新》，臺北：經濟新潮社。

⁶ John Frank Weaver (著)，鄭志峰 (譯) (2018)，《機器人也是人：人工智慧時代的法律》，頁 5，臺北：元照出版。




robot may not injure a human being or, through inaction, allow a human being to come to harm);第二,除非違背第一法則,否則機器人必須服從人類的命令(A robot must obey the orders given it by human beings except where such orders would conflict with the First Law);第三,在不違背第一及第二法則下的前提下,機器人必須儘可能地保護自己(A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws)。在具人工智慧之自動駕駛車的實際運作環境中,前述三法則不但是機器人亦是自動駕駛車設計開發必須遵循的基本原則,也是機器人或自駕車立法中必須充分考慮的原則。前述之機器人三大原則亦被落實且擴大在自駕車應用上,德國政府於2017年推出關於自動駕駛技術的首個道德倫理準則⁷,該準則讓自動駕駛車輛⁸針對意外事故場景作出優先等級的判斷,並加入到系統的自我學習中,德國成為了世界上首個實施此類措施的政府。德國為自動駕駛汽車制定的道德倫理準則將於本文有關德國自駕車政策乙節中詳述,在此先摘要與生命法益及資料相關重點如下:

- 如果自動駕駛系統與人類駕駛相較能降低事故發生,那麼該自動駕駛行為即符合道德倫理規範(第2項)。
- 尊重人民自主決定,惟駕駛方責任必須明確(第4項及第10項)。
- 在窮盡現今技術下,相比對動物或財產造成的傷害,系統必須最優先考慮人類安全(第7項後段)。
- 對於道德上模糊的不可避免事件,人類必須重新獲得控制權(第8項)。
- 如果事故不可避免,禁止任何基於年齡、性別、種族或其它的歧視(第9項)。

⁷ 利榮 (2018/05/15),《德國為自動駕駛汽車制定了世界首個倫理規則》,雷鋒網,載於:
<https://www.leiphone.com/category/transportation/4dmzAl3BcpgCUH6t.html>

⁸ 這份方針是為將來的為全自動化(Level 5)自駕車打基礎。此方針針對自動化汽車—指自動化(Level 3)和高度自動化(Level 4)兩種,此兩層級自動化意味著「人類可以在法令範圍內,將車輛掌控權交由AI」。但人類必須保持警覺,以便在AI發出警訊、或是超出系統限制時,立即回復對車輛的控制,因為自駕系統只是輔助性,最終責任仍在人類。

- 
- 汽車必須安裝儲存駕駛記錄的黑盒子，以釐清責任問題(第 16 項)。
 - 在特定條件下對於是否將駕駛資料轉發給相關廠商或供其使用，人類駕駛具有決定權(第 15 項)。

第三項 人工智慧應用於自駕車

自動駕駛車以人工智慧的大腦操控，整合先進技術提升行動之效率及革新安全之保障，是一場本世紀的交通與社會革命，顛覆過去的交通運輸與產業經濟型態，逐步落實成為現實生活中交通運輸一環。人工智慧的導入，是高度自動駕駛車輛能夠實現的重要基礎，無論影像辨識、導航與行為決策，人工智慧技術已被證明可超越人類，且人工智慧能透過不斷的自我學習中，不斷的提升品質。

然而，人工智慧技術，特別是第三代以資料驅動的機械學習(Machine Learning, ML)及其分支深度學習(Deep Learning, DL)，由於計算過程的不透明且難以理解之自動化決策(automated decision-making)，使得人工智慧技術本身也遭受到許多異議，也有許多應當規範或者限制該技術使用的呼籲。

人工智慧運用於自動駕駛車輛的環境下，因為智慧自駕車的運行必須「蒐集」、「處理」及「利用」⁹巨量的資料，由於這些資料因為大都為當事人所產生，資料被濫用時自然會有侵害當事人隱私的疑慮。例如：自駕車可以蒐集駕駛及乘客的影音、行車目的地及停留時間，或者監控沿路上用路人的行動，然後將這些資料做大量的運用。而過去我們確實也看到這些資料在正面利用上的效益，如：可提升自駕車的安全性及優化行車路徑，另可提供給公務機關作為民刑事偵查的依據；但另一方面，這些巨量資料亦可能作為企業商業之利用、剖析當事人內在思惟，或者監控他人之行為等。對於自駕車輛可能侵犯隱私的探討，亦見於先前幾篇國內文章(殷家瑋(2017);廖曼庭(2020))。

⁹ 本文將「蒐集」、「處理」及「利用」三行為簡稱為「蒐用」

第四項 自駕車亦是智慧城市的一環，集合先進科技與匯集多元資料的移動電腦



車聯網亦是「智慧城市」(Smart City)的一環，過去已經有論者討論智慧城市密布的感測器對隱私侵害之隱憂¹⁰，聯網自駕車輛與智慧城市兩者之連結，併同新興人工智慧、大數據及物聯網等技術之導入¹¹，資料處理與運作極其複雜，聯網自駕車之資料監管的重要性不言可喻。

智慧自駕車能夠在道路上正常行駛，在安全的前提下達成運輸與交通任務，過程中須要蒐集、處理及運用巨量且多元的資料，過程中除了單一的自駕車資料透過各種不同先進的感測器持續不斷地去辨識包含車內及車周遭的環境，並以人工智慧/機械學習(Mechine Learning, ML)的演算法即時處理並做出瞬間反應，若是再結合車聯網(Vehicle-to-Everything, V2X)¹²及雲端資料庫，自駕車間與智慧城市連結更會如圖 1 形成一個資訊網絡，自駕車網絡將會運作巨量而多元的資料。車聯網有其安全上的必要，如圖 2 車輛行經街口時的事故發生率非常高，根據美國聯邦公路管理局(Federal Highway Administration, FHA)資料統計，每年該國十字街口的事故數量，佔了總事故數的 40%;交通意外死亡有 4 分之一，意外受傷有一半是發生在十字路口。是故如何降低十字路口的交通事故，也成了政府與車廠的主要目標之一¹³。從圖 2 為廠商所提的 Smart Intersection 技術，自駕車行經街口常有感測死角，從圖中單一車輛技術角度，無論自身何種感測器皆無法正確偵測到轉角移動個人或車輛。該技術透過街口監視器將感應資訊透過車聯網傳送給轉彎車輛，故車

¹⁰ 林妤捷 (2018)，《探討智慧城市之興起與隱私權之調和》，東吳大學法學院法律學系碩士在職專班碩士論文，中華民國 107 年 7 月，臺北。

¹¹ 吳東凌 (2019)，〈技術參訪〉，《出席第 26 屆智慧型運輸系統(ITS)世界年會報告》，交通部運輸研究所，載於：

<https://report.nat.gov.tw/ReportFront/PageSystem/reportFileDownload/C10803042/001>

¹² 林港喬、黃譽維、曾恕康 (2020)，C-V2X 與自駕車結合之應用，工研院資通所，載於：
<https://ictjournal.itri.org.tw/Content/Messagess/contents.aspx?MmmID=654304432061644411&MSID=1073041765432164773> (最後瀏覽日：2022/04/13)。

¹³ AUTOACCIDENT (2021/03/31). *Statistics on Intersection Accidents*.
<https://www.autoaccident.com/statistics-on-intersection-accidents.html>

聯網提供一個避免感測器死角良好的解決方案，感測隱藏在建築物或障礙物後的物體。我國因為人口密集且集中於城市、街道狹小且路況複雜，路上物件包含：汽車、用路人、uBike、一般機器腳踏車、特種車輛、個人移動裝置等，自駕車的操作更形困難，相對的也需要蒐用更多且質精的資料。

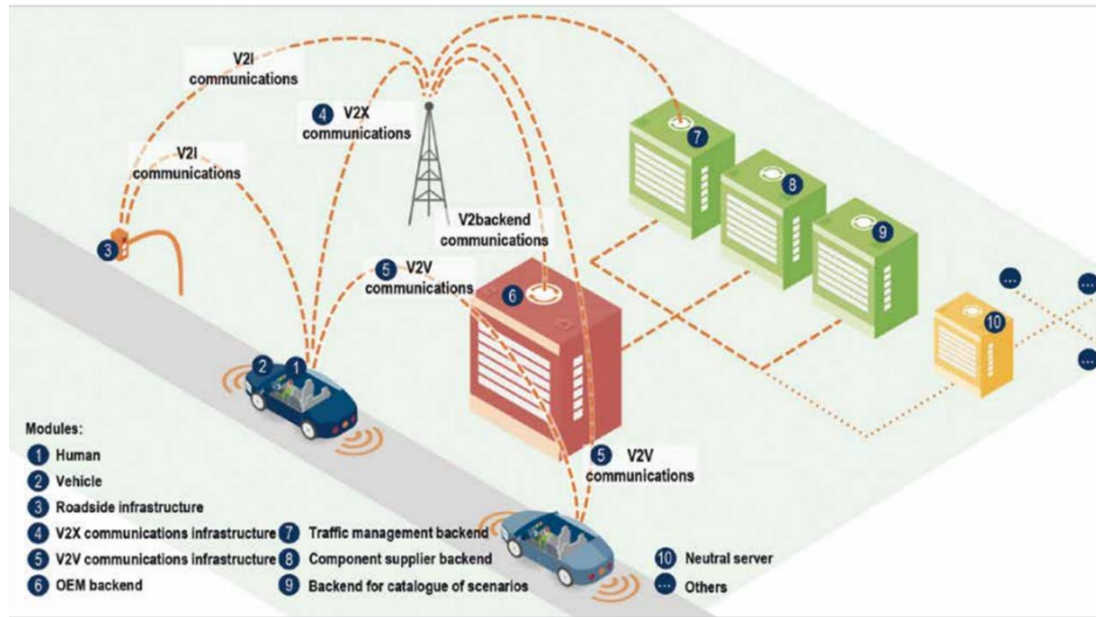


圖 1. 自駕車為新興科技的結合，並會形成一個自駕車網絡，運作巨量且多元的資料。資料來源：《自動化和網聯化車輛交通倫理準則》¹⁴

¹⁴ BMVI (June 2017). *ETHICS COMMISSION AUTOMATED AND CONNECTED DRIVING*, p.27. https://www.bmvi.de/SharedDocs/EN/publications/report-ethics-commission.pdf?__blob=publicationFile

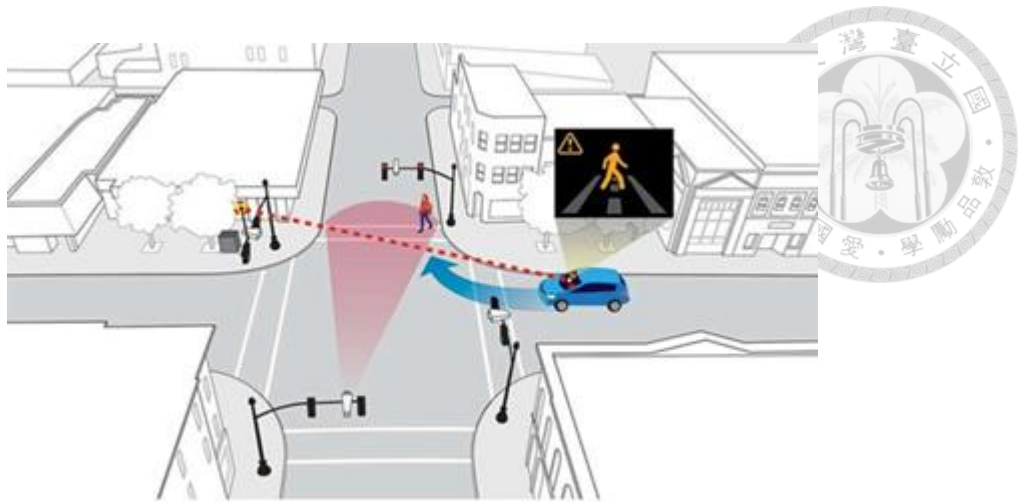


圖 2. Smart Intersection 技術。資料來源：Honda

第五項 智慧自駕車再次衝擊個資保護規範

依我國《個資法》之立法理由，個人資料保護之意涵在於當事人人格權保護與資料合理利用之經濟價值的權衡框架(我國現行《個資法》第一條參照)，資料蒐用之合法基礎包括該當事人事前同意、透明之蒐用過程、符合比例原則、個案經濟利益與個人隱私保護權衡，及合法排除《個資法》適用結果。以車外路人個資為例，人工智慧技術運用下之自駕車運行，為安全或其他特定目的而蒐用個人資料，無論是直接或間接蒐集、一般性或特殊性個資，與當事人相關的各種資料，若能事前告知、徵得當事人事前同意並讓當事人擁有其資料刪除權利，理論上應無太多法律或倫理爭議。然而，在人工智慧/機械學習所需的車外巨量資料規模下，逐筆取得資料當事人之事前同意，對直接蒐集而言，除了取得資料之成本外，更多了取得事前同意的成本；對間接蒐集實務上而言，有幾個顯著窒礙難行之處：1.其一，蒐用目的之前取得同意大幅增加取得成本，這是人工智慧/機械學習之車外路況學習階段資料蒐集的事前同意首要面對之問題；2.其二，人工智慧/機械學習蒐集巨量資料，是否遵守最小化蒐集原則；3.第三，處理的過程不透明與目的不明確；4.第四，自駕車尚有生命法益之保護，在資料利用的模糊地帶，在蒐集、處理與利用上如何評斷比例原則？5.以資料驅動之學習式機械學習演算法，資料之刪除與不完整是否會影響其安全操作？除前述幾點車外資料蒐集外，對於車內駕駛人及使用者之個資，亦有告知、資料結合、車外傳輸、持續性監控等的問題。綜上，相關議題需要更細化的

規範。本文將會針對自駕車內外之隱私個資保護及資料蒐集、處理與利用問題作更
基詳的探討。而我國個人資料保護法規尚無針對智慧自駕車個資蒐集、處理與利用
有細部的規範，使得智慧自駕車的個人資料保護尚有許多待探討的空間，也讓智慧
自駕車企業在國際上推廣時存在個資法遵風險。

回顧 1994 年台灣《電腦處理個人資料保護法》的立法背景，始於當時電腦的
崛起促使資料數位化(digitalized)，變得資料容易被儲存、蒐集、處理、傳輸與運用。
也使得資料運用與個人資料權益間的衝突逐漸被重視。時至 21 世紀，更多新興科
技如人工智慧、物聯網、雲端計算、大數據及邊緣運算等被運用在被視為「移動的
超級電腦」上，巨量資料除了被大量蒐集外，在處理、傳輸與運用上，資料的多樣
性及相關技術水準遠非 1990 年代可想見。此外，現今《個資法》在於個資保護與
促進資料運用兩者間平衡，過去案例還是在於以比例原則來權衡，然而自駕車具有
保護生命的重要使命，在生命保護、資料運用與個資保護的多方考量，自有探討的
必要性。

第六項 國際已有自駕車個資管理規範

2021 年包括歐盟《一般資料保護規則》(General Data Protection Regulation, GDPR) 的《聯網車輛與移動相關產品涉及個人資料處理指南》及同年 10 月中
國的大陸的《汽車數據安全管理若干規定(試行)》已論及針對車輛的個人資料保護。
前者對雖名為針對聯網車之規範，但已經理解到聯網車輛包含智慧自駕車所造成
的隱私侵害新衝擊，且兩者皆看到了自駕車的資料巨大及聯網功能所造成對個資
及隱私的可能影響，除了在自駕車運用下更清楚的定義一般個資與敏感性個資、資
料車內處理原則，對於車內及車外的個資也都涵蓋於其中。

上述針對自駕車資料及個資之規範對象，因為涵蓋自駕車整體產業鏈，我國
相關企業應該投入法令遵循之資源，對於公務機關，可做為我國自駕車或無人載具
規範之借鏡。

第七項 本文研究目的

自駕車網路之資料運用不論是否經過個資當事人或不特定第三人之同意，都會隱含著對駕駛、乘客及用路人各種行為的監視，且自駕車目前以民營企業為主導，資料與個資運用在以營利為前提下，有相當大的可能性會與個人隱私保護或社會公益有所衝突。隨著自駕車的技術不斷提升，而越來越多的功能被整合在一起且資料被長期紀錄，資料間的結合也更容易辨識出特定族群及利於個人檔案剖析 (profiling)之執行;此外，自駕車的滲透率逐年快速提升，自駕車所蒐集的其他片段或廢棄資料也可能透過自動化處理拼湊出個人資訊，對當事人的個資及隱私造成可能的危機¹⁵。

本文重點主題如圖 3 在針對以人工智慧/機械學習驅動的智慧自駕車對於資料運用與個資保護影響探討，透過對自駕車-人工智慧-個資/隱私三者的個別介紹及三者間之互動，探討在智慧自駕車場景下，資料利用與個資保護的平衡。本文從不同國家經驗與案例，討論法規在自駕車科技發展、商業推展、個人隱私、個人資料、生命安全與社會公益間的如何權衡。本文期待以透過法規探討及隱私設計 (Privacy by Design)兩角度，對公務機關及非公務機關提出建議。

¹⁵ 廖曼庭 (2020)，《認識人工智慧技術下的自駕車—從道德到隱私問題》，AI 法律評論網，載於：https://www.acli.com.tw/acli_detail/83.htm (最後瀏覽日：2022/04/13)。

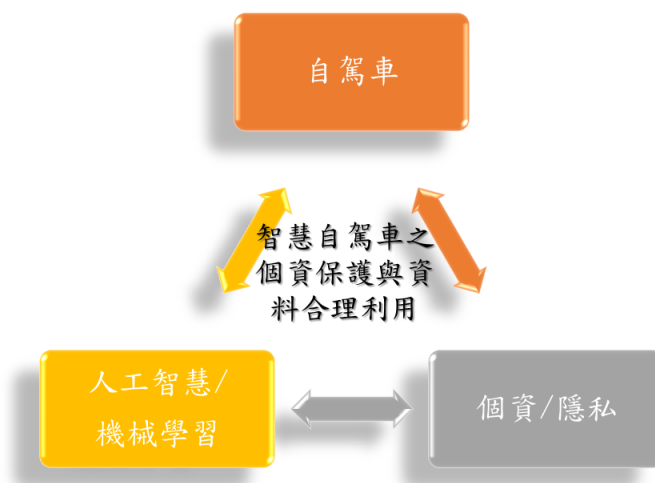


圖 3. 本論文主題圍繞在自駕車-人工智慧/機械學習(AI/ML)-個資/隱私三大區塊。資料來源：本文整理

第二節 研究方法

本論文研究範疇並非單一研究方法所能勝任，故本文採取多元研究方法，藉由不同角度探討「個資/隱私」、「人工智慧/機械學習」與「自駕車」之間複雜交錯的問題，嘗試找出個資/隱私保護與自駕車發展的平衡方法。

首先為概念與案例分析，無論學術之理論、實務之闡述和不同論者之觀點，離不開相關基礎性概念的排列組合，並輔以案例之佐證。隱私權被視為基本人權，自應是個人資料所保護的主要標的，但其定義卻是模糊難以捉摸。本文擬用概念分析方法與實務探討作為隱私與隱私權概念化的基本方法，架構法律所保護之範疇，為個人資料保護的研究奠定基礎，同時作為個案是否為個資法規所涵攝之判斷依據。

同理，研究人工智慧法律的文章雖多，然而對於人工智慧技術分類及其對個資保護的影響大都是概念式的芻議，少見有深入且確切的分析探討。本文必須對人工智慧先做技術上分類，針對目前人工智慧主流的機械學習及深度學習的基本原理與運作概念在前面章節說明，目的為：1.作為個資保護與資料運用兩者平衡探討之基礎；2.在人工智慧/機械學習/深度學習技術快速下，以本文探討範疇來界定該技

術影響層面，深化說明人工智慧/機械學習與個資間關聯。

此外，對於自駕車之探討，首先要定義何謂「自駕車」？與影視電影中的差異何在？以法律觀點出發，相關規範在自駕車運用場景，會有甚麼在法律或者道德層次上的差異？本文會從不同角度來探討自駕車運用場景之於法律上的意義，此一分析有利於最後結論的推展。特別是，自駕車的法律議題研究雖多，但針對自駕車個資探討放眼國際尚在起始階段，國內也尚未有明確規範。然自駕車個資問題牽涉廣泛，所謂自駕車在法律，特別是個資法角度的意義何在，與生命法益之保障孰先孰後？若無清楚定位，自難拿捏立法與執法的分寸。同理，個資是甚麼？隱私與隱私權如何定義？個資法上所謂的「個資」，是否因為先進技術或者自駕車應用場景有所不同？

在個別的人工智慧、自駕車、個資與隱私都有一定的基礎定義之下，第二步就是討論兩兩間的影響，形塑出人工智慧-個資；人工智慧-自駕車；自駕車-個資的互動框架。

其次為比較研究分析方法：隱私權雖然發端於西方先進國家，但所謂「隱私」，隨著在不同的國家區域、社會民眾、風土民情、時代、科技運用場景等條件下存在差異。各國家地區之間除了對隱私權定義及其保護方法各有不同，在於昭顯隱私保護的個人資料保護法規制定更是有顯著差異。本文用以比較研究的主要對象包含歐盟、大陸及美國等對隱私權保護的不同規範，通過互相比較總結其各自特點，為完善智慧自駕車運用景域下，集思廣益個人資料與隱私權的保護方向。

同理，人工智慧技術發展快速，國際相關的道德倫理與隱私規範之研究方興未艾。藉由討論人工智慧技術運用於自駕車發展的必要性，及比較不同國家的人工智慧倫理規範，探索智慧自駕車的運作規則。統整前述針對隱私/個資與人工智慧之比較，並輔以比較各國自駕車資料法規現況，綜合說明智慧自駕車的個資/隱私保護運作之規範，以鞏固本文的立論基礎。

其三，借重歷史研究法：歷史研究法或稱歷史探討方法(historical method or

historical approach)參諸國家教育研究院雙語詞彙之定義為“以「歷史」作為研究的材料，「歷史」是人類過去活動的記載，供我們瞭解過去並預測未來。「歷史法」是研究過去所發生事實的方法，並以科學的態度收集材料，進行檢驗和證實，再透過系統的整理和解釋，以重建過去，推測未來。”¹⁶本文因為牽涉自駕車-人工智慧-個資/隱私三大不同領域，且近年來三者皆有長遠之進展，期間的交錯互動與各自發展的時間點有很大的關聯，法律與科學皆是重視因果關係的研究學門，是故透過歷史研究之方法，包括文獻之蒐集、原文之引用、文獻解釋與分析，並以時間軸(Timeline)闡明三者間之影響，以此說明三者關聯必要性。

最後為法益平衡分析探討：過去個資法的保護著重於私權利益與公共利益間的平衡。對於個資的保護離不開隱私保護與資料運用關係的合理協調，法律的「比例原則」提供一個普世的評量依據，然而在人工智慧自駕車上落實上，有更高的生命法益上的考量，若要探究其多重利益平衡，須要針對每個環節有更深入的基本瞭解分析，更須將必要性有更清楚且明確之說明，並以此知識奠基並延伸探討平衡多方利益。

第三節 研究範圍與限制

因為自駕車及人工智慧技術進步快速，且自駕車牽涉的配套技術與環境日新月异，本文只能就目前及可預見的技術發展為基礎，並以自駕車等級 2 以上，包含被稱為高度自動駕駛車輛(Highly Automated Vehicles, HAVs)的等級 3 至等級 5¹⁷，定為本論文範圍探討。「人工智慧」乙詞尚屬概括式的總稱術語，參諸美國專利商標局(USPTO)在 2020 年發布之《人工智慧和智慧財產權政策的公共觀點》報告，

¹⁶ 顧力仁 (2012/10)，《歷史研究法 historical method》，國家教育研究院雙語詞彙、學術名詞暨辭書資訊網，載於：<https://terms.naer.edu.tw/detail/1678683/> (最後瀏覽日：2021 年 8 月 15 日)

¹⁷ 美國加州 DIVISION 16.6. Autonomous Vehicles [38750 - 38755] (Division 16.6 added by Stats. 2012, Ch. 570, Sec. 2.) 定義自動駕駛車輛為 SAE 3~5 等級，載於：https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=VEH§ionNum=38750

人工智慧並沒有公認的定義¹⁸，故其技術範疇尚屬未定，本文以人工智慧技術中的機械學習技術分支作為探討的基礎。在法規部分，雖然政府、國際大廠與研究文獻將「隱私」與「個資」交互利用，然本文為求定義明確，著重在以個人資料保護為主要探討範疇，並輔以近期所發生之案例及法院判決作為本論文的論述依據；對於資料控制者(data controller)之探討，由於目前自駕車發展快速，以私人企業發展為主，故結論著重探討「非公務機關」之法遵因應，並對公務機關提出建議。

第四節 研究架構及章節順序


本論文共分為六章，第一章為緒論，主要欲先點出本論文之研究動機與目的，並就研究範圍及章節安排做一說明，章節最後將針對本論文研究方法、所考諸引用之重要報導與文獻作一簡單扼要介紹。

由於自駕車與人工智慧技術相當複雜且發展快速，隱私權範疇不明確，各國對於其各自隱私權保護規範也是多面向且爭議方興未艾，遑論本文以三者結合的法規探討，尚有許多待討論的空間。因此，在本論文第二章及第三章作基本知識的介紹，包含第二章的人工智慧、自駕車的技術及第三章的個人資料保護法規，主要是介紹幾個主要名詞及詮釋其主要意涵，藉以釐清目前相關文章容易混淆之處，並界定本文探討之範疇。此外《無人載具科技創新實驗條例》、各國自駕車法規現況及本論文重點探討的隱私與個資保護，也在此二章節作一粗略簡介。

在第二章的第二節中，我們會先介紹人工智慧及人工智慧技術分支包含機械學習與深度學習，另包含人工智慧應用時所連結到之大數據及邊緣運算技術等。「人工智慧」參諸首次提出該詞的 John McCarthy¹⁹定義為：“具有智慧的機器或電

¹⁸ May (2020/10/16)，《美國專利商標局：從公眾眼中來看 AI 人工智慧。科技產業資訊室 (iKnow)》，載於：<https://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=17119> (最後瀏覽日：2022/4/11)。

¹⁹ 維基百科，《約翰·麥卡錫》，載於：<https://zh.wikipedia.org/wiki/%E7%BA%A6%E7%BF%B0%C2%B7%E9%BA%A6%E5%8D%A1%E9>



腦程式”。繼 John McCarthy 之後，持續有論者對人工智慧提出新的定義²⁰，包括人工智慧具備人性化與理性化思維，以及擁有人性化與理性化行為；也有人定義人工智慧是可感知視覺、語音、語言的科技，是可分類、推薦與預測的系統，更是具備學習、邏輯推論與回饋能力的智慧機器，科幻影集“霹靂車”即是這樣理念的實現。由此可知人工智慧是一個不確定性的概念，無論從技術或從法律角度來看都需要進一步的限縮，也因此本章節也會介紹到機器學習。機器學習是人工智慧的一個分支，屬於一種特定的人工智慧技術，機器學習系統特性在於不是採用傳統規則式方法，而會從資料及範例中學習執行工作，因此演算法已經不是由程式設計人員建立規則，或電腦依既定程式聽令行事，取而代之的是一種由資料驅動(Data Driven)的學習式演算法(learning-based algorithm)。相較傳統規則式演算法(rule-based algorithm)，無人載具因為需要面臨到複雜且非規則環境，故採用機器學習演算法有其必要，也正是因為機器學習演算法，所以自駕車的運作須要用到巨量的資料，這些資料的蒐集、處理到運用幾乎是無法避免的，因其資料蒐用牽涉到駕駛、乘客及用路人的生命安全。近年來人工智慧的發展，特別是能落實在自駕車的發展運用，最重要的一項因素是從規則式演算法進展到學習式演算法，也因此有必要針對機器學習作進一步說明。人工智慧/機器學習在近 30 多年已發展為一門多領域交叉學科，涉及資料探勘、機率統計、訊號處理、統計學習等多門學科。本文並不會深入探討人工智慧或者機器學習技術細節，只有針對基礎技術背景及本論文論述所可能牽涉到的法規問題說明。在此章節中，無人載具的介紹也是一個重點，包含無人載具定義及運作原理，並限縮到本論文主要討論的自駕車的介紹，包含自駕車定義及分級(Level)、所運用到之各種感測器(Sensor)、資料融合(Data Fusion)技術、邊緣計算(Edge Computing)運用、車聯網、先進駕駛輔助系統(Advanced Driver Assistance Systems, ADAS)、到適用於 L3 以上高度自駕車的自駕車系統(Automated Driving

%94%A1. (最後瀏覽日：2021/3/12)。

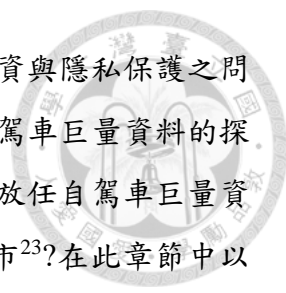
²⁰ ScienceDaily. *Artificial intelligence*.
https://www.sciencedaily.com/terms/artificial_intelligence.htm

System, ADS)等技術。此部分除了介紹自駕車的採用技術及發展現況外，重要的是鋪陳後面可能引發的法律問題。

在第二章的第三節中，現行自駕車政策法規回顧是本章的重點²¹，包含台灣的自駕車推動政策及《無人載具車技創新實驗條例》與相關子法；美國的自駕車規範現況包含《聯邦車輛安全標準》(Federal Motor Vehicle Safety Standards, FMVSS)、《聯邦自動駕駛車輛政策》(Federal Automated Vehicles Policy, FAVP)等。FAVP 政策所稱之高度自動駕駛車輛 (Highly Automated Vehicles, HAVs)，係指監控車輛操駕環境之系統，屬於美國汽車工程師學會 (Society of Automotive Engineers, SAE) SAE J3016 所定義之部分自動駕駛 (等級 3，簡稱 L3)、高度自動駕駛 (等級 4，簡稱 L4)，與完全自動駕駛 (等級 5，簡稱 L5) 之車輛。在適用於所有車載高度自動駕駛系統，包括資料之紀錄與共用、隱私、系統安全性、車聯網安全性、人機介面、車體抗撞性、消費者教育與訓練、碰撞後車輛行為等；聯邦、各州與地方之相關法規及道德層面的考量因素等。2017 年 9 月 6 日眾議院通過《Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution Act, H. R. 3388》，本法案又名《自動駕駛法案(SELF DRIVE ACT, SDA)》，SDA 旨在順利實現自動駕駛汽車的安全規範與推動相關研究，是全美首部立法宗旨在確保自動駕駛汽車的安全創新、研發、測試及部署的專門法案。SDA 法案內容涵蓋搭載高度自動駕駛功能之後裝或前裝車輛所應適用之安全標準、後座乘客警示系統、車頭燈、自動駕駛系統之網路安全與隱私計畫、車輛測試或性能評估、對未來消費者所應提供之高度自動駕駛系統資訊，以及高度自動駕駛車輛諮詢委員會之設置等。除了美國及台灣，還有包含德、日、英、新加坡等各國政策法規檢視。

在第三章中，個資與隱私的法律依據是該章節探討的對象。自駕車目前的技術發展還是以安全性(Safety)為首要考量，在資料的處理與運用上，雖然各國已有

²¹ 趙亮 (2019/06)，《自動駕駛汽車監管制度研究》，吉林大學法律碩士論文，中國吉林。



明文例示具必要性的特殊情形，然個資保護與安全間的權衡、個資與隱私保護之問題在各國自駕車的發展中還是持續被提出²²，此節延續前面對自駕車巨量資料的探討，並深思智慧自駕車巨量資料量遠非過去近似案例可相比，若放任自駕車巨量資料被私人企業運用，未來您我生活是否會落入被綁架的智慧城市²³?在此章節中以台灣《個資法》及隱私權見解與判例為主，輔以歐洲 GDPR 與美國加州消費者隱私保護法（California Consumer Privacy Act 2018）討論說明。在法規、判例與媒體揭露個案中，「個資」與「隱私」常被混為一談，然而個資與隱私的定義與範疇在此必須嚴謹的被檢視，在《個資法》下個人資料定義之落入否，其中首要的就是「去識別化」概念探討；另外，將在公開場所或活動所電子記錄之影音資料蒐集，並經前述先進技術拼湊組合，是否可能將個人資料揭露或計算推估而得，而使隱私權有受侵害之可能？經自駕車蒐集之影音資料是否得依個人資料保護法第 51 條第 1 項第 2 款規定，主張不受該法之規範？本章節除了回顧個資法與隱私權的保護法益，探討法治保障與生命安全間取捨，另一方面也為後續自駕車可能引發的個資或者隱私問題做為討論之基礎。

基於本文第二及第三章的背景知識說明，第四章開始以個案探討人工智慧驅動之自駕車對於隱私權益的影響。在本此章節中討論以自駕車目前所引起的隱私權或個資侵害疑慮，此議題分為兩個部分來探討，其一為對車內人員特定人員，如：駕駛及乘客之個資或隱私可能侵害之疑慮；其二，也探討對不特定對象，例如車外用路人或者其他私人領域個資或隱私侵害疑慮，近似的案例會以 Google 街景圖 (Google Street View) 及道路監視器 (street-level surveillance cameras) 作為借鏡，並推論以自駕車集先進高科技於一身的載體，其中包含光達 (LiDAR) 感測與辨識、影像感測與辨識、高精地圖、車輛定位、人工智慧/機械學習決策控制等，所引發可能法規適用問題。自駕車因為資料量遠大於一般攝影機百倍以上，且單一自駕車運行

²² 蕭文生 (2021/112), 〈自駕車法制之發展 (下)〉, 《月旦法學》, No.319, 頁 69。

²³ 班·格林 Ben Green (2020), 《被科技綁架的智慧城市 (The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future)》, 台灣：行人出版社。

時在資料蒐集、處理與運用幾乎同時進行，再加以導入車聯網後，破碎資料可透過大數據運用迅速且幾乎無法避免的集成有用資訊²⁴。特別是自駕車目前都以私人企業發展較快速且已導入商品化，在私人企業為主導下，這些大量的資料對於商業發展有無限發展的可能，在利益引誘下相關個資運用與社會公益衝突在所難免，且在自駕車另有安全上考量，相關的監管法規應更謹慎。

第五章本文就前面所回顧之背景知識及案例，就人工智慧/機械學習驅動之自駕車，資料/個資蒐用的高度頻繁與不可預測性²⁵、資料/個資運用與社會公益衝突幾乎難以避免，提出依目前法規的制約與企業責任與自我要求角度下可能的調和方案，包含自駕車廠商應依循國際如 GDPR 及大陸等資料法規的規定，如：必須針對蒐集資料的目的設限；蒐集個人資料時必須秉持具體、明確且正當的目的為之；蒐集前應經駕駛及乘客同意為原則，如需進一步處理，處理方式不得與其目的相悖等。依個人資料保護之原則，但凡進一步處理個人資料之行為，原則上不得有蒐集時所告知目的外之利用；而針於疑似個資的資料，應遵守之資料處理原則及組織內部的管控原則。回歸到自駕車的任何資料蒐集、處理、儲存到利用應以保障生命安全為其原始目的，若有個資或隱私侵害之疑慮，應遵守相關法規並有預先且整體性的隱私保護設計。此外，自駕車廠商還必須儘可能減少需要蒐集與儲存的資料，以符合 GDPR 第 5 節第 1(c) 條的資料最小化原則，舉凡個人資料從蒐集到處理、儲存與利用，皆須適當、相關，且僅止於符合資料處理目的所需的程度。對於境外資料傳輸應注意遵守 GDPR 及大陸資料法規的「原則禁止、例外允許」的規定。

在目前人工智慧/機械學習為技術基礎的條件下，上述個人資料處理原則已有所衝擊，這是因為人工智慧模型(AI model)需要大量資料蒐集、不透明的處理與利用，資料也需要持續更新，且運用到自駕車會有生命安全上的考量等等新型態問題，增加由公部門管理及監督相當困難。因此從企業責任與自我要求角度，透過隱私設

²⁴ Ohm, P. (2009). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA l. Rev.*, 57, 1701.

²⁵ 張文憶 (2020/07),《大數據應用世代下的資訊隱私規範》，台灣大學進修推廣學院事業經營法務碩士在職學位學程碩士論文，臺北。


計 (privacy by design) 的概念套用到自駕車設計、開發到營運全生命週期。自駕車廠商應該要有的企業隱私設計內部管理與企業隱私權保護責任更顯重要。

在第六章結論部分，將就前五章之討論作一總結，除了回顧本論文探討議題的重要性，包含：1.自駕車深入生活，影響深遠；2.資料量巨大；3.隱密不易被察覺；4.自駕車事關生命安全，管理須謹慎；5.人工智慧/機械學習技術採用之必要，增加規範上的困難；6.法律上之「蒐集」、「處理」到「利用」行為難切割；7.資料須更新；8.資料與模型在地化；9.探討對內乘客與駕駛，亦討論不特定的用路人；10.自駕車目前以企業為主導，個資運用可能與社會公益有所衝突；及 11.國際間對於自駕車個資的規範現況等。另第六章節中提出對非公務機關及公務機關的建議，特別指出因技術開發與資料運用，企業內部理應最為熟悉，惟有透過導入隱私設計，內部自我管理約束，甚或將產品的隱私功能為商業競爭優勢，藉此強化品牌形象與商譽，在自駕車產業發展與社會公益間才能最終取得一個平衡。

智慧自駕車發展與資料法規與時俱進，且有部分重要趨勢與本文緊密連結，故在第六章最後，羅列相關事項以展望未來，期待讀者能更全貌的瞭解智慧自駕車之個資及資料法規規範。

第五節 專有名詞、術語、法律用語與標準符號使用說明

本文因為涵蓋「自駕車」、「個資」與「人工智慧」三大領域，三大領域都是熱門且跨國際的研究，用詞上有相當大的差異，而研究上為講求精確嚴謹，旁徵博引同時必先定義名詞與解析用語上的差異，本文在專有名詞使用都會說明定義，若為翻譯也會附註英文原文以真實反應各國法規制定上原意。以下是舉例幾個重要名詞：一.**人工智慧**(Artificial Intelligence, AI)定義：人工智慧(AI)雖然已有多方從不同面向嘗試提出「人工智慧」的定義，但是還是屬於概括式的總稱術語(umbrella term)，綜觀目前各方現今對於「人工智慧」分歧解釋，不論從**科學或法律專業都不是精準用語**，其定義與涵蓋範圍都未定，然而因為不論政府、國際大廠或者法律學者都還是以「人工智慧(AI)」直接註明。而在本文因為牽涉到資料及個資研究，需



要正確且清晰的闡述自駕車-個資-人工智慧間的互動，真正影響資料/個資運用之技術是指人工智慧下的機械學習(Mechine Learning, ML)或者機械學習技術下的分支深度學習技術。因機械學習為第三代人工智慧技術，是以資料驅動(Data driven)的人工智慧技術分支，也才是與本論文的個人資料與隱私議題密切相關之技術；且機械學習會有三階段的資料運用，對於資料如何運用?及運用下對《個資法》的衝擊與影響卻少有法律文章敘明。是故本文在不同章節及對照不同參考資料之同時，兼顧文章易讀性與專業，爰第二章介紹各名詞及對資料影響後，第三章起使用人工智慧/機械學習(AI/ML)用詞以求精確。二.「資料」、「數據」、「信息」、「資訊」、「data」與「information」區別：一般在參考資料中，「資料」與「數據」解釋比較接近，都是比較原始的訊息，雖兩者還是有基本上的差異，但本文為求文章之易讀性，將兩者統一為「資料」，英文為「Data」，除了專有名詞如「Big Data」，尊重引用資料之慣用翻譯為「大數據」。另外兩岸不同之處，例如《中華人民共和國個人資訊保護法》，其中「資訊」應同為台灣用語「資訊」，然因其「個人資訊」法律解釋與我國「個人資料」相似，皆為保護個人資料與隱私，在台灣大部分論者還是用「資料」表述；對照美國《加州消費者隱私法》(California Consumer Privacy Act, CCPA)亦是使用「個人資訊」(personal information)。然「資料」(data)與「資訊」(information)從知識管理角度實為不同，以大數據及人工智慧/機械學習觀點更可理解中間差異，本文將於第五章中說明。三.國際大廠以英文為主：因為無論自駕車、隱私及人工智慧，會提到國際大廠如 Google、Tesla、Apple、Facebook 等，本文將以**英文原文呈現，不做翻譯**。理由是各國際大廠為**知名企業**，讀者**不易混淆**；再者英文在專有名詞第一個字皆為大寫，相較中文更為嚴謹且好閱讀。綜上，本文在用詞上以英文原文同步呈現為先，引用資料的用詞若與本文有異將說明其中差異理由。此外在法律用字用語部分，本文依照司法院公布之《法律統一用字表》²⁶統一使用之法律文字。

在符號及重點標註部分，本文參照教育部公布之《重訂標點符號手冊》並做

²⁶ 司法院法律用字用語統一表網站，《法律統一用字表》，<https://www.judicial.gov.tw/tw/cp-2008-163354-de8c4-1.html>

部分調整。在本文中之中文專有名詞會以專名號標註，以區分一般性概論與專有名詞，例如文中所探討之「個人資料」(簡稱：個資)並非全都是《個資法》所謂之「個資」；若屬《個資法》涵攝之個資，本文中將會以專名號標註；再如自駕車，若屬 SAE 標準之定義，則以自駕車表述，並會註明其等級。以上詳細使用符號之說明請參考本文附錄(I)。本文中文「註解」及「參考文獻」之格式參考《台大法學論叢》²⁷ 格式範本 2020 年 9 月 23 日修正通過版²⁸；英文「參考文獻」之格式則參照 APA 第七版。

²⁷ 依據《台大法學論叢》(新修)格式範本之二、參考文獻規定：參考文獻放在正文及附錄之後，英文摘要及關鍵詞之前。此規定與《國立台灣大學碩博士論文格式規範》不同，本文還是依照《國立台灣大學碩博士論文格式規範》之規定。另外，《台大法學論叢》規定參考文獻不加編號，本文考量參考文獻較多，且大多法律碩士論文依然有將參考文獻編碼，故本文參考文獻有加以編號。除此，日期編排大部分文獻及 APA 以(年-月-日)排列，本文為求一致，統一以(年-月-日)排列。


²⁸ 國立臺灣大學法律學院 (2020)，《台大法學論叢》(新修)格式範本，載於：
<http://www.law.ntu.edu.tw/law3/index.php/zh-tw/%E6%A0%BC%E5%BC%8F%E7%AF%84%E6%9C%AC.html>

第貳章 人工智慧與自駕車概觀



第一節 前言

汽車(vehicles)是現代經濟活動的中心之一，是大眾主要交通工具，亦代表社會的經濟發展狀況與社會生活型態。私人汽車除了是一種交通工具，也代表一個私人領域空間，人們可以在其中享受某種態樣的決策自主與部分不受外界干擾之自由，也因此汽車使用者對於車內的空間具有一定的隱私期待。如今，隨著智慧自駕汽車進入主流，這樣的願景已經可能逐漸受到威脅。近年來，智慧自駕車從高端品牌迅速擴展到大眾市場，加以越來越多的感測裝置，自駕車正在成為巨量資料中心。近年來在市場上推出自駕車可蒐集：1.車輛狀態、行駛距離相關的資料、車輛零件耗損、位置資料或行車紀錄器所蒐集的資料等；2.車內使用者資料，包含：駕駛者習慣、駕駛人眼動監測、駕駛者精神警示、交通的地點、停留時間，甚至可能是駕駛者脈搏或生物特徵數據等直接或間接與特定駕駛者相關的一般個資與敏感性個資；3.路上車輛動態、都市景觀、商業活動及用路人的影音資料。前述資料從過去不曾被大量蒐集與長期儲存，惟於短短的近 10 間，如今因為人工智慧、大數據、物聯網、雲端計算等技術導入車輛而被輕易蒐用，也因此產生一個新的複雜的自駕車產業生態系統。前述車輛狀態及車內使用者資料由當事人所產生，這些新的產業生態系統參與者透過蒐用車輛使用人或用路人個資轉變成資料控制者，在此新生態系統中之資料控制者不限於傳統汽車行業的製造商，也誕生屬於資料經濟(Data Economic)的新參與者，包含智慧車輛營運商、車輛製造商、網路服務商、保險業者等。這些資料控制者可能透過所控制個資，提供車輛使用者提供個別化之娛樂服務，例如：在線音樂、路況和交通資訊，或提供駕駛輔助系統和車況服務，例如：自動駕駛軟體、行車路徑建議、車輛狀況更新、基於使用的使用率保險(Usage Based Insurance, UBI)或動態服務等。這些因資料而生的新型態服務從正面來看，提供過往傳統車輛所沒有的服務與提升安全性；但若資料管理不甚，亦有濫用個資、侵害隱私的疑慮。



2016 年，國際汽車聯合會 (Fédération Internationale de l'Automobile, FIA) 在整個歐洲開展了一項活動稱為 “My Car My Data”²⁹，以瞭解歐洲人對汽車聯網 (或稱聯網車) 的看法。雖然這活動顯示了駕駛對新增聯網功能的高度興趣，但它也強調了必須警惕在使用車輛產生的資料以及遵守個人資料保護原則的重要性。因此挑戰是對於新的產業生態系統中的資料控制者及每個利益攸關方，將個人資料保護行動的廣度與深度從產品設計、製造到使用、營運每一個階段與環節，並確保汽車用戶享有資料透明和控制權能根據 GDPR 第 78 條運作。這種方法正面而言有助於增強使用者信心，從而促進這些商業模式及技術的長期發展。聯網車輛因商品及技術不斷的快速成長，創造了新的商業模式與服務型態，擴大更多影響大眾生活可能，2017 年後再加入而以資料為運作引擎的人工智慧自駕車，更是將這些包含駕駛、乘客、用路人之資料與個資隱私與管理與法規問題推上高峰。

隨著人工智慧、半導體與感測等技術的發展成熟，人工智慧晶片硬體化使得汽車廠商得以更便宜、穩定的將智慧電子技術應用在汽車設計及製造上³⁰，使得汽車除了從過去的封閉獨立系統轉變成能與外界開放溝通互動的聯網車外，更進一步進化為具有智慧感測、反應及即時處理的智慧型可輔助半自駕，甚至可高度自駕的車輛。智慧自駕車發展的目的是為了達到民眾與廠商的共同夢想目標：一個聰明、自動、安全、舒適且具環保的交通工具。根據 Yole 報告 2019 年全球車用 AI 晶片市場約 1.4 億美元，2025 年可達 27.5 億美元，而其中先進駕駛輔助系統的 AI 晶片市場為 25 億美元，佔比約 90%，意即幾乎每輛新車都會配裝先進駕駛輔助系統 AI 晶片³¹。

在實務上面，由於 Tesla 自駕車成功商轉運用且逐年快速成長，加上全球各傳統車廠如 Nissan、BMW、Daimler、Ford、Volvo、Toyota 及科技巨頭如 Google、

²⁹ Fédération Internationale de l'Automobile (2017/05/17). *MY CAR MY DATA*.
<http://www.mycarmydata.eu/>

³⁰ 洪德欽 (2020/07/05)，〈歐盟自動駕駛車之發展策略與法律規範〉，《歐美研究》，第五十卷第二期，頁 358-359。

³¹ 蕭瑞聖 (2021/01/15)，〈人工智慧在自駕車的應用 Application of Artificial Intelligence in Autonomous vehicles〉，IEK 產業情報網，載於：
https://ieknet.iek.org.tw/iekrpt/rpt_more.aspx?rpt_idno=33882896

Apple、鴻海等研發自動駕駛車技術的成果展現與推動企圖，使得世人對於自動駕駛汽車技術更具信心、對市場展望樂觀，也帶動各式輔助駕駛的先進駕駛輔助系統的商業化，在商業的驅動下使得技術更能快速蓬勃發展，如下圖 4 所示，是人工智慧(Artificial intelligence, AI) 應用於自駕車市場預測，預測 2018~2023 年人工智慧應用於自駕車(Autonomous Driving)、半自駕車(Semi Autonomous Driving)、人機介面(Human Machine Interface)與車輛追蹤(Vehicle Tracking)等技術項目市場比例較高，隨著自駕車與電動車輛比例的增加，人工智慧應用於停車管理系統(Parking Management System)與廢氣排放(Carbon Emission Management)的比例逐年減少。由此可見，由人工智慧技術所驅動的自駕車已經深入我們生活，提高車輛使用效率也保障生命安全。

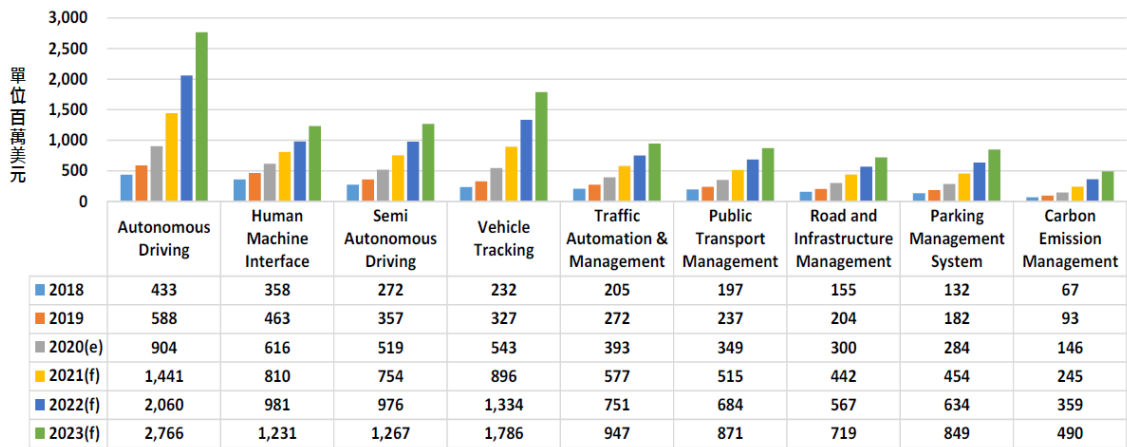


圖 4. 人工智慧應用於自駕車市場預測。資料來源：Mind Commerce(2019);工研院產科國際所(2021/1)³²

「自駕車」、「人工智慧」及「個資」三者各別議題之探討已如雨後春筍，但是本文框架下，自駕車-人工智慧-個資三者間激盪下引發的新議題卻少有深入文獻討論。以下就三者定義及兩兩間關聯與互動作深入的探討，以作為後續智慧自駕車個資保護討論之基礎。

³² 蕭瑞聖 (2021/01/15)，前揭註 31，頁 1。

第二節 人工智慧、自駕車與個資法



「人工智慧(AI)」、「自駕車(AV)」與「《個人資料保護法》」是三個生活中常見的名詞，而這正反應三者對現在人生活之影響甚鉅；然而也正因為三者的影響廣泛且深遠，相關研究與案例如雨後春筍般不斷，常也因此見到相關用詞不同，定義有所不清。本文在探討前先界定人工智慧、機械學習與深度學習定義；自駕車的定義與自駕等級；個資與隱私(privacy)，以明確本文探討的範疇。另外，很重要的是三者間的互動、關聯與必要性是本章節所要探討重點，以利本論文所要探討的人工智慧自駕車之資料利用與個資保護議題界定。

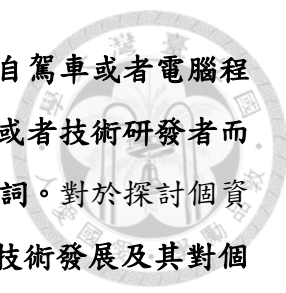
第一項 人工智慧技術簡介

一. 人工智慧定義與發展歷史

參諸首先提出「人工智慧」乙詞的人工智慧之父約翰·麥卡錫(John McCarthy)於1955年提案中所定義：“有人類相同的行為特性的機器稱為具有智慧(a machine behave in ways that would be called intelligent if a human were so behaving)”³³。繼 John McCarthy 之後，持續有論者對人工智慧提出新的定義，包括人工智慧為具備人性化與理性化思維，以及擁有人性化與理性化行為等；英國政府定義：“人工智慧為使用數位技術，創建能夠執行通常認為需要智慧的任務的系統(AI can be defined as the use of digital technology to create systems capable of performing tasks commonly thought to require intelligence)”³⁴；亦有定義人工智慧是可感知視覺、語音、語言的科技，是可分類、推薦與預測的系統，且是具備學習、邏輯推論與回饋能力的智慧機器，科幻影集《霹靂車》即是這樣的理念實現。綜前所述，因為「人工智慧」泛

³³ J. McCarthy, M. L. Minsky, N. Rochester, C.E. Shannon (1955/08/31). *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, p.11. <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>

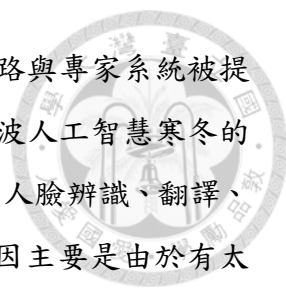
³⁴ UK Office for Artificial Intelligence (2019/06/10). *A guide to using artificial intelligence in the public sector*. <https://www.gov.uk/government/publications/understanding-artificial-intelligence/a-guide-to-using-artificial-intelligence-in-the-public-sector>



指任何使機器或電腦能夠模仿人類行為的技術，包含機器人、全自駕車或者電腦程式等能模仿人類行為技術，所以「人工智慧」乙詞不論對於法律或者技術研發者而言，皆屬概括式的總稱術語(umbrella term)，並非嚴謹的專有名詞。對於探討個資與人工智慧問題的法律研究者而言，需要更瞭解人工智慧後續技術發展及其對個資的衝擊，並用更精確的用語以探討兩者間的關係。

如下圖 5 人工智慧發展歷史來看，自從電腦 (Computer) 在 1950 年代被發明後，如何讓「以電驅動之大腦」變得和人類一樣聰明或者如何能代替人們進行所有的工作等問題，一直被科學家及研究人員所提出。被稱為人工智慧之父的艾倫·麥席森·圖靈 (Alan Mathison Turing) 於 1950 年所發表的文章《Computing Machinery and Intelligence》首次談到電腦是否能思考的問題，並發展出所謂的圖靈測試(Turing Test)來分辨人與電腦。到 1956 年 John McCarthy 在達特茅斯研討會首次提出「人工智慧」(Artificial Intelligence，簡稱 AI) 一詞，世人第一次認識此概念想法，並將第一波人工智慧研究推到高點。從 1950 年代到人工智慧洛陽紙貴的今日，之間這段漫長的過程中，人工智慧的發展並不是那麼的順遂，期間歷經了兩次起伏，直到近 10 年來因為在多個領域，如圖形辨識、語音辨識、棋藝、翻譯等，被證實優於人類普遍的表現才有了顯著的進展，而這個進展因為人工智慧應用廣泛且導入商品中還在持續快速進行中。

第一波人工智慧的發展，隨著電腦的應用而開始在 1950 年代啟蒙，1950 年艾倫·圖靈(Alan Mathison Turing)在論文中預言人工智慧機器的可能，並設計圖靈測試;到 1956 年 John McCarthy 在達特茅斯研討會首次提出人工智慧一詞，人工智慧自此被廣為人知且被確立為一門集合數學、腦科學、電腦工程學等的時代熱門學科，除此之外，數位通訊理論也在第一波人工智慧發展中提出，第一波人工智慧熱潮衝擊當時的科技界。然而第一波的發展卻因為當時的硬體環境，包含**有限的計算機能力**(limited computer processing power)、**有限的儲存空間**(limited database storage capacity)、及**連網速度及能力**(limited network ability)都局限了當時的人工智慧技術發展，也使得人工智慧發展在 1960~1970 年間進入第一個寒冬。



在歷經第一波寒冬 10 年後，在 1975~1982 年間，類神經網路與專家系統被提出，也使得光學辨識及語音辨識研究成為當時的顯學。然而第二波人工智慧寒冬的到來，也是因為無論專家系統或者類神經網路，還是無法解決如人臉辨識、翻譯、組合爆炸 (Combinatorial explosion) 等真實世界的問題。失敗原因主要是由於有太多實務上的難題連人類自身也只是基於經驗行事，人們泛指的常識 (common sense)³⁵，其實並無法明確指出規則，比如影像辨識、物件辨別、反應火災、水災等生活問題。在實務上，人類即便有能力解答，也多是依賴所謂的經驗累積，過程中也不一定能把規則或者邏輯清楚描述並轉化成程式語言並執行，特別如棋藝、傳統醫療等。這是人類在人工智慧發展遭遇的第二次挫敗主因。

前面兩波人工智慧技術的失敗，也一度讓相關人工智慧的發展受到質疑，人工智慧投入如此多資源但是在實務上如生活中的圖形辨識，陷於一直無法超越人類水準的困境。但也是因為基於這些前面兩波早期先進的理論及初期實驗，也才有 2010 年後光輝的第三波發展。近 10 年來相關技術的成熟，包括**演算法的突破**、**計算機能力的突破**、**儲存空間拓展**、**連網速度提升及能力突破**，也為近 10 年來人工智慧的發展醞釀良好的環境，重要技術如**物聯網**、**大數據**、**雲端計算**、**人工智慧/機械學習/深度學習**都是在 2010 年後如雨後春筍般的出現、突破並成長茁壯。

³⁵ John McCarthy (1958/12). Programs with common sense. *Teddington Conference on the Mechanization of Thought Processes*. <http://jmc.stanford.edu/articles/mcc59/mcc59.pdf>

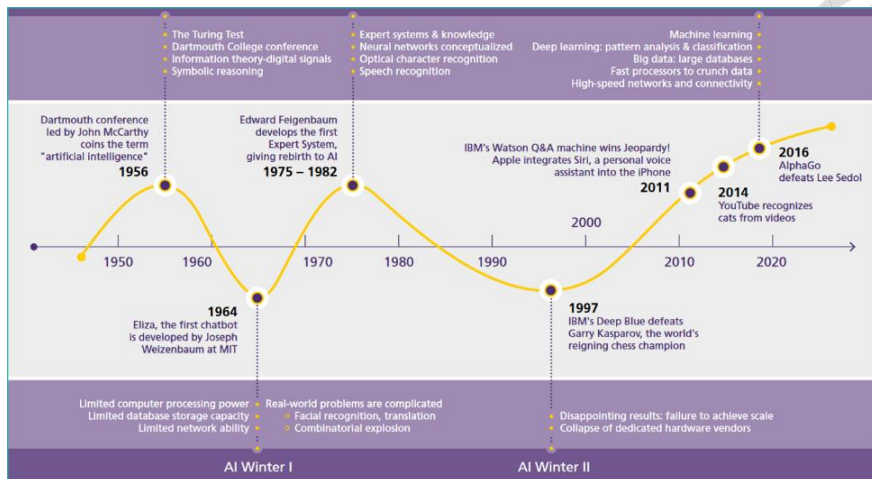


圖 5. 人工智慧(AI)的三波演進，目前第三波是以機械學習(ML)演算法為基礎。資料來源：
Business Science³⁶


二. 人工智慧技術主流-機械學習與深度學習

第三波人工智慧的發展，大約始於 2010 年，有位華裔科學家李飛飛科學家從自己兒子身上想到，讓電腦學習人類的學習經驗，因為人類的學習也是在一次次的教導與辨識中成長。於是科學家僅告訴機器如何識字，然後予電腦大量的資料，讓電腦機器自己判斷，並讓電腦自我學習並找出規則，這就是現代機器學習的開端，機器學習及其分支深度學習技術讓人工智慧技術有了大躍進並在圍棋中戰勝了人類的智慧，震驚的全人類，而且如今機械學習/深度學習還在自我不斷進化中³⁷。

李飛飛 (Fei-Fei Li) 為史丹佛大學電腦科學系教授，兼任 Stanford HAI (Human-Centered AI Institute, 「以人為本」人工智慧研究院) 共同主持人，她的成名之作，就是在史丹佛建立了 ImageNet 這個全球最大的圖形識別資料庫，以及 ImageNet 的圖形識別競賽，李教授從在加州理工學院攻讀博士開始，到領導史丹佛的視覺實驗室，李飛飛試圖讓電腦擁有如人類一般的智慧之眼，其目標就是教導機器能夠像人一樣除了看到並且理解所見之物，像是識別物品、辨認人臉、推論物

³⁶ Fabrizio Fantini (2020/06/20). Data Science is Dead. Long Live Business Science! *Towards Data Science*. <https://towardsdatascience.com/data-science-is-dead-long-live-business-science-a3059fe84e6c>

³⁷ Fei Fei Li (2015/03/23). How we teach computers to understand pictures. *TED*. <https://www.youtube.com/watch?v=40riCqvRoMs>



體的幾何形態，並進而理解其中的關聯、情緒、動作及判斷意圖。要電腦達成這個目標的第一步，就是教導它辨別物品，這是機械視覺的基石。簡單來說，教導電腦的方法就是給電腦看一些特定物體例如貓咪的影像，其想法如同沒有人教導孩童如何去「看」，特別是在早期發育階段，孩童他們是從真實世界的經驗中學習。把孩童的眼睛當成生物相機的概念，就如同眼球移動平均時間每 200 毫秒就拍一張照片一樣。以這樣的資料累積，年紀到了三歲時，孩子們已經看過了真實世界中數以百萬計的照片，這樣的訓練概念對電腦而言是需要很巨量的資料。但李飛飛教授以孩童的學習經驗法則，並提供兼具質與量之訓練資料給電腦，取代提供更好的程式演算，讓電腦自己如同人類在經驗中找出規則。李飛飛教授利用 ImageNet 多達百億幅圖形的資料庫，以及「卷積神經網路」，正如同大腦是由無數個緊密連結的神經元所組成，神經網路的基本運作單位也是一個類神經元的節點。它的運作方式是從別的節點得到資料，然後再傳給其他的節點。而且這些數不清的節點擁有層層的組織架構，就好像我們的大腦一樣，在物品辨識領域中，這樣的架構獲得令人興奮的嶄新成果，而此種新作法被稱為深度學習演算法，屬機械學習的分支技術。質言之，深度學習是指如圖 9 具有多層次的機器學習法，一層層的節點如同前述人類的神經元接受或者傳遞資料，透過層層處理將大量的初始資料訊號漸漸轉為有用的資訊。深度學習之運作於後傳統演算法與機械學習法比較中說明。

電腦影像識別在西元 2014~2015 年後就超越人類(下圖 6)，就此奠定機械學習/深度學習在圖形識別技術的地位。

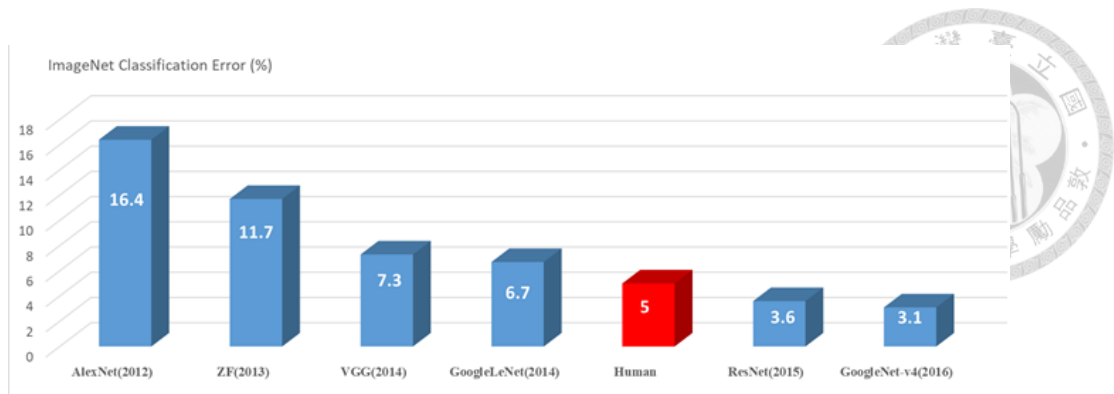


圖 6. 人眼與電腦視覺在影像分類上的競賽，人工智慧在 2014~2015 間後就擊敗了人類。資料來源：ImageNet³⁸;本文整理

如圖 7 中之簡略定義，人工智慧是泛指任何使計算機能夠模仿人類行為的技術(“any technique which enables computers to mimic human behavior”)，以此定義自然包含深度學習與機械學習。機械學習可解釋為一種不需特定明確程式，可賦予電腦學習能力的技術;深度學習是機械學習的一支，並利用多層神經網路的神經網路(Neural Network, NN)計算。總結前述人工智慧、機械學習與深度學習三者關係及發展年代如圖 7 所示。人工智慧的發展重要里程碑可參考表 1 所示，從表中可看出整個人工智慧發展近 10 年來的突破，及機械學習/深度學習新演算法的成功。以下就機械學習/深度學習與資料及個資間的互動說明，分析機械學習與傳統演算法的差異，並針對法規面衝擊做一初步說明。

³⁸ IMAGENET. <https://www.image-net.org/index.php>

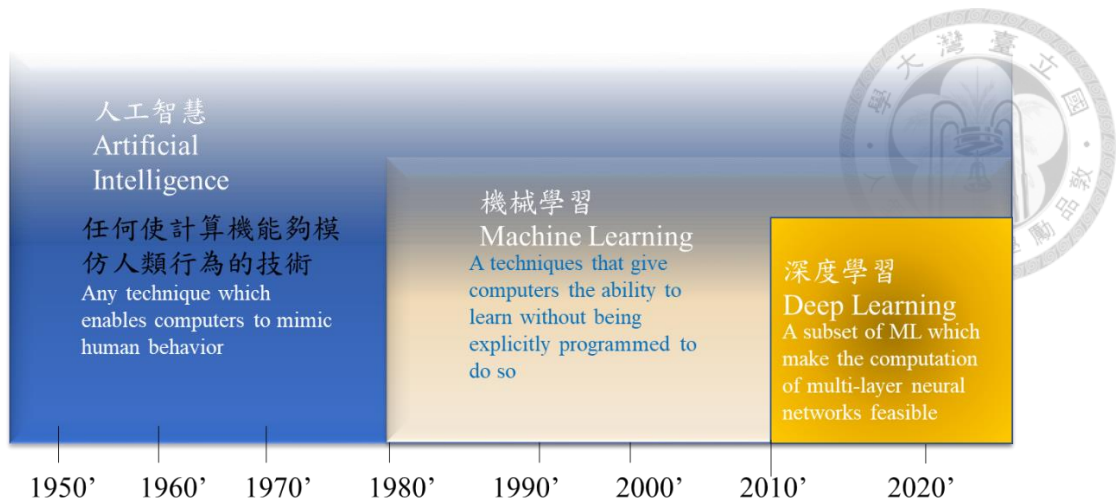


圖 7. 人工智慧(AI)、機械學習(ML)與深度學習(DL)的發展年代與定義。資料來源：
Oracle³⁹; 本文整理

機器學習是以數據為基礎的新演算法，是一種實現人工智慧的方法，透過演算法探勘大量的數據及經驗，找到其運行規則，並對真實世界中的事件做出決策和預測。簡而言之，如圖 8 所示「機器學習是透過大量的數據訓練機器，告訴機器何者正確，讓機器能夠自行做出預測」。深度學習是一種實現機器學習的技術，深度學習屬於機械學習的分支技術，透過層層的函數堆疊，如同人類神經網路架構。深度學習模型需要透過大量的訓練數據及更強大的計算能力，才能得到更好的預測結果。例如垃圾郵件判別的常見應用，每當使用者收到任何一封電子郵件，電子信箱都會評估其中的內容來判定這封信是正常郵件或是垃圾郵件，並分別分類至收件或垃圾郵件資料夾。雖然工程師可以預先設定已知特定的規則，來歸納垃圾郵件的特性，不過機器學習演算法卻可以經由分析過去的電子郵件，來偵測到更細微、複雜且可以用於分辨垃圾郵件的規則。機器學習相較過去工程師預先轉寫好程式的規則式演算法，機器學習更能應付複雜的真實世界，也正是為何自駕車之運行必須導入機械學習/深度學習的原因，然而採用機器學習付出的代價就是需要巨量資料與強大計算能力。一言以蔽之，機器學習就是讓機器根據一些訓練資料，自動找

³⁹ Aditya Tiwari (2020). *Difference between AI vs ML vs DL*.
<https://medium.datadriveninvestor.com/difference-between-ai-vs-ml-vs-dl-d6382f851dcb> (最後瀏覽日：2021/3/10)

出有用的規則(rules) 或函數(function)。資料對於機器學習/深度學習(ML/DL)相當重要，如果訓練資料不夠全面縝詳，人工智慧/機械學習系統就會形成偏見，並開始傾向特定的結果。因為智慧系統是透過資料來學習，系統最後可能會將輸入資訊中含有的錯誤或偏見情況重現出來。常見之例子是如果要訓練人工智慧系統辨識鞋類，卻只提供運動鞋的圖形，人工智慧將無法學會辨識高跟鞋、涼鞋或靴子等鞋款。在自駕車中，如果只訓練高速公路的行車資料，那自駕車對於小巷子及用路人的反應可能就資料不足且有偏見產生。以資料驅動的人工智慧/機械學習，因為要持續且完整的資料來訓練模型，對於資料的刪除權行使有一定程度上的困難，例如

- 1.必須完整蒐集路況資料，若有人要求刪除部分個人資料影響，可能影響模型的正確性，且影響難以評估;
- 2.因為需長期訓練，所以舉例 1 輛自駕等級 2 的車輛，過去在接受美國的路況資料，無法處理台灣小巷弄的路況，所以車商必須持續學習、儲存包含路況、駕駛人狀況資料，除了為了自駕車等級 2 的運作，也為將來提升到自駕等級 3~5 時因應。

目前不論機械學習及深度學習只能針對特定需求來設計，如 AlphaGo 只會下圍棋，不能要求它預測天氣。通用型機械學習雖有在研發，因為尚未技術成熟，本文暫不討論。

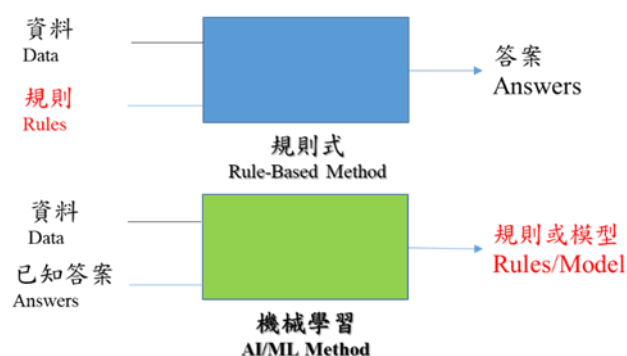


圖 8. 傳統規則性(Rule-based)與機器學習(ML)演算法的差異，在於機器學習(ML)利用數據來訓練模式(Model)，而非由程式設計人員預先給定規則。資料來源：Google;本文整理

深度學習是一種特定的「深度神經網路」(Deep Neural Network)機器學習法。「深度神經網路」就是模擬人的大腦訊號傳輸與處理，在此網路中包含許多神經元，

每個神經元各司其職，部分負責接受資料，有些負責傳遞資料。最基礎的深度學習網路包含三層神經元，除了輸入和輸出層外，中間有一層隱藏層(Hidden Layer)，傳遞並處理資料。其實，隱藏層可以有一層以上，而複數個隱藏層的神經網路通常被稱為深度神經網路，在實務上神經網路可以高達數十層至數百層。深度神經網路也因為層數眾多且層與層間之連結複雜，整個被訓練出來的系統或模式，難以被人類理解，包含參與其中的工程師，也導致人工智慧/機械學習的不透明且難以解析，近年也引起諸多法律上探討。

「深度神經網路」是一種如圖 9 類似人類神經網路(Neural Network) 的方式，透過建構「多層神經網路」的運作，讓人工智慧可以一層一層逐層學習，並進化到可以自我學習的階段，且只要有充分的學習資料輸入類神經網路，不需要人為的幫助它就能自行分析資料找出特徵值。在圖 9 中，如果目標是要辨識出圖右輸出層(Output layer)的方形、圓形及三角形共三種圖形。第一步先將左邊待辨識圖形(28*28=784 pixels)輸入至輸入層(Input layer)，透過層層隱藏層(Hidden layer)的函數堆疊，如同人類神經網路架構。深度學習模型需要透過大量的訓練數據及更強大的計算能力，才能得到更好的預測結果。

深度學習的人工智慧演算法，是一個革命性的進展。以上述圖形辨識為例，技術開發者不須先瞭解或分析方形、圓形及三角形共三種圖形，如同人類成長過程依樣，是透過一次次的經驗去學習到各種圖形的差異；同樣的，深度學習的人工智慧演算法，也同樣地透過大量資料去學習分辨三種圖形差異，並自動產生一個辨識三種圖形的模型(model)。

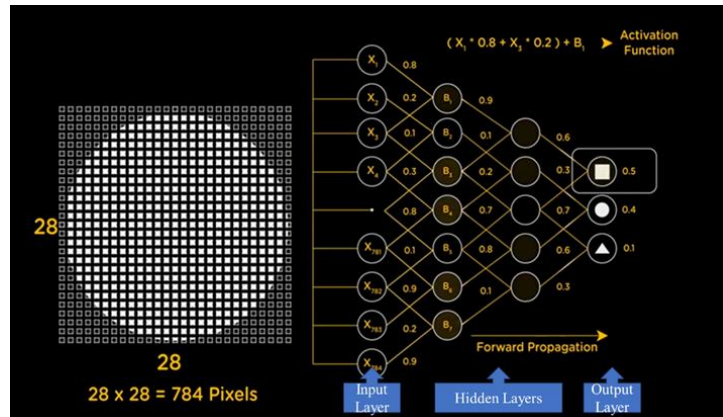


圖 9. 深度學習的運作方式。資料來源：Simplilearn⁴⁰;本文整理

機器學習/深度學習後續對人類最大衝擊的就是 Alpha Go 在一片不看好聲中，擊敗世界第一棋士柯潔⁴¹。最終版本 AlphaGo Zero 擁有更加強大的學習能力，可自我學習，經過僅僅三天的自我訓練，AlphaGo Zero 擊敗了先前發布的版本 AlphaGo，而 AlphaGo 本身已經擊敗了 18 屆世界賽冠軍的南韓圍棋九段棋手李世石；在 21 天達到勝過中國頂尖棋士柯潔的 AlphaGo 大師(Master)的水準；經過 40 天的自我訓練，AlphaGo Zero 變成了更強大，勝過所有的 AlphaGo 版本⁴²。至此，人類在棋類的領域，包含西洋棋、圍棋等，已經永久的輸給電腦，且結果已經不可逆。也因機器學習及深度學習優異的表現，至今仍被寄予厚望是高度自駕車能真正被實現的必要手段，而自駕車操作的人工智慧模型(AI Model)就是依據這些資料而訓練(training)出來的。機器學習與傳統統計的流程如圖 10，機器學習運作需要三個步驟：包含蒐集資料、訓練模式(Training Model)及實際運用。資料從步驟①之蒐集、處理(包含資料清理及訓練模型)，後續步驟②再輸入資料到已訓練中應用，有多次資料的運用流程。此外，機器學習所訓練的模型還需要步驟③除錯(debug)、回饋(feedback)、維護(Maintenance)等。相較下圖 10 右之傳統統計方式較為單純，輸出結果也較容

⁴⁰ Simplilearn (2019/06/19). *Neural Network In 5 Minutes | What Is A Neural Network? | How Neural Networks Work*. <https://www.youtube.com/watch?v=bfmFfD2RIcg>

⁴¹ Silver, D., Schrittwieser, J., Simonyan, K. *et al.* (2017/10/19). Mastering the game of Go without human knowledge. *Nature* **550**, 354–359. <https://doi.org/10.1038/nature24270>

⁴² Deepmind (2017/10/18). *AlphaGo Zero: Starting from scratch*. <https://deepmind.com/blog/article/alphago-zero-starting-scratch>

易詮釋。

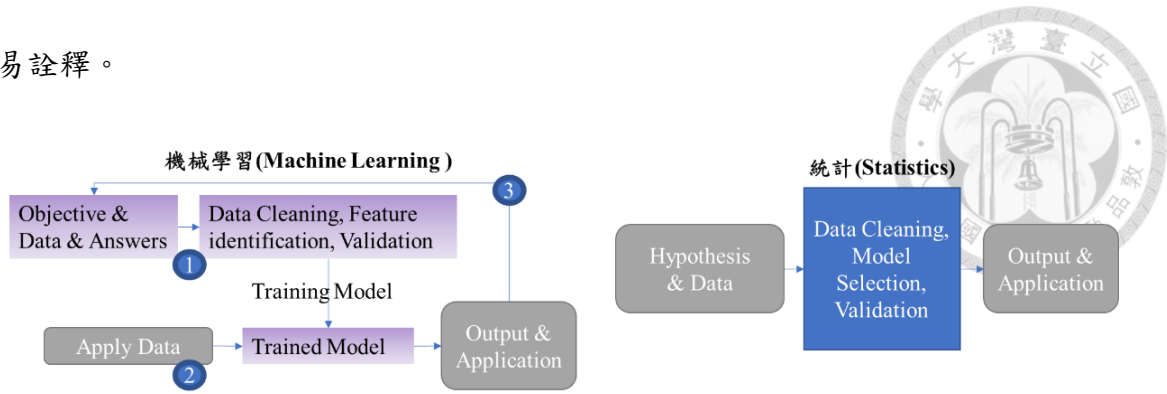


圖 10. 機械學習(ML)運作需要三個步驟：包含蒐集資料、訓練模式(Training Model)及實際運用;圖右為傳統統計方式。資料來源：本文整理

機械學習因為是以資料來訓練模型(model training)，所被訓練出的模型其內涵連程式設計工作者都未必瞭解其運作，故常被視為一個黑盒子⁴³，AI 人工智慧的倫理、透明性、可歸責性、隱私與資料處理迨至今日還是熱門的倫理法律研究議題。2019 年歐盟執委會成立人工智慧高層專家小組(High-Level Expert Group on AI)，訂定可信任 2019 年版的 AI⁴⁴倫理準則(Ethics Guideline for Trustworthy AI);2021 年 4 月歐盟執委會發布《人工智慧法案》(Artificial Intelligence Act)立法草案，並將 AI 用途分不同風險來監管。

除上述人工智慧自身的監管，人工智慧技術機器學習/深度學習導入自駕車開發，除了自駕車蒐集的數據與操作與安全就具有相當關鍵的因素，其他的人工智慧的透明性、可歸責性疑慮，更增添自駕車資料與個資管理的重要。此外，而自駕車操作依據的人工智慧模型(AI Model)，也需要持續即時性滾動式維護，以確認自駕車能適應最新的狀況。資料更新對於機器學習/深度學習相當重要，若有資料缺失或者偏頗而導致的偏見⁴⁵，都有可能導致自駕車功能的失效引起傷害生命安全的疑

⁴³ 機械學習(ML)所訓練出的模型因為多變數且非線性，所以難以清楚理解。

⁴⁴ 申言之，此處所謂「人工智慧(AI)」的主要還是第三代人工智慧技術，機械學習及深度學習所引發的議題。

⁴⁵ 偏見(bias)是機器學習/深度學習常見的問題，可細分成因資料互動而生的互動偏見(interaction bias)、因特定領域既定印象而導致的潛在偏見(latent bias)、而資料選擇不齊或偏頗而導致的選擇偏見(selection bias)等。偏見議題重要且廣泛，本文不作深入的介紹，此處強調資料持續及即時更新的必要性。

慮。在台灣的高速公路就發生自駕車追撞施工的防撞車，或撞擊正在擺放三角錐的工作人員，這都是因為這些防撞車與放三角錐的工作人員影像資料不存在或者資料過少被忽視。綜合上述說明，與本文有關的是以資料驅動的機械學習及其分支深度學習，並非泛指 AI 人工智慧。為了兼顧論文嚴謹及文章易讀性，後續以「人工智慧/機械學習」簡稱；若單獨以「AI」註明之處，一則可能技術有後續發展，人工智慧技術不限於機械學習；二則為尊重引用文章。

目前 Tesla 自駕車是以空中下載技術(Over-the-Air Technology, OTA)技術完成軟體及機械學習模型更新，OTA 技術將於後說明。以上議題已可初見人工智慧運用在自駕車個資與資料問題上的複雜與困難。

表 1. 人工智慧大事記。資料來源：數位時代⁴⁶；本文整理

年代	人工智慧(AI)大事件
1943 年	形式神經元的數學模型 ⁴⁷ 被提出，開創類神經網路研究時代。
1950 年	艾倫·圖靈(Alan Turing)在論文中 ⁴⁸ 預言人工智慧機器的可能，並設計圖靈測試。Alan Turing 又被稱為人工智慧之父
1956 年	John McCarthy 在達特茅斯研討會首次提出人工智慧一詞。
1959 年	John McCarthy 及 Marvin Minsky 在美國 MIT 創立第一個人工智慧實驗室 ⁴⁹ ，開啟人工智慧計畫。 亞瑟·塞繆爾設計出全球第一個自動學習的西洋跳棋系統，機器學習和遊戲 AI 開始發展。

⁴⁶ 郭芝榕 (2016/03/08)，《不是未來，就是現在！人工智慧走入商用領域》，數位時代，載於：<https://www.bnext.com.tw/article/38812/BN-2016-03-02-142445-196> (最後瀏覽日：2021/5/14)。

⁴⁷ McCulloch, W.S., Pitts, W (1943). A logical calculus of the ideas immanent in nervous activity. *Bulletin of Mathematical Biophysics* 5, 115–133. <https://doi.org/10.1007/BF02478259>

⁴⁸ Turing, A. M. (1950). Computing machinery and intelligence. *Mind*, LIX, 433–460. doi:10.1093/mind/LIX.236.433

⁴⁹ MIT CSAIL. <https://www.csail.mit.edu/about/mission-history>

年代	人工智慧(AI)大事件
1980 年	專家系統 R1 (XCON) 出現，全球公司開始研發專家系統。
1986 年	大衛·魯姆哈特等人發明倒傳導類神經網路(Back Propagation Neural Network)，類神經網路研究沉寂多時再度活躍。
1997 年	IBM 超級電腦深藍打敗全球西洋棋冠軍蓋瑞·卡斯帕洛夫。
2005 年	美國 Stanford University 大學開發出自動行駛機器人，贏得 DARPA 挑戰大賽頭獎。
2007 年	Siri 用自然語言處理技術開發 iOS 人工智慧助理軟體，2010 年被蘋果收購。
2010 年	Google 實驗室 Google X 發表自動駕駛車專案(圖片來源：Google) 
2011 年	<ul style="list-style-type: none"> ● IBM 超級電腦華生在益智搶答競賽中打敗節目史上最強冠軍。 ● Google Brain 成立
2012 年	Google Brain 用 YouTube 的 1 千萬張相片自動學習辨識貓臉
2014 年	GoogleLeNet 以 6.7%的影像辨識錯誤率，在影像辨識領域首次接近人類的 5.0%
2015 年	ResNet 以 3.6%的影像辨識錯誤率，在影像辨識領域首次擊敗人類的 5.0%。自此電腦圖形識別超越人類。
2015 年	MIT、紐約大學及多倫多大學開發出貝葉斯程式學習 BPL，讓電腦能舉一反三。
2015 年	Google 子公司 DeepMind 的 AlphaGo 系統用深度學習打敗歐洲圍棋冠軍。

年代	人工智慧(AI)大事件
2016 年	AlphaGo 挑戰世界冠軍韓國職業棋士李世石九段，對弈結果為 AlphaGo 4：1 戰勝了李世石
2017 年	AlphaGo 以精準的 4 分之 1 子差距擊敗中國棋王柯潔，自此 AI 正式稱霸圍棋界。
2017 年	AlphaGo 的團隊在《Nature》雜誌上發表介紹 AlphaGo Zero 文章，是一個沒有與人對弈的新版本，卻較先前任何擊敗人類的版本都要強大。單純藉由電腦間對戰，AlphaGo Zero 經過 3 天的學習，以 100：0 的成績超越了 AlphaGo 的實力，21 天後達到了 AlphaGo Master 的水準，並在 40 天內超過了之前的所有版本

第二項 無人載具的定義與自駕車發展

一. 無人載具及感測技術介紹

隨著人工智慧、大數據、雲端運算、物聯網和邊緣運算之成熟發展，各種以人工智慧為大腦的智慧載具推陳出新，其中，最顯著改變生活的莫過於無人行動載具。無人行動載具包含無人機及智慧車輛等的高速發展正持續在改變我們的產業型態與生活模式。以自駕車為例，最為關鍵之操控系統從逐步輔助人類駕駛、採用先進駕駛輔助系統(ADAS)之半自動化駕駛，到透過運用自動駕駛系統(ADS)之全自動化之無人操控的逐步提高，對於該行動載具操控的型態也在逐步轉變，人與智慧行動載具之間的法律責任歸屬也變得模糊與複雜；此外，在人與無人載具間的互動，例如交通生命安全與自駕車發展、個資保護與產業發展間的權衡更顯得微妙且須與時俱進。因此，如何在科技創新、經濟與社會發展與法律管制間取得平衡，對各先進國家來說已成為一現實上迫切的課題。

「無人載具」依《無人載具科技創新實驗條例》定義為「車輛、航空器、船舶或其結合之無人駕駛交通運輸工具，透過遠端控制或自動操作而運行，且具備以下技術：(一) 感測技術：可偵測及辨識行駛過程之周遭環境或事件狀況之訊息。(二) 定位技術：藉由導航模組或資通訊應用，可進行定位輔助、地理位置傳達，並協助路徑及任務等規劃。(三) 監控技術：監控操作人員透過自動系統與無人載

具間保有持續與雙向之通訊連結，得以掌控整體運程，並得隨時取得無人載具之完全控制權。(四) 決策及控制技術：綜合前三目技術所提供之資訊，進行路徑及任務規劃之決策判斷，進而控制無人載具之因應方式或運行」。無人載具在各國及眾多廠商都已經是重要的發展方向，且不同載具有不同人機操控介面與技術屬性，且因為技術發展快速且影響層面不斷擴大，各國都已經陸續制定相關規範。而道路使用之自駕車因為發展快速且深入民眾生活，故本文先針對自駕車議題來探討。

自駕車雖屬於無人載具的一種，但並非所有自駕車都是屬於無人車，自駕車分級與責任分工將由後面自駕車分級章節探討。現今自駕車的應用領域包括個人車、大眾運輸、快遞貨運，以及農業與礦業專用車。不論設計理念為何，所有智慧自駕車可略分為四大系統，包含「感測」、「認知」、「決策」、「反應行動」⁵⁰。其中「感測」須仰賴感測器(sensors)來偵測外在環境，以程式軟體將蒐集到的資訊過濾處理，並透過來具「認知」、「決策」及「反應行動」等的智慧自駕車大腦來執行決策。「感測器」如同是自駕車的五官，是感受外界資訊的基礎裝備，以下簡略介紹自駕車的感測器技術，以利後續探討自駕車資料及個資之議題。

自駕車感測器主流區分為「被動感測器」(passive sensors)與「主動感測器」(active sensors)兩類，前者負責偵測環境中物體所反射或主動發出的光能量，後者則透過感測器自身主動發送特定訊號並偵測、處理反射訊號來計算該被偵測物件。因兩者各有其優缺點，而現實中自駕車環境複雜且多變，加以自駕車對安全性要求甚高，一般而言會混和使用兩種感測器⁵¹。

1.1 被動感測器

⁵⁰ 季平 (2021/08/04)，《感測器融合技術臨門缺了哪一腳？》，CTIMES，載於：<https://www.ctimes.com.tw/DispArt-tw.asp?O=HK58481XCV0ARASTD6> (最後瀏覽日:2021/11/10)

⁵¹ 林玥彤、張國鈞、蔡玉琬 (2020/06/24)，《自駕車技術與自駕車上路之政策準則》，科技觀測平臺，載於：<https://outlook.stpi.narl.org.tw/index/focus-news?id=4b114100784393680178fc6cfb4b4a44>

被動感測器，係指該感測器自身不主動發出偵測訊號之裝置，又被稱為無源感測器⁵²。因為此類硬體技術與產業鏈已成熟、穩定且性價比高，以影像感測技術為主的被動感測器得以率先使用於自駕車。被動感測技術又可分為二維(2D)及三維(3D)之感測技術，另外依據感測之影像波段，另可分為可見光及紅外光，紅外光感測器可作為包含夜間或低亮度環境時的輔助代替影像感測來源。感測器之感測單元由單一微小的圖元(pixel)所組成，單一圖元透過光電轉換累積的電荷量，決定該個圖元所偵測訊號的強度，並可搭配濾光片可分別偵測不同可見波長的光，取代人眼紀錄顏色及影像強度資訊。

大部分車輛的被動相機感測器系統中，會使用多個感測器來偵測車子周邊多個方向，並將不同影像感測器所得到的資料融合(Data fusing)後，並應用深度感測器(Depth camera)及深度計算演算法，以此建構之影像應用於三維(3D)測距，並將所即時擷取之多個物體建構成 3D 立體動態圖資。

綜上，影像資料的擷取與多影像資料的即時融合是自駕車必要的技術，其中也隱含若其中資訊若含有個人資料在個資法規適法性上困難。目前 Tesla 為以影像式被動感測元件為自駕車主要感測器的代表廠商。

1.2 主動感測器

相對於被動感測器，主動感測器具備訊號發送源，被動與主動感測之比較可見圖 10。主動感測亦可分為 2D 或者 3D 感測技術，3D 感測技術包含結構光(Structure light)感測、超音波(Ultrasound sound)或飛時測距(Time of Flight, ToF)⁵³。其中最廣為應用的飛時測距原理是透過測量光學訊號自來源與目標來回的時間來計算距離。以下介紹三種主動感測器，其中超音波主要用於極短距離偵測，雷達可於雨天或霧氣等惡劣天候中偵測物體，但無法判斷複雜的形狀，光達偵測形狀的表

⁵² 雙語詞彙、學術名詞暨辭書資訊網，國家教育研究所網站，<https://terms.naer.edu.tw/detail/1299326/> (最後瀏覽日：2022/1/15)。

⁵³ WIKIPEDIA. *Time of flight*. https://en.wikipedia.org/wiki/Time_of_flight

現較佳，但易受周遭光線與天候影響：



(1) 超音波感測器(Ultrasonic sensors, SONAR)

超音波感測器特性為歷史悠久，成本最低之技術。但此技術容易受到雨水、灰塵，或其他超音波等環境因素干擾，需同時使用多個感測器以及額外類型的感測器來輔助。超音波能量隨距離遞減，被廣泛適用於短距離環境，如停車及倒車輔助。

(2) 雷達(Radio Detection And Ranging, RADAR)

累積至今長達半世紀實務經驗的成熟技術，雷達(Radar)是第二次世界大戰期間所開發並長期一直被用來精確計算長距離之移動物件如飛機、船艦和其他移動物體的位置、速度和方向。傳統雷達優點為技術成熟、成本低廉、可靠度高，且基於其主動式偵測方式，還可抵抗低光源或惡劣天候條件；相對的缺點為空間解析度低，無法提供物體詳細的空間形狀。而現今另一種成像雷達或稱影像雷達(imaging radar)採用高能量電波，最長可掃描約 300 公尺距離及約 100 度視野內的範圍，帶來 4D 超高畫質的雷達影像，可在任何光照或天氣條件下，將雷達的功能從測量距離、速度、水準方位角擴展到涵蓋距離、方位、俯仰角和相對速度的量測，顯著增強了雷達的性能消除前述解析度的限制，在約 300 米的距離內對不同物體加以區分辨識。隨著自動駕駛等級的不斷提高，成像雷達目前也是熱門自駕車安裝的感測器選項之一⁵⁴。

(3) 光達(Light Detection And Ranging, LIDAR)

光達(LIDAR)亦為主動式感測器⁵⁵，不受天候及夜間低光源條件的限制。光達使用脈衝雷射(pulsed laser)，每秒送出數萬個脈衝涵蓋某一區域，接收雷射光之反

⁵⁴ 邵樂峰 (2021/07/15)，《走進毫米波雷達「4D 成像」時代》，EE Times China，載於：<https://www.eettaiwan.com/20210715nt61-mmwave-radar-4d-image/> (最後瀏覽日：2022/3/17)

⁵⁵ 徐志偉，楊宗賢及鄭致灝 (2019/09/16)，〈探索光達感測器 提昇環周感知能力〉，《電腦與通訊》，載於：<https://ictjournal.itri.org.tw/content/Messages/contents.aspx?&MmmID=654304432061644411&CatID=654313611255143006&MSID=1036010376166635147> (最後瀏覽日：2022/3/17)

射訊號後，將訊號重建成周遭物件 3D 點雲(point cloud)，可偵測物件及其移動，建立最高達數百公尺範圍的 3D 地圖。但解析度差且物件分辨能力低是其主要缺點。

現今運用於自駕車各種主動感測器中，以光達應用最廣泛，其近期發展也最為蓬勃，從傳統笨重昂貴的機械式掃瞄系統(mechanical scanning)、新式的微機電鏡片系統(microelectromechanical mirrors, MEMS)，以及未使用機械元件的系統。未使用機械元件的光達，稱為固態光達(solid-state LIDAR)，包括快閃光達(flash LIDARS)以及相位陣列光達(phased-array LIDARS)。

1.3 感測器之比較分析

上述感測器各有利弊，目前各家百花齊放，尚未有一統之技術。易言之，尚無單一感測器足以應付所有路況及情景，通常必須混合使用，以確保自駕車的行車安全與效能。如前所言，目前業界普遍將光達(LIDAR)感測器視為必備元件，並搭配其他感測技術。然而有部分業者持不同作法，如 Tesla 公司直至今日主要還是仰賴攝影機搭配超音波，而 Wayve 僅採用攝影機。影響感測器選擇的技術層面如下：

- (1) 反應時間：決定感測到物件後之反應時間
- (2) 解析度：決定感測器提供的訊息精細度
- (3) 主被動偵測：一般而言主動感測器偵測訊號是主動發射再予以偵測反射訊號，故能比較不受環境影響；相反的，被動式較受環境條件限制。
- (4) 視野或角度解析度：以涵蓋欲偵測的區域，決定感測器數量多寡
- (5) 感測距離及有效偵測範圍：自駕車因為需要兼顧偵測移動物體及感測物體物理外觀形貌，故要有不同的感測距離考量
- (6) 以 3D 成像區別多項靜態與動態物件之能力：3D 影像為判斷靜動態物件重要依據，以此決定能夠追蹤的物件數量



- (7) 不同環境條件下的操作可靠性與準確性
- (8) 成本
- (9) 資料量

1.4 地理定位(geolocalization)與導航

自駕車的高階路線規劃(higher-level path planning)，除了使用全球定位系統(Global Positioning System, GPS)，也可利用多個衛星系統、擴增(augmentation)技術與額外的感測器來協助定位，達到公分等級甚至更細的精確度，具備如此高幾何精度與詳細內容的資料又被稱為高精地圖(high definition maps)。高精地圖或稱高解析度地圖亦為目前許多自駕車必備的資訊來源，更深入之高精地圖說明於後章節。

綜前述之討論、本文考諸之文獻，整理各主要感測器之優缺點比較如表 2 所示。讀者可從這些感測及感知階段所需要的不同感測器，及可預知的複雜初始資料及整理後資料，瞭解到自駕車資料量的巨大及處理後之複雜，且此些資料與處理過程都牽涉到生命安全，其管理的複雜度遠非過往的案例場景，如路口監視器、Google 街景圖、行車紀錄器、網路應用所可比擬。

表 2. 各種感測器之優缺點比較。資料來源：工研院資通所⁵⁶

感測器種類	光達 LiDAR	雷達 Radar	攝影機 Camera	超音波 Ultrasound
物件分辨能力	Fair	Poor	Good	Poor
物件障礙偵測	Fair	Good	Poor	Good
物件輪廓偵測	Good	Poor	Good	Fair
最遠距離估測	Good	Good	Fair	Poor
車道線追蹤	Poor	Poor	Good	Poor
偵測範圍	Good	Fair	Fair	Poor
惡劣氣候下之爭測能力	Fair	Good	Poor	Fair
低光源條件下偵測功能	Good	Good	Poor	Good

⁵⁶ 徐志偉 (2020/12/10)，《工研院聯網自駕車關鍵技術與應用場域》，IEKConsulting。

除了技術與應用場景之比較，感測器以主動型及被動型分類，其應用距離、價格及網路速度整理比較如圖 11 所示。



圖 11. 感測器特性、應用距離、價格及網路速度之比較。資料來源：STPI; 科技發展觀測平臺。

二. 自駕車對社會及消費者有巨大的利益

如前所述，自駕車與自動駕駛技術帶來對國家、經濟、社會及科技發展帶來廣泛影響，自動駕駛技術集先進技術於一身，能有顯著的引領創新、創造就業，帶動產業發展並結合智慧城市，改變社會生活型態。自駕車除了直接改變車輛產業及交通型態，同時提升各國的產業經濟，包含了龐大的自駕車產業經濟、生產力提高、低碳經濟 (Low-Carbon Economy) 等等，也因此包含美國、大陸、歐盟、新加坡等先進國家都將之列為國家策略性的政策方針。

除了上述優點且市場看好外，自駕車推展與法規研究，最基本也最重要的是在於生命法益的保障。根據報導指出汽車自動化可以大幅提升汽車安全性，以 2015 年數據為例，美國因為車禍受傷的人數有將近兩百五十萬人，而車禍死亡人數逾三萬五千人。行車意外發生的原因有九成四是人為疏失；在 2015 年，幾乎三分之一的車禍死亡人數是和酒駕有關；其他一成的死亡車禍則是因為分心駕駛。美國獨立調查機構「Eno 交通中心」(Eno Center for Transportation) 的分析指出，如果美國有

九成的車輛是自駕車，每年將可以減少 42 百萬次車禍，車禍死亡人數也會減少 2 萬 1 千 700 人，等於是每天可以拯救 60 條生命⁵⁷；英國經濟學人預估 2030 年自駕車發展，在美國會減少道路車輛數達 60%，廢氣排放量達 80%以及降低 90%之交通事故⁵⁸；Tesla 發布的「2020 年影響報告⁵⁹」指出，如下圖 12 在 2020 年美國啟動 Autopilot 功能的 Tesla 電動車、每行駛 100 萬英里僅出現 0.2 次事故，相對的美國整體平均值為每 100 萬英里的行駛里程數出現 2.0 次事故，只有約 1/9 倍的發生率（“In 2020, a Tesla vehicle with Autopilot engaged in the U.S. experienced just 0.2 accidents per million miles driven while the U.S. average was ~9x higher at 2.0 accidents per million miles driven”）。此外，相對自駕車的穩定與一致性，人類駕駛的意外機率，會隨著駕駛人老化而提升⁶⁰，高齡化下因駕駛者身體老化造成包括：反應時間的延長、知覺動作表現衰退、認知方面有關注意力及辨識力降低、視覺感應方面的改變等，嚴重影響安全駕駛能力。包含日本、新加坡及台灣等高齡化社會也是看重此重要性，故自駕車若能成功落實，對於現代社會不會只是一個需求(Need)，而是必要(Must)。

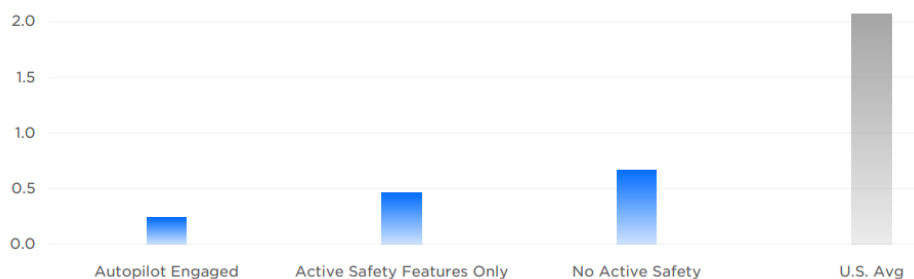


圖 12. 每 100 萬英里的行駛里程數出現事故次數，數據顯示自駕車(<1)相較人為操作(>2)可大幅降低車輛事故。資料來源：Tesla(2020)

⁵⁷ Hod Lipson & Melba Kurman (著)，徐立妍 (譯) (2019)，前揭註 5。

⁵⁸ The Economist (2018/03/01). *Autonomous vehicles are just around the corner*. <https://www.economist.com/special-report/2018/03/01/autonomous-vehicles-are-just-around-the-corner>

⁵⁹ Tesla (2020). *Tesla 2020 Impact Report*. https://www.tesla.com/ns_videos/2020-tesla-impact-report.pdf

⁶⁰ 公路總局網站，《高齡駕駛人駕駛執照管理制度說明》，載於：<https://www.thb.gov.tw/page?node=6b8d246a-ae4-4a05-9b9f-4783c946870b>

自駕車也可以大幅提升旅行的速度，且相較於人類駕駛，自駕車的感知、處理和反應能力都大幅超越人類，因此不需要大幅度的技術突破，也能達到高速旅行的目標。Eno 交通中心估計，推估在自駕車市佔率達到九成的情況下，阻塞狀況則會下降多達六成。由此可見，自駕車對國家、社會與人民影響深遠，相關議題探討不可不慎。

如前所述，自駕車在大規模化運用後將會顯著提升道路交通的安全性，提高交通的運輸效率，有望顯著提升交通安全、提高經濟生產力，並減少燃料消耗、碳排放、節約能源等多方面展現出巨大的社會效益和經濟效益。更明確之量化數據依美國保障未來能源協會 (Securing America's Future Energy, SAFE)的一份研究報告如圖 13，其中至 2050 年社會利益和消費者利益預計將接近 8,000 億美元。另如表 3 所示，自動駕駛將為美國創造包含消費者利益及公眾利益分別大約在 1.6 千億與 6.3 千億美元的經濟效益。

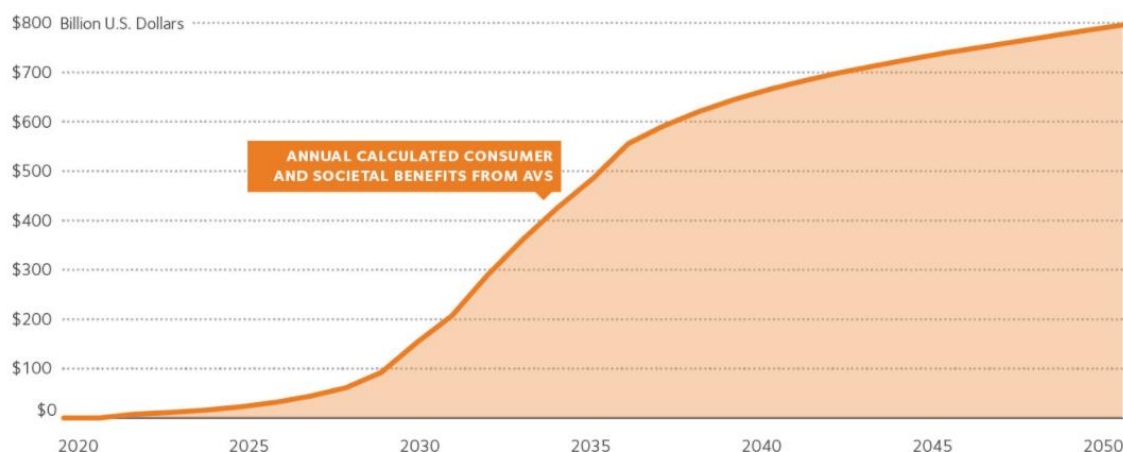


圖 13. 自駕車所創造消費者與社會利益，2050 年預估可達 800 Billion 美元。資料來源：
SAFE⁶¹; David Montgomery⁶²

在上述利益的量化數字，可分為公眾利益與消費者利益，具體細部項目展開

⁶¹ SAFE (2018/09/21). *What are the Societal Benefits of Autonomous Vehicles?*
<https://avworkforce.secureenergy.org/society/>

⁶² David Montgomery (2018/06). *Public and Private Benefits of Automous Vehicles.*

及其預估價值如下表 3：

表 3. 具各種感測器之自駕車至 2050 年產生的公眾與消費者利益預估達美元 796B。資料來

源：SAFE;本文整理

利益	預估價值(單位：美元 Billion)
2050 年度公眾利益	\$633 Billion
減少塞車	\$71 Billion
車禍減少-經濟衝擊	\$118 Billion
車禍減少-生命品質提升	\$385 Billion
降低石油消費	\$58 Billion
2050 年度消費者利益	\$163 Billion
時間價值	\$153 Billion
減少現今計程車服務費用	\$10 Billion
2050 年度利益總和	\$796 Billion

以上多方資料報告都可顯著看到自駕車對於汽車的安全性提升及社會公眾帶來巨大且顯而易見的利益。本文著重在於生命安全的保護，理由在於平衡受法律保護的利益時，保護人類生命仍是重中之重。申言之，若該資料之蒐用為生命法益保護的必要性，生命安全理當優先個資保護考量。

三.自駕車定義與歷史發展

3.1 自駕車歷史與夢想

現行大廠與科技不再滿足於所謂自駕車只是輔助駕駛之工具而已，更已經朝向無人駕駛之型態發展。無人駕駛自駕車的想法與實踐並非今日天外飛來一筆，科幻影集《霹靂遊俠》(Knight Rider) 中先進科技的結晶，一部人性化的「霹靂車」(Knight Industries)⁶³即為一例。「霹靂車」全自動行駛的場景屬於自動駕駛技術的一個夢想，除了前面所提的「霹靂車」影集之外，更早在 1939 年的紐約世界博覽會的展覽和乘車展 Futurama⁶⁴，以當時的概念展示出未來 20 年 (1959-1960 年) 的世

⁶³ 《霹靂遊俠》(Knight Rider) 是自 1982 年至 1986 年起源自美國的熱門電視劇。

⁶⁴ WIKI. *Futurama (New York World's Fair)*.
[https://en.wikipedia.org/wiki/Futurama_\(New_York_World%27s_Fair\)](https://en.wikipedia.org/wiki/Futurama_(New_York_World%27s_Fair))

界可能模型。Futurama 由通用汽車所贊助，通用汽車公司(General Motors, GM)在展會展示自動化高速公路系統(automated highway system)及導引的無人駕駛車輛。由此可見，人類對於自駕車的開發歷史已經有快 100 年時間，甚至早於現今人工智慧技術的發展。自駕車的夢想與發展從沒停歇，2004 年至 2007 年美國國防高等研究計劃署(DARPA) 舉辦自動駕駛挑戰賽讓自動駕駛汽車有了高速發展的契機，2005 年的冠軍由史丹佛大學團隊研發出的 Stanley 自動駕駛汽車奪得，該團隊使用 LIDAR、攝影機、GPS 和慣性感測器等多種感測器組合，蒐集即時資訊並透過電腦軟體技術反覆分析人類駕駛干預處理的緊急情況紀錄，並從中總結出感知模型及決策模型，而這一系列的比賽也促成自動駕駛技術投資熱潮的興起。

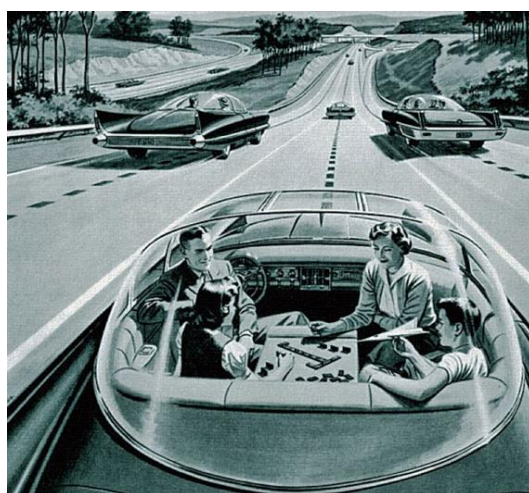


圖 14. 自駕車的理念發展已超過 60 年。資料來源：VeloceToday.com⁶⁵

早於人工智慧技術應用自駕車之前，人們早已應用智慧電子元件啟動在車輛駕駛上開發、運用各種駕駛輔助系統 (Driver Assistance Systems, DAS)，譬如盲點偵測系統、停車輔助系統、後方碰撞警示系統、車道偏離警示系統、適路性車燈系統、夜視系統、主動車距控制巡航系統、碰撞預防系統及停車輔助系統等等，運用感測器、電子運算單元處理並執行以完成各種駕駛輔助功能;近年來因為包括演算法及半導體技術的精進，輔助能力與效能得以大幅提升，將早期駕駛輔助系統已經


⁶⁵ Pete (2014/08/05). *Self-Drive Cars and You: A History Longer than You Think*. VeloceToday. <https://velocetoday.com/self-drive-cars-and-you-a-history-longer-than-you-think/>

更進一步提升為高度自駕發展的先進輔助駕駛系統。並透過物聯網與雲端運算技術提高行車安全及服務品質，並將車輛從單一獨立機器提升為聯網裝置的一環，如前述車聯網之一環。也因為新興技術的興起，使得自動駕駛的進展順利，自駕車市場獲得政府及企業的樂觀期待，根據當年 Google 旗下的 Waymo CEO John Krafcik 說法“在未來的幾十年內，我們將可以預見自動駕駛技術無法做到無處不在，雖無人駕駛汽車也存在一些限制，惟有條件的無人駕駛在技術上可做得好，並且此技術開發過程對產業發展相當具有價值！”自動駕駛技術已確實從 2000 年到 2010 年的探索期(Discovery)因為各種新技術的導入，正式跨越研發期，並在 2010 年 2020 年逐項落實自動化的夢想，並在 2020 年之後進入大量商用期。從今日回顧，正是近 20 年來的研發基礎與經驗累積使得商品化自動駕駛的功能，也從低度的輔助自動化到轉化到具高度的自動操控能力，自駕車的夢想已經從過往嘗試落實到今日的周遭隨處可見的智慧自駕車裡。

3.2 名詞定義

「自動駕駛車輛」在國內簡稱為「自駕車」，「自駕車」所使用之英文字彙包括「Automated Vehicle」、「Autonomous Vehicle」、「Self-driving Vehicle」及「Driverless Vehicle」，SAE (Society of Automotive Engineers)對於自駕車使用技術名詞為「自動(automated)」而不是「自主(Autonomous)」。一個原因是自治「Autonomy」這個詞的含義超出了自動化機電而是意涵具有自主意識。一輛「完全自主(autonomous)」的汽車將具有自我意識並能夠做出自己的選擇，例如車主做出可能傷害生命的動作，而車輛基於自主意識決定趨吉避凶的行為；相對的，一個「完全自動化的汽車」(Fully Automated Vehicle)，會服從命令然後驅動車輛器具自身去行動。技術名詞「自動駕駛」(Self-Driving)⁶⁶通常與「自主」(Autonomous)互換使用。然而，這是兩種不同的使用情境。一個自動駕駛的汽車(Self-Driving Vehicle)可以駕駛自己的一些甚至全部的情況，但人的乘客必須始終存在，並準備採取控制。自動駕駛汽車(Self-

⁶⁶ SYNOPSIS (2022). *What is an Autonomous Car?* <https://www.synopsys.com/automotive/what-is-autonomous-car.html>




Driving Vehicle)將屬於 3 級-有條件駕駛自動化(conditional driving automation)或 4 級高度駕駛自動化(High driving automation)。它們受到地理圍欄的約束，不像一輛可以去任何地方的完全自主的 5 級完全自動化(Full Automation)。本文依循美國高速公路安全管理局(National Highway Traffic Safety Administration, NHTSA)⁶⁷採用的「Automated Vehicle」，基於「駕駛輔助(Driver Support Systems)」到「自動駕駛(Automated Driving Systems)」的差異，將自動(Automated)與自駕(driverless)二者用語分開使用。SAE 更將自駕等級(Automated Driving Level)分為六級。NHTSA 及 SAE 有關自駕車從分級與定義會在下文中說明。

目前因為各國都尚未有如同「霹靂車」的車子，為避免誤導大眾，國際間已傾向不使用「Self-Driving」乙詞。在 1. Autonomous; 2. Automated 兩者間，以 SAE 角度認定「Autonomous car」是指一台自動感測環境，在不需要人類介入可自行決定的車輛。本文採用 SAE 之定義，故英文以「Automated」比較合適，英文縮寫 AV。本文將「自駕車」定為 SAE 所定義之自動駕駛車輛，並以專名線劃分。

3.3 人工智慧技術應用於自動駕駛車輛系統

如前所述，自動駕駛技術開發早於人工智慧/機械學習大量的商業化，例如早期的自動倒車系統或者駕駛輔助系統等低度自動化系統並無人工智慧技術的導入。然而也因為技術的限制，使得早期高度自動化的自動駕駛車輛進展緩慢。伴隨人工智慧技術的發展益發成熟，大約自西元 2015 年後搭載人工智慧技術之智慧自駕車，自動駕駛系統從暫時性地暫代駕駛人執行車輛駕駛任務，到持續性暫代甚至不須駕駛人的高度自駕車已逐步實現。人工智慧自動駕駛已被證實能實際應用並解決各種不同自駕車功能問題，也大幅提升高度自駕車實踐的可能，並因此預期具有極大社會及商業價值前景。是故，許多企業也爭相導入人工智慧技術發展高度自動駕駛車輛。但為了發展高度自駕車，勢必將面臨各種因人工智慧導入而產生的潛在風險及爭議，也因此需要展開風險監理與爭議預防的法制課題。

⁶⁷ NHTSA 網站，<https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety>



由於人工智慧自駕車技術的高度複雜性，且直接與民眾生命安全相關，自駕車的修法必須參照國際間自駕車的技術發展進程與時俱進。中國、歐盟、美國、德國等政府早已針對自駕車行駛投入法規研究，制定相關行車法規，以期釐清自駕車輛之自動化程度下，首要釐清人與車的責任關係。以 SAE 標準 Level 3 自駕定義為例，在此自駕等級之車輛要求駕駛人必須將雙手放在駕駛方向盤上；反之，駕駛人若僅只是坐在駕駛座上並放開雙手，萬一發生交通事故時，屆時責任歸屬難以認定，因此目前各國政府大都僅開放在特定場域或選定路徑中進行測試高度自駕車。在此狀況下，雖然多數汽車廠商與 Google、Apple 等科技業者，依然持續在 Level 4 以上等級的測試與開發，至於目前市面上的量產自駕車，自駕等級主要則是以 Level 2 為主，如 Ford Co-Pilot360、Tesla Autopilot、Nissan ProPilot 2.0 等。

為在自駕車高速發展與競爭下在全球市場取得領先地位，不少業者自 2020 年開始推出接近 Level 3 的 Level 2 功能，如 Ford 推出的 Co-Pilot360 2.0⁶⁸，即新增 Active Drive Assist 駕駛輔助系統功能，允許駕駛者在車內的紅外線攝影鏡頭監控下，適時放開雙手以減少長途駕駛疲累。至於 Tesla 則讓車主可加購全自動輔助駕駛系統 (Full Self-Driving, FSD) 套件，可在特定狀況下提供駕駛輔助功能。

⁶⁸ 蕭有為 (2020/06/19)，《可以放雙手了！福特「Co-Pilot360 2.0」將於 2021 年上路》，8891 汽車，載於：<https://c.8891.com.tw/news/10781> (最後瀏覽日：2021/12/11)



SAE LEVEL	Year	OEM Plans
0-2	2018	Available today. Eg: Tesla's Autopilot, GM's SuperCruise
3-5	2019	  
	2020	    
	2021	    

圖 15. 宣稱擁有 SAE L3-L5 自駕車(AV)廠商⁶⁹，至 2021 年有超過 10 家車商擁有 L3 以上車輛

目前成功運用自駕車的人工智慧 AI 的技術是深度學習，在本文中因為不深究技術細節，故還是以人工智慧/機械學習技術稱之。人工智慧/機械學習運用在自駕車上的過程，如本文前面章節所述可略分為四大系統：包含「感測」、「認知」、「決策」及「反應行動」。其中感測已於前面感測技術介紹乙章節中說明，「認知」、「決策」、「反應行動」三者其整體系統流程架構如圖 16，搭配硬體建立軟體發展平臺，確保自駕車之人工智慧/機械學習/深度學習之演算邏輯符合規範，能與其他控制硬體即時溝通，且自駕車必須以聯網(Connecting)方式保持軟體更新(renew)狀態，車輛感測器提供即時路況資訊至處理器運算，並搭配 V2X 功能，協助自駕車快速計算並即時正確決策，確保行車安全。機械學習/深度學習過程必須包含 1.要有標記圖資資料庫之建立，以提供人工智慧模型訓練所需要的圖資;2.人工智慧/機械學習軟體模型與硬體加速器，如邊緣運算晶片以加速運算，以及深度學習模型的建立;3.人工智慧/機械學習物件感測技術跟物件分類技術，如清楚分辨用路人、汽車、機車、自行車、交通標誌、道路標線等，同時也用人工智慧/機械學習分析並預測這些人、車移動物件行為;4.依據前者之判斷，控制自駕車之煞車、加減速或轉彎。目前上述人工智慧/機械學習驅動自駕車之測試，各國亦有驗證測試環境及法

⁶⁹ The Guardian (2019/05/29). *How Far Away are Autonomous Vehicles?*
<https://www.counterpointresearch.com/far-away-autonomous-vehicles/>

規，要求在人工智慧/機械學習驅動之自駕車上路前先能通過測試。

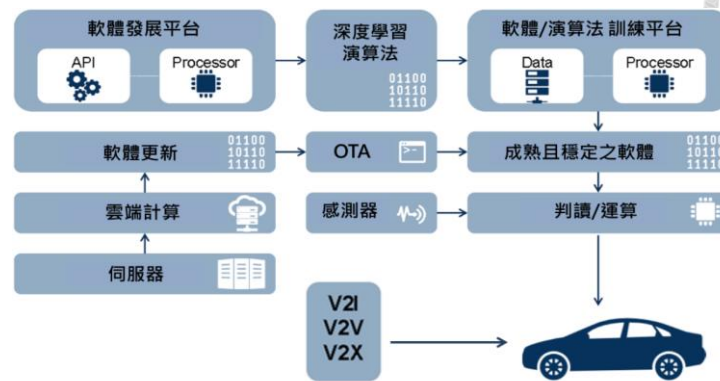



圖 16. 人工智慧/機械學習運用於自駕車的流程架構。資料來源：Mind Commerce(2019)；
工研院產科國際所(2020/12)⁷⁰

四. 現代自駕車分級、定義與責任分工

如本文前面章節所述，並非所有自駕車都是屬於無人車，自駕車分級與責任分工需要客觀且法制化的規範。近年來，國際及主要汽車產業國家和地區的標準法規組織廣泛展開汽車駕駛自動化分級的研究與標準制定。首先是美國 NHTSA 在 2013 年提出將汽車駕駛自動化分為：1.無自動化、2.特定功能自動化、3.組合功能自動化、4.有條件自動化和 5.完全自動化共 5 個等級；德國聯邦交通研究所(BASt)根據研究，將汽車駕駛自動化分為：1.僅駕駛員、2.輔助駕駛、3.部分自動駕駛、4.高度自動駕駛以及 5.完全自動駕駛共 5 個等級；國際自動機工程師學會 (SAE-International) 發布的 SAE J3016 標準提出了 0-5 級分類法，將汽車駕駛自動化分為從無駕駛自動化 (0 級) 直至完全駕駛自動化 (5 級) 在內的 6 個等級；國際標準化組織 (ISO) 與 SAE 組成國際標準聯合制定 ISO/SAE PAS 22736:2021 《道路機動車輛駕駛自動化系統相關術語的分級和定義》(Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles)已經於 2021 年公布。

⁷⁰ 蕭瑞聖 (2021)，前揭註 31，頁 3。



目前國際上產業界及學術界對自駕車的定義普遍採用汽車工程師學會 (Society of Automotive Engineers, 英文簡稱：SAE)J3016 標準(J3016 Levels of Automated Driving), SAE J3016 依車輛自動化程度區分為 6 等級評價為等級零至等級五(Level 0 至 Level 5, L0~L5), 各等級與對應之定義如表 4 所示。SAE 等級 0(L0)是指完全由駕駛人操作, 車輛沒有自動功能, 駕駛人必須負責控制車輛的所有功能, 車輛有基本的警示裝置, 例如: 自動緊急煞車 (Autonomous Emergency Braking System, AEB)、盲點偵測 (BSD)、車道偏移 (Lane Departure Warning System, LDW) 等, 可以協助駕駛人控制車輛, 但沒有任何自動控制的功能。SAE 等級 1(L1)是指具有一種或多種的自動控制功能, 但只能單獨作用, 例如: 車道維持(Lane Keeping Assist, LKA)、主動式巡航定速(Adaptive Cruise Control, ACC)等。SAE 等級 2(L2)是指具有多種自動控制功能並可以同時作用, 例如: 車道維持、主動式巡航定速、自動緊急煞車, 作用為替代駕駛人處理外在行車環境的變化, 減輕駕駛人的負擔, 但駕駛人仍需注意行車環境, 隨時有可能需要自行介入車輛控制。SAE 等級 3(L3)是指車輛可以完成部分自動駕駛任務, 可以有限度的監控行車環境, 例如: 塞車駕駛功能, 讓車輛接手自動跟車、車道維持、停止車輛、停後重啟等功能。L3 為有條件性的自駕, 駕駛人須隨時準備拿回車輛控制權, 在跟車時雖然可以暫時免於人工作業, 但當汽車偵測到需要駕駛者的情形時, 會立即回歸讓人工駕駛。SAE 等級 4(L4)是指在一定條件下(如在高速公路上, 平順的車流與標準化的路標等), 車輛可以自動完成所有駕駛和監控行車環境, 當自動駕駛功能開啟時, 駕駛人不需要介入, 但自動駕駛僅限於特定道路如高速公路、封閉式高架道路上使用。SAE 等級 5(L5)是指在所有條件下, 車輛都可以自行駕駛。自動駕駛可以在所有道路上使用, 可以執行所有與安全相關的控制功能, 即使沒有人在車上也可以自動駕駛, 完全自動化的車輛不再需要方向盤、油門踏板、剎車踏板、方向燈桿等, 人車操作裝置。

加州法律規定所謂自駕車為「自動駕駛汽車」具備自動駕駛技術且已經測試到該車輛符合 SAE International 的《道路機動車輛駕駛自動化系統相關術語的分級和定義》第 3 級、第 4 級或第 5 級定義的任何車輛道路機動車輛自動化系統

⁷¹。SAE 定義第三級以上(L3~L5)的為「高度自動化自駕車」。

SAE 所定義的自駕車等級如表 4 所示，包括無自駕之狀態(SAE 等級 0(L0))，到全自駕(L0)狀態。L1 及 L2 因為駕駛人的介入較多，感測及運算較為單純。SAE 等級 3(L3)算是無人駕駛車的開始階段，迄 2022 年已經有幾款車輛宣稱有 L3 等級，而車輛為因應 SAE 等級 3 以上的安全條件，須具備相當多的先進感測器及資料處理能力，L3 及 L3 以上自駕車，也被稱為高度自駕車，正是與本文探討法規最密切相關的運用場景。

表 4. SAE 所定義之自駕車等級。資料來源：SAE

SAE	自駕等級	方向與加減速操作	行車監控	行為負責	應用環境
L0	無自駕	人類駕駛	人類駕駛	人類駕駛	無自駕
L1	輔助駕駛	人類駕駛 + 單項系統	人類駕駛	人類駕駛	限定環境
L2	部分自動駕駛	人類駕駛 + 多項系統	人類駕駛	人類駕駛	限定環境
L3	條件自動駕駛	車輛系統	車輛系統	人類駕駛	限定環境
L4	高度自動駕駛	車輛系統	車輛系統	車輛系統	限定道路與條件
L5	完全自動駕駛	車輛系統	車輛系統	車輛系統	所有環境

自駕車仰賴先進駕駛輔助系統⁷²與車聯網等先進科技為基礎來實現。其中

⁷¹ “Autonomous vehicle” means any vehicle equipped with autonomous technology that has been integrated into that vehicle that meets the definition of Level 3, Level 4, or Level 5 of SAE International’s “Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, standard J3016 (APR2021).”

⁷² ADAS 是先進駕駛系統技術的統稱，泛指利用安裝於車子上各式各樣的感測器(包含偵測光、速度、空間等參數之感測器，如超音波 (Ultrasonic)、攝影機 (Camera)、雷達 (Radar)、飛時測距 (ToF)、紅外線 (Infrared)、光達 (Lidar) 等)，在第一時間收集車內外的環境資料，進行靜態及動態物體的辨識、偵測與追蹤等技術上處理，因為感測器功能不同，ADAS 應用，皆會採用資料融合 (Data Fusion) 方式處理環境感知。

SAE 等級 3 以上之自駕車相當依賴自動駕駛系統，其中包含光達感測器、影像感測器、高精度地圖以及人工智慧運算等關鍵技術，而資料融合與即時處理的邊緣運算能力更是不可或缺。正是因為自駕車技術門檻相當高及需要高度資料的鏈結，廠商因此透過結盟形成技術互補的合作關係。當前自駕車產業主要由傳統整車廠、零組件供應商、科技公司、晶片業者以及電信業者等構成產業鏈。

		第0級	第1級	第2級	第3級	第4級	第5級
駕駛人工作	駕駛人主導汽車行駛				即使駕駛人坐在駕駛座，但未主導駕駛		
	必須持監督汽車駕駛相關功能，包含煞車、加速與方向控制等以確保安全性				必要時自駕車會要求駕駛者介入	自動駕駛汽車不會要求駕駛人接管駕駛工作	
		駕駛人行為			汽車的自動駕駛特性		
汽車具備的功能	僅能提警告或暫時性協助	提供駕駛操作或煞車/加速等輔助	提供駕駛操作及煞車/加速等輔助		在特定條件下，汽車可自行駕駛		汽車可在所有情況下自行駕駛
功能	<ul style="list-style-type: none"> 自動緊急煞車 盲點警告 車道偏離警告 (Lane departure warning) 	<ul style="list-style-type: none"> 車道居中 (Lane Centering) 或 自適應巡航控制 (Adaptive cruise control) 	<ul style="list-style-type: none"> 同時能車道居中與 自適應巡航控制 		塞車駕駛	區域性無人計程車不一定會安裝踏板與方向盤	與第4級相同，但汽車可在任何條件下自行駕駛

圖 17. SAE 定義的自駕車(AV)自動化程度程度與責任分工。L3-L5 被稱為高自動化自駕車，也代表著越仰賴智慧化技術。資料來源：SAE International;科技發展觀測平臺

2021 年 4 月 30 日，SAE International 更新了其《道路機動車輛駕駛自動化系統相關術語的分級和定義》，編號為 SAE J3016_202104。此更新版本取消並取代了 2018 年 6 月的版本，標記為 SAE J3016_201806。其基本對於自駕級別框架保持不變，有六個級別的駕駛自動化，從無駕駛自動化（0 級）到完全駕駛自動化（5 級）。

2021 年 4 月的修訂版在其介紹中解釋說：“SAE J3016 的修訂版是在 SAE 道路自動駕駛 (ORAD) 委員會和 ISO TC204/WG14 之間通過 2018 年成立的聯合作業組密切合作進行的，透過跨領域及跨國之合作，增加了幾個新的專有名詞和其定義，並進行了多次更正和澄清，以解決經常被誤解的概念並提高檔的實用性，尤其是對於非英語母語者。”根據修訂版，Level 1 級和 2 級現在被稱為“駕駛輔助系統”，3 級到 5 級猶被標記為「自動駕駛系統」。級別 1 和級別 2 系統的新

定義刪除了先前版本將 Level 1 系統稱為自動化的混淆。上面描述六個級別的圖表自 2019 年上次更新以來保持不變，但修訂版提供更清晰的解釋，特別是對於 3 級和 4 級系統兩者的差別。一般來說，Level 3 和 Level 4 系統都只允許在滿足特定條件的情況下自動駕駛。對於 Level 3 之系統，駕駛員需要根據系統的要求重新控制車輛，即當出現故障或不再滿足系統運行所需的條件時。相對的，Level 4 不再要求駕駛員隨時重新控制車輛。因此，配備 Level 4 之系統的車輛不需要方向盤或踏板等傳統控制裝置。

此次修訂還定義了兩個新的相關技術名詞：「遠程協助(remote assistance)」和「遠程駕駛(remote driving)」。SAE 將「遠程協助」定義為在系統不知道自己該做什麼的情況下向自動化系統提供的指導和協助。提供遠程協助的人員不會控制車輛，而只是協助車輛系統。然而，「遠程駕駛」被定義為不在車內的人控制車輛並進行駕駛的情況。SAE 不認為這是一種自動駕駛。SAE 還將「故障緩解策略(failure mitigation strategy)」的概念定義為一種車輛功能，旨在“針對駕駛員長時間未能重新控制 3 級系統或使自動駕駛系統失效的系統故障或外部事件”。


相對於 SAE 之分類，中國大陸國家市場監管總局⁷³（標準委）於 2021 年 8 月 20 日發布了由該國工業和資訊化部所提出針對自動駕駛功能的《汽車駕駛自動化分級》⁷⁴國家推薦標準。《汽車駕駛自動化分級》為推薦性國家標準，推薦標準實施過程中的各相關依據其需求參考使用，該標準將於 2022 年 3 月 1 日正式實施。瞭解《汽車駕駛自動化分級》有助於本文後續中國有關自駕車資料運用之探討。

根據《汽車駕駛自動化分級》公布的定義，並參考台灣物聯網產業技術協會之文章⁷⁵，汽車的自動駕駛等級是以下列 6 個要素進行劃分：

⁷³ 中國大陸國家市場監管總局網站，<https://www.samr.gov.cn/>

⁷⁴ 中國國家標準全文公開系統，《汽車駕駛自動化分級》，標準號：GB/T 40429-2021，載於：<https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=4754CB1B7AD798F288C52D916BFECA34>

⁷⁵ TWIOTA (2021)，〈GB/T40429-2021《汽車駕駛自動化分級》標準制定過程及相關情況〉，載於：<http://www.twiota.org/assets/202109271621061456.pdf> (最後瀏覽日：2022/3/05)

- 
- 1、駕駛自動化系統是否持續執行動態駕駛任務中的目標和事件探測與相應；
 - 2、駕駛自動化系統是否持續執行動態駕駛任務中的車輛橫向或縱向運動控制；
 - 3、駕駛自動化系統是否同時持續執行動態駕駛任務中的車輛橫向和縱向運動控制；
 - 4、駕駛自動化系統是否持續執行全部動態駕駛任務；
 - 5、駕駛自動化系統是否自動執行最小風險策略；
 - 6、駕駛自動化系統是否存在設計運行範圍限制。

基於這 6 要素，中國國家標準再將駕駛自動化系統劃分為 0 級（應急輔助）、1 級（部分駕駛輔助）、2 級（組合駕駛輔助）、3 級（有條件自動駕駛）、4 級（高度自動駕駛）、5 級（完全自動駕駛）共 6 個等級。而這 6 個等級，也有對應的 6 個標準。在汽車駕駛自動化的 6 個等級之中，0-2 級為駕駛輔助，系統輔助人類執行動態駕駛任務，駕駛主體猶為駕駛員；3-5 級為自動駕駛，系統在設計運行條件下代替人類執行動態駕駛任務，當啟動功能時，駕駛主體是系統。各級名稱及定義如下：0 級駕駛自動化（應急輔助，emergency assistance）系統不能持續執行動態駕駛任務中的車輛橫向或縱向運動控制，但具備持續執行動態駕駛任務中的部分目標和事件探測與響應的能力；1 級駕駛自動化（部分駕駛輔助，partial driver assistance）系統在其設計運行條件下持續地執行動態駕駛任務中的車輛橫向或縱向運動控制，且具備與所執行的車輛橫向或縱向運動控制相適應的部分目標和事件探測與響應的能力；2 級駕駛自動化（組合駕駛輔助，combined driver assistance）系統在其設計運行條件下持續地執行動態駕駛任務中的車輛橫向和縱向運動控制，且具備與所執行的車輛橫向和縱向運動控制相適應的部分目標和事件探測與響應的能力；3 級駕駛自動化（有條件自動駕駛，conditionally automated driving）系統在其設計運行條件下持續地執行全部動態駕駛任務；4 級駕駛自動化（高度自動駕駛，highly automated driving）系統在其設計運行條件下持續地執行全部動態駕駛任務並自動執行最小風險策略；5 級駕駛自動化（完全自動駕駛，fully automated driving）

系統在任何可行駛條件下持續地執行全部動態駕駛任務並自動執行最小風險策略。

《汽車駕駛自動化分級》有不同於 SAE J3016 的意義，重要內容包括：

(1). 「駕駛自動化」與「自動駕駛」概念細化分類

本文針對自駕車的定義與英文名詞中即提到不能將現有所有自駕車 (Automated Vehicle) 都假想為等同於自動駕駛車 (Autonomous Vehicle)。與 SAE J3016 類似，大陸《汽車駕駛自動化分級》規定的是駕駛自動化分級，即依據駕駛自動化系統所能執行的駕駛任務情況，將駕駛自動化功能分為不同的等級。其中，0-2 級統稱為「駕駛輔助」(Driving Assistance)，屬於初始級別的駕駛自動化功能；3-5 級統稱為「自動駕駛」(Automated Driving)，屬於相同於 SAE 定義高度自動化自駕的功能。因此，堪認「自動駕駛」對駕駛自動化分級結果的描述，是對等同 SAE L3~L5 的高級別 (3-5 級) 駕駛自動化功能的統稱，而這級別的自駕車輛，也正是高度依賴人工智慧技術的應用領域，人工智慧-資料-安全之間的關聯度也最緊密，三者間議題探討上也最複雜。

(2). 駕駛自動化功能不等同於駕駛自動化能力

《汽車駕駛自動化分級》的主要定位是對汽車駕駛自動化功能進行分級，界定不同級別的駕駛自動化系統需要駕駛人所要承擔的責任，惟於此本文要強調的是不能以依此功能分級評斷駕駛自動化能力和等級。汽車駕駛自動化系統的能力評價需要綜合考慮駕駛自動化功能級別和對應的設計運行條件兩個因素，換言之，自動化級別間的比較是在相同設計運行條件或在相同設計運行條件下才有意義。而這也是國際大廠自行宣稱的自駕等級與官方認證間的落差。是故，本文探討之自駕車個資保護與利用，是因為技術而產生，不會強調與哪一個自駕等級連結。自駕技術之於自駕車個資保護與利用詳細討論於後面第 4 章節，並列於表 21 中。

(3). 各駕駛自動化等級中彰顯安全重要性之理念和要求

針對現今世界上發生的駕駛自動化相關交通事故，《汽車駕駛自動化分級》相

較其他自駕車之自動化級別分類，特別彰顯安全性。例如，針對 3 級駕駛自動化系統提出「適時採取減緩車輛風險的措施」的技術要求。在這種情況下，即使需要依賴駕駛員進行接管的 SAE L3 級駕駛自動化系統，在設計時也應考慮風險減緩措施，從而最大程度的保障車輛運行的安全性。

五. 自駕車市場與展望


面對全球智慧化車輛的崛起，改變汽車的生產、運作與商業模式，同時也顛覆了產業生態及競爭型態，也衝擊到現有的法律規範。各國政府陸續制定自駕車 (AV) 產業政策以加速自動駕駛技術發展，而 Tesla 的成功崛起，科技大廠如 Waymo(Alphabet)、Apple、Baidu、Cisco、Huawei、鴻海等；傳統車輛廠商如 Daimler、Toyota、GM、Volkswagen、Audi、Volvo、Jaguar 等⁷⁶；新創廠商包含理想、蔚來、小鵬、Rivian、Lucid、Canoo 等，眾多廠商競相積極投入下，未來數年自駕車及汽車電子部門將保持高速增長，預計車用電子、車內娛樂和先進輔助駕駛系統市場 2020 年超越目前體量龐大的智慧手機市場⁷⁷。

自駕車由於政府補助、新興技術導入、環保意識、勞力不足及新商業模式等諸多原因推動，各市場研究調查單位報告都對市場成長相當樂觀，根據 2015 年 BCG 發表的自駕車報告，預估到 2025 年自駕車在汽車市場的滲透率會到 13%，約當 1,400 萬自駕車；而 2035 年全球自駕車市場滲透率將成長至 25%，約當 3,000 萬自駕車⁷⁸；根據波士頓顧問公司(Boston Consulting Group, BCG)預測，2025 年自動駕

⁷⁶ CBInsights (2020/12/06). *40+ Corporations Working On Autonomous Vehicles*.
<https://www.cbinsights.com/research/autonomous-driverless-vehicles-corporations-list/>

⁷⁷ 葉芳瑜 (2020/01/20)，《迎向自駕浪潮、掌握產業商機》，STPI 科技政策研究與資訊中心，載於：<https://www.2cm.com.tw/2cm/zh-tw/market/EFA1E560C84342B2B7099A9566220F2A?type=14>

⁷⁸ 曾志偉 (2017)，《由全球產業及專利分析數據 看臺灣 ADAS 產業發展關鍵》，載於：https://www.artc.org.tw/upfiles/EditUpload/file/ccHo/201708/由全球產業及專利分析數據，看臺灣 ADAS 產業發展關鍵_世博.pdf (最後瀏覽日：2020/12/1)。



駛的全球市場產值約達 420 億美元⁷⁹，而 Intel 國際研究機構也樂觀預期，在 2050 年自動駕駛將創造 7 兆美元的「乘客經濟」商機。相關的研究報告對於自駕車市場都相關樂觀；而中國透過政策協助預估 2025 年可達 50%⁸⁰，且逐年快速上升；依 McKinsey 預測，到 2025 年預計可達 2,000 億美元以上產值；IHS Markit 預測，全球自動駕駛(Automated Driving, AD)量產汽車將在 2025 年上市，估計初期銷量可達 60 萬輛；到 2035 年年銷量將達到 2,100 萬輛，約占當年總汽車銷量的 10%，在北美市場自動駕駛占比可達 29%，中國大陸占比可達 24%，歐洲市場份額占比可達 20%。綜上可知，在可見的現在與可預見的未來，不論是哪家市場調查機構都相當看好自駕車市場及前景。

此外，因應巴黎氣候協議及公民環保意識抬頭，各國政府陸續訂出更嚴格的燃油引擎效能規範及獎勵智慧自駕車辦法，導致傳統汽車因售價持續攀高而難以擴大市佔及智慧電動車的快速成長普及；加上美中貿易大戰對經濟帶來的衝擊，2019 年全球汽車銷售量約為 9,100 萬輛，比起 2018 年減少 4%。此種趨勢，加速各大車廠往智慧自駕車發展，如在 2020 年初的 CES 2020 展上，包含 Nissan、BMW、Daimler、Ford 等汽車大廠，紛紛展示自家在智慧車聯網的研發成果。而 Toyota 更在大會上宣布，將啟動 Woven City 的智慧城市計畫，計劃在日本靜岡縣打造實驗城市，為便於為自動駕駛、電動化、共用等，進行測試與驗證。在 2020 年新冠疫情催生汽車產業轉型，自駕車更加速普及化，因疫情衝擊，更大幅衝擊全球汽車的銷售狀況。根據 Marklines 公布的資料顯示，2020 年上半全球銷售總計 3,215 萬輛，相較於 2019 年同期衰退幅度高達 27.7%。由於全球經濟已受到嚴重衝擊，即便日後特效藥、疫苗問世，現代汽車集團認為全球汽車銷售量預估得到 2023 年才會恢復到 2019 年的水準。在短期內銷售量難以恢復到正常水準，加上人工智慧運算能力提升、各國政府積極發展智慧交通，也讓各大汽車廠商加速朝自駕車、車聯網發展，為後疫情時代預先做好準備。

⁷⁹ 葉芳瑜 (2020)，前揭註 77。

⁸⁰ 黃嫻 (2020)，《自駕技術來勢洶洶，5 年後中國一半新車都是自駕車》，載於：<https://technews.tw/2020/11/12/self-driving-cars-in-china-will-boom/> (最後瀏覽日：2020/12/1)。



六. 自駕車其他技術介紹

自駕車之所以被稱為移動的超級電腦在於廣泛運用先進技術，且各家使用之技術所有差異，難以全面涵蓋。以下介紹主要技術，並說明可能對法規衝擊：

6.1 車聯網(Vehicle-to-everything, V2X)

車聯網(V2X)是物聯網的一種，是專指車輛的聯網技術。如圖 18，當車輛其它車輛間或者其他車外裝置連結，互傳資料或程式，聯網化的能力使得這些車子被視為聯網車。車聯網是將汽車和其他車輛或是其他可能影響的裝置所進行的通訊，常見的廣義車聯網包含有 V2I (汽車對基礎設施、汽車對道路系統)、V2N (汽車對網路)、V2V (汽車對汽車)、V2P (汽車對用路人)、V2D (汽車對裝置)。為了提升自駕車的安全性，及避免單一車輛的視角盲點，所以現在結合智慧城市中的智慧裝置，形成一個智慧網路。車輛網有以下 5 種主要模式：

- Vehicle to Infrastructure (V2I)：車輛和交通基礎設施間的通訊，以獲取有關事故、建築、停車等有關資訊。
- Vehicle to Vehicle (V2V)：車輛之間的通訊(通常包括位置資訊等)，可避免交通壅塞和事故。
- Vehicle to Cloud (V2C)：車輛與基於雲的後端系統之間的通訊，使車輛可以處理服務和應用程式間發送的資訊和命令。
- Vehicle to Pedestrian (V2P)：車輛、基礎設施和個人移動裝置間的通訊，以告知用路人環境，從而實現安全性、移動性和環境改善。
- Vehicle to Everything (V2X)：車輛與其他物體或道路使用者間的任何資料交換或通訊，如：交通號誌、道路標記等。

大部分消費者希望所擁有的汽車如與電腦和智慧手機般的功能，而 OEM 廠商正在採用聯網的解決方案來提高銷售量。2030 年，將有 30%的企業依賴數據支

援的服務和共用移動性⁸¹。

美國交通部 US Department of Transportation (USDOT) 於 2000 年左右提出聯網車 (Connected Vehicles) 的概念，目標是藉由上述 V2X 通訊技術提升道路安全 (Road Safety)。主因為 DOT 蒐集美國的車輛事故相關數據分析，有很高比例是在城市間，車輛間因為建築物或者其他建物遮蔽視線而造成事故，如圖 2 十字街口兩個方向的車被街口的建築物擋住視線，駕駛人或車輛感測器在感知到人車後，人與車輛只能反應時間與距離不足，造成難以避免的車禍事故。此種為非視線(Non-Line-of-Sight, NLOS) 的問題，用路人或車輛前述之先進技術，包含光達、雷達、超音波或高精度攝影機等，也會因無法偵測到可能相撞的來車訊號導致事故發生，因此，即時是已經安裝先進感測器，採用各先進技術的智慧自駕車而言，NLOS 也是棘手難題。利用 V2X 解決 NLOS 問題，主要可行的解法是使用此通訊系統來廣播每一台汽車的位置相關資訊 (如：GPS 位置、車速、車頭方位等)，聯網車之運作如圖 18 在接收周遭車輛位置相關資訊後，即可計算彼此相撞的可能性，如果風險很高，就立刻警示駕駛人以達到安全防撞的效果。其中針對車輛與用路人通訊提供用路人警示服務。

前述狀況在世界衛生組織公布《Global status report on road safety 2018》⁸²亦反應出相同問題。參諸該報告的數據，2018 年有將近 135 萬人死於交通事故，其中用路人和腳踏車騎士占全球道路交通死亡人數 26%，機車騎士則占有所有死亡人數的 28%，而機車高度使用的東南亞地區所占比率更是提升到 43%，交通意外同時是 5 至 29 歲年齡層的主要死因。因此車輛聯網與智慧化為強化對用路人、自行車、機車等交通弱勢族群的保障之必要，特別針對弱勢道路使用者包括：用路人、輪椅使用者，嬰兒車、滑板、賽格威、速度在每小時 25 公里以下的自行車和電動自行車以及摩托車等。

⁸¹ 古涵詩 (2021/12/09)，《連網汽車資安發展趨勢與重要國際規範》，IEK 產業情報網。

⁸² WHO (2018/06/17). *Global status report on road safety 2018*.
<https://www.who.int/publications/i/item/9789241565684>

綜上之有關車聯網之論述，足見該技術對於智慧自駕車之運作有其安全上的必要性。此外，車聯網亦可視為是如圖 1 智慧城市的一環，其資料與疑似個資的蒐用與傳輸更值得探討。

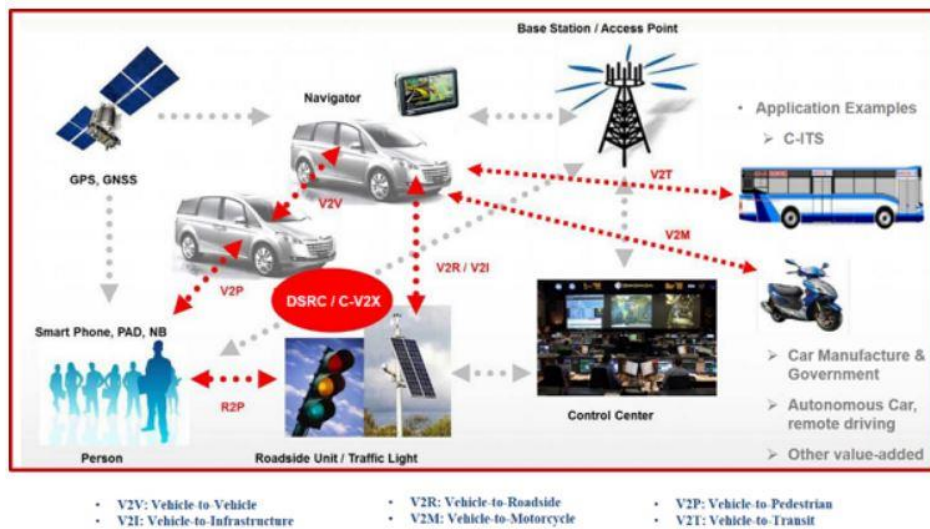


圖 18. 車聯網技術示意圖。資料來源：工研院⁸³

6.2 邊緣運算(Edge Computing)

「邊緣運算」是自駕車高要求反應低延遲性下必要採用的技術之一，近年來因為晶片的快速發展已相當普及且廣泛應用於自駕車，邊緣運算是一種分散式運算架構，將服務功能、應用程式、數據資料的處理與運算，由過往集中雲端中心，改由邊緣節點進行處理。邊緣端因為較接近用戶終端裝置如感測器或運算裝置，如此便可以加快資料處理與降低資料的傳輸負荷，提高反應速度，減少延遲性並提高資料隱私保護。

根據 Gartner 研究顯示自動駕駛車一天產生高達 4,000 GB 的資料量⁸⁴，因此須要能夠在要求在低延遲的處理行動、網路覆蓋率不佳、網路連線不穩定等狀況下

⁸³ 工研院資通所 林港喬、黃譽維、曾恕康 (2020/11/19)，〈C-V2X 與自駕車結合之應用〉，ITRI College+，載於：<https://collegeplus.itri.org.tw/2020/11/19/c-v2x> 與自駕車結合之應用/ (最後瀏覽日：2021/4/8)。

⁸⁴ 陳右怡 (2018/03/29)，〈A.I.邊緣運算趨勢下，五大終端載具成首波落地目標〉，IEK。

採用邊緣運算。由於國際大廠 Tesla、Google、Apple、Audi 等皆積極投入自駕車應用的發展，如 Tesla 已宣布開發自有自駕車 AI 晶片，未來國際大廠在自駕車架構上，有極高的邊緣運算需求。



表 5. 自駕車邊緣運算需求。資料來源：陳右怡，IEK(2018);本文整理

需求指標/必要性	自駕車現況
延遲性要求/必要性高	自駕車所有資料運算反應時間需在 10ms 內完成，須使用邊緣運算。例如前述的資料融合及物件識別，都是直接與安全相關，低延遲性要求非常高。
網路頻寬/必要性高	須考量大量資料同時蒐集、運算即傳輸的需求，網路頻寬不足或者連線不穩都會直接影響到安全問題
網路覆蓋/必要性高	在偏遠寬頻覆蓋率不佳地區，考量網路可能中斷的情況
隱私與安全/必要性中(視法規規範)	<ul style="list-style-type: none"> ● 車輛移動軌跡因各國車輛法規及隱私要求可能需要獨立存放在車內 ● 資安問題，必須在車內完成

另外，因為以人工智慧/機械學習運作在影像辨識具有較傳統演算法的優勢，已經被廣泛應用於自駕車且被晶片廠商。包含物件辨識，人臉辨識等都可採用晶片處理。人工智慧/機械學習資料巨大且須要處理即時，且應用到張量(tensor)運算，故計算量大所以需要以特製化晶片化來加速運算。

6.3 資料融合(Data Fusing)

所謂智慧自駕車除了需要感測器如錄攝影機和雷達等以感測周遭的世界，除此也需要運算能力與先進的機器大腦，整合分析眾多有時可能產生衝突的不同來源資料，進而產生的單一旦精確視野，如同人類的雙眼融合(Binocular Fusion)過程。對自駕車來說，「資料融合」顯然是相當重要的前提，但要加以實現卻是項重大的技術挑戰。如下圖 19 所示，不同的感測器，如光達(LiDAR)、超音波(Ultrasound)、攝影機(camera)及雷達(Radar)等有不同的感測距離極感測的空間角度。

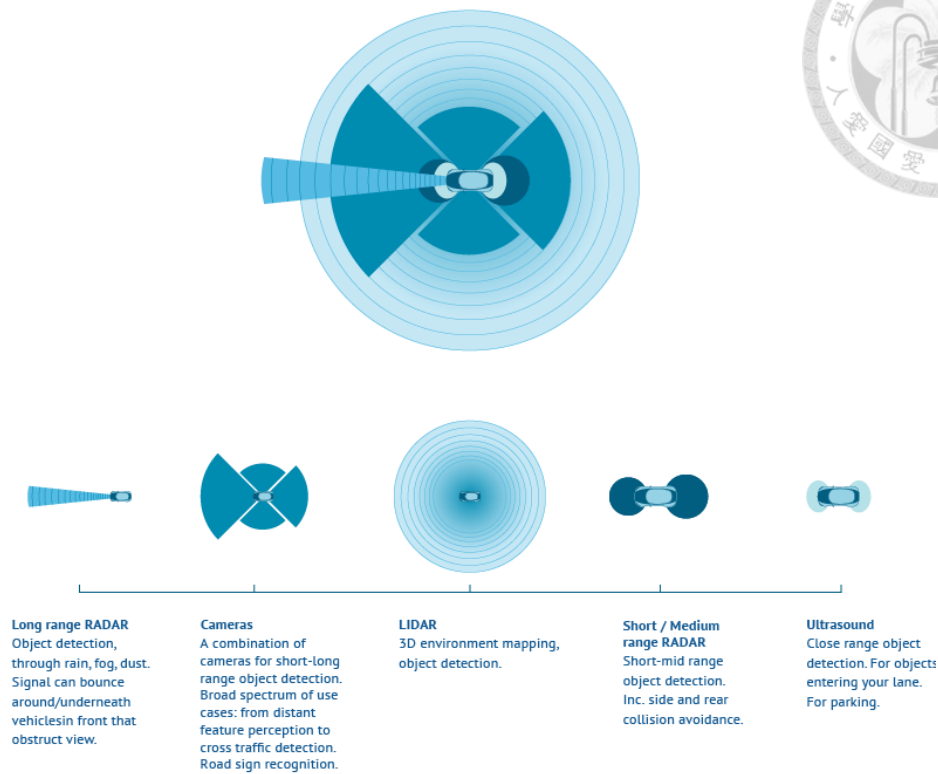


圖 19. 自駕車感應器與涵蓋範圍。資料來源：WEVOLVER⁸⁵

在自駕車運行之前，依據不同的自駕等級需要瞭解其車輛位置、周遭環境，以及路上可能碰到的事物。目前等級 L1 及 L2 的自駕車已裝設位置及影像感測器，協助定位及判斷車況如車輛、單車騎士和用路人等危險狀況。等級 L3 以上的自駕車因為必須能夠在有限的環境下自行駕駛，也與高解析度地圖資料整合，具有對道路更完整的瞭解與準確的動作判斷與反應，是故資料融合為其能實踐關鍵技術。一般也將 SAE 定義 L3 以上自駕車車輛稱為高度自駕車。

⁸⁵ WEVOLVER (2020), 《2020 自動駕駛技術報告 (2020 Autonomous Vehicle Technology Report)》, 載於: <https://www.wevolver.com/article/2020.autonomous.vehicle.technology.report>。

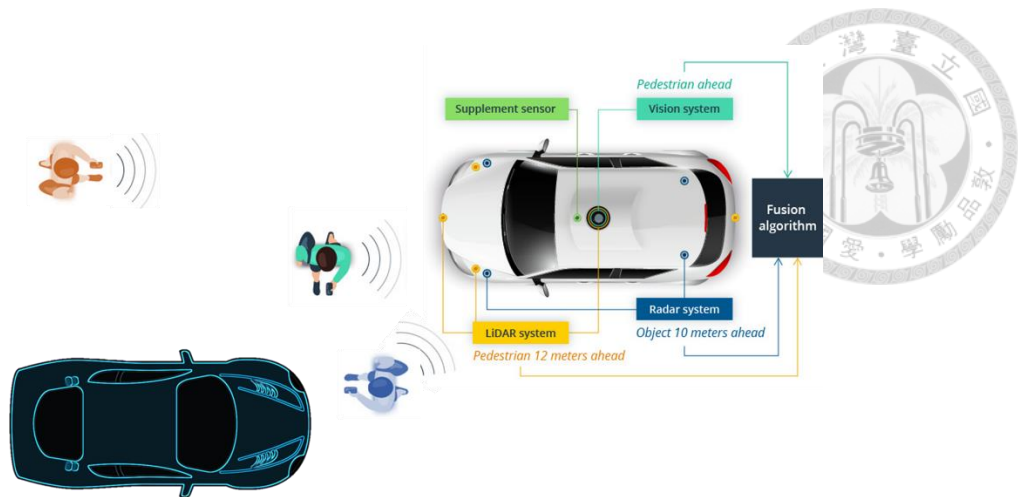


圖 20. 自駕車會遇到不同的緊急狀況，對於單一物件的警示須透過不同感測器並將影像融合以作為後續動作判斷。資料來源：Intellias Global⁸⁶;本文整理

基於安全考量，高度自駕車必須能夠全天候、精準、縝密地感測並能如人類瞭解、分析周遭環境，而最後關鍵在於車輛必須能與道路動靜態物件，如用路人、車輛、雜物等即時互動反應，並能在確保不同天候條件、光源亮度及分布、物件位置、物件型態等條件下操作都安全無虞，而且至少要有相同或高於人類的立刻反應。要準確察覺環境並做出安全的駕駛決策，需仰賴結合不同技術的感測器，利用各感測器特性截長補短，如同人眼的雙眼視覺融合，自駕車亦透過資料融合這項技術將來自不同感測的資料進行處理，有效地建構出取代並超越人眼感測的資訊。

資料融合不但是需要多種資料的融合，且必須在極短時間內完成從蒐集、處理及利用。這些過程一定會蒐集到包含車牌、人臉及人資體動作等資料，資料並需要進一步判斷包含人的肢體動作、臉孔等。是故，此技術所牽涉到資料若為個資，就有可能侵害隱私的可能。

6.4 生理偵測技術

車輛運行的安全，除了車況的感知與反應外，如前所述，車輛意外有逾 90%

⁸⁶ Intellias (2020/04/30). *The Way of Data: How Sensor Fusion and Data Compression Empower Autonomous Driving*. <https://intellias.com/the-way-of-data-how-sensor-fusion-and-data-compression-empower-autonomous-driving/>

以上都是因為人為所引起，這些人為因素若能偵測且預先警示，預期可為行車安全提供良好輔助。包括監控駕駛者的身體、生理或行為特徵等生物特徵，如：駕駛者分心與疲勞、打盹、心跳數據、眼球移動監測、人臉辨識等的駕駛者監控系統(Driver Monitoring System, DMS)就因應而生。駕駛者監控系統是一種汽車安全系統，駕駛者監控系統最早是於 2006 年由 Toyota 所提出，並導入其 Lexus 車款，用以監控駕駛者的注意力，並與碰撞預防系統共同運作。目前駕駛者監控系統的技術已經從單純的偵測及警示功能，已經提升到評估駕駛的行車習慣並推論風險，並可與保險業者合作的使用率保險車險⁸⁷。另外，在美國高速公路交通安全管理局(NHTSA) L3 等級的規定「可執行自動駕駛，但提供駕駛者足夠舒適的轉換時間進行人工駕駛」，故等級 3 的自駕車若有意外事故，駕駛人與自駕車製造業者的責任釐清就很需要駕駛者監控系統的輔助。

駕駛者監控系統因為技術成熟，且價格大眾化，已經廣泛應用於商用運輸車隊駕駛行為監控，這些技術可望陸續導入一般民生自動駕駛車上。

6.5 高精度地圖(High Definition Mapping)

高精度地圖(或稱高精地圖、高解析地圖)是實現自駕車的必要性且基礎技術之一，沒有高精度地圖就失去安全的自動駕駛基礎。高精地圖擁有公分等級⁸⁸的極高精度，擁有精確的車輛位置訊息和豐富的道路數據資訊，例如精準路寬、車道數、不同車道的交通規則屬性為何，都必須要在地圖資訊上面呈現出來，這些資訊可以幫助自駕車瞭解並分析路面複雜訊息如坡度、曲率、道路邊界、車道位置、交通號誌等，構建類似於人腦對於空間認知的功能，是實現自動駕駛的關鍵，因為自駕車系統就是要取代理人類駕駛，高精地圖的尺度必須與真實世界相符，所謂的「高精地圖」並非將 Google 地圖的圖資導入自駕車當中就可以了。綜上，自駕車所需的地圖(如圖 21)不論在精度上或維度上都遠高於 Google 地圖。

⁸⁷ 現代保險雜誌 (2018/03/27)，《InsurTech 保險全新觀念 國泰產險推出 UBI 車險》，載於：<https://www.cathayholdings.com/holdings/information-centre/intro/latest-news/detail?news=xiRuT0hdz0CdtiOwP5pD3w>

⁸⁸ GPS 的誤差大約是在幾公尺，故高精地圖精度是其百倍

從資料-個資轉化的角度，高精度地圖若結合其他個人直接或間接可識別之資訊，資料控制者可輕易自動化剖析每個用路人的行為特徵。

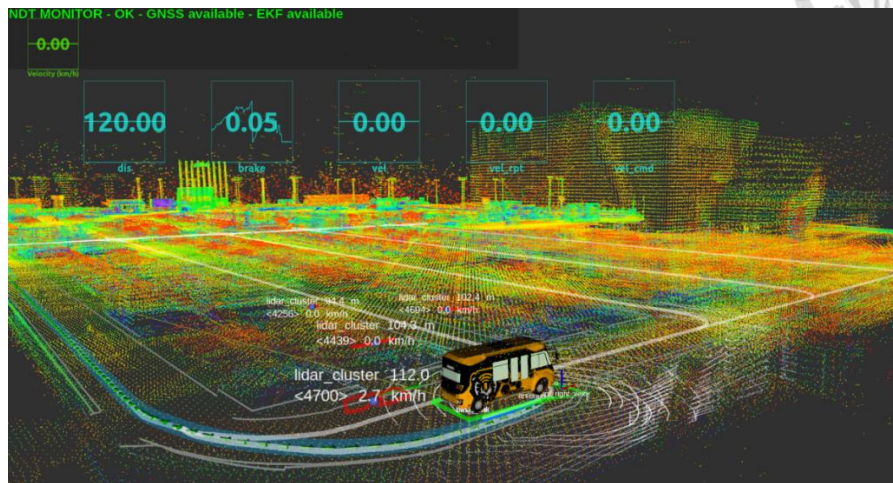


圖 21. 高精地圖態樣，不論解析度或維度上遠高於 Google 地圖。資料來源：科技新報⁸⁹

6.6 OTA (Over-the-Air Technology, OTA)更新升級

OTA 是英文 (Over the Air Technology) 的縮寫，OTA 中文翻譯為「空中下載技術」，OTA 成功的範例是指通過電信網路對手機進行遠程管理的技術。OTA 技術的應用，使得移動通信不僅可以提供語音和數據服務，而且還能提供新程式或服務下載，也使得手機的更新與管理更靈活。

隨著車子越來越聰明，車就如同電腦跟手機，需要更新維持運作順暢，各家車廠，特別是 Tesla 也在加速車輛智慧化，使 OTA 軟體更新變得更重要。軟體更新除了提供新功能或服務外，在自駕車因為牽涉到安全問題，包括電腦修補漏洞，或是移除後門等，這些都需要透過軟體更新獲得；另外若自駕車有運用到人工智慧/機械學習，而如街道車禍資料需要更新地圖資料或模型時，OTA 更是有其必要。OTA 應用於車輛的現況，目前車廠除了自己閉門造車，也在過去幾年開始與系統

⁸⁹ 邱捷芯 (2021/04/18)，《告別老司機，自駕車的導盲犬，為什麼高精地圖這麼重要？》，科技新報，載於：<https://technews.tw/2021/04/18/autonomous-cars-high-definition-maps/> (最後瀏覽日：2021/12/15)

商合作，開發 OTA 功能。BMW 2020 年 7 月宣布，會在配有 iDrive 7 系統的車輛，開始逐步提供 OTA 服務，包括更好的語音辨識、導航圖資更新等。Nissan 也提供配有 Nissan Connect 的車款，透過 Wi-Fi 更新服務。南韓現代、中國比亞迪等車廠也都完成 OTA 部署。賓士與 NVIDIA 聯手，Toyota 則與車用零件大廠 Denso 合作，也正在緊鑼密鼓打造自己的 OTA 系統。電動車部分，福斯則與系統提供商 Continental 合作，替旗下最新電動車 ID.3 提供 OTA 服務⁹⁰。

以 Tesla 為例，從自動輔助駕駛、語音控制元件、車內影音娛樂等，全都是透過軟體 OTA 更新提供。因為 Tesla 的車輛都配有自動輔助駕駛 (autopilot)，電腦輔助功能已從過往單純的行車電腦，控制車輛狀況之外，到現今自駕車應用時必須監視路況，處理大量影像資料完成任務。舉一重要案例，Tesla 的動力全靠電腦控制電動馬達的電流配置，如果不保持更新，不僅會危害電池壽命，更可能有安全疑慮。此外，Tesla 採用數位孿生 (digital twins) 技術，每輛出廠車，都有一輛虛擬車存在資料庫裡，需要車輛保持連線，持續回饋數據，可以讓製造及維護端快速累積經驗，用來改進製程及提升服務品質。過去十年來，Tesla 的軟體已更新數百次，光是 2020 年就有 60 幾次更新，這些更新其實造就了今天我們看見的 Tesla，從自動輔助駕駛、語音控制元件、車內影音娛樂等，全都是透過軟體更新提供。而 Tesla 從一家缺乏經驗的新手車廠，初期自駕車許多設計尚不成熟，透過了 OTA 技術修補過去的不足跟錯誤，將手機運作的成功經驗套用在智慧自駕車上，將電動車的智慧與連線優勢徹底發揮，獲得巨大成功並保持在市場上的優勢。

OTA 是一種已經應用於電腦、手機及自駕車上的成熟技術，OTA 技術優勢在於透過軟體更新，而非花費大量金錢與時間每次都是更新硬體，有其**降低成本及安全上的必要性**。然其要求就是硬體必須已經有超過現有需求的規格(或稱為「超規」)。舉例來說，手機要能一直用軟體來更新功能，前提是手機目前的 CPU、鏡頭規格、

⁹⁰ Chen Kobe (2020/08/18)，《為什麼汽車需要軟體更新？OTA 能帶來哪些好處？》，科技新報，載於：https://technews.tw/2020/08/18/why-car-need-ota-what-good-in-it/?fbclid=IwAR2AudT5CiBW4PAXHpP2Rb2iAthEIPyydrtsPQ-ga9Z_crG9fG71F-5bHYY (最後瀏覽日：2022/4/11)。

DRAM、其他感測器規格與數量都是超過現在的版本軟體(Version 0)所需規格，以在下一代新版本軟體(New Version)更新時，硬體還能夠操作;反之，使用者必須購買更高等級硬體規格手機以利更新軟體，享受新服務。自駕車硬體的「超規」在理論上就是跟「資料最少蒐集原則」有所違背。

第三項 資料是石油

因為資料如 21 世紀之石油，其重要等同於 20 世紀的土地、資本、勞力等，重要性不言而喻。而自駕車擁有如此多的資料，且可能透過聯網形成智慧城市的一環，擁有如此多的巨大且質優的資料，自駕車資料的運用重要性不言可喻。以下就智慧自駕車應用的觀點，瞭解其資料的重要程度與運作方式，並以不同觀點探討自駕車資料的意義。

一.自駕車資料量巨大

自動駕駛所需的運算有數個執行步驟：感測、處理、(即時)決策並依該決策做出反應，每個階段都需要不同的運算程度及類型。參諸 2017 年 Intel 資料顯示單一自駕車的一天需要資料量，將高達 4 TB⁹¹的資料量，大量需要處理的資料，以影像感測資料量而言，每秒將有 20~40 MB；光達 (Lidar) 資料量為每秒更高達 10~70 MB。加上雷達、超音波、GPS…等車輛週邊零組件的資料，再經高速運算後，才能即時執行車輛安全操控的目的⁹²。雖然每家自駕車的硬體及軟體處理不盡相同，但面對如此巨大的資料量，也讓當年的 Intel CEO Brian Krzanich 以“我們是資料公司(We are a DATA company)”定位該公司。

相對的，以一個街口監視器，分別以不同壓縮技術的儲存比較，以 CIF 及 4CIF 比較(CIF：352X240 Pixels；4CIF：704X480 Pixels)，每天約為 10~100GB(如表 6)。

⁹¹ T 是 Tera 的縮寫，代表 10^{12} ; G 是 Giga 縮寫，代表 10^9 。4TB=4,096GB

⁹² 江柏風 (2017/10/23)，《Intel 如何跨入巨量資料的汽車電子新領域》，IEK。

這數量是單台自駕車的 1/40~1/400;換言之，單台自駕車所蒐集的資料約為 40~400 台監視器的資料。

表 6. 不同格式與儲存容量。資料來源：中華技術專題報導⁹³;本文整理

影像壓縮技術 特性	H.264		MPEG-4		M-JPEG	
	CIF	4CIF	CIF	4CIF	CIF	4CIF
傳輸速率(30FPS)	0.8Mbps	10.8Mbps	1.2Mbps	2Mbps	5Mbps	10Mbps
儲存容量/ 每天	10GB	13GB	13GB	21GB	35GB	100GB
壓縮率	200:1		150:1		10:1	

當然，以上是粗估的數據，會因不同各家硬體技術及軟體發展而有所不同，然而，如前所述，自駕車未來並非一個單一個體，若要成功的運作及提高安全性，則自駕車會與智慧城市連成一體，其所見的數據量與影響遠非傳統監視器所可比擬。

二. 資料商機龐大

對比於在 20 世紀，人們掌握石油就掌握全球話語權;到了 21 世紀，世界的資產則藏在資料(Data)裡。資料的利用推動著今日人類社會運轉，使得資料成為新時代的經濟源頭，也是最重要的資源與資產。《經濟學人》宣稱，「資料已經是所有成長與改變的驅動力。」於是乎所謂的《資料經濟》(Data Economy)被各國視為顯學，不同行業與不同企業也互爭雄長，避免在資料驅動經濟時代被遺棄⁹⁴。

資料的商機可從 Facebook 與 Apple 間的爭辯中略窺一二。在 2021 年年中兩家科技巨擘，起源於 Facebook 對 Apple 針對其平台開發商的隱私的條款不滿，兩家公司因此做出公開的對戰。Facebook 在聲明中，援引 Deloitte 的調查，指出 44% 的中小型客戶在疫情衝擊下，開始在社群媒體上增加利用個人化廣告；然而在沒有個人化廣告下，根據 Facebook 的數據顯示，小型客戶花相同的預算，銷售額減少

⁹³ 林啟豐、劉邦俊等 (2011/07)，〈數位元影像平臺與監控系統之整合應用〉，《中華技術專題報導》，No.91。

⁹⁴ 天下雜誌第 637 期 (2017/12/06)，《數據經濟特輯》。

60%以上。

以 Facebook 觀點，強調該公司正為小型或微型企業說話，並表示：「我們現在正在採取措施，因為我們聽到了你們中的許多人，特別是小型企業，你們擔心蘋果公司的變化，將會影響廠商如何有效地吸引客戶，更不用說在 Covid-19 疫情中生存。」此外，使用者個資交換也代表著免費的服務或者免費的 App 可下載使用，過於強調個資隱私，除代表著廠商的成本提高與廣告效果降低，也可能反噬使用者的免費權益。徹底改變目前網路的生態，這也並非消費者之福。

Facebook 和蘋果雙方商業利益相互衝突，突顯在數字經濟下「用戶隱私權」、「用戶財產權」、「廣告商權益」、「平台業者權益」間匹此交錯的複雜問題。

三.機械學習、大數據(Big Data)與統計學習- 從資料到資訊

3.1 大數據定義與應用

大數據是指以多元形式，匯集來自不同蒐集來源而來的龐大資料庫，在具有特定實用的目的下，過程將大量結構型或非結構性資料，加以處理、分析、判斷並輔導決策。例如大數據在不同商業行為過程中，取得資料來自社交網路、電子商務網站、瀏覽紀錄、購買紀錄、顧客來訪紀錄及既有顧客背景資料等，還有許多其他來源的多態樣資料。這些資料，並非公司顧客關係管理資料庫的常態數據組或結構性資料，因此大數據無法用以往結構式的軟體工具讀取、存儲、搜索、共享、分析和處理的巨量且多元的資料集合，業界通常用 4V (Volume、Variety、Value、Velocity) 來概括其資料特徵。大數據乙詞的盛行在於電子商務上的取得巨大成功，改變過往商業型態並將資料變成新經濟推動力量，並觸發資料經濟(Data Economic)之崛起，引發新產業革命。

3.2 廢棄資料(Data Exhaust)與個資保護

利用個人資料來創造商業利益並非是新穎技術，過去商家利用當事人所留存的位址及電話號碼作為廣告，這部分的行為可明確被現今的個資法所規範。大數據

相較過去的資料科學不同特點之一，在於利用「廢棄資料」或稱「衍生數據」(Data Exhaust)⁹⁵來預測個資當事人的行為。「廢棄資料」(Data Exhaust)，顧名思義指的是當事人在各種活動的副產品所留下的各種資料記錄或數位足跡(Digital Footprint)，數位足跡指當事人在網際網路或棟因為主動式或被動式之留存紀錄，例如當事人在網路搜尋引擎首頁輸入字詞進行搜尋時，網路搜尋引擎除記錄輸入的搜尋關鍵字外，還記錄了該當事人搜尋某個詞或相關詞彙數次，搜尋引擎也記載當事人關鍵字停留時間及使用期間、在網頁連結觸發、網頁觸發次數等，任何人在搜尋引擎上的動作，包含主動或被動、有意或無意的，都已經記錄在搜尋引擎的資料庫中；本文中數位足跡延伸到自駕車的所有、無論片斷或完整的數位人為活動紀錄。原本這些被視為片段、瑣碎、非結構式、沒什麼價值的資料，近年來在科技的進步下在經過分析、整理、資料結合、資料挖掘後並找到有經濟利用價值的資訊，或者將已經匿名化的個資轉化為可辨識個人之資料⁹⁶；「**Data Exhaust**」從英文本意有**資料耗盡或資料耗竭的意思**，在國內一般則作為名詞來翻譯，稱為「**資料廢氣**」，意即「**廢棄資料**」。廢棄資料是破碎且大都屬於非結構式資料，是利用統計、訊號處理等數學技術來產生有用價值，並非都有明確的跡象與學理可支撐。最著名的美國 Walmart 超市曾經用大數據找到了一個有趣分析：啤酒、尿布銷售與星期五，三者間的關係，並利用如此資訊來提高銷售額。此經典案例是由 Walmart 超市利用數據統計所找出，數據分析顯示在週五晚上跟尿布一起搭配購買最多的商品竟是啤酒，一開始 Walmart 並不明所以，經訪查後才瞭解因為每逢週五年輕爸爸們常會奉太太之命去買尿布，到了超市後，同時想到週末晚上要看球賽，又順便拿手啤酒回家。於是，尿布和啤酒的銷售量聯同增加。這是一個典型的案例，代表著一個片段的資料轉化成具有商業價值資訊的例子，過程並非如此直觀或者每個資料控制者都具有能力將廢棄資料轉化成有用的資訊；依我國《個資法實施細則》之規定，可能會變成在不同資料控制者中之資料，可能會是個資亦可能不是個資的情況；另一個問題在於廢棄資料如何規範是否滿足 GDPR 第四條原則「**準確無誤**，且必須酌

⁹⁵ 黃章令 (2020)，《使用衍生數據及其預測結論之法律關係研究》，台灣：新學林出版社。

⁹⁶ Ohm, P. (2009), *supra* note 24.

情保持更新」?是否滿足該原則由誰來判斷?

大數據技術所採用的資料，若是要歸屬於「可間接識別」個資，就必須要先定義資料控制者及資料蒐用者的主體、評估主觀上是否有意願及能力，及當時代的技術。此種廢棄資料的蒐集、處理及利用是否為個資法律所規範?此類資料的應用是否有侵害當事人隱私權?這些問題並非當初個資法規範時所考慮到。若大數據搭配人工智慧/機械學習技術，更是直接挑戰所謂「隱私」：引申前面所述的啤酒與尿布案例，是否可進階推論在週五購買尿布和啤酒當事人有「另一半」且是要回「家」，若再仔細分析比對啤酒數量與尿布數量與規格等多樣資料，對於現今許多都市年輕人的「感情隱私」與「家庭隱私」是否又可另被推論出來?並據以產生更多的行銷策略。現今企業主與品牌方建置屬於自家的完整會員數據庫，不再將精準定位當事人，透過建置完整的消費足跡，不追蹤特定的使用者行為，更可以利用以模型推演的方式，找出特定興趣群組的受眾定位，雖然可能比之前鎖定個人用戶還要有落差，但也能做到一定程度上的精準投放⁹⁷。這是一個革命性的資料轉化成資訊及知識的過程，在紀錄片《The Human Face of Big Data》中 MIT 麻省理工媒體實驗室⁹⁸總監伊藤穰一稱：‘在過去我們寫下所思考的事物，然後成為知識;大數據卻正好相反，你有成堆的數據，卻還不能算是知識，直到你開始審視並思考：“嘿，如果這樣看或那麼看”，才將這些資料轉變成有趣的資訊(Before what we did was we thought of things and then we wrote it down and that became knowledge; Big Data is kind of opposite you have a pile data that isn’t knowledge really, until you start looking at it and noticing wait maybe if you shifted this way, and you shift it this way this turns into this interesting piece of information.)’。如此資料轉化成資訊及知識的過程，在個人資料認定與個資法法遵上會產生問題，因為這些資料一開始蒐集時並無法認定為個資，且即使轉化成資訊階段，亦難以判斷，自然無個資法適用問題。

⁹⁷ Amy (2021/03/22), <【硬塞評論】蘋果 iOS 14 隱私政策更新：為何臉書從一開始「反對到底」，轉變為「樂觀其成」呢?>，《INSIDE》，載於：<https://www.inside.com.tw/article/22927-ios14-privacy-apple-facebook> (最後瀏覽日：2021/7/18)。

⁹⁸ M.I.T. Media Lab

如下圖 22 所示，大數據，包含結構型與非結構型資料，經過多道處理程序，包含任務/目標理解、資料理解、資料整理、建立模型、成果評量與回饋到最後之應用，足見大數據除了需要眾多數據外，尚須包含資料科學家及領域專家等基本門檻，而每家所產生出的模型與結果亦可能不同。大數據發展並非一蹴可幾，而是許多跨領域如統計科學家、資通訊技術、軟體工程及商管人員一統努力的成果，具有相當高的技術水準及複雜度。

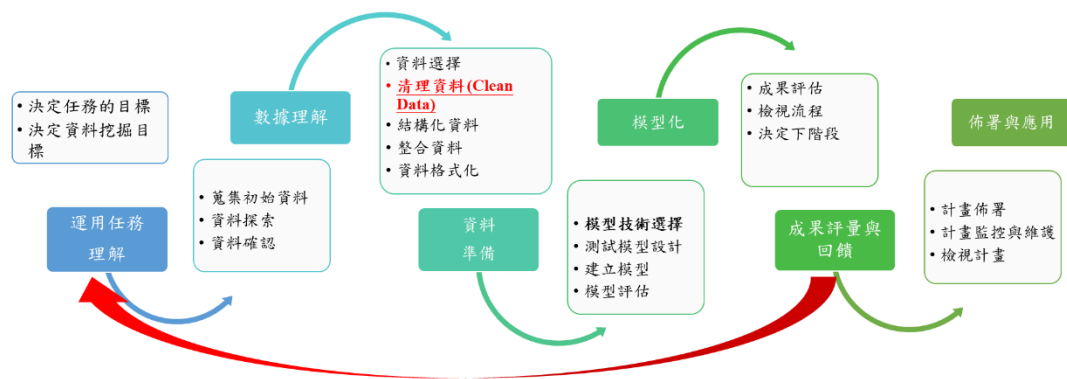


圖 22. 資料處理流程。不同原始資料、不同模型與不同任務目標都直接影響結果。資料來源：本文整理

這些數據是統計後數據，對應到個人只是機率，是否符合個資法的間接定義：「間接方式識別，指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該『特定』之個人」？在《使用衍生數據及其預測結論之法律關係研究》乙書中認為⁹⁹：“……「廢棄資料/衍生數據」本身並不是隱私，但其預測結論屬於隱私的觀點。”但這樣的個人化行銷，或者是特定群組行銷是否已經可能影響個人隱私權，侵犯到「To be let alone」的權利？此外，階段性的認定資料是否為個資，亦可能衍生出我國民法第 185 條之共同侵權的疑慮？

3.3 人工智慧結合大數據對個資法的挑戰

⁹⁹ 黃章令 (2020)，前揭註 95，封面頁。

統計學(Statistics)結合人工智慧/機械學習已經新的「統計學習」(Statistical Learning)乙詞，三者間關係如圖 23。「統計學習」不同於傳統統計在於可處理如圖 24 多變量且不同型態的資料，包括完整及零散、結構及非結構性的資料，不但具有推論(因果推理)，並可有預測的能力¹⁰⁰。結合前述廢棄資料的論述，大數據及人工智慧/機械學習使得零碎、片面的資料變成有用的資訊，資料控制者並透過更多資料結合或者持續追蹤修正，可一次次的更精準針對當事人的個人檔案剖析。

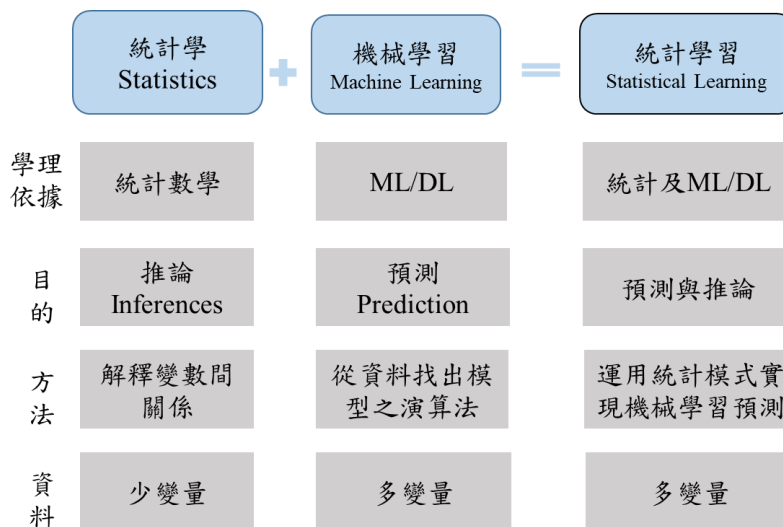


圖 23. 統計與人工智慧的結合，成為統計學習，能處理更多變量且達成更多目的。資料來源：本文整理

¹⁰⁰ 科技報橘 (2019/05/02)，《機器學習跟統計學差在哪？哈佛博士：機器學習重視預測結果，統計學在乎因果推理》，載於：<https://buzzorange.com/techorange/2019/05/02/difference-between-statistics-and-machine-learning/> (最後瀏覽日：2021/9/13)。

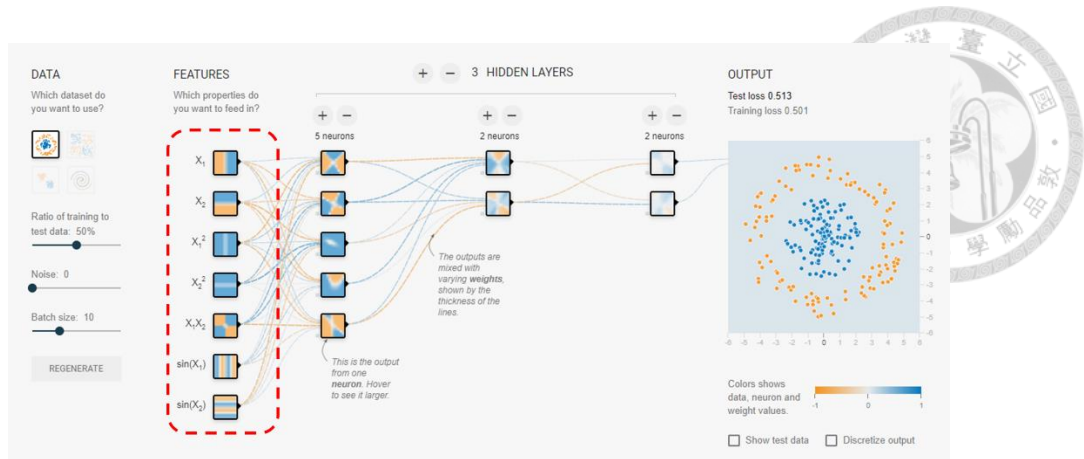


圖 24. 深度學習(DL)可輸入多變量/不同特徵之資料。資料來源：Playground.Tensorflow¹⁰¹;
本文整理

從圖 25 可初步瞭解對於機械學/深度學習(ML/DL)來說，工程人員不需要對於待分類的原理做清楚的理解，只要將資料輸入，並做基本的特徵設定，調整隱藏層及啟動函數等，從而可從大量的數據中得到分類的規則。

再舉 ML/DL 商業應用，為找出一個顧客的信用預測模型(Credit Predit Model)，左邊可輸入如年紀、性別、地區、消費紀錄等已有的可靠數據，大量數據經過類神經網路的訓練與比對已知結果後，就可得到一個訓練模型。

¹⁰¹ TensorFlow 網站，<https://playground.tensorflow.org/>

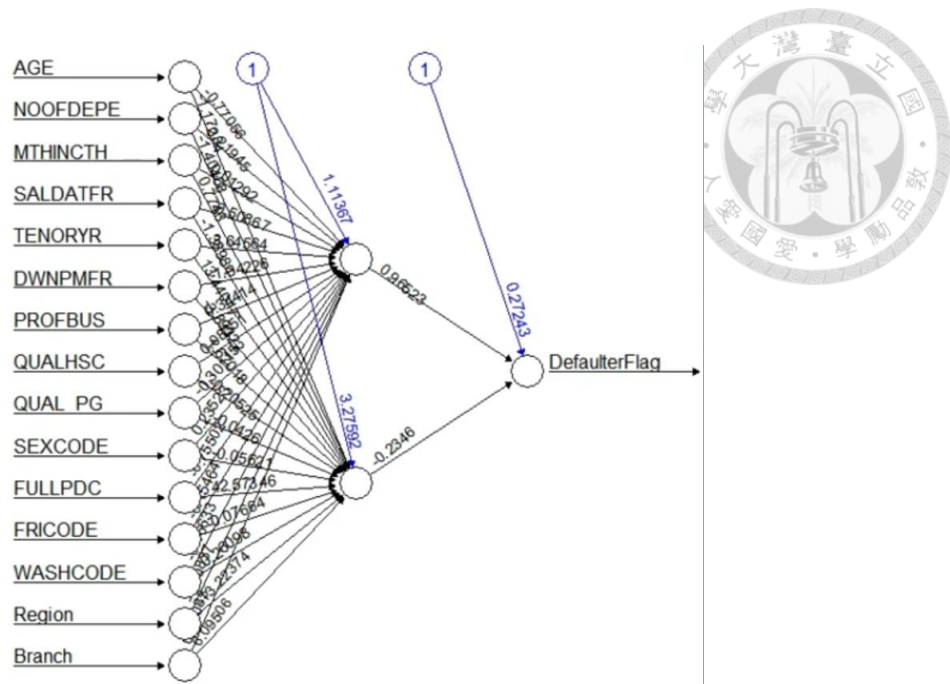
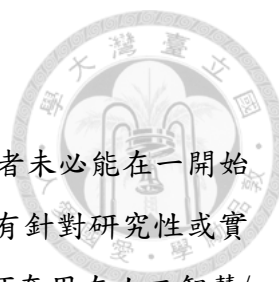


圖 25. ML/DL 在商業上應用。資料來源：Carlos Martinez;本文整理¹⁰²

- 難以界定是否個資?特別是「廢棄資料」

「廢棄資料」，望文生義是一般普羅大眾或者多數人認為並沒有價值的資料，然而近年來因為電子商務公司在累積許多資料且成功使用資料挖掘(Data Mining)技術使得其價值漸漸被人看見。爾後崛起的大數據及資料經濟(Data Economic)即是立基於此，並在人工智慧/機械學習之推波助瀾下更顯得廢棄資料之重要。於是乎，除了明文例示與傳統認知上的可間接識別個資外，「廢棄資料」是否屬個資也是一個重要的議題，包含：1.如何認定為個資?2.如何保護當事人的個資權益?3.如何保護資料控制者的財產權?4.當事人及資料控制者兩造之利益平衡?《個資法》的制定是在平衡資料經濟發展下個人隱私保護與促進個資運用兩者，而「廢棄資料」是否屬個資這議題，因為在自駕車擁有更多資料、資料共多元、運算更快、資料間融合與串接更容易，並且首要考慮安全等複雜特性使得此問題更顯得棘手。

¹⁰² Carlos Martínez (2021/05/19). Credit Scoring Model with NeuralNet in Rstudio. <https://www.youtube.com/watch?v=BTy4nZswvBo>



- 難以限定蒐集範圍?

因為大數據是透過數據分析來結果來推論，資料控制者未必能在一開始就知道資料的運用目的並限定蒐集範圍。各國個資法規皆有針對研究性或實驗性的資料蒐集行為給予特殊規定，然而這立法精神是否可套用在人工智慧/機械學習及大數據等新興技術上?

如前所述人工智慧/機械學習之所以被應用在自駕車上，在於真實環境的多變與不確定，同樣的“STOP”告示牌因為自然環境而有所不同，人工智慧/機械學習優於規則式演算法而被大量應用於自駕車，正式因為人類正式透過經驗(大量數據)來學習及找到規則，而人工智慧/機械學習也正是如此。如何在整個截取圖形中排除特定個認資料而不採用，或者判定與結果的關聯性，這些議題在人工智慧/機械學習領域至今都是研議的課題，更何況自駕車牽涉到**生命法益**，有**直接、立即且必要的理由**去蒐用各種包含影像資訊。

- 難以透明化

如前就自駕車的社會公益性質討論而言，自駕車除了生命法益外還有其他的社會價值。資料、個資、運用到目的中間的過程並非有統一標準，難以透明清晰。可從大數據及人工智慧/機械學習角度來觀之。

因為大數據的運用在初始階段未必能夠知道輸入資料其效益及其意義，需要資料科學家及領域專家(Domain expert)共同分析，過程複雜且須反覆測試，對於個資的運用過程未必能在第一時間清楚對外傳達。

人工智慧/機械學習的黑盒子運作，一直是科技法律研究的課題，並非應用在自駕車上的獨特課題，而今大數據與人工智慧/機械學習的結合更增添其解釋的困難。

- 運用疑似個資只是過程，難以界定其運用目的

如前所提，資料與個資間關係並非直觀，個資自身的定義本來有其灰色

地帶，如此之下，增添取捨資料之困難。同前面所提的蒐集範圍，人工智慧/機械學習應用如何在整個截取圖形中排除特定個認資料而不採用，或者判定與結果的關聯性，這些議題在人工智慧/機械學習領域至今都是研議的課題，更何況自駕車牽涉到生命法益，有直接、立即且必要的理由去蒐用各種資訊。

- 更難以界定可間接識別資料

大數據具有數據巨大及重視資料間串接，前者已經打破過去如街頭攝影機只能儲存 3 月的限制，後者因為不斷的資料串連時，即使是片段的資料可能被拼湊成個人資料。資料可能被辨識成個人資料的可能性大增。

3.4 隱私已死?

從資料可識別性來談，隱私被侵犯幾乎是無法避免，主要是每個人都會留下生活的足跡，這些足跡又因為被數位化且串聯，如紀錄片《The Human Face of Big Data》提出大數據是革命性的改變，片中指出資料量在 2020 年就會高達 40ZB 位元，是全地球砂粒總數 75 倍。就前面的廣義隱私定義，在如此多資料的個人檔案剖析下，確實隱私很難不被侵犯到。隱私已死¹⁰³?這已經是在公共空間眾多討論的議題，2013 年論者認為大數據即宣告隱私的終結(Big Data spells end of Privacy)¹⁰⁴，更遑論現今更多新科技的加入，而自駕車更是集先進技術於一身，自然對於隱私的衝擊更是遠非過往時代可想見。現代人一方面由於現代人樂於社交媒體上分享自己的資訊，一方面也是技術發展對於當事人的瑣碎數位足跡(digital footprint)都能勾勒出完整的標示出特定群組或個體特性與行為習慣。相對宣稱隱私已死的警示或悲觀者，另一派樂觀者稱現在人本來就是透明的，個人資料已經是遍布網路世界，且過往的個資揭露其實並沒有真正造成太多的衝擊。

¹⁰³ 愛範兒 (2014/7/22)，《隱私已死？還是我們誤解了隱私的涵義？》，科技新報，載於：[https://technews.tw/2014/07/22/privacy-is-dead-yet/#_ =](https://technews.tw/2014/07/22/privacy-is-dead-yet/#_=) (最後瀏覽日：2021/8/18)。


¹⁰⁴ Neil M. Richards and Jonathan H. King (2013). Three paradoxes of big data. *Stan. L. Rev. Online*, 66, 41. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2325537

四. 監控資本主義

承前所謂資料為 21 世紀石油之說，哈佛商學院榮譽教授肖莎娜·祖博夫 (Shoshana Zuboff) 於 2019 年所著之《監控資本主義時代》(The Age of Surveillance Capitalism) 出版後，一般大眾才得以知曉資料經濟之商業模式早就統治了我們的世界，此書也名列美國前總統歐巴馬在同年最愛的書籍之一。《監控資本主義時代》書中以 GAFAG(Google、Apple、Facebook、Amazon)¹⁰⁵ 等幾個掌握資料的科技巨擘，利用個人之個人資料與「廢棄資料」，形塑當事人的行為模式，透過個人檔案剖析 (profiling)，進而侵犯隱私。資料資本主義利用前述之「個人行為模式資料」¹⁰⁶，取代 20 世紀的石油、勞力、土地與資本，持續強化發展各種生產手段；而監控資本家與其他市場參與者，則以資料為新石油結合大數據及 AI 人工智慧技術，驅動資料經濟時代，讓電腦機器控制的力量愈來愈穩固、強大，進而無形中控制整個資本市場，貫穿《監控資本主義時代》的核心問題是知曉、掌握與決定資料與隱私的主體。從該書可以從中思考監控資本主義不同以往的權力形態和帶給民主體制的危機，如美國最高法院 Louis Brandeis 法官明言「隱私」為“文明人最全面且最有價值的權利 (the most comprehensive of rights and the right most valued by civilized men)”、“對民主政府至關重要 (essential to democratic government)”。同樣的《監控資本主義時代》作者稱監控資本主義的權力型態為「機器控制主義」，破壞支撐現代民主的自律、自由意志等原則，並且這樣一種權力型態下當事人與資本家處在一個不對等的位階上，兩者對於資料流通關係建立在不公平交易、過程不透明與資訊不對等的基礎上。資料掌握的不對等問題，落實在智慧自駕車上，其風險也被《聯網車輛與移動相關產品涉及個人資料處理指南》所指出，詳細內容將本文後面章節探討。相同《監控資本主義時代》乙書的警示亦可見於紀錄片《個資風暴：劍橋分析事件》(The Great Hack)及《智慧社會：進退兩難》(The Social Dilemma)。有關個資保護與

¹⁰⁵ 除了 GAFAG，另有加上 BATH(百度、阿裡巴巴、騰訊、華為)共八家的另種說法。

¹⁰⁶ 「個人行為模式資料」是否等同於個人資料，是本文探討重點。



隱私權之關係，將於本文後面個資與隱私章節中論述，透過此些論述，除了能瞭解資料的重要性，也對於個資利用之積極光明面與消極人權之保護有更不同角度之思考¹⁰⁷。監控資本之機會與風險不僅於此，在大數據及統計學習的發展下，獲得更多消費者的資料並鏈結先進 ABCD (A: AI; B: Block Chain; C: Cloud; D: Big Data) 技術等，強化經濟活動與資本利益，過去已在金融科技(FinTech)領域獲得具體且全面性成功。正面的用途能夠協助提升產品服務及創造更好的商業體系；負面使用的部分就可能侵犯個人隱私，並由企業家掌控整個消費者行為，並反而導致企業壟斷而做出如「大數據殺熟」等傷害消費者權益之行為。迄今如此的爭議仍然持續中。此外，《監控資本主義時代》書中所描繪的社會背景，當時候人工智慧/機械學習尚未普遍應用於各行各业，人工智慧/機械學習配合大數據的自動化資料蒐用及自動化決策，更是使得過程難以被普羅大眾所掌控，不透明與難以歸責，使得現今的個資與隱私保護更顯得困難。

相較過去金融科技的應用與個資保護法規，兩者是在個人隱私與經濟發展間取得平衡；來到自駕車的個資探討，如圖 26 因為自駕車運用上的生命法益之優先其他公益性質而有所不同。但無論資料在何種新的應用環境，從個人電腦、網路、手機、無所不在的監視器、通滿各種感測器與資料處理的智慧城市、到隨時穿梭任何人身旁的自駕車高科技感測器。回顧《監控資本主義時代》乙書針對民眾對於「監控資本主義」看法不論可能是無知還是無感？亦或者是無能為力？在自駕車應用場域，智慧自駕車巨量的個資，透過先進人工智慧技術與資料經濟飛快的持續發展下去，將影響著普羅大眾的生活每個片刻。

¹⁰⁷ 邱文聰 (2009)，〈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》，第 168 期，頁 172-189。

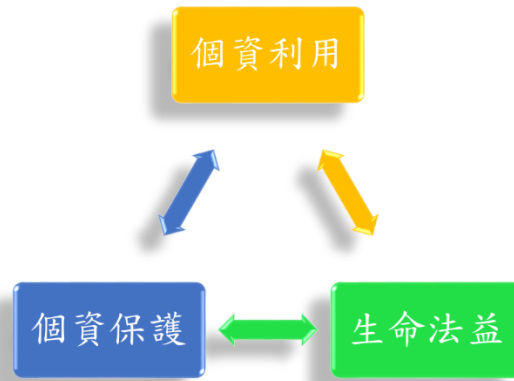


圖 26. 資料與個資管理，圍繞在個資保護-資料運用及生命法益保護三者。資料來源：本文整理

第四項 個資與隱私

個人資料保護(Personal Data Protection)與隱私權(Privacy Right)是目前常見主張的權利，在資料驅動(Data Driven)的現代經濟社會，是現在各國政府、企業與民眾相當重視的權利，兩者間關係如美國隱私權法專家 Daniel J. Solove 所言，個人資料本質上是一種資訊隱私，法律上作為一種隱私權加以保護，可以界定其權利範圍¹⁰⁸。在本段將說明兩者的定義、關聯與差異。

一.個人資料

所謂「個資」，依現行個資法第二條第一項第一款：「個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。」國際間個資之法規與準則的個人資料的定義比較如下表 7：

¹⁰⁸ Solove, Daniel J., and Paul M. Schwartz (2009). *Information Privacy Law* (3th ed.), New York: Aspen Publishers.

表 7. 不同國家地區對個人資料/資訊的規定。資料來源：各國法規資料庫;本文整理

國家地區	法律規範	對個人資料/資訊的規定
OECD	隱私保護與個人資料跨境流動準則 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980 年)	個人資料是指任何可以識別或可能識別當事人的資訊。 "personal data" means any information relating to an identified or identifiable individual (data subject)
歐盟	一般資料保護規範 GDPR (2016 年 4 月生效)	得以直接或間接方式識別當事人之任何資訊。Personal data are any information which are related to an identified or identifiable natural person.
美國加州	消費者隱私法 (The California Consumer Privacy Act, CCPA) (2020 年生效)	個人資訊是任何可以識別、關聯或合理連結當事人或其家庭的資訊。Personal information is information that identifies, relates to, or could reasonably be linked with you or your household
新加坡	個人數據保護法(Personal Data Protection Act, PDPA)	個人資料是指可以從該資料或從該資料和組織有權或可能有權存取的其他資訊中辨別出的有關個人的資料。 Personal data refers to data about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access.

國家地區	法律規範	對個人資料/資訊的規定
中國	中國民法典	個人資料是以電子或者其他方式記錄的能夠單獨或者與其他資訊結合識別特定自然人的各種資訊，包括自然人的姓名、出生日期、身分證件號碼、生物識別資訊、住址、電話號碼、電子郵箱、健康資訊、行蹤資訊等。個人資料中的私密資訊，適用有關隱私權的規定；沒有規定的，適用有關個人信息保護的規定。
	中華人民共和國汽車數據安全管理若干規定（試行）	個人資料，是指以電子或者其他方式記錄的與已識別或者可識別的車主、駕駛人、乘車人、車外人員等有關的各種資訊，不包括匿名化處理後的信息。 敏感個人資料，是指一旦洩露或者非法使用，可能導致車主、駕駛人、乘車人、車外人員等受到歧視或者人身、財產安全受到嚴重危害的個人資料，包括車輛行蹤軌跡、音頻、視頻、圖像和生物識別特徵等資訊。

何謂「個人」？依照 105 年 3 月頒布施行「個人資料保護法施行細則」（以下簡稱《個資法施行細則》）第 23 條：「...指現生存之自然人」；至於何謂「間接」方式，而依照同法第 3 條：「...指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。」在現行《個資法》、第 51 條，亦有兩種個資排除個資法適用情形：1. 是自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料；2. 係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人資料結合之影音資料。同條第二項將境外行為亦納入：「公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法。」

上述對於個資及個資法初步說明主要以為我國 105(西元 2016)年公布現行《個資法》定義。然而，因為技術快速演進，各國對於隱私與個資法規範已有不同或者更細節的規範，我國現行《個資法》是否能與時俱進，適用本文所探討的自駕車應

用?留待第三章後討論。

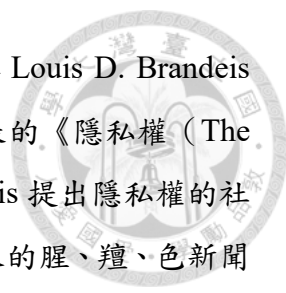


二. 隱私(Privacy)與隱私權(Privacy Right)

綜觀全球無論政府政策、法規、企業政策與相關論文研究，常將個資保護與隱私保護緊密相連，且基於隱私權被許多國家視為基本之人權，是故欲探求個資保護對應人格權保障之真意，亦必須瞭解「隱私」之意涵及「隱私權」之範疇。「隱私」英文為「Privacy」，參諸劍橋線上英文解釋為“某人維護其個人事務及關係秘密(someone's right to keep their personal matters and relationships secret)”或為“一種獨自的狀態(the state of being alone)”；牛津字典解釋為“一種不被他人監視或打擾狀態(A state in which one is not observed or disturbed by other people)”，不論中文「秘密」、「不願暴露之私事」或英文有關隱私(privacy)之解釋都有私密、隱密之意涵，然而如此解釋是否過於直觀?與現今資料經濟衝擊下的隱私保護有如何之連結?隱私、隱私保護與隱私權三者之關係如何界定?

隱私權概念之萌芽，可追溯自美國在 18 世紀末期照相機興起之年代，並歷經二戰政府監控與人權迫害，不斷演進、成熟，迨至近代新興科技崛起與資料經濟的轉變，聯合國所頒布《世界人權宣言》第 12 條明白揭禁：「任何人的私生活、家庭、住宅或通訊不得任意干涉，他的榮譽和名譽不得加以攻擊。人人有權享受法律保護，以免受這種干涉或攻擊 (“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks”）」¹⁰⁹，隱私(Privacy)已是普世的基本人權之一。我國憲法雖未將隱私權(Privacy Right)明文例示保障，但基於人性尊嚴的理念，維護個人主體性及人格發展的完整，保障個人生活私密領域免於他人侵擾及個人資料的自主控制，司法院釋字第 603、689 多號解釋等及憲法法庭 111 年憲判字第 13 號判決，均肯認其屬應受憲法第 22 條所保障的基本人權。

¹⁰⁹ United Nations. *Universal Declaration of Human Rights, Art. 12*. <https://www.un.org/en/about-us/universal-declaration-of-human-rights>



「隱私權(Privacy Right)」最早乃源於 Samuel D. Warren 與 Louis D. Brandeis 於 1890 年 12 月在哈佛法學評論 (Harvard Law Review) 所發表的《隱私權 (The Right to Privacy)》¹¹⁰ 乙文。Samuel D. Warren 與 Louis D. Brandeis 提出隱私權的社會背景是當時照相技術的技術革新，照相技術的普及化與隨之來的腥、羶、色新聞報紙的興起，美國許多政商名流的自身及家人之私人領域及家庭生活遭到記者媒體的嚴重侵擾，於是 Warren 與 Brandeis 兩人共同發表了這篇文章《隱私權》，旨在探討美國法架構之下是否足以提供一個可以適當地被援引的原則，以保護個人私領域不被干擾的權利。文中兩位學者主張隱私權屬基本權利之一種，為不可侵犯之人格權，並以「獨處不受他人干擾」(to be let alone) 表彰其內涵，成為美國隱私權發展的基礎。但 Warren 與 Brandeis 也特別強調，隱私權並非絕對的權利，是有其界限存在，其主張有下列情況時，隱私權是不受保障：(一)、涉及公共或一般利益時 (The right to privacy does not prohibit any publication of matter which is of public or general interest)；(二)、依據法律有傳播的權利時 (The right to privacy does not prohibit the communication of any matter, though in its nature private, when the publication is made under circumstances which would render it a privileged communication according to the law of slander and libel)；三、口頭之散布而未造成「特別損害」(special damage) 時 (The law would probably not grant any redress for the invasion of privacy by oral publication in the absence of special damage)；四、由本人散布或經其同意者(The right to privacy ceases upon the publication of the facts by the individual, or with his consent)。除了「獨處不受他人干擾」(to be let alone)之概念，2002 年美國學者 Daniel J. Solove 在著作《概念化隱私(Conceptualizing Privacy)》¹¹¹ 整理共六種主要學者提出之學說，包含：1. 獨處不受他人干擾之權(the right to be let alone); 2. 對個人擷取的限制(limited acces to the self); 3. 秘密(secrecy); 4. 個人資訊的控制(control over personal information); 5. 人格(personalhood); 6. 親密關係(Intimacy)。

¹¹⁰ WARREN, S. (1890). The Right to Privacy. *Harvard Law Review*, 14(5), 193-220.

¹¹¹ Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review*, 90(4), 1087-1155. <https://doi.org/10.2307/3481326>

1960年，William L. Prosser教授在加州法學評論(California Law Review)上發表了《隱私(Privacy)》乙文¹¹²，該文指出以往的研究與案例皆著重於探討隱私權的存在與否，然卻未就隱私權的具體內容提出說明。據William L. Prosser教授的整理分析，法律上的隱私權侵害應包含4種侵權行為，它涉及了4種不同的法益類型，這4種類型的侵害包括了：(1)對某人之隱居生活或私人事務所為之侵擾(Intrusion upon a person's seclusion or solitude, or into his private affairs.)；(2)公開揭發使人覺得難堪之私人資料(Public disclosure of embarrassing private facts about an individual.)；(3)使某人處於人為誤解情況之侵害(Publicity placing one in a false light in the public eye.)；(4)基於他人之利益，擅用某人之肖像(Appropriation of one's likeness for the advantage of another)。至此後，Prosser對於隱私權分類為四種侵權行為，奠立了隱私權在民事法領域穩固的基礎。至於資訊隱私權的發展始則於1977年聯邦最高法院的Whalen v. Roe案，該案中美國聯邦最高法院認為避免資訊洩漏本來就是公共蒐集及使用資訊所衍生之附隨義務。

2008年美國學者Daniel J. Solove出版的有關隱私的書籍《瞭解隱私(Understanding Privacy)》¹¹³，《瞭解隱私》書中提供了隱私概念的現代歷史，特別是哲學家和法律理論家所討論的範疇，引述美國最高法院Louis Brandeis法官名言：「隱私」為“文明人最全面且最有價值的權利 (the most comprehensive of rights and the right most valued by civilized men)”、“對民主政府至關重要(essential to democratic government)”、“我們創造和維持不同的能力與不同人的各種社會關係的關鍵(critical to our ability to create and maintain different sorts of social relationships with different people)”、“允許並保護自主生活的必要(permitting and protecting an autonomous life)”、“對於情緒化的和心理安寧很重要(important to motional and psychological tranquility)”、“是人性的一節(an integral part of our humanity)”、是“自由的心臟(heart of our liberty)”，及“自由的開端(the beginning of all freedom)”。此

¹¹² William L. Prosser (1960). Privacy. *California Law Review*, 383-423, Vol. 48, No. 3, Aug. , 383-423.

¹¹³ Daniel Solove (2008/05). *Understanding Privacy*. Harvard University Press. ISBN: 978-0674035072.

著作為許多人的隱私概念提供了一個具體且明確框架，以及作者自己關於隱私涵蓋的內容的理論。相較先前文章對隱私的描述還是概念式論述，Daniel J. Solove 更廣泛地歸納各種隱私問題，並進而提出了十六種隱私問題。在此之前學者 Prosser 認為「隱私權」只不過是共通使用單一名稱來保障四種不同的利益的泛稱；同樣的，學者 Solove 也將隱私視為一個涵蓋各種問題的概括式的總稱術語(umbrella term)，並且認為各問題所要保障的利益各不相同，“具體可行的隱私理論須考量不同文化的看法，且必須認知到隱私會隨著歷史演化 (a workable theory of privacy should account for the differing attitudes toward privacy across many cultures. It should recognize that notions about what information or matters are private have evolved throughout history.)”，因此“焦點應該在隱私問題上，當我們提到所謂保護隱私，應該是指防止某些活動受到干擾(.....I argue that the focal point should be on privacy problems. When we protect privacy, we protect against disruptions to certain activities.)”¹¹⁴。

這些隱私態樣的瞭解、隱私權與個資保護間關聯探討，有助於本文後面所探討「何謂個資?」、「個資保護之精神?」及「資料-個資如何轉換?」等議題，特別是在智慧自駕車的個資保護與資料利用研究。故在此本文參考《瞭解隱私》及論者研究¹¹⁵，將學者 Solove 之論述說明如下：首先，Solove 依照侵害方式是否與個人資料有關，以及資料的「蒐集」、「處理」和「利用」流程，將隱私權區分為四種基本的隱私侵害態樣，分別是：一、「資訊蒐集」(information collection)。二、「資訊處理」(information processing)。三、「資訊傳遞」(Information dissemination)。四、「侵犯」(invasion)。依循著此四種基本分類，學者 Solove 再對每個基本分類做了進一步的細分，成為合計十六種隱私侵害態樣的架構，如下表 8。從這些侵害隱私的態樣，結合前述各種先進技術之資料蒐集、結合與利用，可想像到的是為何有人會提出「隱私已死」的隱憂。

¹¹⁴ *Id.* at 9.

¹¹⁵ 李明勳 (2013)，《合理隱私期待之研究-以定位科技為例》，頁 18-22，國立政治大學法律研究所碩士論文。

表 8. 四種隱私基本侵害態樣及展開的 16 種隱私問題。資料來源：《Understanding Privacy》，本文翻譯/整理

四種隱私基本侵害態樣	侵害態樣細項
資訊蒐集 (information collection)	<ul style="list-style-type: none"> ● 監控(Surveillance) ● 審問(Interrogation)
資訊處理 (information processing)	<ul style="list-style-type: none"> ● 匯集(Aggregation) ● 識別(Identification) ● 不安全(Insecurity) ● 目的外使用(Secondary use) ● 排除(Exclusion)
資料傳遞(information dissemination)	<ul style="list-style-type: none"> ● 違背信賴(Breach of confidentiality) ● 揭露(Disclosure) ● 暴露(Exposure) ● 增加取得可能(Increased accessibility) ● 勒索(Blackmail) ● 冒名(Appropriation) ● 扭曲(Distortion)
侵犯 (invasion)	<ul style="list-style-type: none"> ● 侵擾(Intrusion) ● 決定性的干預(Decisional interference)

四種基本態樣中的「資訊處理」¹¹⁶，是對於蒐集而來的資訊進行使用、儲存和操控。Solove 學者認為，在資訊處理過程中，至少有五種隱私侵害的型態，分別包括「匯集」(aggregation)、「識別」(identification)、「不安全」(insecurity)、「目的外使用」(secondary use) 以及「排除」(exclusion)。所謂「匯集」是將片段或零散的資料相結合，以獲得更多的資訊，而大數據技術的崛起，正是整合這些片段資料，進而辨識特定當事人；「識別」則是將資訊連結到特定的個人。「匯集」及「識別」與現在個資法所討論的「間接可識別」有很大關係，片段資料透過資料的結合容易識別出特定的當事人，而自駕車巨大的資料及先進的科技，使得前述兩者更可輕易完成，可能造成對個人隱私的侵害。而「不安全」是源自於資料的處理和保護的方式不當，導致資料洩漏、被竊取、修改等問題，「不安全」此議題與自駕車的聯網功能之所導致資料透過傳輸洩漏或者資安危害有相同的擔憂。「目的外使用」則是在未經過當事人(資料主體)的同意下，將因某種目的而蒐集來的資訊作另外不

¹¹⁶ 李明勳 (2013)，同註 115，頁 20。

同目的使用，「目的外使用」與本文所探討的人工智慧驅動自駕車在資料利用目的不明確，容易有目的外使用有著相當緊密的關聯。至於「排除」，是指未能使當事人知悉他人所持有關於自身的資訊，或者不讓當事人參與資料的處理與使用。「排除」與本文探討的「資料偏見」及「大數據殺熟」議題有緊密關聯。

在「資料傳遞」流程，Solove 學者認為存有下列隱私問題：「違背信賴」(breach of confidentiality)、「揭露」(disclosure)、「暴露」(exposure)、「增加取得可能性」(increased accessibility)、「勒索」(blackmail)、「冒名」(appropriation)、「扭曲」(distortion)。其中「違背信賴」是違背了維持個人資訊秘密的承諾。而「揭露」是指披露當事人真實而不願公開的資訊。「暴露」則是指洩露了當事人因暴露在外會感到尷尬或羞恥的身體特徵及活動。而「增加取得可能性」是指將已經公開的資訊變得更容易讓人取得，例如資料上傳到網路等。「勒索」是掌握資訊而形成一種優勢地位之人，利用該等優勢地位來威脅資訊主體以獲得金錢等利益。而「冒名」則是為了個人目的或利益而冒用當事人的身分。至於「扭曲」則是散布失真、不正確或容易讓人誤解的資訊¹¹⁷。智慧自駕車可蒐用車輛使用者包含駕駛及乘客之音私密資訊，並可透過長期監控或資料結合比對，若無法規之規範，對於「違背信賴」、「揭露」、「暴露」等侵犯態樣具有嚴重威脅。

最後，在對於與資料無關的「侵犯」類型中，Solove 學者總結包括「侵擾」(intrusion)和「決定性的干預」(decisional interference)這兩種隱私問題。所謂「侵擾」是指妨礙到當事人的私人活動，侵犯到 Warren 與 Brandeis 所說的“獨處而不受外界干擾的權利”。雖然「侵擾」可透過實體物理侵入的方式，然非不可透過資訊之監視、詢問等非侵入的方式來實施；「侵擾」時常伴隨著蒐集資訊目的，但也可以在伴隨其他態樣侵犯下對個人造成傷害。至於「決定的干預」是指政府干預、介入人民對於自己事務的決定¹¹⁸。

針對「資訊的蒐集」，可區分為兩種資訊蒐集的型態，分別為「監控」

¹¹⁷ 李明勳 (2013)，同註 116，頁 20。

¹¹⁸ 李明勳 (2013)，同註 116，頁 20。

(surveillance) 與「審問」(interrogation)，都會產生隱私侵害問題。所謂「監控」，是對於當事人的言行舉止進行注視、觀察、紀錄等。基於社會通念，任何當事人被持續監看與注視，必定會產生焦慮和不舒服的感覺(釋字第 689 號解釋參照)。長此以往的持續監看與注視，此種不舒服或不安感覺最後可能逐漸改變該當事人的言行舉止，影響當事人人格之正常發展。而所謂「審問」則是對個人施壓來揭露資訊。當過度或壓迫性地對當事人探尋一些問題，而這將迫使當事人去思索該如何回應問題與否，進而造成個人資料的洩露，甚至對於個人的言論、信仰等自由權的行使，產生莫大的傷害¹¹⁹。「監控」此點是自駕車對車位使用者及車聯網隊車外用路人可能造成的疑慮，本文在討論中也會提及此點是現今《個資法》所忽略的，透過持續的監控，片段之資料不需要透過不同資料間結合，亦可能轉化成可識別特定人的個人資料，並對當事人之隱私造成傷害。

綜整前述學者 Solove 對於四種隱私基本侵害態樣所推論出的「隱私權」。全球目前已有美、日、加及歐盟多國將隱私權列為憲法保障。基於我國《憲法》並沒有對於「隱私權」明文例示，其精神與涵攝可從司法院大法官所做的解釋探詢。大法官遵循國際對於隱私保護的主流趨勢，肯認隱私權為憲法保障的基本權利，並且發展出隱私權的類型。在司法院大法官釋字第 585 號解釋中，首次提到隱私權受《憲法》第 22 條保障：「……其中隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活秘密空間免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障（大法官釋字第 509 號、第 535 號解釋參照）。」

從大法官 603 號解釋文中，可以歸納以下四個隱私權¹²⁰類型：

¹¹⁹ 李明勳 (2013)，同註 116，頁 19。

¹²⁰ 此部分與學者 James Michael 看法接近，James Michael 認為隱私可分為 1.Information Privacy, which involves the establishment of rules governing the collection and handling of personal data such as credit information and medical records; 2.Bodily privacy, which concerns the protection of people's physical selves against invasive procedures such as drug testing and cavity searches; 3.Privacy of communications, which covers the security and privacy of mail, telephones, email and other forms of



- 資訊隱私權：

根據司法院大法官釋字第 603 號解釋：「……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」。「資訊隱私權」也是國內學者在闡述個資保護時重要的理論基礎。

- 空間隱私權：

依司法院大法官釋字第 535 號解釋：「……臨檢實施之手段：檢查、路檢、取締或盤查等不問其名稱為何，均屬對人或物之查驗、干預，影響人民行動自由、財產權及隱私權等甚鉅，應恪遵法治國家員警執勤之原則。……除法律另有規定外，員警人員執行場所之臨檢勤務，應限於已發生危害或依客觀、合理判斷易生危害之處所、交通工具或公共場所為之，其中處所為私人居住之空間者，並應受住宅相同之保障；對人實施之臨檢則須以有相當理由足認其行為已構成或即將發生危害者為限，且均應遵守比例原則，不得逾越必要程度。」

空間隱私權指的是個人對於自己所屬空間的隱私權，如私人住宅就屬於空間隱私權的保護範圍。然而汽車內的空間，普認為具有高度個人操控的私人空間，是否可視為等同私人住宅具有較高的隱私保護之期待？迄今尚未有明確的見解。

- 秘密通訊隱私權

根據司法院大法官釋字第 631 號解釋：「憲法第十二條規定：『人民有秘密通訊之自由。』旨在確保人民就通訊之有無、對象、時間、方式及內容等事項，有不受國家及他人任意侵擾之權利。此項秘密通訊自由乃憲法保障隱私權之具體態樣

communication; and 4. Territorial privacy, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space.。請參考 James Michael, Privacy and Human Rights: An International and Comparative Study, With Special Reference to Developments in Information Technology First Edition, Faculty of Laws, University College London, 1994. ISBN: 978-1855213814

之一。」


秘密通訊隱私權是指個人在通訊內容、對象、時間、方式有其自由與隱私的權利。自駕車車內包含駕駛人及乘車，因為有私密的資訊(如車內交談、車內通話及隱私行為)及可能長時間被監控(如 GPS 移動位置及時間)，相關的資料被侵擾，亦可能侵害秘密通訊隱私權。

● 生活私密隱私權

司法院大法官釋字第 689 號解釋：「……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。」

車輛雖為透明的空間，有無法完全阻閉車外視線限制的特性，然私人汽車除了是一種交通工具，也代表一個私人空間領域，當事人可以在其中享受某種形式的決策自主權與活動自由，對於車內的空間具有一定的隱私期待。判例中關於生活私密領域的隱私權非常廣泛，如台灣臺北地方法院 95 年度訴字第 540 號刑事判決指出，某週刊拍攝某藝人與友人在別墅內與友人擁抱、親吻等行為，這些親暱動作屬於個人主觀上具有隱私的合理期待，並且是生活私領域中相當私密的部分，屬於生活私密隱私權的範圍，而受到保障。

如果是私人之間的隱私權侵害，可以透過民法所謂「人格權」的保障，也就是對具人格法益性質的非財產上損害賠償。依民法第 18 條規定：「人格權受侵害時，得請求法院除去其侵害；有受侵害之虞時，得請求防止之。前項情形，以法律有特別規定者為限，得請求損害賠償或慰撫金。」又民法第 195 條第 1 項前段規定：「不法侵害他人之身體、健康、名譽、自由、信用、隱私、貞操，或不法侵害其他人格法益而情節重大者，被害人雖非財產上之損害，亦得請求賠償相當之金額。」



《中國民法典》第一百一十條：「自然人享有生命權、身體權、健康權、姓名權、肖像權、名譽權、榮譽權、隱私權、婚姻自主權等權利」；同法第一千零三十二條規定：「自然人享有隱私權。任何組織或者個人不得以刺探、侵擾、洩露、公開等方式侵害他人的隱私權」。隱私權是自然人的私人生活安寧和不願為他人知曉的私密空間、私密活動、私密信息。可看中國是以比較狹義來定義「隱私」，《中國民法典》第一千零三十三條有針對侵犯隱私行為規範如下：「除法律另有規定或者權利人明確同意外，任何組織或者個人不得實施下列行為：（一）以電話、短信、即時通訊工具、電子郵件、傳單等方式侵擾他人的私人生活安寧；（二）進入、拍攝、窺視他人的住宅、賓館房間等私密空間；（三）拍攝、窺視、竊聽、公開他人的私密活動；（四）拍攝、窺視他人身體的私密部位；（五）處理他人的私密信息；（六）以其他方式侵害他人的隱私權。」

在我國大法官釋字第 689 號解釋，針對狗仔跟拍與個人隱私權問題，大法官做出以下見解：

（一）人身行動自由為憲法所保障之自由權

「基於人性尊嚴之理念，個人主體性及人格之自由發展，應受憲法保障（司法院釋字第 603 號解釋參照）。為維護個人主體性及人格自由發展，除憲法已保障之各項自由外，於不妨害社會秩序公共利益之前提下，人民依其意志作為或不作為之一般行為自由，亦受憲法第 22 條所保障。人民隨時任意前往他方或停留一定處所之行動自由（司法院釋字第 535 號解釋參照），自在一般行為自由保障範圍之內。惟此一行動自由之保障並非絕對，如為防止妨礙他人自由，維護社會秩序所必要，尚非不得以法律或法律明確授權之命令予以適當之限制。」大法官認為除非有妨礙他人自由，違反社會秩序等受法律限制之狀況下，憲法保障人身行動自由之自由權。

（二）新聞自由受憲法第 11 條所保障

「為確保新聞媒體能提供具新聞價值之多元資訊，促進資訊充分流通，滿足人民知的權利，形成公共意見與達成公共監督，以維持民主多元社會正常發展，新

聞自由乃不可或缺之機制，應受憲法第十一條所保障。……。惟新聞採訪自由亦非絕對，國家於不違反憲法第 23 條之範圍內，自得以法律或法律明確授權之命令予以適當之限制。」大法官在本案中，認為前述人身自由之保障同時，新聞自由也受憲法之保障。

（三）隱私權原則應不受侵擾

「蓋個人之私人生活及社會活動，隨時受他人持續注視、監看、監聽或公開揭露，其言行舉止及人際互動即難自由從事，致影響其人格之自由發展。尤以現今資訊科技高度發展及相關設備之方便取得，個人之私人活動受注視、監看、監聽或公開揭露等侵擾之可能大為增加，個人之私人活動及隱私受保護之需要，亦隨之提升。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。……」

在此可理解大法官認為不論私人或公開場合，個人有不受他人侵擾的自由；惟在公共場域，個人若主張此權利，須符合 1.其不受侵擾之期待已表現於外,2. 且該期待須依社會通念認為合理者。而這些隱私期待，是否因為滿街的自駕車與充斥的路口監視器而使得如此期待更顯得困難？使得自駕車的個資管理更形重要？

（四）新聞自由保障與其他法益間之平衡

「新聞採訪者縱為採訪新聞而為跟追，如其跟追已達緊迫程度，而可能危及被跟追人身心安全之身體權或行動自由時，即非足以合理化之正當理由，系爭規定授權員警及時介入、制止，要不能謂與憲法第十一條保障新聞採訪自由之意旨有違。新聞採訪者之跟追行為，如侵擾個人於公共場域中得合理期待其私密領域不受他人干擾之自由或個人資料自主，其行為是否受系爭規定所限制，則須衡量採訪內容是否具一定公益性與私人活動領域受干擾之程度，而為合理判斷，如依社會通念所認非屬不能容忍者，其跟追行為即非在系爭規定處罰之列。是新聞採訪者於有事實

足認特定事件之報導具一定之公益性，而屬大眾所關切並具有新聞價值者……，如須以跟追方式進行採訪，且其跟追行為依社會通念所認非屬不能容忍，該跟追行為即具正當理由而不在系爭規定處罰之列。」依此論述，可得知大法官雖肯認新聞自由之基本權利，惟應在符合重要公益且不危及當事人身體權或行動自由條件下。是故，新聞自由與個人隱私之保護之權衡，應符合比例原則。

司法院釋字第 689 號解釋引用美國法院之兩步驟式之主、客觀期待標準來評斷「隱私合理期待」(Reasonable Expectation of Privacy)，即使在公眾場合自然人也應有不受他人干擾之自由或個人資料自主：「……新聞採訪者之跟追行為，如侵擾個人於公共場域中得合理期待其私密領域不受他人干擾之自由或個人資料自主，其行為是否受系爭規定所限制，則須衡量採訪內容是否具一定公益性與私人活動領域受干擾之程度，而為合理判斷，如依社會通念所認非屬不能容忍者，其跟追行為即非在系爭規定處罰之列。是新聞採訪者於有事實足認特定事件之報導具一定之公益性，而屬大眾所關切並具有新聞價值者（例如犯罪或重大不當行為之揭發、公共衛生或設施安全之維護、政府施政之妥當性、公職人員之執行職務與適任性、政治人物言之可信任性、公眾人物影響社會風氣之言行等），如須以跟追方式進行採訪，且其跟追行為依社會通念所認非屬不能容忍，該跟追行為即具正當理由而不在系爭規定處罰之列。……」

針對個人隱私的規範，除了憲法的保障，在刑法中也有妨害秘密罪之規定，例如第 315 條之一：「有下列行為之一者，處三年以下有期徒刑、拘役或三萬元以下罰金：一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。其構成要件有二，1.無故;2.非公開。

另有一派學者¹²¹將「隱私」(privacy)與「隱私權」(the right to privacy)分開來，認為「隱私」是一種客觀社會事實，而「隱私權」是「隱私」保護的客體，是一種

¹²¹ 黃章令 (2020)，前揭註 95，頁 63。

主觀價值判斷。大多數學者沒有區分其中兩者表述，也沒有落實到具體分析比對。清楚區隔下，「隱私」是客觀存在的，而「隱私權」是經由法律所賦予的保護權利，例如身分證字號、住宅、個人基因等作為隱私範疇，不同時空皆無法改變其隱私的屬性；相對的，因為不同時間背景，例如「分享或公開」的行為對當事人是否具有「隱私權」就有直接影響¹²²。

三. 個資與隱私小結

綜上所討論，個人資料之保護關係隱私權之保護；同樣的，個人資料保護之解釋亦可適用隱私權保護的解釋。兩者意涵與彼此間差異綜整如下：

3.1 個人資料保護與隱私權保護相關兩者關係

我國個資法第 1 條規定保障個人資料的基礎來自於保障人格權，在大法官 603 釋字亦揭禁個人資料自主控制權為憲法第 22 條保障之隱私權。故個資法所保護個資之範圍與隱私權保護隱私之範圍，有重疊競合處，亦有各自不同之部分。

3.2 隱私(Privacy)隨時代與公眾認知有關，難以客觀界定其範圍

我國釋憲實務見解上，如釋字 585 號、603 號、689 號有關隱私權之闡述，較側重於個人私生活領域不受干擾及基於個人資料自主為內容，以此觀點論述隱私權之概念，相較國際論者對於隱私內涵的論述，難謂已完整闡明隱私權之概念及範疇。「隱私」雖理應為客觀存在且為普世認同對於個人私領域內的事務保障，然而隨不同時代科技快速發展，衝擊生活型態、公眾認知並導致輿論變遷，至今猶屬樣態不定、內涵未明確之狀態；相對的，「隱私權」作為隱私在法律上的具體化權利，同樣會隨不同應用場域、時空背景有所變化，亦難有全球共通、一成不變的規範。根本原因在於隱私權為個別當事人主張自身私領域不被第三人侵擾或私事不被揭露的權利，權利判斷與個別當事人主觀認知、時下風土民情、媒體輿論、科技發展

¹²² 黃章令 (2020)，前揭註 95，頁 65。

或社會文化有密切關連；學者 Daniel J. Solove 亦在《瞭解隱私》乙書摘要中指出“隱私是我們這個時代最重要的概念之一，但它也是最難以捉摸的概念之一。隨著快速變化的技術使資料越來越容易獲得，學者、活動家和政策制定者一直在努力定義隱私，許多人承認這項任務實際上是不可能的 (Privacy is one of the most important concepts of our time, yet it is also one of the most elusive. As rapidly changing technology makes information increasingly available, scholars, activists, and policymakers have struggled to define privacy, with many conceding that the task is virtually impossible.)”，「隱私」本質上屬相對性高之權利概念，隨著不同文化與歷史而異，亦因快速的技術發展而變動¹²³，難謂有一普世、客觀、亙古不變之標準以界定其範圍。以本文的智慧自駕車為例，私人汽車除了是一種交通工具，其內部空間意味著一個私人領域，人們可以在其中享受某種形式的決策自主權及擁有私人活動之自由，汽車使用者對於車內的空間具有一定的隱私期待，如同法律上針對私人住宅有更高的法律保障。而如今集合一身先進科技的智慧自駕車，以不同的資料蒐用方式，隨時隨地且持續性的監控不特定當事人，對於隱私侵害的疑慮為過往案例所不能比擬。

3.3 個人資料(Personal Data)定義相較為具體

相對隱私權的不確定，「個人資料」(Personal Data)之概念為具有特定個人識別性之資料。「個人資料」之範疇相較「隱私」之界定，不問是否具有私密性，且不介入當事人主觀認知，其範圍客觀容易界定。個人資料以《個資法》明文例示之個資為例，可分為直接可辨識的資料如姓名、身分證字號等；亦有須與其他資料對照結合，才能辨識當事人的資料如車牌、IP address、電話號碼等間接可識別個資；個人資料除為彰顯當事人在社會社交活動的屬性資料外，亦包含個人在經濟活動之所有活動紀錄，因此其性質差異極大，以資料公示性分類：首先如當事人面容、姓名、聯絡方式、工作地點、姓名等因工作或生活必須所必須經常性揭露，其公示性較高而私密性較低之資料；其二為經濟活動須揭露如身分證字號、存放款等有關

¹²³ Solove, D. J., & Schwartz, P. M. (2009). *Privacy, information, and technology*. Aspen Publishers.

資料(釋字第 293 號解釋參照)，屬於經濟活動與社交必要時對特定對象揭露但私密性較高之資料；其三，亦有性向、DNA、病歷、前科等資料，則為該當事人私密性高且無對外第三者公開揭露必要之資料，且該資料揭露後對當事人會有極大影響之個人資料，如我國《個資法》第 6 條將醫療、基因、病歷、前科等私密性高且敏感之個資列為敏感性資料 (sensitive information data) 或稱特種資料 (special categories of personal data)。

再者，從前述空間隱私權及生活私密隱私權，個人對自己私生活領域單純不被干擾，如尾隨侵犯空間隱私權，或如偷窺或偷聽等侵犯生活私密隱私權之行為，此些行為若無資料之蒐用即非個資法所規範，但為傳統隱私權及人格權之保障範疇；另一個類別為私生活領域具有高私密性之資料，如前科、病歷、基因、性生活、健康檢查、犯罪前科(《個資法》第二條參照)，故亦為個資保護之範疇，此兩者差異可從「隱私」與「資訊隱私」兩者差異得知，易言之，在可能侵害隱私權的態樣中，資料之數位化及數位化後所為之處理與利用行為，是「隱私」與「資訊隱私」差異所在。類比「資料」與「數據」兩者之差異，正反應「隱私」與「資訊隱私」之差異，及科技對隱私保護之衝擊，「資料」與「數據」兩者差異本文將於後面第五章中探討之。故個資法所保護個資之範圍與隱私權保護隱私之範圍，有重疊競合處，亦有各自不同之部分，如論者¹²⁴在 2013 年《個人資料保護法關於「個人資料」保護範圍之檢討》著作中對於「隱私權-隱私」-「資訊隱私」-「個人資料」之差異闡述，除前面所提兩種態樣，另一方面個人出入公共場所、或公開活動之活動資料，如姓名、聯絡方式、特徵舉止，因無法合理期待不被任意第三人知悉，故該文中認為該些資料本質上不具私密性，與中文「隱私」兩字含有「秘密」或「隱匿性」之字義比對，難以認定為隱私權保護之範圍¹²⁵，惟本文認為該些資料在被蒐用下可藉由該資料識別並追蹤特定個人，以監控(Surveillance)、識別(Identification)、侵擾

¹²⁴ 范姜真嫩 (2013)，《個人資料保護法關於「個人資料」保護範圍之檢討》，東海大學法學研究，第四十一期，頁 107。

¹²⁵ 范姜真嫩 (2013)，前揭註 124，頁 102。

(Intrusion)等態樣(表 8 參照)影響人格發展，亦屬學者 Daniel J. Solove 所歸納的隱私侵犯態樣，亦有學者將此部分定為資訊自主權¹²⁶，並區分「資訊隱私權」與「資訊自主權」兩者。綜上之分類如下圖 27 所示，此種分類方式以資料的**公示性與隱密性作為分類**，然而因為科技的快速進展，是否應該還有更細分的分類及保護等級？這些可能的疑問在第四章的案例探討後，綜合前述技術之背景知識，本文將在第五章作進一步的探討。

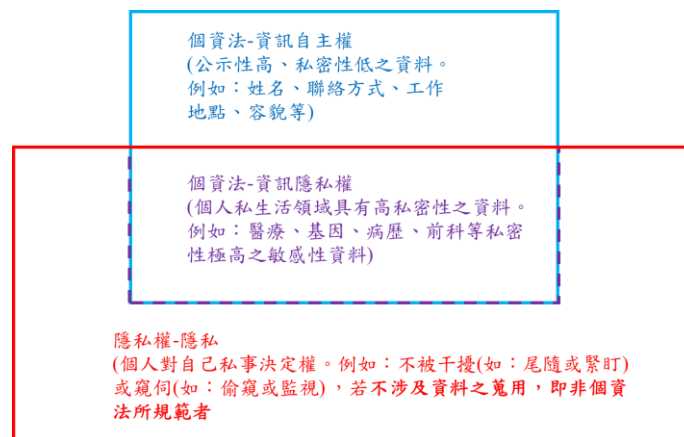


圖 27. 「個人資料」、「資訊隱私權」及「隱私權」三者性質與關係。資料來源：本文整理

綜上之所述，「個人資料」與「隱私」兩者間其實還是有所差異，因為個人資料有個人資料保護法所明確定義，不問是否具有私密性，不介入當事人主觀認知，其範圍相較客觀且易界定。為明確本論文探討之範疇，故以「個資」來探討。除此，「個資」之定義是否因為新技術如人工智慧、物聯網、大數據等之導入而變化，或者因為自駕車之應用場域而須有所調整？將於本文第五章作進階的探討。

3.4 隱私與個人資料保護應衡量公眾利益

無論隱私權或個資資料之保護並非絕對，都是在兩者與公眾利益間之平衡。然所謂公眾利益亦依個案狀況判定，我國《個資法》立法時亦謂公共利益屬於不確定的法律概念，目前我國《個資法》並沒有明確定義何謂公共利益或重大公共利益。

¹²⁶ 邱文聰 (2009)，前揭註 107。

以我國行政法觀點，學者全鍾燮提出八項是否符合公眾利益準則：“1、公民權利：是否有證據顯示新政策已將多種公民權利納入考量，而且不會侵犯這些權利？2、倫理與道德標準：行政機關的新政策及其行動能否禁得民眾之倫理與道德層面的檢驗？3、民主程序：相關人等是否已充分表達意見？行政機關除了聆聽民眾意見外，是否已經儘可能地把相關意見納入對話過程？4、專業知識：所做的建議是否考量專業意見？5、非預期結果：所做的建議是否進行充足的分析，俾提供可能的長期效果說明？6、共同利益：所做的建議是與特定利益較有關聯性，或是它可反應較大群眾的利益？7、輿論民意：對於社會爭論問題、媒體、公聽會所反映的議題所呈現出來的民意或輿論，是否試圖加以查覺並納入考量？8、充分開放：在政策形成過程中，有關協商、決策、背景資料、專業意見等，是否可供外界監視？”

在歐盟 GDPR 規定為重大公共公益之必要蒐集，須符合：“1.必須根據歐盟或成員國法律進行處理；2.該法律應與所追求的目標相稱；3.尊重資料/個人資料保護權的本質；4.並提供適當和具體的措施來保障基本權利和當事人(資料主體)的利益”¹²⁷。

人工智慧自駕車的應用如前所述，除了生命法益外，對於環保、節能、減碳及人口老化等社會公益皆有明顯助益，這些理應都屬社會公益的效益，在與個人資料/隱私保護間如何權衡？很難一言以蔽之。此外，在自駕車的應用上有兩點特別值得注意，1.民眾對車輛內個資的合理期待為何，是否與私人居住有等同水準？2.自駕車部分資料之應用直接與安全有關，且為該應用場域中普遍之現象，在此考量下資料法規是否該以隱私保護為中心？

四. 隱私權與財產權

上述以隱私權觀點探討個人資料還是偏重於保障隱私權與人格權，避免因為個人隱私暴露而導致影響當事人人格發展。然而從我國個資法第一條後段「促進個人資料之合理利用」，亦有將個人資料視為具財產權屬性。另外以美國《加州消費

¹²⁷ GDPR, Article 9(2)(g).

者隱私法(CCPA)》將個人資料視為一種可交易的財產，其中還規定了資料經紀人及經紀商。在此架構下，是以數字經濟著眼，建立一個以資料當事人、資料控制者、資料蒐用者及監管者等多邊經濟生態體系。

承前所述的廢棄資料是否為個人資料範疇爭點?若否，則廢棄資料是否還屬當事人的個人財產?當事人是否還有個資保護法規範下的資料自主權?此外，若廢棄資料不屬個人資料，自不屬《個資法》所管轄。那透過廢棄資料所資料挖掘(Data Mining)的個人資料，財產權到底屬於資料當事人還是資料控制者?資料所屬當事人是否還保有刪除權利?

第三節 各國自駕車政策與法規規範

基於各式無人載具科技創新應用與商業行為蓬勃發展，大量商品化產品通行、創新商業營運模式與新科技運用，也因此對各國現行無人載具政策、法規環境與監理機制帶來衝擊及挑戰。考諸各國官方資料及文獻報導，下面就自駕車主要國家的自駕車政策與法規規範作一介紹，值得注意的是與本文相關的資料及隱私問題已被多個國家自駕車政策列為重要項目，自駕車資料與隱私之重要性已臻明灼。

第一項 美國自駕車政策

一.聯邦自駕車主要法規或政策

作為全球汽車消費及製造的大國，美國為確保自身在自駕車全球領導地位，並引領全球自駕車立法潮流，2016年歐巴馬總統主政時代建立自動駕駛專門法，美國交通部(DOT)於同年9月頒布《聯邦自動駕駛政策(Federal Automated Vehicles Policy, FAVP)》¹²⁸，**FAVP**被視為全球首部關於自駕車的政策，此政策主要由DOT

¹²⁸ U.S. DOT (2016/09). *Federal Automated Vehicles Policy*.
<https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016>

所主導，目標是加速下世代的道路安全革命(Accerlerating the next revolution in roadway safety)，特別是高度自駕車(highly automated vehicles, HAVs)。此政策重點摘要¹²⁹如下：一. 提出自駕車發展要點指南架構 (Framework for Vehicle Performance Guidance)，建議自駕車應滿足數據紀錄及分享(Data Recording and Sharing)、隱私(Privacy)、系統安全(System Safety)、汽車網路安全(Vehicle Cybersecurity)、人機介面(Human-Machine Interface)、耐撞性(Crashworthiness)、消費者教育與訓練(Consumer Education and Training)、撞擊後車況(Post-Crash Vehicle Behavior)、聯邦，州及地區法令(Federal, State and Local Laws)和道德考量(Ethical Consideration)等 10 項要點，若以安全評估(Safety Assessment)則再另加入登錄與認證(Registration and Certification)、操作設計(Operational Design Domain, ODD)、物件擊事件偵測與反應(Object and Event Detection and Response)、最小風險狀態(Fall Back/ Minimal Risk Condition)及驗證方法(Validation Methods)；二. 明確聯邦政府與州政府個別之權責定位與分工，鼓勵各州制定高度自駕車(HAVs)之規範¹³⁰；三. 自駕車分類採用 SAE 標準的六等級，不使用 NHTSA 自訂的自駕車等級分類；四. 考慮隱私及道德風險並獨立列式。依此政策及其架構，廠商可作為發展自駕車功能方向，所屬主管行政單位則可研議細部的標準或法令，惟當時 FAVP 發布要點建議中，要求自駕車廠商，特別是高度自駕車(HAVs)，資料紀錄去識別化之後需與其他第三方分享共用¹³¹，以促進產業之發展，此規定對於正在發展的自駕車廠商來說會造成商業機密洩漏之疑慮，因此備受爭議。2017 年 9 月美國眾議院通過《確保車輛演化的未來部署和研究安全法案 (Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution Act, H.R.3388)》，此法案亦稱為《自動駕駛法案 (SELF DRIVE Act, SDA)》，SDA 法案優先於各州頒布有關高度自動化車輛或自動駕駛系統的設計、構造或性能的法律，旨在“保障安全與創新發展、車輛測試及促進自動駕駛交通工具的部署，建立全美統一的規則體系，以促進企業在政府監管下安全地

¹²⁹ NHTSA (2016/09). *Federal Automated Vehicles Policy*.

<https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf>

¹³⁰ NHTSA (2016/09). *Id.*, at p.37-47.

¹³¹ NHTSA (2016/09). *Id.*, at p.18 and p.104.

支持自駕車科技創新，並潛在保障道路上生命、改善移動力並增加新的全美商機 (The SELF DRIVE Act is first-of-its-kind legislation to ensure the safe and innovative development, testing, and deployment of self-driving cars. This bipartisan bill provides a much-needed federal safety framework to support self-driving technology and its potential to save lives on the road, improve mobility, and create new economic opportunity across the country.)”¹³²。此法雖目前因為參議院希望 NHTSA 提供更多有關車輛撞擊及軟體的資料，截至今年(2022年)4月 SDA 法案尚未通過¹³³。NHTSA 於今(2022)年3月另發布首創自動駕駛系統車輛之乘員保護安全標準¹³⁴。

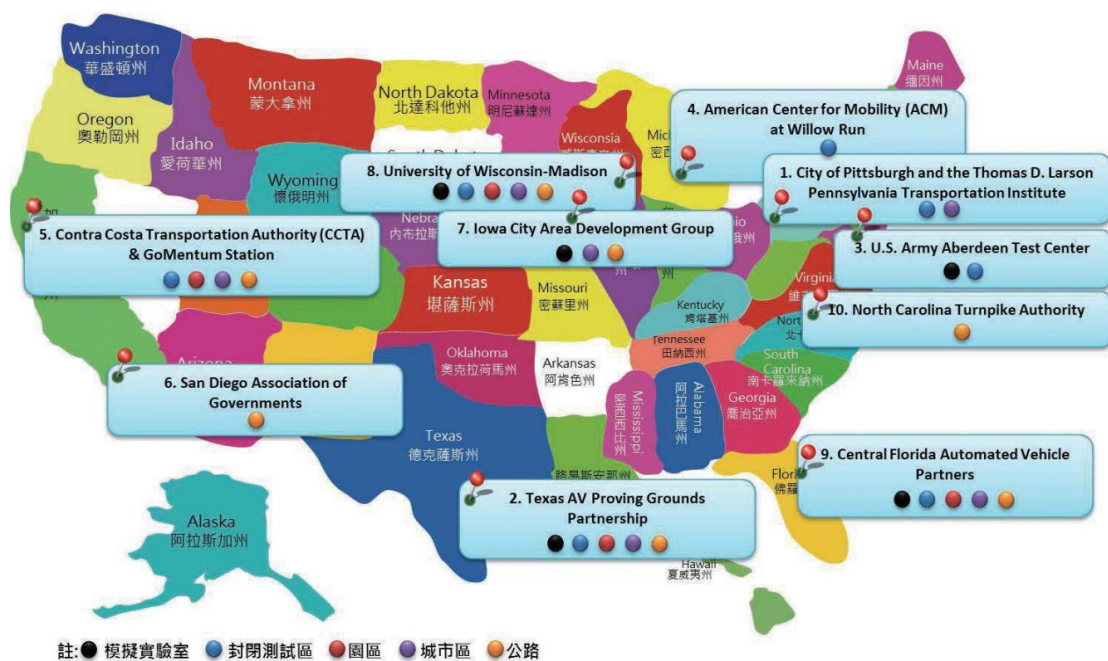


圖 28. 美國官方指定測試區。資料來源：ARTC¹³⁵

從下表 9 可看出，自 2016 年以來美國交通部及國家道路交通安全管理局持

¹³² E&C Republicans. HOUSE PASSES BIPARTISAN LEGISLATION PAVING THE WAY FOR SELF-DRIVING CARS ON AMERICA’S ROADS. <https://republicans-energycommerce.house.gov/selfdrive/>

¹³³ H.R.3388 - SELF DRIVE Act, 115th Congress (2017-2018). <https://www.congress.gov/bill/115th-congress/house-bill/3388>

¹³⁴ NHTSA (2022/03/10). NHTSA Finalizes First Occupant Protection Safety Standards for Vehicles Without Driving Controls. <https://www.nhtsa.gov/press-releases/nhtsa-finalizes-first-occupant-protection-safety-standards-vehicles-without-driving>

¹³⁵ 陳敬典 (2018)，《自動駕駛車發展與未來趨勢》，車輛中心，2018 車輛研測專刊。

續 1~2 年間格時間，持續更新一版自動駕駛政策，這些政策是作為指南而非法律規章提供給相關自駕車產業，對各州公務機關前期規章制度框架和最佳實施範例提供指南;對自駕車汽車製造商和其他車輛團體在自動駕駛的安全設計、開發、資料處理、測試、隱私保護和應用等各個系節提供明確方向。且每一年的新的政策除了反應 NHTSA、車輛廠商、供應商、消費者等的建議，並反應出自駕車而科技整合創新及新技術導入而不斷更新變化的情況。

表 9. 美國交通部(DOT)公告的自動駕駛政策。資料來源：DOT;NHTSA;本文整理更新

時間	檔案名稱	發布單位
2016 年 9 月	自動駕駛 1.0 《Federal Automated Vehicles Policy : Accelerating the Next Revolution In Roadway Safety》	DOT NHTSA
2017 年 11 月	自動駕駛 2.0 《Automated Driving Systems 2.0 : A Vision for Safety》	DOT NHTSA
2018 年 10 月	自動駕駛 3.0 《Automated Vehicle 3.0:Preparing For The Future Of Transportation》	DOT
2020 年 1 月	自動駕駛 4.0 《Automated Vehicles 4.0: Ensuring American Leadership in Automated Vehicle Technologies》	NSTC DOT
2021 年 1 月	自動駕駛綜合計畫 Automated Vehicles Comprehensive Plan	DOT

承前所述，美國 NHTSA 於 2016 年 9 月公布聯邦自動駕駛政策「Federal Vehicle Policy」之後，2017 年 9 月 DOT 頒布《自動駕駛系統 2.0：安全願景 (Automated Driving Systems 2.0: A Vision for Safety (簡稱：ADS 2.0))》，此非強制性法規而是**指導意見**，係提供汽車產業、州政府與相關單位未來發展之參考。此份 ADS 2.0 檔案充分參考 FAVP，延續對於自動駕駛自願性指導及對於各州監管的支持，適用範圍為 SAE 等級 Level 3 至 Level 5 自動駕駛技術能力之車輛，提出 12 項於設計、測試最重要的評估指南，以安全為主軸延伸建議各層面應思考及應符合的事項，其被自駕車產業廣泛作為研發的圭臬。另外 ADS 2.0 闡明聯邦政府與州政府的權責

範圍，總括來說，NHTSA 主要為自駕車及其設備的安全設計以及與社會大眾溝通並進行安全教育之負責單位，州政府則負責人類駕駛與車輛操作行為制定規範與管制。



表 10. FVAP 與 ADS 2.0 比較。資料來源：FVAP;ADS;資策會 MIC¹³⁶;本文整理更新

	FVAP	ADS 2.0
適用範圍	採用 SAE 標準的六自駕車等級分類	SAE 等級 L3 至 L5 之 HAVs
自駕車發展要點	<ul style="list-style-type: none"> ● 數據記錄 ● 隱私 ● 系統安全 ● 網路安全 ● 人機介面 ● 耐撞性能 ● 消費者教育 ● 註冊與認證 ● 碰撞後表現 ● 政府法規 ● 道德判斷 ● 操作適用範圍 ● 偵測與反應 ● 退出機制 ● 驗證方法 	<ul style="list-style-type: none"> ● 系統安全 ● 操作設計領域 (ODD) ● 物件與事件偵測與反應 (OEDR) ● 退出機制 (最小化風險) ● 驗證方法 ● 人機介面 ● 車輛網路安全 ● 車輛剛體性 (耐撞度) ● 事故後表現 ● 資料紀錄 ● 消費者教育與訓練 ● 聯邦、州政府與地方法令
權責劃分	NHTSA 主導車輛安全標準，促使廠商召回與修復不合格的自駕車，並持續推動制定自駕車相關的聯邦法規；州政府則應建立自駕車專責機關以監管當地的自駕車測試資格，並可以依據地區特性規定自駕車測試的範圍	<ul style="list-style-type: none"> ● 聯邦政府權責 ● 制定新興整車與零組件所適用的美國聯邦 ● 汽車安全標準 ● 強制應符合美國聯邦汽車安全標準 ● 調查及管理全國不遵守規定者與有關車輛 ● 安全瑕疵之召回與改正 ● 有關車輛安全議題，應向民眾進行教育，或一同交流 ● 州政府權責 ● 發放駕駛員執照，並在其管轄範圍內登記車輛 ● 同意並實施交通法律與規定 ● 執行安全審查，但內容由政府自行決定制定車輛保險與責任的規章

¹³⁶ 何心宇 (2019/4/12)，《主要國家自駕車政策發展現況》，MIC AISP 情報顧問服務，載於：<https://mic.iii.org.tw/AISP/Reports?docid=CDOC20190408001> (最後瀏覽日：2022 年 3 月 5 日)

而 2018 年 10 月公布《自駕車 3.0 政策檔 (Preparing for the Future of Transportation: Automated Vehicles 3.0 (簡稱: AV 3.0))》，以 ADS 2.0 基礎上將範圍擴充到地面道路運輸系統，且 AV 3.0 並建構三個關鍵領域：1.推進多模式安全 (Advancing multi-modal safety);2. 減少政策之不確定性 (Reducing policy uncertainty);3.概要與美國交通部之合作流程(Outlining a process for working with U.S. DOT)¹³⁷。在此所謂多模式安全(Multi-modal safety)泛指道路上可能之安全利益相當當事人，除了基本的駕駛與乘客之外，並泛指行人、自行車、機動車輛等之安全考量。

AV 3.0 提出 DOT 對於自駕車之原則為：1.安全優先 (prioritize safety)，DOT 將致力於確認可能安全風險，提升自駕車對駕駛、乘客、行人、自行車、機動車輛及其他使用道路之旅人等之安全保障，並提高其拯救生命的潛力，以強化公眾對於新興技術之信心；2.技術中立 (remain technology neutral)：秉持美國政府對技術中立與彈性的一貫政策，以促使競爭與創新成為實現安全、機動性和經濟目標的途徑；3.法規的與時俱進 (modernize regulations)；DOT 將會現代化並滾動檢討並修正可能阻礙自駕車發展之過時交通法規；4.鼓勵法規與操作環境的一致性 (encourage a consistent regulatory and operational environment)；DOT 將致力於讓美國各州與聯邦之自駕車法規環境一致，降低法規不協調所導致的發展阻礙與抱怨，讓自駕車在全美有一致性的共通法規環境；5.對自動化主動積極 (prepare proactively for automation)；DOT 將主動提供指南、最佳實施、駕駛訓練等各種協助，並將針對車聯網等相關支援技術及環境建構進行準備；6.保障並促進(美國人)自由 (protect and enhance the freedoms enjoyed by Americans):除尊重美國公民在開放道路上的駕車自由以及消費者自由選擇滿足出行需求的能力，並支援年長者和身障人士實現安全和獨立行動的選擇。

參諸前述原則，AV 3.0 執行策略為：1.鼓勵利害關係者（與企業有利害關係

¹³⁷ U.S. DOT (2019/12/13). *Preparing for the Future of Transportation: Automated Vehicles 3.0*. <https://www.transportation.gov/av/3>

的相關人員或機構)參與 (Stakeholder engagement); 2. DOT 將為州和地方政府提供最佳實踐方案(Best Practices)與政策考量; 3. 支持自願性技術標準 (**Voluntary standards**) 制定; 4. 目標導向之研究 (Targeted research); 5. 鼓勵和支持監管現代化 (Regulatory modernization)。



為確保美國在自動駕駛汽車技術方面的領先地位，美國政府又在 CES 2020 年一月宣布提出自動駕駛汽車 4.0 (簡稱 AV 4.0)，AV 4.0 建立在對交通的未來做準備，AV 4.0 建立在為交通的未來做準備及 AV 3.0 的基礎上，將範圍擴大到 38 個相關的美國政府治理 (United States Government, USG) 單位，這些單位具有直接或間接監管自駕車 AV 技術的安全開發和整合。

AV 4.0 不同於先前三個版本，前三版本為 USDOT 單獨提出。而 AV 4.0 的制定為美國交通部與掌管白宮科技政策之行政辦公室(White House Office of Science and Technology Policy (OSTP))聯名提出，足見自駕車發展政策已上升到總統層級。AV 4.0 圍繞三個關鍵領域構建：USG AV 原則(USG AV Principles)、支持 AV 技術發展和領導的管理工作 (Administration Efforts Supporting Automated Vehicle Technology Growth and Leadership)以及 USG 活動和協作機會(USG Activities and Opportunities for Collaboration)。AV 4.0 旨在確保 USG 對自駕車(AV)技術採取一致的方法，並詳細說明整個 USG 的授權，研究和投資，以便美國可以繼續領導 AV 技術的研究、開發和組裝。2021 年針對自駕車創新的障礙，如免除自駕車製造商設置方向盤、煞車腳踏板、駕駛座等人類駕駛裝置的義務等作積極的排出。

AV 4.0 三大核心重點項目(Three core focus areas)與細節展開如下：

- 保護使用者與社群(Protect Users and Communities)
 - 安全至上(Prioritize Safety)：以美國政府主導，促進自動駕駛技術安全並解決潛在的安全性風險。
 - 重視機密與網路安全(Emphasize Security and Cybersecurity)：強調自駕技術從設計到實施的安全性;對於實體與網路安全性標準與基礎的建構與



提升。

- 確保隱私及資料安全(Ensure Privacy and Data Security)：相關資料的蒐集、處理、使用及共用等，確保個人隱私與資料安全獲得保障。
- 強化機動性與可及性(Enhance Mobility and Accessibility)：保護消費者能有最適且可觸及的交通選項。
- 推動有效率的市場(Promote Efficient Markets)
 - 技術中性原則(Remain Technology Neutral)
 - 推動美國創新與創意(Protect American Innovation and Creativity)
 - 法規現代化(Modernize Regulations)
- 促成一致的標準和政策 (Facilitate Coordinated Effects);
 - 推動一致性的標準與政策(Promote Consistent Standards and Policies)：美國政府領導參與且倡導國際標準與基於數據上的法規。
 - 確保一貫的聯邦做法(Ensure a Consistent Federal Approach)：持續美國自駕技術的成長與領導地位理念並貫徹。
 - 改善交通運輸系統層級的影響(Improve Transportation System-Level Effects)：以系統層級提升交通解決方案。

2021 年 1 月 11 日，架構於 AV 4.0 並為具體落實 DOT Automated Driving Systems (ADS)，美國 DOT 提出自動駕駛汽車綜合計劃(Automated Vehicles Comprehensive Plan, AVCP)，並定義以下三個目標：

- 促進合作 (Promote Collaboration)
- 使監管環境現代化(Modernize the Regulatory Environment)

➤ 準備交通運輸系統(Prepare the Transportation System)

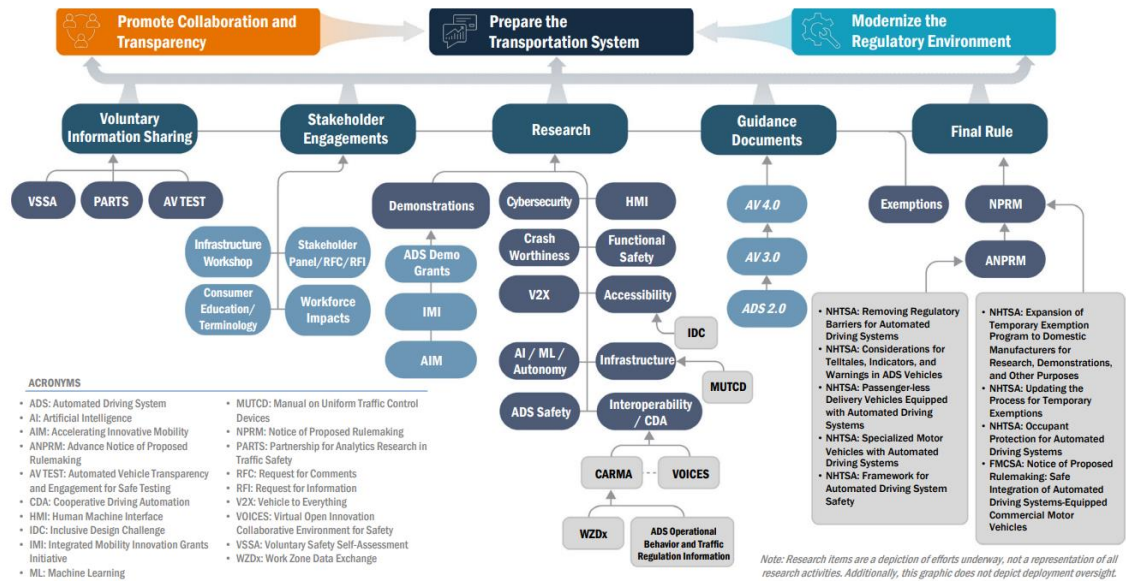


圖 29. AVCP 的架構。資料來源：DOT¹³⁸

二. 全美各州自駕車立法

州政府為監管地方自駕車產業發展，根據全美州議會聯合會（National Conference of state Legislatures）官方有關自駕車法案的統計¹³⁹，自 2012 年至 2020 年 2 月，逾 41 個州和華盛頓哥倫比亞特區(D. C.)考慮自駕車相關的立法¹⁴⁰。截至 2020 年 3 月，美國已有 32 州頒布公共道路上有關自動駕駛測試或部署的立法，此外，亞利桑那州、內布拉斯加與內華達州已授權在特定的環境中進行無人為操作的 L5 全自動駕駛。

¹³⁸ US DOT (2021/01). *Automated Vehicles Comprehensive Plan*, p.15.
https://www.transportation.gov/sites/dot.gov/files/2021-01/USDOT_AVCP.pdf

¹³⁹ NCSL (2022/07/20). *Autonomous Vehicles State Bill Tracking Database*.
<https://www.ncsl.org/research/transportation/autonomous-vehicles-legislative-database.aspx>

¹⁴⁰ NCSL (2020/02/08). *Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation*.
<https://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx>

在各州的州法政策立法進程上，首先自內華達州車輛監理處(Department of Motor Vehicles, DMV)2011 年頒布自動駕駛汽車道路測試規定(Nevada Revised Statutes (NRS) Chapter 428A)¹⁴¹及自動駕駛車輛測試許可證，爾後其餘各州產官界對於自動駕駛技術研發與政策立法就如雨後春筍，在具指標之加州、密西根州、亞利桑那州與佛羅里達州，由於各州的企業發展、科技導入、道路條件、立法程序、經濟環境等有所差異，除確保自駕車之安全優先，測試條件與驗證自駕能力是基本且必要的之外，各州有各自因地制宜的自駕車測試法規制定，頒布自駕車法規與行政命令程度亦有所不同。為確保自駕車之安全優先且累積意外之資料數據，測試條件與驗證自駕能力之資料之蒐集與回饋相當重要，限定公用道路測試場域之實測里程是被要求的基本項目；此外，大多數已開放無須駕駛者的自駕車道路測試，如加州已於今年(2022 年)核准通用汽車(GM)下的 Cruise 完全自駕車在舊金山讓公眾免費搭乘，並於 6 月開始收費。

位處高科技與新創企業集中的加州為美國自駕車發展的代表，以該州車輛監理處(DMV, CA)的無人自駕車測試計畫與部署規範里程碑為例¹⁴²，從 2015 年 12 月首次發布了部署規範草案以供公眾審查；2016 年 9 月 30 日發布了經修訂的部署規範草案，並於 2016 年 10 月 19 日在州議會大廈舉行了關於規範草案的公開研討會；2017 年 3 月 10 日為在加州測試和部署全自動駕駛汽車建立路徑的擬議法規發布，並開始了為期 45 天的公眾意見徵詢，並於 2017 年 4 月 25 日在 Sacramento 舉行了公開聽證會，以收集有關擬議法規的意見；2017 年 10 月 11 日，車輛監理處發布了修訂後的法規，涵蓋無人駕駛測試和自動駕駛汽車的部署。該版本開始了為期 15 天的公眾意見徵詢期，於 2017 年 10 月 25 日結束；2017 年 11 月 30 日，車輛監理處發布了第二個為期 15 天的公眾評議期的修訂條例，該期於 2017 年 12 月 15 日結束；2018 年 1 月 11 日，將涵蓋無人駕駛測試和部

¹⁴¹ DMV(NV). *CHAPTER 428A - AUTONOMOUS VEHICLES*.
<https://www.leg.state.nv.us/nrs/nrs-428a.html>

¹⁴² DMV(CA). *AUTONOMOUS VEHICLE MILESTONES*.
https://www.dmv.ca.gov/portal/vehicle-industry-services/autonomous-vehicles/california-autonomous-vehicle-regulations/autonomous-vehicle-milestones/?fbclid=IwAR0tzPLGd9XE1dQcqANGNGC1sA_VwKjpCx-P9M0tj7H4Jti375CbVhbO2UI

署的最終監管包提交給行政法辦公室 (Office of Administrative Law, OAL) 以供批准;2018 年 2 月 26 日, OAL 批准了無人駕駛測試規定。2018 年 3 月 2 日, 車輛監理處在其網站上發布了批准的公告, 並在 2018 年 4 月 2 日通知後 30 天開始批准申請。



第二項 德國自駕車政策

汽車產業為德國經濟發展重要的命脈, 眾多國際知名品牌如 MERCEDES-BENZ、BMW、Volkswagen、PORSCHE、Audi、MAYBACH、OPEL、SMART 等都是產自該國, 因此該國的自駕車政策相當值得關注。德國因應車輛智慧自動駕駛之發展趨勢, 在 2015 年德國聯邦交通及數位基礎設施部 (Bundesministerium für Verkehr und digitale Infrastruktur, BMVI) 提出《自動與聯網駕駛策略方案 (Strategie automatisiertes und vernetztes fahren)》^{143,144}, 其被視為德國自動暨聯網駕駛策略重要的一環, 也做為未來法規框架修訂與建構的重要依據。據此, 並因應 2016 年 3 月維也納道路交通公約 (Vienna Convention on Road Traffic 1968) 之修正允許自動駕駛技術應用於交通運輸。德國為落實維也納道路交通公約朝向道路交通 4.0 邁進, 2017 年 3 月德國聯邦議院提出《道路交通法規 (des Straßenverkehrsgesetzes)》¹⁴⁵修正案¹⁴⁶, 《道路交通法規修正案》為自動暨聯網化駕駛系統車輛訂定規範, 並定義事故責任, 並允許駕駛人可操作具備部分自動駕駛功能 (Level 3) 及高度自動駕駛功能 (Level 4) 的車輛, 同年 6 月德國聯邦議院通過《道路交通法規修正案》。2017 年《道路交通法規修正案》尚未針對 L5 全自駕車有所規範, 此次修正針對 L3

¹⁴³ 何心宇 (2019), 《借鏡美/德/日三大國法規 自駕車政策發展促進創新》, 新通訊, 2019/8/13, 載於: <https://www.2cm.com.tw/2cm/zh-tw/market/5B2C469E82C04FC7B22D0E252782BDD8> (最後瀏覽日: 2022/2/10)

¹⁴⁴ 潘俊良 (2017), 〈簡析德國自動駕駛與車聯網發展策略〉, 《科技法律透析》, 第 29 卷第 4 期, 頁 25。

¹⁴⁵ Federal Ministry of Justice, Road Traffic Act (Straßenverkehrsgesetz). <http://www.gesetze-im-internet.de/stvg/>

¹⁴⁶ 資訊工業策進會科技法律研究所 (2021/03/10), 《德國聯邦政府內閣通過自駕車草案》, 載於: <https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=8637> (最後瀏覽日: 2022/2/10)

及 L4 等級之道路交通法規修法共有 4 大重點 1.駕駛者控制權：駕駛雙手可移開方向盤，並將控制權移轉給自動駕駛系統，不過駕駛猶須因應路況，隨時取代自動駕駛系統操控車輛，此點與 SAE 之規範相同；2.行車紀錄與黑盒子：要求配備自動駕駛汽車需配備行車記錄器的黑盒子，以紀錄行車數據及駕駛狀況，以用來協助判定車禍肇事責任；3. 肇事責任：在肇事責任依照事故原因界定駕駛人及汽車製造商之責任¹⁴⁷，若因自動駕駛缺失所導致的交通事故，提高最高賠償金額；4.資料保留時間與刪除之規定：前述黑盒子記錄資料如逾法規規定時間，資料需予以刪除，未依照規定刪除將可處以罰款¹⁴⁸。

在《道路交通法規修正案》法案通過後不久，BMVI 轄下之自動駕駛倫理委員會於同年 6 月頒布《自動化和網聯化車輛交通倫理準則(ETHICS COMMISSION: AUTOMATED AND CONNECTED DRIVING)》¹⁴⁹，主要針對 L 4 與 L5 兩個高度自駕車，此準則被視為全球因應自動駕駛技術的首套道德倫理標準，目的除了賦予自動駕駛合法性，更企圖在安全、人類尊嚴、自由選擇與資料保護上設立「德國標準」，發揮並保有德國於歐盟國家中在自動駕駛領域的領先地位。德國成為全球首個訂定「自動駕駛倫理」政府¹⁵⁰，《自動化和網聯化車輛交通倫理準則》包含 20 項自動駕駛暨聯網車輛的倫理準則，準則如本文第一章所述，從過往人類之於機器人之觀點，希望智慧自駕車系統如同機器人服從人類的道德原則。

¹⁴⁷ 財團法人資訊工業策進會科技法律研究所 (2018)，〈自駕車法制政策發展〉，《自駕車的第一本法律書》，臺北：資訊工業策進會科技法律研究所出版，書泉經銷。《自駕車的第一本書》

¹⁴⁸ 何心宇 (2019)，前揭註 143。

¹⁴⁹ BMVI (2017)，前揭註 14

¹⁵⁰ 利榮 (2018)，前揭註 7。

表 11. 德國自駕車《倫理指南》之 20 項倫理準則。資料來源：科技法律透析¹⁵¹，本文整理更新 2017 年版本

項次	準則	準則(英文)
1	<p>主要目標是針對部分自動及完全自動駕駛系統，改善所有用路人安全並提升交通效率。另一個目的是增加流動機會並使進一步的利益成為可能。科技發展服從個人自治原則，這意味著個人享有由他們自己負責的行動自由。</p>	<p>The primary purpose of partly and fully automated transport systems is to improve safety for all road users. Another purpose is to increase mobility opportunities and to make further benefits possible. Technological development obeys the principle of personal autonomy, which means that individuals enjoy freedom of action for which they themselves are responsible.</p>
2	<p>人身安全的保護優先於其他考量，當自動駕駛系統肇事機會小於人為駕駛，自動及聯網駕駛行為即符合道德倫理規範。目標是降低危害程度，迨至完全避免。許可自動化系統的數量是不合理的，除非它承諾至少在傷害方面與人類駕駛相比會減少，換言之，風險的積極平衡。</p>	<p>The protection of individuals takes precedence over all other utilitarian considerations. The objective is to reduce the level of harm until it is completely prevented. The licensing of automated systems is not justifiable unless it promises to produce at least a diminution in harm compared with human driving, in other words a positive balance of risks.</p>

¹⁵¹ 潘俊良 (2017/08/15)，〈德國自動駕駛倫理委員公布自動駕駛系統規劃指引〉，《科技法律透析》，第 29 卷第 08 期，頁 2-4。

項次	準則	準則(英文)
3	<p>於公共交通環境引進並允許自動及網聯化系統，政府應負保證責任。駕駛系統需要監管部門審核及監控，並以避免事故為宗旨。因此，駕駛系統需要官方許可和監控。指導原則是避免事故，儘管如果風險平衡從根本上是積極的，技術上不可避免的殘餘風險不會影響自動駕駛的引入。</p>	<p>The public sector is responsible for guaranteeing the safety of the automated and connected systems introduced and licensed in the public street environment. Driving systems thus need official licensing and monitoring. The guiding principle is the avoidance of accidents, although technologically unavoidable residual risks do not militate against the introduction of automated driving if the balance of risks is fundamentally positive.</p>
4	<p>個人為其做出的決定負責任是社會一種以個人為核心之展現，他們有權獲得個人發展和他們需要之保護。因此，所有政府和政治監管決定的目的都是促進自由發展和保護個人。在一個自由的社會中，一般發展制度中唯有最大的個人自由選擇與他人的自由及其安全之間取得平衡時，該技術才能被法律支持式。</p>	<p>The personal responsibility of individuals for taking decisions is an expression of a society centred on individual human beings, with their entitlement to personal development and their need for protection. The purpose of all governmental and political regulatory decisions is thus to promote the free development and the protection of individuals. In a free society, the way in which technology is statutorily fleshed out is such that a balance is struck between maximum personal freedom of choice in a general regime of development and the freedom of others and their safety.</p>

項次	準則	準則(英文)
5	<p>自動化和互聯技術應盡可能防止事故發生。基於現有技術，該技術的設計方式必須使危急情況一開始就不會出現。前述包括兩難境地，換句話說，自動駕駛汽車必須“決定”兩種弊端中的哪一個，在兩者之間無法權衡取捨，它必須執行。在這種情況下，整個技術選擇範圍——例如從限制應用範圍到可控交通環境、車輛傳感器和製動性能、危險人員的信號，直到通過“智慧”道路基礎設施預防危險——應該使用並不斷發展。道路安全的顯著增強是發展和監管的目標，從車輛的設計和程式編碼開始，使它們以防禦性和預期性的方式駕駛，儘可能減少對弱勢道路使用者構成的風險。</p>	<p>Automated and connected technology should prevent accidents wherever this is practically possible. Based on the state of the art, the technology must be designed in such a way that critical situations do not arise in the first place. These include dilemma situations, in other words a situation in which an automated vehicle has to “decide” which of two evils, between which there can be no trade-off, it necessarily has to perform. In this context, the entire spectrum of technological options – for instance from limiting the scope of application to controllable traffic environments, vehicle sensors and braking performance, signals for persons at risk, right up to preventing hazards by means of “intelligent” road infrastructure – should be used and continuously evolved. The significant enhancement of road safety is the objective of development and regulation, starting with the design and programming of the vehicles such that they drive in a defensive and anticipatory manner, posing as little risk as possible to vulnerable road users.</p>

項次	準則	準則(英文)
6	<p>引進可能是社會和道德上的強制要求的更高等級的自動駕駛，特別是自動碰撞預防選項，如果它具有可以超越現有的損害限制潛力。相反，使用全自動運輸系統的法定義務或實際不可避免的原因在道德上是有問題的，如果它需要服從技術要求（禁止將主體降級為單純的網路元素）</p>	<p>The introduction of more highly automated driving systems, especially with the option of automated collision prevention, may be socially and ethically mandated if it can unlock existing potential for damage limitation. Conversely, a statutorily imposed obligation to use fully automated transport systems or the causation of practical inescapability is ethically questionable if it entails submission to technological imperatives (prohibition on degrading the subject to a mere network element).</p>
7	<p>在被證明是不可避免的危險情況下，儘管採取了所有技術預防措施，惟於平衡受法律保護的利益時，保護人類生命仍是重中之重。因此，在技術可行的範圍內，必須對系統進行程式編碼，以便在衝突中接受對動物或財產的損害，如果這意味著可以防止人身傷害。</p>	<p>In hazardous situations that prove to be unavoidable, despite all technological precautions being taken, the protection of human life enjoys top priority in a balancing of legally protected interests. Thus, within the constraints of what is technologically feasible, the systems must be programmed to accept damage to animals or property in a conflict if this means that personal injury can be prevented.</p>

項次	準則	準則(英文)
8	<p>真正的兩難決策，例如兩個人的生命之間的決定，取決於實際的具體情況，包括受影響各方的“不可預測”行為。因此它們不能被明確標準化，也不能被程式編碼且認為他們在道德上是毋庸置疑的。技術系統的設計必須避免事故。然而，它們不能標準化為複雜或直觀的評估以能夠替代或預測事故決定的方式，並對事故的影響有道德能力做出正確判斷的負責任的駕駛。的確，一個如果人類駕駛員在緊急情況下為了救人而殺死了一個人，那將是非法行為為一個或多個其他人的生命，但他的行為不一定是犯罪的。此類法律判斷，在回顧和考慮特殊情況下作出，不能輕易地轉化為抽象/一般的事前評估，因此也不能進入相應的程式編碼活動。出於這個原因，也許比其他任何原因，希望有一個獨立的公共部門機構系統地處理吸取的教訓。</p>	<p>Genuine dilemmatic decisions, such as a decision between one human life and another, depend on the actual specific situation, incorporating “unpredictable” behaviour by parties affected. They can thus not be clearly standardized, nor can they be programmed such that they are ethically unquestionable. Technological systems must be designed to avoid accidents. However, they cannot be standardized to a complex or intuitive assessment of the impacts of an accident in such a way that they can replace or anticipate the decision of a responsible driver with the moral capacity to make correct judgements. It is true that a human driver would be acting unlawfully if he killed a person in an emergency to save the lives of one or more other persons, but he would not necessarily be acting culpably. Such legal judgements, made in retrospect and taking special circumstances into account, cannot readily be transformed into abstract/general ex ante appraisals and thus also not into corresponding programming activities.</p> <p>For this reason, perhaps more than any other, it would be desirable for an independent public sector agency (for instance a Federal Bureau for the Investigation of Accidents Involving Automated Transport Systems or a Federal Office for Safety in Automated and Connected Transport) to systematically process the lessons learned.</p>

項次	準則	準則(英文)
9	<p>如果發生不可避免的事故情況，任何基於個人特徵的區別（年齡、性別、身體或精神體質）是嚴格禁止的。也禁止使受害者間相互替代。</p> <p>一般程式編碼，以減少數量人身傷害可能是合理的。</p> <p>參與因移動產生的各方風險，不得犧牲非相關方。</p>	<p>In the event of unavoidable accident situations, any distinction based on personal features (age, gender, physical or mental constitution) is strictly prohibited.</p> <p>It is also prohibited to offset victims against one another. General programming to reduce the number of personal injuries may be justifiable. Those parties involved in the generation of mobility risks must not sacrifice non-involved parties.</p>
10	<p>法律責任規定及司法實務認定必須充分考量未來駕駛人責任轉至自動及「聯網系統製造商、技術系統營運商之情形。</p>	<p>In the case of automated and connected driving systems, the accountability that was previously the sole preserve of the individual shifts from the motorist to the manufacturers and operators of the technological systems and to the bodies responsible for taking infrastructure, policy and legal decisions.</p>
11	<p>製造商與營運商對於自動及聯網駕駛系統負有損害賠償責任，且其必須不斷優化並更新已交付產品。</p>	<p>Liability for damage caused by activated automated driving systems is governed by the same principles as in other product liability.</p>
12	<p>公眾有權利充分瞭解新技術及其應用差異化知識之權利，應該儘可能以更透明的形式傳達，同時由專業獨立機構對其進行審查。</p>	<p>The public is entitled to be informed about new technologies and their deployment in a sufficiently differentiated manner.</p>

項次	準則	準則(英文)
13	<p>目前尚無法評估未來軌道及航空交通工具，是否可完全自動暨聯網化並集中控制，在此些基礎建設未確定前，尚的道德疑慮。</p>	<p>It is not possible to state today whether, in the future, it will be possible and expedient to have the complete connectivity and central control of all motor vehicles within the context of a digital transport infrastructure, similar to that in the rail and air transport sectors.</p>
14	<p>對於自動及聯網駕駛的通訊安全要求僅限於合理範圍內，不應過度憂慮而破壞新技術發展之信心。</p>	<p>Automated driving is justifiable only to the extent to which conceivable attacks, in particular manipulation of the IT system or innate system weaknesses, do not result in such harm as to lastingly shatter people's confidence in road transport.</p>
15	<p>在道路使用者的自主性和資料主權方面的限制下，允許商業模式利用自動駕駛和聯網駕駛產生的資料，無論對車輛控制重要或不重要的。</p> <p>駕駛人有權利決定車輛資訊可否轉供他人使用。</p> <p>此類資料的自願性揭露以存在難以替代方案和實用性為前提。</p>	<p>Permitted business models that avail themselves of the data that are generated by automated and connected driving and that are significant or insignificant to vehicle control come up against their limitations in the autonomy and data sovereignty of road users. It is the vehicle keepers and vehicle users who decide whether their vehicle data that are generated are to be forwarded and used. The voluntary nature of such data disclosure presupposes the existence of serious alternatives and practicability</p>

項次	準則	準則(英文)
16	<p>在任何情況下必須明確界定誰負責駕駛任務，並需記錄儲存行車情況，以釐清可能賠償責任的問題。</p>	<p>It must be possible to clearly distinguish whether a driverless system is being used or whether a driver retains accountability with the option of overruling the system.</p>
17	<p>高度自動化之車輛無法於緊急狀況下瞬間轉換由駕駛人操作，為了實現高效、可靠、安全運作，系統設計應更符合人類使用需求，而非賦予駕駛人過重的要求。</p> <p>實現高效、可靠和安全的人機溝通並防止過載，系統必須更多地適應人類的交流行為，而不是要求人類增強適應能力。</p>	<p>The software and technology in highly automated vehicles must be designed such that the need for an abrupt handover of control to the driver (“emergency”) is virtually obviated. To enable efficient, reliable and secure human-machine communication and prevent overload, the systems must adapt more to human communicative behaviour rather than requiring humans to enhance their adaptive capabilities.</p>
18	<p>車輛在某種程度上能連結中央資料庫，並實現自我學習，自我學習應通過相關驗證測試。</p> <p>除非滿足安全要求，否則不得部署自學系統關於與車輛控制相關的功能的要求，並且不破壞在此制定的規則。</p> <p>將相關情景移交給中立機構的集中情景目錄，以便開發適當的通用標準，包括任何驗收測試。</p>	<p>Learning systems that are self-learning in vehicle operation and their connection to central scenario databases may be ethically allowed if, and to the extent that, they generate safety gains. Self-learning systems must not be deployed unless they meet the safety requirements regarding functions relevant to vehicle control and do not undermine the rules established here. It would appear advisable to hand over relevant scenarios to a central scenario catalogue at a neutral body in order to develop appropriate universal standards, including any acceptance tests.</p>

項次	準則	準則(英文)
19	<p>在緊急情況下，車輛必須在沒有人類協助下自主進入安全狀態。</p> <p>協調與平衡，尤其是符合定義的安全條件或切換例行工作，是可行的。</p>	<p>In emergency situations, the vehicle must autonomously, i.e. without human assistance, enter into a “safe condition”.</p> <p>Harmonization, especially of the definition of a safe condition or of the handover routines, is desirable.</p>
20	<p>適當使用自動及聯網化系統被視其為數位教育的一環，相關人員應接受正確且適當的訓練和測試。</p> <p>在駕駛教學和測試期間，應以適當的方式教授自動駕駛系統的正確處理。</p>	<p>The proper use of automated systems should form part of people’s general digital education.</p> <p>The proper handling of automated driving systems should be taught in an appropriate manner during driving tuition and tested.</p>

20 項準則可分為六大核心重點：1.當自動駕駛系統肇事機會小於人為駕駛時，自動駕駛及聯網化駕駛行為即符合道德規範；2.如果無法避免危險，自駕系統首要任務是保護人命，必要時可接受犧牲動物或財物；3.嚴格禁止自駕系統以個人特徵，如年紀、性別、身心狀況，做出差別待遇；4.任何情況下必須明確界定誰負責駕駛任務，並須紀錄儲存行車情況，以釐清可能賠償責任；5.駕駛人有權決定車輛資料是否可再轉供他人利用；6.公眾有獲知足夠新技術及其應用差異化知識之權利。

綜合上述六大核心重點，德國自駕車倫理要求：1.人的生命應該始終優先於財產或動物；2.要求自駕系統不能權衡受害者的條件，來決定誰應該受害，意即不贊成以某種演算法對自駕進行「道德程式化」¹⁵²，但卻也認為「減少人命損失」可

¹⁵²在此「道德程式化」意指將道德以程式來寫定，等同將生命之抉擇交給工程師或方程式來決定。



視為合理；3.民眾有權知道新技術的內容，生產者應該儘可能透明化。但這並不是指要企業公布演算法機密，而是要公開蒐集何種道德資料、如何將資料量化，以及完整保存所有自動化相關決策等資料。

另外，德國為最先推動聯合國歐洲經濟委員會(UNECE) L3 低速自動車道維持系統規範的國家之一，該國政府監管駕駛(消費者)對 L3 低速 ALKS 的使用，允許在時速不超過 60 公里情況下，啟動 ALKS，讓車輛在無駕駛干預下在固定的車道內直行，可適用於高速公路塞車之情境。目前該國進一步提出高速 ALKS 法案，最高時速提高至 130 km/hr，並可在高速公路上變換車道，德國內閣於 2021 年 2 月批准了該法律草案，並已提交至聯邦議院和聯邦參議院做進一步審議。此外，2021 年 5 月，德國通過《自動駕駛法》，2022 年允許自駕車開上公共道路¹⁵³。

第三項 日本自駕車政策

日本為傳統汽車生產製造大國，擁有許多世界知名且具競爭力的汽車企業，該國也是聯合國歐洲經濟委員會 (United Nations Economic Commission For Europe, UNECE) 所屬之「世界車輛法規調和論壇」(World Forum for Harmonization of Vehicle Regulations, WP. 29)¹⁵⁴ 成員國之一，故日本在自駕車發展與監管之策略方面上為領先國家之列。該國首相安倍晉三任內內閣轄下之 IT 總合戰略總部 (IT Strategic Headquarters) 於 2013 年 6 月 14 日公布《世界最先進 IT 國家創造宣言 (Declaration to be the World's Most Advanced IT Nation)》¹⁵⁵，《跨部會戰略性創新推動方案》。

¹⁵³ 馬飛 (2021/10/09)，《淺析德國自動駕駛法對中國自動駕駛產業的啟示》，超凡研究院，載於：
<https://www.chofn.com/academy/61615f97b95d001d583004/%E6%B5%85%E6%9E%90%E5%BE%B7%E5%9B%BD%E8%87%AA%E5%8A%A8%E9%A9%BE%E9%A9%B6%E6%B3%95%E5%AF%B9%E4%B8%AD%E5%9B%BD%E8%87%AA%E5%8A%A8%E9%A9%BE%E9%A9%B6%E4%BA%A7%E4%B8%9A%E7%9A%84%E5%90%AF%E7%A4%BA> (最後瀏覽日：2022/3/5)

¹⁵⁴ UNECE. *World Forum for Harmonization of Vehicle Regulations (WP.29)*.
<https://unece.org/transport/vehicle-regulations/world-forum-harmonization-vehicle-regulations-wp29>

¹⁵⁵ IT Strategic Headquarters, Prime Minister of Japan and His Cabinet. *Major Steps and Decisions Taken*. https://japan.kantei.go.jp/policy/it/index_e.html

2014 年內 IT 綜合戰略總部發布「官民 ITS 構想・藍圖」以來¹⁵⁶，政策方針每年滾動更新¹⁵⁷，各府廳省依此架構針對自動駕駛相關各自觀點積極進行研議。2014 年開始推動自動駕駛系統戰略創新促進項目 SIP-adus 計畫(如圖 30)。《跨部會戰略性創新推動方案》計畫英文全名為 Cross-ministerial Strategic Innovation Promotion Program，英文簡稱 SIP¹⁵⁸，為集合日本各大車廠投入發展自駕車重要技術。SIP-adus 計畫第 1 期(2014~2018) 主要聚焦「動態地圖」、「資訊安全」、「人機介面」、「減少用路人事故」及「下世代城市交通」等 5 個重要議題進行大規模研究與實驗；SIP-adus 計畫第二期(2018~2020) 則專注於「區域操作測試(Field Operational Test, FOT)」、「科技發展」、「公眾接受」與「國際合作」等 4 大面向¹⁵⁹。



圖 30. 日本 SIP-adus 計畫。資料來源：車輛中心¹⁶⁰

2017 年 6 月日本第十次《未來投資戰略 2017》會議中，以針對 Society 5.0 戰

¹⁵⁶ ARTC (2020), 《全球自駕車產業發展現況與未來趨勢》，頁 5，2020 車輛研測專刊，載於：https://www.artc.org.tw/upfiles/ADUupload/knowledge/tw_knowledge_659798677.pdf (最後瀏覽日：2021 年 12 月 10 日)

¹⁵⁷ 垣見 直彦 (2017/12/24), 《日本的自動駕駛技術推進政策》，(日本)經濟產業省，載於：https://jcpage.jp/f17/05_automobile/05_automobile_08-01_meti_kakimi_cn.pdf?1655078400025 (最後瀏覽日：2021 年 8 月 15 日)

¹⁵⁸ SIP-adus 英文網站，<https://en.sip-adus.go.jp/>

¹⁵⁹ SIP-adus. *About SIP 2nd Phase*. <https://en.sip-adus.go.jp/sip/>

¹⁶⁰ ARTC (2020)，前揭註 156，頁 5。

略領域移動革命的實現，提出 L4 以上自駕汽車、自動駕駛卡車、開放資料與 3D 自動駕駛地圖及對應之地域限定型監理沙盒規劃指導原則¹⁶¹，計畫透過無人自動駕駛移動服務等無人載具，提高物流效率與實現高度化移動服務，並減少交通事故和解決人力不足等問題。日本為推動發展 Level 3 等級自駕車，在 2019 年修訂了《道路交通安全法》¹⁶²及《道路運輸車輛法》¹⁶³，實現在高速公路和人口稀少地區自動駕駛，說明自動駕駛啟動時，可以使用智慧或傳統手機，但駕駛仍有責任應隨時注意行車狀況，以即時介入應付緊急情況，促使 Level 3 量產車在日本上路成為可能，於 2020 年實施。此外，日本於 2019 年 APEC 第 30 屆汽車對話會議時，亦有提出要求¹⁶⁴。2020 年 4 月，日本《道路運輸車輛法》和《道路交通安全法》修正案生效，正式允許駕駛在公共道路上使用 L3 自駕車。2021 年 3 月，日本本田(Honda)汽車推出 Legend Hybrid EX，為首款供消費者使用的量產 L3 自駕車車款。

第四項 英國自駕車政策

英國在自駕車法規進展，首見於 2013 年該國《國家基礎建設計畫 (National Infrastructure Plan)》，開始檢視無人駕駛車輛(driverless cars)於英國公路之法規架構¹⁶⁵，該些計畫並載於《2013 年秋季聲明 (Autumn Statement 2013)》¹⁶⁶，預期建立 1 千萬英鎊獎勵參與測試的城市。英國交通部(The Department for Transport, 簡稱 DfT)

¹⁶¹ 何介人 (2019/12/04)，《借鏡日本沙盒 發展新科技》，創科技。載於：
<https://itritech.itri.org.tw/blog/japansandbox-newtech/>

¹⁶² 日經中文網 (2019/03/08)，《日本敲定自動駕駛車上路規則 解禁開車看手機》，載於：
<https://zh.cn.nikkei.com/politicaeconomy/economic-policy/34638-2019-03-08-15-14-19.html>

¹⁶³ 日經中文網 (2019/05/17)，《日本 2020 年或實現高速公路自動駕駛》，載於：
<https://zh.cn.nikkei.com/industry/icar/35626-2019-05-17-13-11-51.html>

¹⁶⁴ 陳郁淇，沈聰明，劉信宏 (2019/7/16)，《2019 年第 1 次 APEC 汽車對話(AD30)會議》，經濟部國際貿易局，頁 3，載於：
<https://report.nat.gov.tw/ReportFront/PageSystem/reportFileDownload/C10801600/001>

¹⁶⁵ DfT (2015/02). *The Pathway to Driverless Cars: Summary report and action plan*, page 14.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/401562/pathway-driverless-cars-summary.pdf

¹⁶⁶ HM Treasury (2013/12). *Autumn Statement 2013*. UK GOV. ISBN 978-0-10-187472-4.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/263942/35062_Autumn_Statement_2013.pdf

也指出自駕車於英國公共道路上試驗將從《2013 年秋季聲明 (Autumn Statement 2013)》開始著手推動進行，在有關規定就已經有提到利益相關者之資安(Cyber Security)¹⁶⁷及隱私(Privacy)¹⁶⁸問題。

2015 年 2 月英國 DfT 發表《通往無人駕駛汽車的途徑：自駕車科技法規的詳細檢視 (The pathway to driverless cars: a detailed review of regulations for automated vehicle technologies)》¹⁶⁹，該報告檢視在英國道路上進行自動車輛技術測試、保持道路安全需要解決的問題，涵蓋了在有能力控制汽車的合格人員在場的情況下試用車輛的最適和最安全的方法，還進一步展望了全自動駕駛汽車的潛在用途。

Dft 在 2017 年 3 月也對英國國會 (Parliament of the United Kingdom)發表一份報告《聯網車與自駕車之未來 (Connected and Autonomous Vehicles: The future?) 》¹⁷⁰。報告中多次就有提到隱私(Privacy)問題，在建議 28 項(Recommendation 28)中英國 ICO(Information Commissioner's Office)就提出任何由自駕車蒐集資料必須遵循資料保護法(It is essential that any data gathered from CAV (Connected and autonomous vehicles, CAV) are used in accordance with data protection law); 在建議 29 項也提到目前(2017 年)所謂個人資料在 CAV 應用環境下並不是被定義的很清楚，未來在 CAV 的安全性及效率考量同時，如何保持個人及社群的隱私是相當的重要(However, the meaning of personal data is unclear in the context of CAV. It will be important to achieve privacy for individuals and communities, while using data to achieve efficiency and safety of CAV operations.)。Dft 於今年(2022 年)1 月發布《自駕科技於公眾領域測試 (Trialling automated vehicle technologies in public)》¹⁷¹及同年四月公

¹⁶⁷ DfT (2015)，前揭 165，頁 28-29。

¹⁶⁸ DfT (2015)，前揭 165，頁 38。

¹⁶⁹ DfT (2015/02). *The Pathway to Driverless Cars: a detailed review of regulations for automated vehicle technologies*.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/401565/pathway-driverless-cars-main.pdf

¹⁷⁰ HOUSE OF LORDS (2017). *Connected and Autonomous Vehicles: The future?*
<https://publications.parliament.uk/pa/ld201617/ldselect/ldsctech/115/115.pdf>

¹⁷¹ DfT (2022). *Trialling automated vehicle technologies in public*.

布《大不列顛島可使用自駕車明細 (Self-driving vehicles listed for use in Great Britain)》¹⁷²。另依資策會科法所網站資料¹⁷³，英格蘭與威爾斯法律委員會(The Law Commission of England and Wales)與蘇格蘭法律委員會(The Scottish Law Commission)於 2022 年 1 月 26 日聯合提出「自駕車修法建議報告(Automated Vehicles: joint report)」¹⁷⁴，提出 75 項法律修正建議，其中就支持自動駕駛汽車安全全部署的新法律框架提出了建議，該建議已提交英格蘭及蘇格蘭議會決議是否採納並修法。在該報告 1.15 就有關 data protection and privacy;在資料保障(Safeguarding data)(5.81)，要針對資料如何被記錄、儲存、讀取及保護要有詳細的規範。2022 年 4 月 25 日英國交通部更新自動駕駛汽車安全使用規則諮詢結果¹⁷⁵，一些受訪者表示，根據 2018 年自動和電動汽車法案¹⁷⁶，ALKS 不應被視為自動駕駛汽車，因為在安全性和能力方面存在一些不足，另外應該教育所謂自駕車的定義，並區分先進輔助駕駛系統與自動駕駛等。

第五項 新加坡自駕車政策

在借鏡各國的自駕車政策，與台灣同為華人世界的新加坡值得特別我國重視。新加坡人口密集且集中於都市，參諸維基百科(WIKI)2021 年資料顯示該國擁有逾 560 萬人口常住人口，不到 725 平方公里，面積可約為紐約市面積的三分之二，為世界上人口第三密集的國家。新加坡作為典型的都市型國家，被稱為「花園城市」，其自駕車發展策略有幾個重要任務為對抗高齡社會、解決人口老化(老化)、勞力缺

<https://www.gov.uk/government/publications/trialling-automated-vehicle-technologies-in-public>

¹⁷² DfT (2022). *Self-driving vehicles listed for use in Great Britain*.

<https://www.gov.uk/guidance/self-driving-vehicles-listed-for-use-in-great-britain>

¹⁷³ 楊至善 (2022/03)，《英國法律委員會提出 75 項自駕車修法具體建議，突破框架建構新體系》，資訊工業策進會科技法律研究所，載於：<https://stli.iii.org.tw/article-detail.aspx?no=66&tp=1&d=8798> (最後瀏覽日：2022/08/01)

¹⁷⁴ Scottish Law Commission, *Automated Vehicles: Summary of joint report*. <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/01/AV-Summary-25-01-22-2.pdf>

¹⁷⁵ UK Department for Transport (Updated 25 April 2022). *Rules on the safe use of automated vehicles: summary of responses and government response*. <https://www.gov.uk/government/consultations/safe-use-rules-for-automated-vehicles-av/outcome/rules-on-the-safe-use-of-automated-vehicles-summary-of-responses-and-government-response>

¹⁷⁶ UK Legislation. *Automated and Electric Vehicles Act 2018*. <https://www.legislation.gov.uk/ukpga/2018/18/contents/enacted>

乏(缺工)、土地發展侷限等結構性問題，故因此技術往高度自駕車、無人駕駛發展，並為城市帶來環保、安全的交通運輸環境。新加坡城市規劃是亞洲典範，並已有紮實的資通訊環境建設、優良的理工大學、良好的交通規劃、智慧城市等基礎建設，都是自駕車與無人車駕駛發展要求的生態環境；另一方面人口密集、華人文化(如夜市、路邊快炒店等歐美較無類似的場景)、氣候潮濕多雨、交通工具多樣也是與台灣類似，新加坡自駕車政策與發展相當值得我國參考，且台灣有更強大的硬體製造基礎及更完整的工程人才，應該有優於新加坡發展的潛力。

在新加坡政府積極推動下，該國是全球最快實現高度自動駕駛生態系統的國家之一，安侯建業會計師聯合事務所(KPMG)2019年的「自駕車準備度指數」報告指出，新加坡排名全球第二，和亞洲第一¹⁷⁷，KPMG 2020年調查報告，新加坡擠下了前兩年皆為第一名的荷蘭，這反應新加坡為成為全球最積極打造智慧城市的國家，自2019年積極為推動自駕車採取許多措施，如公布自駕車的標準，及大幅增加電動車充電站等¹⁷⁸。

新加坡政府對於自動駕駛的發展，開始於2014年成立專門委員會管理自動駕駛車，而新加坡陸路交通管理局¹⁷⁹(Land Transport Authority, LTA)近年來也積極的和多家發展無人駕駛技術的廠商密切合作。2016年8月世界首次讓無人駕駛計程車，代號nuTonomy，在新加坡正式開始營運載客，乘客可以用智慧手機免費預約體驗。新加坡陸路交通管理局針對無人駕駛車輛的試驗設定時間和空間限制以及相關道路交通條例進行修訂，允許無人駕駛車在規定區域內測試和上路。

新加坡在2014年開始新坡陸路交通管理局(LTA)、新加坡科技研究局(Agency

¹⁷⁷ KPMG International (2019), 《2019年自動駕駛汽車準備度報告》。載於：
<https://home.kpmg/tw/zh/home/insights/2019/02/2019-autonomous-vehicles-readiness-index.html>

¹⁷⁸ KPMG International (2020), 《2020年自動駕駛汽車準備度報告 (2020 Autonomous Vehicles Readiness Index) 》，Publication date: July 2020. 載於：
<https://home.kpmg/tw/zh/home/media/press-releases/2020/07/autonomous-vehicles-readiness-index-2020.html?>

¹⁷⁹ Land Transport Authority. <https://www.lta.gov.sg/content/ltagov/en.html>

for Science, Technology and Research, ASTAR)與新加坡裕廊集團(JTC Corporation)合作「新加坡自駕車倡議」(Singapore Autonomous Vehicle Initiative, SAVI)¹⁸⁰，簽署了 5 年期的備忘錄以發展自駕車，包含研究對自駕車的規範管理及技術研發，並設立試驗設計中心。

2016 年 LTA、JTC 與新加坡南洋理工大學(Nanyang Technology university, NTU)於潔淨科技園(Clean Tech park)合作成立「駕駛汽車試驗和研究卓越中心」(Centre of Excellence for Testing & Research of Autonomous Vehicles NTU, CETRAN)，發展並制定自駕車標準與法規，所有公司汽車都必須先接受其試驗及認證，方能正式駕駛於公共道路。CETRAN 智慧車測試中心，是東南亞地區第一個自動駕駛測試中心，它的設計如圖 31 看起來就像一個真正的城市道路網路，包括交通街口、公共汽車站和斑馬線;另可模擬熱帶降雨和洪水情況，以反應新加坡及周邊地區的氣候。

¹⁸⁰ Alan Quek (2019), Singapore Autonomous Vehicle Initiative (SAVI), ITS World Congress, 21 - 25 October 2019. [https://www.itu.int/en/ITU-T/extcoop/cits/Documents/Workshop-201707-Singapore/010%20-%20Alan-Quek-Singapore%20Autonomous%20Vehicle%20Initiative%20\(SAVI\).pdf](https://www.itu.int/en/ITU-T/extcoop/cits/Documents/Workshop-201707-Singapore/010%20-%20Alan-Quek-Singapore%20Autonomous%20Vehicle%20Initiative%20(SAVI).pdf)



- | | | |
|--------------------------|--|-----------------------|
| ① Bus stop with bay | ⑥ Signalled intersection | ⑨ Urban canyon |
| ② Rain simulator | ⑦ V2X communication | ⑩ Pedestrian crossing |
| ③ Slope | ⑧ Charging station for vehicle and AutOnomous Vehicle Monitoring and EValuation System (OLIVE) | ⑪ Crank course |
| ④ Signalled intersection | | ⑫ Bus stop |
| ⑤ S-course | | ⑬ Flash flood area |

圖 31. 東南亞地區第一個自動駕駛測試中心 CETRAN。資料來源：CETRAN

新加坡於 2022 年修訂《公路交通法》(Road Traffic (Amendment) Bill)並持續依照現況修正，今年(2022)最新版本業已於 6 月公告¹⁸¹，主要強化道路安全等規定。該《公路交通法》從 2002 年制定後持續修訂，並自 2017 年增訂章節規範自駕車的試驗和使用，針對無人車測試有關之條文透過法規的架構修正促進自駕車科技發展 (“More Responsive Regulatory Framework to Support Autonomous Vehicle Trials”)，並在能確保道路使用者的安全條件下，增加自駕車能於公眾道路測試的法規彈性 (“The proposed amendments to the RTA will give LTA the flexibility to create and amend rules to facilitate AV trials on public roads, as and when needed, while ensuring the safety

¹⁸¹ Parliament, Road Traffic (Amendment) Bill (2022).
<https://www.parliament.gov.zm/sites/default/files/documents/bills/Road%20Traffice%20%28Amendment%29%20Bill%2C%202022.pdf>

of road users”)¹⁸²，該修正案於同年 3 月總統簽署公告，並新增針對無人車測試與使用(“Trials and use of autonomous motor vehicles, etc.”)之條文 6C，6D 及 6E¹⁸³。2017 年 11 月 22 日在如圖 32 緯壹(One-North)園區開始進行自駕車道路試驗，建立全球首個自駕車試驗場，園區內將打造駕駛之事前安全測試、試驗區域規劃、路況障礙模擬、試驗監測，並建立充電站、信號台等相關支援性基礎設施。

新加坡於 2018 年開始實際道路測試，除授予交通部訂定道路測試的相關規定，包含：保險、押金、測試公告、測試許可、測試期間、測試天氣狀態、測試中使用之技術及裝置、車輛配備、資料紀錄及移交、終止測試要件、上訴權利、費用及政府保密義務；另豁免測試申請者及測試相關人員及車輛排除《公路交通法》及其衍伸之相關規定適用，最後對干擾測試者訂出處罰機制。

¹⁸² Singapore LTA (2017). *Factsheet: Second Reading of Road Traffic (Amendment) Bill*. <https://www.lta.gov.sg/content/ltagov/en/newsroom/2017/2/2/factsheet-second-reading-of-road-traffic-amendment-bill.html>

¹⁸³ Singapore Statutes Online. *ROAD TRAFFIC (AMENDMENT) ACT 2017*. <https://sso.agc.gov.sg/Acts-Supp/10-2017/Published/20170321?DocDate=20170321#pr6->



圖 32. 新加坡的緯壹(One-North)園區的自駕車服務測試計畫。資料來源：iThome¹⁸⁴

2018 年 11 月 12 日新加坡運輸營運商 ComfordelGro 宣布聯合法國新創造製造業者 EasyMile、新加坡汽車經銷商 Inchcape Singapor 展開為期一年的自主試驗計畫，於新加坡國立大學(National University of Singapore, NUS)並透過模擬真實道路境的交通條件¹⁸⁵。

2019 年 3 月 5 日新加坡南理工大學(NTIJ)與瑞典廠商 VOLVO 合作研發全球款 12 公尺長的電巴士，該公車可以供 80 名乘客乘坐，配備了光學測器和光達、360 度鏡頭衛星導航系統，用多個資料庫提供位置訊息，於當年度(2019)可準確到 1 公分定位，並在校園裡進行試驗，在佔地 2 公頃的試驗場內含一條配備數個急彎的道、紅燈、一個斜坡和一個公車站牌等並設有雨水模擬器和洪水區，以模擬真實

¹⁸⁴ 蘇文彬 (2017/02/23)，《新加坡以無人車結合 IoT 改善當地交通，期許成為第一個自駕車商用化的國家》，iThome，載於：<https://www.ithome.com.tw/news/112286> (最後瀏覽日：2021/08/18)。

¹⁸⁵ 陳明陽 (2018/11/17)，《新加坡全電動自駕巴士載客明年首度上路測試》，DigiTimes。

的駕駛情況，試驗相關設備在不同天氣條件下之性能。

新加坡自動駕駛汽車試驗和研究卓越中心(Centre of Excellence for Testing and Research of Autonomous Vehicles, CETRAN)於 2020 年 1 月 21 日提出「評估自動駕駛汽車的情境方案」¹⁸⁶ (Scenario Categories for the Assessment of Automated Vehicles) 報告說明，為了對自動駕駛汽車落地實施進行安全評估及試驗，藉之大量真實資料蒐集及軟硬技術的反饋結果，針對不同環境驗證自動駕駛運行的安全性，包括交通參與者的動作、道路和基礎設施的典型以及天氣與照明條件等。

在本文作者 2019 年在新加坡參加研討會，並參訪相關研發機關後，綜合上述文獻及自身體驗整理該國自駕車發展：新加坡政府對於高度自駕車或無人車態度較為積極且開放，並由政府單位身先士卒領先規劃並推動，有清楚的發展藍圖、明確的發展策略、具體落實之規劃，並且積極檢討回饋；在法規上，2017 年法規修正預留彈性用以降低無人車發展測試與現行法規的衝擊，並能逐年檢討修正；另一方面除了與既有的資通訊廠商合作外，也與多間新創無人車公司合作，建構了完整的自駕車發展生態體系。

第六項 中國大陸自駕車政策

目前中國針對自駕車規範僅針對自駕車測試進行監管，並以一線城市的自駕測試相關法規為首，最早由北京市發布自駕政策，上海市亦不甘落後，搶先發出境內首張自駕車測試牌照。以北京為例，2017 年發布《北京市加快推進自動駕駛車輛道路測試有關工作的指導意見(試行)》和《北京市自動駕駛車輛道路測試管理實施細則(試行)》並於 2018 年 4 月正式試行¹⁸⁷，該意見包含：1.自動駕駛定義；2.責任

¹⁸⁶ CETRAN (2020), Scenario Categories for the Assessment of Automated Vehicles. http://cetransg/wp-content/uploads/2020/01/REP200121_Scenario_Categories_v1.7.pdf

¹⁸⁷ 北京市經濟和資訊化局 (2018)，關於印發《北京市關於加快推進自動駕駛車輛道路測試有關工作的指導意見(試行)》和《北京市自動駕駛車輛道路測試管理實施細則(試行)》的通知。載於：http://jxj.beijing.gov.cn/zwgk/zcwj/bjszc/201911/t20191113_511307.html (最後瀏覽日：2022 年 4 月 11 日)。

主體;3.測試要求;4.測試管理及事故責任認定等，測試要求乙節中對於測試車輛、測試駕駛員、測試主體等有要求及責任規定¹⁸⁸。

2020 年北京進一步規範《自動駕駛車輛道路測試能力評估內容與方法》¹⁸⁹，主要有 1.測試操作要求，含測試車輛基本要求、測試記錄要求、測試場景布置要求、測試設備要求及數據採集精度；2.能力評估內容與方法，包含一般要求、通用技術測試、專項技術測試及一致性測試。此份規範共 151 頁，有非常詳細且清楚的圖示檢驗自駕車輛的能力，值得台灣自駕車檢驗規範參考。

2021 年 3 月，深圳市政府率先提出《深圳經濟特區智慧網聯汽車管理條例》草案，向社會公開徵求意見，並已於今年(2022)7 月頒布全文共計 9 章，包含第二章道路測試和示範應用;第三章准入和登記;第四章使用管理;第五章車路協同基礎設施;第六章網路安全和資料保護;第七章交通違法和事故處理;第八章法律責任等，共計 64 條並自同年 8 月 1 日正式實施¹⁹⁰，該條例涵蓋「有條件自動駕駛」、「高度自動駕駛」及「完全自動駕駛」。透過該條例深圳已經允許智慧網聯汽車將在深圳劃定區域路段行駛，該條例之特點為無人駕駛之完全自動駕駛已可合法上路，根據條例，完全自動駕駛的汽車可以不具有人工駕駛模式和相應裝置，可以不配備駕駛人，在深圳交通管理部門劃定的區域、路段行駛，市民可在深圳免費乘坐這批自動駕駛車輛。該條例第 48 條明文禁止利用智能聯網車輛從事(一)非法收集、處理、利用個人資訊;(二)採集與本車輛行駛和交通安全無關的資訊;(三)非法採集涉及國家安全的資訊。

¹⁸⁸ 北京市 (2018)，北京市關於加快推進自動駕駛車輛道路測試有關工作的指導意見(試行)，載於：<http://jxj.beijing.gov.cn/zwgk/zcwj/bjszc/201911/P020191113697901034358.pdf> (最後瀏覽日：2022 年 4 月 11 日)

¹⁸⁹ 中關村智通智慧交通產業聯盟 (2020/11/02)，《自動駕駛車輛道路測試能力評估內容與方法》，載於：<http://www.mzone.site/Uploads/Download/2020-12-18/5fdc0b7940984.pdf>

¹⁹⁰ 新浪財經 (2022/07/11)，《深圳經濟特區智慧網聯汽車管理條例(全文)》，載於：<https://finance.sina.com.cn/china/dfjj/2022-07-11/doc-imizmscv0970497.shtml> (最後瀏覽日：2022 年 7 月 11 日)

在全國性規章部分，2018 年中國政府頒布《智慧聯網汽車道路測試管理辦法》，該辦法並於 2021 年 7 月正式試行¹⁹¹，該辦法由中國工業和信息化部、公安部、交通運輸部聯合發布¹⁹²，主要針對智慧聯網車的道路測試，允許自 2018 年《智慧聯網汽車道路測試管理規範（試行）》後經過一定時間或里程道路測試、安全可靠的智慧自駕車輛展開實際載人載物的應用示範，並將測試示範道路擴展到包括高速公路在內的公路、城市道路和區域。中國各省、市級政府主管部門可依當地情況，辦理智慧聯網汽車道路測試工作，自該辦法 2017 年頒布至 2021 年 8 月有 27 個省頒布管理細則。該試行規範除第一章總則外包含 1. 道路測試與示範應用主體、駕駛人及車輛（第二章）；2. 道路測試申請（第三章）；3. 示範應用申請（第四章）；4. 道路測試與示範應用管理；交通違法與事故處理（第六章）及附則（第七章）。2020 年發布《智能汽車創新發展戰略》；2021 年 4 月發布《道路交通安全法》第三次修正版本¹⁹³。

第七項 聯合國 UN-R157

2020 年 6 月 25 日，聯合國歐洲經濟委員會世界車輛法規協調論壇通過了有 ALKS 的型式統一規定，UN-R157 法規¹⁹⁴。UN-R157 法規是首個針對 SAE L3 級別自動駕駛功能決議的具有約束力的國際法規，現已於 2021 年 1 月 22 日起正式生效，最新版本為 R157e，於 2021 年 5 月 3 日更新。德國聯邦汽車運輸管理局也

¹⁹¹ 工業和資訊化部 公安部 交通運輸部 (2021/7/27)，《工業和資訊化部 公安部 交通運輸部關於印發〈智慧聯網汽車道路測試與示範應用管理規範（試行）〉的通知》，載於：http://big5.www.gov.cn/gate/big5/www.gov.cn/zhengce/zhengceku/2021-08/03/content_5629199.htm (最後瀏覽日：2022 年 4 月 11 日)

¹⁹² 工業和信息化部網站 (2021/08/13)，《〈智慧聯網汽車道路測試與示範應用管理規範（試行）〉解讀》，http://big5.www.gov.cn/gate/big5/www.gov.cn/zhengce/2021-08/03/content_5629202.htm

¹⁹³ 鄭州外資企業服務中心 (2022/06/07)，〈《中華人民共和國道路交通安全法》（2021 年修訂版全文）【附 PDF 版下載】〉，載於：<https://www.waizi.org.cn/doc/111374.html> (最後瀏覽日：2022 年 3 月 10 日)

¹⁹⁴ UNECE (2021/05/03). *UN Regulation No. 157 - Automated Lane Keeping Systems (ALKS)*. <https://unece.org/transport/documents/2021/03/standards/un-regulation-no-157-automated-lane-keeping-systems-alks>

援引「UN-R157」認證，允許採用「Level 3」自駕技術「DRIVE PILOT」的賓士車，在德國上路，駕駛者可在車流量大或交通壅塞的德國公路使用這套自駕系統，但時速必須低於 60 公里。



第八項 台灣自駕車主要政策與實驗條例

一. 台灣現行車輛相關法規

台灣現行車輛法規可分為正式法規及實驗條例¹⁹⁵。正式法規為針對車子管理依公路法第六十三條第五項規定訂定之《車輛型式安全審驗管理辦法》，及針對人員管理的《道路交通管理處罰條例》《車輛行車事故鑑定及覆議作業辦法》。其中《車輛行車事故鑑定及覆議作業辦法》並規範相關人員可能的可能如民法第 191-2 條駕駛人在使用中加損害於他人者之責任及刑事刑法第 185-4 條，駕駛人肇事逃逸之刑責之責任。

我國參酌各國的自動駕駛車輛道路測試之規定¹⁹⁶，有關無人載具之規範為 2018 年 12 月 19 日開始實施的《台灣無人載具實驗條例》，該條例內容將詳敘於後。對於自駕巴士之管理，亦有相關法制之倡議¹⁹⁷。

二. 台灣自駕車主要政策

根據 KPMG 全球總部 2020 年發布之《2020 年自動駕駛汽車準備度報告》研究調查指出¹⁹⁸：“自駕車發展與政策、法規、基礎設施、科技、消費者接受度有關，台灣首次參與名列 13，超越德國、澳洲、法國等先進國家”。該報告透過前述四項

¹⁹⁵ 黃兆儀 (2020/02/26)，《淺析自動駕駛發展現況》，立法院議題研析，載於：<https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=6590&pid=191993>

¹⁹⁶ 張開國、葉祖宏、賴靜慧、洪憲忠 (2019/07)，《自動駕駛車輛道路測試規定之研議》，交通部運輸研究所，載於：<https://grb-topics.stpi.narl.org.tw/file/download?fileId=4b1141c270f6ca7e017115f523b20d32>

¹⁹⁷ 資訊工業策進會科技法律研究所 (2021/05/25)，《簡析自動駕駛巴士應用於我國上路營運所需面臨之法制預備方向》，載於：<https://stli.iii.org.tw/article-detail.aspx?tp=1&i=180&d=8675&no=64> (最後瀏覽日：2021 年 12 月 18 日)

¹⁹⁸ KPMG International (2020)，前揭註 178。

「政策」、「法規」、「基礎設施」及「科技指標」，綜觀本文前述包含美、歐、日、中國等各國對自駕車的觀察，我國在科技、法規、場域與應用環境具備發展潛力。我國身為資通訊技術(Information and Communications Technology, ICT)之大國，有深厚的技術之基礎，並透過 2018 年通過之《無人載具科技實驗條例》，建構自駕車「政策」、「法規」、「基礎設施」等產業生態體系，《2020 年自動駕駛汽車準備度報告》中指出：“政府積極以「實驗沙盒」精神評估和研擬適當的法令框架、民眾對自駕車發展的認知程度與科技創新的包容力更令人讚賞”¹⁹⁹。可見公務機關與非公務機關對自駕車發展之共識與創新精神，及「實驗沙盒」的調性法規架構是我國重要發展自駕車的國際競爭力。而我國公務機關除法規之制定外，中央政府以科技會報辦公室為首，輔以地方政府提供基礎環境與場域設施，如下圖 33 由經濟部、交通部、金管會、科技部、國發會和內政部等跨部門間合作分工規劃、建置基礎措施，結合中央政府及地方政府兩邊之力量，支援國內研究法人和業者發展與掌握自動駕駛系統或功能的關鍵性能量。

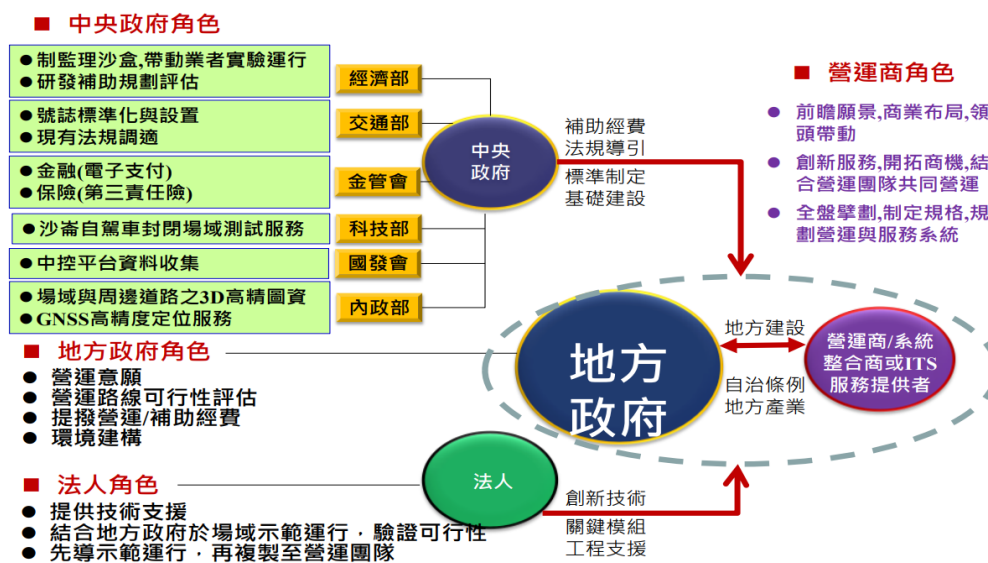


圖 33. 台灣自駕車政策之中央與地方跨部會配套規劃。資料來源：經濟部(2019/5)

¹⁹⁹ KPMG (2020),《KPMG 發表《2020 自動駕駛汽車準備度》台灣首次參與名列 13, 超越德、澳、法》, 載於：<https://home.kpmg/tw/zh/home/media/press-releases/2020/07/autonomous-vehicles-readiness-index-2020.html> (最後瀏覽日：2022 年 2 月 12 日)

三. 台灣無人載具實驗條例

自駕車雖是台灣的發展重點產業，目前台灣尚未針對自駕車的專屬法律規範，然為推動台灣與世界各國無人載具科技發展齊頭並進，我國經濟部參考金融科技發展與創新實驗條例之監理沙盒精神^{200,201}制定《無人載具科技創新實驗條例》。金融監理沙盒（Financial Regulatory Sandbox）概念於自英國，構想源自如同讓未成年之孩童在一個沙盒中盡情揮灑創意與創新，其實質內涵提供投入業者及新創企業在一定期間內，依規定提出申請並取得執照或認證，於特定規範下排除部分現行法規之限制，以降低新創業者或創新技術觸犯現行法律之疑慮並降低成本。《無人載具科技創新實驗條例》比照前述監理沙盒之精神，賦予無人載具之研發產學研各界於特定範圍及條件下進行載具之科技、服務及營運模式之創新實驗時，透過該條例暫行排除現行相關法律監理之適用，藉此科技沙盒空間鼓勵各界投入研發，促進產業技術及創新服務發展。

《無人載具科技創新實驗條例》於 2018 年 11 月 30 日業經我國立法院三讀通過，並於同年 12 月 19 日公告實施，該條例上路後容許在特定條件下，排除現行相關法律限制，運用地方政府場域以彈性空間鼓勵各界投入無人載具科技研發與創新應用，帶動我國無人載具產業發展。該條例主管機關由經濟部負責，從產業面角度切入，鼓勵台灣產學研各界發展無人載具的創新科技和相關應用。《無人載具科技創新實驗條例》後續並有兩個《無人載具科技創新實驗管理辦法及無人載具科技創新實驗審查會議運作辦法》及《無人載具科技創新實驗計畫牌照核發辦法》子法於 2019 年 6 月 1 日公告施行。

²⁰⁰ 金管會金融科技發展與創新中心 (2021/06)，《金融科技創新實驗簡介(監理沙盒)》，載於：
<https://www.fsc.gov.tw/websitedowndoc?file=chfsc/202107061711340.pdf&filedisplay=%E7%9B%A3%E7%90%86%E6%B2%99%E7%9B%92%E6%87%B6%E4%BA%BA%E5%8C%85.pdf> (最後瀏覽日：2022 年 3 月 11 日)

²⁰¹ WIKIPEDIA，《金融監理沙盒》，載於：<https://zh.m.wikipedia.org/zh-tw/%E9%87%91%E8%9E%8D%E7%9B%A3%E7%90%86%E6%B2%99%E7%9B%92> (最後瀏覽日：2022 年 3 月 15 日)

如前關於創新沙盒之所述，廠商或新創團隊可參諸《無人載具科技創新實驗條例》讓載具於特定場域試驗，以沙盒之彈性空間鼓勵各界投入無人載具科技研發與創新應用。《無人載具科技創新實驗條例》中有三項重要定義，分別為無人載具、無人載具科技和創新實驗。依該條例之說明，「無人載具」指“車輛、航空器、船舶或其結合之無人駕駛交通運輸工具，透過遠端控制或自動操作而運行，且具備以下技術：感測技術、定位技術、監控技術、決策及控制技術”；「無人載具科技」是指“無人載具或與其結合應用之科技”；「創新實驗」是指“以創新應用為目的之無人載具科技實驗”。

我國《無人載具科技創新實驗條例》共有 7 章 24 條，該條例參諸《無人載具科技創新實驗條例草案總說明》²⁰²之說明，制定過程主要參考美國加州、新加坡、日本、丹麥等國針對無人載具建立之規範，其規範主要是包含無人載具定義、申請及審查程序、實驗場域的管理通報機制、實驗場域安全與事故處理、資訊安全及個人資料保護與創新實驗的契約規範與實驗報告，範圍涵蓋陸海空的無人載具。實驗條例項目列舉如下表 12 所示：

表 12. 無人載具科技創新實驗條例內容綱要。資料來源：立法院法律系統;行政院;本文整理

章節	條文	內容
第一章 總則(§ 1~ § 4)	第 1 條	本條例之立法目的
	第 2 條	主管機關
	第 3 條	名詞定義
	第 4 條	主管機關得由專責單位或委託法人團體協助辦理本條例相關事宜
第二章 申請及審 查程序(§ 5~§ 12)	第 5 條	創新實驗所應檢具之申請書、申請人資料及創新實驗計畫應包含事項
	第 6 條至 第 12 條	創新實驗審查、期間與展延、實驗計畫變更、網站揭露資訊及規費

²⁰² 經濟部，《無人載具科技創新實驗條例草案總說明》，載於：
https://www.moea.gov.tw/Mns/populace/news/wHandNews_File.ashx?file_id=62077 (最後瀏覽日：
 2021 年 1 月 12 日)



章節	條文	內容
第三章 實驗場域 之管理及 安全(§ 13~§18)	第 13 條	創新實驗所需無線通訊應用及管理
	第 14 條	創新實驗監管措施及實地訪查、特定實驗資訊通報、資料蒐集與留存等事項。
	第 15 條 至第 17 條	創新實驗申請人公告與告示相關資訊、實驗場域安全與事故處理、 <u>資訊安全及個人資料保護</u> ，並授權主管機關會同中央交通主管機關訂定公告與告示、事故通報、暫停實驗相關程序等事項之辦法。
	第 18 條	參與實驗契約應遵守之原則及申請人之注意義務
第四章 創新實驗 之辦理、 廢止及報 告(§19~ §21)	第 19 條至 第 21 條	創新實驗相關日期之通知、創新實驗之限期改善及廢止、創新實驗報告。
第五章 法令於實 驗期間之 排除適用 (§22~§ 23)	第 22 條及 第 23 條	創新實驗期間及核准範圍內排除適用法律、法規命令及行政規則之規定。
第六章附 則(§24)	第 24 條	條例施行日期

《無人載具科技創新實驗條例》是期望能替我國無人載具創新實驗所建立的法規環境，目前僅明文確保洗錢防制法、資恐防制法、相關法規命令或行政規則不得被排除適用，同條例第 17 條及經濟部於 2019 年 10 月發行的《無人載具科技創新實驗計畫申請須知》規定：「申請人蒐集、處理或利用個人資料，應遵守個人資料保護法之相關規定」。無人載具之個資規範依照我國《個資法》規定，除了創新實驗如何與實際狀況銜接，備受關注無人載具相關的公示個資之保護亦無特別規定，除了將可能對民眾的隱私權造成侵害，也可能導致新創公司基於我國無人載具

實驗沙盒研發的無人載具技術，於國際間實際應用時產生法遵風險²⁰³。



第九項 自動駕駛測試計畫與場域發展案例

如前自駕車發展狀況所述，全球自駕車針對 SAE 所訂定之高度自駕車已經積極開發，並已有許多 L3 等級之自駕車商品化。部分國家地區的技術測試與發展已達到 SAE 所定義的較高程度自動化的 L4 及 L5 發展。而由本章前述之各國無人載具政策檢視，大多數國家的自駕車發展策略，特別是針對高度自駕車之發展，相當重視場域及實際資料數據之回饋，也因此許多國家及自駕車廠商接連展開自駕車實際試驗、測試場域規劃，有助於建構完善的自動駕駛環境²⁰⁴，透過此些國際的自駕車場域之規劃之瞭解²⁰⁵，有助於台灣無人載具相關法規之制定，本國自駕車法規也可與日俱進，協助台灣高度自駕車之推動發展；對於本文所探討之智慧自駕車技術導入、資料及個資之法規規範，亦有重要的參考價值。如本文第一章之說明，自駕車之發展需要整體的先進的先進技術導入、巨量資料之蒐用及法規之適應性。自駕車因為牽涉到生命安全，其實際操作下蒐用之資料與回饋相當重要，也因此需要相對應的實驗場域。

綜觀各國及國際大廠對自駕車的測試和部署，測試場域與實測資料為不可或缺一環，國際著名封閉型測試場域包括美國「Mcity」 13 公頃、日本「Jtown」 16 公頃、韓國「K-city」 36 公頃、新加坡「Cetran」 1.8 公頃、中國「國家智能網聯汽車（上海）試點示範區」英文稱「ANice City」 500 公頃、中國「國家智慧網聯

²⁰³ 王嫻文(2020/02/12)，《無人載具是目前的趨勢，但真的安全嗎？》，Makerpro，載於：<https://makerpro.cc/2020/02/unmanned-vehicles-are-the-current-trend-but-is-it-really-safe/> (最後瀏覽日：2021/4/13)。

²⁰⁴ 張艾琦 (2021/09/28)，《自駕車法規現況與測試環境發展案例》，科技發展觀測平臺。

²⁰⁵ 陳敬典 (2018)，頁 21-26，前揭註 135。

汽車與智慧交通北京&河北示範區」27 公頃²⁰⁶及瑞典「AstaZero 200」公頃等²⁰⁷，前述測試場域包含各國公務機關的自駕車環境之建構，例如台灣台北信義路、新竹、台中²⁰⁸及台南沙崙園區、美國加州及中國大陸北京及深圳、新加坡也不斷擴大自駕車測試路段，至 2019 年已達上千公里等；在非公務機關方面，特別是汽車大廠，對於自駕車發展場域及所因此而建構的未來世界多有著墨，如：日本的汽車大廠豐田汽車(Toyota)自 2021 年 3 月起在日本富士山腳下動土打造布滿感測器之「織城(Woven City)」，取其 Woven 之含意。「織城」雖不為智慧自駕車專屬打造，但透過棉密的區域網絡，成為發展與測試高度自駕車、人工智慧、機器人、智慧家居等先進技術之智慧城市²⁰⁹；南韓由三星電子、現代與韓國電信共同主導位在華城市(Hwaseong)，以 5G 通訊為基礎之自動駕駛測試城市「K-City」²¹⁰。「K-City」計畫於 2016 年啟動，由南韓的多家民間領導企業及韓國政府共同投入，該基地之建置面積為 2015 年位於美國由密歇根大學打造之 Mcity²¹¹的 2 倍有餘，並領先導入更多的低延遲的 5G 及其配套技術，且因為 K-City 為廠商參與主導，提供真實世界的場景模擬，有更多接近現實環境的裝置設備，K-City 亦接受國外廠商測試之申請；在中國，2021 年小鵬汽車測試了從廣州到北京智慧車聯網試驗，全程採用該公司之智慧導航輔助駕駛(Navigation Guided Pilot, NGP)系統挑戰逾三千公里之遠征。值得注意的是，除新加坡外，其他國家非公務機關與政府機關密切合作的實驗場域，

²⁰⁶ 重磅數據 (2018)，《中國智慧網聯汽車測試示範區發展現狀分析研究報告》，載於：

https://www.ambchina.com/data/upload/image/20220305/%E4%B8%AD%E5%9B%BD%E6%99%BA%E8%83%BD%E7%BD%91%E8%81%94%E6%B1%BD%E8%BD%A6%E6%B5%8B%E8%AF%95%E7%A4%BA%E8%8C%83%E5%8C%BA%E5%8F%91%E5%B1%95%E7%8E%B0%E7%8A%B6%E5%88%86%E6%9E%90_%E9%87%8D%E7%A3%85%E6%95%B0%E6%8D%AE_2018.pdf

²⁰⁷ 黃品誠 (2018/12/06)，〈台灣自駕車測試與驗證環境建構〉，發表於：《自駕車發展與台灣產業之機會與挑戰研討會》，財團法人中技社，台北，載於：
<https://www.ctci.org.tw/8838/research/9483/40327/>

²⁰⁸ 徐志偉 (2020)，前揭註 56，頁 7-11。

²⁰⁹ 中央通訊社 (2021/02/23)，《富士山腳動土造「網城」 日本豐田實驗都市結合自駕與 AI》，<https://www.cna.com.tw/news/ait/202102230306.aspx> (最後瀏覽日：2021 年 11 月 13 日)

²¹⁰ Smart City Korea. *K-City Network*.
<https://smartcity.go.kr/en/%EA%B8%80%EB%A1%9C%EB%B2%8C-%EC%8A%A4%EB%A7%88%ED%8A%B8%EB%8F%84%EC%8B%9C/k-city-network/>

²¹¹ University of Michigan (June 1, 2021). *Mcity's Autonomous Vehicle Testing ABCs*.
https://www.youtube.com/watch?v=LM5_zVC544o

都相當重視智慧城市原有資通訊裝置與自駕車的資訊連接，這也是本文於第一章就提到智慧自駕車應該視為智慧城市的一環，資料透過車聯網與城市中的裝置作一緊密之連結，是故正面而言提高經濟活動與生活之便利，也同時提升交通之安全；反之，透過資料頻繁的蒐用，許多個資與隱私之侵害也正默默的發生。

由上述自駕車測試場域之介紹，顯見各國公務與非公務部門對自駕車發展與測試環境建置之熱衷，整理測試場域與本文相關之重點：1.自駕車測試環境及與之對應經驗與數據資料之重要性；2.公務與非公務部門合作之重要；3.車輛安全的看重；4.各國對新興科技導入車輛之積極，與相對應產生結果之未知不確定性；5.法規適應的探索等。另外有關自駕車測試之等級，以下是參諸科技發展觀測平臺整理目前世界各國允許自駕車最高測試之自動化等級²¹²，由資料中可見除了少數如印度及墨西哥外，各國都有 L4 以上的自駕車最高測試等級規劃，詳細資料如下圖 34 所示。

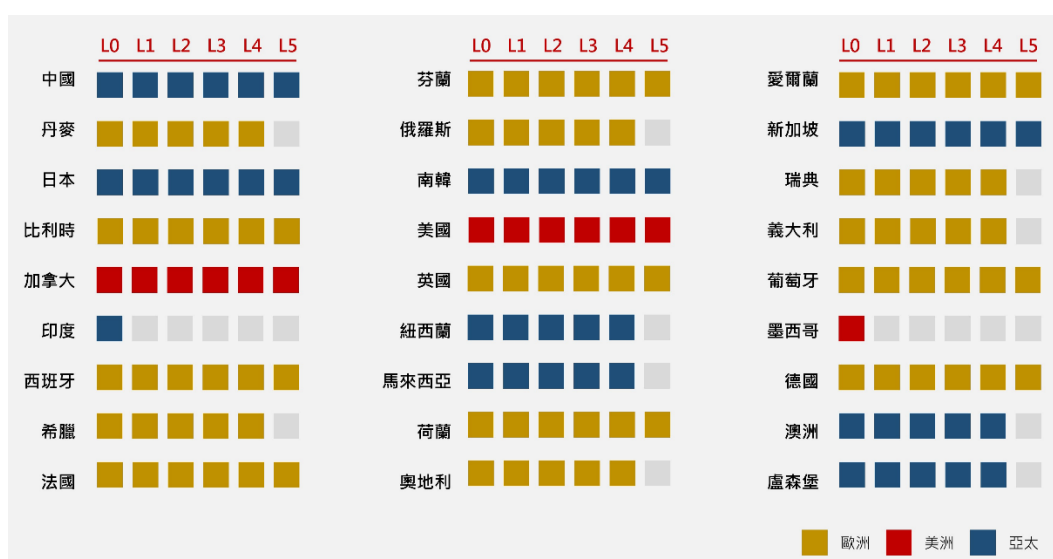


圖 34. 2021 年各國自駕車最高測試等級概況。資料來源：科技發展觀測平臺²¹³

²¹² 有關自駕車等級之定義，經本文查證各國的標準並未一致，例如美國各州並非全部採取 SAE 之自駕車分級。可參考本文圖 35 各國對自駕車等級定義，及本文針對自駕車英文名詞定義之討論。

²¹³ 張艾琦 (2021)，前揭註 204。

第十項 不同國家地區自駕車政策法律比較



一. 主要國家自駕車法規異同

智慧自駕車，特別是高度自駕車，其擁有最先進技術及服務，且直接與生命安全相關，各國的自駕車法規立法的精神皆在於前述如人工智慧、物聯網、邊緣運算等先進技術與新興無人服務運用於自駕車上達成穩定且成熟前，對於如生命安全、隱私及個資等影響明確前的事先測試與資料回饋，期望達成自駕車，特別是高度自駕車，安全上路的最高宗旨，同時降低未來大量自駕車商品化，運用於社會各層面時可能帶來未知的社會負面衝擊，而除了生命安全考量之外，其中最為關鍵的就是本文所要探討的自駕車資料與個資，然因為各國自然環境、道路、法規、資通訊基礎建設、生活習慣等差異而對自駕車之規範有所差異，IMF 2020 年 10 月發表之各國之自駕車政策報告中，比較幾個重要國家的自駕車政策與發展的優劣勢²¹⁴，分析國家包含以色列、美國加州、美國亞利桑納州、新加坡、大英國協及澳洲，該報告指出自駕車政策四大要點：1. 安全性(Safety); 2. 無人駕駛測試及操作(Driverless testing and operation); 3. 乘客運輸(Passenger Transport); 4. 資料分享政策(Data sharing policies)，其中高度自駕車、安全性與資料蒐集與分享正是本文的探討重點。以下稽之本章前述整理資料、《主要國家自駕車規範比較》報告²¹⁵，該報告主要引述前述 IMF 發表之自駕車政策報告²¹⁶，及本文圖 35²¹⁷，就幾個國家地區與本文相關之法規整理分析比較如下：

- 各國皆重視新科技導入與法規彈性：綜前各國政策法規之檢視，各國或地區對於新科技應用於自駕車都保有導入之彈性空間，並逐步修正既有

²¹⁴ IMF (2021). *Autonomous Vehicle (AV) Policy Framework, Part I: Cataloging Selected National and State Policy Efforts to Drive Safe AV Development*.

<https://innovationisrael.org.il/sites/default/files/Autonomous%20Vehicle%20Policy%20Framework-.pdf>

²¹⁵ 張國鈞、蔡玉琬 (2021/04/23)，〈主要國家自駕車規範比較〉，科技發展觀測平臺。

²¹⁶ IMF (2021), *supra* note 203, at 43.

²¹⁷ NTC (2022/02). *The regulatory framework for automated vehicles in Australia*.

<https://www.ntc.gov.au/sites/default/files/assets/files/NTC%20Policy%20Paper%20-%20regulatory%20framework%20for%20automated%20vehicles%20in%20Australia.pdf>



之法規。

- 安全性優先之共識：不論哪個國家地區，對於自駕車之測試都以包含駕駛人、車輛使用人及用路人的**生命安全為首要考量**。
- 重視測試場域與實測資料：不論是封閉式場域，或者已經逐步開放到公有道路之測試，對於測試場域之建置及實際測試資料都視為**最重要的資源**。
- 對技術的中性看待：除美國、澳洲及 IMF 有明確提出對技術的中性態度，尚未看到任一國家自駕車政策有排除或者限制特定技術的使用。
- 對資料的管理的政策尚未明確：目前各國除了歐盟及中國之外，對於自駕車之資料尚未有明確約束管制的規範，甚至美國有開放或交換資料的政策。惟對於隱私部分，美國有法規管理或以車輛協會之道德自我約束。
- 自駕車測試許可之申請：綜前本文之檢視，大多數國家皆要求需要申請測試許可，並限定在特定道路及規定駕駛者測試條件，惟英國無須特殊的許可，但須檢附詳細的執行標準，例如車輛、駕駛、操作行為以及順從性等資料。
- 意外事件的處理：自駕測試過程中若有脫離(disengagement)或撞擊(crash)等異常情況發生時，基於安全及責任認定之考量，目前所知之各國皆要求必須提供自駕車運作過程保存紀錄並提出報告。
- 車輛與駕駛人或操控者之權責劃分：如本文自駕車分級乙節所談，自駕車若採取 SAE 之分級標準，則針對自駕車與駕駛人之間責任有較清楚的界定，但因為各國尚有其各自的分級定義，導致各國對於駕駛人責任

並不夠明確²¹⁸，例如在英國，如果自動駕駛系統不操作時，則駕駛人必須負責，法律委員會也針對此進一步釐清；澳洲也認定在自動駕駛系統運作時由操作員負責，一旦系統交出控制權時，則由駕駛人負責。除此，對於不同態樣之自駕車輛如巴士或者工程車之責任規定，及不同無人載具如無人機或者無人船舶，各國另行規定。

- 緊急應變計畫：中國、美國加州及亞利桑那州、英國等的作業規範都要求制定詳細的應變計畫。

條件	美國-加州	美國-亞利桑那州	中國	澳洲	英國	新加坡
安全駕駛人的自駕車監管	有					
非公務機關的安全駕駛人的自駕車試驗	有					
對自動化之定義	參考SAE L3-L5	除交通法規與罰則有另外註明	有	假定L4-L5為自動化		
無安全駕駛人的自駕車監管框架	有	有	有	無	無	無
非公務機關進行的無安全駕駛人的自駕車試驗	無	有	有	無	無	無
法規	法規	行政命令	部門規章	聯邦業務法規	作業規範	監理沙盒
適用商業部屬的監管規範	無	有	有	無	無	無

圖 35. 主要國家自駕車規範比較。資料來源：WEF²¹⁹;科技發展觀測平臺²²⁰;本文整理

二.台灣自駕車法規與各國比較

就我國的自駕車法規與各國相較，1.尚未建立自駕車分類或自駕能力認定標準;2.自動駕駛尚無對應的車輛型式安全審驗規範;3.未有法律規定自駕車駕駛人履行之操作義務;4.尚未針對不同用途、不同使用場域的自駕車做出分類;5.尚未針對自駕車的個資或資料處理有特別規範。

²¹⁸ 張國鈞、蔡玉琬 (2021)，前揭註 215。

²¹⁹ IMF, *supra* note 214, at 43.

²²⁰ 張國鈞、蔡玉琬 (2021)，前揭註 215。

以下各章節就針對包含自駕車個資保護、資料運用及各國自駕車個資的規定
做一介紹。



第參章 個人資料保護相關法規



第一節 中華民國個人資料保護法簡介

第一項 立法歷史

我國現行《個人資料保護法》，簡稱《個資法》，原名為《電腦處理個人資料保護法》，《電腦處理個人資料保護法》之制定是為規範電腦處理個人資料，避免人格權受侵害，並促進個人資料之合理利用，參酌「經濟合作暨發展組織」(OECD)所揭櫫之保護個人資料八大原則，於民國 84 年 8 月 11 日公布施行。

個人資料之保護，如《個資法》立法理由所述：「本法所保障之法益為人格權，惟個人資料種類繁多，…，某些資料雖未直接指名道姓，但一經揭露仍足以識別為某一特定人，對個人隱私仍會造成侵害」，**個人資料本質為個人資訊隱私，為隱私權或人格權所保護之範圍**。如本文第二章所述資料的利用雖有助於社會生活之便利，並為現今資料經濟的動力來源，但不可諱言的因為大量運用資料而引發的個資洩漏導致的隱私權侵害事件亦逐年上升。近年來由於民間企業與政府機關大量且普遍使用手機及電腦等資訊產品及網路系統蒐用大量個人資料及資訊，加上人工智慧、物聯網、雲端技術的快速發展，使得以蒐用資料與個資成為經濟發展基礎與趨勢，才堪以因應科技社會的大量資料處理與未來快速變遷；相對的，也因資料與個資如此寶貴，近年因為個資被濫用、洩漏之爭議時有所聞，且影響層面逐漸擴大，並因此衍生出如：買賣個人資料、網路詐騙、帳號盜取、個人生活被大量廣告干擾、網路肉搜、虛擬財物盜竊、跨國金融犯罪等不同態樣的新犯罪型態，從而使當事人感到寢食不安，造成國人對於個人資料之蒐用產生負面的觀感，是以《個資法》之立法精神即為避免個人隱私受到不當侵害，並兼具促進個人資料之合理運用，而就個人資料之蒐集、處理及利用方式制定相關規範，平衡隱私保護及資料利用兩者。

我國《電腦處理個人資料保護法》之基本架構參酌「經濟合作及發展組織 (Organization for Economic Cooperation and Development, OECD)」於 1980 年「隱

私保護與個人資料跨境流動準則(OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)」（下稱「OECD 隱私準則」）²²¹中，所提出之八項個人資料保護原則，八項原則²²²如下：



（一）**蒐集限制原則**(Collection Limitation Principle)

有關個人資料之蒐集，原則上應加以限制。蒐集個人資料時應合法、公正，並通知當事人獲得其同意後，始得為之。（“There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.”）

（二）**資料關聯性及正確性原則**(Data Quality Principle)

個人資料與利用目的應具有合理之關聯性，且於該利用目的之必要範圍內，應係**正確、完整及保持最新狀態**。（“Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.”）

（三）**目的特定原則** (Purpose Specification Principle)

個人資料之蒐集目的，**最遲應於蒐集時即已明確化**，且於其後資料的利用，不得與所蒐集的目的抵觸，於目的變更後應加以明確化。（“The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.”）簡言之，資料之利用應於蒐集目的範圍內。

²²¹ 參見立法院公報，第 83 卷第 45 期，頁 523，臺北:立法院。

²²² 「OECD 隱私準則」於 2013 年再更新兩個主題包含 1. 通過基於風險管理的方法專注於隱私保護的實際實施，以及 2. 需要通過改進互動操作來解決全球各國間隱私問題。並提出幾個候選議題：1. 國家隱私策略：雖然目前各國有效的法律必不可少，但當今隱私的戰略重要性還需要多國間隱私合作與協調；2. 隱私管理計劃：這些是組織實施隱私保護的核心運行機制；3. 數據安全性漏洞通知：包括向當局發出通知和向受到影響個人數據的安全性漏洞影響的個人發出通知。

(四) 使用限制原則 (Use Limitation Principle)

個人資料不應作為蒐集目的以外之其他目的之查詢閱覽利用或其他使用，除非經過當事人(資料主體)之同意或依據法律之規定。換言之，個人資料除非 a).當事人同意;或 b).法律另有規定者外，不得為蒐集目的外之揭露或利用。(“Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law.”)

(五) 安全維護原則 (Security Safeguards Principle)

個人資料應予以合理的安全措施加以保護，以避免其遭受遺失、未經授權存取、破壞、利用、竄改、揭露等危險。(“Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.”)

(六) 公開透明原則 (Openness Principle)

須制定一般性政策，針對有關個人資料之蒐集、處理、運用，應對社會大眾為公開，並以最簡便之方法，使公眾知悉個人資料之蒐集目的、性質及主要的利用目的，個人資料控制者有明白揭示之必要。(“There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.”)

(七) 個人參與原則 (Individual Participation Principle)

當事人關於自身的資料得享有以下的權利：a).具有權利向資料控制者確認是否管理擁有關於自己的資料；b).當事人得於合理期間內，以合理方法、不過當之費用及容易理解之形式，接近有關其個人之資料；c).就前述 a)及 b)項權利之行使，如受到資料控制者拒絕時，資料控制者應附理由且當事人得對資料控制者提出異

議；d).於前項 c)異議成功時，當事人得要求資料控制者刪除、修改、完整及補充其個人資料。(“An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.”)

(八) 課責原則 (Accountability Principle)

資料控制者負有依循前揭原則下提出處置個人資料方式之責任。(“A data controller should be accountable for complying with measures which give effect to the principles stated above.”)

「OECD 隱私準則」雖然只是建議性質，其具體規定內容並不够明確，而且對於會員國的規定並沒有強制拘束力，然而時至今天幾乎所有的 OECD 經合組織國家都據此頒布個人資料保護法規，堪見該準則具有一定的影響力。

鑒於 1.個資法保護客體不再限於經電腦處理之個人資料，且該法規範行為除個人資料之處理外，將擴及至包括蒐集、處理及利用行為；2.落實我國對亞太經濟合作會議(APEC)之承諾：亞太經濟合作會議(APEC)於 2004 年 11 月 18 日部長級會議決議通過「隱私權保護綱領」(APEC privacy Framework)，明確宣示“「**保護資訊隱私**」與「**維持資訊流通**」同樣重要²²³，……且二者間應求取平衡，以兼顧隱私權保護，並促進各會員經濟體相互間貿易往來與經濟繁榮及發展”。我國既是 APEC 會員國，自應遵守 APEC 決議，對於個人資料保護之規範必須達到國際水準，方能與世界各國法制接軌。其後 APEC 非常重視隱私權保護之落實，對於各會員經濟

²²³ 立法院公報處 (2008)，《立法院公報》，第 97 卷第 28 期委員會紀錄，214 頁，臺北：立法院。

體之個人資料保護法是否將「APEC 隱私保護綱領」納入規範並確實執行，每年均列入年終成效檢討之要項之一。我國自民國 99 年 4 月全文修正《電腦處理個人資料保護法》，並將名稱修正為《個人資料保護法》，104 年《個資法》修正進一步擴大適用的範圍，將「公務機關」與「非公務機關」納入規範對象，且規範之客體亦包含透過電腦或非自動化方式獲取的個人資料。然而，個資法於 104 年修正公布施行以來迄今，因技術發展及不同產業間個資監管落地後猶有諸多爭議與模糊空間，亦無針對自駕車之個資規範。因此，如有個人資料保護之獨立監督機制(憲判字第 13 號判決參照)，針對個資定義與個資法保護範圍能詳細界定，並能涵蓋新技術的衝擊與時俱進，對各別領域應用制定實施細則，不僅能減少爭議，更可於落實保護個人人格法益之下，達到個資法建立合理利用個人資料之立法目的。

根據《個資法施行細則》第 2 條規定：「個人，指現生存之自然人。」；有關個人資料中的「得以間接方式識別」規範於同法第 3 條；「病歷」、「醫療」、「基因」、「性生活」、「健康檢查」、「犯罪前科」規範於第 4 條。我國個資保護法規制定及重要相關大法官釋字時間表如下圖 37 所示。

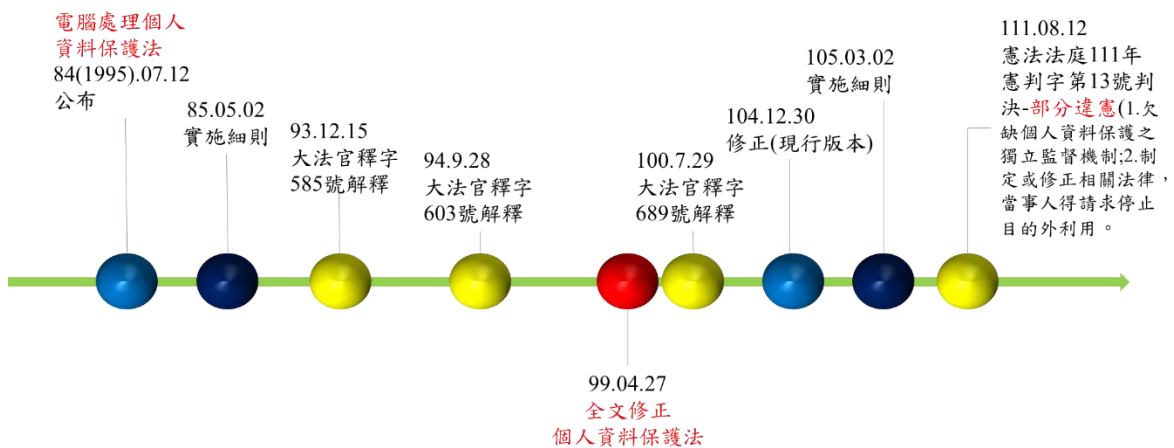


圖 36. 個人資料保護法立法歷程與重要大法官釋字。資料來源：立法院法律系統;司法院判決書查詢系統;本文整理



第二項 個人資料保護法立法目的

一.保護個人之人格權

人格權乃構成人格不可缺少之權利，我國法律肯認一般人格權，亦即存在於權利人自己人格上之權利，包括人格獨立、人格自由、人格尊嚴，並由此產生和規定具體人格權的基本權利。民法第 18 條規定之人格權，係指凡存於權利人自身上之權利，例如生命，身體、自由、名譽、秘密等權皆屬之。其中所謂「秘密權」，係就私生活所不欲人知之事實有不被他人得知之權利。而所謂「隱私權」，雖不為我國法律所明定，但為大法官肯定隱私權為憲法保障的基本權利：“其中隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活秘密空間免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障”（釋字第 509 號、第 535 號解釋參照）。

二.促進個人資料之合理利用

亞太經濟合作會議(APEC)之《APEC 隱私綱領》明確指出該綱領為：「提升亞太經濟體隱私保護並避免資訊的自由流動障礙」(“Promotes a flexible approach to information protection across APEC member economies, while avoiding the creation of unnecessary barrier to information flows”)。由《個資法》立法目的：「為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用……」觀之，《個資法》除為保障個體的「人格權」外，其更強調「促進」對個人資料的「合法利用」，以徹底落實任何個體對個人資料的「資訊隱私權」。足見我國《個資法》是在平衡保障個人人格權與隱私與資料利用，隱私之保障並非絕對。

第三項 敏感性個資定義

針對「敏感性個資」，對該等資料的蒐集、處理或利用，恐怕會對個人產生重大的危害與畏懼，因此，必須嚴格規範此等敏感性資料之蒐集、處理及利用行為。



《個資法》第 6 條第 1 項規定：「有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：

- 法律明文規定。
- 公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
- 當事人自行公開或其他已合法公開之個人資料。
- 公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
- 為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
- 經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

一般個資與敏感個資依據《個資法》處理方式可整理如下表 13 所示：

表 13. 一般個資與敏感個資依據《個資法》處理方式

資料種類 \ 處理原則	一般個資	敏感(特種)個資
事前告知	◎	◎
當事人同意	◎(含默認同意)	◎(書面同意)

第四項 資料自決權

為具體落實保障資訊自決權，當事人擁有其個人資料之控制權利，依《個資法》第 3 條規定，當事人本人就其個人資料得以行使下列權利：“1.查詢或請求閱覽;2.請求製給複製本;3.請求補充或更正;4.請求停止蒐集、處理或利用;5.請求刪除”。

前述該條規定之權利並且不得預先拋棄或以特約限制之。也就是說身為個資的所有人，依照《個資法》的規定，可以向蒐集研究資料的資料控制者請求查詢、閱覽、複製本、補充或更正個人資料，也可要求資料控制者停止蒐集、處理或利用個資，甚至可以請求刪除資料，而且該資料控制者不得要求個資所有人拋棄或限制個人資料行使的權利。此外，其中在查詢、請求閱覽、製給複製本方面，公務機關或非公務機關可以酌收必要成本費用（《個資法》第 14 條參照）。又為避免國家或公共利益或其他第三人之權益因本人行使上述權利而受損害，《個資法》第 10、11 條明文限制本人權利行使。

第五項 「資料可識別性」與「個資去識別化」概念之區分

一. 可識別性之規定

按我國《個資法》第 2 條第 1 款之規範，資料可否識別個人是所謂「個人資料」的構成要件，若非個人資料，自無《個資法》之適用。可識別性「資料」可分為「可直接識別性」與「可間接識別性」；《個資法實施細則》第三條進一步闡明「可間接識別性」，乃指「指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人」。除了《個資法》第 2 條第 1 項資料可否辨識個人之規定外，同法第 6 條第 1 項第 4 款、第 16 條第 5 款、第 19 條第 1 項第 4 款及第 20 條第 1 項第 5 款等規定，亦規範有個資可否識別特定當事人之規定。從 GDPR 的「已識別或足資識別」(identified or identifiable)定義，「已識別」(identified)是指一個自然人在群體中可被區分開來；「足資識別」(identifiable)乃指資料控制者或任何其他他人透過所有可能、合理的方式，得以辨別出該特定自然人。我國《個資法》與 GDPR 所謂「個人資料」定義與內涵將於後面章節探討，而有關「資料-個資-個資」之關係是本文探討的重點，也正是以人工智慧驅動的自駕車對現有個資保護法規衝擊最大之處。

二. 無從識別特定當事人

「無從識別特定當事人」如何判別？參諸《個資法實施細則》第 17 條：「.....

指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者。」故依我國之規定，以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人之資料，反向推論通稱為「去識別化」資料，而「去識別化」資料非屬《個資法》所定義之個資。然而該條文中並沒有明文規範辨識主體，但從一般普羅大眾對「代碼」、「隱藏部分資料」的認知，顯然此類別的資料勢必可能被掌握「代碼」、有能力還原或推測「隱藏部分資料」的資料控制者能辨識出特定的人。立法時限於技術與資料，該條文尚能適應當時之社會環境，保障當時民眾的隱私，然因大數據及人工智慧/機械學習之發展，如此定義是否可適用於實務上案例？是否可詮釋本文之智慧自駕車的資料利用與個資保護？

三. 「資料可識別性」與「個資去識別化」之於個資法

「資料可識別性」與「個資去識別化」兩者皆在於判斷資料是否可辨識出特定個人，但「資料可識別性」是在定義資料隱私保護程度，特定當事人有多少的可能被辨識出，或者資料控制者以當時候技術需要花費多少資源去辨識特定當事人；而後者「個資去識別化」則是在定義資料的可識性程度與滿足當事人的隱私保護關聯。「資料可識別」可依我國個資法進一步分為「直接可辨識」及「間接可辨識」；「個資去識別化」則指該資料不具辨識特定個人特性的資料。申言之，「個資去識別化」是資料是否為個資法適用的構成要件，若一資料若經去識別化，理論上便無可辨識出特定當事人的可能(表 15 參照)，便無侵害個人隱私權利的疑慮，自無須個資法規之保護；「資料可識別性」則是進一步探討去識別化程度與具體個案中始能滿足當事人的隱私保護。針對「資料可識別性」本文將於後面第五章進一步討論「已識別」、「足資識別」及「辨識主體」，及新興科技應用下之衝擊。

第六項 「資料可識別性」的判斷標準

我國個資法第 2 條第 1 款定義之個資，包括得以直接方式識別特定個人的資料，也包括「在與其他資料結合後，可識別特定個人」(得以間接方式識別)的資料，然後者之認定標準究應依資料使用者主觀條件或資料本身客觀條件來判別「得以間接方式識別特定個人之資料」？以「記名悠遊卡卡號是否屬個資」的個案而言

224，法務部以「就持卡人以外之第三人而言，倘該個人資料係屬查詢有困難或需耗費過鉅始能足以識別特定個人者，客觀上即屬無法識別之個人資料」。申言之，資料是否屬於個資法實施細則所規範的可識別性資料，必須從蒐用的資料控制者角度，並無一致性之標準。之《個資法施行細則》第三條即明定：「……指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。」

前揭函釋引發兩個重要問題：1.何為辨識主體?2.辨識之主客觀條件。在辨識主體問題上，我國前揭函釋以保有資料的資料控制者標準來評斷該資料是否為個資，是目前我國主流的「資料可識別性」判斷標準，然而這標準是否可解釋現今實際案例?是否以可達到《個資法》保護個人隱私的立法理由?是否與國際趨勢如GDPR的規定一致，將於完整介紹GDPR後一併比較說明。此外，以「查詢有困難或需耗費過鉅」當附加條件來做為評斷個資依據是否符合立法精神?這樣標準是否要考慮資料控制者的主觀意願與技術能力?若是，又如何評斷之?

第七項 個資法排除適用情形

在有關個資法不適用之特殊狀況訂於《個資法》第51條第一項：「有下列情形之一者，不適用本法規定：一、自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。二、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人資料結合之影音資料。」以下就本條兩項條文說明如下，

一.避免個資保護與社會利益衝突

其中有關51條第1項第二款之規定：「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人資料結合之影音資料。」如圖37見於該法99年修正版本，三讀通過之附帶決議(如. 主要國家自駕車規範比較。資料來源：WEF;科技發展觀測平臺)，由中國國民黨林鴻池及民主進度黨李俊毅委員共同提出，其目的為

²²⁴ 法務部法律字號第0999051927號函釋(2011/05/13)

避免「避免個人隱私與資料運用之社會利益衝突」。立法者的思維乃認為與個人相關的影音資料屬個資法第 2 條第 1 款明文例示之個人資料，“惟該影音資料已公開，在未與其他個人資料結合之前，故隱私保障程度較低，在平衡個資保護與資料流通兩者，且合於憲法對隱私權之限定下，排除個資法的適用”。足見我國個資法對於個資保障與個資運用的社會利益是等同重視。

立法院公報 第 99 卷 第 29 期 院會紀錄

問院會，有無異議？（無）無異議，通過。

繼續處理協商所作的附帶決議，宣讀附帶決議。

附帶決議：

有關本法之不確定法律概念，例如公共利益、一般可得之資料來源，顯有更值得保護之重大利益、公開場所或公開活動等，由政府機關邀請民間團體、學者專家等共同研議於施行細則中確定，避免個人隱私保護與資料運用之社會利益衝突。

中國國民黨立法院黨團 林鴻池

附帶決議：

有關本法之不確定法律概念，例如公共利益、一般可得之資料來源，顯有更值得保護之重大利益、公開場所或公開活動等，由政府機關邀請民間團體、學者專家等共同研議於施行細則中確定，避免個人隱私保護與資料運用之社會利益衝突。

民主進步黨立法院黨團 李俊毅

圖 37. 個資法三讀時加入該法第 51 條第一項第 2 款。資料來源：立法院公報第 99 卷第 29 期院會紀錄，立法院法律系統

二.個人隱私並非絕對權利

由上述立法理由可知該法並非將「個人隱私」視為絕對權利，而是必須與「資料運用之社會利益」做一個平衡。此觀點與大法官 603 號解釋文之但書一致：「惟憲法對資訊隱私權之保障並非絕對，國家得於符合憲法第二十三條規定意旨之範圍內，以法律明確規定對之予以適當之限制。」國家得在公益之目的且符合比例原則下，依法運用個人資料。

在其他法定權利與個人隱私權間，大法官釋字第 689 號，亦針對新聞採訪權與個人隱私間做出須符合比例原則。釋字第 689 號另提出「隱私之合理期待」(reasonable expectation of privacy) 之保護乃成為公示個資保護重點。所謂「隱私之合理期待」須包含 1.當事人主觀上其不受侵擾之期待已表現於外，2. 該期待須依

社會通念認為合理者。



第八項 現行個資法重點

由前述可綜整民國 104 年個資法修法(現行個資法版本)與本文所要探討相關重點為：

- 現今《個資法》擴大保護客體，不再以電腦處理之資料為限。然而當初《電腦處理個人資料保護法》的立法背景在於當時個人電腦普及與網路興起，大量資料能被快速處理、複製與傳輸。時至今日，被稱為「移動電腦」的智慧自駕車興起，其資料利用與個資保護之背景與立法理由依然值得探究智慧自駕車個資法規時借鏡。
- 依我國現行《個資法》，個資保護並非絕對。個資法立法理由為「規範自然人個人資料之蒐集、處理及利用，以避免人格權受侵害」，並「促進個人資料之合理利用」兩者間的平衡。
- 公務機關及所有行業之企業、團體及個人等非公務機關均納入適用主體
- 排除部分私人用途及公共區域之運用

第九項 我國個資法與聯網車

我國《個資法》或《無人載具科技創新實驗條例》目前並沒有針對聯網車輛或自駕車有特別的個人資料使用規範，以下只能就《個資法》的規定來瞭解可能的資料規範。

一.告知義務

1.1 一般性個資：事前告知+當事人同意(含默認同意)

自駕車所蒐集資料包含地理位置、生物辨識資料等。其中生物辨識資料應屬敏感性個資；地理資訊屬一般性個資，但若地理位置資料若與其他敏感性資料連結，

則該地理資料位置易轉變為敏感性個資。



1.2 敏感性個資：事前告知+當事人同意

《個資法》第 6 條第 1 項本文規定，列舉出五項敏感性個人資訊如下：1. 有關醫療之個人資料；2. 有關基因之個人資料；3. 有關性生活之個人資料；4. 有關健康檢查之個人資料；5. 有關犯罪前科之個人資料。敏感性個資依同條之規定：「有關病歷、.....、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：.... 六、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。」，故敏感性個資原則上不得蒐集、處理或利用，應採**事前告知並須取得當事人書面同意且蒐集、處理或利用不可逾越特定目的之必要範圍**，而在自駕車中常見敏感性個資為偵測駕駛或乘客的生理資訊、犯罪前科與紀錄；前述犯罪紀錄若只是事實的呈現，則不為敏感性個資(個資法實施細節第四條第六項)；而地理位置資料若能利用大數據或其他技術拼湊當事人的性生活，亦有構成敏感性個資之可能。

二.去識別化資料：非個資法之適用範圍

依《個資法》第 2 條依定義，所謂「個人資料」指：『指自然人之姓名、出生年月日、.....、社會活動及其他得以「直接」或「間接」方式識別該個人之資料。』，反之若一資料並無法識別該個人之資料，則不能被稱為「個人資料」。反之，若可能落入個資法範疇，則無論蒐集、處理及利用各階段皆應該遵循個資法(最高行政法院 106 年度判字第 54 號判決；法律字第 10603512680 號²²⁵參照)。自駕車資料多樣且巨大，除可聯網結合，亦可長期持續性紀錄，過往不被視為個資的資料，是否

²²⁵ 民國 106 年 11 月 10 日法律字第 10603512680 號。要旨：個人資料保護法第 2、11 條等規定參照，倘業者基於當事人同意合法蒐集、處理個人資料，當事人事後撤回同意，則自撤時起，如蒐集特定目的或要件已不存在，除有該法第 11 條第 3 項但書規定情形外，業者應主動或依當事人請求，刪除、停止處理或利用該等個人資料；又非公務機關如將保有之個人資料，運用各種技術予以去識別化，而依其呈現方式已無從直接或間接識別該特定個人者，即非屬個人資料，自非該法適用範圍。

就可能被轉化成得以「直接」或「間接」方式識別特定個人的個資?自駕車之資料若被列入個資保護，隨之而來的蒐用過程是否符合個資保護原則等問題就接踵而來。



第二節 歐盟《一般資料保護規範》(GDPR)

第一項 《一般資料保護規範》(GDPR)簡介

《一般資料保護規範》(英語: General Data Protection Regulation, 縮寫作 GDPR) 或稱《通用資料保護規則》，是在歐盟法律中對所有歐盟個人關於資料保護和隱私的規範，並涵蓋了歐盟以外的個人資料境外傳輸。GDPR 主要目標為個人對於自身個人資訊的控制及保護個人隱私權，以及為了國際有關資料運用商務之歐盟境外統一規範，各歐盟會員國可依此訂定更嚴格之個資管理規定。

GDPR 取代了歐盟在 1995 年推出的歐盟個人資料《資料保護指令》(Data Protection Directive) 95/46/EC，該條例包含有關處理歐盟內部當事人(資料主體)的個人可識別資訊的條款和要求，適用於與歐洲做生意的所有企業，不論實體位置何在。GDPR 要求處理個人資料的業務流程必須在設計和預設情況下構建資料保護，即是個人資料必須使用「假名化」或「匿名化」進行存儲，並且預設使用儘可能最高的隱私設置，以避免公開資料未經明確同意，並且不能用於識別沒有單獨存儲附加資訊的主題。任何個人資料除非在合法基礎上完成，否則資料控制者或資料處理者即使已經從資料所有者那裡獲得明確的選擇同意，當事人有權隨時撤銷此權限。

相對我國《個資法》並沒有針對區分資料蒐集、資料處理、資料利用及資料控制者，GDPR 第 4 條第 7 款規定所謂「資料控制者」(Data Controller)²²⁶是指對於

²²⁶ GDPR, Art. 4 (7). 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law.'

個資蒐用之目的與方式，該控制者具有自我決定權，或者與他人具有共同決定權之自然人、法人、國家組織或其他機構。同條第 8 款定義所謂「資料蒐用者」(Data Processor)指代表資料控制者處理個資的自然人、法人、國家組織或其他機構，前述之「處理」(processing)²²⁷包含我國《個資法》之「蒐集」、「處理」及「利用」三個行為，本文統稱為「蒐用」。在比較我國《個資法》與 GDPR 的名詞定義差異時，除了翻譯上的問題，尚有部分是雙方在基本名詞就存在無法對照的問題，本節第二項文中就有整理《個資法》與 GDPR 在名詞使用上及其定義上比較表。

個人資料蒐用者必須清楚地披露任何資料蒐集，聲明資料蒐用的合法基礎和目的，保留資料的時間以及是否與任何協力廠商或歐盟以外的國家共用資料。用戶有權以通用格式請求處理器蒐集的資料的便攜式副本，並有權在特定情況下刪除其資料。公共主管部門和以核心活動為中心定期或系統地處理個人資料的企業需要設立個資保護長 (DPO) 負責管理 GDPR 的合法性。如果資料洩露對用戶隱私產生不利影響，企業必須在 72 小時內報告任何資料洩露。

GDPR 法案在 2016 年 4 月 27 日通過，兩年的緩衝期後，在 2018 年 5 月 25 日強制執行。根據歐洲聯盟運作條約第 288 條第 2 項，因為 **GDPR 屬於歐盟條例 (regulation)**，不是指令(directive)，所以不需經過歐盟成員國立法轉換成各國法律可直接適用。隨著英國在 2019 年脫離歐盟，它於 2018 年 5 月 23 日批准了 2018 年資料保護法案。該法案包含了相應的法規和保護措施。

一.管轄

原則上只要處理歐盟境內人民的個人資料，就必須遵守 GDPR 的規範。包含客戶中歐盟公民、歐盟供應商、雇用歐盟員工及非營利組織與政府機構，並握有其客戶或成員相關資料者，皆應受 GDPR 管轄。

²²⁷ GDPR. Art. 4 (8). 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.'



二.個人資料定義與保護範圍

何謂「個資」依各國個資保護法規之定義略有不同，但都泛指能辨識特定個人之資料。換言之，凡是個人所能相關聯或由個人活動產生出的任何資料，幾乎都被可能定義為個人資料並理應受到保護，包括：個人身分，如電話號碼、地址、車牌等；生物特徵，如指紋、臉部辨識、視網膜掃描、相片等；電子紀錄，如 Cookie、IP 位置、行動裝置 ID、社群網站活動紀錄等。這些所謂個人資料(Personal Data)依據個資法規之規定可區分為以下兩種：

- 一般資料：姓名、可識別之號碼、網路識別碼、位置資料、生理、基因、心理、經濟、文化、社會認同等可識別自然人之因數。
- 敏感資料：種族或人種、政治意見、宗教或哲學信仰、工會、生物特徵識別、健康資料、性生活、性傾向、犯罪前科。

以上兩種分類是目前各國主流的分類方法，分類之精神是基於該資料洩漏對當事人造成影響而定，是故各國明文例示的個資有所不同。然而此分類是否可滿足現今資料充斥，平衡資料利用與個資保護兩者？在擁有最先進技術且巨大資料的智慧自駕車應用領域是否還可適用？本文於第 5 章有更深入的探討，並提出本文之個資分類見解。

三.個資處理原則

GDPR 有基本資料處理原則，個資蒐用必須符合該原則，包含 1.合法性、公正性及透明性；2.目的限制；3.最少蒐集資料；4.資料正確性；5.儲存限制及 6.資料的完整性和保密性，共 6 大原則(GDPR 第 5 條第 1 項參照)。以下就這些原則簡要說明：

- 合法性、公正性及透明性原則(lawfulness, fairness and transparency)：處理當事人之個人資料應合法、公正及透明。
- 目的限制原則(purpose limitation)：個資蒐集目的須特定、明確及合法，



且不得為該等目的以外之進階處理，但依照第 89 條第 1 項規定，為達成公共利益、科學研究或統計目的所為之進階處理，不應視為不符合原始目的。

- 資料最少蒐集原則(data minimisation)：個資蒐集應為適當、相關且限於處理目的所必要者。
- 「正確性」原則(accuracy)：在符合個人資料處理之目的下，以正確且必要時應隨時更新個人資料，且應採取一切合理措施，確保不正確之個人資料立即被刪除或更正。
- 儲存限制原則(storage limitation)：當事人之識別資料保存於一定形式，不得長於處理目的所必要之期間。該個人資料得以被儲存較長時間之情形，只有為達成公共利益之目的、科學研究目的或統計目的，且符合同法第 89 條第 1 項規定，實施適當之技術上及組織上之措施以確保當事人權利。
- 完整性和保密性原則(integrity and confidentiality)：處理應以確保個人資料適當安全性之方式為之，包括使用適當之技術上或組織上之措施，以防止未經授權或非法處理，並防止意外遺失、破壞或損壞。

四.資料控制者與處理者的其他責任

包含侵害通報、資料保存、資料保護影響評估、隱私設計、個資保護長(Data Protection Officer, DPO)及歐盟境內代表。

五.當事人權利

包含近用權、更正權、刪除權、限制處理、可攜權、拒絕權。

六.「假名化資料」(pseudonymised data)與「匿名化資料」(anonymous



data) 之區別

我國《個資法》條文上並未就「匿名化」及「假名化」予以解釋或規範，但概念上猶得透過我國個資保護法規、判例及函釋等探詢其內涵。相對的，GDPR 針對「假名化資料」(pseudonymised data) 與「匿名化資料」(anonymous data) 兩種資料分類之是依資料處理後可識別程度來區分，有較為明確的定義與區別。所謂匿名化資料，據歐盟資料保護工作小組的 Article 29 Data Protection working Party，簡稱 WP29 之《個資概念意見書》規定，必須達到不論是資料控制者(data controller) 或是協力廠商(third party) 採取可能合理之手段皆無法識別出特定當事人(資料主體)之程度，換言之，資料經匿名化處理後，斷然無識別特定當事人之可能。GDPR 前言第 26 點亦有提及，已不可再識別當事人之匿名化資料，即非為 GDPR 所規範之客體。

GDPR 第 4 條中則就假名化予以定義：經假名化之個人資料，指非透過其他資訊之對照，不能再識別出特定當事人(資料主體)。「假名化」處理(pseudonymization)，是指將個人資料予以「標示」或「編碼」，一般人無從識別，但「假名化」非真正「無從識別特定當事人」之「去識別化」(de-identification)。同時 GDPR 規定資料控制者應將其他資訊應與假名化之資料分開存放，並採取其他技術上或組織上之保護措施，確保無法透過該個人資料連結至特定當事人或可識別之當事人。GDPR 前言第 26 點²²⁸對於假名化資料亦有闡述：若可透過額外資訊之使用而識別出假名化個資之當事人，則該資料應視為可得識別之當事人的資料。換言之，假名化之資料猶屬個人資料而應受 GDPR 所規範。

有鑑於前述 GDPR 立法上有關「匿名化」及「假名化」之定義與論述，可得知所謂「匿名化」資料因已喪失資料之個人屬性、不論是資料控制者(data controller) 或是任意第三方(third party) 採取任何可能合理手段亦無法辨識出特定當事人，自無侵害當事人隱私權之疑慮，故不受 GDPR 所規範；然而，相較下「假名化」

²²⁸ GDPR, Recital 26.

資料仍可能透過與其他資料對照而識別出當事人，但 GDPR 以資料利用之觀點仍認定假名化屬於資料處理之適當保護措施。

從我國《個資法》關於「直接或間接識別特定個人」資料可反向推論之「去識別化」資料之定義。然而相較 GDPR 之區分，我國《個資法》所謂「去識別化」資料之定義，於當事人資料權利之保護似乎未盡完善，在案例中時常有平衡資料利用與個資保護的矛盾。依《個資法》第 2 條第 1 款可反向推論：無從直接或間接識別該個人之資料，該資料則**非屬《個資法》所保護之個人資料**；《個資法施行細則》第 3 條規定並進一步闡述「間接識別」之概念：「所謂間接識別，係指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人」。上揭條文將「去識別化」資料規定**排除於我國《個資法》規範外**，與 GDPR 所稱「匿名化」資料定義目的相同。

然而《個資法》中其他條文之「無從識別當事人」概念，是否能夠全部以 GDPR 匿名化之定義理解其內涵？「無從識別當事人」概念是否等同於不會有侵害當事人隱私權的疑慮？依照《個資法施行細則》第 17 條規定：「……無從識特定當事人，指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者」。該條文將「匿名」與「代碼、隱藏部分資料」一併明文例示為去識別化方法，然而條文中並無就該些資料是否有侵害當事人之個資隱私疑慮予以區分。深究本條所定義之「無從識別」，為保護當事人資料權利及隱私之措施，較為接近 GDPR 之「假名化」定義與屬性，此定義顯然與個資法第 2 條第 1 款之斷無侵害當事人隱私權可能之去識別化資料有所區別。最高行政法院 106 年度判字第 54 號健保資料乙案中亦相同爭議：“衛福部所稱之「加密」，充其量僅為以一組特定之亂碼取代個人身分證字號的「假名化」處理 (pseudonymization)，而非真正「無從識別特定當事人」之「去識別化」(anonymization) 處理。”

我國《個資法》上並無關於「假名化」、「匿名化」之區分與定義；對於「去識別化」定義與概念未臻明確，結果導致無法與國際接軌且我國法律規範與案例解釋不一致，在個資保護與資料利用的衝突案例中，亦衍生出實務上法律適用及解釋間

衝突。本文在探討自駕車個資保護時，以歐盟之「假名化」及「匿名化」化概念定義為範本，透過國際個資保護法律之規範內涵省思我國《個資法》之「去識別化」定義與規範。然而，縱使以 GDPR 嚴格的資料分類，是否足夠因應智慧自駕車時代的資料利用與個人資料保護問題?在本文在後面章節從資料特性及資料控制者(Data Controller)之角度將有更深入的探討。

七.罰則

GDPR 最高可罰以 2000 萬歐元或全球營業額 4%的罰鍰。

第二項 GDPR 與我國個資法之比較

我國《個資法》前身為《電腦資料保護法》，嗣後因為國際趨勢與技術發展，於 99(西元 2010)年全文修正，並於 104(西元 2015)年再次修正。目前 104 年版本為現行版本，後續於 105(西元 2016)年公布現行《個資法實施細則》。歐盟 GDPR 於 2018 年施行，由於影響廣泛與罰則嚴厲，故實務上對於我國無論公務或非公務機關都有重大衝擊，故本文以時間軸整理近年來重要法規及判例時間點如圖 38。圖 38 中並詳細幾個重要判例，如 93 年大法官釋字 585 號解釋：“...隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障”；94 年大法官釋字 603 號解釋：“捺指紋始核發身分證規定違憲”；100 年大法官釋字 689 號解釋：“記者跟拍-隱私的合理期待”；106 年最高行政法院 106 年度判字第 54 號判決：“國家建置全民健康保險資料庫之資訊隱私保護爭議”；107 年度臺上字第 1096 號最高法院刑事判決：“行車紀錄器紀錄資料-比例原則”及 109 年臺中高等行政法院作出 109 年度交上字第 59 號判決：“監視錄影所得之車牌影像為個資，可能會侵害隱私-無論是否實際識別”；111 年憲法法庭 111 年憲判字第 13 號判決【健保資料庫案】判決：“欠缺個人資料保護之獨立監督機制，對個人資訊隱私權之保障不足，而有違憲之虞”、“個人健康保險資料得由衛生福利部中央健康保險署以資料庫儲存、處理、對外傳輸及對外提供利用之主體、目的、要件、範圍及方式暨相關組織上及程序上之監督防護機制等重要事項，於全民健康保險法第 79 條、第 80 條及其他相關法律中，均欠缺明確規定，於此範圍內，不符憲法第 23 條法律保留原則之要求，違反

憲法第 22 條保障人民資訊隱私權之意旨²²⁹。”及“……原始蒐集目的外利用，由相關法制整體觀察，欠缺當事人得請求停止利用之相關規定；於此範圍內，違反憲法第 22 條保障人民資訊隱私權之意旨……”。隱私權之內涵與個人資料之保護隨科技衝擊社會並與公眾認知有關，難以客觀界定其範圍，以時間軸來觀之，有利於後續深入探討。

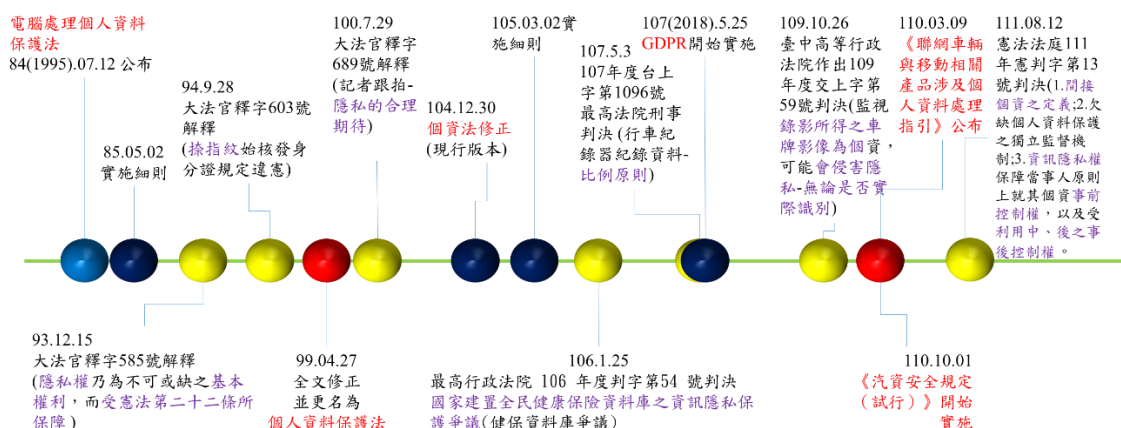


圖 38. 我國現行個資法、重要判例與 GDPR 施行之時間。資料來源：本文整理

一.GDPR 與我國個資法名詞使用與定義比較

由於 GDPR 與我國《個資法》在許多地方規定不同，且名詞所代表的意義亦有出入，為對照兩者不同及本文所使用的名詞如表 14，方便後續論述說明。

表 14. GDPR、我國個資法與本文名詞使用。資料來源：GDPR;我國《個資法》;本文整理

GDPR (英文/中文)	個資法 (中文/英文)	本文用法
Personal Data/個人資料	個人資料/Personal Data (第 2 條第 1 項第 1 款參照)	「個人資料」，簡稱「個資」
Data Subject/資料主體	當事人/Data Subject (第 2 條第 1 項第 9 款參照)	「當事人」

²²⁹ 邱文聰 (2018/01)，〈被淘空的法律保留與變質的資訊隱私憲法保障——評最高行政法院一〇六年度判字第五四號判決與相關個資法條文〉，《月旦法學雜誌》，第 272 期，頁 32-44。

GDPR (英文/中文)	個資法 (中文/英文)	本文用法
Data controller, processor and recipient 資料控制者、處理者及接收者	現行《個資法》未如 GDPR 區分資料控制者、蒐用者及接收者;但就資料蒐集、處理、利用者區分公務機關與非公務機關。	因 GDPR 之規定較為清楚,本文依 GDPR 的 4 條定義
processing (依據 GDPR 第 4 條第 2 款定義 'processing' 指對個人數據或個人數據集執行的任何操作或一組操作,無論是否通過自動方式,例如蒐集、記錄、組織、結構化、存儲、改編或更改、檢索、諮詢、使用、披露通過傳輸、傳播或以其他方式提供、對齊或組合、限制、刪除或破壞)	<ul style="list-style-type: none"> ● 蒐集:指以任何方式取得個人資料。 ● 處理:指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。 利用:指將蒐集之個人資料為處理以外之使用。	本文採論者 ²³⁰ 之用詞「蒐用」
profiling 個人檔案剖析	個人資料檔案: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	因剖析個人資料為一連串動態過程,故本文採「個人資料剖析」用詞
Personal data breach 個人資料破壞	None	本文依 GDPR 的 4 條定義

二.GDPR 與我國現行《個資法》之基本項目比較

GDPR 與我國個資法在個資的蒐用上有所不同,故下表 15 比較兩者間的差異,包含個資定義、蒐集個資之同意之方式、規範對象與去識別化等比較。

²³⁰ 張陳弘,莊植寧(2019),《新時代之個人資料保護法制:歐盟 GDPR 與臺灣個人資料保護法的比較說明》,頁 vii,臺北:新學林出版有限公司。

表 15. GDPR 與我國現行《個資法》之基本項目比較。資料來源：GDPR;《個資法》;我國
法院判決;本文整理

	個資法(104 年版本)	GDPR
個資定義	<ul style="list-style-type: none"> • 一般：得以直接或間接方式識別個人之資料。 • 敏感/特種：病歷、醫療、基因、性生活、健康檢查及犯罪前科等。 	<ul style="list-style-type: none"> • 一般個資：得以直接或間接方式識別當事人之任何資訊，包括透過網路 IP、瀏覽紀錄產生之數位軌跡並得追蹤識別特定當事人之身分。 • 敏感(特種)個資(第九條)：揭示人種、血統、政治意見、宗教、哲學信仰、工會身分、基因資料、生物特徵、健康相關、性生活與性傾向之資料。 • 刑事定罪和犯罪有關(第十條)：前科與犯罪紀錄。
蒐集個資之同意	可能取得默示同意	須明示同意
去識別化	<ul style="list-style-type: none"> ● 未明文規定 ● 「完全切斷資料內容與特定主體間之連結線索」(第 54 號判決參照) ● 「使一般人採取當時存在技術與合理成本，在不使用額外資訊時，不能識別當事人」(憲法法庭 111 年憲判字第 13 號判決參照) 	<ul style="list-style-type: none"> ● 有匿名化之定義 ● 有匿名化與假名化之清楚區分
規範對象 適用地域	歐盟境外企業對於歐盟境內當事人提供商品、服務或監控其於歐盟境內行為，該個資處理活動仍適用 GDPR。	我國公務及非公務機關於境外對我國人民個資之蒐集、處理及利用。
個資處理 原則	應依誠實及信用方法，不得逾越特定目的之必要範圍，並應與蒐集之目的具正當合理關聯。	應符合合法性、公平性及透明度、利用目的限制、資料最少蒐集、正確性、儲存限制、完整性與保密性等處理原則。

		個資法(104 年版本)	GDPR
當事人權利		請求製給複製本、更正權、刪除權、拒絕權。	更正權、刪除權、個資可攜權、拒絕權。
監管機關		分散式管理制度，各中央目的事業主管機關執行檢查、糾正、裁罰權。	至少一個獨立公務機關，監督 GDPR 之適用。
企業責任	要求設置個資保護長 (Data Protection Officer)	建議配置適當管理人力	要求在企業內部設置直接向最高管理層報告之個資保護長
	要求企業進行隱私影響評估(Privacy Impact Assessment, PIA)	<ul style="list-style-type: none"> 個資風險評估。 	<ul style="list-style-type: none"> 於特別使用新技術之處理方式，應於處理前，實行該處理對於個人資料保護的影響評估。(Article 35 Data protection impact assessment)
	事故通報	事故通報及應變機制。	知悉個資侵害事故 72 小時內通報與通知。
	其他	<ul style="list-style-type: none"> 使用紀錄及軌跡資料與證據保存 設備安全管理 	<ul style="list-style-type: none"> 文件紀錄。 個資保護之設計及預設
罰則		<ul style="list-style-type: none"> 非公務機關違反個資法規定者，中央目的事業主管機關或直轄市、縣(市)政府得按次處新臺幣 2 萬元以上，20 萬元以下；或 5 萬元以上，50 萬元之罰鍰(個資法第 47 條至第 49 條參照) 第 41 條及第 42 條另有刑事責任。 	最高得處以 2,000 萬歐元或其年度總營收 4%之罰鍰，適用對象限於企業，未針對自然人或公務機關之違反行為制定處罰規範，而係委由各會員國自行訂定有效、適當且具懲戒性的罰則(§ 83)

第三項 GDPR 針對聯網車之規範

歐盟個資保護委員會(European Data Protection Board, EDPB)針對聯網車輛在 2021 年 3 月公告《聯網車輛與移動相關產品涉及個人資料處理指南(Guidelines

01/2020 on processing personal data in the context of connected vehicles and mobility related applications)》, 此指南初版於 2020 年 1 月 28 日公布, 經公眾諮詢至 2021 年 3 月 9 日版本參考相關回饋, 版本歷史如表 16。



表 16. Guidelines 01/2020 版本歷史

版本	日期	註明
Version 1.0	28 January, 2020	Adoption of Guidelines for public consultation
Version 2.0	9 March, 2021	Adoption of the Guidelines after public consultation

《聯網車輛與移動相關產品涉及個人資料處理指南》基於聯網車輛所運用到的資料如圖 39, 包含路況偵測、用路人偵測與行為判別、駕駛偵測、移動管理、車輛管理及個人化娛樂等, 許多資料與個資有相當緊密之關聯, 特別針對聯網車輛的個資管理以下就 2021 年 3 月版本做一介紹。

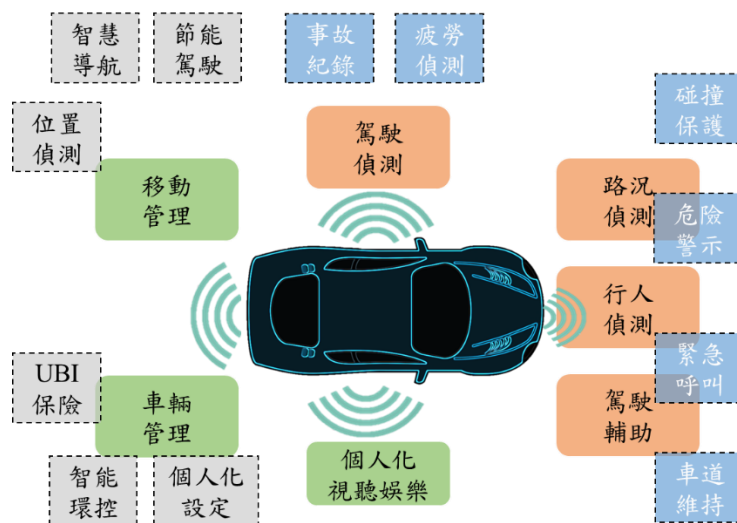


圖 39. 聯網車擁有許多資料, 其中包含許多個人資料。資料來源: EDPB; 本文整理

一. 歐洲數據保護委員會 (EDPB) 成員國家的倡議

EDPB 有關聯網車輛的數據管理倡議已有多年時間, 自 2016 年 1 月, 德國聯邦和州數據保護會議當局和德國汽車工業協會 (VDA) 發布了一分連接和非連接

數據保護原則的共同聲明²³¹。2017年8月，英國聯網和自動駕駛汽車中心(CCAV)發布了一份指南，闡明聯網和自動駕駛汽車的網路安全原則以提高汽車行業對此問題的認識²³²。2017年10月法國數據保護機構委員會 Nationale de l'Informatique et des Libertés (CNIL) 發布了聯網汽車的合法性包裹，以提供協助利益相關者如何按照設計和默認情況整合數據保護，使當事人能夠有效控制其資料²³³。

二.為何 GDPR 要特別針對聯網車輛之個資規定?

在 WP29 有關物聯網系統應用於可聯網車輛(IoT systems that can also apply to connected vehicles)²³⁴規定，基於物聯網技術運用於聯網車輛有幾點特點，特別針對聯網車輛的個資管理，理由在於：1. 移動車輛跟道路安全有關，且對駕駛的身體安全造成衝擊，故資料機密(security)與控制(control)更為敏感。相對的，傳統相關的車輛獨立處理資料，並在避免外界干擾的環境下操作。2. 由於聯網車輛處理位置數據(location data)引發了重大的數據保護和隱私疑慮，因為其越來越具有侵入性，會給當前保持匿名的可能性帶來衝擊。EDPB 希望特別強調和提高利益相關者對使用定位技術需要實施具體的保障措​​施，以防止對個人監控和濫用數據。

2.1 規範對象

《物聯網系統應用於可聯網車輛》規範對象包括資料控制者、資料蒐用者與資料接受者。其中謂為資料控制者，例如車輛保險業者、服務提供者與汽車製造商；謂為資料蒐用者包含設備製造商與汽車零件供應商等為資料控制者處理個人資料

²³¹ VDA (2016/01/26). *Data protection aspects of using connected and non-connected vehicles*. https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf

²³² US CCAV (2017/08/06). *Principles of cyber security for connected and automated vehicles*. <https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles>

²³³ CNIL (2017/10). *Compliance package for a responsible use of data in connected cars*. https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf

²³⁴ Article 29 Working Party (2014). *Opinion 8/2014 on the Recent Developments on the Internet of Things*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

者；謂為資料接收者為服務提供的商業夥伴等接收個人資料者。

從此規範對象中可看出，本指南業將汽車產業鏈的軟硬體廠商幾乎涵蓋，這也是台灣廠商須謹慎看待該指南的原因。



2.2 聯網車定義

在此指南中對於聯網車採廣義之定義，以配有許多電子控制單元(Electronic Control Unit, ECU)的車輛，ECU 透過車載網路與聯網設施連結在一起，使其能夠與車輛外的其他設備分享資訊之車輛皆適用之。

2.3 當事人(資料主體)及適用情境：

本指南中有明確定義當事人(資料主體)，包含：駕駛員、乘客、車主與用路人等 (“The scope of this document focuses in particular on the personal data processing in relation to the non-professional use of connected vehicles by data subjects: e.g., drivers, passengers, vehicle owners, other **road users**, etc.”)。由主體定義指出本指南除了注意到車內的使用者如駕駛者、乘坐者等使用者，另外還包括車主及用路人。其中「用路人」雖被然被明確定為當事人(資料主體)，然而其相關侵犯態樣及權利內涵等，尚未有明確規範。

另外一個重要的是本指南適用情境只適用於 1.非職業使用(non-professional use);2.功能需與駕駛有關:例如不包含介紹附近地標之應用程式;及 3.須涉及 GDPR 定義下之個資：直接或間接可辨識個人身分之資料。

2.4 不適用情境：

相對適用之正面臚列，指南亦明確規範不適用之情境包含：1.協作式智慧運輸系統(Cooperative Intelligent Transport Systems, CITS)：符合由歐盟小組專門小組負責之特殊資料保護狀況;2.被動式追蹤：由 ePrivacy 規範之項目，例如透過藍芽/Wi-Fi 追蹤;3.影像錄影：依各國法規規範，例如拍攝公共場合;4.僱用人使用其提供的車輛監控受僱人行為：包含受僱人到班時間、貨物運算狀況等，依各國勞工相

關法規規範。

2.5 隱私與資料保護風險(Privacy and Data protection risks)

《物聯網系統應用於可聯網車輛》所提出應注意之個資包含：1.位置資料處理(processing of location data);2.生物辨識資料：依據 GDPR 第九條之規定，生物辨識資料屬敏感個人資料，原則上不得處理，例外取得當事人明確同意 3.可能揭示刑事犯罪或其他違法行為之資料：依據 GDPR 第十條，可能揭示刑事犯罪或其他違法行為之資料，資料處理上應受到特殊限制，僅能在官方或的控制或受歐盟成員國保障資料主體權利自由之法律授權的情況下進行。

這些個資都是因應聯網車輛所特別注意的個資，其中包含 GPS 持續監控行為在我國《1096 號判決》肯認為侵犯隱私的行為，然而位置資料處理尚未被我國《個資法》所規範。除此，生物辨識資料、可能揭示刑事犯罪或其他違法行為之資料之管控，皆值得我國借鏡。

《物聯網系統應用於可聯網車輛指南》也指出個資保護五大風險，這五大風險包括：1.缺乏控制與資訊不對稱：聯網車處理個人除非有特別告知，往往不被察覺;且車商若未提供控制其個資設定之功能，個人所有人無法有效保護其權利。2.當事人同意之品質：一般取得當事人同意的方式在聯網車的情況下難以使用，特別是針對非車主及乘車更難以取得其同意。3.未經同意之目的外利用(further processing)：聯網車相關之個人資料可基於多種目的進行處理，且處理時若非有特別告知，當事人不意察覺。4.資料過度蒐集：聯網車感測器數量日益多元、量增且功能提升，容易蒐集遠大於實際所需之資料量。5.安全性與機密性。

個資保護五大風險與現行的各國個資法規有所衝突，也是本文多次提醒以現行《個資法》去管理智慧自駕車個資之要點所在，本文亦會於後面章節表列自駕車技術與現行個資法規可能衝突之處。前述五點，其中資訊的不對稱是本文前言就指出之重點，因為軟體或晶片之運作及資料傳輸本屬於企業之營業秘密，蒐用過程極其隱密不透明，危害更甚於現今網際網路的隱私侵犯。侵害之行為通常是在大規

模侵犯或者內部吹哨者暴露才易被外界察覺。申言之，若無法規之規範，這些巨量個資的蒐用及隱私的侵害是不易被外界或當事人所察覺。



2.6 EDPB 一般性建議(General Recommendations)

在本指南中一般性建議中，包含 1.資料對等暨有效同意，落實告知義務：有效告知：使用服務契約、車輛維護手冊、車載電腦等不同方式，以易懂且方便取得之格式，輔以清楚簡易語言告知消費者或使用者。EDPB 並規定不得使用汽車買賣契約取得概括同意;2.實際落實：提供不同語言選擇，並以不同資訊之重要性，階層選項以圖示標示;3.特殊狀況：例如車輛跨越國界，若會變換資料控制者，新資料控制者應及時告知取得同意。

此外，車輛內建立個人檔案管理系統規定除了儲存常用駕駛人的個資設定，可輕易變更設定並能進行刪除權的行使;在未經同意資料的處理與進階處理：聯網車相關之個人資料可基於多種目的進行處理，然依照 GDPR 目的限制原則(Principle of Purpose Limitation)，包括第五條規定「目的必須具體、明確和合法正當，且不得為目的外之進階處理」及第六條「原則上須告知當事人新使用目的並取得同意，但若為保護當事人(資料主體)之重大利益，或與原始蒐集目的相容者，得進階處理個人資料」。

第三節 中華人民共和國《民法典》與《個人信息保護法》

第一項 背景介紹

中國由於電子商務發展相當蓬勃，對於資料(中國大陸慣稱：數據)的運用相當活躍，2015 年時任阿里巴巴主席的馬雲就提出：“數據為 21 世紀的石油”，資料之重要性將取代石油地位，足見資料的商業價值與地位早已被世人所看見。然而，伴隨著資料的在全球各地大量商業化，雖創造很多中國經濟活動，亦帶來許多個人隱私權益侵害，《中華人民共和國民法典》(以下簡稱《中國民法典》)頒布之前，中國相關的民事法律規範所確定的個人資料法益請求權並不明確。《中國民法典》通過

設置專章，明文個人資料的性質是一種法律保護的民事權益，確定了個人資料的基本原則、權利義務的基本內容和構成要件、個人資料免責事由、個人對自己個人資料的決定權等。透過上述規定，《中國民法典》構造了個人資訊權益請求權的基本結構，使得個人資料權利的可訴性強化，具體化法律上個人資料保護的體系。

除了《中國民法典》對於個人資訊保護之規範明確化，中國官方為強化資料管理、促進個人資料合理利用的基礎，另頒布施行如 2017 年 6 月 1 日《中華人民共和國網絡安全法》(以下簡稱《中國網絡安全法》)、2021 年 11 月 1 日《中華人民共和國個人資訊保護法》(以下簡稱《中國個資法》)及 2021 年 9 月 1 日《中華人民共和國數據安全法》(以下簡稱《中國數據安全法》)。

《中國網絡安全法》共有 7 章 79 條，不少內容針對近年的網路安全隱患，如個人資訊洩露等。該法明確了網路詐騙等行為的定義和刑罰，明確了網路業者的責任，要求其處置違法資訊、配合偵察機關工作等。此法旨在防止網路恐怖襲擊、網路詐騙等行為，並賦予了政府在緊急情況下斷網等權力。此外，該法也對關鍵資訊基礎設施的執行安全以及懲治攻擊破壞該國境內關鍵資訊基礎設施的境外組織和個人進行明確規定。

另一部中國有關資料安全的法律為《中國數據安全法》，該法是中國第一部有關資料安全的專門法律，聚焦資料安全領域的特殊問題，在法規中確立了資料分類分級管理，建立了資料安全風險評估、監測預警、應急處置，資料安全審查等基本制度。

此外，針對自駕車的數據資料，目前中國試行《中華人民共和國汽車數據安全管理若干規定(試行)》。上述法規制度的推動實施，也代表著資料管理業已超越個人資料管理，資料不僅是重要的商業資源和生產要素，也是基礎性的國家戰略資源，為各行業發展帶來新的機遇與挑戰，亦為經濟及國家發展注入新的活水與衝擊。以上中國數據三法的探討已經超越本文探討方式，除了個人資料及車輛的資料管理會在本文探討外，其他已牽涉到國家安全與國家資料主權的議題本文只載於未來展望乙章。以下針對上述法規介紹與整理如下：



一. 《中國民法典》與個人資訊保護

《中國民法典》是中華人民共和國的第一部民法典，也是首部以「法典」命名的法律。該法於 2020 年 5 月 28 日頒布，2021 年 1 月 1 日起實施，算是近年來中國重量級的新實施法規。《中國民法典》一共有一千兩百六十條，共七編並附則，該法第一百一十一條明確規定個人資訊(本文稱為個人資料)為受法律保護之自然人權利：「自然人的個人資訊受法律保護。任何組織或者個人需要獲取他人個人資訊的，應當依法取得並確保資訊安全，不得非法蒐集、使用、加工、傳輸他人個人資訊，不得非法買賣、提供或者公開他人個人資訊。」。另外有關個人資訊規定主要在第四編人格權編之第一章一般規定(第 999~1023 條)、第五章名譽權和榮譽權(第 1024~1031 條)及第六章隱私權和個人信息保護(第 1032~1023 條)。

由關個人資訊之保護規定如第九百九十九條：「為公共利益實施新聞報道、輿論監督等行為的，可以合理使用民事主體的姓名、名稱、肖像、個人信息等；使用不合理侵害民事主體人格權的，應當依法承擔民事責任。」其他相關個人資訊保護規定載於第一千零三十條、第一千零三十四條。

二. 《中國個資法》及其他個人資訊保護專門法律

有鑒於 GDPR 及美國加州的 CCPA 接連對於個人資料有所規範，中國借鏡國際經驗之《中華人民共和國個人資訊保護法》(以下簡稱《中國個資法》)，在 2021 年 8 月 20 日通過，並已於 2021 年 11 月 1 日施行。《中國個資法》共 8 章 74 條，是中國第一部個人資料保護方面的專門法律。《中國個資法》的頒行緊接在《中國民法典》之後，其對於個資之保護有更細緻之規定，接軌國際個資與隱私之趨勢，亦加強個人資料保護的法制。換言之，可說《中國個資法》立基於《中國民法典》有關個人資料的規定之上，在個人資料保護方面形成了更加完備的制度。《中國個資法》、《中國數據安全法》及《中國網絡安全法》三法鼎足而立，被稱為中國資料三法，此三法為目前中國網路安全和資料保護領域的基礎法規，從此也可看出中國在資料及個人資料管理上的嚴謹與重視。

與台灣《個資法》立法在於規範個人資料處理，避免人格權受侵害，並促進個人資料之合理利用相似，《中國個資法》亦旨在實現個人資料保護、促進個人資料合理利用。《中國個資法》所指之個人資料，是以電子或者其他方式記錄的與已識別或者可識別的自然人有關的各種資料，類似歐盟 GDPR 之識別或可得識別自然人之任何資訊（Personally Identifiable Information, PII），或我國《個資法》法條之直接或間接方式識別該個人之資料之規定；然不包括匿名化處理後的資料。

個人資料權益是自然人針對個人資料享有的受到法律保護的權益《中國個資法》是保護個人資料權益的專門法律，該法重要立法目的在於保護個人資訊權益，如《中國個資法》第一條就明確規定：「為了保護個人信息權益，規範個人信息處理活動，促進個人資訊合理利用，根據憲法，制定本法」。第 2 條再次明確指出「自然人的個人資訊受法律保護，任何組織、個人不得侵害自然人的個人信息權益。」架構於《中國民法典》之上，《中國個資法》可說是為了對個資權益的更全面的、更充分的保護，並進一步細化、完善個人資料保護，及規範應遵循的原則和個人資料處理規則，明確個人資料處理活動中的權利義務邊界。相同的，《中國個資法》規定亦是後面《汽車數據安全管理若干規定（試行）》之基礎，也是本文在探討中國在智慧自駕車車個資保護法規不可或缺的一塊。

《中國個資法》2021 年 11 月 1 日施行前，在中國個人資料保護主要適用法規是 2021 年 1 月施行之《中國民法典》，《中國個資法》第 3 條第 1 項規定，「凡在中國大陸境內處理自然人個人信息的活動，適用該法」。故《中國個資法》與《中國民法典》兩者間應為普通法與特別法之關係。依特別法優於普通法的原則，處理自然人之個資應以《中國個資法》為優先。

《中國民法典》及《中國個資法》兩部法律對於所謂「個人資訊(個人資料)」界定範圍仍有差異。其中《中國民法典》第 4 編人格權之第 6 章為隱私權和個人信息保護。依該法第 1034 條第 2 項規定之個人資料為：「以電子或者其他方式記錄的能夠單獨或者與其他資訊結合識別特定自然人的各種資訊，包括自然人的姓名、出生日期、身分證件號碼、生物識別資訊、住址、電話號碼、電子郵箱、健康

資訊、行蹤資訊等」，違法者將負擔相關損害賠償等民事責任。而《中國個資法》第 4 條第 1 項規定一般個人資料為：「個人資訊是以電子或者其他方式記錄的與已識別或者可識別的自然人有關的各種資訊，不包括匿名化處理後的信息」。至於敏感性個人資料（或稱特種個資），則依第 28 條第 1 項規定：「敏感個人資訊是一旦洩漏或者非法使用，容易導致自然人的人格尊嚴受到侵害，或者人身、財產安全受到危害的個人資訊，包括生物識別、宗教信仰、特定身分、醫療健康、金融帳戶、行蹤軌跡等資訊」。足見《中國個資法》資料保護範圍除較《中國民法典》為廣泛且詳細。在法律責任部分，《中國個資法》包含民事、刑事及行政三種責任。

第二項 中國個資法重點

《中國個資法》之重點包括：1. 遵循國際趨勢，確立個人資訊保護原則；2. 規範個資處理活動之原則，保障當事人權益；3. 因為中國大數據的商業化盛行，特別規範自動化決策活動的規則，特別是演算法對不同當事人歧視的管制；4. 與國際趨勢一致，除一般個資外另定義敏感個人個資並嚴格保護，其中特別的是未滿 14 歲的為成年人的個資也被列入敏感個資；5. 規範國家機關處理活動；6. 明文賦予個人充分權利；7. 與歐盟及台灣個資法不同的是《中國個資法》有關亡者個人信息特別規定；8. 賦予大型網際網路平台特別義務，要求承擔更多責任；9. 健全個人資訊保護工作機制；10. 信息管轄範圍與跨境流動；11. 《中國個資法》採納歐盟 GDPR 的重罰策略；12. 同 GDPR，區分「去標識化」與「匿名化」個資（《中國個資法》第 73 條參照）；13. 除外適用規定。除外條款同台灣《個資法》第 51 條第 1 項規定，但無同條第 2 項之規定。詳細討論如下：

一. 確立個人資料保護原則

由於《中國個資法》立法時間較晚，借鏡國際經驗並依境內中國實際民情調整，立法強調處理個人資料應當遵循合法、正當、必要和誠信原則，與國際個資保護精神一致。依據該法第 6 條：「處理個人資訊應當具有明確、合理的目的，並應當與處理目的直接相關，採取對個人權益影響最小的方式」；同法第 7 條：「處理個人資訊應當遵循公開、透明原則，公開個人信息處理規則，明示處理的目的、方式

和範圍。」從上述條文得知，依照《中國個資法》蒐集個人資料與我國《個資法》及 GDPR 之個資處理原則相符：應遵守最少化原則，資料處理目的的最小範圍，不得過度蒐集個人資料；遵守目的性原則，具有明確、合理的目的並與處理目的直接相關、必要，採取對個人權益影響最小的方式，限於實現處理目的的最小範圍；合法、公平與透明性原則：公開與透明處理個資；正確性原則：保證資料品質；資料安全性原則：採取安全保護措施等。

二. 規範處理活動，保障權益

《中國個資法》為規範個人資料處理活動、保障個人資料權益，建立了以「告知-同意」為核心的個人資料處理規則，該規定見於第二章「個人資訊處理規則」。「告知-同意」規則是保障個人對其個人資料處理知情權和決定權的重要手段。依據該法要求，處理個人資料應當在事先充分告知的前提下取得個人同意，個人資料處理的重要事項發生變更的應當重新向個人告知並取得同意。同時，針對現實生活中常見的包裹授權、強制同意等問題，同法特別要求，個人資料蒐用者在「處理敏感個人資訊」、「向他人提供」或「公開個人資訊」、「跨境轉移個人資料」等環節應取得個人的單獨同意，明確個人資料蒐用者不得過度蒐集個人資料，不得以個人不同意為由拒絕提供產品或者服務，並賦予個人撤回同意的權利，在個人撤回同意後，個人資料蒐用者應當停止處理或及時刪除其個人資料。考慮到經濟社會生活的同步發展，與台灣《個資法》相同，《中國個資法》除了從維護公共利益和保障社會正常生產生活的角度，規定在個人同意之下可以合法處理個人資料的情形。此外，《中國個資法》還分別對共同處理(第 20 條)、委託處理(第 21 條)等食物中較為常見的處理情形作出有針對性規定。

三. 自動化決策活動的規則

在自動化決策活動常見的商業利用為調整不同消費者的價格或者價格歧視行為中，最典型的例子為大陸慣稱的「大數據殺熟」行為。「大數據殺熟」一詞是指廠商通過掌握消費者的個人資料，如：財務狀況、消費習慣、交易紀錄等，並加以自動化剖析個人檔案，對價格不敏感者特別是熟客施行同物不同價的商業行為，

此等被稱為「價格歧視」類似商業手段違反了《中國個資法》誠實信用原則，侵犯了消費者權益保護法規定的公平交易條件的權利。

針對這近年來各國飽受詬病的手機或電腦軟體過度蒐集個人資料、「霸王條款」²³⁵等問題，《中國個資法》規定了處理個人資料所要遵循的基本規則。對於「大數據殺熟」、「應用竊聽」等問題，該法明確了自動化決策活動的彈性規則。同法第 24 條第一項規定：「個人資訊處理者利用個人資訊進行自動化決策，應當保證決策的透明度和結果公平、公正，不得對個人在交易價格等交易條件上實行不合理的差別待遇」；同條第二項規定：「通過自動化決策方式向個人進行資訊推送、商業營銷，應當同時提供不針對其個人特徵的選項，或者向個人提供便捷的拒絕方式」；同條第三項規定：「通過自動化決策方式作出對個人權益有重大影響的決定，個人有權要求個人資訊處理者予以說明，並有權拒絕個人信息處理者僅通過自動化決策的方式作出決定。」

四. 定義敏感個人資料並嚴格保護

敏感個人資料於《中國個資法》第二節有特別規定，該法第二十八條第 1 項前段謂：「考慮到敏感個人資訊一旦洩露或者被非法使用，極易導致自然人的人格尊嚴受到侵害或者人身、財產安全受到危害……」，因此，對處理敏感個人資料的活動應作出更加嚴格的限制。

《中國個資法》將生物識別、宗教信仰、特定身分、醫療健康、金融帳戶、行蹤軌跡等資訊列為敏感個人資料。該法要求，只有在具有特定的目的和充分的必要性，並採取嚴格保護措施的情形下，方可處理敏感個人資料(第二十八條);應當事前進行影響評估(第五十五條)，並向個人告知處理的必要性以及對個人權益的影響資訊(第三十條);權責單位應制訂保護規章及標準(第六十二條)。

²³⁵ 「霸王條款」指若不同意服務業者蒐集使用者的個資，就停止提供當事人服務的不對等約定。在汽車業界，就有不同意個資條款就不能開車的案例。

值得關注的是，為保護未成年人的個人資料權益和身心健康，《中國個資法》第二十八條特別將不滿十四周歲未成年人的個人資料確定為敏感個人資訊予以嚴格保護；要求處理不滿十四周歲未成年人個人資料應當取得未成年人的父母或者其他監護人的同意，並應當對此制定專門的個人資料處理規則。

五. 規範國家機關處理活動

《中國個資法》第三節為國家機關處理個人資料的專門規定，特別強調國家機關處理個人資料的活動適用本法，並且處理個人資料應當依照法律、行政法規規定的權限和程序進行，不得超出履行法定職責所必需的範圍和限度(第 33~37 條參照)。

六. 賦予個人充分權利

《中國個資法》在第四章「個人在個人資訊處理活動中的權利」，第四十四條至第五十條，將個人在個人資料處理活動中的「知情權」及「決定權」，包括「知悉個人資訊處理規則和處理事項」、「刪除資訊」和「撤回同意」(第十五條及四十七條)，以及個人資料的「查詢」、「複製」、「更正」、「補充」等，明確個人有權掌控個人資料的處理。

同時，《中國個資法》「個資可攜帶權」亦作了原則規定，「個資可攜帶權」要求個人資料蒐用者應當提供個人資料的轉移方案，除了國際跨境、適應互聯網應用，並滿足跨平台服務多樣化服務轉移個人資料的需求，但要求「個資可攜帶權」必須在符合國家網信部門規定條件的情形下，

七. 亡者個人資料特別規定

與台灣及歐盟只針對自然人之個人資料保護相同，依《中國個資法》第二條及第三條之規定，亦旨在保護自然人的個人資料。但《中國個資法》第四十九條另有特別規定：「自然人死亡的，其近親屬為了自身的合法、正當利益，可以對死者的相關個人資訊行使本章規定的查閱、復制、更正、刪除等權利；死者生前另有安

排的除外。」依據此條規定，明確亡者之近親屬為其自身合法、正當利益，可以對亡者個人資料行使查閱、複製、更正、刪除等權利，惟尊重亡者生前之自行安排。



八.加重大型網路平台(ISP)責任

網際網路平台業者(Internet Service Provider, ISP)提供重要網路平台服務、用戶數量巨大、業務類型複雜的個人資料蒐用者對平台內的交易和個人資料處理活動具有強大的控制力和支配力，因此各國皆有立法要求大型網路平台業者在個人資料保護方面應當承擔更多的法律義務。

以中國為例，《中國個資法》第 58 條加重對這些用戶數量巨大、業務類型複雜的大型網際網路平台之個人資料保護責任：「(一)按照國家規定建立健全個人資料保護合法制度體系，成立主要由外部成員組成的獨立機構對個人資料保護情況進行監督；(二)遵循公開、公平、公正的原則，制定平台規則；(三)對嚴重違法處理個人資料的平台內產品或者服務提供者，停止提供服務；(四)定期發布個人資料保護社會責任報告，接受社會監督」。該法的前述規定是為了提高大型網際網路平台經營業務的透明度，完善平台治理，並強化外部監督。

同理，汽車資料控制者及資料蒐用者，未來發展是否如同是智慧車輛領域的平台業者，理應加重這些主體的個資保護之責任？

九.資料管轄範圍與跨境流動

這部針對資料應用監理而來的《中國個資法》，導入歐盟 GDPR 的域外效力規定，讓境外企業一樣受到拘束。依同法第 3 條第一項之規定：「在中華人民共和國境內處理自然人個人資訊的活動，適用本法。」及第 3 條第二項之規定：「在中華人民共和國境外處理中華人民共和國境內自然人個人資訊的活動，有下列情形之一的，也適用本法：(一)以向境內自然人提供產品或者服務為目的；(二)分析、評估境內自然人的行為；(三)法律、行政法規規定的其他情形。」自駕車或其他電商等的跨國企業、跨境電商要注意，就算不在中國境內設點，然從中國境外向境內的消費者提供商品或服務；或在中國境外分析、評估境內人民的行為，仍然受到

《中國個資法》的管轄。



一〇. 健全個人資料保護工作機制

個人資料保護涉及的領域既廣且深，相關制度措施的落實有賴於完善的監管執法機制。《中國個資法》第 60 條規定中國國家網信部門和國務院有關部門在各自職責範圍內負責個人資料保護和監督管理工作，同法第 61 條對個人資訊保護和監管職責作出規定，包括：“展開個人資料保護宣傳教育、指導監督個人資訊保護工作、接受處理相關投訴舉報、組織對應用程式等進行測評、調查處理違法個人資料處理活動等”。此外，為了加強個人資料保護監管執法的協同配合，同法第 62 條還進一步明確了中國國家網信部門在個人資料保護監管方面的統籌協調作用，並對其職責作出具體規定。前述個人資料保護工作機制說明，足見中國在個資保護的權責機關與負責之項目有具體規範以確保個資保護之落實。

一一. 重罰策略

《中國個資法》採與歐盟 GDPR 相同的重罰策略，第 66 條第 1 項規定違法者最高可處 100 萬元人民幣罰款，情節嚴重的最高可處 5000 萬元人民幣、或上一年度營業額 5% 的罰款（第 66 條第 2 項前段）。與台灣相比，這是台灣《個資法》第 47 條規定最高額罰鍰新臺幣五十萬的百倍之多；除此，台灣《個資法》並所沒有的「上一年度營業額 5%」罰款計算方式。

除了法人的罰款，依《中國個資法》66 條第 1 項後段，直接負責主管和其他直接責任人員也將一併受罰，情節嚴重時最高可處 100 萬元人民幣罰款（第 66 條第 2 項後段）。這不僅是台灣《個資法》第 50 條前段規定負責人最高額罰鍰的近 10 倍，也無台灣《個資法》第 50 條後段中「已盡防止義務者」之免責條款。

一二. 明確區分「去標識化」與「匿名化」

對於資料處理，《中國個資法》第八章第 73 條用語的含義中謂「去標識化」為：「……指個人資訊經過處理，使其在不借助額外資訊的情況下無法識別特定自

然人的過程」;所謂「匿名化」為:「指個人資訊經過處理無法識別特定自然人且不能復原的過程。」

對照歐盟對於假名化與匿名資料之定義,依 GDPR 第 4 條第 5 款之定義,假名化 (pseudonymisation) 指處理個人資料之方式,使該個人資料在不使用額外資訊時,不再能夠識別出特定之當事人,且該額外資料已被分開存放,並以技術及組織措施確保該個人資料無法或無可識別出當事人²³⁶;而匿名資料(anonymous data)因非屬識別或可得識別自然人之任何資訊(Personally Identifiable Information, PII),故原則不適用 GDPR。

至於我國並未細分匿名化或假名化,統稱「去識別化」,參照我國《個資法實施細則》第 17 條,所謂「去識別化」,或稱「無從識別特定當事人去識別化」者,包含「代碼」、「匿名」、「隱藏部分資料」或其他方式,無從辨識該特定個人者,皆屬之。本條規定比較有爭議的是:1.此「匿名」是否等同 GDPR 所指之「匿名化(anonymization)」?2.在此「無從辨識該特定個人」,是以主觀的資料控制者角度,還是以客觀之辨識技術?從文義中可見我國所指之「去識別化」,與 GDPR 所規定之假名化較為接近。

綜上說明比較之, GDPR 與《中國個資法》針對匿名資料之定義一致,該定義之個資皆已非屬個資保護之個資範疇;而《中國個資法》之「去標識化」資料與 GDPR 之假名化資料定義接近,但與我國個資法規所定義「去識別化」資料有所差異²³⁷。

一三. 個資保護法除外適用規定

《中國個資法》第八章第 72 條第 1 項有規定:「自然人因個人或者家庭事務

²³⁶ GDPR, Article 4(5)). Pseudonymisation means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable individual.

²³⁷ 讀者應注意「去標識化」與「去識別化」以中文字面上容易混淆,但其內涵不同。

處理個人資訊的，不適用本法。」這部分規定與台灣《個資法》第 51 條第 1 項第 1 款：「自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料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人資料結合之影音資料」規定很接近。另外 72 條第 2 項規定：「法律對各級人民政府及其有關部門組織實施的統計、檔案管理活動中的個人資訊處理有規定的，適用其規定。」故公部門可依法另行規定有關個人資料的處理。

然而，特別注意的是《中國個資法》並沒有台灣《個資法》第 51 條第 1 項第 2 款：「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人資料結合之影音資料」的規定。相對地，《中華人民共和國汽車數據安全管理若干規定(試行)》就有針對車外的用路人個資做了明確的規範。

第四節 中華人民共和國汽車數據安全管理若干規定(試行)

中國針對汽車資料安全之管理規定《汽車數據安全管理若干規定(試行)》(以下稱：《汽資安全規定(試行)》)，經中國國家發展和改革委員會、工業和資訊化部、公安部、交通運輸部同意，已自 2021 年 10 月 1 日起施行。

《汽資安全規定(試行)》是中國首個汽車行業資料安全管理的部門規章，是針對目前智慧汽車發展過程中日益引起關注的資料安全問題的監管規定。由於自駕車猶處於快速發展過程中，是故該規定既針對現在，也可能影響未來可能的法規制定，值得自駕車法規領域研究者參考。該規定重點如下：

第一項 更廣泛的適用範圍和對象

《汽資安全規定(試行)》明確其適用於在中華人民共和國境內，在設計、生產、銷售、運維、管理汽車的過程中，對於個人資訊或重要資料的蒐集、分析、存儲、查詢和跨境傳輸等各項行為。

與《網絡安全法》下的網路運營者概念類似，《汽資安全規定(試行)》針對

汽車行業界定了其規範的對象為「汽車資料處理者²³⁸」(汽車資料蒐用者)，並對汽車資料處理者的概念作了非常寬泛的定義，幾乎囊括了汽車行業上下游的所有主體，包括汽車製造商、部件和軟體提供者、經銷商、維修機構、網約車企業、保險公司等。鑒於《汽資安全規定(試行) 汽車資料安全規定(試行)》對於汽車資料處理者的定義使用了不完全列舉的表述，除了現已列舉的主體外，實際可能受到監管的物件範圍還有進一步擴大的可能，所有涉及汽車設計、製造、服務企業或者機構都可能被認定為汽車資料處理者，進而受到《汽資安全規定(試行)》的約束。

第二項 個人信息的界定

「個人信息」(個人資料)在《中華人民共和國民法典》(下稱“《民法典》”)、《網絡安全法》、《中華人民共和國個人資訊保護法》(以下簡稱《中國個資法》)中均有規定。其中，《網絡安全法》和《民法典》對個人信息的定義類似，即指能夠單獨或者與其他資訊結合識別自然人的各種資訊。近似台灣《個資法》將個人資料界定為與已識別或者可識別的自然人有關的各種資訊。

《汽資安全規定(試行)》作為中國行政部門之部門規章，直接使用了「個人信息」的概念，將汽車資料中的個人資料界定為包括“以電子或者其他方式記錄的與已識別或者可識別的車主、駕駛人、乘車人、車外人員等有關的各種信息(個資)，不包括匿名化處理後的信息”。上述定義不難看出，汽車資料的當事人主要涉及車主、駕駛人、乘車人以及用路人。其中「車外人員」如用路人的資料已經明確被納入個人資料，惟不包含匿名化處理後的資料。

第三項 敏感個人資料

《汽資安全規定(試行)》亦有定義敏感個人資料，包括：車輛行蹤軌跡、音頻、視頻、圖像和生物識別特徵等。在此法中敏感個人個資之定義為：「一旦洩露或者非法使用，可能導致車主、駕駛人、乘車人、車外人員等受到歧視或者人身、

²³⁸ 在此資料處理者對照 GDPR 應為資料蒐用者(Data Processor)。

財產安全受到嚴重危害的個人資訊(個資)」。



第四項 重要資料的範圍

與台灣相關規定不同的是，除了個人資訊(資料)的界定與規定，《汽資安全規定(試行)》是首個針對汽車行業的「重要資料」給出明確的範圍界定，具體包括：

- (一.)軍事管理區、國防科工等涉及國家秘密的單位、縣級以上黨政機關等重要敏感區域的人流車流資料；
- (二.)高於國家公開發布地圖精度的測繪資料；
- (三.)汽車充電網的運行資料；
- (四.)道路上車輛類型、車輛流量等資料；
- (五.)包含人臉、聲音、車牌等的車外音視頻資料；以及
- (六.)國家網信部門和國務院有關部門明確的其他可能影響國家安全、公共利益的資料。

從上述重要資料範圍可以看出，《汽車資料安全規定(試行)》將對汽車行業產生重大影響，且將汽車資料規範的精神從先前《中國民法典》及《中國個資法》保護當事人人格的立法目的更進一步升高到國家安全的層次，這部分的思維已超出本文所探討的範疇，本文不多深究；但也呼應本文一開始所呼籲要重視自駕車所擁有巨大且質精資料，相關法制亦應與時俱進，才能行穩致遠。自動駕駛技術在使用過程中難免涉及蒐集個人資訊及道路環境資訊，有些還會涉及車內音視頻資訊以及駕駛習慣資訊，汽車充電網的運行資料則與新能源汽車、充電站樁等清潔能源企業及其上下游的智慧網聯設備息息相關，而「測繪資料」和「車輛流量」則是導航電子地圖服務商經常處理的資料，該規定的施行對於前述企業的資料處理均提出了更高的合法標準。

換句話說，上述謂「重要資料」範圍的界定使用了較為嚴格的標準。比如目

前自動駕駛汽車道路測試過程中均可能涉及包含人臉、聲音、車牌的車外音視頻資料，這就使得從事自動駕駛技術研發的企業面臨更高的合法要求，特別是資料的傳輸影響。



第五項 車輛資料處理基本原則

《汽資安全規定(試行)》列舉了處理個人資訊和重要資料的五大原則，即「默認不蒐集」、「車內處理」、「匿名化或去標識化處理」、「最少保存期限」以及「精度範圍適用」原則。根據中國《資料安全法》，「資料處理」包括了資料的蒐集、存儲、使用、加工、傳輸、提供、公開等。

《汽資安全規定(試行)》倡導「默認不收集原則」，即汽車資料處理者預設不蒐集使用者資料原則，即每次駕駛時預設為不蒐集狀態，並且駕駛人的同意授權只對單次駕駛有效，是個人資訊「合理有效利用」蒐集原則的具體展現。

《汽資安全規定(試行)》提出了「車內處理」和「脫敏處理」原則，除非確有必要企業不得向車外提供，確有必要向車外提供的，儘可能地進行匿名化和去除敏感資料(大陸稱：脫敏處理)。此外，「精度範圍適用原則」要求汽車資料處理者根據所提供功能服務對資料精度的要求確定攝影機、雷達等的覆蓋範圍、解析度。這一要求可能會對將來智慧汽車感測器的配置標準產生影響，也就是說解析度或功能覆蓋範圍高於所提供功能服務的感測器可能會被大陸監管部門認為超出了「精度範圍適用」這一原則。如前所述之 OTA 技術，OTA 技術已經廣泛應用在個人筆記型電腦或者手機等移動裝置上，在不變動硬體規格下以軟體更新，修正缺失或更新功能；OTA 在自駕車運用上亦透過軟體線上修正缺失、更新的資料(如人工智慧/機械學習更新路況資料及模式)或提升功能，在 OTA 運用此之下硬體需超越所謂的已知精度或規格。若以目前已知的精度或規格要求自駕車製造商，一旦發現新的缺失或者需要功能提升，可能需要回到連同硬體一起提升，對於自駕車的安全性及維護成本皆是一大挑戰。

第六項 汽車行業特殊資料蒐集規定

關於蒐集資料取得使用者授權的規定，在 2021 年 10 月由全國資訊安全標準化技術委員會發布《汽車採集資料處理安全指南》²³⁹就有針對汽車行業之特殊狀況作出傳輸、儲存和出境等處理活動的安全要求。《汽資安全規定（試行）》明文針對汽車資料處理者處理個人資訊應當通過使用者手冊、車載顯示面板或其他適當方式對使用者進行告知(第 7 條)並取得當事人同意或符合法律(第 8 條第 1 項)。與一般性個人資訊的蒐集相類似，在蒐集時還應告知蒐集資料的類型，包括車輛位置、生物特徵、駕駛習慣、音視頻等(第 7 條第 1 項第 1 款)，以及蒐集每種類型資料的觸發條件以及停止蒐集的方法(同項第 2 款)；蒐集各類型資料的目的、用途；資料保存地點、期限，或者確定保存地點、期限的規則(同項第 3 及 4 款)；以及刪除車內、請求刪除已經提供給車外的個人資訊的方法步驟(同項第 5 款)。

此外，《汽資安全規定（試行）》專門針對汽車行業列舉了**敏感個人資訊**，包括**車輛位置、駕駛人或乘車人音視頻**，以及可以用於**判斷違法違規駕駛**的資料，並對於敏感個人資訊的蒐集和向車外提供相關資料提出了更高的要求。在蒐集目的上，僅可為具有直接服務於個人的目的，包括增強行車安全、智能駕駛、導航等(第 9 條第一項第 1 款)。敏感個人資訊須通過用戶手冊、車載顯示面板、語音以及汽車使用相關應用程序等顯著方式告知必要性以及對個人的影響(同項第 2 款)；在保證行車安全的前提下，以適當方式提示收集狀態，為個人終止收集提供便利(同項第 4 款)。此外，如果駕駛人要求刪除敏感個人資料，汽車資料處理者應當在十個工作日內刪除(同項第 5 款)。對於個人敏感資訊型態，《汽資安全規定（試行）》還特別要求汽車數據處理者「俱有增強行車安全的目的和充分的必要性，方可收集指紋、聲紋、人臉、心律等生物識別特徵信息」(第九條第二項)。足見該規定對於感性資料蒐用規範之嚴謹。

²³⁹ 全國資訊安全標準化技術委員會 (2021/10/08)，《汽車採集資料處理安全指南》，載於：<https://www.tc260.org.cn/file/jswj01.pdf>

有鑒於車輛使用環境的開放性，自駕車通過攝影機蒐集車外音視頻資訊時難以取得車外眾多個人的同意，而這些資訊對於輔助駕駛或自動駕駛功能往往又是必要的。《汽車資料安全規定（試行）》規定確難獲得個人同意的情況下，對於蒐集的資訊進行匿名化或去除敏感資料即可。具體而言，應當刪除能夠識別自然人的畫面或對畫面中的人臉進行局部輪廓化處理。這也是實務上汽車或軟體企業的常用的方法。

一.要求重要資料處理報告

《汽資安全規定（試行）》明確了汽車資料處理者處理重要資料之活動，須按規定展開風險評估，並向主管機關陳送風險評估報告，該報告應當包括“處理的重要資料的種類、數量，開展資料處理活動的情況，面臨的資料安全風險及其應對措施等”（第10條）；另汽車資料處理者就處理重要資料之活動須每年12月15日前向主管部門報告的要求，即汽車資料處理者處理重要資料，應當提前向省級網信部門和有關部門報告資料種類、規模、目的、必要性、保存地點與時限、使用方式，以及是否向第三方提供等（第十三條）。

二.要求資料當地語系化和境外傳輸

《汽資安全規定（試行）》與《工信部准入指南草案》的境內存儲原則基本一致，須通過由國家網信部門組織資料出境安全評估（第11條參照）。此外，資料境外傳輸除汽車數據安全事件和處置情況還須要報告境外接收者的基本情況，出境汽車數據的種類、規模、目的和必要性及在境外的保存地點、期限、範圍和方式（第13及14條參照），對因境外傳輸造成用戶合法權益或公共利益受損的（第17條第二項參照），營運者應當承擔相應責任。因此，鑒於境內存儲原則在立法趨勢上已基本明確，建議台灣企業在中國蒐集的汽車資料儘可能做到在地儲存，將伺服器或資料中心設在境內。

此外，《汽資安全規定（試行）》對於資料分享和商業利用進行了明確的限制，要求無論科技研究和商業合作夥伴需要查詢利用境內存儲的個人資訊和重要資料

的，應當採取有效措施保證資料安全，防止流失；同時，汽車資料處理者應嚴格限制對重要資料以及車輛位置、生物特徵、駕駛人或者乘車人音視頻，以及可以用於判斷違法違規駕駛的資料等敏感性資料的查詢利用。



三. 資料安全管理與年報制度

另外，值得注意的是《汽資安全規定（試行）》對於符合特定條件的個人資訊和重要資料處理提出了「年報」的要求。根據同法第 3 條及第 13 條之規定，處理個人資料涉及個資當事者逾 10 萬人或者處理重要資料的汽車資料處理者，應每年 12 月 15 日前向省級網信部門和有關部門報告資料安全管理情況。《汽資安全規定（試行）》第 13 條還另列舉了需要報告的內容，包括：資料安全負責人；處理資料的類型、規模、目的及必要性；資料安全保護措施及保存地點、期限等。涉及資料跨境傳輸的，還需要報告出境資料的類型、數量、目的以及境外的存放地點、使用範圍和方式等。

此外，如果有向境外提供資料的情況，在年報時，除了前述資訊外，還需要提供接收者的名稱和聯繫方式；出境資料的類型、數量及目的；資料在境外的存放地點、使用範圍和方式；涉及向境外提供資料的使用者投訴及處理情況等。

如本文在中國《個資法》乙節論述，在智慧自駕車領域中，汽車資料控制者及資料蒐用者如同是網際網路領域的平台業者，理應加重這些主體的個資保護之責任，避免車輛駛使用者及用路人資訊上的不對稱，本文《聯網車輛與移動相關產品涉及個人資料處理指南》乙節中「個資保護五大風險」論述，其中「缺乏控制與資訊不對稱」風險乙項，該是由政府機關由法規面去強化資料管理，此點值得台灣主管機關參考借鏡。

四. 《汽資安全規定（試行）》個資保護整理

既然中國有針對車輛個資保護有特別的規範，以下就該規範之個資保護包含主體、告知義務、要求及敏感個資等規定做一整理如下表 17：

表 17. 《汽資安全規定（試行）》個資保護整理。資料來源：本文整理

合法義務	具體條文	解釋
個資當事人	車主、駕駛人、乘車人、車外人員等	指以電子或者其他方式記錄的與已識別或者可識別的車主、駕駛人、乘車人、車外人員等有關的各種資訊， 不包括匿名化處理後的資訊。
告知義務	<p>第七條 汽車數據處理者資訊應該通過用戶手冊、車載顯示面板、語音、汽車使用相關應用程序等顯著方式，告知個人以下事項：</p> <p>（一）處理個人資訊的種類，包括車輛行蹤軌跡、駕駛習慣、音訊、影片、影像和生物識別特徵等；</p> <p>（二）各種個人資訊的具體場景以及停止蒐集的方式和途徑；</p> <p>（三）處理各種個人資訊的目的、用途、方式；</p> <p>（四）個人資訊儲存地點、儲存期限，或者確定儲存地點、儲存期限的規則；</p> <p>（五）查閱、複製其個人資訊以及刪除車內、請求刪除已經提供給車外的個人資訊的方式和途徑；</p> <p>（六）使用者權益事務聯絡人的姓名和聯絡方式；</p> <p>（七）法律、行政法規規定的應當告知的其他事項。</p>	汽車資料處理者處理個人資料應該告知處理個人資料種類、蒐集人群、停止蒐集方式相關等資料
徵得同意義務與匿名化要求	<p>第八條(授權與脫敏) 汽車資料處理者處理個人資訊應當取得個人同意或者符合法律、行政法規規定的其他情形。</p> <p>因保證行車安全需要，無法徵得個人同意採集到車外個人資訊且向車外提供的，應當進行匿名化處理，包括刪除含有能夠識別自然人的畫面，或者對畫面中的人臉資訊等進行區域性輪廓化處理等。</p>	汽車資料處理者處理個人資料應該取得個人同意或遵守法規規定的其他情況。因保證行車安全需要，無法徵得個人同意採集到車外個人資料且向車外提供的，應當進行匿名化處理或者對畫面局部輪廓化處理

合法義務	具體條文	解釋
敏感個資保護要求	<p>第九條(採集前提) 汽車資料處理者處理敏感個人資訊，應當符合以下要求或者符合法律、行政法規和強制性國家標準等其他要求：</p> <p>(一) 具有直接服務於個人的目的，包括增強行車安全、智慧駕駛、導航等；</p> <p>(二) 透過使用者手冊、車載顯示介面、語音以及汽車使用相關應用程序等顯著方式告知必要性以及對個人的影響；</p> <p>(三) 應當取得個人單獨同意，個人可以自主設定同意期限；</p> <p>(四) 在保證行車安全的前提下，以適當方式提示蒐集狀態，為個人終止蒐集提供便利；</p> <p>(五) 個人要求刪除的，汽車資料處理者應當在十個工作日內刪除。汽車資料處理者具有增強行車安全的目的和充分的必要性，方可蒐集指紋、聲紋、人臉、心律等生物識別特徵資訊。</p>	<p>在履行告知、徵得個人同意等義務基礎上，汽車資料處理者處理敏感個人還應該滿足特定的處理目的、蒐集狀態、為個人終止蒐集提供方便等具體要求。針對個人生物識別特徵資訊提示，明確汽車安全汽車資料處理者俱有增強行車的目的和充分的必要性方可蒐集</p>

五.結語

自中國《網絡安全法》施行以來，中國大陸不斷加強網路安全、資料安全以及個人資訊保護的立法和監管。隨著自動駕駛及通信技術的蓬勃發展，車輛人工智慧化、網聯化發展愈趨明確，智慧聯網汽車領域的個人資訊保護和資料安全日益突出、生物辨識及個資濫用的情況，中國大陸加快了智慧車輛行業相關的法律法規、政策標準制定的步伐，然而後續在中國實施狀況，歐盟的相關資料法規制定狀況²⁴⁰以及是否還有其他國家跟進，相當值得關注。

《汽資安全規定(試行)》的相關規定無疑會強化中國汽車行業個人資料和重

²⁴⁰ 陳曉莉 (2022/2/24)，〈歐盟提出《Data Act》法案，準備建立存取連網裝置資料的規則〉，iThome，載於：<https://www.ithome.com.tw/news/149527> (最後瀏覽日：2022/7/11)

要資料的保護，無論從使用者個人權利、企業責任、資料經濟之資料管控到國家安全層面皆有相當程度的意義；另一方面，大數據與人工智慧及對應的巨量資料需求是智慧自駕車快速反應運算的重要基礎，技術創新與資料安全如何平衡發展？是值得後續探討之處。

第五節 《數據出境安全評估辦法》

參諸中國《網絡安全法》、《數據安全法》、《個資法》等法律法規，為了進一步規範資料出境活動，保護個人資訊權益，維護國家安全和社會公共利益，促進資料跨境安全、自由流動，另外中國國家網際網路資訊辦公室於2022年7月頒布《數據出境安全評估辦法》²⁴¹，並將於今年9月1日起施行。

《數據出境安全評估辦法》第四條中明確規定資料處理者向境外提供資料，符合以下情形之一的，應當通過所在地省級網信部門向國家網信部門申報資料出境安全評估：(一)關鍵資訊基礎設施的運營者蒐集和產生的個人資訊和重要數據；(二)出境資料中包含重要資料；(三)處理個人資訊達到一百萬人的個人資訊處理者向境外提供個人資訊；(四)累計向境外提供超過十萬人以上個人資訊或者一萬人以上敏感個人資訊；(五)國家網信部門規定的其他需要申報資料出境安全評估的情形。

除此，同時依據同法第五條規定，資料處理者在向境外提供資料前，應事先開展資料出境風險自評估，重點評估以下事項：(一)資料出境及境外接收方處理資料的目的、範圍、方式等的合法性、正當性、必要性；(二)出境資料的數量、範圍、種類、敏感程度，資料出境可能對國家安全、公共利益、個人或者組織合法權益帶來的風險；(三)資料處理者在資料轉移環節的管理和技術措施、能力等能否防範資料洩露、毀損等風險；(四)境外接收方承諾承擔的責任義務，以及履行責任義務的管理和技術措施、能力等能否保障出境資料的安全；(五)資料出境和再轉移後洩露、

²⁴¹ 人民網 (2022/7/10)，數據出境安全評估辦法公布，載於：
<http://cpc.people.com.cn/BIG5/n1/2022/0710/c64387-32470917.html> (最後瀏覽日：2022/7/11)

毀損、篡改、濫用等的風險，個人維護個人資訊權益的管道是否通暢等；(六)與境外接收方訂立的資料出境相關合同是否充分約定了資料安全保護責任義務。



第六節 敏感性個資比較

敏感性個資，或稱特種個資，因性質特殊，不當蒐集、處理或利用容易侵害個人資訊隱私，故各國原則上皆禁止蒐集、處理或利用之，例外始得蒐集、處理或利用。各國個資保護法規上皆有針對敏感性個資特別規定，然各國對於敏感性個資涵蓋資料範圍與得例外蒐集的規定不同，故將規定比較如下：

第一項 敏感性個資規範差異

我國《個資法》第六條第1項規定，包含病歷、醫療、基因、性生活、健康檢查及犯罪前科共六類個資原則上不得蒐集、處理或利用，一般稱這六種個資為我國個資法所訂之敏感性個資。比較 GDPR 所定之特種個資(special categories of personal data) 種族、政治理念、宗教信仰、工會會籍、健康或性生活、性取向、基因資料或生物辨識數據等。兩者相同者包含「病歷」、「醫療」、「健康檢查」、「基因」及「性生活或性傾向」等，比較特別的是 GDPR 不將「犯罪前科」列為特種個資。而 GDPR 另有「種族」、「政治理念」、「宗教信仰」、「工會會籍」及「生物特徵」(biometric) 資料台灣個資法所沒有的敏感個資種類。值得注意的是 GDPR 在第四章定義中對於「生物特徵資料」(biometric data) 定義為：「透過自然人的身體、生理或行為特徵相關的特定技術處理產生的個人資料，這些資料允許或確認該自然人的唯一身分，例如面部圖形或指紋資料」(“personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data”)。生物特徵識別資料包含生理特徵與行為特徵，生物特徵識別技術所能涵蓋的技術相當的廣泛，除了人臉辨識、指紋辨識、虹膜掃描外，其他能辨識行為特徵的包含步態辨識、敲擊鍵盤、說話、簽名與認知等模式皆是常見可供分析的行為特徵，包含之行為相當廣泛。在台灣的

行車環境，用路人的突然行為通常是最難預測，自駕車(AV)在實際運作時，用路人行為預測是重要的技術²⁴²。



第二項 例外得蒐集之合法事由

特種個資或稱敏感性個資，原則上皆是不得蒐集，本文就不同個資保護法之例外得蒐集之規定整理如下表 18：

表 18. 例外得蒐集之合法事由。資料來源：本文整理


	台灣 個資法	GDPR	中國個資法	汽車數據安全管理若干規定（試行）
敏感性 個資法 條定義	無法條明示，但可從第 6 條規定可推得	特種個資 (special categories of personal data)	「一旦洩露或者非法使用，容易導致自然人的人格尊嚴受到侵害或者人身、財產安全受到危害的個資」	「一旦洩露或者非法使用，可能導致車主、駕駛人、乘車人、車外人員等受到歧視或者人身、財產安全受到嚴重危害的個人資訊」
敏感性 個資類 型	病歷、醫療、基因、性生活、健康檢查及犯罪前科	種族、政治理念、宗教信仰、工會會籍、健康或性生活、性傾向、基因資料或生物特徵等	生物識別、宗教信仰、特定身分、醫療健康、金融帳戶、行蹤軌跡等資訊，以及不滿十四周歲未成年人的個人信息	車輛行蹤軌跡、音頻、視頻、圖像和生物識別特徵等

²⁴² 工研院資通所 柳青浩、吳依玲、劉耿豪、林修宇、侯翔文、曾蕙如等 (2020/09/23)，《聯網自駕巴士之行人預警技術剖析及場域試運行》，工研院，載於：
<https://ictjournal.itri.org.tw/content/Messages/contents.aspx?&MmmID=654304432061644411&CatID=654313611255143006&MSID=1071256576026170547> (最後瀏覽日：2021/11/01)。

	台灣 個資法	GDPR	中國個資法	汽車數據安全管理若干規定 (試行)
例外得 蒐集之 事由	<p>一、法律明文規定。</p> <p>二、公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。</p> <p>三、當事人自行公開或其他已合法公開之個人資料。</p>	<p>1. 當事人表示明確之同意，但若歐盟法或各會員國之法令明訂特種資料處理之禁止不得藉由當事人同意而解除時，則不在此限。</p> <p>2. 該處理為資料管理者或當事人主張其基於勞動法或社會安全或保護之法令所享有之權利所必要。</p> <p>3. 該處理係為保護當事人或其他自然人具生存重要性之法益所必要，且當事人出於身體或法律上原因無法表示同意。</p> <p>4. 該處理透過基於政治、世界觀、宗教或工會所設立之基金會、社團或其他組織提供適當保障，非以營利為目的且係於其法定權限範圍內所為，但該處理僅限於其成員或昔日成員或與為達成其業務目的而有經常性聯繫之人，且該個人資料在未經當事人同意前不得對外公開。</p>	<p>在具特定目的和充分必要性下，並採取嚴格保護措施的情形，個資處理者方可處理敏感個資。另據《個人資訊保護法》第二十九條規定，處理敏感個資時，處理方應取得個人的單獨同意；法律、行政法規規定處理敏感個資應當取得書面同意的，從其規定。</p>	<p>本法無敏感個資不得蒐集或得例外蒐集之規定。惟第9條有處理敏感個資之要求。綜觀《中華人民共和國網絡安全法》、《中華人民共和國數據安全法》亦無敏感個人資訊之規定。</p>

	台灣個資法	GDPR	中國個資法	汽車數據安全管理若干規定(試行)
例外得蒐集之事由	<p>四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。</p> <p>五、為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。</p> <p>六、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。</p>	<p>5. 欲處理之個人資料已明顯由當事人公開。</p> <p>6. 該處理係為執行、行使或保護法律上之請求權或為法庭審理範圍內之司法職權所必要。</p> <p>7. 該處理係依據歐盟法或會員國法令，與其所欲達成目的間具合理關聯性，維護個人資料保護權利之本質，並訂有保護當事人基本權利及利益之適當特殊措施，而基於有重大之公益理由，認有必要者。</p> <p>8. 該處理係出於健康照護或為判斷受僱者工作能力之勞動醫學，為了醫學上之診斷、健康或社會領域之照護或治療或為了健康或社會領域之體系或服務之管理，依據歐盟法、會員國之法令或與擔任健康相關職業之成員間簽訂之契約，並符合 GDPR 第 9 條第 3 項所定要件及保障，而認有必要。</p>		

不同國家或地區對敏感資料的定義與界定是不同的，這與 OECD 針對每個國家地區依據該區傳統與態度而自行界定敏感資料態度是接近的。值得注意的是中國《汽車數據安全管理若干規定(試行)》有規定包含「車輛行蹤軌跡」、「音頻」、「視頻」、「圖像」和「生物識別特徵」等明文例示為敏感性個資。在此規定中敏感性個資定義與《中國個資法》及 GDPR 接近，惟該規定中並無敏感個資不得蒐集或得例外蒐集之規定。在《汽車數據安全管理若干規定(試行)》第 6 條說明數據處理原則為(一)車內處理原則，除非確有必要不向車外提供；(二)默認不蒐集原則，除非駕駛人自主設定，每次駕駛時默認設定為不蒐集狀態；(三)精度範圍適用原則，根據所提供功能服務對資料精度的要求確定車用攝影機、雷達等的覆蓋範圍、解析度；(四)脫敏處理原則，儘可能進行匿名化、去標識化等處理。在同



規定第 7 條中要求，汽車資料處理者處理個人資訊應當通過使用者手冊、車載顯示面板、語音、汽車使用相關應用程序等顯著方式，告知個人處理個人資訊的種類，包括車輛行蹤軌跡、駕駛習慣、音訊、視頻、圖像和生物識別特徵等；蒐集各類個人資訊的具體情境以及停止蒐集的方式和途徑；處理各類個人資訊的目的、用途、方式；個人資訊保存地點、保存期限，或者確定保存地點、保存期限的規則等。同規定第 8 條第 1 項說明汽車資料處理者處理個人資訊應當取得個人同意或者符合法律、行政法規規定的其他情形。第 8 條第二項還針對車外無法征得個人同意採集到車外個人資訊且向車外提供的，應當進行匿名化處理，包括刪除含有能夠識別自然人的畫面，或者對畫面中的人臉資訊等進行局部輪廓化處理等。從第 8 條第二項可瞭解中國大陸對車外的生物辨識的務實態度，基本上除承認車外人臉資訊為個資外，該個資亦是敏感性個資，但只務實的要求刪除或者對臉部局部輪廓化處理，此點應是採納 Google 街景圖同樣做法，並不需要取得個人(當事人)同意或者規定不得對車外用路人做蒐集。同規定第 9 條要求敏感性資料得「處理」的構成要件，包含應當符合法律、行政法規和強制性國家標準等其他要求，或者應當符合以下要求(一)具有直接服務於個人的目的，包括**增強行車安全、智慧駕駛、導航**等；(二)通過使用者手冊、車載顯示面板、語音以及汽車使用相關應用程序等顯著方式告知必要性以及對個人的影響；(三)應當取得個人單獨同意，個人可以自主設定同意期限；(四)在保證行車安全的前提下，以適當方式提示蒐集狀態，為個人終止蒐集提供便利；(五)個人要求刪除的，汽車資料處理者應當在十個工作日內刪除。在此中國《汽車數據安全管理若干規定(試行)》有將「**蒐集**」與「**處理**」分開規定。

第七節 境外傳輸比較

我國《個資法》第 21 條有關個資國際傳輸規定，採原則允許，例外限制。而《中國個資法》和歐盟 GDPR 的個資境外傳輸安全維護措施相對我國個資法有相對嚴格的規定，《中國個資法》和歐盟對比如下表 19：

表 19. 中國個資法及 GDPR 對於境外傳輸規定之比較。資料來源：各國個資主管單位網站；

本文整理

	中國個資法	GDPR
評估機構	透過國家互聯網監管機關安全評估	無
個資保護認證	取得專業機構個資保護認證	取得經核可的認證機構認證，且境外接受方做出有法律約束力的承諾，同意執行適當安全維護措施
境外接收方標準契約條款	境外接收方訂立網信部門制定的標準契約條款(第三十八條)	境外接收方訂立歐盟執委會或會員國監管機關制定的標準契約條款
合法條件	<ul style="list-style-type: none"> ● 符合法律、行政法規、網信部門規定的條件 ● 符合國際條約或協定之個資境外傳輸規定 	無
適足性認定	無	境外接受方所在國已取得歐盟個資保護適足性認定 (adequacy decision , Article 45)
企業守則	無	存在有拘束性的企業守則 (Binding Corporate Rules, BCR)
行為準則	無	存在經核可的行為準則，且境外接受方做出有法律約束力的承諾，同意執行適當安全維護措施

第肆章 人工智慧自駕車無人載具與個資權益影響

自駕車集最新科技於一身，被稱為移動的超級電腦，自駕車的盛行是否如當初「電腦資料保護法」(修正為「個人資料保護法」)立法時的背景雷同，巨量的資料是否因為蒐集、處理與利用技術之突破而受到新的威脅?近 10 年來先進的技術，在人工智慧技術的引領下，對於隱私與個資之保護是否有所差異?

人工智慧自駕車之個資與隱私問題，首見於 2016 年 10 月舉行的第 38 屆國際資料保護及隱私委員會議(International Conference of Data Protection and Privacy Commissioners)中，歐洲資料保護監督員(European Data Protection Supervisor, EDPS)在該研討會中針對自駕車(self-driving car)的資料及隱私問題有初步的探討²⁴³，例如：
1.如何規範自駕車處理大量的地理位置資訊問題(“How to regulate self-learning machines (self-driving cars) processing huge amounts of geolocation data?”);2.肯認自駕車對於生命安全及經濟之意義，但對於智慧自駕車產生的資料經濟對於當事人、資料控制者、資料處理者產生的新經濟模式、資料所有權等議題衝擊有所疑慮(“What will be the impact of new business and ownership models on data subject/data controller/data processor relations?”);3.自駕車的道德風險(“There are plenty of ethical considerations on self-driving cars (as the most current and popular example of autonomous machines), how are selfdriving cars going to impact fundamental rights close to privacy and data protection like freedom of expression or freedom of association?”)。國內亦見於論者之文章中²⁴⁴，然因時值人工智慧/機械學習/機械學習技術發展之初期，自駕車人工智慧技術之運用尚未成熟，機械學習對於資料之利用及可能對於隱私之侵害尚不明確，文中並無針對三者間有深入之探討。

²⁴³ European Data Protection Supervisor (2016/10). Artificial Intelligence, Robotics, Privacy and Data Protection, Room document for the 38th International Conference of Data Protection and Privacy Commissioners, p.13. https://edps.europa.eu/sites/default/files/publication/16-10-19_marrakesh_ai_paper_en.pdf (last visited Jan. 1, 2022).

²⁴⁴ 潘俊良 (2017)，〈歐盟和德國對於自動駕駛及智慧交通系統之個人資料保護發展〉，《科技法律透析》，第 29 卷 第 9 期，頁 55。

迄資料經濟時代，現今企業對於「資料(Data)」或「個人資料」(Personal Data)的需求殷切，如馬雲所講的“數據是 21 世紀的石油”般，無時無刻穿梭在大街小巷的自駕車感測巨量資料與網路資料結合運用，面對如此巨大資料商機，企業在利益驅使下資料或個資可能被大量商業利用，是否使我們陷入「監控資本主義」或者「被綁架的智慧城市(Ben Green, 2020)」兩書中所說的困境?類似的論述亦可見於前述章節所引述之文章(謝碩駿(2018)、林妤捷(2018)、廖曼庭(2018))。

本章所要就是針對人工智慧/機械學習所驅動之自駕車，在於個資保護與資料利用上的問題探討。智慧自駕車廣泛被使用於交通運輸，其於運作的過程中，需要蒐集、傳輸大量的資訊，針對其可能會蒐集或傳輸的資訊，目前我國《無人載具科技創新實驗條例》除了第 14 條第 3 項：「申請人應蒐集及留存創新實驗期間之紀錄資料，並應自創新實驗期間屆滿後留存至少三年。主管機關基於創新實驗安全或公共利益之必要，得命申請人提供相關資料」及同法第 17 條：「申請人蒐集、處理或利用個人資料，應遵守個人資料保護法之相關規定」；另外還有我國經濟部發行的《無人載具科技創新實驗計畫申請須知》第拾壹條執行計畫應注意事項第一項第十款規定：「申請人蒐集、處理或利用個人資料，應遵守個人資料保護法之相關規定」。對於我國目前無人載具所規定的資料管理與個資保護是否妥適?另一方面是否滿足在國際上個資或資料法規接軌時的適足性?其中差異是否導致台灣企業或新創公司基於我國《無人載具實驗沙盒》研發的實驗性無人載具技術於國際間實際應用時產生法遵風險?畢竟所謂實驗沙盒還是在特定地區及創新實驗案的經驗，如何落實到實際道路上尚有諸多未知的風險。自駕車運作的過程中，從感知、處理到執行，需要大量的資訊，針對其可能會蒐集或傳輸的資料，本文就我國的相關法規，及綜合本文前面章節之討論，列舉針對可能侵犯隱私及個人資料有疑慮之處說明：

- 民眾對車子的隱私期待：自駕車也是車輛，車子對駕駛或乘客而言，是一個可掌控、私人空間、家庭出遊的空間，大眾對於在車內的隱私期待是否應該可等同住家?縱然車輛因其特殊環境，如透明的窗戶及公示的車牌，存在可能有不特定第三人可蒐集資訊之情況，然而其個資保護是否還是應該在隱私合理的期待下獲得一定的保障?再者，車內人員的影音紀




錄、生物辨識、駕駛行為特徵、行車之 GPS 軌跡紀錄等一般性個資或敏感性個資，是否理應符合前述空間隱私權或生活私密隱私權而有更多的保障？

- 先進技術結合下之衝擊：自駕車被視為一台移動的超級電腦，亦即其蒐集、運算、傳輸、儲存能力都是先進技術的展示，前面章節所提及的不論大數據、人工智慧/機械學習、統計學習、V2X、OTA 等，都會挑戰現有的個資法規，包括「個資的認定」、「目的限定」、「資料蒐集最小化」、「資料刪除權」、是否「採取必要措施保護個人資料之安全」等。
- 自駕車的時代意義：承上，既然自駕車被視為一台移動的超級電腦，集合所有先進的人工智慧、大數據、物聯網、邊緣運算、雲端計算等技術；若回顧到 1994 年電腦資料保護的立法背景，一個個人電腦大量普及加上網際網路開端的時代。如今自駕車的到來是否又是另一個時代的轉捩點？
- 自駕車是智慧城市的一環：如前所提，自駕車非單一個體，自駕車的聯網及聯網車所編織成的網路，可對偵測到的物件或自然人持續性及動態性的監測。而過往智慧城市的隱私侵害問題，是否加入移動自駕車，會讓所有民眾的行蹤更是無所遁形？
- 載具內人員的敏感個資：無人載具為確認乘客的身分，並確保其有權使用無人載具，可能會蒐集乘客的生物辨識資料，例如指紋、聲紋或虹膜等，這些敏感性個資原則上不能蒐集，然而如何平衡公共利益與個資保護，若無法規明定是否造成執行上困難？
- 位置、軌跡資訊：自駕車為順利運作，勢必需蒐集位置資訊，其所蒐集的位置資訊包含到達目的地、路程中的交通資訊、車輛的速度與路徑等軌跡資訊。自駕車可透過蒐集某特定使用者經常造訪地點的位置資訊或行程軌跡，自駕車業者若將該等資訊提供給與行銷公司或保險公司，據以判斷該名乘客的生活習慣、消費偏好或健康狀況，作為廣告推播或評

估當事人保險費計算之參考?此些資訊之蒐用是否應侵害個人隱私之疑慮?

- 車內影音資料：自駕車可以持續蒐集、分析載具內駕駛及乘客的對話內容，並根據其對話內容，推斷當事人可能有興趣的事物或產品，再據此透過載具的影音系統推播個人化的廣告內容，以提升廣告業者的行銷效果。
- 車外周遭大量且質優資料：自駕車裝設有有各式最先進及最佳品質的感測裝置，如前所述之光達 (LiDAR)、視覺模組、雷達等感測器，以偵測其四周的車輛、用路人或路況等資訊，並可搭配 GPS 或高精地圖記載所有過程。而基於安全，針對用路人行為之判斷，可能必須採用人臉辨識或步態辨識精準判斷行人行為特徵。如此巨大、質優且經過結合運算的資料，對於資料蒐用者如同是一個大寶庫;反之，若有個資濫用或外洩，則將是隱私保護的一大威脅。
- 資料傳輸與結合：為避免視覺及感測器死角，降低交通事故發生，自駕車通常有採用車聯網通訊技術，其中包含 V2V (vehicle-to-vehicle)、V2I (vehicle-to-infrastructure) 等，即允許無人載具透過網路或其他方式，與其他載具、物聯網設備或交通號誌裝置共用各類資訊。
- 商業利益誘因與公益價值之界線模糊：因自駕車巨量資料，不論車內或車外資料都是龐大的商機，對於業者容易做目的外的運用。這些目的外的利用，包含計算最佳路徑及提供個別化服務等，另也包含商業用途，例如計算人流、人潮的年齡及性別特性、停留時間等。這些目的不能斷言只有商業上的利益，相反的，這些資料透過人工智慧/機械學習的運用，計算最佳運輸路徑以提高行車安全並降低碳排，亦具有公益之價值。是故，在自駕車資料管理上，會有多用途的用途，加以人工智慧/機械學習演算法的不透明性，資料管理上更增添困難與複雜。

- 
- 國際已有相關法規：自駕車的資料管理與個資保護，業已逐漸引起各國的注意，目前有歐盟《聯網車輛與移動相關產品涉及個人資料處理指南》及中國大陸《汽資安全規定（試行）》。
 - 跨國法遵：從前面章節羅列之案例可知，若主管機關依照《無人載具科技創新條例》及針對自駕車個資並無特別規定，台灣企業遵循我國個資法，是否就不會有跨國運用時之法遵風險？新創事業於研發無人載具技術時，應考量該等技術日後極有可能與各大車廠合作生產無人載具，也就是說，台灣企業的無人載具技術將被使用於國外的無人載具中。以中國大陸《汽資安全規定（試行）》為例，其管制的主體包含汽車設計、生產、銷售、使用、營運等過程中可能掌控個人資料之企業。台灣企業若為自駕車產業鏈的一環，自然不能忽視國際的法規趨勢。

台灣《個資法》於民國 101 年施行並經 104 年修正後，雖然具有一定程度的個資保護作用，惟相較於近年備受關注的歐盟 GDPR 或者《中國個資法》保護之廣度與深度，仍有一段差距。舉例來說，我國《個資法》對於個人資料的認定係指可以直接或間接方式識別個人的資料，如姓名、健康等，GDPR 的認定則更廣泛，只要是可用以識別自然人的任何資訊都包含在內，例如明文將 GPS 位置資訊納入個人資料的定義中。

另按我國《個資法》規定，告知當事人相關事項後，當事人如未表示拒絕，並開始提供其個人資料(默認同意)，即會被認作適法的個人資料蒐集，惟相同之情形如依照 GDPR 的規範則不一定皆屬合法；另外，我國《個資法》原則上允許將個人資料跨境傳輸至國外，僅在例外情形下加以限制，GDPR 與《中國個資法》的規範則相反，對於個資的跨境傳輸採取原則禁止，例外允許的態度；除此之外，我國《個資法》並未設置單一主管機關，而係採分散式管理，雖於 107 年國發會成立「個人資料保護專案辦公室」²⁴⁵協調各部會強化執法工作的落實與一致性，但依然

²⁴⁵ 國家發展委員會網站 (2018/07/04)，「個人資料保護專案辦公室」正式揭牌，載於：https://www.ndc.gov.tw/nc_27_29899

可能發生各個單位於執法上標準寬嚴不一的情形;相對的 GDPR 則要求歐盟各會員國皆應設置獨立的個資保護主管機關，以監督 GDPR 的適用情形。

綜上所述，台灣企業研發無人載具技術時，縱然業已遵循我國《個資法》的相關規定，然而未必當然符合 GDPR、《中國個資法》及《汽資安全規定(試行)》等國際個資保護法規。台灣企業或新創事業若僅遵循我國《個資法》，未來於海外市場推行無人載具技術的業務時，或將面臨歐美以及中國等地的法遵風險。

為避免法遵風險，台灣企業於研發智慧智駕車的過程中，可以先從瞭解各國個資保護法及針對自駕車之個資與資料保護相關法規，並遵循政府及業界個資利用與保護指導原則著手：首先，台灣企業應注意各國對於無人載具個資保護的法規或政策，於研發自駕車的過程中，即預先設想可能的行銷業務區域，並確認各該地區是否有制訂或施行相關的個資法規，若有，更應初步瞭解其內容，並確保自駕車不會違反各該法規的限制。除此，非公務機關隱私保護，汽車業界為因應智慧自駕車技術的發展，亦開始制定個資隱私保護指導原則，舉例來說，汽車製造商聯盟（Alliance of Automobile Manufacturers）與全球汽車製造商協會（Association of Global Automakers）就汽車科技的發展定有「隱私原則」（Privacy Principles）²⁴⁶，希望聯盟或協會遵守個資保護原則。綜上所述，台灣企業及新創業者於研發無人載具技術的過程中，如果未將歐盟、中國以及美國等地的個資保護議題列入考量，於國外市場推行相關業務時很可能因法遵問題而受到嚴重影響。故台灣企業不妨考慮於技術研發初期，即先行確認其自駕車技術涉及個資蒐集的情形，並盤點各國個資保護法規與協會指南，以確保未來在歐美及中國等地推廣時，能將法遵風險降到最低。

第一節 人工智慧、自駕車發展與個人資料總覽

²⁴⁶ ALLIANCE FOR AUTOMOTIVE INNOVATION, INC (Established: November 12, 2014 Reviewed: May 2018, March 2022). *Consumer Privacy Protection Principles- PRIVACY PRINCIPLES FOR VEHICLE TECHNOLOGIES AND SERVICES*. https://www.autosinnovate.org/innovation/Automotive%20Privacy/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21-19.pdf

本章前面各節已分別介紹自駕車、人工智慧與個資/《個資法》三者定義與發展現況，本節綜整三者間的關聯與彼此結合下產生的影響下，作可能爭點之簡介。爾後在第三章以近似案例來討論個資保護上的爭議與可能的解決趨勢，並在第四章針對智慧自駕車運作下，資料與個資關聯、個資保護及侵害可能等問題以本文之觀點探討之。

第一項 人工智慧應用於自駕車

在本文第二章有說明，早於人工智慧應用自駕車之前人們其實已經嘗試在車輛駕駛上開發、運用各種駕駛輔助系統(Driver Assistance Systems, DAS)及先進駕駛輔助系統(ADAS)，諸如盲點偵測系統、支持型停車輔助系統、碰撞預防系統及停車輔助系統等等。然而相關技術大都運行在 SAE 所定義的低度自動駕駛等級(L0~L2)，距離所謂的理想自駕車實踐還是有相當大的落差。直到人工智慧/機械學習/深度學習的突破，才使得高度駕駛的夢想自駕車(L3~L5)得以逐步實現。智慧車輛發展的目的是為求人們及汽車製造商的共同目標：安全、便利、舒適、環保，而這些夢想也在各汽車廠商將初階自駕車技術的成果成功商業化之後，使得世界各國車廠對於自動駕駛汽車技術未來更具信心，也帶動各式輔助汽車駕駛人的先進自動駕駛技術的蓬勃發展，而成功的關鍵就在於人工智慧之應用。以下就人工智慧/機械學習運用於自駕車領域所產生的議題作出以下整理及探討。

一.人工智慧技術應用於自駕車的必要性

人工智慧技術應用廣泛，但在討論智慧自駕車的法規的之前，必先探討人工智慧應用於高度自駕車的必要性。綜合前述對於人工智慧技術的介紹，首先要必需要闡述的是在此指的人工智慧技術是指機械學習及其分支深度學習技術。目前在機械學習/深度學習的技術應用下，如圖 6 所示電腦的物件分辨能力才能超越人類並持續改善，也因為。而若一特定技術能夠超越人類，回顧德國自駕車《倫理指南》第二條：“……當自動駕駛系統肇事機會小於人為駕駛，自動及聯網駕駛行為即符合道德倫理規範。”雖然圖形辨識能力不直接等同駕駛技術，但不可否認的是能超越人眼辨識水準並持續精進的人工智慧技術目前就屬以資料驅動機械學習/深度學



習。

過往高度自駕車之所以難以實現，在於實際路況有太多不可預測的現象，現今自動駕駛系統設計方法主要有幾個主流技術，一為規則性方式 (Rule Based Method)，即利用感測器感知整個場景，分析當時環境資訊，並以規則性研擬自駕車行駛之決策行為；另為人工智慧/深度學習模型 (Deep Learning Model)，即藉由車輛周邊環境影像與車輛動態等資訊進行駕駛行為學習與預測。規則性方式 (Rule Based Method) 設計方式其優點為有嚴謹的規則定義，系統可解釋性高，容易編修及維護，缺點為規則建構較複雜且難以自駕車多變環境，並且須依賴不同感測器，難以完善的建構整套規則；深度學習模型則不須訂定複雜規則，但決策完全依賴圖像或感測器的特徵資訊。另外有研究提出綜合上述兩種做法，先將感測器資訊預處理成重要特徵後，經由深度學習模型學習駕駛行為稱為直接感知方法 (direct perception approach)，進而預測自駕車行為，其優缺點介於規則性方式與深度學習之間。以下比較兩者特性及優缺點之整理如表 20：

表 20. 不同演算法比較。資料來源：本文整理

演算法 優缺點比較	規則式演算法 (ruled -Based algorithm)	人工智慧/機械學習 /深度學習 (AI/ML/DL)	綜合演演算法 (Hybird)
適合應用環境	規則清楚，環境變化不大	多變環境	依不同使用環境
優點	嚴謹的規則定義，系統可解釋性高，容易維護	可適應不同環境，比較接近真實使用場景	平衡前兩者的優點
缺點	無法應對複雜多變環境，且實驗室環境與真實應用常有落差	依賴大量感測器 (sensor)取得數據，系統不易解釋，且需要更新	

下面舉一個實際使用場景，下圖 40 為美國道路上常見的《STOP》警示圖，人眼可輕易辨識 4 種實際狀況都為“STOP”意涵，然而使用傳統的規則式演算法是非常難以做到像人的辨識能力。這代表者自駕車理念的實踐，使用人工智慧/機械

學習演算法是必須的。



圖 40.生活中不同 STOP 警示，這些不同的單一警示牌告對人類容易辨識，但對於傳統規則式演算法卻是難以駕馭。資料來源：Grow with Google, Google

二.資料是人工智慧/機械學習的基礎

承上之所述，現今主流驅動自駕車的技術屬人工智慧/機械學習，而量大且質優的資料就是人工智慧/機械學習運用成功與否的關鍵。自駕車所蒐集之資料不但量大、多態樣且必須即時處理與反應，是故資料從蒐集、處理到利用間，往往都是緊密不可分。且因為智慧自駕車上在快速發展，各廠商也在累積經驗與數據，資料蒐集往往衡量最小資料量且難以細化其目的性。

若這些資料可能被視為是個資，則這麼巨大的資料的所牽涉的個資及隱私問題自然不能小覷，蒐用的過程是否符合個資保護法之精神與規定?那些個資在人工智慧/機械學習配合既有的物聯網、大數據等技術下，對個資保護產生甚麼影響?有

關人工智慧/機械學習與資料及個資間的關係於後面章節詳述之。



三.人工智慧自動駕駛技術介紹對法規的可能影響

自駕車目前技術發展還是戰國時代階段，但不論採用何種技術同樣要克服白天、晚上、下雨、下雪、濃霧、灰塵等複雜環境以及前方車輛或遮蔽物的影響下蒐集不完整的路況資訊，並能夠進行障礙物偵測及處理，並完成交通運輸使命(如下圖 41)。而無論採用何種技術去克服前述問題，人工智慧自駕車能運作的背後支持的就是巨大的原始資料及計算資料。智慧自駕車目前所使用的都是最先進尖端的軟硬體技術，透過感測器辨識週邊環境資料，包括光達、影像感測器、毫米波雷達、超音波、3D 深度攝影機等，透過多元感測器資料融合(Data Fusion)整合出準確環境參數，並配合上人工智慧演算法(人臉辨識²⁴⁷、步態辨識²⁴⁸、物件偵測等)，利用巨量之資料計算出正確的操作。

自駕車透過「影像物件偵測」、「用路人行為預測」以及「預警煞車控制」等系統模組，有效提供自駕車提前掌握前方路況來車與用路人，以驅動自駕車進行決策控制，未來多重感測與路側資訊如何快速因應實際場域需求，同時兼顧自駕安全及乘客舒適度²⁴⁹。而這過程就必須有人臉辨識、步態辨識、物件偵測等人工智慧演算法，並配合快速即時反應的邊緣運算晶片才能達到。

²⁴⁷ *Id.* at 133

²⁴⁸ Lie Guo, Ping-Shu Ge, Ming-Heng Zhang, Lin-Hui Li, Yi-Bing Zhao (2012). Pedestrian detection for intelligent transportation systems combining AdaBoost algorithm and support vector machine, *Expert Systems with Applications* vol. 39, pages 4274–4286.

²⁴⁹ 柳青浩等 (2021)，前揭註 242。



圖 41.自駕車基本要具有可以辨識交通號誌、車輛及用路人之障礙物偵測系統

資料來源：技術處網站²⁵⁰

目前各家不論在硬體或者軟體上都沒有統一標準，例如 Tesla 的 Autopilot 技術就包含 8 個環景攝影機提供車體周圍 360 度的視角，範圍可達 250 公尺及 12 個更新版的超音波感測器。如下圖 42 中為 Tesla 增強版自動輔助駕駛(EAP, Enhanced Autopilot)，可看出不同感測器有其不同的偵測距離、角度與範圍，由此也可看出自駕車感測器的複雜。不同的自駕車廠商，不同技術、硬體感測器裝備與演算法，就會具有不同的資料型態及資料量。英特爾(Intel)公司近年來相當看重自駕車市場，該公司在 2017 年收購自駕車平台商 Mobileye 時表示，自駕車每天會產生 4,096GB 的資料²⁵¹，而 4,096GB 是一台現行監視器每天產生約 10GB²⁵²的 400 倍；而 level 5 的單台自駕車數據，粗估可能逾目前單台監視器數據 1,200 倍以上。

綜上，過往我國《個資法》重於平衡社會公益與人格權益之保護，然而在人工資料/機械學習因生命法益的保障必須蒐用並結合如此巨大的資料下，《個資法》

²⁵⁰ 財團法人車輛研究測試中心 (2018)，《智駕未來 自動輔助駕駛辨識快又準》，科技專案成果。 https://www.moea.gov.tw/MNS/doi/achievement/Achievements2.aspx?menu_id=5391&ac_id=1475 (最後瀏覽日:2020/12/10)。

²⁵¹ Patrock Nelson (2016/12/07). Just one autonomous car will use 4,000 GB of data/day, Network World. <https://www.networkworld.com/article/3147892/one-autonomous-car-will-use-4000-gb-of-dataday.html>.

²⁵² 台灣世曦工程顧問股份有限公司經理林啟豐 (2011)，《數位元元影像平臺於監控系統之整合應用》，中華技術專題報導，No.91, p.28-41. July, 2011。

之現行規範尚有許多模糊空間待釐清?

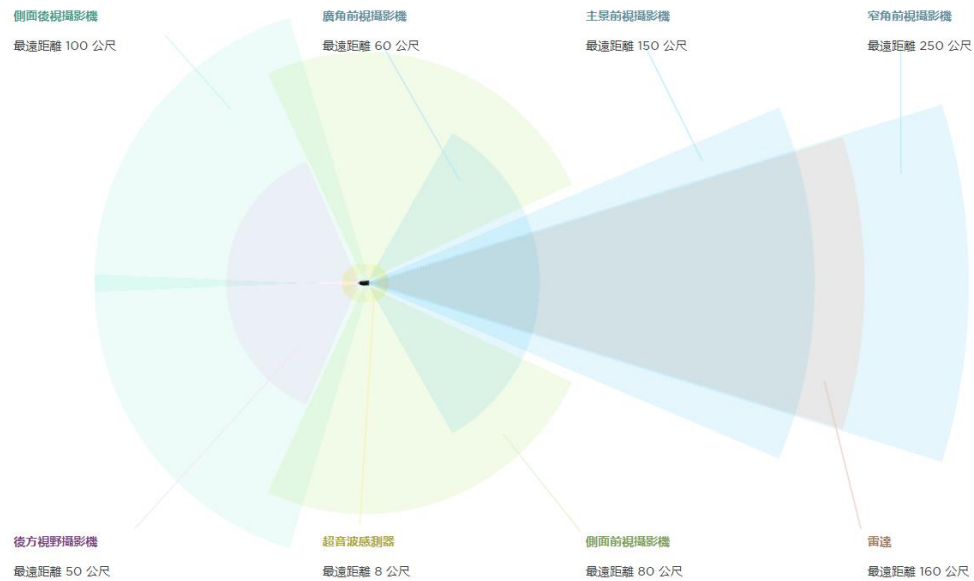



圖 42. Tesla 增強版自動輔助駕駛。資料來源：Tesla 網站²⁵³

前述是以工程角度來描述人工智慧、機器學習/深度學習。以法律角度可摘要重點如下：

- 目前是以機械學習為基礎的人工智慧為自駕車的大腦操控，故本文限定在探討機械學習為基礎的人工智慧
- 人工智慧的倫理、透明性、可問責性、隱私與資料處理迨至今日也是正在探討的議題
- 機械學習/深度學習需要持續且大量的資料驅動，數據的質與量決定機械學習/深度學習成敗，不易遵循資料最小蒐集原則，若資料牽涉到個資與生命法益兩者間比例原則更難以拿捏。在本文中主要探討個資與資料問題，將深度學習涵蓋在機械學習中，不深究其中技術問題。

²⁵³ Tesla 網站，https://www.tesla.com/zh_TW/autopilot (最後瀏覽日：2022/04/10)。

- 
- 承上，以數據為驅動的人工智慧/機器學習，被視為黑盒子的演算法邏輯不易詮釋，對於資料蒐集目的性難以明定
 - 人工智慧/機器學習以多變量且巨量的資料驅動，不同資料間的連結與個資法上資料的結合限制有衝突的疑慮
 - 以機械學習為基礎的人工智慧模型(AI Model)需要隨時更新資料，在積極運用與監管間權衡有其難度
 - 以機械學習模型(ML model)為大腦操控的自駕車運作時，資料必須快速且即時蒐集(collection)、處理(processing)到利用(use)，從法律觀點資料的蒐集、處理到利用難以分離或切割
 - 以資料驅動的人工智慧/機器學習，因為要持續且完整的資料來訓練模型，對於資料的刪除權行使有一定程度上的困難
 - 綜合上述說明，與本文有關的是以資料驅動的機械學習及其分支深度學習，並非泛指人工智慧。先前論者並未將「人工智慧」直接與「自駕車」之間的必要性說明清楚，即是導因於並未清楚「人工智慧」、機械學習及深度學習三者定義與彼此間之關係，及現今人工智慧/機器學習/深度學習之技術發展。若要探討自駕車、資料與個資之關係，前述人工智慧/機器學習的基礎為其根本。

以上是就人工智慧/機械學習可能在個資法規上模糊或衝突點芻議，結合後續自駕車及個資介紹，將會更有系統性的整理三者間的爭議點。

第二項 人工智慧與個人資料之關聯探討

一.人工智慧對隱私侵害之風險

本文第二章各國政策法規比較文中提及，各國針對自駕車的先進技術導入態度皆是保持中性，且尚未約束特定技術採用的政策趨勢。惟在近年人工智慧的興起

與大量商品化，卻產生許多實務上人工智慧道德疑慮與侵犯隱私的案例，以往過於人工智慧的法律道德再次掀起討論。各國人工智慧相關法律研究已經是長久以來在法律界被關注的議題²⁵⁴，過往在電腦及網路時代，學者 Lawrence Lessig 的名言：“編碼就是法律”²⁵⁵，在 1990 年代 Lawrence Lessig 認為計算機硬體和軟體編碼的組合，如同虛擬網路(Cyberspace)法規監管，可以探索網路使用者的隱私、約束和指導人類行為，甚至可決定人的求職工作等命運；本文第二章德國自駕車《倫理指南》(表 11)第 8 點也有提到對於兩難的抉擇不能被標準化或由軟體編碼決定。綜此，故有約束人工智慧技術之探討。

本文在第二章特別指出「人工智慧」目前尚屬概括式的總稱術語(umbrella term)，並非嚴謹的專有名詞，其泛指任何使計算機能夠模仿人類行為的技術，包含機器人、全自駕車或者電腦程式等能模仿人類行為技術。對於非科技背景的論者亦會將「人工智慧」與「機器人」相關法律議題混為一談²⁵⁶。故本文特別指出自 2014~2015 年後，真正對產業產生衝擊，特別是本文所要討論的是指第三代之以資料驅動之人工智慧/機械學習，及其技術分支深度學習。人工智慧對資料及隱私之侵犯，也導因機械學習是以資料學習式之演算法(圖 8 參照)，過程中所大量訓練模型的資料被轉化成個人資訊(圖 25 參照)，自動化描繪每位當事人的特徵，進而可能侵犯該當事人隱私，而如此之隱私近年來被廣泛地探討，其中具代表性的報告當屬聯合國人權理事會(Human Rights Council, UN)之報告。


聯合國人權理事會在 2021 年 9 月 15 日發布《數位時代的隱私權》(The right to privacy in the digital age)²⁵⁷，該份由聯合國人權事務高級專員辦事處(Office of the

²⁵⁴ Bench-Capon, T., Araszkiwicz, M., Ashley, K. et al (2012). A history of AI and Law in 50 papers: 25 years of the international conference on AI and Law. *Artif Intell Law* 20, 215–319. <https://doi.org/10.1007/s10506-012-9131-x>.

²⁵⁵ Lawrence Lessig (1999), *Code and Other Laws of Cyberspace*, Basic Books. ISBN 978-0-465-03913-5

²⁵⁶ Balkin, Jack M., The Path of Robotics Law (2015/05/10). *California Law Review*, Forthcoming, Yale Law School, Public Law Research Paper No. 536, Available at SSRN: <https://ssrn.com/abstract=2586570>

²⁵⁷ United Nations High Commissioner for Human Rights (2021/09/15). *The right to privacy in the*



High Commissioner for Human Rights) 出具之報告，分析了國家和企業廣泛使用人工智慧，包括自動化決策和機器學習技術，這些技術正面而言可以成為一股巨大的力量，幫助社會克服當今時代的一些巨大挑戰，並相對探討技術如何影響隱私權和相關權利。該份報告一開頭就指出”隱私是一種基本人權(The right to privacy is a fundamental human right)”²⁵⁸，該份聯合國報告亦強調了人工智慧可能對隱私在各個方面可能侵犯，並舉例數個對隱私權和相關權利的影響關鍵。聯合國示警人工智慧科技對人權的威脅，並呼籲各國在保護個資與隱私配套措施到位以前，重視人工智慧生物特徵辨識技術等先進以資料驅動技術(data-driven technologies)對於隱私及基本人權之潛在風險。

聯合國該報告中，分析了人工智慧，包括資料分析、自動化決策和其他機器學習技術，如何影響人們的隱私權和其他權利，包括健康權、教育權、行動自由權、和平集會和結社自由權以及言論自由權。聯合國高級專員認為：“大數據及人工智慧等資料密集技術(data-intensive technologies)現在幾乎滲透到我們社會、文化、經濟甚至社交等每個現代生活”。“許多政府及企業採用的人工智慧精準預測技術，用於每個個人之分析、剖析、財富狀況、分類，並可能確定人的權利抉擇，影響當事人一生的關鍵事項，而這一切都已經被技術自動化(Many systems used by Governments and business enterprises are built for that precise purpose —maximizing the amount of information on individuals in order to analyse, profile, assess, categorize and eventually make decisions, often automated, about them.)”。²⁵⁹”

該報告著眼於國家和企業經常急於納入人工智慧應用程式，而未能進行盡職調查與採取配套措施。而如今已經有許多因為使用人工智慧技術而受到不公正對待的案例，比如因為人工智慧程式判定下具有條件上缺陷而被拒絕享受社會保障福利的既有弱勢族群，或者因為面部識別有缺陷而被因此被刑事拘捕之無辜當事

digital age, Report of the United Nations High Commissioner for Human Rights.
<https://www.ohchr.org/en/calls-for-input/2021/right-privacy-digital-age-report-2021>

²⁵⁸ United Nations. *Universal Declaration of Human Rights, article 17.*

<https://www.un.org/en/about-us/universal-declaration-of-human-rights>

²⁵⁹ United Nations High Commissioner for Human Rights, *supra* note 257, at 5.



人等歧視案例。

該報告詳細介紹了人工智慧系統如何依賴大型資料庫，並以多種且不透明的方式蒐用和分析有關個人的資訊，而其用於建構人工智慧模型的資料可能是不準確、錯誤、歧視、過時的或不相關的;資料的長期儲存也帶來了特殊的風險，因為資料將來可能會以現有知識未知的方式被利用。人工智慧技術執行對人類行為模式的推理、預測和監控功能，包括尋求對當事人行為模式的分析與預測，自動化剖析當事人，除威脅構成對當事人的隱私，也可能因資料或模型有誤導致偏見(bias)或歧視而引發了嚴重的問題。本文第二章即指出人工智慧系統依賴的有偏見的資料庫可能會導致具歧視之決策，這導因於依賴資料為驅動的機械學習/深度學習演算法(圖 10 參照)為現今之主流技術，而這偏見風險對於社會邊緣的弱勢族群、最缺乏資源的群體來說卻影響最為嚴重，甚至導致此類既有弱勢族群在人工智慧運作下的惡性循環。報告中也指出公司和國家還需要在如何開發和使用人工智慧技術方面提高透明度，但這困難來自於 1.政府和私人資料控制者的將人工智慧系統開發和運作基礎的資料環境、演算法和模型以營業秘密方式保護;2. 人工智慧/機械學習/深度學習等學習式演算法所訓練出的模型其內涵連程式設計工作者都難以詮釋。這些都是破壞公眾認識與瞭解人工智慧系統對社會或個人隱私影響的基礎，過程的不透明更加深大眾對人工智慧運用上的擔憂。

同理，在人工智慧/機械學習驅動自駕車環境中，因為使用非常多資料、個資，且蒐集、自動化處理及決策複雜、涉及營業秘密、缺乏透明及可追溯性，導致民眾缺乏信任，各國逐漸對自駕車個資規範也彰顯探討人工智慧自動化決策下偏見或者歧視議題的重要性。

二.生物特徵影像辨識技術相當成熟且應用廣泛

生物特徵辨識資料被列為敏感性資料，其法規管控標準高於一般性資料，故有探討相關技術在自駕車上運用的狀況，並說明其利用的必要性。生物特徵影像辨識技術，包含人臉辨識、眼動追蹤、步態分析等技術已經相當成熟，除了價格低廉且性能成熟穩定，也因為相關技術已發展多年，有許多商品化產品在販售，是故大

樣運用在包含智慧自駕車上是可預期的，且近年來因為應用廣泛且規格特殊(如：低延遲，高度資料整合)，廠商將演算法直接寫入晶片產品，更是大幅降低應用於智慧自駕車成本與提高整合運用的機會。

同樣的，其他的生物感測器如心跳、溫度、血壓計等一樣多廣泛應用在各層面。這些感測器如同人工智慧/機械學習自駕車的感官裝置，將不同型態與不同資訊彙整到自駕車上，形成不同的資料庫。這些巨量且多樣的資料掌控與資料庫間串接，對於資料控制者塑造一個資料與個資寶庫;相對的，也因為這些成熟的技術與完整的資料庫，及商業上應用的誘因，也引起諸多隱私侵犯的疑慮，甚至部分國家地區禁止使用的管制趨勢。而自駕車的生物辨識，因為可能與生命安全相關，故其管理上不會只有單方面考量，以下是相關技術應用之介紹。

三.生物特徵辨識在自駕車上應用

駕駛者監控系統 (Driver Monitoring System, DMS) 廣義為監測駕駛員的使用環境，包含車外狀況與駕駛人的生物資訊。駕駛者監控系統主要監控駕駛者的身體、生理或行為特徵等生物特徵，如駕駛者分心與疲勞、心跳、眼球移動、人臉辨識、聲音偵測等，可為行車安全多加一道防線。從圖 43 可分類為生物特徵(Biometrics)、專注度(Visual Attention)、情緒(Emotion)、駕駛行為(Driving Behavior)與駕駛特性(Driving Style)等。此外，還有車外環境及車況的監測等，都是廣義的 DMS 系統的一部分。上述資料有很大部分都屬個資，且很多在不同國家之個資保護法規皆屬於敏感性個資的範疇。

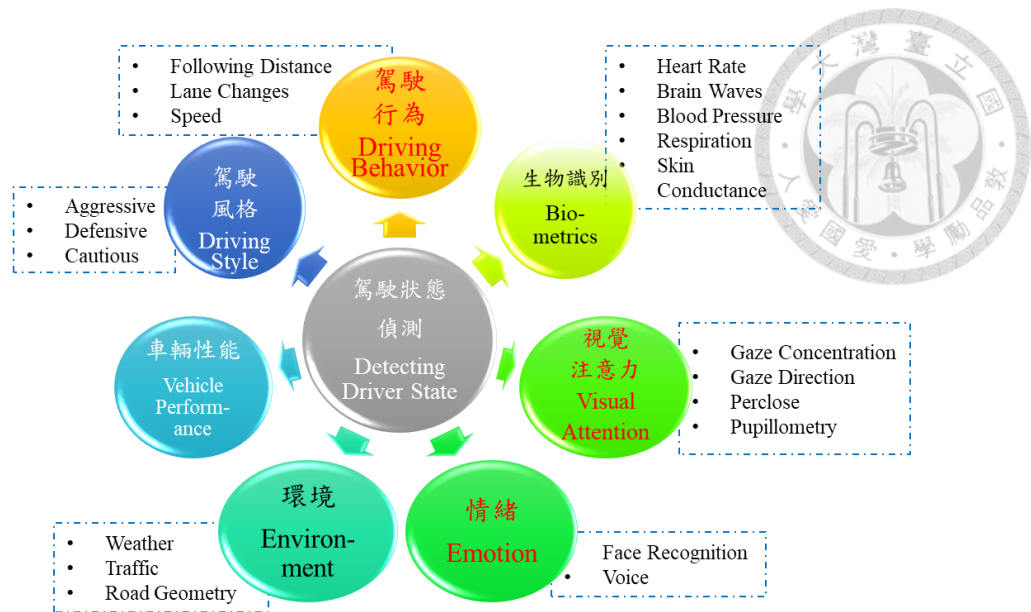


圖 43. 駕駛生物特徵偵測，包含人臉、聲音、心跳等一般及敏感個資。資料來源：IEEE²⁶⁰；
本文整理

歐洲議會已更新了其《一般安全法規》(General Safety Regulation, GSR)²⁶¹，確定了要求安裝 DMS 的車輛類型，歐盟新車安全評鑒協會(NCAP)也正在完善其 DMS 測試規程²⁶²。

四.公權力介入資料庫

為保護隱私、提高透明度暨提高國家對資料的主權，目前先進國家法規趨勢是除要求資料能留在國家境內，亦有探討是否由國家來建立公用資料庫，以保障國家資料經濟的提案。例如 2021 年歐洲委員會提出一個關於歐洲數位身分(European Digital Identity)的框架，建議建立「數位錢包」(digital wallet)的身分認證，可以在歐盟成員國間使用，用來存取公共服務或是儲存文件²⁶³。

²⁶⁰ Joseph F. Coughlin, Bryan Reimer and Bruce Mehler (2011). Monitoring, managing, and motivating driver safety and well-being. *IEEE Pervasive Computing*, 10(3),14-21.

²⁶¹ Junko Yoshida (2021/02/03),《能讓 ADAS 和 DMS 協同工作嗎?》，EETIMES。

²⁶² 蘇一峰 (2022),《智慧座艙監控技術介紹》，ARTC，載於 https://www.artc.org.tw/chinese/03_service/03_02detail.aspx?pid=13645 (最後瀏覽日：2022/4/30)

²⁶³ May (2021/06/17),《歐盟宣布歐洲數位身分和錢包框架預計 2022 年 9 月推出》，科技產業資訊室 (iKnow)。載於：<https://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=17927>



前述理念套用在自駕車上，因為自駕車資料巨大且隨時更新，此外資料格式多元無統一標準且多屬非結構式資料，由國家資料庫來管理是否適當？需要更多專家學者的進一步探討。

我國《個資法》於此部分並沒有特別規定，境外傳輸也較寬鬆。未來針對自駕車個資是否要由國家介入管理，可觀察各國的規範走向。

第三項 自駕車與個人資料之關聯探討

隨著自駕車興起及人工智慧與聯網技術的大量運用，自駕車個資問題也跟隨著被探討。然而事實上，如同網際網路(Internet)之於個人電腦，聯網車輛(connected vehicle)興起，許多相同的個資問題如前「聯網車」已經被歐盟所注意，以下綜整智慧自駕車上個資的可能問題：

一. 自駕車資料有許多當事人足跡，資料容易轉化成個資

在探討個資保護之前，可先探討資料與個資間關聯。自駕車雖有巨量的資料，但是否代表這些資料就會違反個資保障及侵害隱私？若非個人資料，自無探討個資保護之必要。

自駕車隨著駕駛的意識從出發地點到目的地，過程中除了駕駛及乘客的人行為、影像、對話音訊、行車的軌跡及生理辨識，另外還可能包含用路人及周遭車牌資料等都可能被記錄且分析。這些基於當事人的資料因為可能因為自駕車上的技術，被大量蒐集、高速計算、儲存、透過資料結合等等，巨量資料被轉換成個資並且利用，並且透過自動化軟體**持續不斷的監控、自動化個人檔案剖析**，進而可能侵犯當事人的隱私。

二. 自駕車的資料量巨大且易於串接

如本文第一章所述，自駕車本身亦是聯網車，運作上除了車與車間相連，亦會與智慧城市的感測器資訊相通，資料間容易結合。如本文表 8 對於隱私權之侵

害，包含個資的監控、匯集、識別等可能的侵害態樣，在巨量及聯網的狀況之下是否相較傳統車輛具有較高侵害人們生活隱私的可能？

此些問題過去在傳統且非聯網的車輛不容易被重視，或者有基於當時科技而管制的法規有其侷限。而如今因為先進技術導入智慧自駕車，故而可能引發對於當事人的隱私侵犯機率大幅提升，其中最具代表的就是車輛 GPS 紀錄，已經被 GDPR 明文例示為個資；從過去行車紀錄器案例到自駕車的多元攝影機新型態，是否尚有個資保護與運用間平衡討論空間？個資保護法規是否應該隨著科技的進展與日俱進？

三. 自駕車內隱私的期待

基於一般大眾對於車輛的認知，私家汽車除了是一種交通工具，也代表一個私人領域，人們可以在其中享受自主決策旅程與通話、活動之自由，普世對於車內的空間及或活動具有一定程度的隱私期待，符合本章第二節所述之空間及生活私密隱私權之保障範疇，是故在自駕車的個資及隱私之保障，是否應有特別的規範？申言之，其個人資料不論一般個資或敏感性個資之蒐用是否該有更細膩的規範？

第四項 人工智慧自駕車的個資問題小結

綜合本節所討論，自駕車-人工智慧-個資間的關聯如下圖 44 之所示，是自駕車-人工智慧-個資三者間爭點的總覽。本章以智慧自駕車的框架下，分別介紹「自駕車」、「人工智慧」及「個資」三者的定義與意涵，並分別說明「自駕車-人工智慧」、「自駕車-個資」、及「人工智慧-個資」兩兩結合下可能產生的議題。圖中紅字部分為本文所提出尚未見聞於現有法律文獻，紫色為先前文獻業據涉及，但套用到智慧自駕車領域有所不足，本文提出補充。

本文自駕車之自駕等級區分依據 SAE 定義，分為 0~5 級共 6 級。就自駕車與個資保護之討論，應先探討自駕車之個資/隱私保護之意涵，本文第一章指出不僅是一種交通工具，私人汽車也具有私人空間的意涵，在此空間理當有更高的隱私期待；自駕車也是一種機器人態樣，應符合機器人三原則，以安全為最高原則；智慧自

駕車也是智慧城市的一環，資料運用與個資保護可能影響著都市中的每一個人；此外對於車外用路人的個資討論尚未模糊不清之處，例如：1.車外用路人個資蒐集的必要性？2.有哪些個資？3.是否因公示性排除個資法保護？國際間有關自駕車個資規範為何？綜上，自駕車的個資/隱私保護尚有許多值得探討之處，也引發一個基礎問題，資料-個資-隱私三者間之關係？本文第二章也探討個資與隱私兩者的差異與關係。隱私權被視為基本人權，若有現有個資法規規定不清的情景，應回到《個資法》保護隱私權及人格權的立法理由上，雖然隨著各國對於隱私見解不同，相異國家地區個資保護法規規範不盡相同，但各國其立法理由值得我國參考。

人工智慧技術，本文第二章說明人工智慧發展歷史，並明確說明與本文探討相關的是第三代技術-機械學習/深度學習，此種機械學習演算法因已被證明在圖形辨識(圖 6 參照)、語音辨識等優於人類決策，加以機械學習/深度學習是為資料驅動的學習式演算法，是故採用資料/個資有其必要性，且資料必須更新。本文也提到機械學習之特性，也使得決策不透明且難以歸責的問題浮現，再加以資料若有偏誤，會導致偏見之結果，此些爭議已見於人工智慧之報告，但落實於自駕車之運用場景，因事關生命法益，更顯得資料利用與管理之兩難。智慧自駕車以人工智慧/機械學習為大腦，結合其他先進技術如物聯網、大數據及雲端運算等結合，更可能衝擊現有個資法之原則 (表 21 參照)。




圖 44. 自駕車-人工智慧-個資三者間關聯與必要性表示圖。圖中紫色字體為先前文獻已有初步探討，本文補充；紅色字體為本文提出。資料來源：本文整理

以人工智慧驅動的自駕車個資研究，自駕車-人工智慧-個資間的緊密相依，其必要性與產生的議題，三者綜合觀之才能鳥瞰智慧自駕車個資問題所在。綜合前述論述，可以安全必要性與否整理技術對個資處理原則如下表 21，以利後面章節討論。前揭技術如人工智慧/機械學習、OTA、資料融合、車外用路人之生物辨識等皆有安全上的資料蒐用必要性，其對應的可能衝擊如 OTA 之使用下，硬體規格必須高於出廠時之需求以利使用軟體更新，與蒐集限制原則有違。此點在《汽資安全規定（試行）》的第六條有具體規定要求確定攝像頭、雷達等的覆蓋範圍、解析度之精度範圍適用原則；再如前者所提的人工智慧/機械學習為資料驅動之學習式演算法，可能衝擊的包含個資的認定(廢棄資料)、蒐集限制原則、目的特定原則、公開透明原則及刪除權等；資料融合與車聯網衝擊資料結合、對照、組合、連結等。以表中羅列，可知智慧自駕車之新興技術運用下，有許多現行《個資法》窒礙難行之處。此外，還有已經被重視的 GPS 移動軌跡，反而並無安全上之必要，但 GDPR 與《汽資安全規定（試行）》都已經被明文例示為個資保護標的。

表 21.安全必要性觀點探討技術對個資資料處理原則可能衝擊。資料來源：本文整理

技術	是否有安全之必要	可能衝擊之個資資料處理原則
OTA(空中下載技術)	是	蒐集限制原則(硬體高於當時軟體規格)
AI/ML 及大數據	是	個資的認定(廢棄資料);蒐集限制原則;目的特定原則;公開透明原則;刪除權
資料融合(Data Fusion)	是	資料結合、對照、組合、連結;個資的認定
車聯網	是	資料結合、對照、組合、連結;個資的認定;傳輸權
GPS	否	資訊隱私
生物辨識(人臉;步態)	是	車內：基於安全或車輛環境監控之個資，尚無明確規範 車外：個資的認定;個人參與原則;公開透明原則;個資法排除適用

第二節 對車內駕駛及乘客個資保護之規範




目前自駕車對於車內駕駛與乘客之個資，都有基本的要求，包含資訊安全以及資料保護、資料的流向和資料的使用的決定權在自駕車擁有者和使用人的身上，美國《未來載具研發中的生命安全確保法案》，要求汽車製造商於銷售無人載具前，應制定隱私保護計畫，歐盟網路和資訊保安局（EU Agency for Network and Information Security）亦公布了關於智慧汽車及網路安全的研究，並建議於智慧汽車發展的過程中，應注意對個人資料的保護。各國政府都有要求自駕車業者必須保護資料的完整性，以及必須投入大量心血在網路安全的研發上面。

最高法院於民國 107 年 5 月 3 日作成 107 年度臺上字第 1096 號刑事判決(下稱《1096 號判決》)指出：“取得、使用行車紀錄器紀錄資料，仍應存有尊重他人隱私權之概念，倘藉口懷疑或有調查配偶外遇的必要，即恣意窺探、取得他方隱私領域，難認具有法律上的正當理由。”

《1096 號判決》事實為上訴人坦承確有自行取得他人車內所裝行車紀錄器的電磁紀錄，製成錄影資料作為證據向警提出，憑為控告他人涉嫌妨害家庭之證據，經原判決論以上訴人犯無故取得他人電腦相關設備之電磁紀錄罪刑的判決，上訴人不服提起上訴。《1096 號判決》首先指出「比例原則」：“……行車紀錄器顯示使用人當時行車的路徑、言談或活動等等，不免攸關個人私密領域及個人資料自主，因此如何取得、使用該紀錄資料，仍應存有尊重他人隱私權的概念。而社會現況，妨害他人婚姻的不法行為（如通姦、相姦），常以隱密方式為之，並因保護隱私權之故，被害人舉證不易，但允許當事人提出事實主張及證據，乃程序正義，而為憲法所保障人民享有訴訟權的展現，則被害人的訴訟權保障與不法行為人的隱私權保護，即可能因此發生衝突，如何從中調和，憲法第 23 條所揭櫫的比例原則（包括適合性、必要性及狹義比例原則），應可作為審查標準，具體以言，應權衡行使的手段，須可達成其目的；在所有可能達成目的的方法中，選擇最少侵害的手段；所欲完成的目的及使用的手段，不能與因此造成的損害或負擔不成比例。”

《1096 號判決》進一步指出所謂「無故」與「侵犯隱私」之條件：“……刑法第 36 章妨害電腦使用罪之「無故」，指欠缺法律上正當理由者，須綜合考量行為的



目的、行為當時的人、事、時、地、物等情況、他方受干擾、侵害的程度等因素，合理判斷其行為所構成的妨害，是否逾越社會通念所能容忍的範圍，並非其行為目的或動機單純，即得謂有正當理由。然而，夫妻雙方縱然互負忠貞、婚姻純潔的道德上或法律上義務，但其人格各自獨立，非謂必使配偶之一方放棄自己的隱私權，被迫地接受他方可以隨時、隨地、隨意全盤監控自己日常生活或社交活動的義務；倘藉口懷疑或有調查配偶外遇的必要，即恣意窺探、取得他方非公開活動、言論、談話等隱私領域，尚難肯認具有法律上的正當理由。上訴人未循合法途徑，擅自複製行車紀錄器記憶卡內儲存之電磁紀錄作為提控外遇的證據，顯已侵害他人對於其在該車內非公開活動的「合理隱私期待」。”

對於電磁紀錄取得與複製，《1096 號判決》指出，“……刑法第 359 條（破壞電磁紀錄罪）所規範之「取得」他人電磁紀錄，乃指透過電腦的使用，以包括複製在內的方法，將他人的電磁紀錄，移轉為自己所有的情形。故在「無故取得」電磁紀錄的行為態樣中，縱使原所有人仍繼續保有電磁紀錄的支配佔有狀態，然如行為人藉由電腦設備的複製技術，使自己同時獲取檔案內容完全相同、訊號毫無減損的電磁紀錄，仍該當此罪的成立。據此，上訴人擅自複製行車紀錄器記憶卡內儲存之電磁紀錄後，被害人縱使仍可使用該行車紀錄器之記憶卡，且其內所錄製影像檔案之電磁紀錄亦未減損，上訴人仍然該當刑法第 359 條所禁制的「無故取得」他人電腦相關設備之電磁紀錄罪。”

而他人是否具有「合理的隱私期待」，必須要滿足下列兩個要件才算：1.不受侵擾的期待已表現於外；2.該期待須依社會通念認為合理者。「車子」對於駕駛人或乘客，一般認知並非只是單純的交通運輸工具，更有可操控的私人空間的預期，所以車內人員的個資，包含 GPS 路徑、車內影像、車內人員交談、車內活動等都應以更高的隱私期待來觀之。以下就幾個面向來探討目前車內駕駛與乘客之個資問題。

第一項 對駕駛或者乘客的個資蒐集是否有公眾利益與保護生命法 益之目的？

就目前所知道的自駕車技術或輔助駕駛技術來分，可以安全必要性作為初步區分，目前包含 GPS 位置紀錄、以錄影或錄音並持續偵測、分析載具內使用者的對話內容等，都屬於非強制之要求，對於自駕車之安全的關聯性也並非直接或高度相關；而自駕車判斷駕駛手是否離開方向盤或者是否離開駕駛座等行為，屬於與安全相關，有其必要性。

對於前面非關乎安全之蒐集資料或者個資之行為，若非法規另有規定，可參照目前手機用戶與 App 開發商或者手機製造商對於資料蒐集、處理與利用之合法管理規範，可回歸駕駛或乘客與自駕車營運企業間約定。在歐洲 GDPR 第 6 條第一項(f)款規定：「……為資料管理者或第三人合法利益(legitimate interest)所必要」即得蒐集、處理或利用一般個人資料；但「資料當事人(特別是兒童時)對該資料的保護，具有更重要的利益、權利或自由者，不在此限」。此即所謂利益平衡(balance of interests)條款。而該規定旨在適應現今社會個人資料蒐集多變的情況，進而平衡個人資料保護與個資的合理利用。

在歐盟市場相關車輛及相連結之服務除應遵守 GDPR 規定外，並補充以下五大原則：1.確保車輛製造商處理方式的透明性；2.提供客戶選擇；3.資料保護為必要考量；4.維護資料安全；5.處理個資應考量比例原則。此意味著，只有在當事人同意下，資料控制者方能將之個人資料提供給協力廠商，協力廠商也僅於當事人同意約定上，將資料用於該商業目的。此外，除依據服務契約有提供地理位置之必要或其他賦予例如緊急呼叫之緊急或安全上法律義務，否則客戶將可取消其車輛和所提供服務之地理位置追蹤功能，此亦適用於車輛製造商將個人資料傳送給相關服務提供商之情況²⁶⁴。

²⁶⁴ 潘俊良 (2017)，前揭註 144，頁 60。

但對於前述有關安全性之監控，就必須探討是否合乎目前個資法之規定？或者應該有如歐盟駕駛者監控系統之特別規定，讓保障生命安全之技術得以在一定的框架下自由的開發？



第二項 資料是否等同於個資？人工智慧與大數據下的挑戰

綜上前述各章節分別對「資料」、「個資」之探討，在自駕車所蒐集的巨量數據中，是否就等同個人資料？若為「個人資料」，是否屬《個資法》所謂之「個資」？

我國《個人資料保護法》對個人資料定義為「自然人之姓名、出生年月日、國民身分證一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。」個人資料保護法保護客體須具備直接或間接識別特定個人之性質，此與歐盟 GDPR 之定義大致相同，然而隨著技術的快速進展，對於間接可識別個人的技術不斷在發展，這些疑似個資是否有侵害隱私的疑慮？另外，在自駕車運作中，是否有部分特別的資料，例如 GPS 路徑，《聯網車輛與移動相關產品涉及個人資料處理指南》已明文例示為個資？如本文第二章所提到的廢棄資料，與自動化決策下的個人檔案剖析資料，在人工智慧與大數據等新進技術的運用下，這些資料到底要用何種標準來判斷是否為個資？

再者，對於基於安全性之監控，是否以目前技術可將疑似個資或個資，一則可以輕易去識別化以排除個資法之適用？二則對於部分個資，如車外的路人生物特徵，是否賦予該資料蒐用特別規範？

第三節 公開場合個資保護近似案例探討

自駕車運作的過程中，需要蒐集、傳輸大量的資訊，針對其可能會蒐集不特定人之資料且加以傳輸的行為，如同可移動之街口監視錄影設備。過往街口固定式監視錄影設備除了用以監控違規、犯罪行為並發生嚇阻作用之外，亦有助於案發後迅速過濾搜尋嫌疑人並作為證據之用，例如新北市警察局於 2013 年 1 月啟用與中

華電信合作的「e化天眼」租賃式監錄系統²⁶⁵，整合監視器、車牌辨識、地理資訊、警車衛星定位及報案等系統，另加入行車軌跡紀錄追蹤、智慧影像搜尋等功能，透過雲端監控大量快速運算，可協助警方快速篩選調閱監視器畫面，提供民眾全天候的安全保障。臺北市政府也於2013年7月1日公布實施「臺北市錄影監視設備設置管理自治條例」，市政府所屬各機關得基於維護公共安全、社會秩序、犯罪預防及偵查之目的，向警察局提出申請並經核准後於臺北市公共場所設置攝錄影音設備；2018年開始臺北市推廣「多功能」智慧路燈，不只監測車流、還有人臉辨識^{266;267}；2021年後台灣多個都市又將監視器結合人工智慧功能，不但能管控車流，人工智慧電眼亦能取締違停與併排²⁶⁸。自此，街口監視器不止有「蒐集」之功能，並同時具備「處理」及「利用」之作業。

然而，從另一方面討論，上述技術的發展往往是非公務機關遠快於公務機關，且資料之運用從正面來看對於治安或者防疫有所助益，然而相同技術應用在自駕車上也同步引發的對於個資保護及隱私侵害問題。

過往實務上有認為在如道路等公共場域中之個人資料，因第三人得以共聞共見致民眾欠缺隱私的期待，或者以《個資法》51條第1項第2款規定：「……於公開場所或公開活動中所蒐集、處理與利用而未與其他個人資料結合之影音資料，不適用個資法」（法務部99年4月13日法律字第0999009760號函、100年6月9日法律字第1000014276號函、102年1月28日法律字第10203500150號函、法務

²⁶⁵ 中華電信 (2013/01/25)，《新北市警局、中華電信共同打造全台最大警政雲》，載於：<https://www.cht.com.tw/zh-tw/home/cht/messages/2013/msg-130125-143952> (最後瀏覽日:2021年8月11日)

²⁶⁶ INSIDE (2018/05/31)，《智慧路燈：隱身民間的大數據基地！臺北全 16 萬路燈將變身 AIoT 基礎建設》，<https://www.inside.com.tw/article/13096-pmo-smart-street-light-project> (最後瀏覽日:2021年8月11日)

²⁶⁷ 自由時報 (2018)，《北市智慧路燈人臉辨識惹議 副市長林欽榮回應了！》，載於：<https://news.ltn.com.tw/news/politics/breakingnews/2436175> (最後瀏覽日:2021年8月11日)

²⁶⁸ 小丰子 (2022/2/10)，《小心荷包失血！全台 AI 交通科技執法路段懶人包》，最新科技新聞，載於：<https://www.kocpc.com.tw/archives/426264> (最後瀏覽日:2022年3月15日)

部 102 年 3 月 27 日法律字第 10203502790 號參照)。然而，大法官釋字第 689 號解釋理由書則闡述：「現今資訊科技高度發展及相關設備之方便取得，個人之私人活動受注視、監看、監聽或公開揭露等侵擾之可能大為增加，個人之私人活動及隱私受保護之需要，亦隨之提升。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。」²⁶⁹如今隨著監視器的普及、人臉辨識技術成熟只需約 100X100 圖元²⁶⁹，當事人可能被持續追蹤、資料可長久儲存且易與其他資料庫比對，各國對於公開領域的影像普遍都已經有了警覺，此一疑慮在疫情的足跡追蹤應用下達到了高峰，公開場所影像之蒐用並逐漸被大家所重視。從第 689 號解釋得到重要的觀念是 1. 公開場合之資料未必不受隱私權之保護；2. 個人隱私之侵害，不限於與其他個資之結合，亦包含「持續」的持續注視、監看、監聽、接近等行為。

基此，無論非公務機關或民眾運用錄影監視設備，除為安全考量、資訊保全證據、社會公益之外，亦應注意避免不法侵害他人的隱私或個資，遵守合理合法的界限，否則除了可能造成民眾的恐慌及亦有隱私違法侵害之可能。以下就數個案例及相關的法條做一探討。

第一項 Google 街景圖

一. 事實背景

2005 年，美國 Google 公司推出名為 Google Maps 的電子地圖服務，該電子地圖是將地圖及座標予以數位化，公開於網際網路上供不特定使用者免費瀏覽使用，兼併提供交通、店家商情資訊與導航等服務。2007 年，Google 公司在 Google Maps 的電子地圖服務項目下，推出 Google Street View (以下稱：Google 街景圖) 之功能，該功能具顯現電子地圖中街道的實境環景圖 (Panorama) 之功能，環視該道

²⁶⁹ 王維嘉 (2020)，《AI 背後的暗知識：機器如何學習、認知與改造我們的未來世界》，頁 232，臺北：大雁出版。

路沿線所實際拍攝影像。為了提供 Google 街景圖服務，該公司派出街景車、單人街景背包至各大街小巷攝取影像，爾後亦允許民眾貢獻者上傳圖片²⁷⁰。以 Google 街景車為例，其車頂安裝了球型攝影機進行 360 度環景拍攝的鏡頭。當 Google 街景車穿梭行進於大街小巷，該街道上的一切景物，包括人、車、房屋等，其影像都將被清楚攝影並儲存。

二. Google 街景圖所引起爭議

Google 街景圖功能的出現，引發不少爭議性的法律問題，因該功能取得之資料雖為公示資料，但內容廣泛且詳實紀錄，如車牌號碼、門牌號碼、用路人生活百態等均包含在內，且該資料可於網路上隨時瀏覽且持續被儲存，使特定當事人之個人資料處於隨時被不特定第三人蒐集、比對或被利用之狀態，對個人隱私及人格權有侵害之疑慮²⁷¹。如下圖 45 中，圖上左：兩個男人進入性商店；圖上中：一個女人在做不文雅的動作；圖上右：可能喝醉男人躺在草地上；圖中左：兩個作陽光浴的女生；圖中右：一個正在嘔吐的男人；圖下左：一個男人正在被逮捕。諸如此類的公示生活照片卻因為網路特性而影響當事人之生活，特別是即使部分圖片其實沒有拍攝到明顯的人臉或生物特徵，然居住當地的人、照片當事人熟識朋友，或者有心人第三人透過照片比對、搜尋或與其他資料之比對，依然可分辨出照片中特定的當事人。以下就 Google 街景圖與個人資料保護法適用之探討。

²⁷⁰ Google 地圖，街景服務，<https://www.google.com/intl/zh-TW/streetview/explore/>

²⁷¹ 謝碩駿 (2018)，〈Google Street View 法律問題初探：公物法與個資法之視角〉，《臺大法學論叢》，第 47 卷第 2 期。

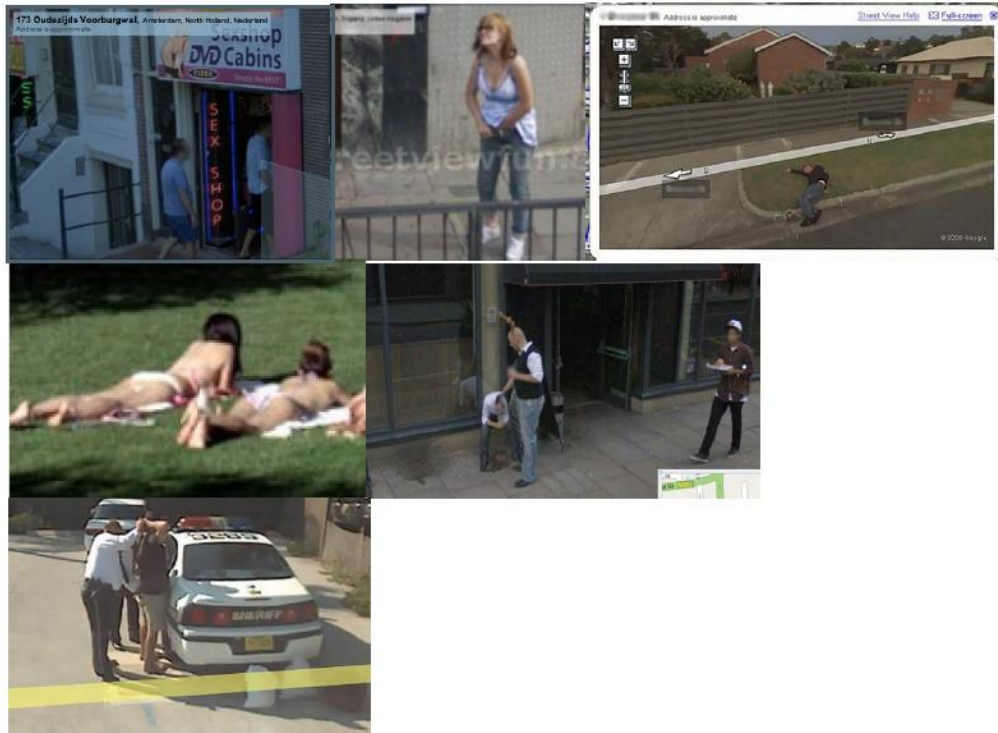


圖 45. Google 街景圖爭議圖片。資料來源：Privacy Rights in the Age of Street View²⁷²

三. Google 街景圖所拍攝影響是否為個資法所定義之個資？

《個資法》第 2 條第 1 項第 1 款將個資定義為：「個人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料」。在此所稱之「個人」，依據《個資法施行細則》(下稱：《個資細則》)第 2 條之規定指「現生存之自然人」。在前述定義下，《個資法》第 2 條明示之個人所屬資料，已被立法者劃入個資的範疇，但至於不在該條明文例示的資料，是否屬於個資，判斷標準則為：「能否從該資料直接或間接識別某一特定個人」。所謂「得以直接方式識別」之個資，指僅以該資料不須與其他資料結合，便可辨識出特定當事人；「得以間接方式識別」之個資，依《個資細則》第 3 條規定，係指該資料，“保有該資料之公務或非公務機關....，須與其

²⁷² Ben Lopez (2010/10). Privacy Rights in the Age of Street View, *ACM SIGCAS, Computers and Society, Volume 40 Issue 4*, pp 62–69. <https://doi.org/10.1145/1929609.1929617>

他資料之對照、組合、連結等始能辨別該特定之個人”。

對於評斷某一資料可能辨識特定當事人之標準，在學說上有「絕對認定標準」以及「相對認定標準」兩種不同見解²⁷³。稽之前者「絕對認定標準」，以現今或現今可見之科技的發展，一筆資料在被處理或與其他資料對照、組合、連結之後，始得以識別特定個人，則該筆資料即屬個資，至於保有該筆資料之資料控制者是否有能力或意圖透過該筆資料識別特定當事人，則無關乎該筆資料是否屬於個資之認定。易言之，「絕對認定標準」下個資的認定標準具有「客觀化」、「絕對化」的見解，並取決於當今或可預見之技術足以讓該筆資料(不論結合其他資料與否)能辨識出特定個人，而不考慮資料控制者能力與意圖。反之，若採「相對認定標準」之認定，則一筆資料唯有在資料控制者有能力或意圖透過科技與資料庫與其他資料之對照、組合、連結，而讓特定當事人被辨識出來，則稱之為個資。易言之，若採取「相對認定標準」之見解，則何謂個資的認定就變成「相對化」且為個案之判斷，舉例某資料或個資的控制者若：1.沒有能力或意圖；2.查詢上有困難；3.耗費過鉅等因素無法辨識出特定當事人，那麼該筆資料或個資對於該資料控制者而言就不視為是個資。

綜上，「相對認定標準」由該資料控制者角度判斷是否得以直接或間接方式識別，而非「依據當今技術成熟度，或在理論上得以直接或間接方式識別」。綜上可得知依據現行我國《個資法施行細則》第 3 條對於「如何認定資料是否具有間接識別性」，採取的是「相對認定標準」。

於此案例中，因 Google 街景圖平台上供大眾瀏覽的街景影像，因為被放置照片具有「不特定之第三人」可「長期」觀看之特性，且因為數位化容易被不特定之第三人處理比對，或俗稱的「人肉搜索」，在未去識別化前一般認為應屬個資範疇。

²⁷³ 黃耀賞 (2015)，〈淺談「得以間接方式識別特定個人之資料」〉，《科技法律透析》，201501(27:1 期)，頁 35

四. Google 街景圖是否可引用個資法 51 條排除適用

Google 街景圖若要引據《個資法》第 51 條第 1 項第 2 款「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人資料結合之影音資料」此一除外規定，則必須符合「於公開場所或公開活動中所蒐集、處理或利用之影音資料」以及「未與其他個人資料結合」這兩個要件。由於 Google 公司是在道路上拍攝街景影像，並將街景影像資料放置在任何人均可透過網路連結進入的 Google 街景圖網站供大眾瀏覽，就此而言，Google 街景圖所涉及的，確實是「於公開場所或公開活動中所蒐集、處理或利用之影音資料」。

五. Google 街景圖模糊化處理是否已去識別化?

我國關於個資去識別化實務發展，依據我國個資法第 1 條立法目的在個資之隱私保護與資料合理利用之間尋求平衡，實務上爭議在於達到合理利用目的之個資處理，參酌法務部 103 年 11 月 17 日法律字第 10303513040 號函說明「個人資料，運用各種技術予以去識別化，而依其呈現方式已無從直接或間接識別該特定個人者，即非屬個人資料，自非個資法之適用範圍」，在保護個人隱私之前提下，資料於必要時應進行去識別化操作，確保特定個人無論直接或間接皆無從被識別。若從前面我國採取「相對認定標準」，所以去識別化之圖片應屬非個資資料。

然此一個資之相對認定標準尚有許多爭議，本文於後將詳述各國對於個資定義及去識別化之討論。

第二項 街口傳統監視器

一.傳統監視器

在此討論傳統監視器拍攝之畫面，是否屬於個資範疇?民國 103 年(西元 2014 年) 2 月 24 日法務部法律字號第 10300511510 號函：「...來函所詢之錄影資料(指民間監視(錄)器)，倘因含有車號、經過時間、經過地點等，且技術上貴署(指警政署)仍得透過其他資料之比對而識別該車輛所有權人或使用人，即屬個人資料保

護法(下稱個資法)所定「得以間接方式識別」之個人資料(101年11月8日法律字第10103109010號函參照)。在此函文中強調的是1.資料是否具與當事人連結的特性;2.與其他資料庫比對。另外以此論點而言,一分資料是否屬個資,必須在資料「處理」階段才能做出判決,「蒐集」階段並無限制。

2020年10月26日,臺中高等行政法院作出109年度交上字第59號判決(以下稱第59號判決)。針對街口監視是否有個資法之適用問題,該判決認為,「……公務機關以街口監視器攝得之車輛監視錄影畫面,如**包含車牌者**,為個資法規範之個人資料。而此監視錄影即使尚未實際識別被攝錄者,仍可對被攝錄者之人格自由發展產生妨礙,是個人資料保護法乃明文規範之個人資料蒐集、處理及利用行為²⁷⁴。」

第59號判決中提到上訴人主張:「各地方政府於重要街口設置監視器所攝錄之畫面,因其取得並無法律依據,侵害上訴人依個人資料保護法受保護之個人資訊,並無證據能力,不得作為本案裁罰事實之證據使用(參見臺北高等行政法院104年度交上字第78號判決、臺灣桃園地方法院103年度交字第203號判決、103年度交字第221號判決、104年度交字第18號判決、104年度交字第132號判決)。」對於車牌號碼是否符合個資法施行細則第3條:「保有該資料之公務或非公務機關僅以該資料不能直接識別,須與其他資料對照、組合、連結等,始能識別該特定之個人。」而認定為個資法第2條第1款之「間接方式識別該個人之資料」?第59號判決書說明:「又考諸監視錄影之目的大多在於取得『將來』可以辨識特定人之資料,在未實際識別前,因可能對當事人言行舉止、人際互動或社會生活產生自我抑制的效果,甚至因遭到濫用而使被攝錄之人產生隱私受侵害之恐懼,而對人格自由發展產生妨礙,是個人資料保護法乃明文規範個人資料之蒐集、處理及利用行為。」

這裡的問題癥結點在於蒐集的公開片面資訊與當事人的連結關係,以及是否

²⁷⁴ 臺中高等行政法院109年度交上字第59號判決,載於:
<https://law.judicial.gov.tw/FJUD/data.aspx?ty=JD&id=TCBA.109%2c%e4%ba%a4%e4%b8%8a%2c59%2c20201026%2c1>

可連結其他資料庫或個資系統，是公開片面資訊是否可稱為「(間接)個人資料」的關鍵？



二. 監視器影像人臉辨識

影像人臉辨識已經商業化多年，且廣泛應用在民眾的手機解鎖、海關通關判定及政府的刑事辦案業已多年，最著名的當屬中國大陸的天網系統。人臉辨識已經是相當成熟的技術，只需要約 100*100 圖元的畫面，就可以識別。目前監視器的生物特徵辨識，包含人臉辨識功能，因為技術成熟而應用過於廣泛，不斷有限制其使用的呼籲。然而，承前述車牌辨識，若以第 59 號判決之說明，自當屬個資之範疇。但若以相對標準說論之，若資料控制者並沒有與比對之個資資料，則單一監視器之人臉辨識，似乎並沒有《個資法》適用問題。目前市場上還是看到具有人臉的商業應用，具辨識功能的監視器在司法上尚有許多模糊空間。然而，緊接在單一辨識功能的監視器，近期加入人工智慧之聯網監視器，引起更多的爭議。美國業據禁用人臉辨識的規範，台灣雖有已有的對此應用的質疑與討論，但尚未見到相關的立法。在疫情下，許多公共場所及賣場，無論公務機關或非公務機關，都大量地使用人臉辨識及測溫來管理追蹤可能的患者，對於此技術的個資討論只局限於學者間。

三. 智慧監視器

近年來，監視攝影機不再只是單純用於被動紀錄影像，可以主動使用人工智慧/機械學習識別影像進行分析以輔助決策，並引起大眾的關注。由於直接在影像分析及推論上。目前台灣各地方政府已經在推科技執法，利用街口監視器結合人工智慧，自動判斷是否違法目前還有許多爭議，特別是人工智慧運用下的蒐集及處理結合一體，及其自動化決策的過程不透明，目前國內並沒有太多的討論，相信這塊也是未來爭議的空間。

四. 歐盟「使用攝錄影裝置設備處理個人資料之指南」

鑑於監視器設備和影像之使用對個人資料保護和隱私之影響，以及臉部辨識

影像潛藏的歧視風險等問題，歐盟資料保護委員會 (European Data Protection Board, EDPB) 依據數據保護影響評估 (Data Protection Impact Assessments, DPIA)²⁷⁵ 於 2019 年 7 月 10 日公布「監視器影像個人資料處理指南 3/2019」(Guidelines 3/2019 on processing of personal data through video devices)，說明如何在符合 GDPR 規範下處理個人資料，並在公布前揭指南後，又於 2020 年 1 月 29 日修正公布第二版指南。歐盟於 2020 年 1 月發布「使用攝錄影裝置設備處理個人資料之指南」(Guidelines 3/2019 on Processing of Personal Data Through Video Device, Version 2.0)²⁷⁶。在「使用攝錄影裝置設備處理個人資料之指南」(以下簡稱「錄影裝置個資指南」)背景說明時，就提到目前的監視器已經可能影響到個人資料權益。「監視器影像個人資料處理指南 3/2019」強調監視器影像資料之利用，必須避免目的外利用，且管理者應仔細衡諸 GDPR 第 5 條有關監視器之規範，並採取適當之預防措施，防止設備故障及潛在的風險等，並針對監視器處理個人資料之合法性、當事人(資料主體)權利、個資儲存和刪除等常見問題加以說明。必須注意的是，雖然根據 GDPR 規定，在單純的個人或家庭活動中處理個人資料，並非 GDPR 所欲規範之行為²⁷⁷，惟在使用監視器狀況下有關家庭豁免 (Household exemption)²⁷⁸之規定必須限制其解釋為僅限於與私人或家庭活動過程中有關之行為。是故，即便是在公共空間，如以監視系統蒐集與儲存個人資料，此種行為亦無法被認為是單純的個人或家庭活動，並應遵守 GDPR 之規範。

²⁷⁵ Data protection impact assessments (DPIA) According to Article 35 (1) GDPR controllers are required to conduct data protection impact assessments (DPIA) when a type of data processing is likely to result in a high risk to the rights and freedoms of natural persons.

²⁷⁶ EDPB, Guidelines 3/2019 on processing of personal data through video devices, Version 2.0.

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

²⁷⁷ 財團法人資訊工業策進會 (2020/12)，智慧建築安全監控資料應用之法制課題及對策之研究，內政部建築研究所委託研究報告。

<https://ws.moi.gov.tw/Download.ashx?n=5pm65oWn5bu656%2BJ5a6J5YWo55uj5o6n6LOH5paZ5oeJ55So5rOV5Yi26Kqy6aGM5Y%2BK5bCN562W5LmL56CU56m25oiQ5p6c5aCx5ZGKLnBkZg%3D%3D&u=LzAwMS9VcGxvYWQvNDA0L3JlbGZpbGUvOTQ0S8yMTM5MDkvNjQ2ZGVlYmYtZjZhOS00ZDNjLTlmMmUtMTM3NDQwZGM3MDQ1LnBkZg%3D%3D>

²⁷⁸ GDPR, Article 2 (2) (c)

第三項 影像式行車紀錄系統



傳統影像式行車紀錄系統主要包含車用攝影裝置、影音主機、影像判讀演算法及音訊蒐集等各種軟硬體項目組成，現今影像式行車紀錄系統結合 AI 影像處理演算法，已提供警示及偵測等功能，使影像式行車紀錄系統不僅有釐清事故責任歸屬，亦具備降低事故發生率、提升行車安全之智慧功能。

桃園地方法院 102 年度桃簡字第 66 號民事簡易判決，原告認定被告將行車紀錄資料上傳至影音平台 youtube，縱使該影片設為「非公開影片」，但已有逾百人觀看過該影片，加諸影片內容**包含原告的车牌號碼**，由於原告與被告為同一公司之員工，故公司其他同仁，足以輕易得知原告之身分，桃園地方法院認為駕車雖係社會活動之一，“惟我國車號是由主管機關依據統一規格配發，除車主個人自行公開外，僅公務機關得依職權查詢，並非一看即知該車號屬於特定車主，故解釋上並未符合「直接或間接方式識別該個人之資料」之要件，因此，**被告雖將內含原告車號的影片上傳至 youtube，惟因未能將其與原告特定**，自不生侵害原告個人資料之問題。”該判決法官認為傳統影像式行車紀錄因非可直接或間接識別當事人，不符合個資之要件。

行車紀錄器隨時隨地蒐集影像的特性，使駕駛在意外發生時可以依據影像證據保護自身利益，惟近年隱私及資安疑慮備受重視，各國對於車載錄影設備有不同規範²⁷⁹。如下圖 46 之 VIA 2020 年報告，該年全球使用行車紀錄器的規範概況圖示，以個別地區使用行車紀錄器與否：紅色框標示葡萄牙、盧森堡及奧地利等國家於公共場合使用行車紀錄器或其他錄製設備是完成非法的，違法者將面臨高額罰金；在西班牙及英國使用行車紀錄器是合法的，惟不得公開於網路，若要作為交通事故之證據，必須交給警察單位；在北美洲如加拿大是可自由且合法使用行車紀錄器，在加拿大並可自由作為民刑事之證據，但美國雖之憲法保護公用影片之錄製，但私人錄製卻是各州不同。對於錄製影片之公開：在德國、英國及西班牙等，公開

²⁷⁹ 陳昆彥(2021/12/10)，《AI 技術使影像感測裝置如虎添翼》，IEK 產業情報網。

錄影畫面須模糊人臉及車牌;法國與比利時不能將影片公開;而最嚴格的葡萄牙、陸森堡及奧地利是禁止使用並有高額罰款。



圖 46. 全球 2020 年行車紀錄器使用概況。資料來源：VIA²⁸⁰

第四項 聯網車所拍攝之車牌

德國聯邦和各邦政府獨立資料保護機關會議及汽車工業協會(Verbandes der Automobilindustrie, VDA)於 2016 年 1 月共同針對聯網及非聯網交通工具之資料保護發表聯合聲明²⁸¹：如車輛為離線狀態，而將資料持續儲存車輛本身或覆蓋其記錄，當無生聯邦資料保護法第 3 條第三項所稱資料蒐集之行為，然而當資料以類似聯邦資料保護法第 6 C 條個人行動儲存和處理的介面輸出或於介面處理時，或車輛存儲的資料透過維修目的被讀取時，該資料則應受保護。反之如車輛為連線狀態，並將資料傳輸於後端伺服器儲存，即屬於資料蒐集行為。在連線狀態車輛的案例，接收個人資料之個人或機構將視為權責單位，即製造商及協力廠商服務提供商皆受聯邦資料保護法規範，例如製造商提供車輛加值服務，並將資料傳輸於後端伺服器儲存時，即為資料處理之權責單位。

²⁸⁰ Bria Rosenberg (2020/8/26), 《全球行車紀錄器使用概況》，威盛視角，載於：
<https://www.viatech.com/tw/2020/08/dash-cams-around-the-world-tw/> (最後瀏覽日：2021/11/30)。

²⁸¹ 潘俊良 (2017)，前揭註 264，頁 64。

按此規定，以車牌或其他資料是否有儲存、傳輸、連網作為資料是否為個資保護適用與否的判斷依據。我國車牌號碼辨識系統結合 E-tag 辨識系統，並聯結公司資料庫，若所蒐用之資料有聯結識別車主之可能性，乃屬個人資料而有《個資法》之適用（法律決字第 10403501110 號參照），應遵守我國《個資法》之規定處理。

目前 Tesla 的「哨兵模式」²⁸²就是循此模式儲存在車上記憶卡上，然而開放車主可手機觀看及控制是否有違精神，尚未看到相關案例。另外，依目前自駕車的狀況對前方影像的處理，其資料若屬個人資料之範疇，如本文第一章第五項《智慧自駕車再次衝擊個資保護規範》文中所提出之議題，對於涉及個資的蒐用、告知、同意與刪除等議題，以現行《個資法》之規定，實有窒礙難行之處。

第五項 防疫足跡

2020 年 Covid-19 傳染病席捲全球下，個人隱私、足跡監控與防疫公衛間的爭議更是隨時可見，與本文相關的就是人工智慧/機械學習與監視器資料，並結合其他手機防疫 APP 等個人資訊，其過程可能有個資與隱私的侵犯疑慮。防疫足跡其牽涉的適法性包含目的限制原則(purpose limitation)、資料最小化(data minimization)原則、透明性(transparency)要求、是否有告知與蒐用必要性之判斷，如：疫病調查或公共衛生在新興科技之發展下，包括相關個人資料傳送或交換時，蒐集資料範圍為何？非公務機關如商家透過民眾下載之 APP 所蒐集之個人資料，其告知後同意之程序與內容是否有依循個資法規，並遵守處理透明原則及消費者要求刪除之權利？是否有目的外之使用？這些防疫資料是如何被利用並儲存保管？保存之資訊安全要件及期限為何？

在個資法之規範下，主管之機關應針對上開資料以資料庫蒐集、處理、利用、對外傳輸及對外提供利用之主體、目的、範圍及方式等，暨資料之監管防護機制等重要事項，以相關法律規定之，且該規定應受法律明確性原則及比例原則之審查。

²⁸² Tesla 網站，載於：https://www.tesla.com/ownersmanual/modely/zh_hk/GUID-3C7A4D8B-2904-4093-9841-35596A110DE7.html (最後瀏覽日：2022/1/12)

前揭問題顯示出，即使在疫病之緊急狀況下之下，應用科技防疫時，基本之個人資料保護法規遵循之重要，而一些不明確之規範也有必要在藉著防疫經驗，漸進修改補足並滾動式調整。



第六項 以當事人權益無侵害作為合法事由之判斷依據

按我國個資法第 15 條及第 19 條規定，無論公務或者非公務機關只要在特定目的下個人資料蒐集或處理對於當事人權益沒有造成侵害，即可合法為之，此一規定是否有違當事人之個資自主決定權尚有疑慮²⁸³。在最高行政法院 106 年度判字第 54 號判決中：「……上訴人乃是為維護其等『個人資料隱私權』而提起主觀爭訟，則其等主張僅需排除其 8 人之健保資料，即可確保其等『個人資料隱私權』云云，亦需針對個案事實，指明隱私權可能受侵犯之程度及其蓋然率，方能謂隱私權有受侵害之虞。而上訴意旨對此亦從未為具體主張。」析言之，法官認為當事人應該主動提出其隱私權有受侵害之虞的具體主張，也據此作為上訴人敗訴的原因之一。

按前述之我國立法理由，理應當事人對於其個資有知悉、控制與刪除權利。未經當事人同意即蒐用個資，就有侵犯其資訊隱私權的疑慮，須正當合法理由來支持該蒐用個資之行為。對照 GDPR 第 6 條第 1 項規定，個資蒐用除了合法外，同項第 d 款規定須是為保護當事人的重要利益(“processing is necessary in order to protect the vital interests of the data subject or of another natural person”)。當蒐集或處理個資時，除引用我國《個資法》第 19 條第 1 項第 5 款「經當事人同意」外，亦可引用同項第 3 款「當事人自行公開」或第 8 款「對當事人權益無侵害」。單以對當事人權益無侵害無法構成合法蒐集、處理個資之條件，並無衡諸個資當事人的資訊隱私權，即使當事人公開之個資，並不代表同意任意第三人蒐用其個資，亦不等同該當事人放棄其刪除權利。

第四節 自駕車與個資保護之探討

²⁸³ 張陳弘，莊植寧 (2019)，前揭註 230，頁 106。

自駕車因為首要的功能是提供一個對駕駛、乘客及用路人安全的使用環境，而以人工智慧/機械學習驅動之自駕車所計算之基礎即是這些外在的巨大的資訊，並包含前述當事人的個人資料。



回顧我國《個資法》立法理由在於平衡人格權保障，促進個人資料之合理利用兩者。以過去案例的比例原則在於個資保護與社會公益，在本文智慧自駕車的利用場域下，自駕車除了生命保障之首要責任與義務，另外在減少排氣、減少塞車、降低能源消耗、提升使用者之時間價值等間接社會公益上的意義，法律的落實是在於權衡「個資保護」、「社會公益」與「生命法益」三者。以下就這三者的爭點作一說明。

第一項 生命法益之保護

若提到生命之保障，乃普世之最高價值。如前所述，不論將自駕車視為一個機器人，還是德國的自駕車《倫理指南》，無論對於駕駛、乘客、用路人還是動物的生命保障，都是自駕車設計的最高原則。

然而，哪些資料是可能有具有個資在其中？個資是屬於一般個資還是敏感性個資？蒐集前述資料對於自駕車運作的必要性？以下針對這些爭議問題作初步的說明。

一.用路人偵測的必要性

自駕車首重安全，且由於自駕車大都是在城市中運作，該場域因為狀況複雜，相對安全性技術也最困難，其中最直接與生命法益連結的包括用路人偵測與防撞的技術。如圖 47 物件偵測首要分辨出用路人與車輛等重要物件並做標示，如第二章人工智慧技術之說明，人工智慧/機械學習技術相較傳統規則性演算法更能協助辨識分別出更多的細節並予以標示並追蹤。人工智慧/機械學習技術的採用也是近年自駕車能走出實驗室，進入商品化進展的重要里程碑。

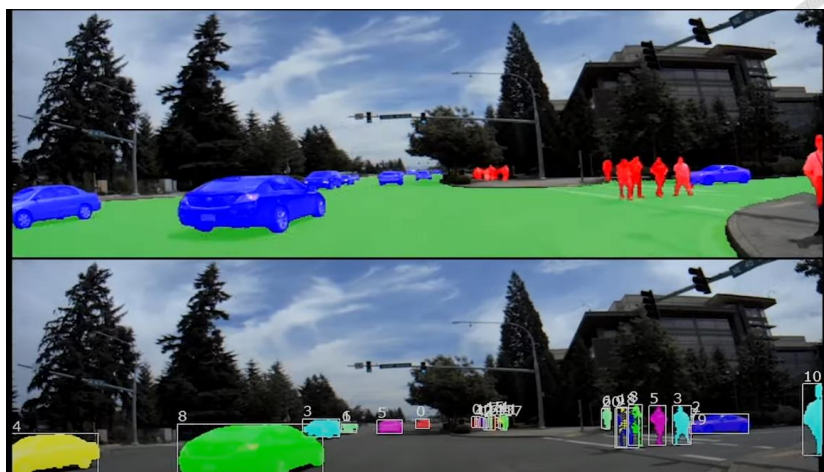


圖 47. 對於複雜的路況，首先要標示出車輛及用路人等重要物件²⁸⁴。資料來源：Nvidia

用路人偵測包含物件辨識與行為判斷等，自駕車的感測器，如影像感測器在偵測前方物件時，必須先辨識是否為自然人或其他物體，對於自然人再予以偵測其生物特徵並藉以判斷是否車輛要做出反應。在所述的生物特徵辨識，包含人眼辨識及步態辨識。人臉辨識主要判斷當事人是否有注意到車輛，包含如東京理科學²⁸⁵及車商 Ford 的人臉辨識²⁸⁶、Hyundai 的用路人行為預測²⁸⁷皆有開發相關技術。在 Ford 所申請美國專利 US10082796B2 中，如圖 48 自駕車偵測到用路人後，再以偵測人眼以判斷行為是否有注意到車輛，若用路人的眼睛沒有偵測到，可預估當事人可能沒有警覺(awareness)到車輛，車子就會以圖 49 之流程動作並做減速或煞車。

²⁸⁴ NVIDIA DRIVE Labs (2019/10/24). *How AI Helps Autonomous Vehicles See Outside the Box*. <https://www.youtube.com/watch?v=HS1wV9NMLr8&t=1s>

²⁸⁵ Shinya Saito; Yuki Ishii; Takeki Ogitsu; Hiroshi Mizoguchi (2015). Face Detection-based System to Sense Pedestrians At High Risk of Collision, *2015 6th International Conference on Intelligent Systems, Modelling and Simulation*. DOI: 10.1109/ISMS.2015.21

²⁸⁶ US patent no. 10082796B2, Pedestrian face detection,

²⁸⁷ Hyundai (2018/10/11). *Hyundai Cradle Invests in Perceptive Automata - Pedestrian detection for self-driving cars*. https://www.youtube.com/watch?v=yC4kYosO_Sk

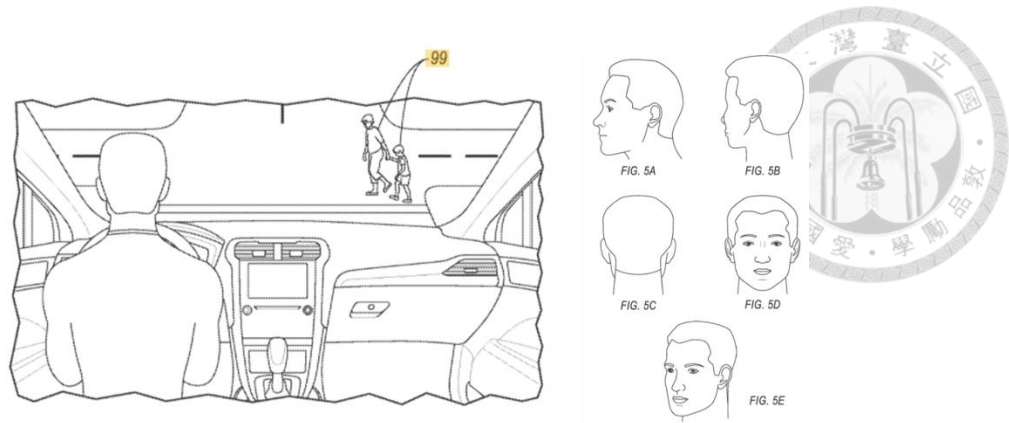


圖 48. 自駕車偵測到用路人後(圖左)，再以偵測人眼以判斷行為是否有注意到車輛(圖右)，
資料來源：US10082796B2

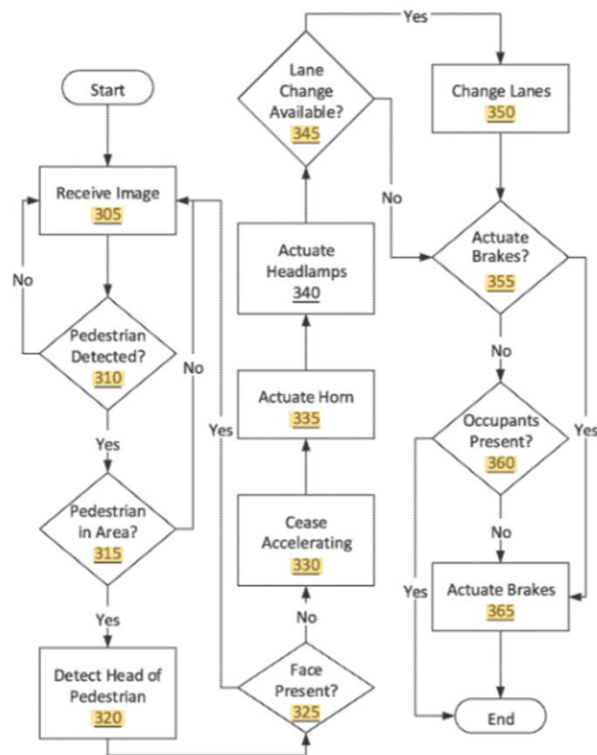


圖 49. 用路人人臉偵測與自駕車動作判斷，資料來源：US10082796B2

類似的技術也被車商 Hyundai 所採用，如圖 50 所示自駕車除偵測用路人外，並依據人臉與步態辨識判斷 1.行為對車輛的警覺程度(Awareness)及 2.過馬路的意願(Intention)。行為對車輛的警覺程度主要以人眼偵測判斷當事人是否知道車輛已經來了；過馬路的意願在於判斷被偵測的用路人是否有意願要橫越馬路。

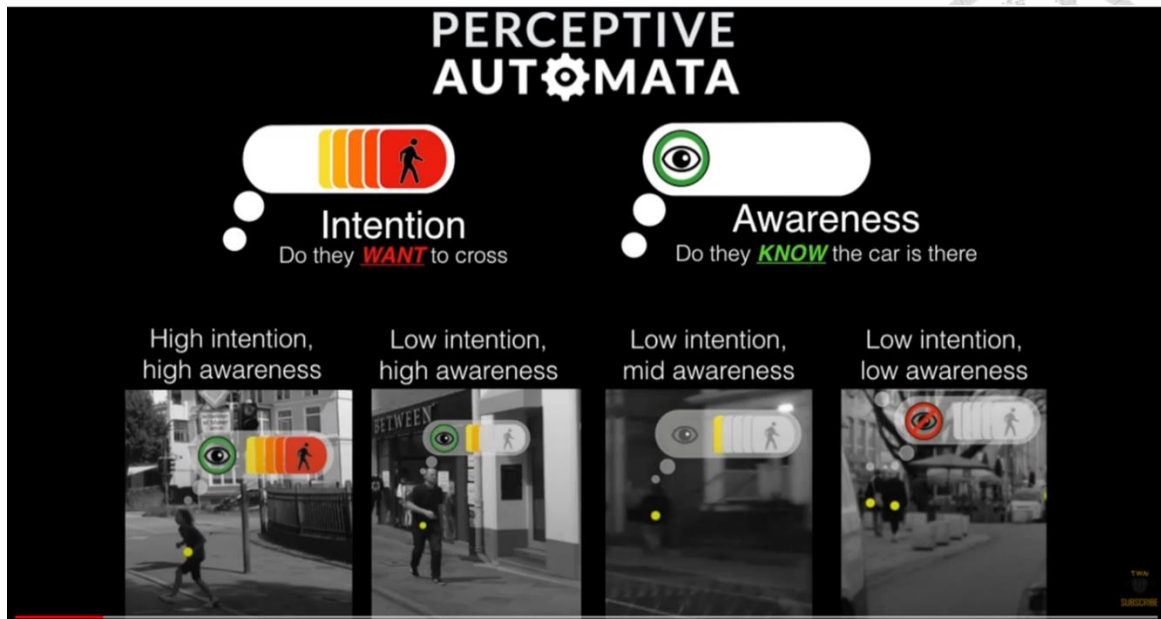


圖 50. 自駕車除偵測用路人外，並依據人臉與步態辨識判斷 1.行為對車輛的警覺程度 (Awareness)及 2.過馬路的意願(Intention)²⁸⁸。資料來源：Hyundai

這些生理特徵偵測技術，包含人眼與步態辨識，廣泛被應用於自駕車的使用場域，並為用路人的安全提供更多的保障。相對的，該如何管制個資以避免資料濫運用，也是值得探討的問題。

二.自駕車對車外用路人個資影響之探討

相對監視器對用車外用路人等的個資與隱私影響，自駕車相較又有更多的資料連結性。在此討論自駕車拍攝車外之畫面，是否屬於個資範疇?2020年10月26日，臺中高等行政法院作出109年度交上字第59號判決。針對街口監視是否有個資法之適用問題，該判決認為，公務機關以街口監視器攝得之車輛監視錄影畫面，如包含車牌者，為個資法規範之個人資料。而此監視錄影即使尚未實際識別被攝錄者，猶可對被攝錄者之人格自由發展產生妨礙，乃《個人資料保護法》明文規範之個人資料蒐集、處理及利用行為。

²⁸⁸ *Id.*

第二項 個資保護、社會公益與生命法益

綜前之所述，超越我國《個資法》當事人人格權保護與資料合理利用，本文自駕車個資討論環繞在如下圖 51「生命之保障」-「避免人格權受侵害」-「促進個人資料之合理利用」三者間之權衡。三者的在自駕車運用的場域下的意涵，與彼此間的權衡，將於後面章節詳述。

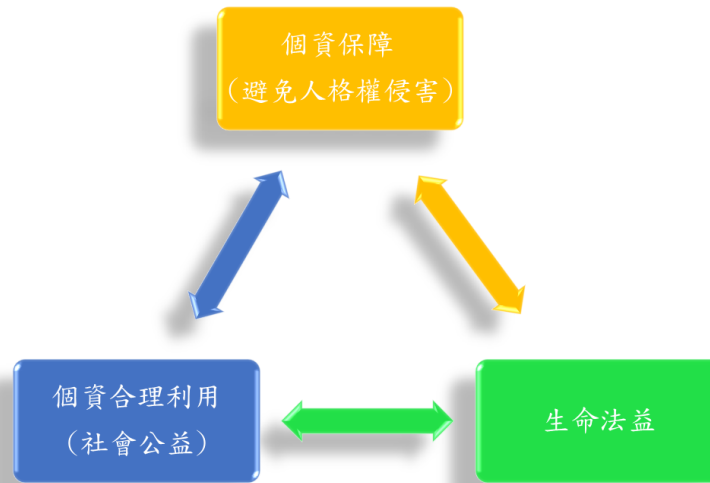


圖 51. 在本文智慧自駕車的應用環境下，是權衡個資保護-社會公益-生命法益三者。資料來源：本文整理

第五章 個人資料保護法與人工智慧機械學習驅動

自駕車之調和探討



第一節 技術與產業發展對個資法之挑戰

人工智慧、自駕車與個資三者影響現在人生活甚鉅，也因為三者的影響廣泛，相關研究雖如雨後春筍，但卻因為相關用詞差異、定義不清及研究範疇混淆，使得三者之跨領域研究混沌不明。故本文在前面章節先界定人工智慧、機械學習與深度學習、自駕車的定義與自駕等級；個資、個資保護法、隱私與隱私權等，以明確本文議論之主題與探討的範疇，聚焦三者間的互動與本章節所要探討智慧自駕車資料利用與個資保護的議題。

本文前面章節已經有提到包含大數據、廢棄資料、人工智慧與大數據結合的統計學習對於資料是否屬個資判定上的困難，及運用資料可能構成對隱私的侵害等問題。前述這些問題在很多先前研究就已經有提過，然而因為出發點差異且研究分散在不同領域的技術中，造成對於新興的自駕車個資保護有更多難以定義與判斷的模糊空間。以我國《個資法》第1條立法精神來看，我國因為相對重視個資的流通與運用，對於個資解釋空間及個資保護趨於保守，也導致許多判例與解釋上對於個資保護與資料利用的矛盾與衝突；相對的，與歐盟規定相較，**GDPR** 是將個人隱私視為基本人權，故其立法精神首要在於保護個資，所謂對於「個人資料」以廣義的定義方式，將任何可能連結特定個人的資料皆納入個資，但相對的在自駕車資料利用上是否過分偏向隱私保護而導致自駕車安全性及公益性技術發展上阻礙？綜上，不論何種定義，在新興科技人工智慧導入及本文自駕車的應用場域下，兩者是否都能適用？可能衝擊是甚麼？如何平衡個資保護-公眾利益-個資運用？

本章就從基本的原理與定義上去探討目前個資學術研究或個資法規上所忽略且易混淆的細節。並探討在人工智慧/機械學習驅動自駕車下資料利用與個資保護的衝擊。

第一項 資料與資訊(Data and Information)

資料(Data)與資訊(Information)為各國有關個人資料保護法上常見的基礎字彙，且兩個字有交叉引用的情形，如 GDPR 第 4 條：「『個人資料』指與已識別或足以識別的自然人相關的任何『資訊』(“personal data” means any information relating to an identified or identifiable natural person)」，此兩字彙是否指同樣的意涵？亦或者有兩個不同的保護標的？不同國家個資法上分別運用兩個字，在解釋或翻譯上也常有因人而異，例如依據線上 Cambridge Dictionary 對「Data」解釋為“information, especially facts or numbers, collected to be examined and considered and used to help decision-making, or information in an electronic form that can be stored and used by a computer”²⁸⁹。然而本文認為兩者有相當程度的不同，以下從「知識管理」、「大數據」、「數據科學」及「人工智慧/機械學習」多角度來詮釋其中差異。

以「知識管理」²⁹⁰(Knowledge Management, KM)、「大數據」「及人工智慧/機械學習」角度來解釋兩者之內涵確有不同，並透過這些不同之處也反射出目前所謂「個人資料」定義上的不同點，也因個資定義上的適用與排除，亦此可推理出過去為何過往判例的歧異。以 Anthony Liew 所著的《Understanding Data, Information, Knowledge And Their Inter-Relationships》²⁹¹，一般所稱的「資料」(Data)是「離散的客觀事實」、「未整理過的資訊」、「分析元素」，而「資訊」(information)是「具有一定意義的資料」、「整理過濾的資料」，且介於「資料」與「知識」之間。Anthony Liew 在書中並整理出如下表 22，各家對於 Data 與 Information 定義的差異，一致

²⁸⁹ Cambridge Dictionary 網站，
<https://dictionary.cambridge.org/zht/%E8%A9%9E%E5%85%B8/%E8%8B%B1%E8%AA%9E/data> (最後瀏覽日：2022/04/1)

²⁹⁰ 「知識管理」包括一系列企業內部定義、創建、傳播、採用新的知識和經驗的戰略和實踐。這些知識和經驗包括認知，可以是個人知識，以及組織中商業流程或實踐。在管理上會將知識分為資料、資訊、知識及智慧四個階段。從此學問中很清楚的是將「資料」(Data)與「資訊」(Information)分開定位。

²⁹¹ Anthony Liew (2007/06). Understanding Data, Information, Knowledge And Their Inter-Relationships. *Journal of Knowledge Management Practice*, Vol. 8, No. 2.
<http://www.tlinc.com/artic1134.htm>



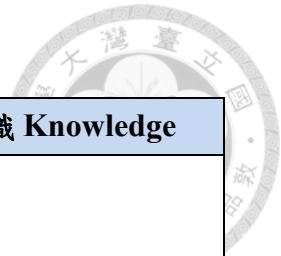
性的認為兩者間有顯著不同意涵。



表 22. Data 與 Information 意涵與關係整理。資料來源：Anthony Liew²⁹²; 本文整理

資料來源\名詞	資料 Data	資訊 Information	知識 Knowledge
Knowledge Nirvana – Achieving The Competitive Advantage Through Enterprise Content Management and Optimizing Team Collaboration; by Juris Kelley, 2002, Xulon Press	「資料」是基本，但尚未過濾與處理的資訊 Data is comprised of the basic, unrefined, and generally unfiltered information	原文定義： Information... is much more refined data... that has evolved to the point of being useful for some form of analysis	原文定義： Knowledge resides in the user... happens only when human experience and insight is applied to data and information
Innovation Strategy for the Knowledge Economy: The Ken Awakening; by Debra M. Amidon, 1997, Butterworth-Heinemann	「資料」是分析的基本元素 Data are elements of analysis.	原文定義： Information is data with context.	原文定義： Knowledge is information with meaning
Working Knowledge: How Organizations Manage What They Know. By Thomas H. Davenport and Laurence Prusak, 2000. Harvard Business School Press.	「資料」是客觀、片斷的事實集合 Data is a set of discrete, objective facts about events... as structured records of transactions	原文定義： Information... as message... in the (various) form of communication... to have an impact on judgment and behavior	原文定義： Knowledge is a fluid mix of framed experience, values, contextual information, and expert insights that provides a framework for evaluating and incorporating new experiences and information...

²⁹² *Id.*



資料來源\名詞	資料 Data	資訊 Information	知識 Knowledge
Merriam Webster's Collegiate Dictionary 10 th ed.	<p>「資料」是 1.作為推理、討論之基礎事實資訊...</p> <p>Data: 1. factual information used as a basis for reasoning, discussion, or calculation; 2. information output by a sensing device or organ that includes both useful and irrelevant or redundant information and must be processed to be meaningful; 3. information in numerical form that can be digitally transmitted or processed.</p>	<p>原文定義：</p> <p>Information: 1. the communication or reception of knowledge or intelligence; 2. knowledge obtained from investigation, study, or instruction; 3. Facts, Data; 4. quantitative measure of the content of information.</p>	<p>原文定義：</p> <p>Knowledge: 1. Cognizance; 2. the fact or condition of knowing something with familiarity gained through experience or association; 3. the range of one's information or understanding; 4. the sum of what is known: the body of truth, information, and principles acquired by mankind.</p>

另以大數據角度詮釋更為清楚，因為大數據就是運用許多片面且沒過濾的資料(Data)，所以需要資料清洗(Data Clean)或稱資料淨化。資料清洗是從資料庫表檢測、校正或刪除損壞或不準確的紀錄的過程，將辨識資料的不完整、不正確、不準確或不相關部分，然後替換、修改、或刪除髒資料(dirty data)或原始資料(raw data)。資料淨化實務可以人工處理與資料加工工具互動執行，也可以通過程式進行批次處理，這過程每個資料控制者的作法不一，流程與結果檢驗並無統一標準。或許有人會質疑在 GDPR 或「OECD 隱私準則」也同樣也要求資料關聯性及正確性原則(Data Quality Principle)，但兩者是否相同?本文舉一個例子，例如有當事人刻意留

下錯誤的姓名及身分證號空缺，在數據科學家就會將這資料 1.刪除或 2.若為重要客戶或個體，則以推估資料補足。不論何者在資料科學家重視的是最後的結果及反饋來確認正確與否，而這些過程未必需要知道每個「獨立資料個體」，而是以群體來看。

另外從人工智慧/機械學習的觀點也類似，基本上機械學習的資料比傳統統計可處理更多變量資料。以機械學習技術之「自動化決策」模式，係指資料控制者透過演算法等自動化方式處理輸入資料(Input Data)，在無人為介入的情況下對資料或當事人做成決策的過程。人工智慧/機械學習相對傳統規則式演算法而言，並不重視資料控制者對「資料」(Data)的詮釋，也不在意其意義。所以在此人工智慧/機械學習運用下，這些輸入「資料」(Data)更難謂為「資訊」(Information)。

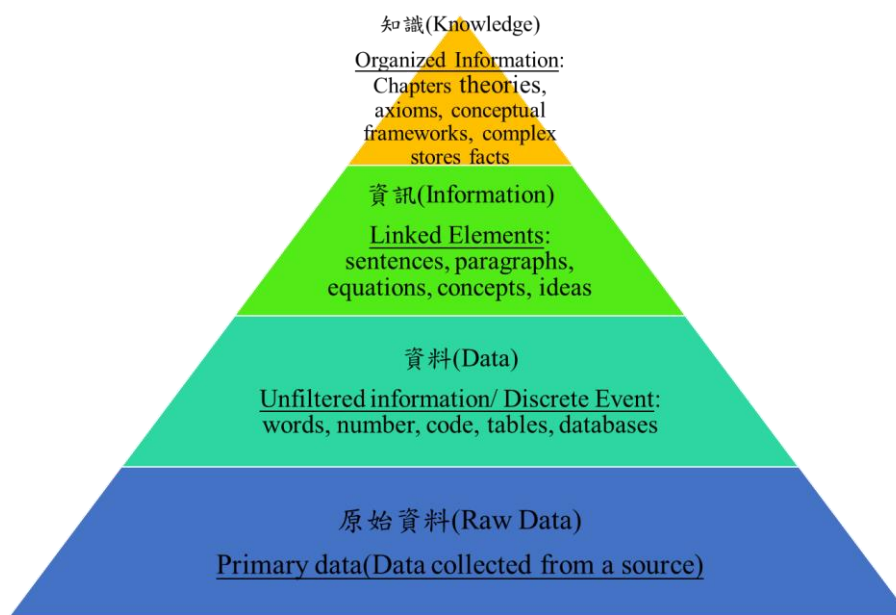


圖 52. 原始資料、資料、資訊到知識。資料與資料以知識管理、人工智慧/機械學習、大數據觀點都具不同意涵。資料來源：本文整理

綜上以科學觀點，大都將「資料」與「資訊」視為不同的兩者。同樣的，這也是為何本文認為資料與資訊是有基本上的差異，中國大陸的《個人信息保護法》以台灣用語應該稱為《個人資訊保護法》而非《個人資料保護法》。而清洗前的資料，是否符合 GDPR 的「正確性」規定?是否有可能屬於「間接可辨識個資」?再

則，若以清理過的正確資料為判斷是否個資的起始點，那麼個人資料英文應為「Personal Information」；「個資」全名應為「個人資訊」而非「個人資料」。

在 GDPR 中的「任何資料」(any information)定義，歐盟在 95 Directive 時期對於個資保護的大原則是儘可能將任何有可能辨識特定個人的資料納入個資法保護範疇。此一從寬界定個資之立場，已延續到 GDPR 儘量以最寬解釋個人資料(“Since the definition includes “any information,” one must assume that the term “personal data” should be as broadly interpreted as possible²⁹³)。延續此概念，GDPR 規定的個人資料乃指任何無論客觀或主觀觀點與特定人相關的資訊。

第二項 數據或資料

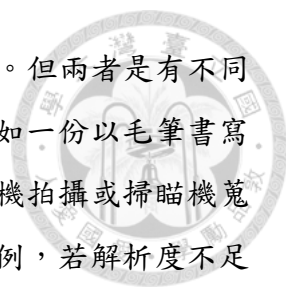
「Data」不論在資料管理或者個資保護的都是其基礎元素，一般中文翻譯有「數據」或者「資料」。兩者間是否有差別?以本文探討之範疇是否要區分?

觀之「Data」來自拉丁語「datum」，是「給予」的意思。依據我國國家教育研究院辭書對「data」解釋為：“代表任何的資源，諸如數位元元影像、資料庫、圖書、博物館的藝術品、檔案館的檔案記錄、後設資料記錄、服務、實際地點、人、事件、概念等²⁹⁴”；「資料」解釋為：1.“可供參考或研究的材料或記錄。”及 2.“計算機中一切數值、記號和事實的概稱。通常指尚未加以處理者。”；「數據」解釋為：“經由調查或實驗而得的數量化資料”。

由上述解釋是將「資料」詮釋為比較廣的初始、任何形式的原始材料;而「數據」是經過「數位化」(Digitization)的「資料」。研究資料或個資的論者兩岸所用不同，台灣慣稱「資料」而中國大陸慣稱「數據」，一般也認為只是兩岸用語不同而忽略差異。這是因為現今電腦或資訊設備太普遍技術成熟，大部分「資料」都已經

²⁹³ GDPR 網站，<https://gdpr-info.eu/issues/personal-data/> (最後瀏覽日：2022/01/19)。

²⁹⁴ 國家教育研究院辭書網站，<https://pedia.cloud.edu.tw/Entry/Detail/?title=%E8%A9%AE%E9%87%8B%E8%B3%87%E6%96%99> (最後瀏覽日：2022/03/11)



被「數位化」(Digitization)，所以大部分的人也都認定兩者一樣。但兩者是有不同意義，特別是從人工智慧/機械學習或大數據角度，舉例而言，如一份以毛筆書寫的字帖，當然是一份「資料」，但尚未成為「數據」，需經數位相機拍攝或掃瞄機蒐集並經程式編碼及儲存才能轉化成「數據」；以攝影機之取像為例，若解析度不足或者取像距離太遠²⁹⁵，可能人臉無法分辨，代表資料透過數位化轉換成數據時失真或失去背後資訊。再舉圖 53 一張笑臉的數位圖片為例，該圖片是「數位化」(Digitization)的「資料」，也是一群 0 與 1 所組成的「數據」，並經過解編譯呈現在顯示器前。然而要從人工智慧判定其是否假笑與笑容程度，且將笑容程度「數位化」(Digitization)成「數據」，那又是另一種資料形式。類似這樣的情形常見於非結構型資料中，要將其笑容程度轉化成「數據」，並非每個資料控制者或資料處理者皆有**能力**，或者縱有能力轉化的結果並非相同，後者換言之，**不同的原始「笑容資料」因不同技術會轉化成不同的「笑容程度數據」**。再從另一角度來分別兩者，「資料」是自古就存在，而「數據」是跟電腦息息發展相關，網路、大數據及雲端更是加速「數據」成長。如此針對「資料」與「數據」之區分，正如本文第二章所前述「**不涉及資料之蒐用即非個資法所規範**」，可呼應本文對「**資訊隱私權**」及「**隱私權**」(圖 27)之差異探討；此外，對於公示資料之隱私保護，如人臉及行車移動等足跡等也是因為第三人可見可聞之公示資料數位化蒐集後之數據易於處理、剖析、傳輸及利用，也是為今日所謂隱私侵害態樣更多元，個資保護之範疇爭議不休之根源。

²⁹⁵ 光學專業會以鑑別能力來表示，學理可用瑞利判別準則 (Rayleigh criterion) 判別之。在本文不細談。

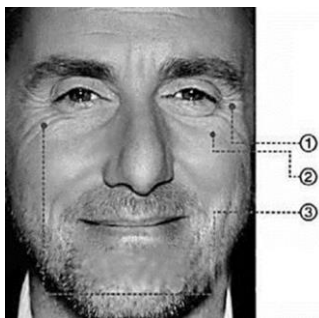


圖 53. 真實的笑容判斷。特徵為 1. 眼角皺紋;2.臉頰鼓起及 3.眼睛周圍肌肉運動。資料來源：《每日頭條》²⁹⁶;本文整理

再以《電腦處理個人資料保護法》時代背景而言，也是當時許多資料因為個人電腦的普及以及網路的興起，大量的「資料」被數位化成「數據」，而引發電腦資料的保護動機。

綜上，所謂「數據」與「資料」其實是有著差異，只是時至今日，數位化資料已是相當方便且廉價的，智慧自駕車中資料蒐集後皆是已經數據化以利於處理及利用，故本文所探討範疇中並不區分兩者之差異。本文除了尊重引用資料以外，皆以「資料」稱呼之。而所謂「資料」(Data)分類，將於後論述之。

第三項 「個人資料」是否真實無誤(True or Proved)?

我國《個資法》依據《OECD 隱私準則》對於資料有「資料關聯性及正確性原則」(Data Quality Principle)，此點與 GDPR 資料處理要求「正確性」原則一致。然而此處的「正確性」意義為何?到底是指資料控制者在資料處理程序上正確無誤?還是要求資料控制者要與當事人真實資料核實?

舉一例子，若某網購平台登錄時要求當事人甲提供生日日期 A 及地址 B，當事人甲故意填寫錯誤生日 A'及正確地址 B，此時該資料管控的網購平台登錄的當事人甲生日 A'及地址 B'，前述所指的正確性是指與真實不同的 A'(A->A')，還是

²⁹⁶ 詮釋雷特 (2019/10/07)，《AI 如何識別假笑容?個人怎麼判斷真假笑容?看完你就懂了》，每日頭條，載於：<https://kknews.cc/news/k4x9ypv.html> (最後瀏覽日：2021/1/11)。

平台儲存錯的 B'(B->B')? 或者兩者皆是? 此點在我國個資法並沒有明示, 只有以「正確性」原則涵蓋。相對的, GDPR 中所謂「個人資料」並無須為真實或被證明, 並已經設想資訊可能並非正確並另有更正權的設計('For information to be "personal data", it is **not necessary** that it **be true or proven**. In fact, **data protection rules** already **envisage the possibility that information is incorrect** and provide for a right of the data subject to access that information and to challenge it through appropriate remedies.'²⁹⁷)。從實務觀點, 對於非公務機關除非依法有據或者與業務直接相關(例如地址填錯, 物件就無法送達), 否則確實很難核實資料是否真實或者驗證資料的對錯。以資料本人對其個人資料有自決權的角度, GDPR 這樣的規定從實務上觀點而言相當合理。

第四項 「個人資料」中資料與個人關聯性探討(Relating to)

若「資料」非屬「個人資料」, 自無《個資法》之適用, 然何謂「個人資料」? 目前「個人資料」爭議何在? 此問題與「個人去識別化」及個資之蒐集、處理、利用等法律規範緊密結合, 然學說卻相當混亂。從各國個人資料保護法規來看, 所謂「個人」, 大部分個資保護法規排除亡者, 以自然人為主體, 自然引申出可以辨識或可能辨識該「自然人」的資料為「個人資料」的定義。然而所謂辨識該特定「自然人」是否為「唯一」(Unique)的「當事人」在法條上並無明示, 但從我國判例或文獻中可常見用「是否容易推知」、「是否可輕易連結」、「是否耗費過鉅始能識別」來評判某資料是否屬個人資料。然而何謂「輕易」? 「連結」以幾次為限? 「連結」多次資料中是否必包含其他「個人資料」?

在 WP29 之「個資概念意見書」²⁹⁸提出包含內容(content)、目的(purpose) 及結果(result)三個判斷因數, 以使資料與個人之關聯性(relating to)具可操作性。這三

²⁹⁷ Rectification could be done by adding contrasting comments or by using the appropriate legal remedies, such as appeal mechanisms

²⁹⁸ WP29, Opinion 4/2007 on the Concept of Personal Data (2007), at 6-7.

者並非並存之關係，只要任一條件符合，該資料即可能滿足資料「關聯性」(relating to)要件之判斷而被視為是個資²⁹⁹。

我國判例或文獻中可常見用「是否容易推知」、「是否可輕易連結」、「是否耗費過鉅始能識別」來評判資料是否屬間接識別之個人資料，惟現行《個資法》及《個資法實施細則》並無相關規定。經查詢法務部於網站³⁰⁰所留存之《電腦處理個人資料保護法施行細則修正草案條文對照表》第三條：「本法第二條第一款所稱得以間接方式識別該個人之資料，指僅以該資料不能識別，須與其他資料對照、組合、連結等，始能識別該特定個人者。但查詢困難、需耗費過鉅或耗時過久始能特定者，不在此限。」其中如下圖 54 之但書為「.....但查詢困難、需耗費過鉅或耗時過久始能特定者，不在此限。」並於該條說明中闡明：「.....惟以間接方式識別之個人資料，如查詢有困難、需耗費過鉅或耗時過久始能特定者，屬技術上太複雜及經濟上不可行，則應屬無法識別之個人資料，爰規定如但書條文，以資衡平個人資料保護與個人資料合理利用。」該但書只列於草案，但不見於正式之條文中，可見我國立法時並沒有將此但書寫入以限縮所謂「個人資料」。

²⁹⁹ 張陳弘，莊植寧 (2019)，前揭註 230，頁 22。

³⁰⁰ 法務部，《電腦處理個人資料保護法施行細則修正草案條文對照表》，載於：
<https://www.moj.gov.tw/media/2799/110271036102.pdf?mediaDL=true>

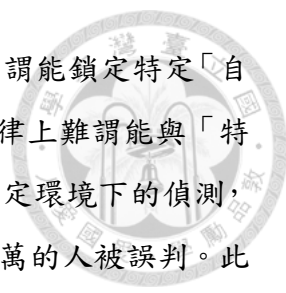


電腦處理個人資料保護法施行細則修正草案條文 對照表

修正條文	現行條文	說明
個人資料保護法施行細則	<u>電腦處理</u> 個人資料保護法施行細則	配合本法名稱之修正，將名稱修正為「個人資料保護法施行細則」。
第一條 本細則依個人資料保護法（以下簡稱本法） <u>第五十五</u> 條規定訂定之。	第一條 本細則依 <u>電腦處理</u> 個人資料保護法（以下簡稱本法）第四十四條規定訂定之。	配合本法名稱及條文之修正，酌作文字修正。
第二條 本法所稱個人，指 <u>現</u> 生存之自然人。	第二條 本法所定個人，指生存之 <u>特定或得特定之</u> 自然人。	本條酌作文字修正。又本法第二條第一款對於個人資料之定義，已修正為得以直接或間接方式識別該個人之資料，規範意義即為特定或得特定之自然人的個人資料，故刪除特定或得特定等文字。另本法立法目之一為個人人格權之隱私權保護，唯生存之自然人方有隱私權受侵害之恐懼情緒及個人對其個人資料之自主決定，故增加「現」字，以為明確。
第三條 本法第二條第一款所稱得以間接方式識別該個人之資料，指僅以該資料不能識別，須與其他資料對照、組合、連結等，始能識別該特定個人者。 <u>但查詢困難、需耗費過鉅或耗時過久始能特定者，不在此限。</u>		一、 <u>本條新增。</u> 二、由於社會態樣複雜，有些資料雖未直接指名道姓，但一經揭露仍足以識別為某一特定人，因而本法第二條第一款個人資料之定義，已將「其他足資識別該個人之資料」修正為「其他得以直接或間接方式識別該個人之資料」，為明確間接方式識別該個人之資料之意義，爰為本條之規定。惟以間接方式識


圖 54. 我國個資法實施細則修正草案對照表，黃底部分但書並沒有被列入最後版本。資料來源：法務部

「特定當事人」是否解讀成唯一之自然人？如此定義從科學角度來看是相當狹隘的定義，現今除了身分證統一編號、護照號碼外，其他例如人臉辨識、姓名等，即使是指紋亦非 100% 的可指向特定人；再例如 IP address (Internet Protocol Address, 簡稱 IP)，若是公用電腦或企業內部工作電腦的網址，亦不能直接指向某個特定的



人。從被列為個資的資料包含：“IP”、“GPS”、“瀏覽紀錄”等難以謂能鎖定特定「自然人」，因為此電腦可能是數個甚至多人的共同使用紀錄。從法律上難謂能與「特定當事人」做直接連結；再例如“人臉辨識”、“聲音辨識”，除非在特定環境下的偵測，不然錯誤率都可達 3%~5%，意即每百萬人中，將會超過 3 萬~5 萬的人被誤判。此等問題在判例與文獻中常被提及，也是判例中兩造攻防之重點，如「第 54 號判決健保資料」乙案判決書：“惟本案去識別化作業模式尚未達到「完全切斷資料內容與特定主體間之連結線索」程度，「個資」屬性並未全然排除而仍有隱私權侵害之虞，故不符合個資法第 16 條第 5 款但書後段「依其揭露方式無從識別特定之當事人」之規定，仍有繼續檢討之必要。」在本年 8 月憲法法庭 111 年憲判字第 13 號健保資料乙案判決主文第 35 段中：「個資若經處理，依其資料型態與資料本質，客觀上仍有還原而間接識別當事人之可能時，無論還原識別之方法難易，若以特定方法還原而可間接識別該個人者，其仍屬個資。當事人就此類資料之自主控制權，仍受憲法資訊隱私權之保障。反之，經處理之資料於客觀上無還原識別個人之可能時，即已喪失個資之本質，當事人就該資訊自不再受憲法第 22 條個人資訊隱私權之保障」，又稱「查個人健保資料....，於客觀上非無以極端方式還原而間接識別特定當事人之可能性，此為科學上之事實。因此，個人健保資料無論為原始型態或經處理，均必然仍屬「得直接或間接識別該個人」之資料，當事人對於此類資料之自主控制權，受憲法保障」(憲判字第 13 號判決主文第 36 段參照)，足見大法官對於所謂個資之認定已歐盟之見解趨於一致。同判決主文第 53 段中對於「去識別化」之定義：「.....使一般人採取當時存在技術與合理成本，在不使用額外資訊時，不能識別特定當事人。」從憲判字第 13 號判決可知 1.對於個資的可識別性採客觀條件說，且不論還原識別之方法難易；2.「去識別化」之定義與 GDPR 之「假名化」定義接近。

再者，從科學或從商業應用的角度，一份資料先不論是否為個資，只要能夠區分出群眾，並能瞭解該族群的各種特性即有科學或商業上意義，並以更嚴謹的將錯誤率分為 1.偽陽性(True positives, TP)：被正確地劃分為正例的個數，即實際為正例且被劃分為正例的實例數（樣本數）；及 2.偽陰性(False positives, FP)：被錯誤地劃分為正例的個數，即實際為負例但被劃分為正例的實例數。在指紋辨識或生



物辨識應用領域，常用的指標是代表安全程度的錯誤接受率(False Acceptance Rate, FAR)，定義為“辨識系統誤將不合法使用者辨認為合法使用者的機率”，及錯誤拒絕率(False Rejection Rate, FRR)，定義為“辨識系統將合法使用者誤判為不合法”。從科學而言，一個重要的轉捩點就是解析度能超越人類，如前影像辨識競賽中人與電腦的競爭，機械學習能被重視就是如本文圖 6 能夠達到甚至超越人類的之圖形分辨能力，而人類的錯誤率大約是 5%。不僅如此，數位化的資料重要的是能夠結合各資料將單一資料錯誤率從 5%降至更低的比例，這原因正是法律上常出現的「資料連結」或者「資料結合」作為個資判斷依據的原因。然而是否可定義「輕易」？從科學或商業上當然是可以訂有指標，並依不同運用場域而調整，然這些指標顯然與不同企業技術能力與不同年代之科技發展而有高度關係，在本文的人工智慧、資料融合、邊緣運用及大數據的衝擊下，相關的資料蒐集、處理、利用等，無論技術發展與成本下降之快速都遠非我國《個資法》立法時刻所能想見的。

綜上之所論，從商業或者科學角度，不須要到獨一無二，識別特定當事人的個資才能具有的價值。實則從統計、人工智慧/機械學習推論的觀點，只要能到達顯著的差異就有利用價值，此時的資料運用，就已經達到侵犯隱私的可能。例如某電腦 IP 正在瀏覽某觀光地區資料，人工智慧/機械學習或大數據運用就可預測使用者可能想要旅遊，乃主動推薦旅行社觀光行程，如果此時該 IP 使用者進行點閱，即可提高該使用者可能花錢旅遊的可能；若再進一步提高觀光旅遊折扣且該 IP 使用者繼續點閱關注，系統一步步的計算出該 IP 使用者的意圖並進行廣告行銷的過程，資料控制者實務上並不需掌握「特定的自然人」為何，資料控制者即可運用資料產生商業價值亦可能侵犯隱私。隨著該 IP 越來越多的資料被蒐集，IP 背後的當事人或者當事人們(可能是同辦公室同仁或者同班同學)的行為特性資料就越準確，也越具商業價值。科學對比法律、不同個案與不同國家等不同角度去詮釋個人資料或個人數位足跡，就會造成一份資料是否能被判定為個人資料、是否排除個資法規適用的差異，這也是造成各國個資法所謂個資定義不同、隱私與個資不分之緣由。

第五項 明文例示的個資是否就屬於直接識別性個資

不論哪國個資法規，都有明文例示一般個資及敏感個資，然而明示個資如姓名、指紋及 GPS 等是否等同於直接識別性個資？

何謂「直接識別性個資」？依現行個人資料保護法施行細則第 3 條可推論出：「指保有該資料之公務或非公務機關僅以該資料能**直接識別**，不需與其他資料對照、組合、連結等，即能識別該特定之個人。」若依此定義，深究例如單一菜市場名(a very common family name)及指紋圖形，其實並無法在不需與其他資料對照、組合、連結等下，即能識別該特定之個人。再依中華民國 101 年 9 月 26 日法務部法令字第 10103107360 號令公布之《電腦處理個人資料保護法施行細則修正條文對照表》第三條修法說明謂：「至於是否得以『直接』或『間接』方式識別者，需從蒐集者本身個別加以判斷，原無一致性之標準，此宜於個案中加以審認，為權衡個人資料之保護與個人資料之合理利用，並避免滋生疑義，應依本法相關規定加以判斷。至於各公務或非公務機關如在適用本條規定要件上有明確之必要者，各公務機關或目的事業主管機關得斟酌訂定裁量基準，俾供所屬機關或所管行業遵循。」從上述說明可見所謂「直接」或「間接」並無公認或一致之標準，還是「回到個案」，並「得由各公務機關或目的事業主管機關得斟酌訂定裁量基準」。

第六項 已識別或足資識別(identified or identifiable)

當一個自然人在一個群體中可被其他人區分開來，此人可定義為「已識別」(identified)之人；而當該自然人無法立即與其他人區分，但有可能可以分別，此人則可被稱為「足資識別」(identifiable)之人³⁰¹。

依據 GDPR 前言第 26 點(Recital 26)，資料保護原則應適用於與已識別或足資識別自然人有關的任何資訊。經過假名化的個人資料(Personal data which have undergone pseudonymisation)，可通過使用資料結合判定為特定自然人之所屬，應被

³⁰¹ WP29，前揭註 298，頁 12。

視為有關可識別自然人的資訊。為確定自然人是否可識別，應考慮所有合理可能使用的方法，例如由資料控制者或其他人直接或間接識別自然人的方式。為了確定是否有合理可能使用的手段來識別自然人，應考慮所有客觀因素，例如辨識的成本和所需的時間，同時考慮到識別當時處理和技術發展的可用技術。因此，資料保護原則不應適用於匿名信息(anonymous information)，即與已識別或可識別的自然人無關的資訊，或與以無法識別或不再可識別當事人(資料主體)的方式匿名的個人數據有關的資訊。因此，GDPR 不涉及此類匿名信息的處理，包括用於統計或研究目的。

GDPR 對於個資有一個整體的想法，然對於現今日新月異科技而言，實在有落實之困難，緣由為前面所提的儲存、傳輸與處理技術飛快發展，一個數據化的資料，一旦被蒐集、處理後，幾乎很難在網路上消失，且不能預期今日的技术不能辨識該當事人，以後技術是否足以辨識？即使 GDPR 已經考慮到以當時處理及技術發展趨勢下的可用技術(taking into consideration the available technology at the time of the processing and technological developments)，但是以何者角度來評斷？法規中並無說明。

第七項 辨識的主體

如前所述，「資料可識別性」的判斷標準，我國依個資法第 2 條第 1 款定義之個資，不但包括得以直接方式識別特定個人的資料，也包括「在與其他資料結合後，可識別特定個人」或謂「得以間接方式識別」的資料，然後者之認定標準究應依資料使用者主觀條件或資料本身客觀條件來判別「得以間接方式識別特定個人之資料」？對於這個問題，在本文第三章「Google 街景圖」案例中有提及在學說上有「絕對認定標準」以及「相對認定標準」兩種不同主流見解。但就資料控制者定義，GDPR 並無相關的規定，或者廣義的解釋成「任何人」說³⁰²。一份資料若不為個資，自然無個資法適用之問題。而如何被判定為個資，「辨識的主體」的居於關鍵的角色，必須就該主體的定義做更深入的討論，茲就相關學說總整如下：

³⁰² 張陳弘，莊植寧 (2019)，前揭註 230，頁 31。



一. 一般人標準說

有論者衡諸“個人資料常為表現自由的材料，更為適當保持資訊之合理流通利用”，主張應當以「社會一般多數人」標準依該資料之內容是否「容易推知」特定個人為判斷基準，可稱之為「一般人標準」³⁰³。一般人標準說存在網路成熟及影音設備興起之時代，大量的個人影像及資料經由影音設備及網路被大量流傳，且經無國界網路的社群討論及挖掘資料的肉搜，使得當事人不勝其擾，例如 Google 街景圖及 Facebook 圖片。

我國個資法並未如日本個資法第 2 條第 1 項有「容易」與其他資料作比對、組合之要件規定，得與「間接識別性」個資為組合、比對之其他資料，是否應為一般人無須經特別調查或支付龐大費用即容易得手之資料？此同樣關係得合理利用個資範圍之界定有所疑慮。是故有「資料控制者標準」之說。

二. 資料控制者標準說

現行《個資法施行細則》第 3 條：「本法第二條第一款所稱得以間接方式識別，指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。」法務部法律字號第 0999051927 號函釋「記名悠遊卡卡號是否屬個資」的個案而言，法務部以“就持卡人以外之第三人而言，倘該個人資料係屬「查詢有困難」或「需耗費過鉅」始能足以識別特定個人者，客觀上即屬無法識別之個人資料”。我國「去識別化」之定義依《個資法施行細則》第 17 條後段稱：「……所稱無從識別特定當事人，指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者」，條文中並沒有將「假名化」與「匿名化」細分。「資料控制者標準說」在我國雖獲得不少論者支持及判例採用³⁰⁴，但其相對性會造成「個人資料」認定上的主觀，徒增認定上之困難與個案

³⁰³ 范姜真嫩 (2013)，前揭註 124，頁 91。

³⁰⁴ 黃耀賞 (2015/01)，〈淺談「得以間接方式識別特定個人之資料」〉，《科技法律透析》，27 卷 1 期，頁 31-35。

化。常見的例子為 IP address、車牌，並非任何資料控制者皆能辨識出特定當事人，如何判斷是否屬於個人資料？再如前者所談的指紋辦案，對於大部分資料控制者，即使是公務機關因為缺乏完整資料庫或當時技術能力所限並無法辨識特定當事人，那是否不符合個資定義？此外，對於非公務機關的資料控制者，能否辨識特定當事人的判定亦是另一個問題。另一問題，以資料控制者標準說，一分資料是否屬個資，必須在資料「處理」階段才能做出判決，「蒐集」階段並無限制。而自駕車因為資料處理時間極短，「蒐集」、「處理」到「利用」行為必須在短時間完成，相對地三個階段行為難切割；若蒐用資料屬於個資，則容易與現行我國《個資法》之規範衝突。

綜觀我國《個資法》與《個資法實施細則》，並無將「查詢有困難」、「需耗費過鉅」或「需耗時過久」等限制放入法條但書中，僅止於個別函釋中補充說明。過於主觀且個案化之評判，也造成資料控制者標準說在實務上解釋之爭議。

三.任何人標準說

相較我國著重於資料控制者的識別能力判斷，GDPR 依其規範著重於資料自身，不論是資料控制者或任何人，透過所有可能，合理的方式下，得以辨識出特定的個人。

何謂「可能、合理」？GDPR 有說明應考慮所有客觀因素，例如識別所需成本和時間，同時考慮當時可用技術與科技發展趨勢(“To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.”)GDPR 採此標準是傾向於個資之保護，故以資料本身客觀條件來做為判別標準。

在本文中為何探討資料控制者之源由，在於技術發展之考量，過去因技術發展的限制，過去任何高成本、時間的問題，都在現今的技術下被克服，例如大數據中的大容量，使得儲存量大增；又如雲端運算及邊緣運算，使得計算成本及時間大

幅下降;技術的發展常突破過去的見解，例如：在本文中文大數據將廢棄資料變成有用個資;人工智慧/機械學習在不被看好中打敗世界棋王，又在短短一年內電腦自己打敗自己。

新技術與新科技的突破，改變的不只是技術內涵，還有人們的思維。以下為本文所提出新的「人工智慧標準說」。

四.人工智慧標準說

在本文中已多次討論人工智慧對於個資的影響，透過前述的人工智慧/機械學習的演算法，任何由人為的足跡，即使是片段的資料或資訊，都有可能被現今的人工智慧透過資料結合或者長時間的監控下，自動化剖析出特定個人的特徵。故本文提出另一個以科學發展觀點的「人工智慧標準說」，以人工智慧，在此不限於機械學習或者深度學習，是否能將資料自動的將當事人辨識或者分群，做為判斷該份資料是否為個資的依據。

本文提出如此看法在於：1.透個「人工智慧標準說」得以解釋為何人們覺得隨時個人行為或動態可能被監控，個人的「To be let alone」權利受到干擾;2.現今資料巨大，不論蒐集、處理到利用，皆因為超過人力之負荷，大都以電腦取代人力，特別是人工智慧技術在部分工作早以超越人腦的能力，精準且有效地做將資料轉成個資作為商業或其他運用，是故應以人工智慧標準據以判斷「資料可識別性」。此觀點在 GDPR 的自動化決策中亦有提及，但因為 GDPR 之規範早於人工智慧/機械學習/深度學習技術之崛起，但並沒有提出本文的論點。「任何人標準」觀點已不足以解釋現今個資的框架與隱私被侵害現象。

第八項 個人資料分類

在各國個資法中對於「個人資料」分類，主要分為一般性個人資料與敏感性(特種)個人資料。這樣子的分類主要著重該資料被洩漏或者被第三者利用時會對當事人造成重大的傷害程度而分類。

根據個人資訊與資料主體和現實的「關係」(relationship)以及企業在獲取和處理此類資料時的智力活動，對個人資訊進行分類。依據學者 Gianclaudio Malgieri³⁰⁵的見解，以此觀點方面可以區分出三類別資料：強關係資料(Strong relationship data)-由客戶直接提供的資料(data provided directly by customers)、中間關係數據(Intermedia relationship data)-觀察或推斷並與消費者當前生活相關的資料(data observed or inferred and related to the present life of consumers)和弱關係資料(Weak relationship)-預測資料(predictive data)。每個類別都反應 GDPR 規定的不同個人的權利。只為強關係資料提供資料可攜性，而弱關係數據不提供控制權。同時，其他權利重新平衡消費者和企業之間的資訊不對稱(資訊權、不被自動分析的權利等)。因此，為了同時尊重公司的知識產權和消費者的資訊隱私權，「最好的平衡方法是將“控制權，包含擷取、可攜性、遺忘”與“反應權，包含資訊權、反對自動化個人檔案剖析”區分 (“the best balancing approach in order to both respect the IP rights of companies and the information privacy rights of consumers is to distinguish “control rights” (access, portability, oblivion) from “reaction rights” (right to information, opposition to automated profiling, etc.)”)³⁰⁶。廢棄資料以三分法可為中間關係資料，而廢棄資料或一般資料透過人工智慧/機械學習所推導出的個資屬於弱關係資料(Weak relationship)。足見人工智慧/機械學習以資料驅動的新技術，不但衝擊原個資法資料處理原則，易可能對於資料財產歸屬與個資刪除權利有很大影響。

第三種分類法，著重於資料控制者本身。一份資料是否屬個資決定在於資料控制者以當今技術是否讓該筆資料去識別個別當事人。反之，一份資料被資料控制者識別各別自然人，則可被稱為個資；反之，則否。

第四種為本文所提出的「三級分類法」，與第二種 Gianclaudio Malgieri 分類精神雷同，一樣依據資料與當事人之間關係而定。依據科技日新月異與儲存技術大幅

³⁰⁵ Gianclaudio Malgieri (2016). Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data. *Privacy in Germany - PinG*, n. 4, 2016, 133 ff. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2916058

³⁰⁶ *Id.* at 1.

增加，當個資洩漏時對當事人影響時間長久而定。

第一級為高度相關，例如人臉辨識、語音辨識、指紋辨識、毛髮、耳道生物辨識資料(genetic data)及遺傳資料(genetic data)如血液、DNA 等。因為此類個人資料為跟隨人的一輩子，極難變更或替換，所以不應以當時技術、當時的技術發展預期、是否公開或具資料庫與否等條件考量是否能否辨識獨特個人或鎖定族群。例如事故或案發現場的指紋或掌紋，或受限於一時未必有資料庫可比對，或受限於當時技術³⁰⁷無法比對出，然而因其具有與當事人高度相關之特性，即使過了多年後依然可循跡尋人，最具代表的國內外案例為案發現場遺留的指紋。縱使第一級資料未必能當下 100%辨識當事人，多年後依然能夠因為技術發展或資料庫的齊備而追蹤到行為人。高度相關個資管制之精神在於該類資料與當事人的高度連結性且不易變更而應嚴格管控，不應受限於當時技術或當時可預見之技術。自駕車因為有許多感測器，且為了生命法益而蒐集、處理與利用，惟應針對類似個資或資料做比較高規格管控，以保護當事人的個人隱私與生物資料。高度相關的個資的嚴格管控，另一個的考量也是因為可能會影響到下一代，例如 DNA、毛髮、血液、人臉辨識、聲音等，以目前技術可推估出家族的隱私，例如疾病、長相、特性及背景等，這些資料是否跟隨自然人死亡就不受個資法保護？

第二級為中度相關，主要是由法規所規範或用途限定，例如車牌號碼、電腦 IP、個人電話等與當事人相關度高且易辨識者。第三級為低度相關，例如個人數位足跡或本文所稱的廢棄資料等，這些資料可分為第三級。

以高中低相關等級來分，主要衡諸技術變化快速及對當事人影響而定。在此強調，本文所提三級分類法並非獨立區分準則，可與先前其他分類方法一併考量。

³⁰⁷ 刑事警察局於 2016 年完成指紋電腦系統更新，使指紋比對效能大幅提升，並於 2017 年針對 2004 年未破的重大刑案現場指紋進行比對，並因此破獲案件。顯見高相關度之個資，不應以蒐集當時的時空環境或技術發展據以判斷是否為個資，或者分類為一般或特種個資。

第九項 個資法排除適用討論

綜整我國《個資法》排除適用之規定，第 51 條第一項規定包含 1. 自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。2. 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人資料結合之影音資料。兩款的規定立法理由都是基於避免個資保護與社會公益間的衝突。

對比國際個人資料保護法，《中國個資法》並沒有台灣《個資法》第 51 條第 1 項第 2 款：「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人資料結合之影音資料」的規定。另在中國《汽資安全規定（試行）》就有針對車外的用路人個資做了明確的規範。

《個資法》第 51 條第一項第二款之規定的立法或係參酌美國法院在聯邦憲法增修條文第四條規定的搜索行為與隱私保障判斷，基於美國最高法院 *Katz v. United States* 判例所建立的「隱私的合理期待判斷準則」(the reasonable expectation of privacy test)³⁰⁸，所發展的「公開揭露法則」(the public exposure doctrine)、「公開領域法則」(the open-fields doctrine)及「目光所及法則」(the plain view doctrine)³⁰⁹。立法者的思維乃認為與個人相關的影音資料屬個資法第 2 條第 1 款明文例示之個人資料，惟該影音資料已公開，若未與其他個人資料結合，故隱私保障程度較低，旨在平衡個資保護與資料流通權益兩者。

惟，對於《個資法》第 51 條第一項第二款之挑戰，承前面所述，何謂可間接辨識得知之個資之判斷標準，已因為大數據而有所衝擊；同樣的「未與其他個人資料結合」，重點變成在於「未結合」，而自駕車因為資料融合、邊緣運算及車聯網的必要性技術導入，資料結合與處理已為基本且必要流程，使得實務上在個資法第 51 條第一項第二款之法條適用難以認定。

³⁰⁸ Legal Information Institute. *Katz and the Adoption of the Reasonable Expectation of Privacy Test*. Cornell Law School. <https://www.law.cornell.edu/constitution-conan/amendment-4/katz-and-the-adoption-of-the-reasonable-expectation-of-privacy-test>

³⁰⁹ *Oliver v. United State*, 446 U. S. 170, 180 (1984); *Katz. United State*, 446 U. S. 347, 361 (1967); *Minnesota v. Dickerson*, 508 U. S. 366, 375 (1993)

綜上，對於因個資認定之困難，導致《個資法》排除適用之爭議與挑戰。本文提出另立專法明文規定其用途，在本文第六章綜合討論。



一. 公示資料個資就不受保護?

綜合前述所談，個人資料本質為個人隱私，為隱私權或人格權所保護之範圍，而公開場合所蒐集之公示個資，是否還為個資法保護之範疇?

目前從前述判例司法院釋字 689 號解釋所談及，單以個資公示與否不足以判斷是否侵犯隱私，或該個資是否該當保護之標的，加以人工智慧/機械學習技術拓展下，對於公示資料的保護亦不可忽視。惟公示資料可為不特定第三人獲得，對於其保護的程度與合理利用之界線如何權衡?是否以《個資法》第 51 條第一項第二款作為依據?以本文前述之智慧智駕車的運用環境下討論，個資除了因為與其他個資資料庫結合以外，持續性的監控亦可能造成對隱私的侵害，《個資法》第 51 條第一項第二款之規範顯然不足以涵蓋現今資料轉換成個資之範疇。

是故本文認為在自駕車所蒐用的對外公示資料中，例如用路人的個資，亦應有相當程度的管理，並平衡行車安全與資料之利用。

二. 「影音資料」是否為特定資料?

如前所述，現今影音資料都可用人工智慧/機械學習即時作內容辨識，包含視訊資料中的車牌辨識、人臉辨識、人眼辨識與步態辨識等，相較 10 多年前的單獨影像「蒐集」，現在的錄攝影機除了蒐集外還有物體偵測、行為辨識、行為預測等資料「處理」及「利用」過程。

本條文會有幾個基本問題，包含 1. 「影音資料」是否為特定資料?其他是否還包含前述所談的 Wifi 訊號、超音波、光達所蒐集資料等資料?2. 「影音資料」是否該是排除的特定資料?就我國《個資法》之立法理由，理應有更具體的規範以避免阻礙資料之流通。



三.未與其他個資資料結合?

此構成要件包含「與其他個資資料結合」與否，亦有其定義不清之處。其一在於何謂「其他個資」，經過本文論述，我國對於《個資法》第二條所謂之個資並沒有清楚的定義，實務上傾向以資料控制者的主觀角度來判斷是否為個資，如果《個資法》所謂之個資並無法有客觀且一致的判斷標準，例如與廢棄資料之結合，自然難以判斷「未與其他個資資料結合」與否。其二，除了「結合」外，資料間之對照、組合、連結等，是否有等同「結合」之功用及法律效果?其三，資料間不結合但持續性監控，例如長期 GPS 位置監控，是否應有等同前述對照、組合、連結、結合等之法律效果?

四.智慧自駕車運用下，個資法排除適用討論綜整

綜合前面之討論，在人工智慧/機械學習的運用下，自駕車所蒐集之不特定自然人錄影資料，如尚未與其他個人資料結合而能辨識特定人階段時，此影像屬間接識別性個資;若結合其他個人資料或資料庫而能直接辨識特定人時，則此影像屬直接識別性資料。

至此，因為人工智慧/機械學習及自駕車其他科技的演進與結合，使得公開領域的個人影音資料也已被廣為認定屬個資的範疇，惟是否該排除個資法適用或者在其他公眾利益下對個資保護有所限制，對於個資之蒐集、處理到利用，才應該是在人工智慧/機械學習的運用下自駕車所擁有的個資要探討之議題。

此外，人工智慧/機械學習驅動的自駕車資料利用，無論對於車內駕駛的行為偵測、路人的生物特徵偵測等，大都是有其必要性，在如此狀況理應以安全性為優先考量，而非以個資法角度出發，個資保障為優先。但如何兼顧當事人個資保護與隱私權保障，值得更細化規範。

第十項 人工智慧機械學習驅動之自駕車再次挑戰個資法

回顧《個資法》的歷程，自民國 84 年(1995 年)立法時期，為個人電腦開始普

遍且網際網路開始興起時，歷經 1995~2010 年間大量光資通訊技術大量普及、2000 年的網路高峰、2010 年後的大數據、物聯網崛起、2014 年後人工智慧/機械學習/深度學習的成功並開始廣泛應用到各行業、《個資法》修正、2019 年後自駕車的滲透市場，這些技術發展、法規及判例時間羅列如圖 55。

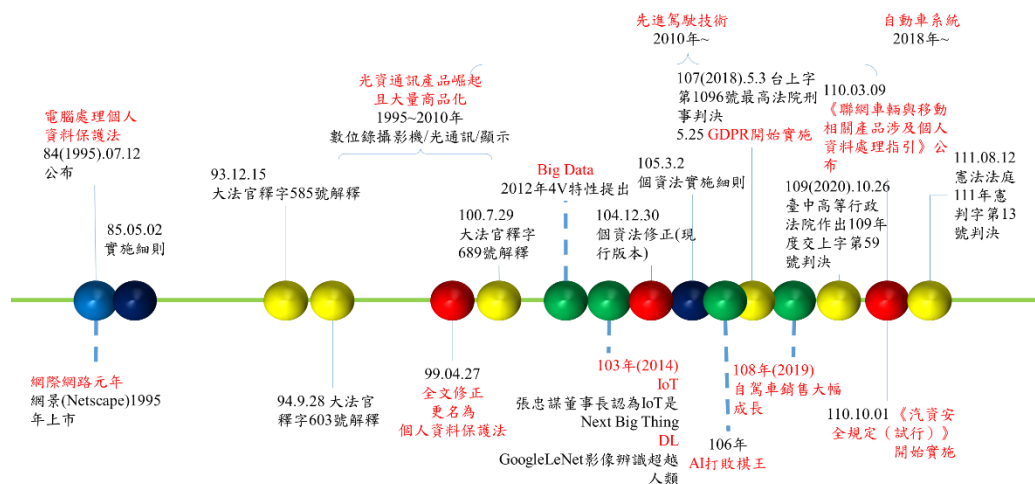



圖 55. 重要技術發展、個資法及重要判例以時間軸展開。資料來源：本文整理

自 1990 年後，個人電腦普及，伴隨光學掃描器、數位錄影機及當時的光纖網路等光資通訊產品的大量運用，使得資料大量被數位化且傳輸，這些技術也導致 2000 年後大眾個人資料逐漸被大量運用及個人資料保護的意識抬頭；隨後在 2010 年後加入物聯網、雲端技術及大數據的資料被大量商業化，使得輔助駕駛開始導入車輛；另一方面也因為資料的濫用導致歐盟重視隱私與個人資料保護，並於西元 2018 年實施 GDPR。至此，新的人工智慧/機械學習的新技術導入，更將資料/個資的利用推向了高峰，而自駕車正是可預見未來爭議的焦點。

一. 自駕車集合最頂尖之技術，輔以大數據等技術挑戰個資定義

同前所述，自駕車被視為一台可移動的電腦，回顧民國 84 年訂定「電腦處理個人資料保護法」第一條之立法理由：「電腦科技進步迅速，使電腦能大量、快速處理各類資料，且運用日趨普及，因而對國民經濟之提昇有重大貢獻。惟個人資料因濫用電腦而侵害當事人權益之情形日漸嚴重，亦引起民主先進國家之關切。」



如今時至 21 世紀，被視為資料(Data)的世紀，如今的資料之量與質、資料處理、資料傳輸之能力都遠非「電腦處理個人資料保護法」立法當時可比擬。而所謂的大數據技術，正是在商業利益下，透過業者所大量儲存使用者的使用紀錄，將這些資料透過巨量分析與資料探勘等方式，萃取出有用或可供預測的資訊，可幫助業者瞭解使用者行為、進而發展新服務，此為大數據在資料經濟開創新的時代，也形成科學發展與商業行銷的新動力，同時也影響國家政策的方向。在大數據巨大商業利益的驅使下，企業以最大程度蒐集、處理、利用資料與個人資料作為提升其產業競爭力的重要手段，使得傳統的隱私受到很大的挑戰，也因而引發各國對於個人資料保護的規範；近年，在人工智慧/機械學習與結合大數據下分析所建構、追求的個性化服務，抑或原為合法蒐集之個資遭到不當處理，《個資法》上「知情同意」、「目的限定」、「資料蒐集最小化」等原則遭受嚴峻的挑戰，尤其在資料處理後難以追溯原有的蒐用背景，且當事人缺乏控制與資訊不對稱的情況下，當事人對於其個人之個資遭他人蒐集後進行何種方式之利用往往毫無察覺。例如：1.因技術演進將不被視為個資的廢棄資料轉化成有辨識特定人的個資；2.因技術演進將個資法排除的個資如公示資料、亡者個資等轉成個資；3.有缺陷的去識別化使得本不受《個資法》所保護的資料，再度恢復為可辨識出特定之個人，這些都對個人的隱私造成莫大威脅，也挑戰現有個資保護法規。這些人工智慧新技術的衝擊，也呼應前述《物聯網系統應用於可聯網車輛》指南所指出個資保護五大風險。

二. 自動化決策下的爭議

2.1 自動化決策與個資處理說明

在智慧自駕車的應用場域中，因為 1.安全考量，有低延遲高反應速度之要求；2.資料巨大，蒐用過程；及 3.人工智慧/機械學習導入之必要等，而有自動化決策之處理過程。所謂自動化決策，係指資料控制者透過演算法自動化處理個人資料，在無人為介入的情況下對當事人做成決策的過程。而隨著電腦軟硬體之快速發展，各界對於利用演算法處理個人資料的自動化決策與個人檔案剖析產生不少疑慮。由於自動化決策可能影響到個人的入學、求職及金融往來等重要權利，而使此等由電腦

決定人類之決策過程，其決策機制背後的演算法透明化問題與當事人之權益逐漸獲得重視。GDPR 設有針對自動化決策之具體規定，分別列在「個人資料保護指令」(Data Protection Directive)的第 15 條以及 GDPR 第 22 條，其他尚有 GDPR 與資料控制者通知義務有關的第 13 條與第 14 條、賦予當事人(資料主體)之資料存取權的第 15 條³¹⁰、以及解釋權之 GDPR 前言第 71 段。

人工智慧應用的過程可能涉及到大量個人資料之蒐用，加以自動化決策取代人類決策過程可能產生如資料運用錯誤所生的偏差與歧視、不透明、難以歸責之問題，並導致的法律與倫理衝擊；特別是在是以自駕車應用領域，前述問題所造成生命危害之可能，更應嚴肅以對。是故，於發展人工智慧應用之際，如何同時保護當事人之權益是值得重視的。從個人資料保護之角度，考諸歐盟因應人工智慧應用發展之趨勢所採之作法，以歐盟 GDPR 自動化個人決策以知悉人工智慧應用過程中有關於其資料的運用，進而能行使法律所賦予的權利。簡而言之，不論是我國《個資法》或是 GDPR，運用人工智慧而涉及個人資料之蒐用者，皆須符合個人資料蒐集、處理與應用之原則與要求。

2.2 自動化決策下的解釋權

有關自動化決策下之解釋權，依據歐盟第 29 條工作小組於 2017 年 10 月 3 日為因應歐盟 GDPR 第 22 條規定發布《自動化個人決策和分析指南》(Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 2018 年 2 月 6 日最新修正)³¹¹，建立對個人資料之自動化決策(automated decision-making)和個人檔案剖析(profile)的指南。

該指南旨在幫助資料控制者合乎 GDPR 對個人資料自動化決策和分析要求的一般性規則與最佳實施建議，內容重點包含幾點：1.自動化決策和分析的一般性規

³¹⁰ GDPR, Art. 15 Right of access by the data subject

³¹¹ European Commission. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01).
<https://ec.europa.eu/newsroom/article29/redirection/document/49826>

定 (GENERAL PROVISIONS ON PROFILING AND AUTOMATED DECISION-MAKING)；2.針對 GDPR 第 22 條中關於自動化決策的具體規定 (SPECIFIC PROVISIONS ON SOLELY AUTOMATED DECISION-MAKING AS DEFINED IN ARTICLE 22)；3.兒童和個人檔案剖析的建立 (CHILDREN AND PROFILING)；4.資料保護影響評估及個資保護長(DATA PROTECTION IMPACT ASSESSMENTS (DPIA) AND DATA PROTECTION OFFICER (DPO))。指南提出 GDPR 如何看待個人檔案剖析被使用：

- 個人檔案剖析之定義：意謂蒐集關於個人（或一群個人）的資料，並分析渠等的特徵或行為模式，加以分類或分群，區分特定的類別或組中，進行預測或評估。
- 原則禁止對個人資料包括有法律上或類似顯著影響之自動化決策的檔案剖析(“general prohibition on solely automated individual decision-making with legal or similarly significant effects, as described above.”)。
- GDPR 第 22 條第 2 項(a)之例外規定(Exceptions from the prohibition)：但有自動化個人決策之必要時，資料控制者必須能夠基於當事人明確瞭解下，提出分析、自動化個人決策的必要性，同時考慮是否可以採取侵害隱私較少之方法，應有措施保障當事人的權利和合法利益。
- 針對兒童須強化上述之資料保護

該指南關於在要求提供有關自動化決策與個人檔案剖析所涉及的邏輯上有意義的資料時，當事人有被知會的權利(Right to be informed)，資料控制者應遵守透明義務，以明確易懂的方法告知 (controllers to provide specific, easily accessible information)，並依據 22 條第 1 項，資料控制者必須，1.告知當事人渠等正在參與自動化決策與個人檔案剖析活動；2.提供有意義的資訊，包含處理之邏輯(logic)；3.解釋關於處理自動化決策與個人檔案剖析上有關重要性和預期後果的資料。

有關上述處理之邏輯(logic)，該指南特別有提到若為機械學習技術，確實會挑戰瞭解如何處理自動化決策與個人檔案剖析的作業邏輯(The growth and complexity of machine-learning can make it challenging to understand how an automated decision-making process or profiling works.)³¹²。除此，GDPR 要求資料控制者對於處理自動化決策與個人檔案剖析處理之邏輯(logic)，應以簡單的方法告訴當事人其背後的理由或依據的標準，並使當事人充分瞭解決策的理由，而不得以自動化決策所使用演算法進行複雜的解釋或者公開完整演算法而拒絕 (“The GDPR requires the controller to provide meaningful information about the logic involved, not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm. The information provided should, however, be sufficiently comprehensive for the data subject to understand the reasons for the decision.”)。

當資料控制者進行 GDPR 第 22 條第 1 項規定³¹³，當發生自動化決策或個人檔案剖析之做成無人為之介入，且該決策或剖析會對當事人產生法律效果或類似之重大影響的狀況時，依該條第 3 項規定，資料控制者須採取適當措施以保護當事人的權利與法律上利益。該些保護措施包括讓當事人在決策過程中要求人為介入、使當事人有權對該決策表達意見、或挑戰該決策等。又根據「歐盟第 29 條工作小組之指導文件」，該條之具體保護措施包含演算法之審查、遵循最少資料原則等，且該等保護措施須有助於降低自動化決策伴隨之風險³¹⁴。

由演算法做成之決策與個人檔案剖析可區分為兩種模式。第一種為本文第二章所提及的「規則式演算法」所執行的「自動化過程」(automated process)，指工程師先將規則定義寫入演算法中，爾後程式只是依照該寫入之已訂定規則，以電腦代替人力完成該已寫定規則所做出之決策過程。在此規則式「自動化過程」中，人類對於做成之自動化決策是完全可預測並可清楚追溯的，資料處理者清楚瞭解決

³¹² *Id.* at 25.

³¹³ GDPR, Art. 22. Automated individual decision-making, including profiling

³¹⁴ 鄭伊廷 (2021/03/10)，〈試析「一般資料保護規則」下自動化決策的解釋權爭議〉，《經貿法訊》第 279 期，頁 13-23。

策過程的所有過程與步驟，在進行解釋或歸責時不會面臨太大困難。另一種模式則為第二章所談人工智慧/機械學習的「自主式決策」(autonomous decision-making)的學習式演算法，於此決策過程中，模型中的變數、門檻值等都是由人工智慧/機械學習模型根據資料處理者輸入之資料自行定義，導致該資料處理者亦無從得知該如何做成決策，決策過程難以追溯及結果難以預期，在此種「自主式決策」下使得偏見、歧視、決策不透明與可歸責性等廣被質疑。這種以資料驅動之機械學習模型下的自動化決策過程與結果，更難以解釋，而這也是前述聯合國人權理事會《數位時代的隱私權》報告所警示的風險。

雖然GDPR的自動化決策與個人檔案剖析條文用語並無區分規則式與學習式演算法，《自動化個人決策和分析指南》雖然有特別提及機械學習，但並沒有明確區分這兩種自動化決策態樣。從GDPR前言第71段中所述，理應包括人工智慧/機械學習的自主式的決策過程，使電腦可以自主地運用資料控制者所提供之資料進行運算與剖析，以達成該自動化決策之目的。

人工智慧/機械學習演算法的不透明與多維度資料之串接，使得資料控制者所應負起之責任顯得更加窒礙難行。在人工智慧/機械學習驅動自駕車應用場域，所應用的資料相關廣泛且巨大，且高度自駕車亦有自動化之決策過程，克難點有1.資料與個資的界定?2.車外用路人個資如何遵守個資保護的規定?3.資料處理須即時反應，短短的幾微秒鐘必須完成;4.生命安全與個資保護如何平衡?

三. 「間接」定義再次被挑戰-智慧自駕車之「資料」-「個資」-「隱私」三者間關聯

按《個資法》將得以間接方式識別該個人之資料亦納入保護範疇，立法之理由在於，“因社會態樣複雜，有些資料雖未直接指名道姓，但一經揭露仍足以識別為某一特定人，對個人隱私仍會造成侵害，爰參酌一九九五年歐盟資料保護指令(95/46/EC)第二條、日本個人資訊保護法第二條，將「其他足資識別該個人之資料」修正為「其他得以直接或間接方式識別該個人之資料」，以期周全”。惟所謂「間接識別」屬不確定法律概念，不易由字面文義直接加以理解判斷，故另於《個資法施

行細則》第三條規範：「本法第二條第一款所稱得以間接方式識別，指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。」進而闡釋所謂「間接識別」：「指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人而言。」」

易言之，雖不能由所蒐集之資料單獨識別出特定個人，但若可與其他資料對照、組合或以連結方式而識別出特定個人，則該訊息資料即符合《個資法》所謂間接識別之定義，而屬於個資法保護之個人資料。

然而智慧自駕車紀錄之資料大都為當事人行為之足跡，即使為破碎、零散之資料，透過人工智慧/機械學習之革命性應用將巨量的自駕車感測器蒐集之資料，自動轉化成一般性或敏感性個資，此過程模糊化「資料」-「個資」-「隱私」三者之間的界線，片段瑣碎的個人活動資料經由一連串的結合或持續追蹤，刻劃出當事人的樣貌，從而給隱私權帶來的挑戰和衝擊。基於數據化之資料可量化一切並透過人工智慧/機械學習忽略資料與結果間因果關係，傳統的隱私權概念已經不能解釋由現今資料經濟下之商業行為而衍生的相關交易手段、消費習慣、群眾心理是否屬於傳統對於隱私保障之範疇，2010年Facebook創始人Mark Zuckerberg提出「隱私不再是一項社會標準。」的觀點；2013年Google首席工程師Vint Cerf在美國聯邦貿易委員會(US FTC)的談話中表示，隱私也許是一個異常的概念(privacy may actually be an anomaly)³¹⁵，可能從歷史上的一些經驗可以幫助我們適應一個即將到來的透明社會，呼應學者Froomkin教授所提出“隱私已死(The Death of Privacy)?³¹⁶”的質疑。這些對於隱私侵害之疑慮在智慧自駕車的領域中更形突出。

³¹⁵ Jacob Kastrenakes (2013/11/20). *Google's chief internet evangelist says 'privacy may actually be an anomaly'*. THE VERGE. <https://www.theverge.com/2013/11/20/5125922/vint-cerf-google-internet-evangelist-says-privacy-may-be-anomaly>

³¹⁶ Froomkin, A. M. (1999). The death of privacy. *Stan. L. Rev.*, 52, 1461. Available at SSRN: <https://ssrn.com/abstract=2715617>



四. 刪除權的行使

由於人工智慧/機械學習與大數據應用都是採用大量資料統計或推論的功能，如果個別資料當事者要求刪除，到底是刪除原始資料，還是達到去識別化的階段？在最高行政法院 106 年度判字第 54 號判決健保資料乙案中，法院認為刪除權對資料庫的完整有重大影響：“如果容許少數人退去，基於執法平等性之要求，多數人也可比照辦理，如此可能引發退出風潮，形成「破窗效應」，造成資料蒐集投入成本之虛耗”，此案於 2022 年 8 月憲法法庭 111 年憲判字第 13 號判決之判決主文第 4 項部分(第 68 段)：“當事人就獲其同意或符合特定要件而允許未獲當事人同意而經蒐集、處理及利用之個資，仍具**事後控制權**，**不因其曾表示同意或因符合強制蒐用要件，當事人即喪失請求刪除、停止利用或限制利用個資之權利**”及“就健保署[將]個人健保資料提供公務機關或學術研究機構原始蒐集目的外利用，**當事人之停止利用權應仍受憲法第 22 條規定保障**”。憲法法庭命令相關機關“應於 3 年內，修正健保法及相關法律，或制定專法**明定請求停止利用及例外不許停止利用之主體、事由、程序、效果等事項**”。針對刪除權另外有學者認為刪除權的任意行使³¹⁷，反而可能影響到資料控制者的財產權。

以與台灣一樣都有全民健保的英國為例，該國國民保健署 (National Health Service, NHS) 做法為國民有兩種選擇將其個人資料退出(Opting out of sharing your data) 英國國民保健署中央資料庫 (NHS Digital)³¹⁸的個人資料分享方式，態樣一是拒絕全科醫師診所 (General Practitioners Surgery)將自己的醫病資料上傳到 NHS Digital (Stop your GP surgery from sharing your data)，態樣二是即使全科醫師診所將資料上傳資料庫後，當事人亦可拒絕 NHS Digital 將資料分享給研究或計劃使用時 (Stop NHS Digital and other health and care organisations from sharing your data for

³¹⁷ 黃章令(2020)，前揭註 95，頁 151。

³¹⁸ NHS Digital. <https://digital.nhs.uk/>

research and planning)³¹⁹。

就 NHS Digital 案例，本文提出三議題：首先在此所指的「資料」應該是「原始資料」，如果是後續源於「資料」產生的「資訊」(information)那是否當事人可要求行使刪除？從科學角度，那資料是否還具有價值？安全性如何評估³²⁰？其次是在技術層次，因為人工智慧/機械學習使用資料訓練模型，如果刪除原始資料，除了導致改變原訓練模型結果正確性，更而影響汽車使用安全外，亦可能導致整個訓練模型須要重新訓練，對於財產與技術發展有重大的影響；第三，若資料屬廢棄資料，一開始蒐集階段不屬於個資，資料的刪除是否會影響資料控制者的財產權，亦是一個爭論的課題。基於上述刪除權以現階段技術難以實施、需要重新執行乙次流程，代價實在太高、或導致「破窗效應」等，目前實務上的作法都只是要求去識別化到無法辨識當事人即可。

綜上，NHS Digital 值得本文參酌之處在於敏感性個資的處理、刪除與目的外之使用的狀況；但不同之處在於新興科技人工智慧/機械學習的導入智慧自駕車，且智慧自駕車資料使用有立即、必要的安全上考量。

第十一項 資料、個資與個資法適用說明

綜合前述，資料、個資與個資法適用之流程可表達如下圖 56 所示，資料與個資間的界線因為人工智慧/機械學習、大數據、物聯網等技術而變得模糊，舉凡只要是當事人產生的足跡，都可能變成數位足跡，而該數位足跡數據都可能轉變成能識別特定人的個資，惟該個資是否為個資保護法所規範之個資？則端視各國法規所規範。若再檢視是否有個資法排除適用的狀況。

³¹⁹ NHS (2021/08/20). Opt out of sharing your health records. <https://www.nhs.uk/using-the-nhs/about-the-nhs/opt-out-of-sharing-your-health-records/>

³²⁰ 周玉文、劉芝吟 (2021/06/07)，〈AI 助陣醫學、防疫，個人隱私難兩全？〉《言之有物》，中央研究院。

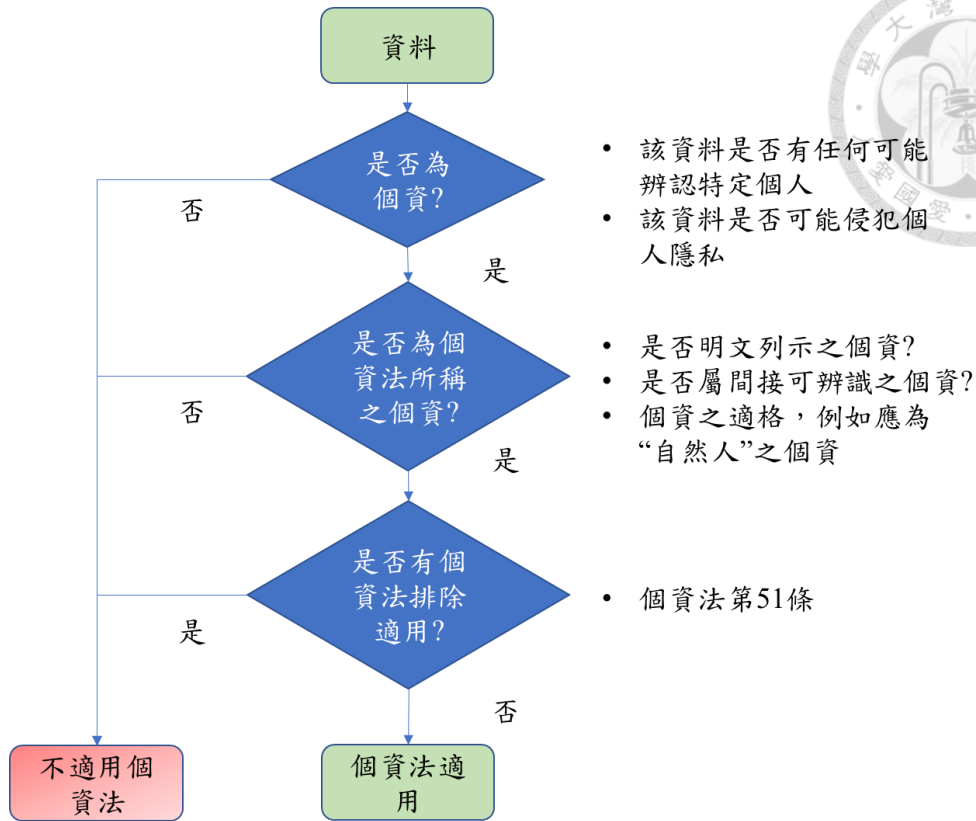


圖 56. 資料、個資與個資法適用流程圖。資料來源：本文整理

以本文自駕車的運用場域，由於有很大一部分的資料都於個人行為有關聯，所以都可能被視為個資，例如車子的 GPS 紀錄，車內外的影音資料等。而這些大量、長期監控或者於其他資料結合之資料，透過人工智慧/機械學習技術導入，也容易突破無法辨識特定自然人的侷限，轉化成個資法上所謂之個資。

以我國現行的《個資法》而言，若被視為《個資法》上所謂之個資，就須遵守該法的資料處理原則。而智慧自駕車之資料利用，實務上就有可能違反《個資法》及侵犯隱私的疑慮。

第二節 社會公益與私人個資權益取舍



第一項 個資保護與個資法保障

在本文第二至第三章已清楚介紹各國個資保護精神及保障內涵，然而基本的問題在於：1.現有個資保障是否可完全適用於自駕車資料利用?2.在自駕車的利用環境中，是否生命法益應高於個資保護?3.面對自駕車及於一身的高端科技如人工智慧/機械學習，其個資之定義、保障之範疇與排出個資法適用之條件，既有各國個資保護法規是否能否適用?4.歐盟與中國另訂的自駕車個資保護是否是一個趨勢?我國《個資法》如何因應?

第二項 公益性的討論

前面所談的自駕車安全性為首要考量，而生命法益之保障應是普世公認價值，優先於隱私或者個資保護。其次是，自駕車的公益性質與個資保護之權衡。回顧我國個資法的立法理由在於同時保障當事人之人格權以及資料的合理利用，本文第三章已羅列相當多新科技與對於隱私侵害及個資保護上的探討，然而除了安全性的考量之外，前案之公益性質相比本文的自駕車應用如何?下面就前面數個個案相對自駕車資料利用的公益性討論。

自駕車的資料利用，其公益價值遠大於 Google 街景圖，Google 街景圖雖然被證實有巨大的商業利益，亦帶給生活許多便利，然而相較自駕車環保及因應人口老化的環境，兩者間公益性質高下立判。第二，借鏡全民健保案例經驗，雖兩造對於健保資料的開放研究公益性並無爭論，然而基於自駕車資料利用的急迫性與不可替代性，本文認為自駕車個資利用的公益性還是略勝一籌。第三，與狗仔跟追的案子相比，自駕車資料利用有其**客觀**且區分為短中期之**資料利用必要性**，本文亦認為自駕車資料利用還是遠勝於狗仔跟追的案例。

綜上，基於資料驅動的智慧自駕車，深入探討所謂自駕車社會公益的意涵，有短短零點幾秒間即時反應的生命法益之保障;亦有短中期效應之節能、減少塞車提升經濟的社會經濟價值;長遠觀之，及老化與身障人口必須仰賴自駕車交通的必要價值。故自駕車之資料利用有其**客觀**、**明確**且**必要**之社會公益。



第三節 法令遵循與風險管控

第一項 智慧自駕車個資風險

綜前之所述，各國對於個資與隱私保護有共同目標，然因各國立法理由及規定有所差異，故以下就我國《個資法》角度簡單羅列幾個可能智慧智駕車面臨的個資保護風險。

1. 高於最低需求的資料蒐集

綜前之所述，智慧自駕車因為安全問題、人工智慧/機械學習計算或者軟體 OTA 更新等問題，常會有過量的資料蒐集。資料蒐集會高於最低需求來源有二：其一，在於自駕車採用 OTA 更新技術，故硬體規格上(如解析度，記憶空間等)必須高於目前之規格。其特性如同我們電腦或手機，透過上網的軟體更新，其要件為硬體能處理更新的軟體功能;若硬體功能只以現今之最低功能來設定，來日新的軟體更新，硬體將不能勝任。其二：在於人工智慧/機械學習以資料來驅動，質優量多的資料才能建立好的模型，然而到底需要多少資料才能達到一定的安全水準，這是初期無法估量的。

是故，如何遵守各國個資保護法的最低資料蒐用原則，在人工智慧/機械學習的運用下是一個具挑戰的問題，目前各國並沒有明確的規範。《汽資安全規定(試行)》第六條第一項第 3 款有「精度範圍適用原則」：“根據所提供功能服務對資料精度的要求確定攝像頭、雷達等的覆蓋範圍、解析度”。

2. 管理的對象

中國大陸的《汽資安全規定(試行)》將設計、生產、銷售、使用、運維等過程中的涉及個人資訊資料和重要資料皆列為汽車資料，以台灣為全球供應鏈的一環，必須注意可能觸犯第三國法規而不自知。

3. 一般個資與敏感性個資處理



如前所述，自駕車因為有安全之首要考量，有其蒐用敏感性個資的必要。自駕車所擁有的巨量一般性與敏感性個資，因應各國規定不同，會有跨國管理上的法遵風險。

4. 車內外生物辨識技術運用

生物辨識之資料一般被列為特種個資，然各國明文例示之自駕車特種個資有所不同，應遵守不同國家規定。

5. 資料庫交互連結

資料之結合是既有個資法的重點，是以蒐用資料非必要不要做資料間結合；若有資料結合，避免非必要的特定人或族群的辨識處理；若有必要，也儘量以去識別化或匿名化處理。若符合 GDPR，則可以個資資料匿名化與假名化處理。

6. 目的外使用

如前所述，自駕車資料之蒐用，除了立即性的生命安全保障之外，尚有其他節能、計算最佳路線、資料回饋、舒適等其他的考量，而在人工智慧/機械學習的新演算法適用，目的未必能夠能於一初始即明確得知。過於限制目的外的使用，會阻礙自駕車的功能發展。

7. 不透明/使用者與用路人的隱私擔憂

資料轉變成間接可辨識個資的過程，除了資料間的結合，還有資料的長期持續性的監控。自駕車蒐集大量且持續性的資料，透過車聯網結合資料，這些資料又在高速的車輛端及雲端運算的人工智慧自動化運算，過程大量蒐用疑似個資且過程不透明，造成個資及隱私的可能侵害。

8. 用路人個資難以告知

我國《個資法》及判例對於公示資料是否適用個資法尚有爭議，對於用路人的影像資訊並沒有特別規定，相對的目前有歐盟 GDPR 及中國大陸的《汽資安全

規定(試行)》皆有將用路人個資，特別是人臉辨識放入《汽資安全規定(試行)》條文規範中，一旦用路人資料被視為個資如何遵守既有個資保護原則尚有疑慮，首先就是用路人個資告知難題。對於此問題《汽資安全規定(試行)》有明確規範，比照 Google 街景圖處理方式。

9. 車輛資料聯網

目前我國《個資法》或《無人載具科技創新實驗條例》等規範並無車內優先處理之原則，然而 GDPR 及中國《汽資安全規定(試行)》皆有規範車內處理原則，是故車子的任何資料，在非必要的情況下，還是優先車內處理。有必要聯網之資料，儘量去識別化。

10. 持續監控

如前述之大法官釋字 689 號解釋及第 1096 號最高法院刑事判決，隱私侵犯之可能，在於持續對當事人之監控。故個資之辨識與隱私的侵犯，除了資料間的結合，亦可能發生於持續性的監控。透過對特定自然人的持續監控，也可描繪當事人的行為態樣進而辨識該特定人。為避免相關的資料利用或研究違反個資保護之規定，應儘量將資料匿名化或去識別化後再利用。

然而，現今個資保護之法規，除了資料之結合外，尚未規範持續性資料之擷取，然自駕車與車輛使用人之生活息息相關，持續之監控也有侵犯個人隱私之虞，此點也是自駕車個資保護法規未來需要特別探討之處。

11. 國際傳輸

我國個資法對於國際傳輸的規定與各國現有規定不同，採較為寬鬆的管理；再者國際有越趨嚴格規範的趨勢。對於自駕車的巨量資料傳輸管理，必定會有在國外實施的差異。故企業應注意國際傳輸的法遵風險。

12. 刪除權

刪除權規定始於 1995 年歐盟個資保護指令第 12 條，在資料存在「不正確」或「不完整」的情形時，得行使「刪除權」。刪除權源自當事人對於其資料的控制權，並於 GDPR 第 17 條中則更進一步發展出「被遺忘權」，該條規定認為除資料不正確或不完整外，在有其他事由時，當事人(資料主體)均得要求刪除控管者所握有之個人資料，甚至控管者有義務通知其他處理該個人資料之控管者刪除。

然而對於資料的刪除，是否能擴及源自資料的資訊權？這問題不論在人工智慧/機械學習或者統計上都會造成資料庫完整與正確性等問題。另一個問題在於若始廢棄資料不屬於個資之範疇，那後續的資料再歸屬於個資，是否當事人都保有上述全部的權利？

第二項 自駕車個資法令遵循原則

一. 落實個資處理原則

1.1 落實目的限制原則

自駕車以安全為第一要務，在我國《個資法》第 20 條第一項第 3 款基於免除當事人之生命、身體、自由或財產上之危險的特定目的外之利用規定；另第 19 條第一項第 6 款及第 8 款亦有目的內合理蒐集處理或處理個資的依據。自駕車因為蒐集到目的外之資料，並透過自動化處理可能辨別特定人並侵害當事人之隱私。本於目的限制原則，資料控制者應該有內部資料之倫理管理指南，落實目的限制原則，刪除不必要之資料及避免可能侵害隱私的資料處理及利用。

1.2 落實個資處理最小化原則

資訊隱私權侵害的基礎在於資料的多寡。落實個資蒐集最小化為原則，對於不能確認為個資之資料，要符合前述蒐用之目的。

1.3 資料邊緣處理為原則(不連線上網)

資料與個資之轉換，常在於資料結合，具體實施的常見態樣就是連線上網。

故資料應以車內處理為原則。中國大陸也已經有明確規範。



1.4 資料在地化，避免國際間傳輸

同前所述，企業內部法遵應注意國際對於資料傳輸的規範趨勢，跨國企業儘量將資料在當地處理，降低國際傳輸的可能。

1.5 資料匿名化與假名化


就本文前面文獻之討論，資料匿名化與假名化是目前公認的現今個資管理重點。資料控制者應重視資料匿名化與假名化，並引進相關資料保護之技術，並做協力廠商之上下游個資保護認證。

1.6 評估對個人隱私是否有損失

按我國《個資法》第 15 條及第 19 條規定，無論公務或者非公務機關只要在特定目的下個人資料蒐集或處理對於當事人(資料主體)權益沒有造成侵害，即可合法為之。以前述不論街口監視器、大樓監視器、車用行車紀錄器等公共場合之應用，可參照法務部法律字第 10603505040 號函釋，依我國《個資法》第 19 條應強調依法蒐用目的的正當性、不做目的外使用，並在我國同法第 5 條比例原則規範下，儘量降低該行為對當事人隱私的傷害。


二.以中國及歐盟個資保護為例之法令遵循

對於從事汽車行業的相關市場主體而言，國際化的供應鏈串接與協力商間的配合是汽車產業的常態，因應不同法規的個資管理是相當艱難的任務，也是自駕車個資法遵之所以重要的原因。不論中國《汽車資料安全規定（試行）》或歐盟《聯網車輛與移動相關產品涉及個人資料處理指南》都有較為台灣《個資法》明確且廣泛的資料控制者的定義，前兩者皆規定相較嚴格的智慧自駕車個資保護標準，且在模糊的用路人的資料及 GPS 資料等明文例示為個資。以下針對不論在中國或歐盟有業務之台灣自駕車企業建議從以下幾方面著手準備，並將隱私設計的概念導入企業，以期最大程度地降低企業運營的侵犯隱私權的風險：

- 
- 在設計、生產、銷售、運維、管理汽車過程中就考慮資料安全問題，檢視資料依據安全性必要性與否分級，盡可能減少汽車資料蒐用的資料量。
 - 瞭解各國個資保護法規針對明文例示一般性個資及敏感性個資的差異，另外 GPS 位置資料，降低跨國遵法風險。
 - 利用大資料進行商業化運作和保障用戶的知情權的同時，採取去識別化技術保障措施對資料採取假名化和匿名化處理，以及防止資料濫用或被協力廠商運用。
 - 承上，若資料為敏感性/特種個資資料，應取得當事人事前書面同意。
 - 承上，若資料屬大陸特別規定的重要資料，應遵守《汽車資料安全規定（試行）》有關重要資料的處理規則。
 - 資料車內處理原則，除非確有必要不向車外提供。
 - 建立國際當地資料中心：對於跨國企業或研發中心在境外的台灣企業，在商品化國境內建立當地資料中心，若無必要不對境外傳輸資料。
 - 設立符合 GPDR 資料保護長或《中國個資法》個資保護負責人，對企業現有資料處理系統進行檢視，對明顯不符合 GDPR 及《汽車資料安全規定（試行）》要求的業務操作及時進行調整，並儘早考慮制訂符合法規要求的內部制度和體系。

另外由於 GDPR 及《中國個資法》與台灣《個資法》存在不少差異，台灣的個資法遵已經不足應付 2021 年 10 月施行《汽車資料安全規定（試行）》及 2021 年 11 月施行的《中國個資法》。相較歐盟與台灣，中國與台灣在製造業上下游及商業上有更密切之合作關係，因此對於自駕車個資之法令遵循工作是台灣自駕車產業鏈企業必須執行的專案項目。本文以下整理出幾點與自駕車資料相關之法遵項目：

1. 台灣企業要在當地設立據點或指派代表



同歐盟 GDPR 之規定，2021 年 11 月開始，若在中國設點的台灣企業，如果因為「從境外對中國境內消費者提供商品或服務（例如跨境電商）」，或「分析、評估中國境內自然人的行為（例如線上行為追蹤）」，因而適用《中國個資法》的話，就必須在中國境內設立據點（專門機構），或者指定個資代表，負責處理個人資料保護相關事宜，並擔任主管機關的聯絡窗口（《中國個資法》第五十三條參照）。

2. 個資蒐集須透明且符合法規細節

台灣企業在取得歐盟居民或中國自然人的資料前，要揭露法定資訊，而且要以「顯著方式」、「清晰易懂的語言」，將前述資訊以「真實」、「準確」、「完整」揭露。鑒於台灣個資法沒有規定這麼細緻，台灣企業在台灣本土的現行作法很可能不符《中國個資法》之要求（《中國個資法》第 17 條參照）。

3. 決策的透明度，無差別、無歧視待遇之合理結果

《中國個資法》明文禁止透過自動化決策對消費者不合理或差別之作法，依該法第二十四條第一項規定：「個人資訊處理者利用個人資訊進行自動化決策，應當保證決策的透明度和結果公平、公正，不得對個人在交易價格等交易條件上實行不合理的差別待遇。」

同條第二項：「通過自動化決策方式向個人進行資訊推送、商業行銷，應當同時提供不針對其個人特徵的選項，或者向個人提供便捷的拒絕方式。」

同條第三項：「通過自動化決策方式作出對個人權益有重大影響的決定，個人有權要求個人資訊處理者予以說明，並有權拒絕個人資訊處理者僅通過自動化決策的方式作出決定。」

台灣企業若利用自駕車或其他個人資料作成自動化決策的時候，要保證決策的透明度，以及結果的公平、公正，不可以對消費者有不合理的差別待遇，例如商品價格的差異。另外，自駕車產業資料控制者如果以自動化決策方式，作出對消費者權益有重大影響的決定，消費者有權利要求企業說明，也有權拒絕企業只利用自

動化決策就作出決定。



4. 公開場所之攝影機，不能用來分析客群輪廓

在大數據、人工智慧等相關技術下，利用營業場所攝影機拍攝到的客戶影像，分析客戶的性別、年齡等屬性，甚至追蹤客戶在場所內的行動軌跡，進而做出商業決策，已經不是新聞。但《中國個資法》禁止得到同意前此類行為，在公共場所安裝攝影機之類的身分識別設備，只能用於「維護公共安全」的目的，並且要設置顯著的提示標識(第二十六條參照)。同理，自駕車對外所攝錄之公示資料若涉個資，理應遵守《中國個資法》及《汽資安全規定(試行)》相關規定。

相對地，如前第三章案例分析，我國並沒有相關的規定，甚至將之因公示性排除《個資法》保護範圍。是故，我國自駕車在公開場合所拍攝到之資料並沒有被規範。跨國智慧自駕車廠商必須注意國際營運的個資法遵風險。

5. 注意公開資料使用及當事人之權益

台灣企業如果為了精準瞭解中國境內自然人客戶，在網路上取得客戶的公開資料，可以在合理範圍內處理，但客戶可以拒絕。惟若對客戶產生重大影響，就必須取得客戶的同意後得以為之(《中國個資法》第 27 條參照)。

6. 兒童及少年個資屬敏感個資

未滿 14 歲的兒童、少年資料，在《中國個資法》是敏感資料，台灣企業以兒童、少年作為處理個資的對象時，必須檢視特定目的與充分的必要性，採取嚴格的保護措施，並且告知處理資料的必要性，以及對個人權益的影響，取得父母或其他監護人的同意，甚至建立處理兒少資料的專門內部管理程序，否則很可能就會違法(《中國個資法》第 28 條至第 31 條參照)。

7. 注意境外傳輸的差異，嚴格的合法條件為國際主流

依台灣《個資法》第 21 條，我國個人資料跨境傳輸至境外，採原則開放，

例外禁止原則，但企業應注意國際的趨勢則相反，並且合法條件愈趨嚴格。台灣企業如果在歐盟或中國境內儲存個人資料，若有境外傳輸必要時，必須滿足 GDPR 及《中國個資法》規定，以中國為例，如：通過中國政府的安全評估、經專門機構認證、與境外接收方訂定中國政府制定的標準契約條款等後，得以為之。

此外，在傳輸個人資料到境外前，台灣企業要向客戶告知境外接收方的相關資訊，包含客戶可以向境外接收方行使《中國個資法》上的權利、方式和規範原則，然後取得客戶單獨同意，才是合法。另《數據出境安全評估辦法》將於今年(2022年)9月1日起施行，相關規定及案例值得台灣企業注意。

台灣企業若在大陸大量雇用大量員工時應特別留意，如果處理的個人資料達到規定的數量，原則上只能將資料儲存境內，若要傳輸境外，必須通過中國政府的安全評估(《中國個資法》第38條至第40條參照)。

8. 資料可攜權

為打破資料壟斷的障礙及尊重當事人資訊自主權，《中國個資法》導入歐盟 GDPR 的資料可攜權，允許自然人在符合中國政府規定的條件時，可以要求企業將個人資料轉移給指定的其他企業。

台灣《個資法》目前沒有這個規定，所以台灣企業除跟進中國政府的規定條件外，也要儘早評估因應方式，滿足中國客戶行使的資料可攜權(《中國個資法》第45條參照)。

9. 處理大量個資的台灣企業，要指定個資保護負責人

類似歐盟的個資保護長 (Data Protection Officer, DPO) 規定，《中國個資法》要求處理個資逾政府規定數量的企業，必須指定個資保護負責人，任務是監督企業對個人資料的處理以及保護措施。企業也須公開個資保護負責人的聯絡方式，並將有關資訊送交主管機關(第五十二條參照)。台灣企業若為符合前述之資料控制者，應注意相關規定。

10. 個資保護影響評估

台灣企業處理個人資料，如果包含《中國個資法》規定的情形之一時（例如處理敏感資料、利用個資作自動化決策、委託處理個人資料等），必須事前執行個資保護影響評估（類似歐盟的 DPIA）。評估內容也須遵守《中國個資法》規定，包含如處理目的或方式的合法性、正當性、必要性，或是對客戶的安全風險、保護措施等（《中國個資法》第 55 條及第 56 條參照）。

在罰則規定部分，《中國個資法》按照違法情節輕重，有不同處罰程度：

- 輕者限期改正、沒收違法所得、暫停或終止違法的應用程式（app），不改正則處人民幣 100 萬元以下罰款，對企業主管及其他應負責人員，也可處人民幣 1 萬元以上 10 萬元以下罰款。
- 重者除限期改正、沒收違法所得外，並處人民幣 5 千萬元以下，或前一年度營業額 5% 以下罰款，也可令停業或吊銷業務許可、營業執照，另對企業主管及其他應負責人員，可處人民幣 10 萬元以上 100 萬元以下罰款，還可禁止在一定期限內，擔任相關企業的董事等高階經營者和個資保護負責人。

以兩岸商業往來之頻繁，製造業上下游分工合作之密切，《汽車資料安全規定（試行）》及《中國個資法》對於台灣自駕車之發展影響更甚於 GDPR，建議台灣企業切勿忽略，應詳實檢視對於兩岸的法遵差異。若有疏失，除罰金以外，最重可能會因此被中國政府驅出市場。

第三項 生物特徵辨識之監管

GDPR 鑒於生物特徵識別資料之高度個人屬性，將其納入特種個資加以規範。於第 4(14)條定義「生物特徵識別資料」為：透過特定技術處理所得，且允許或確認具特定識別性之個人身體、生理或行為特徵資料，例如臉部影像或指紋鑑識資料。進一步於 GDPR 第 9(1)條之規定，在處理（processing）用以識別自然人之生物特



徵識別資料時(biometric data for the purpose of uniquely identifying a natural person)，原則必須予以禁止，除非具有 GDPR 第 9 條其他各款之正當化事由，與符合相關規定時，始得為之。同樣的，美國加州已立法限制公眾場域人臉辨識的應用，公共區域的隱私權與個資保護已經越來越趨於嚴格。



以自駕車而言，相關技術的運用與生命安全保障之間有緊密連結，其法規管理是否應制定特別法?目前看來就歐盟及中國法規已經有這種趨勢。


第四項 跨境規範

我國企業有許多境外業務，個資資料的跨境傳輸依我國個資法 21 條是原則上允許，例外禁止。但相較下歐盟 GDPR、中國《中國個資法》、《數據出境安全評估辦法》都有採原則禁止的嚴格的境外傳輸限制。對台灣廠商實質上影響可能為以下幾點。

一.在國際未設有據點之台灣企業依然可能受到規範

《中國個資法》借鏡歐盟 GDPR，明文對境外實施的個人資訊處理活動者為該法所管轄之對象。GDPR 原則禁止資料控制者將在歐洲經濟區 (European Economic Area, EEA) 內蒐集之歐盟居民個資跨境傳輸至 EEA 以外國家，除非符合特定情形，如 GDPR 第 45 條歐盟執委會認定 EEA 以外國家提供充分程度之個資保護；同法第 46 條資料控制者或處理者已提供適當保障，如歐盟各國個資保護主管機關核准的拘束性企業規則 (Binding Corporate Rules, BCRs) 或歐盟執委會採納的標準契約條款 (Standard Contractual Clauses, SCCs。2021 年 6 月發布最新版)³²¹；第 49 條規定特別情形，如當事人明示同意、傳輸係為執行與當事人間契約所必要。其中歐盟執委會的充分保護認定及 SCCs，為實務上企業最常用的跨境傳輸

³²¹ European Commission (2021/06/04). *Standard Contractual Clauses (SCC)- Standard contractual clauses for data transfers between EU and non-EU countries*. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en



依據。而在中國自駕車資料控制者，《汽資安全規定（試行）》第十一條(境內儲存)及第十二條(出境核查);《中國個資法》第3條，在大陸境外處理境內自然人個人資訊的活動若符合下列條件之一，將有該法之適用：1.以向境內自然人提供產品或者服務為目的；2.分析評估境內自然人行為；或3.法律、行政法規規定的其他情形。自駕車產業鏈廠商，若涉及分析、評估大陸境內自然人行為。《中國個資法》雖未對「分析、評估」加以定義，但從該法對於自動化決策的定義可以推知，此處的「分析、評估」，應包含透過網路追蹤分析使用者行為。換言之，自駕車服務業者利用網站使用 cookie、OTA 軟體下載或 App 使用識別碼等追蹤自駕車使用者或乘坐者之足跡、分析該車輛使用者偏好，即可能構成分析、評估大陸境內自然人行為，並因此需要遵守《中國個資法》。

二.台灣企業可能受到跨境傳輸之規範

即使不直接面對歐盟公民或大陸自然人，台灣業者也可能因與大陸業者業務配合而間接需要遵守當地法律。

以中國大陸為例，台灣業者如自大陸業者取得大陸民眾個人資訊，特別是台灣企業在大陸設廠，將大量大陸員工的個資傳輸回台灣總部之人資部門，將構成大陸個資之境外傳輸。《中國個資法》除透過境外適用條文實現直接適用外，還以專門章節規範個人資訊跨境提供，確保該法保護標準間接適用於境外個資接收方。

《中國個資法》第38條明文要求提供至中國境外的個人資訊，其處理應達到該法規範的保護標準。保障適足保護的工具，包括個人資訊保護認證、簽訂網信辦制定的「標準合同」等。台灣業者作為個人資訊的境外接收方，可能會被要求配合認證，或簽訂標準合同，從而基於認證或契約而有義務遵守《中國個資法》。視與大陸業者的合作模式不同，台灣業者可能作為個人資訊處理者，獨立承擔個人信息保護義務；也可能作為處理個人資訊的受託人，需採取必要措施保障個人資訊安全，並協助委託方履行個人資訊保護義務。《汽資安全規定（試行）》第十一條（境內儲存）規定“重要資料應當依法在境記憶體儲，因業務需要確需向境外提供的，應當透過國家網信部門會同國務院有關部門組織的安全評估”，及第十二條(出境核查)

規定“汽車資料處理者向境外提供重要資料，不得超出出境安全評估時明確的目的、範圍、方式和資料種類、規模等”。

綜上之所述，自駕車的資料控制者，擁有個人資料及重要資料，除了車內儲存之外，另外建議在服務當國設定伺服器將資料以當地儲存為先，對於境外傳輸，應該遵守國際的管理機制。

三.瞭解各國個資法基本的不同並作出對策

自駕車廠商要確認自己的公司是否會受到 GDPR 或《中國個資法》、《汽資安全規定（試行）》的管轄，可分幾個階段檢視，只要符合任一條件，就有受前述兩法規範之可能：

1. 公司是否在歐盟或中國境內有實體營運？
2. 公司是否有銷售商品或服務給歐盟居民或中國居民？縱使公司在歐盟或中國境內並無實體營運，只要公司對歐盟或中國居民販售商品或服務（例如網路商店或網路服務），都有可能被認定為受到 GDPR 或《中國個資法》的管轄。
3. 縱使公司在歐盟或中國境內無實體營運亦無透過網路販售商品或服務給歐盟或中國居民，猶然要確認公司是否有因為任何其他原因接收或處理歐盟或中國居民個人資料？
4. 公司是否有透過網路或任何方式監督歐盟或中國居民的個人行為？這些所謂個人行為，這包含了在網路上取得網頁瀏覽者的所在地資料、網頁瀏覽歷史資料 (cookies) 等可以辨識特定自然人的資料。
5. 除此，《汽資安全規定（試行）》所稱之汽車資料的包含汽車設計、生產、銷售、使用、運維等過程中的涉及個人資訊資料和重要資料。所以只要是自駕車之產業鏈之台灣企業或協力廠商，都應該注意相關法規之規範。

第四節 隱私設計(Privacy By Design)理念的導入

第一項 個人資料保護、合理利用與隱私權保護



如本文第二章針對隱私及個資之探討，隱私權之保護為全球主流的趨勢，也是在資訊時代的普世價值。隱私理應為客觀存在且社會普遍認同之事務，然所謂隱私之概念隨時代發展與社會輿論變遷，迄今猶屬內涵未明之狀態；相應的，隱私權作為一種法律上的隱私權利，為一種帶有法律意識的價值判斷，台灣透過人格權之法律表彰，以維護人性尊嚴與尊重人格自由發展。然而無論我國或他國的個資保護法規，對於何謂個資及所對應保障的隱私權利皆有混沌未明之處，法律之保障同樣會隨科技發展、社會輿論及不同時空背景有所變化，難謂對隱私保障已完備。

近 10 年來包括大數據、物聯網、人工智慧/機械學習等新興技術的普及，對於隱私侵擾的態樣不斷演變，隨之影響的就是對於所謂「個資」及「個資法所謂之個資」之定義不斷調整。透過前述的自駕車法規或指南亦可看出明文例示之個資，也不斷增加。以下是本文針對「隱私」、「個資」、「個資法所謂之個資」及「資料」間關係圖示如下圖 57，本圖中為二維之象限，橫軸右側為「積極利用」；橫軸左側為消極保護。縱軸為保護的法律層次，下面為憲法層次，上面為法律到行政命令的層次。

從《個資法》定義，個資除了消極的保障隱私權及人格權，從個資具財產權的觀點觀之，亦有活化經濟，驅動資料經濟動力的積極正面利用；另從自駕車的個資蒐用觀之，更有保障生命法益，優先同屬基本人權隱私權的合理利用。本文在綜合前面幾章討論，將圖 27 進一步的細分如圖 57。在圖 57，就本文第二章所的隱私文獻研究，隱私權比較偏向消極保護，並沒有積極利用的探討。而相對隱私權的，個資法規除了具有積極利用的目的，並賦予財產權；個資法規亦具有保護人格權及隱私權的消極目的。而隱私權與個資法相較，隱私權包含不被個資法涵蓋部分，亦包含部分資訊隱私權的個資。隨著公示性質越高，代表越不具隱私權保護的意義。

「隱私」、「個資」及「資料」間界線因為先端技術之演變越趨模糊，是故若

要有更高水準之超前布署，就應當導入「隱私設計」之概念並落實。

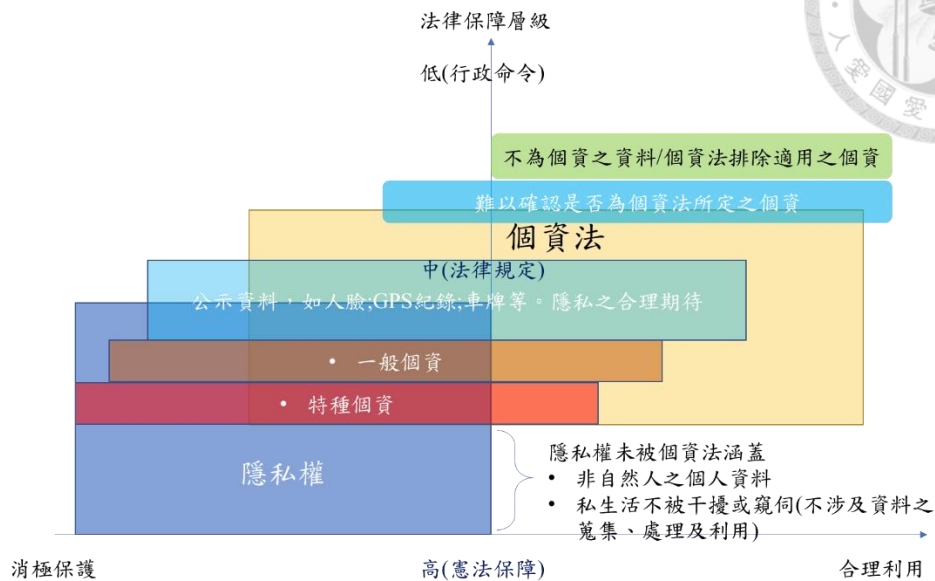


圖 57. 「隱私」、「個資」、「個資法所謂之個資」及「資料」間關係。資料來源：本文整理

第二項 隱私設計(Privacy By Design)介紹

承前針對「隱私」、「個資」及個資保護的不確定性，唯一有共識的如何保障普世價值的隱私權。「設計隱私」(Privacy by Design)和「默認隱私」(Privacy by Default)一直是與個資保護相關的熱門話題。設計隱私的第一個想法是在 1970 年代表達的，並在 1990 年代被納入 RL 95/46/EC 數據保護指令。根據 GDPR 的第 25 條，在規劃處理系統時必須已經採取技術和組織措施 (Technical and organisational measures, TOM) 以保護數據安全。通過「設計隱私」的理念，將個資與隱私保護主動且預防性的嵌入產品或服務全週期期間。

「設計隱私」是一種系統工程方法，最初由 Ann Cavoukian 開發，並由安大略省（加拿大）、荷蘭數據保護局和荷蘭的信息和隱私專員的聯合團隊在一份關於隱私增強技術(privacy-enhancing technology)的聯合報告中正式確定 1995 年應用科學研究組織(Information and Privacy Commissioner of Ontario (Canada))。隱私設計框架(privacy by design framework)於 2009 年發布，並於 2010 年由國際隱私委員會

和數據保護機構大會通過。「設計隱私」是「通過技術設計保護資料」(data protection through technology design)概念，「設計隱私」思維是指當資料處理過程中的資料保護在產品開始設計時已經嵌入到技術開發中，自此後所有流程遵守資料保護原則。GDPR 要求負責人在定義 TOM 時已經包含對處理 TOM 的方法的定義，以滿足「設計隱私」的基本要求和要求。

隱私設計要求在整個工程流程過程中都要考慮到隱私保護，從產品或服務的設計階段，一直到產品或服務的全生命週期期間，包含所有組織的所有層級，均納入資訊隱私的考量設計。這個概念是價值敏感設計的一個例子，即在整個過程中以明確定義的方式考慮人類價值觀。以 GDPR 第 25 條設計和默認的數據保護(Art. 25 GDPR- Data protection by design and by default)中有 3 點如下

- 1.) 考慮到最先進的技術、實施成本和處理的性質、範圍、背景和目的，以及處理對自然人權利和自由造成的不同可能性和嚴重程度的風險，控制者應：在確定處理方式時和處理本身時，實施適當的技術和組織措施，例如假名化，旨在以有效的方式實施資料保護原則，例如資料最小化方式並將必要的保障措施整合到處理中，以滿足本法規的要求並保護當事人的權利。(Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.)
- 2.) 控制者應實施適當的技術和組織措施，以確保默認情況下僅處理每個

特定處理目的所必需的個人資料。該義務適用於蒐集的個人資料量、處理範圍、存儲期限和可訪問性。特別是，此類措施應確保在沒有個人干預的情況下，默認情況下不會將個人數據提供給無限數量的自然人。(The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. 2That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. 3In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.)

3.)根據 GDPR 第 42 條批准的認證機制可用作證明符合同法第 25 條第 1 款和第 2 款規定的要求的要素。(An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.)

Ann Cavoukian 曾對隱私設計(Privacy by Design) 提出了七大基本原則，包含 1. 主動;2. 預設;3. 嵌入設計;4. 正和為目標;5. 全生命週期的保護;6. 可見度與透明度及 7. 尊重，原則說明展開如下：

- (1) 主動而非被動反應；預防而非補救 (Proactive, not Reactive; Preventative, not Remedial)；
- (2) 隱私為預設機制(Privacy as the Default)；
- (3) 將隱私機制嵌入設計(Privacy Embedded into Design)；
- (4) 以完整實用的正和為目標，而非零和概念 (Full Functionality–Positive-Sum, not Zero-Sum)；
- (5) 由始至終之全生命週期的保護(End-to-End Lifecycle Protection)；

(6) 可見度與透明度(Visibility and Transparency)；

(7) 尊重使用者隱私(Respect for User Privacy)



七大基本原則導入到智慧自駕車的個資保護過程是相當的重要，理由在於 1. 自駕車技術發展還是百花齊放，就技術而言難有標準化的資料管理；2. 各國個資保護法也在修正調整中，難有普世一同的保護法規；3. 各國除個資保護法外，因為資料經濟的重要性日增，故還有其他的資料管理法規陸續公布；4. 除了隱私保護，各國更將資料提升到國家安全等級，複雜性已超出本文範疇，惟相關企業卻是無法避免；5. 新技術導入與資料利用，各企業內部最為瞭解，隱私設計之導入才能全週期嵌入設計。綜上，將隱私設計的理念導入自駕車設計、生產到運營之個資管理，以主動、預防、全週期的設計理念，才能真正達到自駕車法令遵循的目標。

第陸章 結論與未來展望



綜合本文前面章節之所述，智慧自駕車牽涉到人工智慧技術-自駕車發展-個資與隱私保護三大議題。由於自駕車安全至上，各國對於先進科技的導入皆保持中性態度，然而本文就人工智慧/機械學習在短短 10 年內興起與導入自駕車之必要論述，自此以人工智慧為大腦的智慧自駕車勢必影響著可見的未來自駕車發展；同時，隨著以資料為驅動的人工智慧/機械學習之發展，對於隱私侵害可能已見於聯合國之報告。人工智慧/機械學習結合自駕車巨量資料且聯網的特性，其資料運用與個資保護之議題油然而生。綜合本文之探討，自駕車資料法規研究的重要性結論為：

- 1.自駕車深入生活，影響深遠：市場預估到 2025 年自駕車在汽車市場的滲透率會到 13%，且逐年快速上升。滿街充斥移動且隨時蒐集、處理或運用巨量資料的自駕車對國家、社會與人民影響探討不得不慎。
- 2.巨量資料：粗估一台 SAE level 3 的自駕車資料量是目前一台監視器的 400 倍；SAE level 5 的單台自駕車資料，粗估可能逾目前單台監視器資料 1,200 倍以上。更加以聯網車輛間資料之結合，所形成的資料量之大更是難以估量。
- 3.隱密不易被察覺，當事人缺乏控制權與資訊不對稱：過去許多大廠運用大數據時外界或消費者不易得知，先前案例是在廣告推播及精準行銷時，消費者才被驚覺自己個資被蒐集，也因此智慧智駕車蒐集如此巨量之資料且可長期儲存的情況下，資料管理是否需要公權力介入，是一個值得討論的議題。
- 4.事關安全，管理須謹慎：自駕車資料蒐集牽涉到道路使用者、駕駛及乘客之安全問題，管理上必須權衡個人資料保護及安全性。
- 5.人工智慧技術採用之必要：自駕車資料因為路況多變，演算法必須採用人工智慧技術，特別是以資料驅動的機械學習技術；而人工智慧技術目前也是在快速演變，故增加規範上的困難。
- 6.法律上之「蒐集」、「處理」到「利用」行為難切割：自駕車因為資料多元及須要即時反應，必須有快速資料融合及決策，就法律觀點，資料的蒐集、處理到利用難以在短時間分離執行。
- 7.資料須更新，監管困難：人工智慧模型與資料都需要持續更新，增加管理維護成本，恐造成政府管理及監督困難。
- 8.資料與模型在地化：人工智慧模型訓練模式成功與否，與實地測試結果有相當大關係，也因此需要在地資料蒐集及持續不斷的模型調整。
- 9.對內沒對外：自駕車對駕駛人或者乘客的隱私業據規範，

但目前比較少對車外的資料或個資有所探討。10.自駕車目前以企業為主導，惟個資涉及人格權，自駕車技術與運營大都為私人企業所有，若為追求商業利益而運用個人資料者，將與個人權益有所衝突。11.國際業據自駕車個資之規範，我國發展自駕車同時，相關法制亦應與時俱進，才能行穩致遠。以下是本文之結論及未來展望。

第一節 自駕車趨勢不可擋，回首電腦網路發展時刻

第一項 自駕車的發展不但是現在進行式，亦是共識的未來趨勢

智慧自駕車是現在進行中的不可逆科技發展與經濟活動趨勢，自駕車發展已經顛覆過往的交通運輸型態，能廣泛應用並解決各種社會問題，因此具有極大社會公益及商業價值。自駕車應用與開發對各國的交通與經濟有雙重的好處，包含了龐大的自駕車經濟，和國家交通安全的提昇、都市規劃空間利用效率的提高、降低交通時間、增加生產力，及改善老人、未成年人與身障者的移動能力等諸多優點，被多個先進國家列為國家策略性的政策方針。由於自駕車技術的高度複雜性，且直接與民眾生命安全相關，自駕車的修法與執法必須參照國際間自駕車的技術發展進程與時俱進。法律是為人類社會服務的，任何法律都必須根植於特定的應用領域才能發揮其最大效用³²²，而本文所談的劃時代人工智慧自駕車資料處理與個資保障之議題，值此自駕車商業化起飛的關鍵時刻，值得重視與深入探討研究。

面對以人工智慧為代表的快速變化的現代科學技術，許多因之而起的新社會衝擊與法律課題隨之而起，如何調和生命安全與經濟發展、人性與新科技，充分利用法律的引導、規範和促進功能，促進法律與技術兩者間的良性互動³²³，相信需要無論科技、經濟、法律不同領域更多的學者專家共同參與。而自駕車被視為移動的超級電腦，集先進技術於一身，且與生命法益直接相關，自然是應受重視的人工智

³²² 趙萬一 (2019/05/12)，《人工智慧應用越來越廣 法律面對人工智慧應該做什麼？》，光明日報，載於：<http://news.cnhubei.com/caijing/p/10706704.html> (最後瀏覽日：2021/12/11)

³²³ John Frank Weaver (著)，鄭志峰(譯) (2018)，前揭註6。

慧技術運用焦點場景之一。人工智慧與自駕車兩者之結合，帶來的正面效應與可能引發侵害隱私的副作用，實非當年《個資法》立法時空可想像。



第二項 回首電腦資料處理保護法，移動電腦的個資法規再次審視

如第二章所述，現今《個人資料保護法》原為民國 84 年制定之《電腦處理個人資料保護法》，該法並於民國 99 年 4 月 27 日全文修正並更名為《個人資料保護法》，後於民國 104 年 12 月修正為現行版本。在「電腦處理個人資料保護法」草案所述：「“電腦”科技進度迅速，使用“電腦”能大量、快速處理各類資料，運用日趨普及，因而對國民經濟之提昇有重大貢獻。由於個人資料舉凡出生、健康、病歷、學業、工作、財產、信用、消費等，經“電腦”處理之後，可輕易彙整而得知其全貌，如有濫用或不當利用之情事，將對人民隱等權益造成重大危害，因而影響社會安定及國民經濟成長，並使政府推展自動化工作增加困擾。」104 年修法理由：“電腦處理個人資料保護法自 84 年 8 月 11 日公布施行至今，已近 18 年，由於資訊通信科技發達的結果，透過電腦及網際網路處理與傳輸個人資料之情形已今非昔比，該法的規範顯然已不足夠，且個人資料外洩事件時有所聞……。”將上述兩段論述中之「電腦」兩字更改為「自駕車」亦若是。現今自駕車聯網能力、儲存空間、運算速度加上人工智慧技術突破與應用，車輛與新興科技兩者相加帶來更多過去立法者並無法思考到的使用情境。

自駕車提高交通安全，解決諸多社會問題，並已經逐步落實於全球各角落。隨自駕車的滲透率逐年快速提升，自駕車所蒐用之資料具以下特色：1.大都是人們活動所產生之資料，資料容易轉化成可識別特定人的個人資料；2.資料量遠大於一般攝影機百倍以上；3.感測器種類日益多元且資料量增，加以功能提升可透過網路更新；4.承前所述，容易蒐集遠大於實際所需之資料量；4.自駕車所蒐集的資料透過現今物聯網、邊緣運算及大數據等技術之「輕易」結合；5.聯網時相關之個人資料可基於多種目的進行處理且持續追蹤；6.資料蒐用時若非有特別告知，當事人不意察覺，且易有未經同意之目的外利用；7.車商若未提供控制其個資設定之功能，當事人無法有效保護其權利；8.自駕車因為運作時牽涉到道路利用者、自駕車駕駛及乘

客之安全上的公共利益問題，包含「蒐集」、「處理」到「利用」行為之資料管理上在社會利益以及私人權益保障的權衡更形重要；9.蒐用到巨量車外公示之資料，可透過結合或持續追蹤獲取商業利益，亦可能同時侵害隱私。綜上，自駕車資料管理不慎可能會對當事人的個資造成的危機；反之，若管理過嚴或不當，亦可能造成生命安全上的疑慮。自駕車之個人資料保護因為直接牽涉到隱私權與生命法益之權衡，對於個人保護與資料運用間的平衡更難拿捏。自駕車資料蒐用以安全的公共利益為首要責任，貿然以既有個資法來管理亦有風險。

回顧整個隱私、個資保護法與重要科技發展歷史，從 1890 年照相機的普遍，狗仔隊的橫行，首先由論者提出隱私權的概念。經過了 100 年後，個人電腦、網路、大數據、物聯網、人工智慧/機械學習/深度學習，到集所有頂尖科技於一身的自駕車，相關的資料轉成個資，再透過個資轉換成對人類社會生活的管理與支配。透過如下圖 58 所示，近 10 年科技不斷創新突破，並急遽改變世界生活型態，不難理解人類對於隱私被侵犯的隱憂，而如此隱憂背後所反應出來的是人們擔心的是當諸多個資被掌握、隱私被侵犯所導致的監控世界。

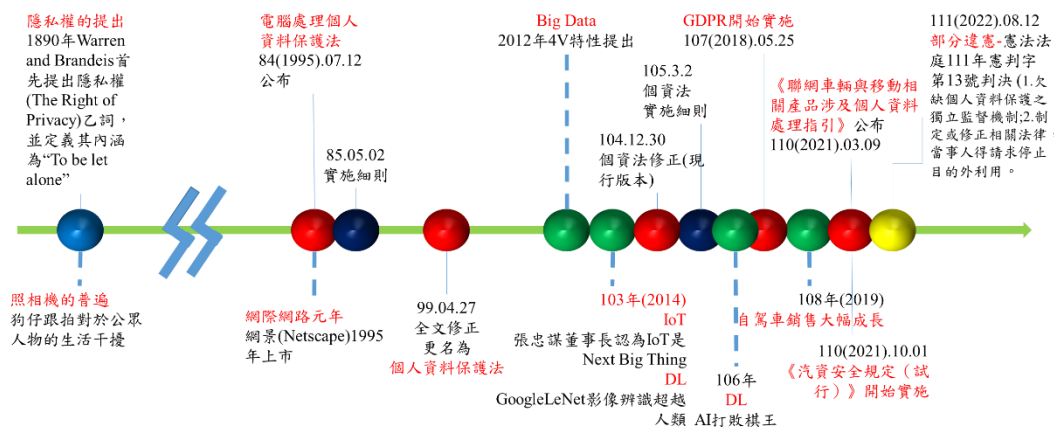


圖 58. 隱私、個資保護與重要科技發展歷史回顧。資料來源：本文整理

第三項 生命法益的保護

以過去電腦或網際網路處理個人資料角度觀之，著重在於隱私保護與資料運用間平衡，並無須立即生命安全之考量；而人工智慧所驅動之自駕車的技術研發與

法規規範，以安全為首要目標，資料運用除了促進產業發展，亦帶來人類社會福祉。人工智慧自駕車的個資管理相較過去更為複雜。

GDPR 將個資與隱私視為如同生命權的基本人權，相對的在台灣，《個人資料保護法》並非將個資視為絕對權利，惟如何拿捏權衡，考量上需要更深且全面性。在個資上保護的分析，特別自駕車在高速發展的技術與多元運用下，如何依個案之狀況調控需要更多的研究。例如：在 GDPR 第一章除規定資料保護雖為基本權利 (“Data Protection as a Fundamental Right”)，亦與其他基本權利要有平衡考量 (“Data Protection in Balance with Other Fundamental Rights”)³²⁴。自駕車安全上考量是國際公認的首要任務，安全與個資保護應當是要平衡考量。

因為人工智慧科技的導入運用，一方面使得自駕夢想得以實踐，另一方面隨著以資料驅動的人工智慧/機械學習的應用，使得近年來對於人工智慧/機械學習倫理之重視與決策過程黑盒子之疑慮也隨之轉到智慧自駕車場景。是故，相關企業在更應著重倫理道德與安全性，並透明化過程，以取得社會大眾的信賴。

然而從歐洲對聯網車輛及中國大陸對聯網車與自駕車的管理條文，目前比較傾向以資料保護為先，雖然法規中有說明在「保證行車安全需要」下之例外行為，但對其內涵並無更進一步說明。在如此管控資料的優先考量下，且法規上並沒有清楚考量到人工智慧技術導入的衝擊，是否因此提高自駕車安全的風險？

就美國國家運輸安全委員會 (NTSB) 公布於 2018 年 3 月 18 日晚上 Uber 自駕車撞死人的調查報告指出當日 Uber 自駕車在亞利桑那州坦佩市以時速 70 公里的速度行駛，49 歲的 Elaine Herzberg 則正推著單車橫越馬路，她離最近的人行穿越道約 109 公尺。事故發生前 5.6 秒，自動駕駛系統首次「看」到 Herzberg。然而，Uber 自動駕駛系統只能判斷前方有物件，無法進一步辨識該物件究竟是什麼³²⁵。以此案例，即使就目前技術發展，尚無法確認每種不同狀況，保障每個生命之前，

³²⁴ Art. 1 GDPR. <https://gdpr-info.eu/art-1-gdpr/>.

³²⁵ 張嘉玲 (2019/11/13)，《【2019.11 自駕車動態】從 Uber 自駕車死亡事故調查報告看自駕車技術缺口》，FINDIT 研究。

對於個資與資料管制不應該凌駕生命安全之上。或至少在蒐集、處理及利用每個階段須要更細化處理。

綜上，相較過往案例平衡個資保護與資料運用之間，人工智慧自駕車發展下資料運用與個人資料保護的研究如圖 59 所示，是在「個資保障」-「個資合理利用」-「生命法益」三者間做一平衡。在自駕車的生命保障上，就在短短的零點幾秒間就可能決定數人的生命安全;若為系統性的問題，如因資料不足或品質不佳導致人工智慧模型有誤(或偏見)，影響範圍可能數十倍甚至百倍於此，故資料之管理不可不慎。

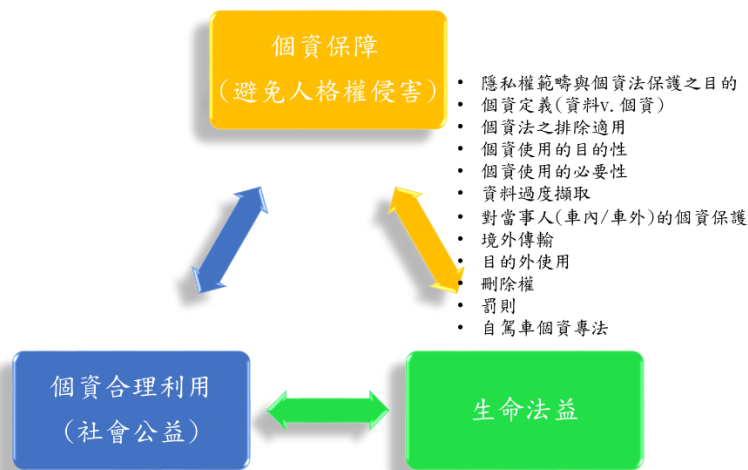



圖 59. 人工智慧自駕車個資討論，在個資保障-個資合理利用-生命法益三者間所衍生的議題。資料來源：本文整理

第四項 過分強調資料管控，可能阻礙科技發展

《個資法》立法當初是以當時的技術觀點做出規範，然而自駕車的夢想實踐，卻是許多如人工智慧、物聯網、大數據、邊緣運算等技術的共同推動下得以完成。自駕車的推動，除了商業上誘因外，具有保障生命法益、節能環保及促進社會進步的公益價值。而這些價值比起 Google 街景圖、街口監視器、或 App 的 GPS 軌跡等案例在個資保護與資料利用間權衡，智慧自駕車之資料利用有更強且更深遠的公益意義。過分強調資料管控，可能阻礙科技發展，理由如下：

- 
- 創新本在於跳脫原來思維框架，一個新技術的開發從廠商角度固然是為了自身商業利益，但自駕車創新除了保障生命，也對節能、環保、老化、人口交通安全等社會公益提供不少助益。以不確定的隱私權之法律概念作為基本權利來約束管制資料的利用，等同是設立框架下的限制創新，約束創新技術的進展，同時也限制的問題被解決的可能，影響安全並可能讓自駕車社會公益價值下降。
 - 無論人工智慧/機械學習或者大數據，許多結果與目的未必在開始能夠清楚瞭解其因果關係，先以個資保護法規來約束資料之蒐用，會提高企業開發新技術的疑慮及違法的不確定性。
 - 隱私權為不確定的法律概念，增加企業技術開發全週期的不確定性。
 - 人工智慧/機械學習及大數據運用，使得間接可識別之個資界定尚有疑慮，增加運用上風險。


若以資料或個資保護列為優先考量，然而忽略以科技創新的自駕車，本來就是跳脫突破現有既定框架與方式，兩者間難免與有所忤逆。也許也是基於與本文相同觀點，各國在自駕車的政策上，基本上還是對於先進技術導入的中性態度，然而在制定細部法規時候，對於平衡技術發展-生命安全-產業經濟-資料利用-個資保護等多面向，尚須更多探討。

第二節 自駕車的議題錯綜複雜，資料管理需要更重視

智慧自駕車因為專業技術門檻高，影響層面廣泛且複雜，所以雖相關研討與論文眾多，然而要能深入探討每個議題，尚需更多有志者投入，以便在各個層面能面面俱到。

自駕車資料法規研究的複雜與重要性更細部說明如下：

- 自駕車深入生活，影響深遠：市場預估到 2025 年自駕車在汽車市場



的滲透率會到 13%，且逐年快速上升。滿街充斥移動且隨時蒐集、處理或運用巨量資料的自駕車對國家、社會與人民影響探討不得不慎。而自駕車的資料與車內外之人們活動資訊緊密連結，相關的資料容易透過人工智慧及大數據等新興技術進行個人檔案剖析，可能對當事人的隱私造成侵害。

- 巨量資料：粗估一台 SAE level 3 的自駕車數據是目前一台監視器的 400 倍；而 SAE level 5 的單台自駕車數據，粗估可能逾目前單台監視器數據 1,200 倍以上。若再以車聯網將自駕車間結合，並成為智慧城市之一環，資料量更是難以估量。
- 集先進技術於一身，資料蒐用隱密不易被察覺：過去許多大廠運用大數據時外界或消費者不易得知，先前案例是在廣告推播及精準行銷時，消費者才被驚覺自己個資被蒐集；公開場合之智能攝錄影機，其個資的蒐用也是直到此次新冠防疫，大眾才驚覺政府可輕易透過這些資料尋找並追蹤特定當事人。同理，本人所探討的巨量自駕車資料管理是一個值得討論的議題；個資當事人與資料控制者間的資訊不對稱是一個侵害隱私的重要風險。
- 事關安全，管理須謹慎：自駕車資料蒐集牽涉到道路使用者、駕駛及乘客之安全問題，特別是在短促零點幾秒內完成資料蒐集、運算處理到決策利用，管理上必須權衡個人資料保護及安全性。是故自駕車資料與個資之管理與法規制定，相較其他應用領域，更有其困難及複雜性。
- 人工智慧技術採用之必要：自駕車運用環境多變，本文特別分章闡述演算法必須採用人工智慧技術，特別是機械學習/深度學習。該技術已經被證明在圖型辨識及棋藝競賽等領域優於人類，近年來更大幅度廣泛應用於各領域。而人工智慧技術目前也是在快速演變，相關人工智慧與法律之間的探討也是如雨後春筍，如人工智慧的可歸

責性、演算法之透明度等，故自駕車採用人工智慧亦同時增加規範上的困難，也讓社會普遍對該技術應用有所疑慮。

- 法律上之「蒐集」、「處理」到「利用」行為難切割：自駕車因為資料多元及需要即時反應，必須有快速資料融合及決策，就法律觀點，資料的蒐集(collection)、處理(processing)到利用(use)難以分離，特別是針對須快速反應且事關安全的影像，若蒐用之影像被視為個資，則依現行台灣個資法將有所窒礙難行。《汽資安全規定（試行）》已將規範用路人的影像蒐集及攝影機之解析度等；該規定對於個資之處理亦有清楚規範。
- 資料須更新，監管困難：人工智慧模型(AI model)需要持續更新，資料也需要持續更新，也因此資料多元、巨大且須更新，再者處理之技術大都為各家廠商之營業秘密，是故增加由公部門管理或協力廠商監督之困難。
- 資料與模型在地化：人工智慧訓練模式成功與否，與交通環境與實際測試結果有相當大關係，也因此需要在地的資料蒐集及持續不斷的模型調整。
- 對內沒對外：自駕車對駕駛人或者乘客的隱私有所規範，但目前比較少對車外的資料或個資有所探討，而本文已經提到國際間包含歐盟及中國都已經將車外路人之影像明文例示為個資。
- 自駕車目前以企業為主導，個資運用可能與社會公益有所衝突：自駕車技術與運營大都為私人企業所有，在巨大的資料經濟誘因下，資料控制者為求商業利益，可能與社會公益有所衝突。除本文前述的生命法益外，在其他社會利益與資料利用間平衡需更多探討。
- 自駕車資料平台的加強管理：自駕車營運業者如同網際網路平台業者，個資數量巨大、蒐用對外不特定用路人之資料眾多、業務類型

複雜，內部資料管理外界不易瞭解。未來可能有加重自駕車營運業者或其他資料控制者的個資保護責任，要求提高業務服務的透明度，完善資料平台治理，並強化外部監督等。

- 國際業據自駕車個資之規範：包含 GDPR 之《聯網車輛與移動相關產品涉及個人資料處理指南》及中國《汽資安全規定（試行）》，都已經查覺到車輛所蒐用之個資特殊性，故有專法之規範，並已產生對我國業者影響。

第三節 國際已看到自駕車個資議題，值得台灣借鏡

各國個資法規因不同國家地區差異有其屬地性，然而技術的發展乃無遠弗屆且日新月異，此外各國對於自駕車的資料保護已經從自駕車的開發商延伸到整個產業的環節，以中國為例已經涵蓋汽車設計、生產、銷售、使用、營運等過程中的涉及個人資訊資料和重要資料，使得國際的法規制定值得我國公務機關及非公務機關關注。

放眼國際，自駕車的個資問題，本文中已指出 2021 年包括歐盟 GDPR 的《聯網車輛與移動相關產品涉及個人資料處理指南》及同年 10 月中國的大陸的《汽資安全規定（試行）》已提及針對車輛的個人資料保護。前者對雖名為聯網車，但已經理解到智慧自駕車所造成的隱私侵害新衝擊，且兩者皆看到了自駕車的巨量資料及聯網功能所造成對個資及隱私的可能影響，除了在自駕車運用下更清楚的定義一般個資與敏感性個資、資料車內處理原則，對於車內及車外的個資也都涵蓋於其中。然而兩者都還是以個人資料保護優先的觀點，似乎忽略到自駕車的基本且首要任務為「安全」。在生命法益的考量下，資料與個資的運用理應優先以安全為考量，這裡「安全」的主體包含駕駛、乘客、用路人及其他可能因車子操控不當而造成生命侵害之主體。在「安全」優先的條件下，如今的人工智慧/機械學習、大數據、車聯網技術在個資運用過程中，是否能完整遵循個資法規的精神？兩者間是否已完整兼顧？除此，自駕車除了生命法益外，亦能滿足節能、環保的功能，在



人口老化時代也有不可替代的價值。在如此高且豐富的社會公益價值下，是否以不確定的法律概念或因技術與時代變化的個資定義而限制自駕車發展？長遠來看，是否符合比例原則？

台灣並沒有針對自駕車的個資法有特別的規定，然國際間已看到自駕車個資問題的獨特性與重要性，或許國際的法規趨勢值得我國參酌。本文從**基本學理探討自駕車-人工智慧-個資保護三者間關係**，可推論出歐盟及中國的立法背景與理由，提供我國在此議題上立法或修法上參考，以**避免東施效顰，人云亦云**。智慧自駕車的個資與隱私問題，殊值國內學理及實務上持續投入研究。

第四節 本文之建議

現代人每天生活的每個片段：購物、飲食、逛街、乘車、上班、求學等生活點滴時刻都被新科技所掌握。新科技帶來的便利也同時引發新時代個資隱私的隱憂，而在自駕車所擁有的巨大資料中，大部分由人活動所產生的資料都可能轉化成影響隱私的個人資料。科技帶來的便利與負面的隱私侵害相伴相隨，然而**新科技不應該為企業忽略消費者隱私保護的藉口**，以下是本文對非公務機關及公務機關的建議。

第一項 非公務機關的建議-隱私設計為核心

一.將個資保護視為社會責任與企業資產

自駕車的到來，乘載著最先進的新科技於一身並緊緊圍繞現在人生活，是截至今日歷史上所有有利於資料經濟發展與不利於個資隱私保護的焦點中心，其兩者之平衡與法規監管亦為最艱難之工作。惟**技術發展不應該為企業逃避消費者個資保護責任的藉口**，因為自駕車業者理應是對技術之採用與資料運用最為清楚，且最有能力去調整資料與個資運用的**資料控制者**。

隨著資料經濟時代的到來，法規規範只會愈來愈多，消費者意識也只會愈來愈

愈高，企業與其被動等待，不如主動制定保護資料的管理策略。《哈佛商業評論》在《數位時代的兩難》³²⁶乙文中建議“企業應該把保護數據資料的隱私與安全，視為競爭優勢”，該文亦認為“消費者愈信賴你的公司有**能力保護個資與數位足跡，就會愈願意分享更多數據資料給你，讓你的公司比競爭對手有更多機會開發新產品與服務，提高競爭優勢**”。換句話說，不積極在保護數據資料安全與隱私保護上做投資之企業，不但將失去顧客信賴，也將面臨政府巨額罰款的風險；唯有企業將個資處理視為社會責任與企業資產，將隱私設計理念深入，平衡資料利用與個資保護，並透明化處理過程，獲得消費者及社會的信賴。

《數位時代的兩難》報告針對這爭議下個明確定論：「**沒有信賴，資料經濟的一切將是空談**」。或許這可為企業在個資隱私處理上提出一個清楚方向。

二.從兩家巨擘戰爭看個資隱私的策略運用

如同 Facebook 與 Apple 公司科技巨擘在網路及行動裝置上對個資的爭議：Facebook 與 Apple 公司兩造爭鋒相對起因於蘋果公布 App Store 的全新隱私政策，要求 App Store 開發商提供更詳細、完善的隱私使用說明，以使用戶在下載 App 前，能夠瞭解自身的隱私資訊，將會被如何使用。面對這項隱私政策的重大異動，Facebook 心急如焚，於是在 2020 年 12 月 17 日在《紐約時報》、《華爾街日報》、《金融時報》和《華盛頓郵報》上刊登大幅全版廣告如下圖 60。

³²⁶ Harvard Business Review, “Digital Dilemma: Turning Data Security and Privacy Concerns Into Opportunities”. November 10, 2017. <https://hbr.org/sponsored/2017/11/digital-dilemma-turning-data-security-and-privacy-concerns-into-opportunities>



圖 60. Facebook 刊登在多家報社的聲明。資料來源：Facebook

然而經過 Apple 在 2021 年 iOS 14.5 更新「App 追蹤透明度 (App Tracking Transparency)」功能，該功能宣稱將把隱私還給用戶，並隨即調整相關隱私策略與作法，無論消費者接受與否尚待考驗，至少在 Apple 展現其該承擔社會責任，朝向將「個資蒐集透明化」及將「個資運用決定權」交還給消費者當事人。相反的據同年 App Store 公布的官方資料，Facebook App 在使用者不瞭解或未經同意的情形下，貿然蒐集了諸多用戶資訊，包括聯絡資訊、瀏覽記錄、使用狀況資料、聯絡人、位置、購買項目、搜尋紀錄等，並會與協力廠商分享部分資料或個資。

資料經濟的威力也從此案可看見端倪，2022 年 Facebook 母公司 Meta 公告財報不佳，Facebook 執行長 Mark Zuckerberg 認為 Apple 對隱私權設定的變更，導致 Meta 公司收益大減，並將原因歸咎於蘋果前述「App 追蹤透明度」功能，讓該公

司在 2021 年的廣告收益損失約 100 億美元³²⁷。兩家巨擘的隱私權之戰，也是隱私與個資運用平衡的寫照。

從兩家不同角度看待隱私保護與資料利用的廠商，可以看出的是在資料利用與公眾利益的天平上，不同的產業、科技變因下，天平的兩側並非那麼黑白分明，孰是孰非、平衡天平兩端還需要更多探討。是故如圖 26 所示，自駕車資料與個資管理，圍繞在個資保護-資料運用及生命法益保護三者。如何平衡三者？社會與自駕車廠商還要更多的經驗需要累積，也相信會有更多爭議等待去探索。

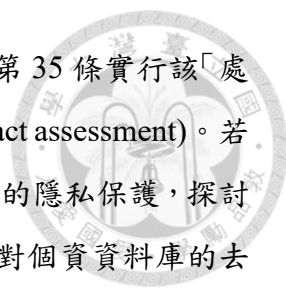
三.落實自駕車隱私設計

在歐盟《聯網車輛與移動相關產品涉及個人資料處理指南》第 2.4 點就規範資料保護設計和默認(Data protection by design and by default)，非公務部門因為有全球性的布局，個資保護必須遵守包含本國在內的全球各國規定，透過法令遵循部門落實《聯網車輛與移動相關產品涉及個人資料處理指南》隱私設計，並將隱私保護視為企業之責任與資產，爭取社會與消費者的信任。將隱私設計從源頭設計開始，一步步到製造、運營到維護都能堅持隱私保護，可包含以下之策略：

3.1 建議針對新科技的導入成立內部評估單位

新興科技不斷崛起，所謂人工智慧背後所代表的技術內涵不會侷限在機械學習或者深度學習，而是持續不斷的發展。透過新科技的溶入生活，快速的改變經濟發展型態與社會生活，使得基本的隱私的範疇也不斷地調整，本文著重在新科技對於自駕車之個資保護的衝擊，並做出整體、系統性的探討。而綜觀國際已經針對自駕車的個資保護立有專法，並詳列其中特殊的爭點做了清楚的規範。我國過去並不強調企業內部對於隱私保護的要求，然而鑑於隱私與個資保護為普世的價值，應建立內部隱私與新科技衝突評估機制。

³²⁷ The Economist (2022/02/03). *How Apple's privacy push cost Meta \$10bn*.
<https://www.economist.com/the-economist-explains/2022/02/03/how-apples-privacy-push-cost-meta-10bn>



企業在新科技導入及個資法規未明之處，可先借鏡 GDPR 第 35 條實行該「處理對於個人資料保護的影響評估」(Article 35 Data protection impact assessment)。若有其他法益上的衝突，應有內部法遵部門及評估機制。透過內部的隱私保護，探討新興科技對於隱私侵犯的可能，並適時引進隱私保護的技術，針對個資資料庫的去識別化或匿名化保護。對於新技術的導入，除了企業外部的國內外法規演變外，企業內部因為對於新技術之應用導入與資料之蒐用過程最為清楚，應有清楚的內部隱私與新科技衝突評估機制，以隱私設計的概念去做個資保護，若有安全上考量，應評估其必要性及對隱私之侵害程度，贏得內部員工及外部社會大眾的信賴。

3.2 遵守國際自駕車倫理指南

同前面所述的人工智慧倫理指南與機器人三大原則，國際間也特別重視自駕車道德倫理準則(表 11 參照)，畢竟車輛的運作與人的生活緊密相連，且若有操作不甚，便有生命危害之風險。故智慧自駕車應重視相關專屬的自駕車倫理指南。倫理指南是高於法規的自我要求，但也是非公務機關在現今重視隱私的時代，保護顧客之個資，贏得客戶與民眾信心，更有利企業發展的長遠之路。

3.3 分級管理

自駕車相關企業，包含自駕車設計、生產、銷售、使用、營運廠商等，可參酌各國資料管理辦法、個資法及自駕車資料與個資管理辦法，羅列一般個資與敏感性個資，並加入內部評估可能疑似個資之資料管理，依照不同等級資料與個資管理，以期皆能符合各國的標準要求。

3.4 分層管理，逐層管控資料

建議分層管理，對單一集團公司管制包含跨國資料傳輸(資料庫留在當地)、跨資料庫管理、聯網管理(如 Tesla「哨兵模式」和「行車記錄器」，不讓資料任意傳輸並儘量讓資料留在車內，管制非必要性跨感測器資料融合並檢視資料之敏感等級，非必要時不使用生物特徵感測等敏感個資等。

3.5 定期發布企業個人保護保護報告

由於現今技術發展快速，且自駕車資料蒐用過程專業、複雜且隱密，定期發布個人資料保護社會責任報告，接受國內外社會監督，將企業內個資管理透明化，降低顧客及大眾的疑慮。



第二項 本文對公務機關的建議

一. 自駕車資料使用關乎生命安全與公眾利益，監管須更細化


綜合因為牽涉駕駛、乘客與用路人之生命安全，加以辨識、傳輸及儲存技術的快速演進，並且由私人企業來主導且未來滲透率高等特性，自駕車個資問題，已經非過去的案例如 Google 街景圖爭議或者現今街口監視器的問題可比擬，也使得問題之解答更加複雜。對於我國公務機關，除了自身業務上的個資處理應於法有據，對於國家的自駕車個資監管亦有新的挑戰。如前所述《物聯網系統應用於可聯網車輛指南》也指出個資保護五大風險，而這五大風險與現行的各國個資處理原則有所衝突，也是本文多次提醒以現行個資法去管理智慧自駕車個資的風險所在，且自駕車資料運用必須平衡生命安全與隱私保護，複雜度非過往個資案例可比擬，影響層面涵蓋行政、立法及司法等各級公務機關。從憲法法庭 111 年憲判字第 13 號判決宣示 3 年內修正或制定《個人資料保護法》須獨立監督機制、目的外利用當事人無退出權等相關法律，本文也多次提出相關既有個資法規矛盾或窒礙難行之處，自駕車資料之管理上與健保資料庫案之判決有異曲同工之妙。根據憲法的 23 條之法律保留原則，「國家限制人民受憲法保障之基本權利，應視規範對象、內容或法益本身及其所受限制之輕重而容許合理之差異，……倘涉及公共利益之重大事項者，應有法律或法律授權之命令為依據之必要，乃屬當然。」(司法院釋字第 443 號解釋參照)，基於資訊隱私權為基本權利，立法者在自駕車個資運用上之若有特別的法律明確授權，以期遵守「性質或保障內容，需仰賴國家基及提供適當組織與程序規定，始能獲得具體實踐者，國家亦應以法律或法律明確授權之命令為之」，符合法治國家法律保留之要求。(憲判字第 13 號判決第 64 段參照)

自駕車因為資料巨大，通常涉及高風險之敏感性個資處理，且有立即生命安全之考量，加以國內並沒有如 GDPR 第 35 及 36 條進行新科技導入時個資影響評估機制，若對應本文所提自駕車個資隱私設計的概念，理應在每個環節都思考到相關個資保護及風險細節。以下是對照目前各國的規定，羅列幾點國內法規差異並可能調整之處：

1. 自駕車個資專法的可能：資料巨大且及先進技術於一身、且牽涉個生命安全，GDPR 及中國大陸都已經有自駕車個資專門法規，自駕車是台灣重要發展方向，是否建立自駕車個資專法？
2. 個資的定義更明確：本文另提出「人工智慧標準說」來判斷「資料可識別性」，以決定資料是否為個資。現今片段資料及廢棄資料都可能透過人工智慧技術，自動化進行個人檔案剖析。是故，對於自駕車「個資」應有更明確的定義。
3. 自駕車種類：自駕車可主要分為企業用途及私人用途。對於非載人為主的其他業務作業使用，如以商業用途的 L3~L5 採礦車、搬運車輛為例，排除車內人員個資法的適用。
4. 因應自駕車另訂的一般性及敏感性個資：自駕車有其容易與其他資料結合的特性，舉例如中國對於自駕車另訂定一般性及敏感性個資規定(《汽資安全規定(試行)》第三條參照)。
5. 資料分類法：承上，本文第四章探討個資法規對於個資之分類，基於該資料被洩漏或者被第三者利用時會對當時人造成重大的傷害程度而為一般性及敏感性個資規定。而基於當今人工智慧、大數據、物聯網等新技術與當事人的聯結緊密程度，本文提出「三級分類法」，主要是著重於因為新科技的導入，一旦該個人聯結資料被蒐集，往後該當事人與該資料脫離的可能性，因為一旦與當事人高度聯結之資料，例如 DNA、指紋、生物辨識等資料被蒐集及紀錄，可能終其一身中的任一時刻，這些資料

被其他資料結合，當事人都可能被辨識出來，對其隱私有終身被侵犯的可能。由此分類法，可清楚解釋現今的隱私爭議案例，如憲法法庭 111 年憲判字第 13 號判決(健保資料庫爭議)、釋字 603 號解釋(捺指紋始核發身分證規定等都可解釋。此外也可理解國際對於包含人臉辨識、生物特徵辨識技術有逐步限制的趨勢。

6. 細化資料運用：我國個資運用包含蒐集、處理、利用及國際傳輸。相對《汽資安全規定(試行)》所謂汽車資料處理，包括汽車資料的蒐集、儲存、使用、加工、傳輸、提供、公開等都有細部之規範。國際對於跨境傳輸都有相較我國嚴格的規範。
7. 蒐集、處理與利用分離：鑒於許多資料在現今新興科技下很難判斷是否為個資?應明確將蒐集、處理與利用分離處理與規範。
8. 區分「去識別化」與「匿名化」：為促進資料的合理使用及避免抑制新科技之發展，我國個資法規應清楚區分「去識別化」、「假名化」與「匿名化」，以利資料控制者的資料利用及資料經濟的發展，而非一味地過分管控或消極的放任個資濫用。
9. 分層管理：落實車內處理原則，對於車輛資料對車外傳輸應有規定。
10. 得以間接方式識別之定義：本文除了提到許多法規上已提及的「與其他資料對照、組合、連結等」爭議外，亦提及須對「持續性監控」進行規範。現今科技下，片面或廢棄資料都可能經過自動化來進行個人檔案剖析以辨識特定人，而在大部分文獻中，忽略了持續性追蹤監控，如 GPS 軌跡之長期追蹤，亦同樣透過個人檔案剖析自動化可能辨識特定人的習性，並進而造成隱私的侵害。
11. 明確規範儲存時間：承上第 10 點，為避免資料結合之風險，是否參照他國規定，規範自駕車資料儲存一段特定時間後必須刪除。

- 
12. 提高透明度：要求具一定資料量者應有年報或其他對公眾揭露制度，提高資料透明度以取得大眾信任。
 13. 疑似個資的保護：對於車外路人的個人資料是否為《個資法》所謂之個資尚有疑慮。然而鑒於國際趨勢及科技發展，例如公共空間資料依然具隱私及個資保護的可能，理應對於疑似個資有特別的規定。如《汽資安全規定（試行）》針對路上用路人的個人資料都已列為個資並有特別的處理規定。
 14. 個資與資料保護一併考量：**鑒於資料/個資的經濟價值與資料/個資界線的模糊化**，如《汽資安全規定（試行）》已將個資與資料一併考量，歐盟已將資料視為國家資產來保護。
 15. 境外傳輸的管理：我國《個資法》第 21 條對於境外傳輸採例外禁止的原則，然自駕車的資料巨大且質優(例如高精地圖)，是否採原則禁止來規範?
 16. 平衡生命安全與個資保護：如前所述，自駕車資料蒐用在瞬間攸關生命安全，是否如 GDPR 或將隱私與《汽資安全規定（試行）》將個資保護列為首要考量，再例外考量生命安全?**還是應以生命安全為優先，兼顧個資保護及產業發展?台灣若要居於自駕車產業的領先者，對於其資料與個資的管理是否有高於各國的視角，並落實於相關立法?**
 17. 針對新科技的導入成立評估單位：對於新科技不斷的演進，應以國家的角度來評估新科技的衝擊。集新科技於一身、以資料驅動的智慧自駕車，理應如 EDPB 的隱私個資評估單位及如 DPIA 的評估機制。

二.自駕車的資料管理需要更滾動式調整，法律平衡產業發展與個資保護

台灣自駕車資料目前有《無人載具實驗沙盒》及《個資法》，然而現有法規是否足以處理集先進科技於一身的智慧自駕車?且科技日新月異，未來隨著自駕車大

量商業運轉，跳脫實驗型計畫時，實際因應新科技所帶來之個資保護衝擊?能否與國際個資保護法規銜接?是否需要法遵風險評估(Compliance Risk Assessment)?

在許多企業爭相發展自駕車同時，企業與民眾勢將面臨各種潛在的風險及爭議，也因此需要展開風險監理與爭議預防的法制課題，有必要結合產官學研，做滾動式的檢討，在**高速發展的智慧自駕車商業化過程中，平衡產業發展與個資保護。**

第五節 其他展望

智慧自駕車的個資問題，牽涉到科技、法律及經濟三面向，法律或許是屬地主義，且其保護的法益可能隨不同社會文化而有所改變;然而，科技卻是無遠弗屆、日積月累、具重覆性與再現性，並不斷精進的。以下就限於本文高度相關，但卻是重要發展的趨勢議題介紹如下：

第一項 個資定義更廣泛

一.公開場合的資料

如前所述，歐盟及台灣原本認定街口監視器因具有公示性，資料從蒐集到利用並無《個資法》適用的問題，然一旦因為被認定可能侵犯隱私，被認定為個資並被個資法所包括的可能性就相當大。過去台灣的判例沒有定論，然而國際因為近年來科技的進展，逐漸開展公開場合的隱私保護，《個資法》對此類公示性高資料的保護也在可預期的方向。

二.廢棄資料

此外，透過人工智慧/機械學習、大數據等先進技術的演化，即使片面、零碎的個人活動所遺留下的廢棄資料都可能轉化成個人資料，這一進展也使得資料與個資間的界線更形模糊，這也是目前各國對於資料的跨國管制甚至高於個資的原因之一。



三.持續性監控

綜合本文探討，只要任何人為的資料，都可能轉換成個資，而個資長期的儲存與監控下，就可能對個人隱私造成傷害，資料是否已公開已非重要的考量依據，取而代之的是資料是否被結合、傳輸或持續性蒐集。在機械學習技術的發展下，也重視到資料於蒐集端運算(如邊緣運算)及限制傳輸的重要性，例如聯邦式學習(Federated Learning)或者隱私計算(Privacy Computing)等技術發展，因為該技術上在發展中且已遠超越本文探討的範疇，故不在此詳述技術內涵。

四.個資解釋過於廣泛下的平衡

如本文第二至第四章之所述，歐盟基於個資/隱私基本權利，對於所謂個資之定義是儘量擴大解釋，而我國因衡諸平衡人格權保護與資料利用，會以先限縮個資的解釋，或者排除個資法適用。如不論哪種處理原則，面對多元價值且技術快速發展的現況，都會有其不能調適之處，本文所提的人工智慧自駕車即為一個典範。除了匿名化、假名化等主流作法，對於不同的個資利用場域，都可能需要更細緻的規範。

第二項 生物特徵辨識為敏感性個資，各國有更嚴格管制趨勢

我們對自駕車個資與隱私問題無法、也不可能忽略，然而在個人隱私、公眾利益與企業私人利益間，並無法一言以蔽之如何平衡。惟有在科技、法律與社會科學各方面的專家，依照自駕車之發展與個案之經驗，逐步逐項找出可能的多方可接受的行動方案。邇來的法規趨勢與案例可看出對於生物辨識技術的管制趨於嚴格，如：1. Facebook 關閉人臉辨識及照片自動加標籤功能。美國伊利諾州的地方法官 James Donato 聯合共 160 多萬名伊利諾州用戶於 2015 年向 Facebook 提起訴訟，控訴 Facebook 未經用戶同意擅自用人臉辨識掃描照片，除了將數據儲存，還自動在照片上添加標籤，此侵犯隱私案件以 6.5 億美元(約新台幣 181 億元)為和解金額

328。伊利諾州的《生物識別數據隱私法³²⁹》允許消費者控告未經同意蒐集其臉孔和指紋等數據的公司，因此伊利諾州的地方法官詹姆斯多納托聯合伊利諾州共 160 多萬名 Facebook 用戶，控訴 Facebook 未經同意使用人臉辨識掃描照片、儲存相關數據以及自動在照片上加上標籤等。此集體訴訟和解後，至少會賠償每位用戶 345 美元（約新台幣 9,614 元）；Facebook 則透過聲明對此表示樂觀看待和解，並覺得如此規範符合社群和股東利益，並於訴訟事後修改原本的照片標記相關功能，此案和解並在 2021 年 2 月獲得法官同意。2. 美國舊金山(San Francisco)首開先例，在 2019 年通過《停止秘密監察條例》(Stop Secret Surveillance Ordinance)³³⁰的，成為全球第一個禁止使用人臉辨識技術的城市。

越來越多人權團體憂心，人臉辨識技術可能為政府濫用，導致各國政府朝「監控國家」方向邁進，濫用人臉辨識科技的最卑劣情況出現在利用人工智慧及臉部或其他辨識科技監控人民的集權政府。而如今疫情下的監控行為使得各國對於公務機關結合非公務機關濫用的生物辨識技術且不受監管的感到擔憂，且如本文所提出的第一級分類資料，這些資料對每個人可能影響是永久，如影隨形。

對於這些生物辨識技術的恐懼與管制趨勢，相關技術應用在事關安全的自駕車上，就更顯得複雜且多變。也正是本文思辨現有個資法規是否可套用在自駕車個資利用上的問題根由。

第三項 超越隱私，資料已被列為國家資產，甚至攸關國家安全

本文探討的著重在於「個資/隱私保護」、「自駕車安全」-「公共利益與技術-經濟發展」三者間的關聯，然而近期所謂「資料」的價值，已經超越個資/隱私的

³²⁸ Facebook. In re Facebook Biometric Information Privacy Litigation, Case No. 3:15-cv-03747-JD, Dkt. No. 537 (N.D. Cal. Feb. 26, 2021)

³²⁹ Illinois Biometric Information Privacy Act, BIPA.

³³⁰ EFF (2019/05/06). *Stop Secret Surveillance Ordinance*. <https://www.eff.org/document/stop-secret-surveillance-ordinance-05062019>

層面，延伸到了國家競爭力與國家安全的戰略討論，此議題已非本論文探討之範疇，
然而而是基於本論文可延伸探討的議題。


本文第二章提到個資是一種資訊隱私權亦是一種財產權，從財產之觀點，資料是 21 世紀最重要的資產。在資料經濟時代下，已有論者將資料之所有視為資本主義與共產主義之爭³³¹。資料的所有權之所屬，也將決定國家經濟的態樣：個資的所有權屬於當事人，是為自由市場經濟之根基；個資的所有權若專屬於國家，則被視為公共財產的共產思維。易言之，財產權是資本主義的根本，把資本的財產權賦予每個自然人，透過的法規之保護或者當事人有意識之自由交易，形成市場經濟；相反的，若把資本的財產權賦予國家，便可能形成共產主義。

資料經濟時代，實體國與國之競爭演變到無疆界的無實體資產的虛擬戰爭。各國已經有逐漸將「資料」或「個資」視為國家的戰略經濟物資，而非當初單以個人隱私保護角度，對於無論資料或個資的境外傳輸管制已日趨嚴格且細緻。《中國個資法》完成立法後，其所規範之個資定義、告知事項、同意要件、特定目的，或對於個資處理者之安全措施等，基本上是基于歐盟 GDPR 及各國近期的爭議個案，本質上與 GDPR 並無根本上差異，不論《中國個資法》或 GDPR 兩法都相較我國《個資法》都較為嚴格。

另一方面，因中國國家安全之考量，涉及個資在內之網路安全審查機制，及境外傳輸規範值得特別關注。且由於大陸體制之特殊，尚有鞏固統治權力之考量，遂衍生出網路安全等級保護機制；而歐盟因為看重資料經濟對產業的影響，同樣對資料管控越趨嚴格。然而，現今國際大勢已由過往國際交流走向聯盟對抗，國際大國資料的管制是否趨向與中國一致？後續發展值得重視。

綜上，在研究個資保護法規議題，以中國為例，除掌握《中國個資法》內涉及個資蒐集、處理或利用等規範意涵外，對於中國大陸及歐盟在個人隱私保護之外，

³³¹ 數位時代 (2000.03.01)，《輕鬆解讀數位經濟》，載於：
<https://www.bnext.com.tw/article/8460/BN-ARTICLE-8460>



涵蓋整體國家安全及經濟戰略之真意，以及其為落實該戰略之配套法規：如中國含現行國安法規，包括《中國國家安全法》或《中國網絡安全法》，或是《中國數據安全法》、《個人資訊保護法》及《關鍵資訊基礎設施安全保護條例》等，都須留意。《中國個資法》、《中國數據安全法》與《中國網絡安全法》三法同為目前中國網絡安全和數據保護領域的頂層架構。這些法規制度的推動實施，意味著資料不僅將是重要的商業要素，也將是基礎性國家競爭力與國與國間對抗之資源，此些去全球化與國與國對抗之轉變也為資料經濟時代發展帶來新的機遇與挑戰。

自駕車資料與個資管理趨勢如圖 61 是在原資料利用/經濟發展-個資保護-生命法益之外，另衡諸國家安全，這也使得自駕車資料/個資之立法目的更多角化，管理上更加複雜，後續世界各國有關資料規範如何發展，殊值持續研究。

而不論前述個人資料是每個個人與資本家或者國家之資料掌控權對抗，或者國與國間競爭之根本。從隱私權的觀點，隱私是人性的一節，也是自由的開端。作為隱私權之保護的個人資料之保護，本文最後再次引述美國最高法院 Louis Brandeis 法官對「隱私」見解：“文明人最全面且最有價值的權利”、“對民主政府至關重要”、“允許並保護自主生活的必要”、“對於情緒化的和心理安寧很重要”、“是人性的一節”、是“自由的心臟”，及“自由的開端”。

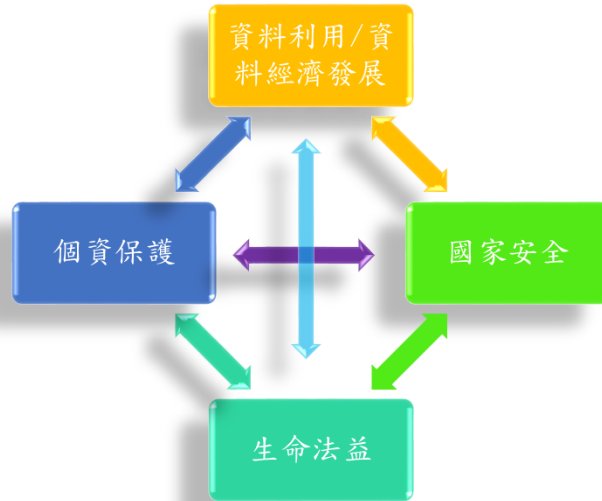



圖 61. 在現今國際局勢的演變下，資料/個資的保護與運用更形複雜。資料來源：本文整理


參考資料




期刊

1. WARREN, S. (1890). The Right To Privacy. *Harv. L. Rev*, 14(5), 193-220.
2. McCulloch, W.S., Pitts, W. (1943). A logical calculus of the ideas immanent in nervous activity. *Bulletin of Mathematical Biophysics* 5, 115–133.
<https://doi.org/10.1007/BF02478259>
3. Turing, A. M. (1950). Computing machinery and intelligence. *Mind*, LIX, 433–460.
doi:10.1093/mind/LIX.236.433.
4. William L. Prosser (1960). Privacy. *California Law Review*, Vol. 48, No. 3, 383-423.
5. Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review*, 90(4), 1087–1155. <https://doi.org/10.2307/3481326>
6. Anthony Liew (2007/06). Understanding Data, Information, Knowledge And Their Inter-Relationships. *Journal of Knowledge Management Practice*, Vol. 8, No. 2.
<http://www.tlinc.com/artic1134.htm>
7. 邱文聰 (2009),〈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》,第 168 期,頁 172-189。
8. Ohm, P. (2009/04/15). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA l. Rev.*, 57, 1701.
9. Ben Lopez (2010/12). Privacy Rights in the Age of Street View. *ACM SIGCAS, Computers and Society*, 40(4), 62-69. <https://doi.org/10.1145/1929609.1929617>
10. Bench-Capon, T. Araszkievicz, M., Ashley, K. et al. (2012). A history of AI and Law in 50 papers: 25 years of the international conference on AI and Law. *Artif Intell Law* 20, 215–319 (2012). <https://doi.org/10.1007/s10506-012-9131-x>.

- 
11. 范姜真嫩 (2013),〈個人資料保護法關於「個人資料」保護範圍之檢討〉,《東海大學法學研究》,第四十一期,頁 91-123。
 12. 郭戎晉 (2013/08),〈隱私法制新趨勢——從設計著手保護隱私 (Privacy by Design)〉,《科技法律透析》,25 卷 8 期,頁 38-44。
 13. 黃耀賞 (2015/01),〈淺談「得以間接方式識別特定個人之資料」〉,《科技法律透析》,27 卷 1 期,頁 31-35。
 14. Neil M. Richards and Jonathan H. King (2013). Three paradoxes of big data. *Stan. L. Rev. Online*, 66, 41.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2325537
 15. Balkin, Jack M. (May 10, 2015). The Path of Robotics Law. *California Law Review*, Forthcoming, Yale Law School, Public Law Research Paper No. 536, Available at SSRN: <https://ssrn.com/abstract=2586570>
 16. Gianclaudio Malgieri (2016). Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data. *Privacy in Germany - PinG*, n. 4, 2016, 133 ff. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2916058
 17. 潘俊良 (2017),〈歐盟和德國對於自動駕駛及智慧交通系統之個人資料保護發展〉,《科技法律透析》,第 29 卷第 9 期,頁 52-69。
 18. 潘俊良 (2017),〈德國自動駕駛倫理委員公布自動駕駛系統規劃指引〉,《科技法律透析》,第 29 卷第 08 期。
 19. 潘俊良 (2017),〈簡析德國自動駕駛與車聯網發展策略〉,《科技法律透析》,第 29 卷第 4 期。
 20. Silver, D., Schrittwieser, J., Simonyan, K. et al (2017/10/19). Mastering the game of Go without human knowledge. *Nature* 550, 354–359.
<https://doi.org/10.1038/nature24270>

- 
21. 吳全峰、許慧瑩 (2018/01),〈健保資料目的外利用之法律爭議——從去識別化作業工具談起〉,《月旦法學雜誌》,第 272 期,頁 45-62。
 22. 邱文聰 (2018/01),〈被淘空的法律保留與變質的資訊隱私憲法保障——評最高行政法院一〇六年度判字第五四號判決與相關個資法條文〉,《月旦法學雜誌》,第 272 期,頁 32-44。
 23. 黃章令 (2018/12),〈重塑大數據時代下的隱私權法理-以隱私權概念為主要內容〉,《月旦民商法雜誌》,第 62 期,頁 131-162。
 24. 謝碩駿 (2018/06),〈Google Street View 法律問題初探:公物法與個資法之視角〉,《臺大法學論叢》,第 47 卷第 2 期。
 25. 林鈺雄、翁逸泓、陳信安、謝銘洋、劉靜怡、陳柏良、黃居正、張陳弘 (2019/03),〈新時代個資法的挑戰(上)〉,《月旦法學雜誌》,第 286 期,頁 51-73。
 26. 林鈺雄、翁逸泓、陳信安、謝銘洋、劉靜怡、陳柏良、黃居正、張陳弘 (2019/04),〈新時代個資法的挑戰(下)〉,《月旦法學雜誌》,第 286 期,頁 210-227。
 27. 李沛宸 (2019/03),〈實施歐盟個人資料保護規章對人工智慧發展之影響〉,《財金法學研究》,第 2:1 期,頁 125-156。
 28. 甘琳 (2019/03),〈Google 違反 GDPR 遭法國國家資訊自由委員會裁罰〉,《科技法律透析》,第 31 卷第 3 期,頁 14-15。
 29. Tabitha S. Combs, Laura S. Sandt, Michael P. Clamann, Noreen C. McDonald (January 2019). Automated Vehicles and Pedestrian Safety: Exploring the Promise and Limits of Pedestrian Detection. *American Journal of Preventive Medicine* 56(1):1-7. DOI: 10.1016/j.amepre.2018.06.024.
 30. 洪德欽 (2020/07/05),〈歐盟自動駕駛車之發展策略與法律規範〉,《歐美研究》,第五十卷第二期,頁 349-431。

- 
31. 劉彥伯 (2020/07/15),〈論自動駕駛車輛事故於我國之過失責任侵權-以德國道路交通法 2017 年修正為借鏡〉,《科技法律透析》,第 32 卷第 7 期,頁 38-52。
 32. 黃昱凱 (2020/12),〈Level 4 等級自駕車道德困境決策行為初探:電車困境的應用〉,《運輸學刊》,第三十二卷第四期,頁 427~462。
 33. 鄭伊廷 (2021/03),〈試析「一般資料保護規則」下自動化決策的解釋權爭議〉,《經貿法訊》,第 279 期。
 34. 蕭文生 (2021/11),〈自駕車法制之發展(上)〉,《月旦法學》, No.318, 頁 102-123。
 35. 蕭文生 (2021/12),〈自駕車法制之發展(下)〉,《月旦法學》, No.319, 頁 68-92。

研討會論文

1. John McCarthy (December, 1958). Programs with common sense. *Teddington Conference on the Mechanization of Thought Processes*.
<http://jmc.stanford.edu/articles/mcc59/mcc59.pdf>
2. Shinya Saito; Yuki Ishii; Takeki Ogitsu; Hiroshi Mizoguchi (2015). Face Detection-based System to Sense Pedestrians At High Risk of Collision. *2015 6th International Conference on Intelligent Systems, Modelling and Simulation*. DOI: 10.1109/ISMS.2015.21
3. Lie Guo, Ping-Shu Ge, Ming-Heng Zhang, Lin-Hui Li, Yi-Bing Zhao (2012). Pedestrian detection for intelligent transportation systems combining AdaBoost algorithm and support vector machine. *Expert Systems with Applications vol. 39*, pages 4274–4286.
4. European Data Protection Supervisor (Oct. 2016). Artificial Intelligence, Robotics, Privacy and Data Protection. *Room document for the 38th International Conference of Data Protection and Privacy Commissioners*.

https://edps.europa.eu/sites/default/files/publication/16-10-19_marrakesh_ai_paper_en.pdf



學位論文


1. 徐新隆 (2005),《數位時代下資訊隱私權問題之研究—以個人資料保護為中心》, 國立臺北大學法律學研究所碩士論文, 臺北。
2. 李明勳 (2013),《合理隱私期待之研究-以定位科技為例》, 國立政治大學法律研究所碩士論文, 臺北。
3. 徐一修 (2013),《被遺忘權之研究》, 世新大學/法律學研究所(含碩專班)碩士, 臺北。
4. 周妙枝 (103),《個人資料保護法中刑罰規定之探討》, 東吳大學碩士在職專班法律專業組碩士論文, 臺北。
5. 楊柏宏 (2016),《被遺忘權之研究—以歐盟個資保護規章及歐盟法院 Google Spain SL 案為中心》, 國立交通大學科技法律研究所碩士, 新竹。
6. 馬意婷 (2016),《由我國個人資料保護法探討 Google 街景攝影衍生之相關法律議題》, 東吳大學法學院法律學系碩士在職專班碩士論文, 臺北。
7. 林好捷 (2018),《探討智慧城市之興起與隱私權之調和》, 東吳大學法學院法律學系碩士在職專班碩士論文, 臺北。
8. 劉彥廷 (2019),《「被遺忘權」之研究—以台日對搜尋引擎業者之檢索結果刪除請求權為中心》, 國立政治大學法律學系碩士, 台北。
9. 廖曼庭 (2018),《自駕車資料法制之比較研究》, 國立交通大學科技法律研究所碩士論文, 新竹。
10. 潘元寧 (2019),《被遺忘權作為網路世界的隱私權-從歐盟概念發展看我法治

回應》，國立中央大學法律與政府研究所碩士論文，桃園。

11. 關華凌 (2019)，《自動駕駛／無人駕駛車輛立法研究》，國立台灣大學事業經營法務碩士在職學位學程碩士論文，臺北。
12. 莊一凡 (2019)，《人工智慧「民主化」與經濟體制變革—以限制競爭規範為出發點》，國立台灣大學事業經營法務碩士在職學位學程碩士論文，臺北。
13. 趙亮 (2019)，《自動駕駛汽車監管制度研究》，吉林大學法學院法律碩士論文，中國大陸。
14. 張文憶 (2020)，《大數據應用世代下的資訊隱私規範》，國立台灣大學事業經營法務碩士在職學位學程碩士論文，臺北。

專書

1. Lawrence Lessig (1999). *Code and Other Laws of Cyberspace*. Basic Books. ISBN 978-0-465-03913-5
2. Daniel J. Solove (May 2008). *Understanding Privacy*. Harvard University Press. ISBN: 978-0674035072.
3. Solove, D. J., & Schwartz, P. M. (2009). *Privacy, information, and technology*. Aspen Publishers.
4. Hod Lipson & Melba Kurman (著)，徐立妍 (譯) (2019)。《自駕車革命：改變人類生活、顛覆社會樣貌的科技創新》。臺北：經濟新潮社。
5. 劉靜怡，顏厥安，吳從周，李榮耕，邱文聰，沈宗倫，黃居正 (2018)，《人工智慧相關法律議題芻議》，臺北：元照出版有限公司。
6. 財團法人資訊工業策進會科技法律研究所 (2018)，《自駕車的第一本法律書》，臺北：資訊工業策進會科技法律研究所出版，書泉經銷。

- 
7. 彭誠信 (2018),《人工智慧與法律的對話》,上海:上海人民出版社。
 8. John Frank Weaver (著), 鄭志峰(譯) (2018),《機器人也是人:人工智慧時代的法律》,臺北:元照出版有限公司。
 9. 蔡甫昌,黃瀚萱等 20 人 (2018),《大數據之醫療運用與人文反省》,臺北:元照出版有限公司。
 10. 陳鈺雄、楊哲銘、李崇僖 (2019),《人工智慧與相關法律議題》,臺北:元照出版有限公司。
 11. 張陳弘,莊植寧 (2019),《新時代之個人資料保護法制:歐盟 GDPR 與臺灣個人資料保護法的比較說明》,臺北:新學林出版有限公司。
 12. 顏上詠等 (2019),《智慧財產權與法律風險析論:人工智慧商業時代的來臨》,臺北:五南出版有限公司。
 13. 班·格林 Ben Green(2020),《被科技綁架的智慧城市(The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future)》,台灣:行人出版社。
 14. 黃章令 (2020),《使用衍生數據及其預測結論之法律關係研究》,台灣:新學林出版社。
 15. 王維嘉 (2020),《AI 背後的暗知識:機器如何學習、認知與改造我們的未來世界》,台灣:大寫出版。
 16. Shoshana Zuboff(著), 溫澤元, 林怡婷, 陳思穎(譯) (2020), 監控資本主義時代(上卷:基礎與演進;下卷:機器控制力量),時報出版,出版日期:2020/07/08。
 17. Shoshana Zuboff(著), 溫澤元, 林怡婷, 陳思穎(譯) (2020), 監控資本主義時代(上卷:基礎與演進;下卷:機器控制力量),時報出版,出版日期:

2020/07/08。

18. 陳家駿 (2021), 《人工智慧 vs 智慧財產權》, 臺北: 元照。



網路資源與媒體報導

1. The Economist (2012/08/30). *Look, No hands*.
<https://www.economist.com/technology-quarterly/2012/08/30/look-no-hands>
2. 中華電信 (2013/01/25), 《新北市警局、中華電信共同打造全台最大警政雲》, 載於: <https://www.cht.com.tw/zh-tw/home/cht/messages/2013/msg-130125-143952>
3. Fei Fei Li (2015, March 23). How we teach computers to understand pictures. *TED*. <https://www.youtube.com/watch?v=40riCqvRoMs>
4. 郭芝榕 (2016/03/08), 《不是未來, 就是現在! 人工智慧走入商用領域》, 數位時代, 載於: <https://www.bnnext.com.tw/article/38812/BN-2016-03-02-142445-196>
5. Singapore LTA (2017/02/07). *Factsheet: Second Reading of Road Traffic (Amendment) Bill*.
<https://www.lta.gov.sg/content/ltagov/en/newsroom/2017/2/2/factsheet-second-reading-of-road-traffic-amendment-bill.html>
6. Singapore Statutes Online (2017/03/24). *ROAD TRAFFIC (AMENDMENT) ACT 2017*. <https://sso.agc.gov.sg/Acts-Supp/10-2017/Published/20170321?DocDate=20170321#pr6->
7. 殷家瑋 (2017/06/07), 《駕駛人對聯網自駕車隱私疑慮 傳統車商比科技巨頭更受信任》, 電子時報, 載於: https://www.digitimes.com.tw/iot/article.asp?cat=158&id=0000503031_1qelid8n4rw3060jux7eh
8. Deepmind (2017/10/18). *AlphaGo Zero: Starting from scratch*.

- <https://deepmind.com/blog/article/alphago-zero-starting-scratch>
9. 天下雜誌第 637 期，《數據經濟特輯》，2017/12/06
10. INSIDE (2018/05/31)，《智慧路燈：隱身民間的大數據基地！臺北全 16 萬路燈將變身 AIoT 基礎建設》，<https://www.inside.com.tw/article/13096-pmo-smart-street-light-project>
11. 陳明陽 (2018/11/17)，《新加坡全電動自駕巴士載客明年首度上路測試》，DigiTimes。
12. 自由時報 (2018)，《北市智慧路燈人臉辨識惹議 副市長林欽榮回應了！》，載於：<https://news.ltn.com.tw/news/politics/breakingnews/2436175>
13. 陳達誠 (2018/12/16)，《一文看懂自駕車：在路上跑的超級電腦》，鉅亨網，載於：<https://news.cnyes.com/news/id/4249673>
14. 利榮 (2018/05/15)，《德國為自動駕駛汽車制定了世界首個倫理規則》，雷鋒網，載於：
<https://www.leiphone.com/category/transportation/4dmzA13BcpgCUH6t.html>
15. 蔡朝安 合夥律師 / 張馨雲 副總經理 / 林勇麒 律師 / 俞仲宣律師 (2019)，《淺談「無人載具科技創新實驗條例」通過後可能涉及的個資議題》，資誠 (PwC Taiwan)。
16. 日經中文網 (2019/03/08)，《日本敲定自動駕駛車上路規則 解禁開車看手機》，載於：<https://zh.cn.nikkei.com/politicaeconomy/economic-policy/34638-2019-03-08-15-14-19.html>
17. 日經中文網 (2019/05/17)，《日本 2020 年或實現高速公路自動駕駛》，載於：<https://zh.cn.nikkei.com/industry/icar/35626-2019-05-17-13-11-51.html>
18. 徐志偉，楊宗賢及鄭致灝 (2019/09/16)，〈探索光達感測器 提昇環周感知






能力》，《電腦與通訊》，載於：

<https://ictjournal.itri.org.tw/content/Messagess/contents.aspx?&MmmID=654304432061644411&CatID=654313611255143006&MSID=1036010376166635147>

19. 趙萬一 (2019)，《人工智慧應用越來越廣 法律面對人工智慧應該做什麼？》，2019年05月12日，光明日報，載於：
<http://news.cnhubei.com/caijing/p/10706704.html>
20. 何心宇 (2019)，《主要國家自駕車政策發展現況》，MIC AISP 情報顧問服務，2019/4/12，載於：
<https://mic.iii.org.tw/AISP/Reports?docid=CDOC20190408001>
21. 何心宇 (2019)，《借鏡美/德/日三大國法規 自駕車政策發展促進創新》，新通訊，2019/8/13，載於：<https://www.2cm.com.tw/2cm/zh-tw/market/5B2C469E82C04FC7B22D0E252782BDD8>
22. 葉芳瑜 (2020/01/20)，《迎向自駕浪潮、掌握產業商機》，STPI 科技政策研究與資訊中心，載於：<https://www.2cm.com.tw/2cm/zh-tw/market/EFA1E560C84342B2B7099A9566220F2A?type=14>
23. 王嫻文 (2020/02/12)，《無人載具是目前的趨勢，但真的安全嗎？》，Makerpro，載於：<https://makerpro.cc/2020/02/unmanned-vehicles-are-the-current-trend-but-is-it-really-safe/>
24. NCSL (2020/02/18). *Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation*. <https://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx>
25. 黃兆儀 (2020/02/26)，《淺析自動駕駛發展現況》，立法院議題研析，撰成日期：109年2月，更新日期：109年2月26日，載於：
<https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=6590&pid=191993>

- 
26. 林信亨 (2020/03/06), 《從新冠肺炎防疫看 AI 身分識別技術商機》, MIC AISP 資料庫, 載於:
<https://mic.iii.org.tw/aisp/Reports.aspx?id=CDOC20200305003>
27. 陳曉莉 (2020/03/24), 《武漢肺炎效應: 已有 13 個國家採用數位追蹤技術》, iThome, 載於: <https://www.ithome.com.tw/news/136531>
28. 蕭有為 (2020/06/19), 《可以放雙手了! 福特「Co-Pilot360 2.0」將於 2021 年上路》, 8891 汽車, 載於: <https://c.8891.com.tw/news/10781>
29. Fabrizio Fantini (2020/06/20). Data Science is Dead. Long Live Business Science! *Towards Data Science*. <https://towardsdatascience.com/data-science-is-dead-long-live-business-science-a3059fe84e6c>
30. 何琳潔、許慧瑩、趙若漢 (2020/07/24), 《餐廳為防疫要求看身分證? 中研院學者: 遊走法律邊緣 | 台灣該用數位身分證嗎 (上)》, 未來城市。
31. 何琳潔、許慧瑩、趙若漢 (2020/07/24), 《新冠肺炎教我們的事: 一旦留下個資, 政府隨時都能用 | 台灣該推數位身分證嗎 (下)》, 載於:
https://futurecity.cw.com.tw/article/1557?utm_source=web_future&utm_medium=website&utm_campaign=web_future-website-extensivereading-inarticlecw
32. 林蕙禎 (2020/02/22), 《無所遁形! 莫斯科採人臉辨識技術偵查檢疫者》, 鉅亨網編譯, 載於: <https://news.cnyes.com/news/id/4445277>
33. 雷鋒網 (2020/03/27), 《2020 最新自動駕駛技術報告出爐! 以特斯拉、Volvo 為例, 全面涵蓋智駕技術》, 科技新報, 載於:
<https://technews.tw/2020/03/27/wevolver-2020-autonomous-vehicle-technology-report/>
34. 林宜敬 (2020/03/28), 《武漢肺炎》中國紅綠黃「健康碼」監控手機控疫情, 西方國家為何不跟進? | 瘟疫、科技與民主自由》, 未來城市, 載於:

- https://futurecity.cw.com.tw/article/1340?utm_source=web_future&utm_medium=website&utm_campaign=web_future-website-extensivereading-inarticlecw
35. 廖曼庭 (2020/08/11)，〈認識人工智慧技術下的自駕車—從道德到隱私問題〉，《AI 法律評論網》，載於：https://www.aili.com.tw/aili_detail/83.htm
36. 洪煥周 (2020/09/14)，《AI 晶片、感測器成自駕車安全關鍵》，Digitimes，載於：
http://www.digitimes.com.tw/iot/article.asp?cat=158&cat1=20&cat2=80&id=0000592824_TQ77JZAP302S9I3HBNH76
37. 國立臺灣大學法律學院 (2020)，《台大法學論叢》(新修)格式範本，載於：<http://www.law.ntu.edu.tw/law3/index.php/zh-tw/%E6%A0%BC%E5%BC%8F%E7%AF%84%E6%9C%AC.html>
38. 博利斯·巴比克 Boris Babic，葛倫·柯恩 I. Glenn Cohen，希奧多羅斯·埃弗基尼歐 Theodoros Evgeniou，莎拉·葛基 Sara Gerke(2021/01)，《力保機器學習不脫軌》，哈佛商業評論·2021年1月號(與競爭者共舞)，載於：<https://www.hbrtaiwan.com/article/20074/when-machine-learning-goes-off-the-rails>
39. 資訊工業策進會科技法律研究所 (2021/03/10)，《德國聯邦政府內閣通過自駕車草案》，載於：<https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=8637>
40. AUTOACCIDENT (2021/03/31). *Statistics on Intersection Accidents*.
<https://www.autoaccident.com/statistics-on-intersection-accidents.html>
41. 盧希鵬 (2021/03/24)，《自駕車技術的春秋戰國時代》，udn/產經/名人 TALKS，載於：<https://udn.com/news/story/121739/5339147>
42. 侯冠州 (2021/04/16)，《自駕車不僅能「算」還要能「看」，專訪 Mobileye 看其關鍵感知晶片布局》，科技新報，載於：



- <https://technews.tw/2021/04/16/av-mobileye/>
43. 邱健芯 (2021/04/18), 《告別老司機, 自駕車的導盲犬, 為什麼高精地圖這麼重要?》, 科技新報, 載於: <https://technews.tw/2021/04/18/autonomous-cars-high-definition-maps/>
 44. 林健生 (2021/05/18), 《台中 2 確診者足跡有落差 擬續比對監視器》, 公視新聞網, 載於: <https://news.pts.org.tw/article/526654>
 45. 資訊工業策進會科技法律研究所 (2021/05/25), 《簡析自動駕駛巴士應用於我國上路營運所需面臨之法制預備方向》, 載於: <https://stli.iii.org.tw/article-detail.aspx?tp=1&i=180&d=8675&no=64>
 46. University of Michigan (2021/06/01). *Mcity's Autonomous Vehicle Testing*. https://www.youtube.com/watch?v=LM5_zVC544o
 47. May (2021/06/17), 《歐盟宣布歐洲數位身分和錢包框架 預計 2022 年 9 月推出》, 科技產業資訊室 (iKnow), 載於: <https://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=17927>
 48. 邵樂峰 (2021/07/15), 《走進毫米波雷達「4D 成像」時代》, EE Times China, 載於: <https://www.eettaiwan.com/20210715nt61-mmwave-radar-4d-image/>
 49. 工業和信息化部網站 (2021/08/03), 《智慧網聯汽車道路測試與示範應用管理規範(試行)》解讀, 載於: http://big5.www.gov.cn/gate/big5/www.gov.cn/zhengce/2021-08/03/content_5629202.htm
 50. 季平 (2021/08/04), 《感測器融合技術臨門缺了哪一腳?》, CTIMES, 載於: <https://www.ctimes.com.tw/DispArt-tw.asp?O=HK58481XCV0ARASTD6>
 51. 馬飛 (2021/10/09), 《淺析德國自動駕駛法對中國自動駕駛產業的啟示》,



超凡研究院，載於：

<https://www.chofn.com/academy/61615f97bff95d001d583004/%E6%B5%85%E6%9E%90%E5%BE%B7%E5%9B%BD%E8%87%AA%E5%8A%A8%E9%A9%BE%E9%A9%B6%E6%B3%95%E5%AF%B9%E4%B8%AD%E5%9B%BD%E8%87%AA%E5%8A%A8%E9%A9%BE%E9%A9%B6%E4%BA%A7%E4%B8%9A%E7%9A%84%E5%90%AF%E7%A4%BA>

52. Jenny Cusack (2021/11/30). *How driverless cars will change our world*. BBC News. <https://www.bbc.com/future/article/20211126-how-driverless-cars-will-change-our-world?xtor=AL-73-%5Bpartner%5D-%5Btw.yahoo.com%5D-%5Blink%5D-%5Bchinese%5D-%5Bbizdev%5D-%5Bisapi%5D>
53. 中國國家標準全文公開系統，《汽車駕駛自動化分級》，標準號：GB/T 40429-2021，載於：
<https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=4754CB1B7AD798F288C52D916BFECA34>
54. TWIOTA (2021)，《GB/T40429-2021 《汽車駕駛自動化分級》 標準制定過程及相關情況》，載於：
<http://www.twiota.org/assets/202109271621061456.pdf>
55. Parliament (2021/12/09). *Road Traffic (Amendment) Bill, 2021*.
<https://www.parliament.gov.zm/sites/default/files/documents/bills/The%20Road%20Traffic%20Bill%2C%202021.pdf>
56. NTC (Feb. 2022). The regulatory framework for automated vehicles in Australia.
<https://www.ntc.gov.au/sites/default/files/assets/files/NTC%20Policy%20Paper%20-%20regulatory%20framework%20for%20automated%20vehicles%20in%20Australia.pdf>
57. NHTSA (March 10, 2022,). NHTSA Finalizes First Occupant Protection Safety Standards for Vehicles Without Driving Controls. Washington, DC.
<https://www.nhtsa.gov/press-releases/nhtsa-finalizes-first-occupant-protection->

safety-standards-vehicles-without-driving

58. 小丰子 (2022/02/10), 《小心荷包失血! 全台 AI 交通科技執法路段懶人包》, 最新科技新聞, 載於: <https://www.kocpc.com.tw/archives/426264>
59. 楊至善 (2022/03), 《英國法律委員會提出 75 項自駕車修法具體建議, 突破框架建構新體系》, 資訊工業策進會科技法律研究所, 載於: <https://stli.iii.org.tw/article-detail.aspx?no=66&tp=1&d=8798>
60. University of Michigan (2021/06/01). *Mcity's Autonomous Vehicle Testing ABCs*. https://www.youtube.com/watch?v=LM5_zVC544o
61. 蘇一峰 (2022/07/11), 《智慧座艙監控技術介紹》, ARTC, 載於: [https://www.teema.org.tw/download/doc/%E6%99%BA%E6%85%A7%E5%BA%A7%E8%89%99%E7%9B%A3%E6%8E%A7%E6%8A%80%E8%A1%93%E4%BB%8B%E7%B4%B9\[20220711\].pdf](https://www.teema.org.tw/download/doc/%E6%99%BA%E6%85%A7%E5%BA%A7%E8%89%99%E7%9B%A3%E6%8E%A7%E6%8A%80%E8%A1%93%E4%BB%8B%E7%B4%B9[20220711].pdf)
62. DfT (2022). *Trialling automated vehicle technologies in public*. <https://www.gov.uk/government/publications/trialling-automated-vehicle-technologies-in-public>
63. DfT (2022). *Self-driving vehicles listed for use in Great Britain*. <https://www.gov.uk/guidance/self-driving-vehicles-listed-for-use-in-great-britain>
64. Judicial Yuan 司法院影音 (2022/08/12), 《憲法法庭 111 年憲判字第 13 號判決【健保資料庫案】、……記者會(1110812)》, 載於: <https://www.youtube.com/watch?v=6IXoQfl8ncc>
65. 經濟部網站, 《無人載具科技創新實驗條例草案總說明》, 載於: https://www.moea.gov.tw/Mns/populace/news/wHandNews_File.ashx?file_id=62077
66. 中華民國統計料網行業分類查詢網站, 載於: <https://mobile.stat.gov.tw/StandardIndustrialClassification.aspx>

67. 雙語詞彙、學術名詞暨辭書資訊網，國家教育研究所網站，載於：
<https://terms.naer.edu.tw/detail/1299326/>
68. MIT CSAIL. <https://www.csail.mit.edu/about/mission-history>
69. NHTSA. <https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety>
70. Federal Ministry of Justice. *Road Traffic Act (Straßenverkehrsgesetz)*.
<http://www.gesetze-im-internet.de/stvg/>
71. 中國大陸國家市場監管總局網站，<https://www.samr.gov.cn/>
72. NCSL. Autonomous Vehicles State Bill Tracking Database.
<https://www.ncsl.org/research/transportation/autonomous-vehicles-legislative-database.aspx>
73. SIP-adus 英文網站，<https://en.sip-adus.go.jp/>
74. Smart City Korea. *K-City Network*.
<https://smartcity.go.kr/en/%EA%B8%80%EB%A1%9C%EB%B2%8C-%EC%8A%A4%EB%A7%88%ED%8A%B8%EB%8F%84%EC%8B%9C/k-city-network/>
75. UNECE. World Forum for Harmonization of Vehicle Regulations (WP.29).
<https://unece.org/transport/vehicle-regulations/world-forum-harmonization-vehicle-regulations-wp29>
76. NHS Digital. <https://digital.nhs.uk/>
77. Google 地圖，《街景服務》，載於：<https://www.google.com/intl/zh-TW/streetview/explore/>
78. United Nations. *Universal Declaration of Human Rights, article 17*.
<https://www.un.org/en/about-us/universal-declaration-of-human-rights>



研究報告



1. J. McCarthy, M. L. Minsky, N. Rochester, C.E. Shannon (August 31, 1955). *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*. <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>
2. 黃銘輝 (2012/12), 《個人資料保護法施行後現行臺北市法規之衝擊與因應》, 臺北市政府法務局委託研究案。
3. HM Treasury (2013/12). *Autumn Statement 2013*. UK GOV. ISBN 978-0-10-187472-4.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/263942/35062_Autumn_Statement_2013.pdf
4. DfT (2015/02). *The Pathway to Driverless Cars: Summary report and action plan*.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/401562/pathway-driverless-cars-summary.pdf
5. DfT (2015/02). *The Pathway to Driverless Cars: a detailed review of regulations for automated vehicle technologies*.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/401565/pathway-driverless-cars-main.pdf
6. NHTSA (2016/09). *Federal Automated Vehicles Policy*.
<https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf>
7. BMVI (2017/06). *ETHICS COMMISSION AUTOMATED AND CONNECTED DRIVING*. https://www.bmvi.de/SharedDocs/EN/publications/report-ethics-commission.pdf?__blob=publicationFile
8. HOUSE OF LORDS (2017). *Connected and Autonomous Vehicles: The future?*
<https://publications.parliament.uk/pa/ld201617/ldselect/ldsctech/115/115.pdf>
9. 曾更瑩合夥律師等 (2018/12), 《人工智慧之相關法規國際發展趨勢與因

應》，國家發展委員會委託研究。



10. 陳敬典 (2018), 《自動駕駛車發展與未來趨勢》, 車輛中心, 2018 車輛研測專刊。
11. 陳右怡 (2018/03/29), 《A.I.邊緣運算趨勢下, 五大終端載具成首波落地目標》, IEK。
12. 重磅數據 (2018), 《中國智慧網聯汽車測試示範區發展現狀分析研究報告》。
13. 張開國、葉祖宏、賴靜慧、洪憲忠 (2019/07), 《自動駕駛車輛道路測試規定之研議》, 交通部運輸研究所。
14. Alan Quek (2019/10). *Singapore Autonomous Vehicle Initiative (SAVI)*. ITS World Congress, 21 - 25.
15. 張書豪、葉芳瑜 (2019/07), 《新興技術之事前影響分析 - 以自駕車為例》, 財團法人國家實驗研究院科技政策研究與資訊中心。
16. 吳東凌 (2019), 《出席第 26 屆智慧型運輸系統(ITS)世界年會報告》, 交通部運輸研究所, 載於：
<https://report.nat.gov.tw/ReportFront/PageSystem/reportFileDownload/C10803042/001>
17. KPMG International (2019), 《2019 年自動駕駛汽車準備度報告 (2019 Autonomous Vehicles Readiness Index) 》, 載於：
<https://home.kpmg/tw/zh/home/insights/2019/02/2019-autonomous-vehicles-readiness-index.html>
18. UK Office for Artificial Intelligence (2019/06/10). *A guide to using artificial intelligence in the public sector*.
<https://www.gov.uk/government/publications/understanding-artificial-intelligence/a-guide-to-using-artificial-intelligence-in-the-public-sector>


- 
19. 陳郁淇，沈聰明，劉信宏 (2019/7/16)，《2019 年第 1 次 APEC 汽車對話 (AD30)會議》，經濟部國際貿易局，載於：
<https://report.nat.gov.tw/ReportFront/PageSystem/reportFileDownload/C10801600/001>
20. KPMG International (2020)，《2020 年自動駕駛汽車準備度報告 (2020 Autonomous Vehicles Readiness Index) 》，Publication date: July 2020. 載於：
<https://home.kpmg/tw/zh/home/media/press-releases/2020/07/autonomous-vehicles-readiness-index-2020.html?>
21. WEVOLVER (2020). *2020 Autonomous Vehicle Technology Report*.
<https://wevolver-project-images.s3-us-west-1.amazonaws.com/Wevolver+2020+Autonomous+Vehicle+Technology+Report.pdf>
22. Tesla (2020). *Tesla 2020 Impact Report*. https://www.tesla.com/ns_videos/2020-tesla-impact-report.pdf
23. ARTC (2020)，《全球自駕車產業發展現況與未來趨勢》，2020 車輛研測專刊。
24. IMF (2021). *Autonomous Vehicle (AV) Policy Framework, Part I: Cataloging Selected National and State Policy Efforts to Drive Safe AV Development*.
<https://innovationisrael.org.il/sites/default/files/Autonomous%20Vehicle%20Policy%20Framework-.pdf>
25. 人工智慧與經濟社會研究中心 (2020/12)，《全球自動駕駛戰略與政策觀察》，中國資訊通信研究院政策與經濟研究所。
26. 徐志偉 (2020/12/10)，《工研院聯網自駕車關鍵技術與應用場域》，IEKConsulting。
27. United Nations High Commissioner for Human Rights (15 September 2021). *The right to privacy in the digital age, Report of the United Nations High*

Commissioner for Human Rights. <https://www.ohchr.org/en/calls-for-input/2021/right-privacy-digital-age-report-2021>



28. 張艾琦 (2021/09/28), 《自駕車法規現況與測試環境發展案例》, 科技發展觀測平臺。
29. 蕭瑞聖 (2021/01), 《人工智慧在自駕車的應用 Application of Artificial Intelligence in Automous vehicles》, IEKConsulting。
30. 張國鈞、蔡玉琬 (2021), 《主要國家自駕車規範比較》, 科技發展觀測平臺, 04/23/2021
31. CBInsights (2020/12/16). *40+ Corporations Working On Autonomous Vehicles*. <https://www.cbinsights.com/research/autonomous-driverless-vehicles-corporations-list/>
32. CBInsights (2021/09/09). *Tech Market Map Report — Autonomous Driving Tech In Auto & Mobility*. <https://www.cbinsights.com/research/report/tech-market-map-report-autonomous-driving-tech-auto-mobility/>
33. ALLIANCE FOR AUTOMOTIVE INNOVATION, INC. (Established: November 12, 2014, Reviewed: May 2018, March 2022). *Consumer Privacy Protection Principles- PRIVACY PRINCIPLES FOR VEHICLE TECHNOLOGIES AND SERVICES*. https://www.autosinnovate.org/innovation/Automotive%20Privacy/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21-19.pdf
34. UK Department for Transport (April 2022/04/25). *Rules on the safe use of automated vehicles: summary of responses and government response*. <https://www.gov.uk/government/consultations/safe-use-rules-for-automated-vehicles-av/outcome/rules-on-the-safe-use-of-automated-vehicles-summary-of-responses-and-government-response>

研討會

- 
1. 黃品誠 (2018/12/06),〈台灣自駕車測試與驗證環境建構〉,發表於:《自駕車發展與台灣產業之機會與挑戰研討會》,財團法人中技社,台北,載於:
<https://www.ctci.org.tw/8838/research/9483/40327/>
 2. 交通大學×理律學堂科技與法律系列講座 (2019/12/11),《面對 AI,你真正該擔心的是甚麼?資訊、隱私與演算法決策的挑戰》,載於:
<https://www.youtube.com/watch?v=EMCIBX08TfQ>
 3. 財團法人人工智慧法律國際研究基金會 (2019/12/26-27),《2019 第二屆人工智慧與法律國際學術研討會》,台北。
 4. 台灣法學會憲法行政法委員會、台灣法學會刑事法委員會及元照出版公司 (2020/10/23),《法治國之科技偵查與科技防疫》。
 5. 財團法人人工智慧法律國際研究基金會 (2021/12/03),《【智慧交通之法律衝擊】2021 第四屆人工智慧與法律國際學術研討會 —「新時代的法律衝擊:一場 AI 與法律的國際思辨」》。
 6. 台灣智慧駕駛公司、高雄大學法學院生醫科技及人工智慧法制研究中心、台南市政府、高雄律師公會、台灣刑事法學會、財團法人人工智慧法律國際研究基金會、高雄大學法學院、高雄大學財經法律學系(2021/11/11),《「自駕車倫理規範」學術講座暨台灣自駕車產業發展倫理指引(芻議)發表會》,載於:
<https://www.youtube.com/watch?v=ejpu0yz-k0Q>
 7. 資策會科技法律研究所 (2021/12/24),《2021 年「自駕車法制研究成果發表會」》,載於:
https://www.youtube.com/watch?v=a_olplFIMIE。

專利

1. Pedestrian face detection, US patent no. 10082796B2
2. Pedestrian notification apparatus, US application no. US20140062685A1

3. Pedestrian Detection, US20070230792A1

紀錄片

1. Sandy Smolan (2014). The Human Face of Big Data.
<https://www.youtube.com/watch?v=4VeITe6EJDU>.
2. Netflix (2019), 《個資風暴：劍橋分析事件》(The Great Hack), 載於：
<https://www.netflix.com/tw/title/80117542>
3. Netflix (2020), 《智能社會：進退兩難》(The Social Dilemma), 載於：
<https://www.netflix.com/tw/title/81254224>



附錄(I)：符號³³²與標註說明



符號或標註	態樣	說明	本文使用
頓號	、	用於並列連用的詞、語之間，或標示條列次序的文字之後。	同左
冒號	:	用於總起下文，或舉例說明上文。	同左。本文以「全形」表現。
引號（引用《重訂標點符號手冊》）	「」及『』	中文先用單引號，後用雙引號。用於以下情景： 一、用於標示說話、引語、特別指稱或強調的詞語。 二、引號分單引號及雙引號，通常先用單引號，如果有需要，單引號內再用雙引號，依此類推。 三、一般引文的句尾符號標在引號之內。 四、引文用作全句結構中的一部分，其下引號之前，通常不加標點符號。	同左。本文針對法條之引用或者強調的詞語採用之
引號Ⅱ（中英文法律文章及判例慣用，《重訂標點符號手冊》並無明文例示）	“”及”	論者或文章所闡述之原始說明段落或文字。英文先用雙引號，後用單引號。	同左，但排除法條或重要詞語之引用
夾注號	甲式：() 乙式：—— —	用於行文中需要注釋或補充說明。	同左。本文採甲式
破折號	——	用於語意的轉變、聲音的延續，或在行文中為補充說明某詞語之處，而此說明後文氣需要停頓。	同左

³³² 本文符號依照教育部公布之《重訂標點符號手冊》修訂版，載於：
https://language.moe.gov.tw/001/upload/files/site_content/m0001/hau/Revised_Handbook_of_Punctuation.pdf (最後瀏覽日:2022/2/10)。

符號或標註	態樣	說明	本文使用
刪節號	……	用於節略原文、語句未完、意思未盡，或表示語句斷斷續續等。	同左
書名號	甲式：乙式：《 》〈 〉	甲式：直行標在書名左旁，橫行標在書名之下。乙式：1、《 》多用於書名，〈 〉多用於篇名。2、直行標在書名上下，橫行標在書名前後。3、每一種符號前半後半各占行中一格。前半不出現在一行之末，後半不出現在一行之首。	同左。本文採乙式，並應用於法規
中文專名號	_____	橫行標在專名之下。用於人名、族名、國名、地名、機構名等。	同左，本文延伸運用到專有名詞。本文中有用詞許多定義不清之處，在專有名詞下都以專名號標示，以利讀者閱讀。例如「個人資料」若為《個資法》所屬之「個人資料」，則以「 <u>個人資料</u> 」表達。
英文專有名詞		第一個字母通常大寫，近年來亦有第二個字大寫(如 iPhone)	
重點標示	粗體字 (Bold)	標註重點字詞或段落	同左。本文將段落重點使用粗體字標示

附錄(II)：汽車數據安全管理若干規定(試行)

第一條(立法理由) 為了規範汽車數據處理活動，保護個人、組織的合法權益，維護國家安全 and 社會公共利益，促進汽車數據合理開發利用，根據《中華人民共和國網路安全法》、《中華人民共和國數據安全法》等法律、行政法規，制定本規定。

第二條(管轄) 在中華人民共和國境內開展汽車數據處理活動及其安全監管，應當遵守相關法律、行政法規和本規定的要求。

第三條(定義) 本規定所稱汽車數據，包括汽車設計、生產、銷售、使用、運維等過程中的涉及個人信息數據和重要數據。

汽車數據處理，包括汽車數據的蒐集、儲存、使用、加工、傳輸、提供、公開等。

汽車數據處理者，是指開展汽車數據處理活動的組織，包括汽車製造商、零部件和軟體供應商、經銷商、維修機構以及出行服務企業等。

個人信息，是指以電子或者其他方式記錄的與已識別或者可識別的車主、駕駛人、乘車人、車外人員等有關的各種信息，不包括匿名化處理後的信息。

敏感個人信息，是指一旦洩露或者非法使用，可能導致車主、駕駛人、乘車人、車外人員等受到歧視或者人身、財產安全受到嚴重危害的個人信息，包括車輛行蹤軌跡、音訊、影片、影像和生物識別特徵等信息。

重要數據指一旦遭到篡改、破壞、洩露或者非法獲取、非法利用，可能危害國家安全、公共利益或者個人、組織合法權益的數據，包括：

(一) 軍事管理區、國防科工單位以及縣級以上黨政機關等重要敏感區域的地理信息、人員流量、車輛流量等數據；

(二) 車輛流量、物流等反映經濟執行情況的數據；



(三) 汽車充電網的執行數據；

(四) 包含人臉信息、車牌信息等的車外影片、影像數據；

(五) 涉及個人信息主體超過 10 萬人的個人信息；

(六) 國家網信部門和國務院發展改革、工業和信息化、公安、交通運輸等有關部門確定的其他可能危害國家安全、公共利益或者個人、組織合法權益的數據。

第四條汽車數據處理者處理汽車數據應當合法、正當、具體、明確，與汽車的設計、生產、銷售、使用、運維等直接相關。

第五條(等級保護) 利用網際網路等信息網路開展汽車數據處理活動，應當落實網路安全等級保護等制度，加強汽車數據保護，依法履行數據安全義務。

第六條(原則) 國家鼓勵汽車數據依法合理有效利用，倡導汽車數據處理者在開展汽車數據處理活動中堅持：

(一) 車內處理原則，除非確有必要不向車外提供；

(二) 預設不蒐集原則，除非駕駛人自主設定，每次駕駛時預設設定為不蒐集狀態；

(三) 精度範圍適用原則，根據所提供功能服務對數據精度的要求確定攝像頭、雷達等的覆蓋範圍、解析度；

(四) 脫敏處理原則，儘可能進行匿名化、去標識化等處理。

第七條(告知義務) 汽車數據處理者處理個人信息應當透過使用者手冊、車載顯示面板、語音、汽車使用相關應用程序等顯著方式，告知個人以下事項：

(一) 處理個人信息的種類，包括車輛行蹤軌跡、駕駛習慣、音訊、影片、影像和生物識別特徵等；



- (二) 蒐集各類個人信息的具體情境以及停止蒐集的方式和途徑；
- (三) 處理各類個人信息的目的、用途、方式；
- (四) 個人信息儲存地點、儲存期限，或者確定儲存地點、儲存期限的規則；
- (五) 查閱、複製其個人信息以及刪除車內、請求刪除已經提供給車外的個人信息的方式和途徑；
- (六) 使用者權益事務聯絡人的姓名和聯絡方式；
- (七) 法律、行政法規規定的應當告知的其他事項。

第八條(授權與脫敏) 汽車數據處理者處理個人信息應當取得個人同意或者符合法律、行政法規規定的其他情形。

因保證行車安全需要，無法徵得個人同意採集到車外個人信息且向車外提供的，應當進行匿名化處理，包括刪除含有能夠識別自然人的畫面，或者對畫面中的人臉信息等進行區域性輪廓化處理等。

第九條(採集前提) 汽車數據處理者處理敏感個人信息，應當符合以下要求或者符合法律、行政法規和強制性國家標準等其他要求：

- (一) 具有直接服務於個人的目的，包括增強行車安全、智慧駕駛、導航等；
- (二) 透過使用者手冊、車載顯示介面、語音以及汽車使用相關應用程序等顯著方式告知必要性以及對個人的影響；
- (三) 應當取得個人單獨同意，個人可以自主設定同意期限；
- (四) 在保證行車安全的前提下，以適當方式提示蒐集狀態，為個人終止蒐集提供便利；
- (五) 個人要求刪除的，汽車數據處理者應當在十個工作日內刪除。汽車數

據處理者具有增強行車安全的目的和充分的必要性，方可蒐集指紋、聲紋、人臉、心律等生物識別特徵信息。

第十條(報送風險評估) 汽車數據處理者開展重要數據處理活動，應當按照規定開展風險評估，並向省、自治區、直轄市網信部門和有關部門報送風險評估報告。

風險評估報告應當包括處理的重要數據的種類、數量、範圍、儲存地點與期限、使用方式，開展數據處理活動情況以及是否向協力廠商提供，面臨的數據安全風險及其應對措施等。

第十一條(境內儲存) 重要數據應當依法在境記憶體儲，因業務需要確需向境外提供的，應當透過國家網信部門會同國務院有關部門組織的安全評估。未列入重要數據的涉及個人信息數據的出境安全管理，適用法律、行政法規的有關規定。

中國大陸締結或者參加的國際條約、協定有不同規定的，適用該國際條約、協定，但中國大陸宣告保留的條款除外。

第十二條(出境核查) 汽車數據處理者向境外提供重要數據，不得超出出境安全評估時明確的目的、範圍、方式和數據種類、規模等。

國家網信部門會同國務院有關部門以抽查等方式核驗前款規定事項，汽車數據處理者應當予以配合，並以可讀等便利方式予以展示。

第十三條(報送年報) 汽車數據處理者開展重要數據處理活動，應當在每年十二月十五日前向省、自治區、直轄市網信部門和有關部門報送以下年度汽車數據安全管理情況：

- (一) 汽車數據安全管理負責人、使用者權益事務聯絡人的姓名和聯絡方式；
- (二) 處理汽車數據的種類、規模、目的和必要性；
- (三) 汽車數據的安全防護和管理措施，包括儲存地點、期限等；



(四) 向境內協力廠商提供汽車數據情況；

(五) 汽車數據安全事件和處置情況；

(六) 汽車數據相關的使用者投訴和處理情況；

(七) 國家網信部門會同國務院工業和信息化、公安、交通運輸等有關部門明確的其他汽車數據安全管理情況。

第十四條(出境補充報告) 向境外提供重要數據的汽車數據處理者應當在本規定第十三條要求的基礎上，補充報告以下情況：

(一) 接收者的基本情況；

(二) 出境汽車數據的種類、規模、目的和必要性；

(三) 汽車數據在境外的儲存地點、期限、範圍和方式；

(四) 涉及向境外提供汽車數據的使用者投訴和處理情況；

(五) 國家網信部門會同國務院工業和信息化、公安、交通運輸等有關部門明確的向境外提供汽車數據需要報告的其他情況。

第十五條(安全評估) 國家網信部門和國務院發展改革、工業和信息化、公安、交通運輸等有關部門依據職責，根據處理數據情況對汽車數據處理者進行數據安全評估，汽車數據處理者應當予以配合。

參與安全評估的機構和人員不得披露評估中獲悉的汽車數據處理者商業秘密、未公開信息，不得將評估中獲悉的信息用於評估以外目的。

第十六條(加強網絡平臺建設) 國家加強智慧(網聯)汽車網路平臺建設，開展智慧(網聯)汽車入網執行和安全保障服務等，協同汽車數據處理者加強智慧(網聯)汽車網路和汽車數據安全防護。

第十七條(建立投訴舉報管道) 汽車數據處理者開展汽車數據處理活動，應當建立投訴舉報管道，設定便捷的投訴舉報入口，及時處理使用者投訴舉報。

開展汽車數據處理活動造成使用者合法權益或者公共利益受到損害的，汽車數據處理者應當依法承擔相應責任。

第十八條(違法處法與追責) 汽車數據處理者違反本規定的，由省級以上網信、工業和信息化、公安、交通運輸等有關部門依照《中華人民共和國網路安全法》、《中華人民共和國數據安全法》等法律、行政法規的規定進行處罰；構成犯罪的，依法追究刑事責任。

第十九條(執行日期) 本規定自 2021 年 10 月 1 日起施行。

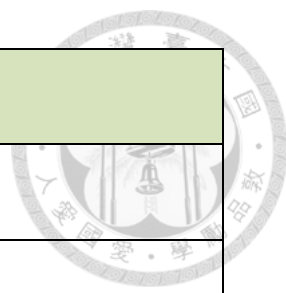
附錄(III)：雙語詞彙(依英文字母排序)

中文	英文
自動緊急煞車	Autonomous/Automated Emergency Braking, AEB
先進駕駛輔助系統	Advanced Driver Assistance Systems, ADAS
自駕車系統	Autonomous/Automated Drive System, ADS
自駕車	Autonomous Vehicle
	Automated Vehicle
	Self-driving Vehicle
匿名化	anonymization
自動化決策	automated decision-making
人工智慧	Artificial Intelligence, AI
人工智慧運算晶片	Artificial Process Unit, APU
車道維持系統	Automated Lane Keeping System, ALKS
偏見	bias
大數據	Big Data
生物特徵資料	biometric data
聯網車	Connected Vehicle
雲端運算	Cloud Computing

中文	英文
資料控制者	Data Controller
當事人/資料主體	Data Subject
資料處理者	Data Processor
資料接收者	Data Recipient
廢棄資料/衍生數據/資料廢氣	Data Exhaust
資料經濟/數據經濟	Data Economics
深度學習	Deep Learning, DL
資料融合	data fusing
數據/資料/信息	Data (information, especially facts or numbers, collected to be examined and considered and used to help decision-making, or information in an electronic form that can be stored and used by a computer)
個人資料保護影響評估	Data protection impact assessment, DPIA
個資保護長	Data Protection Officer, DPO
資料挖掘	data mining
數位足跡	digital footprint
車輛監理處	Department of Motor Vehicles, DMV
(美國)交通部	(U.S.) Department of Transportation, DOT

中文	英文
去識別化	de-identification
無人機	Drone
	unmanned aerial vehicle, UAV
駕駛者監控系統	Driver Monitoring System, DMS
邊緣運算	Edge Computing
歐盟個資保護委員會	European Data Protection Board, EDPB
歐洲資料保護監督員	European Data Protection Supervisor, EDPS
臉書	Facebook
目的外利用	further processing
一般資料保護規則/通用資料保護規則	General Data Protection Regulations, GDPR
一般安全法規	General Safety Regulation, GSR
全球定位系統	Global Positioning System, GPS
谷歌	Google
指引/指南	Guideline
高精地圖/高解析度地圖	high definition map
高度自駕車	Highly automated vehicles, HAVs
(萬)物聯網	Internet of things, IoT

中文	英文
學習式演算法	learning-based algorithm
機械學習	Machine Learning, ML
(美國)國家道路交通安全管理局	National Highway Traffic Safety Administration, NHTSA
(選擇) 退出	opt-out
空中下載技術/空中程式編碼	Over the Air Technology, OTA
防撞預警	pre-crash system, PCS
個人資料;個人信息	Personal Data
隱私	Privacy
個人檔案剖析/個人特徵描繪/側寫	Profiling
隱私設計	privacy by design
默認隱私	privacy by default
個人資料保護法	Personal Data Protection Act
假名化	pseudonymisation
隱私權	Right to privacy
規則式演算法	rule-based algorithm
敏感性資料/特種資料	sensitive information data or special categories of personal data





中文	英文
監控資本主義	Surveillance Capitalism
統計學習	Statistical Learning
張量運算處理器	Tensor Process Unit, TPU
無人載具科技創新實驗條例	Unmanned Vehicles Technology Innovative Experimentation Act

附錄(IV)：法務部函釋整理



時間	字號(法律字號)	主旨	備註
民國 94 年 10 月 27 日	法 律 字 第 0940039602 號	電腦處理個人資料保護法第 3 條規定之個人資料係指自然人之姓名、出生年月日。有關民意代表及建設公司等請求戶政機關提供某門牌地址內之戶數及設籍人數，如其並未與自然人之姓名等相結合，亦無從以此方式直接或間接識別該個人者，則該資料即非上開規定所稱之個人資料，並不發生適用電腦處理個人資料保護法之問題。	
	法 律 字 第 0999009760 號 函		(不再 適用)
民國 100 年 5 月 13 日	法 律 字 號 第 0999051927 號 函釋	參照電腦處理個人資料保護法第 3 條、個人資料保護法第 2 條等規定，倘因悠遊卡技術上仍得透過比對記名卡卡號與內部資料庫系統得知特定持卡人個人資料，非屬查詢上有困難或耗費過鉅，該卡號即屬得以間接方式識別之個人資料	
	法 律 字 第 1000014276 號 函		(不再 適用)
民國 101 年 12 月 18 日	法 律 字 第 10100100770 號	個人資料保護法第 2 條、個人資料保護法施行細則第 3 條等規定參照，如記名悠遊卡、金融卡、信用卡卡號等可間接識別持卡人身份，持卡人為自然人者，仍屬個人資料，又尚不得因可間接識別持卡人身份之卡號加密後而尚未解密前，無遭側錄盜刷風險，或機關沒有持卡人其他詳細個人資料檔案可供比對，即認非屬個資法所稱個人資料	

時間	字號(法律字號)	主旨	備註
民國 101 年 11 月 8 日	法 律 字 第 10103109010 號函	個人資料保護法第 15、16 條規定參照，刑事員警機關向高公局蒐集個人車行紀錄資料，係基於「刑事偵查」特定目的，並符合「於執行法定職務必要範圍內」要件；又高公局提供該等資料屬特定目的外利用，且係為協助偵查犯罪需要，應符合「為維護國家安全或增進公共利益」之情形	
民國 102 年 01 月 28 日	法 律 字 第 10203500150 號函員警機關所建置未具車牌辨識功能之監錄系統，其所攝錄儲存之影像電磁資料，有無個人資料保護法之適用乙案，復如說明二、三，請查照參考。.....至如前開監錄系統所錄存之影像，倘經與其他個人資料結合而成為能識別該特定個人之個人資料，進而有本法之適用，惟當事人權利之行使並非毫無限制，如有本法第 10 條各款所定情形之一（如妨害公務機關執行法定職務等）則不得答覆查詢、提供閱覽或製給複製本；又如監錄系統所攝錄儲存之影像資料係員警機關依員警職權行使本法第 10 條維護治安、調查犯罪嫌疑等目的而為，其蒐集之目的尚未消失或期限尚未屆滿，依本法第 11 條第 3 項規定，則無庸主動或依當事人之請求，刪除、停止處理或利用該個人資料。況依中央法規標準法第 16 條第 1 項前段規定：「法規對其他法規所規定之同一事項而為特別之規定者，應優先適用之。」	

時間	字號(法律字號)	主旨	備註
民國 102 年 03 月 27 日	法律字號第 10203502790 號	法務部就「網路上公布親友照片或影片」、「將第三人之電話提供予友人」、「將行車記錄器畫面放到網路上」、「大樓或宿舍公布監視錄影器錄下之侵入者影像」、「公司在榮譽榜上公布得獎員工之姓名」、「登報道歉刊登被害人姓名或其他個人資料」、「擔任保險業務員者，利用手機上通訊錄邀親友購買保險」、「村裡設置聯絡電話簿」等個人資料保護法適用疑義之說明	
民國 103 年 02 月 24 日	法律字號第 10300511510 號	政府資訊公開法第 3、18 條、個人資料保護法第 5、16 條規定參照，員警機關於具體個案申請提供員警於民間監視(錄)器取得錄影資料時，依職權審認有無應限制公開或不予提供事由；又如為「得以間接方式識別」之個人資料，員警機關如提供，應與蒐集特定目的相符，且屬執行法定職務必要範圍內，惟仍應注意利用不得逾越特定目的必要範圍，並應蒐集目的具有正當合理關聯	

時間	字號(法律字號)	主旨	備註
民國 103 年 11 月 17 日	法 律 字 第 10303513040 號	個人資料保護法第 1、2、16、20 條規定參照，如將公務機關保有的個人資料運用技術去識別化而呈現方式已無從直接或間接識別特定個人，即非屬個人資料，公務機關主動公開或被動受理人民請求提供上述政府資訊，除考量有無特別法限制外，分別依檔案法第 18 條或政府資訊公開法第 18 條相關規定決定是否公開或提供即可；又非可直接或間接識別的個人資料一律均須保密或禁止利用，公務機關及非公務機關對個人資料利用，原則上雖應於蒐集特定目的必要範圍內為之，惟如符合法律明文規定、為增進公共利益等法定事由，仍得為特定目的外利用	
民國 104 年 01 月 26 日	法 律 決 字 第 10403501110 號	個人資料保護法第 2、19、20 條規定參照，汽車公司裝設 E-tag 辨識系統與車牌號碼辨識系統蒐集、處理或利用個人資料，應確認該資料是否屬可直接或間接方式識別之個人資料，始有該法適用；又資料蒐集或處理行為是否合法，應視是否與所定契約為相同特定目的及是否為履行契約必要範圍內，如資料蒐集或處理行為與所定契約特定目的不符且無該法第 19 條第 1 項第 3、4、6、7 款情形之一，則須依第 5 款規定經當事人書面同意，始為適法	
民國 106 年 05 月 10 日	法 律 字 第 10603505040 號函 釋	個人資料保護法第 19 條第 1 項規定，所稱法律係指法律或法律具體明確授權之法規命令，又非公務機關對於個人資料蒐集、處理，應依上述規定為之，並應尊重當事人權益，依誠實及信用方法為之，不得逾越特定目的必要範圍，並應與蒐集目的具有正當合理關聯。	

索引



A

AI xvi, 1, 3, 9, 10, 13, 17, 18, 22, 23, 24, 25, 27, 30, 33, 34, 35, 36, 37, 51, 64, 81, 82, 196, 211, 216, 225, 231, 239, 244, 248, 255, 279, 308, 331, 335, 336, 345, 355

D

DL... xvi, xvii, 4, 30, 31, 77, 78, 211, 356

DPIA..... 291, 356

G

GDPR xviii, xxi, xxii, 8, 16, 17, 22, 73, 84, 102, 156, 158, 162, 163, 164, 166, 167, 168, 169, 170, 171, 172, 174, 175, 176, 177, 180, 181, 182, 185, 186, 187, 189, 198, 199, 200, 201, 202, 203, 208, 209, 223, 228, 229, 238, 242, 248, 249, 251, 252, 253, 255, 256, 261, 262, 264, 265, 266, 271, 273, 274, 275, 276, 283, 284, 285, 286, 287, 290, 291, 292, 294, 296, 297, 298, 304, 309, 314, 316, 318, 322, 327, 331, 357

M

ML....ii, xvi, xvii, 4, 5, 10, 19, 27, 30, 31, 34, 77, 78, 211, 216, 225, 358

O

OTA35, 68, 69, 191, 206, 225, 282, 293, 358

二劃

人工智慧 .i, ii, iv, xvi, xvii, xix, xx, xxi, 1, 2, 4, 5, 7, 8, 9, 10, 11, 12, 13, 16, 17, 18, 21, 22, 23, 24, 25, 26, 27, 29, 30, 32, 33, 34, 35, 36, 37, 47, 49, 50, 51, 52, 55, 58, 60, 64, 68, 74, 75, 76, 79, 80, 81, 82, 91, 101, 102, 149, 156, 157, 191, 204, 205, 206, 207, 209, 210, 211, 212, 213, 215, 216, 218, 219, 220, 222, 223, 224, 225, 229, 230, 237, 241, 243, 248, 249, 252, 254, 260, 265, 266, 269, 270, 271, 272, 273, 276, 277, 278, 279, 280, 281, 282, 283, 285, 289, 295, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 313, 314, 316, 319, 320, 321, 327, 330, 331, 332, 336, 342, 343, 344, 345, 355

三劃

大數據 ..5, 8, 13, 17, 19, 37, 72, 73, 74, 75, 76, 78, 79, 80, 81, 82, 101, 157, 161, 182, 183, 197, 206, 212, 229, 248, 249, 251, 252, 254, 260, 264, 268, 271, 272, 278, 279, 289, 295, 300, 302, 303, 305, 306, 307, 309, 316, 319, 327, 330, 331, 355

四劃

公眾利益 ... 45, 46, 101, 159, 228, 248, 270, 315, 320

五劃

去標識化 181, 186, 187, 201, 317, 350

去識別化..16, 156, 157, 161, 166, 167,
170, 171, 187, 229, 234, 235, 256, 259, 263,
272, 278, 279, 283, 284, 287, 314, 327, 355,
363

生物特徵..... xix, 21, 67, 164, 171, 192,
194, 198, 199, 219, 220, 221, 229, 232, 237,
244, 270, 291, 314, 317, 320, 355

六劃

自動化決策..4, 82, 181, 182, 183, 218,
219, 229, 237, 252, 265, 272, 273, 274, 275,
276, 288, 291, 293, 328, 355

自駕車.i, ii, iv, xvi, xvii, xviii, xix, xx, xxi,
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15,
16, 17, 18, 21, 22, 23, 24, 25, 30, 33, 34, 35,
37, 38, 39, 41, 42, 43, 44, 45, 46, 47, 48, 49,
50, 51, 52, 53, 54, 55, 56, 58, 59, 60, 61, 62,
63, 64, 65, 66, 67, 68, 69, 70, 71, 78, 79, 80,
82, 85, 89, 90, 92, 94, 96, 99, 101, 102, 103,
106, 108, 109, 113, 114, 115, 124, 125, 126,
127, 128, 129, 130, 131, 132, 133, 134, 137,
138, 139, 142, 144, 145, 147, 148, 153, 156,
157, 158, 160, 161, 164, 168, 176, 178, 180,
185, 188, 190, 191, 194, 199, 204, 205, 206,
207, 208, 209, 210, 211, 212, 213, 214, 215,
216, 219, 220, 222, 223, 224, 225, 226, 228,
229, 230, 241, 242, 243, 244, 245, 246, 247,
248, 264, 267, 268, 269, 270, 271, 273, 276,
277, 280, 281, 282, 283, 284, 285, 286, 287,
288, 289, 292, 293, 294, 295, 299, 300, 301,
302, 303, 304, 305, 306, 307, 308, 309, 310,
313, 314, 315, 316, 317, 318, 319, 320, 321,
323, 328, 329, 330, 332, 333, 336, 342, 343,
344, 345, 355

十劃

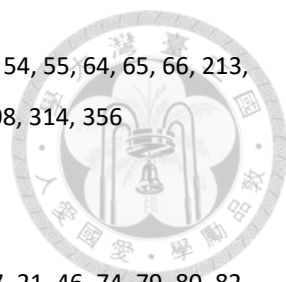
個資 ii, iv, xvi, xvii, xviii, xix, xx, xxi, xxii,
2, 5, 7, 8, 9, 10, 11, 12, 13, 15, 16, 17, 18, 20,
21, 22, 23, 24, 25, 29, 34, 35, 37, 38, 39, 46,
58, 63, 66, 68, 72, 74, 75, 78, 79, 80, 81, 82,
83, 85, 89, 90, 92, 93, 96, 98, 99, 100, 101,
102, 103, 133, 141, 147, 148, 149, 152, 153,
154, 155, 156, 157, 158, 159, 160, 161, 162,
163, 164, 165, 166, 167, 168, 169, 170, 171,
172, 173, 174, 175, 176, 177, 178, 179, 180,
181, 182, 183, 184, 185, 186, 187, 188, 189,
190, 194, 195, 196, 197, 198, 199, 200, 201,
202, 203, 204, 205, 206, 207, 208, 209, 210,
212, 213, 214, 215, 216, 219, 220, 221, 222,
223, 224, 225, 226, 227, 228, 229, 230, 231,
233, 234, 235, 236, 237, 238, 241, 242, 243,
246, 247, 248, 249, 251, 252, 253, 255, 256,
257, 258, 259, 260, 261, 262, 263, 264, 265,
266, 267, 268, 269, 270, 271, 272, 273, 276,
277, 279, 280, 281, 282, 283, 284, 285, 286,
287, 288, 289, 290, 291, 292, 293, 294, 295,
296, 299, 300, 301, 302, 303, 304, 305, 306,
307, 308, 309, 310, 311, 312, 313, 314, 315,
316, 317, 318, 319, 320, 321, 322, 323, 324,
327, 329, 333, 335, 346, 348, 356, 357, 360

十一劃

假名化 ... 162, 165, 166, 167, 187, 261,
263, 283, 286, 287, 297, 320, 358

偏見 31, 34, 91, 219, 276, 305, 355

匿名化 85, 162, 165, 166, 167, 180,
181, 186, 187, 189, 191, 193, 195, 201, 238,
283, 284, 286, 287, 314, 317, 320, 349, 350,



351
敏感個資... xix, xxi, 155, 181, 194, 196,
198, 200, 201, 206, 221, 261, 289, 314

深度學習 xvi, xvii, 4, 10, 13, 19, 24, 26,
27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 51, 77,
210, 211, 215, 216, 224, 248, 265, 271, 303,
307, 313, 356

十二劃

無人載具科技創新實驗條例iv, xxi,
13, 37, 139, 140, 141, 160, 205, 284, 333,
359

雲端運算.....37, 48, 264, 283, 355

十三劃

資料主體....90, 91, 102, 151, 159, 162,
164, 165, 166, 169, 175, 176, 177, 187, 238,
252, 262, 272, 273, 274, 275, 281, 285, 286,
356

資料控制者..13, 21, 22, 68, 73, 74, 76,
79, 103, 151, 152, 156, 157, 158, 162, 165,
166, 170, 174, 177, 185, 194, 219, 220, 228,
234, 237, 252, 255, 260, 262, 263, 264, 266,
270, 272, 273, 274, 275, 276, 278, 279, 285,
286, 288, 290, 292, 294, 309, 310, 317, 356

資料經濟.....21, 71, 72, 78, 81, 82, 86,
149, 197, 221, 272, 295, 299, 310, 311, 317,
322, 323, 356

資料蒐用者.....74, 103, 163, 174, 182,
184, 185, 189, 194, 207

資料融合 ... 14, 54, 55, 64, 65, 66, 213,
225, 260, 268, 300, 308, 314, 356

十四劃

蒐用 ..4, 6, 7, 17, 21, 46, 74, 79, 80, 82,
99, 100, 103, 149, 158, 162, 163, 170, 174,
176, 182, 184, 185, 189, 194, 205, 207, 212,
214, 219, 223, 229, 231, 264, 269, 272, 273,
282, 283, 285, 286, 287, 295, 302, 306, 307,
308, 309, 314, 315

十五劃

數據經濟 19, 356

十六劃

機械學習 ... ii, iv, xvi, xvii, xix, 4, 5, 7, 9,
10, 13, 16, 17, 18, 19, 24, 26, 27, 28, 29, 30,
31, 32, 34, 35, 49, 51, 52, 64, 68, 72, 74, 76,
79, 80, 82, 157, 191, 205, 206, 207, 210, 211,
212, 213, 214, 215, 216, 219, 220, 224, 237,
241, 243, 248, 249, 252, 254, 260, 265, 266,
269, 270, 271, 272, 276, 277, 278, 279, 280,
281, 282, 283, 285, 295, 300, 303, 304, 306,
307, 309, 313, 319, 320, 358

默認隱私296, 358

十七劃

聯網車 ...iv, xviii, 8, 21, 22, 61, 62, 160,
172, 173, 174, 175, 176, 177, 194, 206, 208,
222, 229, 240, 272, 286, 300, 302, 304, 309,
313, 315, 355

隱私 iv, xvi, xvii, xx, xxi, 2, 4, 5, 8, 9, 10,
11, 12, 13, 15, 16, 17, 18, 19, 21, 22, 24, 34,

63, 64, 66, 71, 72, 74, 75, 78, 80, 81, 82, 83,
84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95,
96, 97, 98, 99, 100, 101, 102, 107, 110, 127,
141, 149, 150, 152, 154, 157, 158, 159, 162,
163, 165, 166, 167, 168, 172, 174, 176, 177,
179, 180, 198, 204, 205, 207, 209, 212, 215,
216, 217, 218, 219, 220, 221, 222, 223, 224,
225, 226, 227, 229, 230, 231, 232, 235, 236,
237, 239, 241, 242, 246, 248, 251, 255, 259,
260, 265, 266, 267, 268, 269, 270, 271, 272,
274, 276, 277, 279, 280, 281, 282, 283, 284,
285, 286, 292, 295, 296, 297, 298, 299, 302,
303, 304, 306, 307, 308, 309, 310, 311, 312,

313, 314, 315, 316, 317, 318, 319, 320, 321,
322, 323, 325, 326, 327, 329, 330, 332, 336,
345, 358

隱私設計 9, 18, 165, 286, 295, 296,
297, 299, 310, 311, 313, 314, 316, 358

隱私權 5, 10, 11, 13, 16, 72, 74, 75, 83,
84, 85, 86, 87, 88, 89, 92, 93, 94, 95, 96, 97,
98, 99, 101, 102, 141, 149, 152, 154, 159,
166, 179, 180, 206, 217, 218, 222, 223, 226,
227, 231, 242, 259, 266, 269, 270, 277, 285,
292, 295, 303, 306, 312, 327, 329, 358

