立法院法制局專題研究報告　　編號：1686

本報告僅供委員參考

道路交通事故零死亡願景系列－駕駛隱私蒐集保護機制之研究

法制局 林鈺琪 撰

中華民國 113 年 5 月

道路交通事故零死亡願景系列－駕駛隱私蒐集保護機制之研究

目　次

摘　要

駕駛狀態監測系統在利用影像辨識AI演算法技術，確保自動駕駛時的本身與其他用路人的安全下，同時也衍生數位科技的運用是否會侵犯個人隱私的問題。資料交換對個人隱私的保護帶來新的挑戰，資料處理者若自多個來源取得資料後進行比對串連，將使得個人隱私資料洩漏的風險急遽升高。在我國法制尚未完善前，建議未來在持續微調各項個人資料保護法規時，除了參酌國外規範外，也可廣納公民團體之意見，並衡量產業的需求，讓隱私與技術發展的需求能夠取得良好的平衡。爰本報告擬針對非公務機關(汽車業者)就駕駛隱私蒐集可能涉及的問題及相關保護機制進行研究，並整理外國立法例及相關學者意見，以供委員問政或修法之參考。

道路交通事故零死亡願景系列－駕駛隱私蒐集保護機制之研究

壹、前言

多項調查報告指出，駕駛者分心與疲勞是造成車輛意外事故的重要原因。美國公路運輸安全管理(National Highway Traffic Safety Adminstration, NHTSA)統計資料研究指出，每年因為駕駛者分心與疲勞導致之交通事故保守估計至少約占整體交通事故的10%[1]。

另，歐盟執委會(European Commission)估計，歐洲地區每年因駕駛分心導致交通事故的比例約占總事故的10%至30%，Frost & Sullivan認為透過駕駛監控系統(Driver Monitoring System, DMS)監控駕駛的睡意和注意力，將可提升道路交通安全性。由於法規的要求，歐洲地區DMS的市場滲透率有望由2020年[2]的0%在2024年達到100%，而北美隨著汽車專業代工廠(OEMs)引入具自動駕駛第2級(Level 2)、2+級(Level 2+)和3級(Level 3)功能的車輛，也讓DMS有愈來愈普及的趨勢。預測未來DMS的應用也將由監控駕駛、結合先進駕駛輔助系統(Advanced Driver Assistance Systems, ADAS)，到對車艙(乘客)監控，提供乘客個人化介面的乘客監控系統(Occupant Monitoring Systems, OMS)[3]。

駕駛狀態監測系統(Driver State Monitoring, DSM)在利用影像辨識AI演算法技術，確保自動駕駛時的本身與其他用路人的安全下，同時也衍生數位科技的運用是否會侵犯個人隱私的問題。故本報告擬針對非公務機關(汽車業者)就駕駛隱私蒐集可能涉及的問題及相關保護機制進行研究，並整理外國立法例及相關學者意見，以供委員問政或修法之參考。

---

[1] 張銘方，開車不要玩手機！「駕駛者監控系統」以影像辨識偵測分心駕駛行為，財團法人車輛研究測試中心，107年11月21日，網址：https://pansci.asia/archives/134450，最後瀏覽日期：113年4月9日。

[2] 本報告有關年分之使用，原則以民國紀年表述，惟涉及外國法制或立法例部分，改採西元紀年表述。

[3] 張艾琦，駕駛監控系統市場的成長因素與法律規範發展概況，科技發展觀測平台，110年6月15日，網址：https://outlook.stpi.narl.org.tw/index/focus-news/4b114100791e3859017a0d81b517101f，最後瀏覽日期：113年4月9日。

貳、問題研析與建議

一、駕駛狀態監測簡介及相關規範

（一）駕駛狀態監測簡介[4]

車外環境的偵測固然重要，但車內的狀況，尤其是駕駛者的狀態也是行車安全，甚至是整體道路安全的關鍵所在[5]。駕駛狀態監測系統是以車艙內感測器監測駕駛狀態，係以數位訊號處理器為核心，接收攝影機並輔以紅外線投光器等感測元件，擷取車艙內駕駛人臉影像資訊，透過影像處理技術偵測駕駛面部特徵位置，並結合駕駛行為模型，估計駕駛者行駛行為特徵，判斷駕駛者開車之專注力，當系統判定為異常行為發生時，如分心駕駛、手機通話和吸菸等異常行為發生時，系統透過 GPIO（General- purpose input/output）以揚聲器發出警示聲；亦能透過 CAN BUS 介面讀取車速、方向燈等車身訊號，以輔助判斷系統啟動時機。

1. 分心駕駛行為偵測技術

透過車室內的攝影機與紅外線光源裝置，擷取全天候（日/夜）駕駛面部影像，偵測駕駛人臉五官位置，進行辨識臉部注視方向的駕駛視野分析，並估算頭部（左、右）偏擺量，進而分析駕駛者的分心程度，當超越警示值時，則給予適當的警示，其辨識率可達 95%以上。

2. 違規駕駛行為偵測技術

異常行為偵測演算法主要目的為偵測駕駛者打手機與吸菸狀態，而藉由臉部特徵判斷偏擺角度，角度過大時，其為危險駕駛，角度於容許範圍時，亦同時進行異常行為偵測-打手機與吸菸狀態，打手機行為與吸菸行為辨識係參考前述所得人臉五官位置，並透過臉部邊界與人臉五官之幾何關係，取得打手機與吸菸偵測特徵區域搜尋，其偵測方法以分類器演算法進行比對與估測，辨

[4] 張銘方，同註 1。

[5] 籃貫銘，駕駛注意力與生理狀態偵測系統，CTIMES，107 年 5 月 3 日，網址：https://www.ctimes.com.tw/DispArt/tw/ADAS/1805031041UM.shtml，最後瀏覽日期：113 年 4 月 10 日。

識率可達 90%以上。

因此，駕駛狀態監測系統捕捉駕駛的臉部影像，並透過視覺分析評估其狀況，可以識別打哈欠、閉眼、吸煙、使用手機和分心等行為。如果駕駛出現任何異常行為，它會提供即時音訊警告進行提醒，在一定程度上減少事故發生的可能性。此外，駕駛狀態監測系統會將駕駛的狀態以視訊形式上傳到管理軟體平台，管理人員可以遠端監控，及時提醒；情況嚴重時，系統還可以在出現危急情況時透過 4G 網路通知後台監控中心，以便人工干預和監管，從而降低事故風險[6]。

（二）國外規範

DMS 市場成長快速有很大的因素是各國及各經濟體法令強制要求，國外相關規範如下[7]：

1. 歐盟一般安全規則(General Safety Regulation)

要求 2022 年的新型車款應配備能偵測駕駛睡意和注意力、駕駛分心預警或預防功能[8]。

2. 聯合國歐洲經濟委員會(United Nations Economic Commission for Europe, UNECE)通過第 3 級有條件自動駕駛的自動車道維持系統(Automated Lane Keeping System, ALKS)規範

要求汽車製造商在生產汽車時需安裝駕駛能力識別系統(Driver Availability Recognition System)於車內，藉由 DMS 辨識駕駛是否在座位上、判斷駕駛是否維持駕駛車輛的能力，一旦有異常，或者被監控到不符合標準，系統應立即發出明確警告，或發送駕駛模式切換要求，應自動暫停[9]。該規範於 2021 年 1 月生效，

[6] Why is Driver Status Monitoring(DSM) System helpful to prevent fatigued driving? ICAR VISIONS，110 年 7 月 30 日，網址：https://www.icarvisions.com/ai/why-is-driver-status-monitoring-dsm-system-helpful-to-prevent-fatigued-driving-754.html，最後瀏覽日期：113 年 4 月 16 日。

[7] 張艾琦，同註 3。

[8] New rules to improve road safety and enable fully driverless vehicles in the EU，European Commission，2022 年 7 月 6 日，網址：https://ec.europa.eu/commission/presscorner/detail/en/ip_22_4312，最後瀏覽日期：113 年 4 月 9 日。

[9] UN regulation on Automated Lane Keeping Systems (ALKS) extended to trucks, buses and coaches，UNECE，2021 年 11 月 26 日，網址：https://unece.org/sustainable-development/press/un-regulation-automated-lane-keeping-systems-alks-ex

德國、法國、荷蘭、日本與加拿大計劃實施該規範。

3. 歐盟新車安全評鑑協會(European New Car Assessment Programme, Euro NCAP)

提出 Roadmap 2025 願景藍圖,並計劃於 2020 年開始評價 DMS 的可靠性及準確性。將駕駛監測系統列為安全評分項目，要求汽車製造商提供盡可能最佳的技術，作為所有細分市場和國家的標準，不僅保護各個年齡段的汽車乘客，並且解決其他較脆弱的道路使用者的安全問題[10]。

4. 美國

美國國家運輸安全委員會(National Transportation Safety Board，NTSB)建議美國國家公路交通安全管理局(National Highway Traffic Safety Administration, NHTSA）與 SAE International 及其他機構為具備自動駕駛 2 級與 2+級功能的車輛建立 DMS 表現準則，並以此準則要求所有具備 2 級與 2+級功能的乘用車配備 DMS。

（三）我國規範

我國已有交通法規禁止行車中使用手持式行動電話等駕駛異常行為，以避免駕駛分心，現行駕駛狀態監測的項次，主要分為分心駕駛與疲勞駕駛兩大部分[11]：

1. 分心駕駛部分

針對駕駛人行駛道路，有以手持方式使用行動電話、電腦或其他相類功能裝置進行撥接、通話、數據通訊或其他有礙駕駛安全之行為時，處新臺幣(下同)3 千元、1 千元或 6 百元罰鍰[12]。

---

tended-trucks，最後瀏覽日期：113 年 4 月 9 日。

[10] Euro NCAP Launches Road Map 2025 - In Pursuit of Vision Zero，Euro NCAP，2017 年 9 月 12 日，網址：https://www.euroncap.com/en/press-media/press-releases/euro-ncap-launches-road-map-2025-in-pursuit-of-vision-zero/，最後瀏覽日期：113 年 4 月 9 日。

[11] 張銘方，同註 1。

[12] 道路交通管理處罰條例第 31 條之 1：「汽車駕駛人於行駛道路時，以手持方式使用行動電話、電腦或其他相類功能裝置進行撥接、通話、數據通訊或其他有礙駕駛安全之行為者，處新臺幣三千元罰鍰。

機車駕駛人行駛於道路時，以手持方式使用行動電話、電腦或其他相類功能裝置進行撥接、通話、數據通訊或其他有礙駕駛安全之行為者，處新臺幣一千元罰鍰。

2.疲勞駕駛部分

而汽車駕駛人連續駕車超過 8 小時經查屬實，或患病足以影響安全駕駛者，處 1 千 2 百元以上 2 千 4 百元以下罰鍰，並禁止其駕駛；如應歸責於汽車所有人者，得吊扣其汽車牌照 3 個月[13]。

二、駕駛狀態監測可能涉及的法律規定

（一）妨害秘密罪[14]

1.類型

(1) 窺視或竊聽

無故利用工具或設備窺視、竊聽他人非公開的活動、言論、談話或身體隱私部位。

(2) 竊錄

無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開的活動、言論、談話或身體隱私部位。

2.法律效果

(1) 3 年以下有期徒刑、拘役或 30 萬元以下罰金。

(2) 妨害秘密罪是告訴乃論之罪。

（二）資訊隱私權

依個人資料保護法第 6 條[15]規定，針對病歷、醫療、基因、性生活、

汽機車駕駛人行駛於道路，手持香菸、吸食、點燃香菸致有影響他人行車安全之行為者，處新臺幣六百元罰鍰。

警備車、消防車及救護車之駕駛人，依法執行任務所必要或其他法令許可者，得不受第一項及第二項之限制。

第一項及第二項實施及宣導辦法，由交通部定之。」

[13] 道路交通管理處罰條例第 34 條：「汽車駕駛人，連續駕車超過八小時經查屬實，或患病足以影響安全駕駛者，處新臺幣一千二百元以上二千四百元以下罰鍰，並禁止其駕駛；如應歸責於汽車所有人者，得吊扣其汽車牌照三個月。」

[14] 刑法第 315 條之 1：「有下列行為之一者，處三年以下有期徒刑、拘役或三十萬元以下罰金：
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。」
刑法第 319 條：「第三百十五條、第三百十五條之一及第三百十六條至第三百十八條之二之罪，須告訴乃論。」

[15] 個人資料保護法第 6 條：「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：
一、法律明文規定。

健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用，但是亦有例外情形，例如法律明文規定、公務機關執行法定職務或非公務機關履行法定義務所必要、當事人自行公開或其他已合法公開之個人資料、經當事人書面同意等情形。

另依該法第 19 條[16]規定，非公務機關運用監視錄影器，蒐集涉及個人資料的畫面，應該要有特定目的，並且需要符合個人資料保護法的規範，例如：執行法定職務必要範圍內、法律明文規定、與公共利益有關。

是以，因現行未有法律明文規定，得運用駕駛狀態監測蒐集個人資料，故蒐集者不得蒐集、處理或利用駕駛狀態監測所記錄的有關駕駛之一切資訊，否則恐有違資訊自主權之虞。除非透過駕駛書面同意之意思表示下即時監控駕駛生理狀態，則可適用該法第 6 條第 1 項第 6 款或第 19 條第 1 項第 5 款之規定，「經當事人(書面)同意」，則不受個人資料蒐集之限制。

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。

三、當事人自行公開或其他已合法公開之個人資料。

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。

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。

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。

依前項規定蒐集、處理或利用個人資料，準用第八條、第九條規定；其中前項第六款之書面同意，準用第七條第一項、第二項及第四項規定，並以書面為之。」

[16] 個人資料保護法第 19 條：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：

一、法律明文規定。

二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。

三、當事人自行公開或其他已合法公開之個人資料。

四、學術研究機構基於公共利益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。

五、經當事人同意。

六、為增進公共利益所必要。

七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。

八、對當事人權益無侵害。

蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。」

三、車內空間係屬私人活動領域或公開活動場所之界定問題

就刑法妨害秘密罪而言，依該法第 315 條之 1 規定，無故竊錄他人「非公開活動」，將構成妨害秘密罪；其規範對象係「他人非公開之活動」、「他人非公開之言論、談話」、「他人身體隱私部位」之「窺視」、「竊聽」或「竊錄」等行為。而構成要件中「非公開」要件的功能在於描述刑法所承認的隱私主張，也就是符合「非公開」要件之活動被窺視、竊聽、竊錄後，才形成隱私權侵擾問題[17]。

復依最高法院 100 年度台上字第 4780 號判決[18]指出：所謂「非公開之活動」，係指活動者主觀上具有隱密進行其活動而不欲公開之期待或意願（即主觀之隱密性期待），且在客觀上已利用相當環境或採取適當設備，足資確保其活動之隱密性者（即客觀之隱密性環境）而言（例如在私人住宅、公共廁所、租用之 KTV 包廂、旅館房間或露營之帳篷內，進行不欲公開之更衣、如廁、歌唱、談判或睡眠等活動均屬之）。「非公開之活動」之認定，固應著重於活動者主觀上具有不欲其活動遭他人攝錄之意願或期待，仍須活動者在客觀上已利用相當環境或採取適當設備，足資確保活動之隱密性，始能明確化上述構成要件之內容。

學說上有從美國法隱私的「合理隱私期待」概念來解釋，認為由於「非公開」的解釋是依據當事人之主觀是否有意隱藏來判斷，唯有以外在阻隔或遮掩行為，將自己由眾人焦點下抽離開來，或在身體上隔離自己等行為表現出隱藏的內在意思，才能被確認存在主觀隱私之期待，也才可能討論是否具有合理性，而足資認定為具有「非公開」性質[19]。

學者亦有從活動的場域區分公開與非公開，因為刑法第 315 條之 1 保護法益為隱私，所以應指於專屬於個人私密或私人領域中，身體活動不受他人侵擾而言；當個人處於公共領域中，或是不具保持隱密客觀條件之場所，導致他人得以偶然侵入或窺視其活動，則不得主張或期待享

[17] 蔡蕙芳，〈從美國隱私權法論刑法第三一五條之一與相關各構成要件（下）〉，《興大法學》，第 7 期，99 年 6 月，頁 32、35。

[18] 最高法院 100 年度台上字第 4780 號判決，司法院裁判書系統，100 年 8 月 31 日，網址：https://judgment.judicial.gov.tw/FJUD/default.aspx，最後瀏覽日期：113 年 4 月 10 日。

[19] 蔡蕙芳，同註 17，頁 36。

有在隱私領域中同等的保護[20]。

然而，司法院釋字第 689 號解釋：「……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。」也就是說，即便是在「公共場所」，還是能主張最低限度的隱私權，也就是依社會通念得不受他人持續注視、監看、監聽、接近等騷擾行為。

實務見解[21]認為車輛使用人行駛於道路或其他公共場域，固係處於同時間利用同一空間之他人可得共見共聞之狀態。惟他人之私密領域及個人資料自主，如在公共場域受到干擾，而超出可容忍之範圍，該干擾行為亦有加以限制之必要，俾有不受他人持續追蹤及侵擾之私人活動領域，而得保有「獨處之權利」。因此，車輛在公共道路上之行跡，伴隨駕駛或乘員即時發生之活動行止，除明示放棄隱私期待之情形，通常可認其期待隱沒於道路上之往來車輛，不欲公開其個人行蹤。

綜上，車內活動可能屬於非公開活動，當事人的主觀意願以及客觀上的保密措施，若存在合理的隱私期待，則可以認定車內空間係屬私人活動領域。因此，若車上設置駕駛狀態監測系統，個人之私人活動及隱私受保護之需要，將隨之提升。

四、駕駛狀態監測對個人隱私權之隱憂

根據非營利組織 Mozilla 基金會的調查發現，汽車是其審查過的產品當中，隱私項目做的最糟糕的；高達 92%汽車製造商幾乎沒有給予駕駛人控制個資的權利，84%的廠商還會與外部企業分享客戶的數據，76%

[20] 王皇玉，〈刑法對隱私權的保障：以刑法第三一五條之一為中心〉，《臺灣法學雜誌》，第 122 期，98 年 2 月，頁 37-38。

[21] 臺灣高等法院高雄分院 105 年度上易字第 604 號刑事判決，司法院裁判書系統，106 年 1 月 18 日，網址：https://judgment.judicial.gov.tw/FJUD/data.aspx?ty=JD&id=KSHM%2c105%2c%e4%b8%8a%e6%98%93%2c604%2c20170118%2c1&ot=in，最後瀏覽日期：113 年 4 月 10 日。

的品牌表示他們可以出售這些收集來的數據[22]。當政府或執法人員提出請求時，56%的車廠會分享用戶資訊，特別要注意的是，這裡說的「請求」不是法院的搜索令，僅需要警察局的公文即可[23]。

Mozilla 團隊針對市面上 25 個汽車品牌進行調查，分析其個資保護與隱私處理，結果 25 個品牌全部都獲得了 Mozilla 認證的「隱私未保護」標籤，也讓汽車產業成為這項調查中表現最糟糕的一個產業[24]。會被竊取的資料包括臉部表情、體重、駕駛人的種族、行車地點、車上的通訊設備等等。而竊取方式有感測器、車上的麥克風與監視器，以及透過藍芽連接車上的娛樂系統等，這些因素都導致了駕駛人資料的外洩[25]。此外，Mozilla 調查團隊也遭遇到一個詭異的狀況，在所有調查的汽車製造商中，他們甚至無法確定資料傳輸究竟有沒有加密[26]。

更值得注意的是，除了 Tesla、Renault 和 Dacia 以外的車廠，全部都簽署了汽車創新聯盟提出的《消費者隱私保護原則》，承諾收集最小化個資、透明原則、保有選擇等，不過根據 Mozilla 的說法，沒有任何一家車廠做到這些事，所謂隱私保護原則，只是一層漂亮的糖衣包裝。有論者提及「你在使用這些功能前，都會跳出個資請求，不想要個資被使用就不要同意就好。」問題在於，如果你不同意車輛的個資請求，就會導致許多功能被限制，表面上看來是提供選擇，實質上是強迫使用者乖乖就範[27]。

綜上所述，顯見此調查凸顯了迫切需要強化汽車行業的隱私政策和數據保護措施[28]。

另哈佛大學卡爾人權政策中心（Carr Center for Human Rights Policy）

---

[22] 黃士育，你的車，其實是隱私殺手！25 家車商收集個資、部分還出賣，連性生活也掌握？數位時代，112 年 9 月 11 日，網址：https://www.bnext.com.tw/article/76639/mozilla-cars-data-privacy，最後瀏覽日期：113 年 4 月 10 日。

[23] Chen Kobe，買新車等於個資惡夢，新車個資安全測試 25 家車廠全軍覆沒，資安快報，112 年 9 月 8 日，網址：https://infosecu.technews.tw/2023/09/08/new-car-personal-data-issue/，最後瀏覽日期：113 年 4 月 16 日。

[24] Chen Kobe，同前註。

[25] 黃士育，同註 22。

[26] Chen Kobe，同註 23。

[27] 同前註。

[28] 黃士育，同註 22。

科技人權研究員卡恩（Albert Fox Cahn)指出,「越來越多汽車變成行動竊聽器，駕駛人花錢安裝的汽車電子設備越來越貴，車主和乘客被收集的個資也越來越多；汽車已成為企業界侵入客戶隱私的獨特監控空間。」不過，代表美國市場主要汽車和輕型卡車製造商的組織「汽車創新聯盟」(Alliance for Automotive Innovation)對此說法提出質疑，聯盟並呼籲制定聯邦隱私法，因各州隱私法規不一，令消費者混淆，也讓廠商難以適從[29]。

鑒於資訊隱私權的作用，不只有消極抵抗政府侵害的防禦功能，更具有積極要求國家提供保護的功能。也就是說，國家為保障資訊隱私權，負有配合當代科技發展的保護義務。無論係由國家或私人蒐集、利用個人資料，其皆應有法律基礎，且必須具備特定目的。為確保資料正確及安全，更要建立資料不受濫用與不當洩露的適當防護機制，這些防護機制並應配合當代科技發展而有所提升[30]。因此，隨著資訊科技高度發展及相關設備之方便取得，個人之私人活動及隱私受保護之需要亦隨之提升，其實也考驗著各車廠、決策者及立法者如何在科技與隱私中，找到適合的平衡點。

五、宜制定隱私影響評價機制

（一）定義

隱私影響評價（Privacy Impact Assessment, PIA），PIA 係指在建立以資訊系統收集、處理個資檔案前，對當事人隱私權等權益可能造成之影響須先作評價，並檢視該資訊系統在技術上，是否為對個人權利影響最低限度之設計。此制度之理論依據與環境影響評估類似，因為環境一旦因開發公共事業而遭受破壞，即有難以回復原狀之特性；同理個資一旦依資訊系統處理成為檔案而利用，在網路上流出後，亦難以救濟；故在損害或風險未發生前，應先對系統設計、運用計畫及安全維護措施等事項進行評價，判斷是否能確保個人權利及適當、合法進行個資之處理；

[29] 胡玉立，車主隱私堪憂 25 家車商全未通過保護個資最低標準，世界新聞網，112 年 9 月 6 日，網址：https://www.worldjournal.com/wj/story/121469/7422438，最後瀏覽日期：113 年 4 月 10 日。

[30] 林煜騰、楊劭楷，從健保資料庫案的憲法指標，檢視台灣未來數位政策，鳴人堂，111 年 8 月 23 日，網址：https://opinion.udn.com/opinion/story/10043/6557094，最後瀏覽日期：113 年 4 月 16 日。

此制度之目的有三：1.確保安全、合法處理個資，其重點非僅在事故發生後之救濟，而應更積極在事前建立防止損害發生對策；2.其評價結果則由資料管理者自己公布，提升資料管理制度之透明度，以增加當事人之信賴；3.評價報告須報請獨立監督機關作確認，亦得擔保管理資料系統者落實遵法之義務[31]。

（二）歐盟

歐盟「一般資料保護規則」(General Data ProtectionRegulation, GDPR)更採取具體與抽象要件並列之方式，要求資料管理者針對「基於個人資料之自動化蒐集、處理或利用，對自然人個人進行系統性及大規模分析，並據以對特定個人作成具有法律效果之決定或產生類似影響」、「大規模蒐集、處理或利用第 9 條第 1 項[32]規定之特種個人資料或第 10 條[33]規定之前科資料」、「大規模且系統性地監控公眾場所」，以及「可能造成資料當事人自由權利高度風險之資料利用行為」，於事前進行「個人資料保護影響評估(Data Protection Impact Assessment)」(第 35 條第 1 項[34]及第 3 項[35]參

[31] 新保史生，〈社会保障・税に関わる番号制度の導入とプライバシー〉，《Nextcom》，第 8 号，2011 年 12 月，頁 10；小林慎太郎，〈プライバシー影響評価（PIA）に基づく個人情報の有効活用を考える〉，《NRI Public Management Review》，第 113 期，2012 年 12 月，頁 5。轉引自范姜真媺、劉定基、李寧修，《歐盟及日本個人資料保護立法最新發展之分析報告》，出版地：法務部委託研究，105 年 12 月 30 日，頁 165。

[32] Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

[33] Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. 2Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

[34] Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. 2A single assessment may address a set of similar processing operations that present similar high risks.

[35] A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

照)。至於評估之事項，除個資蒐集、處理或利用行為及其目的之具體描述，蒐集、處理或利用之合法事由為何外，也必須針對該資料使用與所設定目的間之必要性加以檢視；當然，最重要者之評估事項則是該行為對於資料當事人自由、權利可能造成之風險與資料管理者所採取之保護措施、安全措施（第 35 條第 7 項[36]參照）[37]。

換言之，採用特定新科技處理個人資料時，除需考量個人資料處理之本質、範圍、使用情形與處理目的外，若該處理可能產生對自然人權利或自由之高度風險時，資料控管者必須於此個資處理前，進行資料保護之衝擊（影響）評估。其目的在落實個人資料保護之問責可能性，協助資料控管者確保所採用之處理措施符合 GDPR 之要求。尤其當資料處理涉及大規模之自動化資料處理與剖繪，而對相關自然人產生法律效果或重大影響時，或係大規模處理特種個人資料或刑事犯罪資料，或係對於公共區域進行大規模監控時，必須強制進行個人資料保護影響評估[38]。

另值得注意的是，依據歐盟 GDPR 第 83 條第 4 項[39]之規定，違反個人資料保護影響評估規定者，將面臨最高 1 千萬歐元或前一年度全球營業額百分之二之罰鍰（以較高者計），足見歐盟對於個人資料保護影響評估之重視[40]。

（三）英國

---

[36] The assessment shall contain at least:
(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

[37] 范姜真媺、劉定基、李寧修，同註 31，頁 166-167。

[38] 戴豪君、邱映曦，〈從 GDPR 遵循角度看組織資料治理新意識〉，《國土及公共治理》，第 7 卷，第 4 期，總期 28，108 年 12 月，頁 21-22。

[39] Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
(b) the obligations of the certification body pursuant to Articles 42 and 43;
(c) the obligations of the monitoring body pursuant to Article 41(4).

[40] 范姜真媺、劉定基、李寧修，同註 31，頁 167。

英國為因應歐盟 GDPR 之施行，於 2018 年 5 月通過「2018 年資料保護法」（Data Protection Act 2018），透過內國法律程序完成 GDPR 的施行。根據 GDPR 規定，資料保護影響評估須包含：第一，處理之目的；第二，處理之必要性及比例性；第三，對資料當事人權利及自由之評估；第四，應對風險之方法（包含保護措施等）；同時，並要求於事發當時應徵詢當事人或其代表人之意見，並在風險發生變化時，應重新進行資料保護影響評估。而若評估發現在未採取降低風險措施前，該處理將有高度風險時，控管者應於處理前徵詢主管機關[41]。

英國資訊長辦公室提供的指引進一步將資料保護影響評估機制分為 9 個步驟，包含：第一，確認是否需要實施資料保護影響評估；第二，描述所涉及的處理行為；第三，考慮進行諮詢；第四，評估處理之必要性與比例性；第五，辨別其中之風險並加以評估；第六，確認應採取的減輕風險措施；第七，簽核評估結果並存檔；第八，將評估結果落實進處理計畫；第九，持續複查隱私衝擊影響評估；英國資訊長辦公室並針對各個步驟操作時應注意之事項做更細部的規定，同時亦提供評估的模板供業者使用[42]。

（四）小結

我國現行並未具體規定隱私影響評估或資料保護影響評估之機制，惟個人資料保護法第 18 條[43]及第 27 條[44]分別要求公務及非公務機關應採行適當之安全維護措施，而依據個人資料保護法施行細則第 12 條[45]第 2

---

41 財團法人資訊工業策進會，研究數位匯流下通訊傳播產業資料加值應用及隱私保護之法規機制期末報告，國家通訊傳播委員會委託研究計畫，108 年 2 月，頁 39、56。

42 How do we carry out a DPIA? , Information Commissioner's Office (UK),https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-carry-out-a-dpia/（last visited Aug. 2, 2018）.轉引自財團法人資訊工業策進會，同前註，頁 57。

43 個人資料保護法第 18 條：「公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」

44 個人資料保護法第 27 條：「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。

前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。」

45 個人資料保護法施行細則第 12 條：「本法第六條第一項但書第二款及第五款所稱適當安全維護措施、第十八條所稱安全維護事項、第十九條第一項第二款及第二十七條第一項所稱適當之安全措施，指

項第 3 款之規定，所謂安全維護措施得包括「個人資料之風險評估及管理機制」，看似有類似之機制。然，上述「風險評估與管理機制」除內涵不若歐盟 GDPR 清晰、明確外，此一安全維護措施之義務，解釋上應該係資料管理者已經蒐集、處理或利用相關資料「後」之「義務」，此與歐盟法制強調「事前」之影響評估，存在相當大之落差[46]。

在數位時代下，如何於「事前」透過一定之評估程序與機制，確保相關資料利用行為對於資料當事人權益不至造成侵害，恐怕是無法迴避之問題[47]。隱私蒐集評估機制雖並非各國常見之制度，但其設計之本意，在於協助業者在採取新技術之前，透過影響評估識別出風險，並評估可採行之減輕措施。對於業者完善資料治理，建立民眾對資料使用之信任有所助益。此外，對於採用自動化決策處理技術進行資料處理前，應採取隱私影響評估機制的見解，目前雖僅有歐盟有相關規定，各國並未以法律規範此一評估機制，但觀察國際發展，在各國隱私主管機關間，似乎已經逐漸形成「應該引入類似之風險評估機制」之共識[48]。

因此，在損害或風險未發生前，應預先對系統設計、運用計畫及安全維護措施等事項進行評價，判斷是否能確保個人權利及適當、合法進行個資之處理。是以，為妥善控制、避免政府資料開放與大數據分析等可能對於資料當事人權益產生重大影響之資料蒐集、處理或利用行為，建議可參考歐盟或英國有關隱私影響評估之建置方式，課予進行特定資

公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。

前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：

一、配置管理之人員及相當資源。

二、界定個人資料之範圍。

三、個人資料之風險評估及管理機制。

四、事故之預防、通報及應變機制。

五、個人資料蒐集、處理及利用之內部管理程序。

六、資料安全管理及人員管理。

七、認知宣導及教育訓練。

八、設備安全管理。

九、資料安全稽核機制。

十、使用紀錄、軌跡資料及證據保存。

十一、個人資料安全維護之整體持續改善。」

[46] 范姜真媺、劉定基、李寧修，同註 31，頁 167。

[47] 范姜真媺、劉定基、李寧修，同註 31，頁 168。

[48] 財團法人資訊工業策進會，同註 41，頁 87-88、211。

料蒐集、處理或利用行為之非公務機關（判斷標準可以「資料蒐集、處理或利用之規模」及「對資料當事人權利影響之嚴重程度」判斷），進行「事前」隱私影響評估（資料保護影響評估）之義務[49]。或是以「鼓勵」與建議的方式，引導業者在採取應用新的技術之前，得以先採取類似之步驟，以降低技術可能帶來的風險[50]。

參、結論

智慧車輛已成為全球汽車產業發展的重要方向，也開始有相關的鼓勵政策及標準規範，如 The European New Car Assessment Programme (Euro NCAP)所發布的 Road Map 2025，要求從 2020 年開始，想要獲得歐盟 5 星安全認證的車輛就必須具備駕駛監控。此外，Euro NCAP 自 2023 年起將車輛具備「車內兒童偵測」功能作為評分依據之一，此將帶動市場需求，由駕駛監控系統的警示功能擴展到車內人員監控系統，並延伸到兒童遺留偵測。由此可見，隨著汽車產業於智慧駕駛、安全輔助、車用電子與人機介面相關技術發展迅速，整合虛實疊合顯示、駕駛監控、互動功能、物聯網之智慧座艙系統已成為目前趨勢[51]。

隨著資料科學以及人工智慧技術的蓬勃發展，資料逐漸被視為重要的策略性資源，而資料交換對個人隱私的保護帶來新的挑戰，資料處理者若自多個來源取得資料後進行比對串連，將使得個人隱私資料洩漏的風險急遽升高。過去往往認為，如果資料的擁有者不要釋出資料表，而僅僅釋出如平均值、總數等統計值即可保護敏感資訊。但是事實上，僅僅釋出統計數值仍可能導致隱私洩露[52]。

有學者[53]指出，我國個人資料保護法第 2 條[54]第 2 款雖有將個人資料

---

[49] 范姜真媺、劉定基、李寧修，同註 31，頁 199。

[50] 財團法人資訊工業策進會，同註 41，頁 88。

[51] 蘇一峰，智慧座艙監控技術介紹，財團法人車輛研究測試中心 ，111 年 5 月 11 日，網址：https://www.artc.org.tw/tw/knowledge/articles/13648，最後瀏覽日期：113 年 4 月 11 日。

[52] 李思壯、黃彥男，〈數位時代之數位隱私保護〉，《國土及公共治理季刊》，第 7 卷，第 4 期，108 年 12 月，頁 30、35。

[53] 翁逸泓，〈面部自動辨識監控系統與個資保護問題研究：Bridges 案之啟示〉，《政大法學評論》，第 168 期，111 年 3 月，頁 304。

[54] 個人資料保護法第 2 條：「本法用詞，定義如下：
一、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、

檔案定義為「指依系統建立而得以『自動化機器』或其他非自動化方式檢索、整理之個人資料之集合」之關於自動化機器之文字敘述，然所規範之單純得以自動化方式檢索與整理之機器事實上與得作成自動化決策或甚至人工智慧決策之當代資料科技應用方式頗有區別，在適用上仍有落差，故我國個人資料保護法在未經「現代化」之變更之前，難謂有任何個人資料保護法上對於該等自動化機器作成之決策與評價作出明文規範、保護乃至於例外情形之判准。因此，於法制與程序上應預先考量有一特別、明確之指引，而且該等規範必須特別注重平等(不歧視)、透明、比例原則，以及對於自動化決策之課責問題，使人民能有效地獲知該等政策，並使法律規範具有預測性與安定性。

因此，在我國法制尚未完善前，數位化社會發展已屬不可逆的趨勢，如何掌握資料與進行分析，是民間企業掌握市場競爭的關鍵，更是政府形成與推動政策時不可忽略的要素[55]。建議未來在持續微調各項個人資料保護法規時，除了參酌國外規範外，也可廣納公民團體之意見，並衡量產業的需求，讓隱私與技術發展的需求能夠取得良好的平衡。

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。

二、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。

三、蒐集：指以任何方式取得個人資料。

四、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。

五、利用：指將蒐集之個人資料為處理以外之使用。

六、國際傳輸：指將個人資料作跨國（境）之處理或利用。

七、公務機關：指依法行使公權力之中央或地方機關或行政法人。

八、非公務機關：指前款以外之自然人、法人或其他團體。

九、當事人：指個人資料之本人。」

[55] 戴豪君、邱映曦，同註 38，頁 25。

參考文獻

一、期刊

1、 王皇玉,〈刑法對隱私權的保障:以刑法第三一五條之一為中心〉,《臺灣法學雜誌》,第 122 期,98 年 2 月,頁 37-39。

2、 李思壯、黃彥男,〈數位時代之數位隱私保護〉,《國土及公共治理季刊》,第 7 卷,第 4 期,108 年 12 月,頁 30-39。

3、 翁逸泓,〈面部自動辨識監控系統與個資保護問題研究:Bridges 案之啟示〉,《政大法學評論》,第 168 期,111 年 3 月,頁 249-324。

4、 蔡蕙芳,〈從美國隱私權法論刑法第三一五條之一與相關各構成要件(下)〉,《興大法學》,第 7 期,99 年 6 月,頁 29-67。

5、 戴豪君、邱映曦,〈從 GDPR 遵循角度看組織資料治理新意識〉,《國土及公共治理》,第 7 卷,第 4 期,總期 28,108 年 12 月,頁 18-29。

二、研究計畫

1、 范姜真媺、劉定基、李寧修,《歐盟及日本個人資料保護立法最新發展之分析報告》,出版地:法務部委託研究,105 年 12 月 30 日。

2、 財團法人資訊工業策進會,研究數位匯流下通訊傳播產業資料加值應用及隱私保護之法規機制期末報告,國家通訊傳播委員會委託研究計畫,108 年 2 月。

三、網路資源

1、 Chen Kobe,買新車等於個資惡夢,新車個資安全測試 25 家車廠全軍覆沒,資安快報,112 年 9 月 8 日,網址:https://infosecu.technews.tw/2023/09/08/new-car-personal-data-issue/,最後瀏覽日期:113 年 4 月 10 日。

2、 Euro NCAP Launches Road Map 2025 – In Pursuit of Vision Zero,Euro NCAP,2017 年 9 月 12 日,網址:https://www.euroncap.com/en/press-media/press-releases/eur

o-ncap-launches-road-map-2025-in-pursuit-of-vision-zero/ ，最後瀏覽日期：113 年 4 月 9 日。

3、 New rules to improve road safety and enable fully driverless vehicles in the EU，European Commission，2022 年 7 月 6 日，網址：https://ec.europa.eu/commission/presscorner/detail/en/ip_22_4312，最後瀏覽日期：113 年 4 月 9 日。

4、 UN regulation on Automated Lane Keeping Systems (ALKS) extended to trucks, buses and coaches，UNECE，2021 年 11 月 26 日，網址：https://unece.org/sustainable-development/press/un-regulation-automated-lane-keeping-systems-alks-extended-trucks，最後瀏覽日期：113 年 4 月 9 日。

5、 Why is Driver Status Monitoring(DSM) System helpful to prevent fatigued driving? ICAR VISIONS，110 年 7 月 30 日，網址：https://www.icarvisions.com/ai/why-is-driver-status-monitoring-dsm-system-helpful-to-prevent-fatigued-driving-754.html，最後瀏覽日期：113 年 4 月 16 日。

6、 胡玉立，車主隱私堪憂 25 家車商全未通過保護個資最低標準，世界新聞網，112 年 9 月 6 日，網址：https://www.worldjournal.com/wj/story/121469/7422438，最後瀏覽日期：113 年 4 月 10 日。

7、 張艾琦，駕駛監控系統市場的成長因素與法律規範發展概況，科技發展觀測平台，110 年 6 月 15 日，網址：https://outlook.stpi.narl.org.tw/index/focus-news/4b114100791e3859017a0d81b517101f，最後瀏覽日期：113 年 4 月 9 日。

8、 張銘方，開車不要玩手機！「駕駛者監控系統」以影像辨識偵測分心駕駛行為,財團法人車輛研究測試中心,107 年 11 月 21 日,網址：https://pansci.asia/archives/134450，最後瀏覽日期：113 年 4 月 9 日。

9、 黃士育，你的車，其實是隱私殺手！25 家車商收集個資、部分還出賣，連性生活也掌握？數位時代，112 年 9 月 11 日，網址：https://www.bnext.com.tw/article/76639/mozilla-cars-data-privacy，最後瀏覽日期：113 年 4 月 10 日。

10、籃貫銘，駕駛注意力與生理狀態偵測系統，CTIMES，107 年 5 月 3 日，網址：https://www.ctimes.com.tw/DispArt/tw/ADAS/1805031041UM.shtml，最後瀏覽日期：113 年 4 月 10 日。

11、 蘇一峰，智慧座艙監控技術介紹，財團法人車輛研究測試中心，111 年 5 月 11 日，網址：https://www.artc.org.tw/tw/knowledge/articles/13648，最後瀏覽日期：113 年 4 月 11 日。

四、法院判決

1、 最高法院 100 年度台上字第 4780 號判決，司法院裁判書系統，100 年 8 月 31 日，網址：https://judgment.judicial.gov.tw/FJUD/default.aspx，最後瀏覽日期：113 年 4 月 10 日。

2、 臺灣高等法院高雄分院 105 年度上易字第 604 號刑事判決，司法院裁判書系統，106 年 1 月 18 日，網址：https://judgment.judicial.gov.tw/FJUD/data.aspx?ty=JD&id=KSHM%2c105%2c%e4%b8%8a%e6%98%93%2c604%2c20170118%2c1&ot=in，最後瀏覽日期：113 年 4 月 10 日。

附錄：「道路交通事故零死亡願景系列－駕駛隱私蒐集保護機制之研究」專題研究報告（初稿）座談會紀錄及參採情形

時間：113 年 4 月 24 日（星期三）下午 2 時 30 分

地點：立法院法制局 304 會議室

主席：黃組長良瑩　　紀錄：林鈺琪

參加人員：

一、學者專家：

世新大學法律學系　戴副教授豪君

二、法務部：

主任檢察官　劉怡婷

三、個人資料保護委員會籌備處：

科長　曾傑

視察　簡浩羽

四、本局出席人員：

陳研究員世超

楊副研究員盛旺

吳副研究員欣宜（書面）

發言要點：

世新大學法律學系戴副教授豪君：

一、車上蒐集個資的工具有很多，例如車載機，或是安裝其他的裝置，如行車記錄器，例如國外有一些重型卡車，在上車前要求駕駛需強制酒精偵測的外加裝置。所以在定性上處理的是不是只限於車子本身所載的裝置，不包含其他加裝的部分，應先釐清。

二、車子裡的監控會偵測到包括駕駛的特徵，例如眼神、聲音，而依我國個人資料保護法規定，生物特徵不屬於特種資料，這在全世界的立法上是很少見的。因此可能會有一個問題，就是屬於一般個人資

料的同意方式來處理。我國雖然對於同意沒有要求如歐盟 GDPR 須採用所謂的自主的同意，但是在解釋上面來說，同意基本上是必須回到一般的意思表示，所以在車輛上的同意，應是自主的同意。另，現在車載機最大的問題是駕駛同意的範圍是什麼，駕駛沒有被很清楚的告知資料是給車廠的，還是給車載機，還是給 google 系統，所以可能就像報告特別提到，車上裝置沒有提出一個消費者隱私保護的原則，這是可能必須要考慮的。

三、在網站上使用到個資時，會告知使用者通過哪些個資的隱私認證，車輛能不能也有一個自主的隱私認證的標準，如果車輛可以取得隱私認證的標章，就可以得知已達到一定程度的個資保護機制。

四、個資的後端利用也須做規範，因此，問題在於駕駛隱私會不會被做為後端的利用。對除蒐集的同意外，後端的利用也要做一些限制，也就是說，若駕駛監測目的是交通安全，則不可以再做其他的利用。

參採情形：

一、第一點意見，本報告於前言中指出，係針對非公務機關(汽車業者)就駕駛隱私蒐集可能涉及的問題及相關保護機制進行研究，原則上限於車子本身所載裝置。然而，有關蒐集、處理或利用駕駛狀態監測所記錄的有關駕駛之一切資訊，不論是車子本身所載的裝置，或是安裝其他的裝置，都可能會有侵犯個人隱私的疑慮。

二、其餘意見，均錄供參考。

法務部劉主任檢察官怡婷：

對立法院法制局「道路交通事故零死亡願景系列－駕駛隱私蒐集保護機制之研究」一文(下稱本報告)涉及刑法第 315 條之 1 妨害秘密罪構成要件之解釋，本部意見如下：

一、關於本報告引用臺灣高等法院高雄分院 105 年度上易字第 604 號判決相關論述，建請先釐清該判決是否適用於本報告討論議題

本報告第 8 頁以下關於第 2 段有關「車內的空間是屬於私人活

動領域？抑或是公開活動場所？」引用臺灣高等法院高雄分院 105 年度上易字第 604 號判決關於刑法第 315 條之 1 之法律見解，認為「車輛使用人行駛於道路或其他公共場域，固係處於同時間利用同一空間之他人可得共見共聞之狀態。惟他人之私密領域及個人資料自主，如在公共場域受到干擾，而超出可容忍之範圍，該干擾行為亦有加以限制之必要，俾有不受他人持續追蹤及侵擾之私人活動領域，而得保有『獨處之權利』」、「車輛在公共道路上之行跡，伴隨駕駛或乘員即時發生之活動行止，除明示放棄隱私期待之情形，通常可認其期待隱沒於道路上之往來車輛，不欲公開其個人行蹤。」固非無見。

然細繹該判決事實，係有關海巡署人員基於偵查案件目的，裝設 GPS 衛星定位器於某汽車上之行為，該 GPS 衛星定位器裝設於車體之外，主要係利用 GPS 衛星定位器回傳定位功能發送之電池紀錄，私下記錄追踪汽車之所在位置、移動方向及行蹤等資訊，似不具有監控「車內」駕駛及乘客表情、對話、手勢功能，從而，該判決亦僅謂該案中「車輛在公共道路上之行跡」具有合理隱私期待，似與本報告第 8 頁第 2 段論述「車內活動是否屬於私人活動領域抑或是公開活動場所」之法律見解無涉。因此，是否能夠如本報告第 3 段所述，藉由判決見解推認「從前述判決案例可以到可知，車內活動可能屬於非公開活動」，似有再予斟酌餘地。

二、刑法第 315 條之 1 尚以「無故」作為犯罪構成要件，建議宜並參酌實務見解論述藉由車內系統監控行車動態是否該當此構成要件

本報告有關於車內活動是否屬於非公開活動之論述，於第 8 頁第 3 段有主張「應視當事人的主觀意願以及客觀上的保密措施，若存在合理的隱私期待，則可以認定車內空間係屬於私人活動領域」，固值贊同。在法律見解及法制面上，有關：(一)在車主或駕駛已明示同意汽車業者蒐集該等資訊的時候，是否就可以認定個案不存在合理隱私期待？(二)透過車內系統監控駕駛人車內動態及行車動態是否該當「無效(即無正當理由)」之構成要件？(三)立法政策上，

我國若制定本報告第 10 頁有關「隱私影響評價機制」及要求建置本報告第 3 頁有關「車輛監控系統(DMS)」之法律規定，是否可能作為排除刑法第 315 條之 1 適用之基礎？均有重要法學討論價值，是否納入本報告研究範圍，亦建請斟酌。

參採情形：

一、第一點意見，本報告引述臺灣高等法院高雄分院 105 年度上易字第 604 號判決，藉由該判決說明理由：「刑法第 315 條之 1 所稱『非公開之活動』，通常指活動不對公眾公開而具有隱密性，亦即個人主觀上有『合理隱私期待』欲隱密進行其活動而不欲公開，且在客觀上所選擇之場所或所使用之設備亦足以確保活動之隱密性而言。……」係為說明車內空間是否應具備有隱私權保護之基本權利。針對報告可能引起誤解部分，爰酌修報告文字內容。

二、第二點意見，本報告係針對駕駛隱私蒐集可能涉及的問題及相關保護機制進行研究，主要側重於駕駛狀態監測可能對駕駛資訊隱私權的影響，以及如何就可能侵害駕駛隱私建立保護機制。報告提及刑法第 315 條之 1 妨害秘密罪，僅係闡明針對駕駛狀態監測可能違反的法律規定。有關法務部所提之法學討論部分，另做為未來研究方向參考，相關意見錄供參考。

個人資料保護委員會籌備處曾科長傑：

本籌備處為落實憲法法庭 111 年憲判字第 13 號判決要求，在判決宣示之日起 3 年內建立個人資料保護之獨立監督機制，首要任務係研擬並完成組織法之制定，以明定個人資料保護委員會(簡稱個資會)之職掌權限，俟個資會成立後，後續將啟動個資法通盤檢討。我國個資法是否建立 PIA 制度，將持續蒐集相關資料，並由未來之個資會參考歐盟之立法經驗、實務操作、我國國情及本報告所提供之建議進行通盤考量，並做出相對應調整。

歐盟 GDPR 第 22 條所定「自動化處理」(automated processing)之限

制，著重於對資料當事人產生法律效果或類似之重大影響之決策，與本報告所指稱情形似有不同。另針對人工智慧處理個人資料之自動化決策機制，未來個資會將多方參酌外國規範，廣納民間團體及產業界意見，在不過度抑制新興科技發展之下，據以推出適當指引以確保使用者之資訊隱私權。

參採情形：

為妥善控制、避免資料開放與大數據分析等可能對於資料當事人權益產生重大影響之資料蒐集、處理或利用行為，本報告建議參酌歐盟GDPR 第 35 條資料保護影響評估，於「事前」透過一定之評估程序與機制，確保相關資料利用行為對於資料當事人權益不至造成侵害。其餘意見錄供參考。

陳研究員世超：

有關報告所提駕駛狀態監測系統主要係以車艙內感測器監測駕駛狀態，例如接收攝影機並輔以相關感測元件，擷取車艙內駕駛人臉影像資訊，透過影像處理技術偵測駕駛面部特徵位置，並結合駕駛行為模型，估計駕駛者行駛行為特徵，判斷駕駛者開車之專注力。當系統判定為異常行為發生時，如分心駕駛或手機通話等異常行為發生時，透過警示機制提醒駕駛人，此確有助於保障駕駛人與其他用路人安全，惟此亦衍生數位科技的運用是否會侵犯個人隱私問題。

因而為強化個人隱私之保障，報告認為應建立以資訊系統收集、處理個資檔案前，對當事人隱私權等權益可能造成影響之「隱私影響評價」，並檢視該資訊系統在技術上，是否為對個人權利影響最低限度之設計。此制度之理論依據與環境影響評估類似，因為個資一旦依資訊系統處理成為檔案而利用，在網路上流出後，將難以救濟；故在損害或風險未發生前，應先對系統設計、運用計畫及安全維護措施等事項進行評價，判斷是否能確保個人權利及適當、合法進行個資之處理。

因此，報告建議未來除了參酌國外規範檢討相關規定，並廣納公民

團體意見、衡量產業需求，以求取隱私與技術發展的平衡，個人敬表贊同。

參採情形：

贊同本報告內容，錄供參考。

楊副研究員盛旺：

一、本報告貳、問題研析與建議多次提及「駕駛狀態監測」(Driver State Monitoring,DSM)，並於本報告(第 3 頁)(二)國外規範「DMS 市場成長快速有很大的因素是各國及各經濟體法令強制要求，……」提及歐盟 Euro NCAP 及美國的 DMS 相關規範，有關「駕駛狀態監測」(DSM)和前開及壹、前言所提「駕駛監控系統」(Driver Monitoring System,DMS)是否為相同的概念或二者另有功能包含之關係，建請先予釐清，併請參酌。

二、本報告(第 4 頁至第 5 頁)(三)我國規範敘及我國現行交通法規針對分心駕駛、疲勞駕駛之相關處罰規定。按行政院 107 年 10 月間核定臺灣新車安全評等計畫，推動臺灣新車安全評價制度(Taiwan-New Car Assessment Program,T-NCAP)，由政府編列經費建置相關制度規章、安全檢測能量，及購置車輛辦理初步運作測試評價，除可提供消費者車輛安全資訊作為購車參考，亦有助透過市場機制帶動車廠提升車輛安全性，促進臺灣汽車產業發展，本報告前開所提(三)我國規範有否補充 T-NCAP 部分之必要，建請衡酌報告內容之相關性再予考量，併請參酌。

參採情形：

一、第一點意見，根據監控類型，駕駛監控系統分為駕駛狀態監控和駕駛健康監控，主要是在降低受傷機率、預防事故並減輕碰撞的影響，以減少事故的發生[56]。

[56] KBV Research，駕駛員監控系統全球市場規模、份額、行業趨勢分析報告：按車輛推進方式、銷售渠道、組件、監控類型、車輛類型、區域展望和預測，2023-2029 年，Global Information，2023 年 4 月 28 日，網址：

二、第二點意見，臺灣新車安全評等制度（Taiwan New Car Assessment Program, TNCAP）係指由獨立第三方車輛專業機構購買市售車輛，再將該車輛送至檢測機構進行試驗，最後將試驗數據等結果轉換成民眾可理解星級評等，並將其公開揭露供民眾參考。TNCAP 旨在提供消費者公開完整車輛安全資訊，導引民眾購買安全性較高的車輛，同時促進各車廠間產生良性競爭、開發更發安全的主、被動配備，使消費者有更多安全的車輛可選擇，進一步降低道路意外事故傷亡率，進而減少社會成本的付出[57]。此與本報告針對駕駛狀態監控的規範似較不相關，爰錄供參考。

吳副研究員欣宜（書面）：

隨著車聯網之發展，物聯網及智慧型手機等諸多連結設備成為汽車標配之一環，使得有關個人數據之蒐集、使用、儲存皆暴露在公開網路環境中，受攻擊面因而大增，如何保護資料不被擷取、竄改進而影響駕駛人之安全與權益，成為刻不容緩之問題。國際標準組織（ISO）與汽車工程師協會（SAE）針對汽車網路安全，已於 2021 年 8 月 31 日正式發布 ISO/SAE 21434 標準，該標準係著眼於影響駕駛安全性層面之網路安全，其規範從開發、製造、運作、維修到回收等整個車輛完整生命週期所應遵循之安全設計流程，並涵蓋車輛中所有電子元件、軟體以及整個供應鏈。

另一方面，在車輛大量配置攝影鏡頭等感測器之趨勢下，當今汽車所蒐集之資訊將大範圍地揭露使用者之日常生活，甚至是身體狀況，從而可建構出特定使用者之特徵。在個人資料保護及隱私權意識抬頭年代，越來越多人開始注重及保護個人隱私，對此，本報告注意到駕駛人個資與隱私外漏之隱憂已成為不可迴避之議題，以及現有個人資料保護

---

https://www.gii.tw/report/kbv1276841-global-driver-monitoring-systems-market-size-share.html，最後瀏覽日期：2024 年 4 月 25 日。

[57] 認識 TNCAP，TNCAP，網址：https://www.tncap.org.tw/Message/SingleImage?catalogId=567b3509-2d18-447f-b240-3a6e52a2d10a，最後瀏覽日期：2024 年 4 月 25 日。

法制是否足以面對科技發展日新月異之挑戰等問題，殊值肯定。

參採情形：

肯認本報告內容，錄供參考。

散會：下午 3 時 21 分