

國立政治大學法律學系碩士班

碩士學位論文

論刑事審判卷證中個人資料之使用與保護
—以法院權限為中心

The Use and Protection of Personal Data in Criminal Trial

Dossiers: Focusing on the Authority of Court

指導教授：何賴傑 博士

研究生：蔡易融 撰

中華民國 一 一 一 年 六 月

謝辭

撰寫論文時，文章中的主詞往往是「本文」或「本章」、「本節」等等，我想像著這些字句是這篇初試啼聲的論文所欲傳達的話。現在，在寫作時序的最後，也在這篇論文的最前，輪到「我」直接發聲，向曾給予這篇論文成長與養分的所有人事物，謹致上這篇謝辭。

論文得以順利完成，我首要感謝恩師何賴傑教授。在研究所的討論課中，何老師總鼓勵同學們從報告發展想法，將問題問清楚、將論點說完整，而當我欲將報告內容擴展成論文，卻在浩繁的文獻中迷失方向時，何老師也直指出我應討論的核心，讓原本見樹不見林的我，能見到問題的全景。何老師在每次討論中耐心傾聽我尚未成熟的想法，而後給予我的適切引導，總能點醒我尚未考慮到的面向，諄諄善誘的風範更令我十分景仰。在政大上課時，無論是研究所、大學部的課程，或是研討會的發表與提問，何老師的講述與切入點，每每讓我對刑事訴訟法規能有更深的理解，而令我心悅誠服。

我也特別感謝兩位口試委員，楊雲驊教授與王士帆教授。楊老師在口試時給予我的建議由廣入深，使我得以一窺學術的堂奧，而老師的德文課程也是同學們得以通往更廣博學術世界的首站。王老師則就論文的細節給予我建議，使我體會到唯有更加嚴謹與細心，才能使研究經得起考驗。

就讀政大法研期間，刑法組上有開課的老師們，我也都修習過一輪這些課程。謝謝李聖傑教授、謝如媛教授及陳志輝教授，各位教授的教導也給予我形塑研究過程中的重要養分，謝謝您們。

謝謝何門學長姊與同學們，謝謝盈孜學姊在我碩一時的寶貴建議，宜峻學長在助教經驗與研究所生涯的重要經驗傳承，以及律翔學長在我口試時的協助，我還要謝謝同學子儒，在修課與助教職務上的珍貴討論與支援，尤其在疫情之中，仍然安穩度過每個關卡。與晉嘉學長、雯婷學姊的討論，也使我獲益良多。

謝謝同學們在碩士生活中的相互支持，謝謝科榕、瓊文、俊威、詠儀、馨尹、

文馨、景謙等同學，在課業上的切磋、研究上的討論，以及日常中的揪團，祝大家都能去到自己想去的地方，並且天天都能喝到想喝的飲料。

雖然在政大法研的兩年，恰好也是疫情最嚴峻的時候，學期中往往要歷經實體、遠距及二者交錯的修課方式，但回想起這兩年，之中的不便漸已淡忘，記得的多是沉澱的知識與討論的火花。謝謝我在碩士生涯中遇到的每個人，你們或多或少都給予我某種程度上的幫助，我感謝緣分。

謝謝女友施晴媛，我知道你一直在等待我，現在這個階段終於告一段落，我厚臉皮地邀請你在往後很多階段，一起相互扶持。謝謝 Oreó，你是我第一隻認識的小狗，雖然你常常瞪我，但你的可愛也支撐了我。

謝謝父母仍然給予我經濟上的支持，以及自由任性發揮的空間，使我能無後顧之憂地完成學業與這篇論文。



摘要

已確定刑事案件卷證資料，包含訴訟關係人之特徵，甚或醫療、基因、性生活及犯罪前科等資料，而屬於一般性與敏感性個人資料。經由司法系統之偵查、審理程序，這些個人資料經過系統性處理，而具有易於與其他案件卷證中資料連結的特性，而屬於個人資料檔案。這些資料本身足以識別特定自然人，與其他資料結合後，甚至可能勾勒出資料當事人的生活圖像，是故使用該等個資之行為將對其個人資訊自決權造成干預。

本文以刑事法院為觀察重點，整理法院等司法機關使用已確定案件卷證中個資的行為，並進行分類，發現法院的使用行為往往欠缺適當的授權規範。就整體法律體系而言，關於刑事卷證中資料的規範，應以刑事訴訟法為特別法，以個人資料保護法、法院組織法、政府資訊公開法等作為普通法。然而現行刑事訴訟法對於該等資料使用幾無規範，普通法位階之一般性規範則較寬泛，而留下過多解釋空間。

本文觀察到此問題，並比較歐盟一般性資料保護規範(GDPR)、EU Directive 2016/680，以及德國刑事訴訟法、聯邦資料保護法、法院組織法施行法等相關條文後提出解決方案：在現行法下，司法機關得在其使用個資之決定中加入資料保護影響評估(DPIA)之架構，以符合個資保護之透明性原則，亦有助於事後司法審查；在立法構想上，則得以德國刑事訴訟法第八編為借鏡，考慮於我國刑事訴訟法增訂第十編，令刑事卷證使用得以依循明確的特別授權規範，並加入配套保護措施，使個資保護法律體系更加完備。

關鍵字：卷證資料，個人資料，刑事訴訟法，個人資料保護法，司法行政，GDPR，EU Directive 2016/680，DPIA，德國聯邦資料保護法

目錄

目錄.....	I
第一章 緒論.....	1
第一節 問題意識.....	1
第二節 研究方法.....	4
第一項 文獻回顧與歸納.....	4
第二項 比較法.....	4
第三項 政策評估.....	5
第三節 研究範圍與用語說明.....	6
第一項 研究範圍.....	6
第二項 法院角色之說明.....	6
第三項 卷證資料、案卷與卷宗之區別.....	7
第四項 查閱、閱覽與閱卷之區別.....	8
第五項 資料與資訊之區別.....	10
第二章 個人資訊自主權與個資保護理論.....	11
第一節 資訊隱私權與個人資訊自主權的關係.....	11
第一項 德國資訊自決權之濫觴：1983年人口普查法判決.....	12
第二項 歐盟法上之發展.....	13
第一款 歐洲人權法院判決.....	14
第二款 歐盟基本權利憲章.....	16
第三款 學說上之演進.....	18
第三項 我國法上之發展.....	20
第一款 釋憲實務上的發展.....	20
第二款 學說上的發展.....	21
第一目 資訊自決權之獨立基本權地位.....	22

第二目 資訊隱私權與資訊自決權之關係.....	22
第三目 本文見解.....	23
第二節 個人資料的定義與其使用行為之要求.....	23
第一項 個資法的保障範圍.....	24
第一款 直接或間接識別/去識別化	25
第二款 一般性個資/敏感性個資	29
第三款 後設資料.....	29
第四款 個人資料檔案.....	30
第二項 目的拘束原則.....	32
第三項 資料最小化原則.....	35
第四項 透明性原則.....	36
第三節 卷證中的個人資料及其使用規範要求.....	37
第一項 卷證中包含個人資料.....	37
第二項 卷證屬於個人資料檔案.....	38
第三項 現行法就卷證或個人資料檔案並無特殊使用規範.....	40
第三章 法院使用卷證中個人資料之行為.....	42
第一節 基於審判目的使用.....	43
第一項 審判中閱覽卷證之准許.....	43
第一款 閱覽卷證之人：被告、辯護人、程序中與程序外之第三人	43
第二款 閱覽卷證之方式：查閱卷證與提供答覆.....	45
第二項 法庭錄音錄影公開與否之決定.....	46
第三項 卷證資料之移交.....	49
第二節 審判目的外使用.....	50
第一項 新的基本權干預與其正當化基礎.....	51
第二項 另案審判使用.....	53

第一款 使用另案卷證資料.....	54
第二款 使用非刑事目的蒐集之資料：以簡訊實聯制位置資料為例	56
第三項 司法行政使用.....	58
第一款 裁判書公開.....	59
第一目 裁判書公開之制度目的.....	59
第二目 裁判書公開之個資保護：以當事人全名為中心.....	60
第二款 第三人查閱卷證資料.....	62
第一目 所適用之法律.....	63
第二目 第三人查閱卷證資料的類型化.....	66
第三目 學術研究使用.....	67
第四項 已確定案件之卷證中個資之使用與保護.....	69
第一款 論題聚焦.....	69
第二款 法院對已確定案件卷證之角色.....	70
第三款 卷證之範圍.....	71
第四款 卷證資料公開與個資保護.....	72
第一目 卷宗公開之方式.....	72
第二目 證物公開之方式.....	73
第五項 資料當事人之告知後同意.....	74
第一款 告知後同意的意義與適用範圍.....	74
第二款 告知後同意的合法性要件.....	77
第一目 出於自由意志(freely given).....	78
第二目 針對具體特定目的(specific)	80
第三目 受充分告知(informed)	82
第四目 清楚的同意行為(unambiguous indication of wishes) ..	84
第三款 現行告知後同意制度的不足之處.....	85

第三節 小結：授權規範的缺乏.....	86
第四章 卷證中個人資料保護之比較法制探討：以歐盟及德國為對象.....	90
第一節 歐盟法制之發展.....	90
第一項 GDPR 與 2016/680 指令之適用範圍.....	90
第二項 個資保護之其他具體措施.....	91
第二節 德國刑事訴訟法上相關規定.....	93
第一項 刑事程序法與個資保護要求.....	94
第二項 目的外使用行為之依據.....	95
第一款 一般性授權規範.....	96
第二款 個別情形之授權規範.....	99
第一目 對私人及其他機構提供卷證資料.....	99
第二目 為學術研究目的提供卷證資料.....	101
第三款 一般性之限制.....	102
第三項 其他資料使用規則.....	104
第一款 資料使用規則.....	104
第二款 對受干預之資料當事人之義務.....	107
第四項 救濟途徑與法院之審核.....	109
第一款 刑事訴訟法中之救濟.....	109
第二款 法院組織法施行法之救濟.....	110
第五項 小結：卷證中個資保護的基本體系.....	112
第五章 對現行實務之建議及立法構想.....	114
第一節 現行法欠缺及應補足之規範.....	114
第二節 建立事前評估及事後審核機制.....	115
第一項 事前評估之建立.....	116
第一款 資料保護影響評估制度(DPIA)制度介紹.....	116
第一目 歐盟法上之 DPIA 制度.....	116

第二目 德國法上之 DPIA 制度	118
第二款 我國相似制度.....	119
第一目 個資法施行細則第 12 條第 2 項第 3 款個人資料之風險 評估及管理機制.....	119
第二目 於司法機關之裁量中加入 DPIA	119
第二項 法院之事後審查.....	119
第一款 個資使用之事後審查是否應受外部監管.....	119
第二款 事後審查之內容.....	120
第三節 立法建議.....	121
第一項 已確定案件卷證中個資之使用規範.....	121
第二項 對於資料當事人之義務：以告知義務為例.....	122
第三項 救濟程序.....	122
第四項 立法構想之提出.....	123
第六章 結論.....	125
參考文獻.....	129

第一章 緒論

第一節 問題意識

因應 COVID-19 疫情，行政院推行「1922 簡訊實聯制」政策，以便有效掌握大眾行跡，阻斷病毒傳播。然而，日前卻有法官撰文指出¹，目的原為疫情調查之簡訊實聯制資料，竟有警察機關將其作為調查犯罪嫌疑人行蹤的方法，已屬目的外使用該等資料，消息一出遂引起熱烈討論²。司法院亦迅速回應，表示法院調取通聯記錄時，是否涵蓋該等簡訊資料，屬審判獨立範圍，不宜表示意見³。簡訊實聯制資料顯示手機門號持有者之行蹤，得以識別該個人，因此亦屬個人資料⁴。若法院果真依職權調查此類資料，將超出行政機關原先蒐集的目的。刑事司法機關使用個資之行為應否受限制，又如何可能與個資保護調和，即為本文問題意識的起點；而當這些個資進入刑事程序，成為卷證資料後，在法制面上應如何使用與保護，即為本文欲處理的問題。

在刑事審判的卷證中，常常包含大量個人資料，舉凡個人資料處理法(下稱「個資法」)第 2 條第 1 款中所例示之「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」等，常被用於確認當事人身分、認定犯罪

¹ 張淵森 (2021 年 6 月 19 日)，我必須成為吹哨者：「簡訊實聯制」資訊遭利用，指揮中心請儘速反應，聯合新聞網，取自 <https://opinion.udn.com/opinion/story/120701/5542571> (最後瀏覽日：2022 年 6 月 16 日)。

² 李榮耕 (2021 年 6 月 20 日)，警察，我在這裡一簡訊實聯制的法律依據何在？，風傳媒，取自 <https://www.storm.mg/article/3770196> (最後瀏覽日：2022 年 6 月 16 日)；吳忻穎 (2021 年 6 月 21 日)，法官吹哨「簡訊實聯制」遭不當利用，問題在於台灣防疫蒼白的法制面，聯合新聞網，取自 <https://opinion.udn.com/opinion/story/12626/5547273> (最後瀏覽日：2022 年 6 月 16 日)。

³ 劉世怡 (2021 年 6 月 24 日)，實聯制簡訊遭誤解用於辦案 法務部：研議修法保障個資，中央社，取自 <https://www.cna.com.tw/news/asoc/202106240357.aspx> (最後瀏覽日：2022 年 6 月 16 日)。

⁴ 行蹤資料至少符合個人資料處理法第 2 條第 1 款中「得以間接方式識別」之個資，依個人資料保護法施行細則第 3 條規定，「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。」

事實、量刑與保安處分之決定及宣告沒收，貫穿整個刑事程序，足見個資具有不可或缺的地位。

這些個資的來源，可能是偵審機關以強制處分或其他偵查手段取證而來，亦可能為行政機關或私人非基於刑事目的所蒐集之資料，而後用於刑事程序中；在案件終結後，這些涉及個資的卷證資料如何被儲存、甚或再進一步被利用，現行刑事訴訟法上並無相關規定。本文認為，刑事卷證有其特殊性，往往涉及「敏感性個資」，本需較高密度保護⁵，至於卷證中其他資料是否屬於個資而受保護，宜以歐盟個資工作小組提出之資料關聯性(relating to)為判準，只要資料之內容、使用之目的、取得該資料之結果，任一要素得連結至個人，即屬於本文所欲保護的個資，以擴大保護範圍⁶；而在法規適用方面，個資保護措施原則上適用個資法規定，而刑事訴訟法此時作為特別法，但即使已滿足刑事訴訟之基本原則，當涉及個人資料蒐集時，仍有應特別遵守之規範，如目的拘束原則即為必須遵守之重要原則⁷。在現行特別規定欠缺的情況下，應暫先回歸原則，並修法填補法律漏洞。從個資保護的觀點而言，個資的蒐集、處理與利用往往涉及個人資料自主控制權之干預，須以目的拘束原則加以調和，亦即必須合乎授權規範的目的，方為合法；若要進行目的外使用，則構成另外一種干預，亦須符合法律有規範的干預正當化事由⁸。

在本文研究的鋪排架構上，首先說明個人資訊自主權的發展歷程，以及卷證資料中涉及何種個資，接著說明法院使用個資的行為態樣，包含基於審判目的及審判目的外使用，以及經資料當事人同意之情形，再說明比較法上歐盟與德國法

⁵ 依個資法第 6 條第 1 項，敏感性個資乃「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」，原則上不得蒐集、處理或利用，僅在有法定特殊事由時方得為之。刑事卷證中依案情不同，時常涉及上開列舉的個資。

⁶ 張陳弘，個人資料之認定—個人資料保護法適用之啟動閥，法令月刊，第 67 卷，第 5 期，2016 年 5 月，頁 73-74。

⁷ 洪家殷，公務機關資料之蒐集與個人資料之保護，東吳法律學報，第 30 卷，第 4 期，2019 年 4 月，頁 54；李惠宗，個人資料保護法上的帝王條款—目的拘束原則，法令月刊，第 64 卷，第 1 期，2013 年 1 月，頁 49。

⁸ 林鈺雄，刑事程序中的個資保護—德國刑事訴訟法第 8 編 (§§ 474-499 StPO) 逐條釋義，刑事政策與犯罪研究論文集 (22)，2020 年 10 月，頁 206。

制有何規範可供借鑑，接著提出本文論點，論述現行刑事訴訟法欠缺個資保護的相關規範，應將個資保護之原則、法院使用個資的行為規範、有接觸卷證必要之人的個別閱卷規範等納入修法範圍，並考慮建立資料保護風險評估制度以供法院參酌，在修法前法院使用含有個資的卷證資料，則應注意個資法上的原則要求，最後則提出結論。總言之，本文欲以法院為中心，探討刑事審判卷證中之個人資料之使用與保護，其間權衡與互動關係。本文區分刑事審判中法院使用個資情形，分為「基於審判目的使用」與「審判目的外使用」二者，分別說明。

在第一種「基於審判目的使用」情形，本文再區分為「審判中閱覽卷證之准許」、「法庭錄音錄影公開與否之決定」與「卷證資料之傳輸」等情形，分別涉及法院將卷證資料透露給訴訟關係人或其他法院，透露方式可能為付與書面卷證或影音檔案，本文將討論其中差異及對個人資料的影響。

在第二種「審判目的外使用」情形，本文認為其屬於獨立的基本權干預，需有另一法律授權基礎，且應就該行為另為審查新舊目的間是否具備相容性，尤其應注意「敏感性個資」的使用需要較高程度保護。本文在此就法院「另案審判使用」與「司法行政使用」之行為，將再分別說明。基於另案審判使用行為，將討論法院依職權調查非為追訴本案犯罪而蒐集之資料，是否適法；至於司法行政使用行為，法院居於司法行政機關之地位時，就無涉審判權運作的事務，法院應遵循公務機關間資料傳輸的相關一般性規範，其處理及利用資料的行為將更全面地適用個資保護原則。典型的司法行政行為，例如法院作成裁判書並公開，本文在此部分針對「裁判書公開」的相關爭議，討論其制度目的，以及公開之方式、範圍與個資保護的衝突。本文亦將討論「第三人查閱卷證資料」，說明第三人接近使用卷證資料之事由應為類型化之規範，並舉學術研究使用為例，說明現行規範不足之處。

本文亦將考察「資料當事人之告知後同意」在法院使用資料的情形得否與如何解釋運用。除了法定正當化事由外，當事人之告知後同意亦可作為目的外使用個資行為的正當化基礎，惟法院使用個資行為，是否容許以當事人同意作為正當

化基礎，則產生告知後同意制度與法院進行刑事審判或司法行政目的如何嵌合的疑問，本文將嘗試於此釐清。

第二節 研究方法

第一項 文獻回顧與歸納

目前台灣刑事法領域及公法領域學者對於隱私權於大法官解釋中之發展過程、隱私權的內涵與干預態樣、干預的限制等議題，著述頗豐，本文擬就這些重要文獻進行整理與回顧，說明個人資料自主權與隱私權間的關係，發展本文觀點。此外，本文將整理刑事審判中卷證的使用情境與規範，說明其中所含有的個人資料如何被使用與保護，並由此切入主題。

第二項 比較法

本文主要以歐盟一般性資料保護規範(EU 2016/679 Regulations ; General Data Protection Regulations , GDPR) 、 EU 2016/680 Directive (下稱「2016/680 指令」) 等歐盟法上準則⁹，以及德國法作為比較對象。

歐盟通過之規範與指令，對其會員國之法制發展有相當大的引導作用。各會員國均須在一定期限內立法或修法，以不小於歐盟指令要求的程度將其內國法化；而歐盟規範更具有強制性，在各會員國之領土內有同於法律位階的地位。歐盟於2016 年同時通過 GDPR 與 2016/680 指令，將牽涉民事與行政法範疇之個資保護

⁹ 其全名為「2016 年 4 月 27 日歐洲議會與歐盟理事會第 2016/680 號指令，關於主管機關為保護與刑事犯罪之預防、調查、偵查或追訴或刑罰執行而處理個人資料有關之自然人，以及關於此類資料的自由傳輸，並廢除歐盟刑事警察與司法個資保護互助架構 2008/977/JHA。」(DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA)另有學者譯為「歐盟領域內會員國跨境檢警合作打擊犯罪及個資保護的警察與犯罪指令」，參考翁逸泓，資訊委員的時代角色——以 GDPR 及英國 2018 年資料保護法為中心，月旦法學雜誌，第 286 期，2019 年 3 月，頁 34。另外，關於歐盟法上規範(regulation)與指令(directive)之關係，可參王玉葉，歐洲聯盟法研究，元照，2015 年，頁 9。

由 GDPR 處理，設置直接法律效果，對個人的保護較全面；將牽涉犯罪預防、調查、偵查及追訴等執法方面的個資保護交由各會員國自行以內國法規範，而以 2016/680 指令處理，則為尊重各國主權。我國個資法立法時參考此二號規範與指令之前身，歐盟 1995 年資料保護指令為主要對象之一，然而歐盟法制更新頻仍，我國個資法目前最近一次修法是 2015 年，對於歐盟最新的法制要求尚不見回應，而我國刑事訴訟法更是幾乎欠缺個資保護主題的規範，故本文以歐盟規範與指令為比較法借鏡對象。

德國聯邦憲法法院於 1983 年之「人口普查法」判決中，即已從德國基本法中之一般人格權及人性尊嚴，推導出國家不得無限制地取得與使用個人資料，確立了人民享有就其個人資料之自主權利¹⁰。本文在引介個人資料自主權時，擬參考德國法的發展作論述。德國刑事訴訟法第 8 編設有個人資料的保護與使用之四章規範，說明刑事程序中的個資保護有何要求，為我國法所無，故本文欲引為參考對象，與我國刑事程序中的個資使用現狀比較，並提出立法建議。

第三項 政策評估

本文透過觀察我國、歐盟與德國之制度，說明法院使用個資時應受何種限制。個人資料自主權固然需要受保障，但並非絕對不可限制，僅在限制時需有干預正當化事由，作為合法性要件，方不至逾越憲法要求。本文除就基本權干預框架進行論理外，亦將一併說明其配套措施，包含具體上限制個資使用的手段，如進行一定程度匿名處理，明定使用範圍與違反之法律效果，以及參考 GDPR 第 35 條、2016/680 指令第 27 條以下之資料保護影響評估制度，使法院為一定之個資使用行為前，需先就特定事項進行審酌，並讓該個資當事人得以知悉，以兼顧透明性要求。

¹⁰ 此裁判之中文譯介，參考蕭文生，「一九八三年人口普查案」判決－德國聯邦憲法法院裁判選集（一），司法院，1991 年 5 月。

第三節 研究範圍與用語說明

第一項 研究範圍

從偵查機關蒐集、統整證據、製作書類，到法院以卷證內容進行審判程序、納為裁判基礎，刑事案件卷證的形成可謂反映了該案件的歷程；所有訴訟關係人、訴訟參與者的活動，共同構成了卷證，也因此偵查與審判機關均會使用卷證中蘊含的個資，也對這些資料當事人造成了干預。其中，法院乃最終決定是否與如何採擇與使用卷證內容者，而我國現行刑事訴訟法制又以卷證為審判依據，是故本文欲以法院權限切入，勾勒出刑事程序中個人資料使用的樣貌及其隱含的問題。

本文所欲研究的主題如下：

1. 法院於刑事審判中的個資蒐集、處理與利用行為，有無正當化基礎？其內涵為何？
2. 法律對此等行為有無明文授權規範？現行規範是否屬之？
3. 法院可否或如何取得個資當事人的告知後同意，作為法院使用個資的正當化基礎？
4. 是否應建立法院接收或傳輸個資時，對於個資自主控制干預的評估制度？

為了回答這些問題，本文將先統一說明論述中的用語。

第二項 法院角色之說明

本文討論法院使用個資的行為態樣時，將區分法院作為審判機關與司法行政機關的不同角色，以說明其行為須受到的不同程度要求。

法院作為審判機關，依刑事訴訟法第 1 條，其任務在於追訴與處罰犯罪，其行使審判權之地位受憲法層次之法官保留原則保障，但在與追訴、處罰犯罪等行

使審判權無關的事項上，即居為司法行政機關的地位¹¹。法院審判因受憲法層次之審判獨立原則保障，故法院在審判中對於卷證中個人資料之使用行為，屬於司法行為¹²，原則上並不直接受行政法規拘束，而須符合刑事訴訟法之要求¹³。有論者進一步指出，區分法院作為司法行政機關的行為，目的是為了劃分審判權的歸屬與應適用何種救濟途徑，在德國法上，若法院行為屬於「司法行政處分」，則因事務相近性與避免審判分歧等目的，而由普通法院審理之¹⁴。

法院依其行為區分為司法行為或司法行政處分，二者間界線如何劃分，較直覺的區分方式是，法院於審判程序中的行為屬司法行為，而審判程序後的行為屬司法行政行為。然而，法院在審判程序外的行為，亦可能屬於司法行為而屬審判獨立保障範圍，如決定是否交付法庭錄音錄影；或屬於司法行政行為，如公開裁判書與准許第三人查閱卷證等¹⁵。有論者整理德國見解認為，若法院行為乃源自個別作用法之授權，受行政科層拘束，而非來自刑事訴訟法，不受審判獨立保障，則法院乃居於「行政機關」地位從事高權行政行為¹⁶。例如法院決定是否提供第三人閱覽刑事卷證資料，需另受政府資訊公開法或個資法拘束，與本案被告的訴訟權利無直接相關，即為適例¹⁷。

第三項 卷證資料、案卷與卷宗之區別

法院使用於審判程序的資料，依不同的脈絡，有以「卷證資料」、「案卷」、「卷

¹¹ 李建良，訴訟程序與起訴要件（中），月旦法學教室，189期，2018年7月，頁36-37。

¹² 就法院而言，司法行為指的是法官受憲法賦予之審判獨立保障而行使職權行為，包含刑事審判與基於法官保留而由法官所為之強制處分，其救濟僅能在原司法審級救濟中為之。詳細說明參考梁哲瑋，「司法行政處分」概念與其救濟實務之探討，105年度第2次行政訴訟實務研討會實錄，最高行政法院，2017年12月，頁311-312。

¹³ 依個資法第2條第7款，公務機關乃「依法行使公權力之中央或地方機關或行政法人」，是否包含具審判獨立性之法院，參見本文第三章第二節第一項之說明。

¹⁴ 所謂「事務相近性」乃是考量刑事法院對刑事審判本具備較嫻熟的法律知識與專業經驗；「避免審判分歧」則是維持相近事務之救濟途徑單一，避免由行政法院審理造成審判權衝突。詳細說明參考梁哲瑋，註12文，頁294-295。

¹⁵ 整理參見高愈杰，「司法行政處分」概念與其救濟實務之探討 與談(三)，105年度第2次行政訴訟實務研討會實錄，最高行政法院，2017年12月，頁441-442。

¹⁶ 梁哲瑋，註12文，頁301。參見本文第四章第二節第四項第二款之說明。

¹⁷ 梁哲瑋，註12文，頁301-302。

宗」或逕以「檔案」稱之，四者背後的概念是否相同，有釐清的必要。

在行政實定法上，有論者整理「卷宗」與「檔案」，認為卷宗乃經一定處理程序後產生之文字或非文字資料及其附件，凡得以現代科學技術理解之任何資訊均屬之，不以自然人之五感可理解之有形者為限；檔案則為經一定管理程序而歸檔之卷宗¹⁸。惟個資法第 2 條第 2 款所稱「個人資料檔案」，乃「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」，注重於個人資料經整理後得增益其利用的層面，與行政管理之「檔案」仍有不同。

在德國刑事訴訟法領域，「案卷」(Akten)指的是所有經由調查程序所得，用以追訴犯罪、對抗被告之資料¹⁹。在我國，相同概念有同以案卷稱之²⁰，實務上亦有以「卷宗」、「卷證」或「卷證資料」稱之。本文以為，稱「卷宗」者指的是經過整理的該檔案本身，而「卷證」、「卷證資料」或為卷宗與證物的合稱，意義上較為強調卷內資料的內容，但有時亦相互混用，並未特別代表相異的內涵。本文為求統一，行文以「卷證」為主，以指稱卷宗與證物，但在法條文字用語等不同脈絡下之說明，亦可能使用其他上述名稱。

第四項 查閱、閱覽與閱卷之區別

不同的訴訟參與主體，甚或訴訟外之第三人或行政機關，在刑事訴訟法、個資法、政府資訊公開法、檔案法等法律明文規範下，得以向法院或主管機關申請接近使用卷證，然而依照主體或其目的之不同，接觸卷證的方式、接觸內容之範圍也有所差異。在刑事訴訟法中，能最大程度接觸卷證者，除法院與檢察機關外，當屬行使閱卷權之辯護人，依該法第 33 條、第 33 條之 1，辯護人得檢閱全部卷證、抄錄及攝影。而被告接觸卷證之權利，經釋字第 762 號解釋，稱為「卷證資訊獲知權」，其得接觸的內容亦為被訴案件之卷宗及證物全部內容，惟考量被告

¹⁸ 林素鳳，卷宗閱覽之請求與救濟，月旦法學教室，89 期，2010 年 2 月，頁 12-13。

¹⁹ Gunter Warg, Der Begriff der Akte und ihre Vorlage im Strafverfahren, NJW 2015, 3195 (3196-3197).

²⁰ 林鈺雄，註 8 文。惟該文在說明以電子方式儲存之卷證時，又以「電子卷證」、「電子案卷」交互稱之，而觀其原文皆為「Akten」，似無嚴格區別。

與卷證原本間的直接利害關係，其行使方式則以付與影本為原則，與辯護人得接觸原本有所不同²¹。再者如審判中犯罪被害人接觸卷證之權利，原則上由其訴訟代理人檢閱全部卷證、抄錄及攝影，而該代理人無律師資格或無代理人之情形，才例外付與被害人影本²²。不同訴訟參與主體得以接觸卷證的方式、範圍均有不同，然一般認為，若由辯護人或訴訟代理人行使者，以「閱卷權」稱之；若由被告或被害人等與本案有直接利害關係者行使，則以「卷證資訊獲知權」稱之。

就用語上的區分，我國刑事訴訟法之文字描述之「檢閱、抄錄、重製、攝影、請求付與卷證影本」等，均為取得資訊之具體方式。而就法院角度而言，法院如何使訴訟參與主體或訴訟外第三人取得資訊，有論者以德國之資訊自由法 (Informationsfreiheitsgesetz; IFG) 規範之三種方式區分，而為更細緻之說明²³：第一種係「答覆」(Auskünfte)，指法院以口頭、書面或電子方式給予官方資訊內容再現之告知；第二種係「閱卷」(Akteneinsicht)，指申請閱覽官方資訊，不以原本為限，付與申請人影本亦屬之；第三種係「其他資訊接近使用」(Informationszugang in sonstiger Weise)，為概括之概念，除上述兩種形式外，其他得以近用政府資訊之方式屬之。

在德國刑事訴訟法上，亦以「提供答覆」與「查閱案卷」區分是否直接接觸卷證的程度²⁴。提供答覆只由卷證內容中整理資訊，不會接觸到卷證原本或影本；查閱案卷即為閱卷，得以接觸卷證原本或影本。文獻上稱接觸卷證的行為為「查閱」、「閱覽」或「閱卷」等，綜上可知，「閱卷」乃指一種特別的接觸卷證方式，與「提供答覆」有別，「查閱」則是由查閱案卷而來，「閱覽」則非法條用語。本文依此區分，就法院提供資訊之行為，以「提供答覆」或「准予查閱卷證」稱之。

²¹ 參照釋字第 762 號解釋理由書第 4 段至第 8 段。

²² 參照刑事訴訟法第 271 條之 1、第 455 條之 42。相關研究可參吳昭億，犯罪被害人之資訊獲知權－以刑事程序為中心，國立政治大學法律學系碩士論文，2018 年 7 月，頁 23-33。

²³ 蔡明誠大法官提出、黃虹霞大法官加入，釋字第 762 號解釋部分協同意見書，頁 11-13。相關研究可參許願，刑事被告與辯護人獲悉卷證資訊之探討，國立政治大學法律學系碩士論文，2019 年 2 月，頁 21-23。

²⁴ 林鈺雄，註 8 文。

第五項 資料與資訊之區別

法院所提供的卷證資料，或卷證內容中的資訊，二者的差別在於，「資料」(data)是真實世界的事實、信號或表徵，是未經整理的素材；「資訊」(information)則是經過整理的資料，得以影響人的行為或狀態²⁵。法院准予查閱卷證時，所提供的是卷證直接呈現的資料；提供答覆時，提供的則是經過整理而呈現的資訊，可能隱含法院或法規範的價值判斷。本文行文時，就個資保護原則與個資法之說明，將使用專有名詞「個人資料」，而在基本權內涵之說明，則依其脈絡可能出現「個人資訊」，惟二者並不特別強調其是否經過整理。



²⁵ 謝碩駿，政府資訊公開請求權在德國的憲法基礎，法學新論，3期，2008年10月，頁51。林素鳳，註18文，頁12。翁逸泓，OTT發展之隱私與個人資料保護問題初探，世新法學，第10卷，第1期，2016年12月，頁25。

第二章 個人資訊自主權與個資保護理論

本章旨在說明卷證中個人資料之使用行為所涉及的基本權，以界定法院之使用行為究竟牽涉何種基本權，又須遵守哪些保護要求。在刑事審判中，取得卷證中資訊的權利往往與憲法第 16 條之訴訟權、防禦權連結²⁶，是被告實現權利救濟的重要管道；而本文另由個人資料之角度切入，研究法院使用行為與資料當事人自主控制其個人資料的基本權利衝突，說明法院在實現其功能的同時，亦須符合一定要求。本文將依照發展時間順序，介紹德國與歐盟法上個人資訊自主權之演進，再介紹我國釋憲實務與學說上對此權利之評析。本文初步認為，個人資訊自主權關涉人格形成，並不依附於隱私權概念下，而屬獨立之基本權，受憲法第 22 條所保障。本文接著將整理個人資料的定義與其使用行為之要求，說明個人資料的範圍，可描繪出基本權利的保障範疇；說明個資保護的原則，可檢驗個資使用行為是否符合該等要求。最後，本文將說明刑事審判卷證中的資料，往往與個人資料範圍高度重疊，而須遵守前述個資保護原則，並由此開啟對現行規範的檢討。

第一節 資訊隱私權與個人資訊自主權的關係

在釋字第 585 號解釋中，大法官首次較詳細地引介隱私權的概念，闡明其雖非憲法列舉之基本權，然而基於人性尊嚴、個人主體性之維護與人格發展之完整性，並為保障個人生活秘密空間及個人資訊自主控制權，亦受憲法第 22 條所保障，但大法官並未進一步說明所謂「個人資訊自主控制權」的內涵；直到釋字第 603 號之解釋文中，大法官才說明隱私權的內涵中包含「資訊隱私權」，指的是「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、

²⁶ 防禦權概念之發展流變，僅參考蘇凱平，2018 年刑事程序法回顧：刑事被告憲法上防禦權的新篇章，國立臺灣大學法學論叢，第 48 卷特刊，2019 年 11 月，頁 1707-1711。

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」，但資訊隱私權與所謂「個人資訊自主權」的關係，仍尚待釐清²⁷。有論者整理，「資訊隱私權」(informational privacy)乃美國法之概念，而「資訊自決權」則屬德國法之概念，是否同屬一事，又或隱含不同價值，將影響個資法等相關法制的立法與解釋，並認為資訊隱私權維護個人內在形成的彈性空間，資訊自決權則保障個人外在行動的自由²⁸。本文同意資訊隱私權與資訊自決權範圍雖可能重疊，但仍屬兩種不同權利，後者並非前者派生，且並非所有個人資料皆為隱私權所保護²⁹，然而個資必然涉及資訊自決的理念，惟其涉及隱私敏感程度高低，得納入法規範之強度與密度的考量³⁰，以下取徑德國與歐盟法的發展脈絡，說明二者異同。

第一項 德國資訊自決權之濫觴：1983 年人口普查法判決

德國法上發展「資訊自決權」(informationelles Selbstbestimmungsrecht)之理念內涵與相關法制，至今已有超過 30 年的歷史。在 1970 年代的司法判決與解釋均揭示，每個人皆得自行獨自決定其生活圖像(Lebensbild)之全部或特定過程，是否或如何公開³¹。至 1983 年之人口普查案判決中，聯邦憲法法院確立了「資訊自決權」的內涵，而後為成為學說、實務的穩定見解。藉由引介此重要判決，本文欲說明重要基本權內涵，以及國家干預行為必須在與此權衡的前提下得進行。

本判決乃聯邦憲法法院針對 1983 年西德之人口普查法有關人口、職業、住

²⁷ 范姜真嫩，個人資料自主權之保障與個人資料之合理利用，法學叢刊，第 225 期，2012 年 1 月，頁 75。

²⁸ 邱文聰，從資訊自決與資訊隱私的概念區分一評「電腦處理個人資料保護法修正草案」的結構性問題，月旦法學雜誌，168 期，2009 年 5 月，頁 177。

²⁹ 李震山，來者猶可追，正視個人資料保護問題—司法院大法官釋字第六〇三號解釋評析，台灣本土法學雜誌，76 期，2005 年 11 月，頁 228。邱文聰，註 28 文，頁 177。Maria Tzanou, Data Protection as a Fundamental Right next to Privacy? "Reconstructing" a Not so New Right, 3 INTERNATIONAL DATA PRIVACY LAW 88 (2013).

³⁰ 李震山，人性尊嚴與人權保障，元照，2011 年，頁 234。

³¹ 詳參李震山，註 30 書，頁 224。

宅、工作場所調查，與其後對該等資料為使用的相關條文作出違憲宣告³²。現代化之資料處理日趨複雜，其可能性僅有專業人員才能掌握，而立法者決定之調查範圍與使用目的未臻明確，亦可能引起國民對個資登記之恐懼，許多針對該法律的憲法訴訟被提起，而由聯邦憲法法院在此判決中就該法進行全面性的審查。

判決理由中認為，本於基本法第 2 條第 1 項之一般人格權、第 1 條第 1 項之人性尊嚴，可推導出資訊自決權的內涵為，「保護個人資料不受無限制的提取、儲存、使用及轉送，個人享有基本上自己決定其個資透露及使用之權利」。然而此項權利之保障並非毫無限制，判決理由中亦提及，個人對其資料並無所謂絕對、無法加以限制的控制權，亦須依賴個資在社會團體中發展、聯絡交往，亦是社會事實之寫照，故此權利無排他性，而具有可限制性。其認為個人資訊自決權應僅在有關重大利益時方得限制，具有相當高的位階³³。

資訊自決權在此時是否屬基本法未列舉的新的基本權，尚待討論，但本判決的重要價值在於首次揭示資訊自決權在基本法上的依據，得由人性尊嚴與一般行為自由推導而來，而居於憲法位階。有論者進一步指出，資訊自決權若受不當限制，將有害於個人人格發展，如個資之分析、傳輸行為應於最小限度範圍內為之，不得將資料當事人全部暴露於政府資訊中，否則個人已是透明現象，其人格權將嚴重受損³⁴。基於此判決揭示的基本權利，德國法上後續的法制設計與司法解釋均需注意此項權利的保護，以符合憲法要求。

第二項 歐盟法上之發展

歐盟法上關於保障個人資料法制之發展，有幾個重要的里程碑，如 1995 年之 95/46/EC 資料保護指令(Data Protection Directive, DPD)，以及其後更完備的 GDPR、2016/680 指令。在 DPD 指令中，條文較為強調保障隱私權，其最大的

³² BVerfGE 65, 1. 中文譯介參考蕭文生，註 10 文。

³³ 李震山，多元、寬容與人權保障：以憲法未列舉權之保障為中心，2 版，元照，2007 年，頁 198-199。

³⁴ 李震山，註 33 書，頁 200。

貢獻在於將個資定義明確化，並建立個資保護的法制框架，而其他權利則居於次位，較少著墨³⁵，通說亦認為 DPD 的解釋適用，應在不違反歐洲人權公約第 8 條之隱私權規範的前提下為之³⁶。在 GDPR 與 2016/680 指令中，透過對歐盟會員國具有直接拘束效力的 GDPR 規範，並設置個資蒐集之同意與撤回機制、被遺忘權、資料可攜權、個資洩漏通知義務及資料保護影響評估制度(Data Protection Impact Assessment, DPIA)等新規範，也將資訊自決權的要求落實於條文中³⁷。

在這些法制發展的背後，經過 30 餘年，資訊自決權已成為歐盟會員國共同肯認的重要基本權利，由歐盟基本權利憲章(Charter of Fundamental Rights of the European Union，下稱「憲章」)及歐洲人權法院(European Court of Human Rights)判決中可見一斑。在歐洲人權公約(European Convention on Human Rights，下稱「公約」)及歐洲人權法院判決中，雖未明文將個資保護權利列於人權清單中，卻往往透過裁判實務擴張解釋公約第 8 條之隱私權概念，將個資保護納入私人領域保障範圍中³⁸，從而逐漸確立資訊自決權的重要內涵，最後落實於 GDPR 與歐盟會員國內國法等規範。在歐盟基本權利憲章中，則明文將資訊自決權提升至基本權層次，為後續的下位法規範奠定基礎³⁹。

第一款 歐洲人權法院判決

依歐洲人權公約第 8 條，隱私權保護的核心概念在於「尊重私人生活」(respect for private life)，並可分為消極與積極義務兩種面向觀之：在消極義務面，國家需尊重個人之私人、家庭生活，原則上不得干預；在積極義務面，國家則須保護個

³⁵ Norberto Nuno Gomes de Andrade, "Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights," in *Privacy and Identity Management for Life*, ed. Simone Fischer-Hübner et al., vol. 352, IFIP Advances in Information and Communication Technology (Berlin, Heidelberg: Springer Berlin Heidelberg, 2011), 90–107, https://doi.org/10.1007/978-3-642-20769-3_8.

³⁶ 邱文聰，註 28 文，頁 182。

³⁷ 劉靜怡，淺談 GDPR 的國際衝擊及其可能因應之道，月旦法學雜誌，286 期，2019 年 3 月，頁 6。

³⁸ 李寧修，預防性通信資料存取之憲法界限－以歐盟儲備性資料存取指令（2006/24/EG 之發展為借鏡），興大法學，17 期，2015 年 5 月，頁 96。

³⁹ 蘇慧婕，歐盟被遺忘權的概念發展－以歐盟法院 *Google Spain v. AEPD* 判決分析為中心，憲政時代，第 41 卷，第 4 期，2016 年 4 月，頁 477。

人之私生活免於他人侵犯⁴⁰。在隱私權的框架下，歐洲人權法院作出的數則判決，雖以第 8 條為受干預的基本權，但其中說明尊重私人生活之要求，並揭示個人資料自主控制的權利，亦屬資訊自決權之範疇⁴¹。由於本文討論主要對象是法院使用卷證中個人資料的行為，採擇判決時亦以相近者為主，亦即其事實乃國家機關使用個人資料，探討資訊自決權如何被論述。

在歐洲人權公約第 8 條的框架下，並非所有個人資料均受其保護，僅在該等資料涉及私人生活時方屬之，而歐洲人權法院最常肯認者，乃個人醫療資料⁴²，本文將例示簡介兩則個人醫療資料使用之相關判決，說明國家機關使用個人醫療資料之行為，可能涉及第 8 條權利之干預。

在 *Z v. Finland* 案中，芬蘭法院在審理被告 X 涉犯強制性交之判決中使用其配偶 Z 為愛滋病患之資訊，且在判決書中提及 Z 的全名，此判決雖設有 10 年保密期間，當地一家報社卻在其報導中指名道姓提及 X 與 Z，並指出其二人均為愛滋病患⁴³。歐洲人權法院就愛滋病患之醫療資料闡述，若該等資料遭揭露，可能將劇烈影響其私人、家庭生活，及社會、工作關係，其可能面臨遭侮辱或排擠之風險；該法院並揭示，尊重醫療資料保密性的意義不僅在尊重病患隱私，更在於維繫病患與醫療機構間的信賴，否則在醫療資料遭公開的風險下，病患可能選擇不透露其資料，進而危及自己或社會大中的身體健康，故國家亦負有義務，就該等資料的不當揭露或流通提供適當預防措施⁴⁴。

在 *M. S. v. Sweden* 案中，M. S. 因工作時受傷而向勞工傷害保險局申請補償金，而後發現該局與其曾就醫的醫院間之通信紀錄中，醫院未經其同意而提供 M. S. 的醫療紀錄予該局，其中不僅包含其工傷紀錄，還包含其曾墮胎之相關資

⁴⁰ 劉靜怡，說故事的自由？——從歐洲人權法院近年隱私權相關判決談起，台灣法學雜誌，第 146 期，2010 年 2 月，頁 60-61。

⁴¹ 劉靜怡，註 40 文，頁 73-77。

⁴² 林宛怡，以犯罪偵查為目的之 DNA 資料保存——以歐洲人權公約第八條為中心，國立政治大學法律學系碩士論文，2009 年 12 月，頁 31。

⁴³ ECHR, *Z v. Finland*, Reports 1997-I. 案件事實參考林鈺雄，初探醫療秘密與拒絕證言權——從歐洲人權法院之 *Z v. Finland* 判決（愛滋病患案）談起，月旦法學雜誌，127 期，2005 年 12 月，頁 8-11。

⁴⁴ 林宛怡，註 42 文，頁 32-34。

料，最後該局做成不利 M. S. 的決定並拒絕其補償金之請求，M. S. 乃主張該局與醫院間傳遞其醫療紀錄之行為違反公約第 8 條⁴⁵。歐洲人權法院在本案判決中揭示，個人資料保護對於公約第 8 條之私人與家庭生活保障，具有根本上重要性；國家機關與醫療機構間的資料傳遞，亦應受公約第 8 條規範⁴⁶。

最後，單就個人資料的儲存本身，亦可能屬於私人生活之干預。在 *S. and Marper v. the United Kingdom* 案中，S. 和 Marper 均因受刑事追訴而被警察機關依法採取指紋與其 DNA，嗣訴訟終結後，英國政府將當事人之 DNA 樣本留存於國家資料庫中，經當事人請求刪除未果而提起救濟；歐洲人權法院認為，即使蒐集 DNA 的行為合法，亦不當然代表儲存行為毫無限制，國家將在何時，以何種方式、範圍使用此資料，對當事人而言均不明確，因為未來的使用可能性持續存在，故單就儲存行為即認定構成私人生活之干預⁴⁷。

綜上判決可發現，歐洲人權公約下的個人資料保護，以該等資料是否處於私人生活之範圍，或可說隱私權之保障範圍為斷，於此之外者則不受公約第 8 條保護。然而，在上開判決中，其實早已隱含資訊自決權的核心概念，如 *Z v. Finland* 案所爭執的，乃法院得否在判決中表明當事人之敏感醫療資料，並得否公開、其公開之方式等；*M. S. v. Sweden* 案所爭執的，也包含其個人資料之傳遞行為未經其同意，甚至事前未獲知悉，是否侵害其基本權利，又是否屬本案行政程序之瑕疵；而 *S. and Marper v. the United Kingdom* 案更說明國家機關使用個人資料之各環節均應受限制的基本原則。歐洲人權法院判決已勾勒出個人自主決定其資料揭露與否、揭露之對象、方式、範圍等具基本權地位的要求。

第二款 歐盟基本權利憲章

歐盟基本權利憲章在 2009 年之里斯本條約生效後，具有與歐盟條約、歐盟

⁴⁵ ECHR, *M. S. v. Sweden*, Reports 1997-IV. 案件事實參考林宛怡，註 42 文，頁 32。

⁴⁶ 林鈺雄，註 43 文，頁 14-16。林宛怡，註 42 文，頁 29。

⁴⁷ ECHR, *S. and Marper v. the United Kingdom* judgment of December 2008. 林宛怡，註 42 文，頁 61-66。涂偉俊，建構刑事 DNA 資料庫之合理界限，法學新論，35 期，2012 年 4 月，頁 160-161。

運作條約相同的位階，拘束歐盟及其運作機關、會員國及其運作機關，以及私人⁴⁸。此憲章與歐洲人權公約及各會員國憲法的不同之處在於，其分別將私生活與家庭權利，即隱私權，規範於第 7 條，個人資料保護則規範於第 8 條，對此二種權利作出明確區別⁴⁹，其與歐洲人權公約及過往歐洲人權法院判決將此概念置於隱私權框架下，已然不同。更進一步而言，此憲章將個資保護視為前條隱私權之特別規定，並設置獨立條文，不將其視為隱私或人格權的外溢⁵⁰。本文將聚焦說明憲章第 8 條的保障範圍。

憲章第 8 條第 1 項揭示，所有人均有個人資料保護之權利。第 2 項前段明確說明：「個人資料僅得基於當事人同意或其他法律規定的合法原因，為特定目的，公平地被蒐集、處理與利用」，後段則揭示，所有人均有獲知其個人資料蒐集情況與更正其資料之權利。第 3 項則要求，前項規範之執行，由獨立機關監督之⁵¹。第 1 項將個資保護提升為基本權利；第 2 項前段則包含重要的個資保護原則，如目的拘束原則、資料最小化原則，及當事人同意等⁵²；第 3 項則要求歐盟與會員國設置獨立監督機關，以落實本條之保障。

本條的保障範圍，經論者整理指出，可分為物的保障領域及人的保障領域⁵³。在物的保障領域，本條保護客體為個人資料，依 GDPR 第 4 條第 1 款、2016/680 指令第 3 條第 1 款⁵⁴，個人資料指「有關已識別或足以識別之自然人(「資料主體」)的任何資料」，特別是透過「例如姓名、身分證統一編號、位置資料、網路識別碼或有關該自然人之身體、生理、基因、心理、經濟、文化或社會身分等具

⁴⁸ 蘇慧婕，註 39 文，頁 479-480。另關於歐盟基本權利憲章的發展歷程，可參王玉葉，註 9 書，頁 87-88；王泰銓，歐洲聯盟法總論，台灣智庫，2008 年，頁 637-641。

⁴⁹ 翁逸泓，註 25 文，頁 34。

⁵⁰ 蘇慧婕，註 39 文，頁 480。

⁵¹ 第 8 條之中譯參考：劉定基，析論個人資料保護法上「當事人同意」的概念，月旦法學雜誌，218 期，2013 年 7 月，頁 148；蘇慧婕，註 39 文，頁 480-481。

⁵² 個資保護原則之說明，詳見第二章第二節之介紹。

⁵³ 蘇慧婕，註 39 文，頁 481-482。

⁵⁴ 此二規範之文字雷同。原文為「‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person」。

體因素」，進而可特定出該自然人者屬之⁵⁵。憲章第 8 條雖保障個人資料，但與第 7 條所保障的隱私、敏感性資料仍有不同，質言之，任何可識別出特定自然人之資料，無論其已公開與否，均屬本條保障範圍。在人的保障領域，本條保障者乃自然人，法人是否受此保障則有爭議⁵⁶，關於法人之保障與否則不在本文討論範圍。藉由將個資保護納入基本權保障，歐盟基本權利憲章對資訊自決權的意義在於，將個資保護與隱私權區分為不同的權利，回應歐洲人權法院判決的見解發展，並奠定其後歐盟法與會員國內國法的基礎。

第三款 學說上之演進

在學說上，個資保護之權利與隱私權間的關係，亦是長久以來的討論重點⁵⁷。有論者觀察，個資保護與隱私權乃截然二分的權利，前者是「透明性的手段」('tool of transparency')，後者則是「模糊性的手段」('tool of opacity')，在此框架下，個資保護限制並控制資訊的使用行為，課予資料控制者一定義務，並賦予資料當事人一定權利；隱私權則是避免私生活領域受到國家權力與不符比例原則的干預侵擾⁵⁸。延伸此框架，另有學者認為，透明性與模糊性的兩種手段並非相互排斥，而是處於互補的關係；其認為，隱私權屬於實體權利(substantive right)，發揮其隔絕對私人生活之干擾的功能，可輔助個人其他自由之實踐，如言論自由、秘密投票之自由等，而隱私權與其他基本權之保障常有衝突之處，必須經由司法解釋加以權衡；個資保護則屬於程序性權利(procedural rights)，其功能發揮於隱私權與其他權利權衡後，對於資料流通設置一定規則，以保護個人隱私權，並提升資

⁵⁵ 此定義與 1995 年之 DPD 大體相同，故在操作上，過去執行 DPD 的經驗亦可供 GDPR 與 2016/680 指令參考。參照張陳弘、莊植寧，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，新學林，2019 年，頁 20。

⁵⁶ 蘇慧婕，註 39 文，頁 482。

⁵⁷ 以下學說演進亦參考自 Aidan Forde, *The Conceptual Relationship Between Privacy and Data Protection*, 1 CAMBRIDGE L. REV. 135, 138 (2016)。張陳弘，科技智慧防疫與個人資料保護：陌生但關鍵的資料保護影響評估程序，國立臺灣大學法學論叢，50 卷，2 期，頁 356。

⁵⁸ Paul De Hert & Serge Gutwirth, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, in *PRIVACY AND THE CRIMINAL LAW* 61 (E. Claes, A. Duff & S. Gutwirth eds., 2006), https://works.bepress.com/serge_gutwirth/5/.

料控制者之可問責性(accountability)⁵⁹。

然而，此見解招致的批評是，個資保護若與隱私權掛勾，且居於隱私權的下位、補充性權利地位，則個資保護與隱私權終無二致，且個資保護權利之侵害，將會永遠要以隱私權是否遭侵害為斷，因為依據上開見解的推理，居於實體權利地位的隱私權必先受侵害後，才有討論個資保護權利是否受侵害的餘地⁶⁰。另有批評者認為，即使前述論者正確認識到，在歐盟基本權利憲章中，隱私權與個資保護之權利屬不同基本權，以實體/程序性、補充性權利描述其間關係，仍非充分的立論：首先，隱私權與個資保護的區分標準並不明確，其背後的「模糊性」、「透明性」並無精確定義；再者，個資保護亦可保障個人不揭露其資料之自由，而具有某程度「模糊性」，與隱私權產生重疊，但前述論者的觀點就此無法解釋，更無法說明此二種權利間如何可能產生衝突與權衡⁶¹。

另有論者認為，個資保護比隱私權更能確保個人選擇展示自己身分的自由 ('selective presentation' of individual identity)，因為隱私權在資料管理的功能上不如個資保護集中，而藉由賦予個人更程度的資料控制權限，個人得以揭示其人格的不同面向，從而促進人格發展；因此，有效的資料保護框架便立基於資料揭露之控制，並注重於平衡資料當事人與資料控制者間的不對稱地位⁶²。本文亦贊同此見解，此解釋將個人資料受保護之權利，以個人自主決定在社會中展現自己哪些面向的角度闡發，與隱私權固有之保護私人生活領域的內涵做出區隔，但二者位階相同，並無衍生、附屬之關係而喪失對話空間，與資訊自決權之內涵最為相符。

⁵⁹ de Andrade, *supra* note 35, at 96-97. 認為個資保護屬程序性權利的相近觀點，參見邱文聰，註 28 文，頁 179。

⁶⁰ Tzanou, *supra* note 29, at 88-89.

⁶¹ Forde, *supra* note 63, at 146。

⁶² Orla Lynskey, Deconstructing Data Protection: The “Added-Value” of a Right to Data Protection in the EU Legal Order, 63 INTERNATIONAL & COMPARATIVE LAW QUARTERLY 569, 590-594 (2015).

第三項 我國法上之發展

在台灣法上，釋憲與判決實務對於隱私權，乃至於資訊自決權的概念發展，亦經過一番演進。本文將從大法官解釋的脈絡整理隱私權與資訊自決權的內涵，說明實務上亦已經嘗試落實資訊自決權的精神。在我國司法解釋上，同時繼受美國、德國對於隱私權的脈絡，再經大法官與最高法院之解釋及落實，成為現今的樣貌，亦屬本文接下來欲描述的對象。本文就研究對象涉及之基本權在我國法脈絡下作一介紹，並統合前述說明之德國、歐盟法發展，闡述其已確實影響我國法制。

第一款 釋憲實務上的發展

大法官對資訊隱私權或資訊自決權的概念闡述，均由隱私權的發展開始。有論者整理指出，隱私權於釋憲實務上的發展可分為三個階段，第一階段中僅論及隱私權，而未詳做說明；第二階段逐漸建立隱私權的內涵與保護範圍；第三階段則討論隱私權的空間意涵⁶³。本文亦採此架構介紹隱私權在大法官解釋中的發展，並較強調其中個人資料自主控制的脈絡。

我國釋憲實務中首次對隱私權概念進行較詳細的解說，見於釋字第 585 號解釋理由書，其中提及，「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」。在此之前的大法官解釋，如釋字第 535 號解釋，僅提及「隱私權」之名詞，而未進一步闡述。釋字第 585 號解釋對於隱私權的說明可概分為兩點，第一，隱私權乃憲法第 22 條概括基本權所保障之權利，具有憲法上位階；第二，隱私權的包含「個人生活秘密空間免於他人侵擾」與「個人資料自主控制」兩種權利。然而大法官對於這兩個概念，則未再深入說明。

⁶³ 葉俊榮，探尋隱私權的空間意涵—大法官對基本權利的脈絡論證，中研院法學期刊，18 期，2016 年 3 月，頁 5。

第二階段以釋字第 603 號解釋為代表，大法官於解釋文中重申上述隱私權概念，並進一步闡釋，「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。」大法官正式闡釋個人自主決定揭露其資料的權利，並使用「資訊隱私權」稱之。究其內涵，其與前述德國、歐盟法上之資訊自決權，似有重疊。

第三階段以釋字第 689 號解釋為代表，大法官於理由書闡釋，「個人之私密領域及個人資料自主，在公共場域亦有可能受到干擾，而超出可容忍之範圍，該干擾行為亦有加以限制之必要。」本號解釋涉及新聞自由及一般行動自由與他人之一般行動自由及隱私權發生基本權衝突時，如何進行權衡的問題。其意義在於，大法官不僅再度肯認「個人資料之自主權」的保障，並說明即使是在公共場域中亦同，將隱私權的保障範圍由「場所」導向「個人」，以維護個人主體性與人格尊嚴⁶⁴。

隱私權經由大法官的引介與解釋，已成為我國憲法位階的基本權利，然而對其內涵仍有模糊空間，在解釋文中多次提及的「私人生活不受侵擾」及「個人資料自主控制」之間範圍尚待界定，而個人資料自主控制所代表的，是釋字第 603 號解釋所稱的資訊隱私權，抑或學理上所稱的資訊自決權，二者如何區分，亦有待補充。

第二款 學說上的發展

就大法官解釋中尚未釐清的概念，學理上有從美國或德國等繼受法角度進行補充，說明釋字中的基本權利究何所指，本文將整理相關見解，進一步說明資訊隱私權與資訊自決權的內涵，並論述本文的立場。

⁶⁴ 指出隱私權保護的關注對象由空間轉向個人，相關參考文獻僅參見：葉俊榮，註 63 文；劉靜怡，大法官保護了誰？釋字第六八九號的初步觀察，月旦法學雜誌，197 期，2011 年 10 月，頁 55-56。有論者整理指出，此一脈絡乃繼受自美國憲法解釋與其學者理論，「合理隱私期待」的主張立基於空間與身體的隱私權，但在所謂「資訊隱私權」上即會面臨解釋適用的難題，參見張陳弘，隱私之合理期待標準於我國司法實務的操作－我的期待？你的合理？誰的隱私？，法令月刊，69 卷，2 期，2018 年 2 月，頁 98-106。

第一目 資訊自決權之獨立基本權地位

有學者認為，資訊隱私權乃美國法上用語，而資訊自決權則屬德國法上用語，二者分屬不同脈絡；而在我國法上，資訊隱私權指的是不受干擾之私人生活中與個人資料相關的部分，資訊自決權強調的則是個人對其資料的提供與利用，均有積極參與及形成自我決定的可能⁶⁵。無論資訊對於個人的意義為何，只要是與個人相關的資訊，均是個人得為資訊自決的對象，只要此關於個資自主控制之可能性未受外在壓迫，資訊自決權即已獲保障，故本質上其屬於行為自由的一種⁶⁶。申言之，資訊自主權屬資訊隱私權之前哨，每次個資蒐集行為，無論是否涉及隱私，均須尊重資料當事人之決定⁶⁷。

第二目 資訊隱私權與資訊自決權之關係

上述見解說明資訊自決權有別於釋字第 603 號解釋中之資訊隱私權，乃獨立之基本權利，至於各權利之關係，有認為其如同心圓一般，以人性尊嚴為核心，依序外擴至一般人格權、個別人格權之隱私權、隱私權下之資訊隱私權、最後是涉及個人資料之資訊自決權⁶⁸。亦有學者認為資訊隱私權與資訊自決權的內涵、性質不同，保障範圍雖有重疊亦不相同，資訊隱私權維護個人內在形成的彈性空間，資訊自決權則保護個人外在的行為自由⁶⁹。本文同意上述見解對此二權利間關係的描述，即其雖在涉及隱私之個人資料方面的保護重疊，但資訊自決權在不涉及隱私的個人資料方面施加保障，因此更為全面。當然，此兩種保障亦非互斥關係，而可能產生競合，自不待言。

另有學者認為，就美國法的脈絡而言，所謂個人自主控制資料，僅為資訊隱私權下的個資控制利益，在資訊隱私權的保護下，個人就其資料除了控制利益外，

⁶⁵ 李震山，註 33 書，頁 196-200。

⁶⁶ 邱文聰，註 28 文，頁 174。

⁶⁷ 李震山，註 29 文，頁 228。

⁶⁸ 李震山，註 29 文，頁 229。

⁶⁹ 邱文聰，註 28 文，頁 177。

還有其他的隱私利益，如不使個資洩漏以維持私人生活不受干擾的「秘密性」，以及為維護個人所經營人際關係而選擇是否揭露個資的「親密性」，三者屬分立關係，須個別判斷其是否受完整保護；此見解的立論在於，若將個資控制利益理解為包含秘密性與親密性，則一旦在利益權衡中選擇犧牲個資控制利益，秘密性與親密性將一併喪失保障⁷⁰。

第三目 本文見解

本文論述資訊隱私權與資訊自決權的內涵及其關係，目的在說明本文研究對象，即法院使用卷證中個人資料之行為，對資料當事人而言落入何種基本權利的保障範圍，在利益權衡下，法院又因此須受何種限制。上開二種學說的理解差異源於美德二國基本權的體系出入，但所欲保障之權利內涵則大抵相同。經由上開整理，本文認為就涉及個人隱私之資料，當屬資訊隱私權的保障範圍無疑，而除此之外的其他個人資料，亦常為法院所使用，卻不受資訊隱私權所保障，故本文以為保障範圍更大之資訊自決權方能涵蓋之。學說中依美國法體系，將個資自主控制、秘密性與親密性利益均置於資訊隱私權的保護大傘下，在德國法體系上，則由部分範圍重疊之隱私權與資訊自決權保護之，亦為完備。本文在後續論述中欲討論的基本權，為德國法上之資訊自決權，或有稱為「個人資料自主權」、「個人資訊自主權」等，其保護範圍乃個人對其資料之自主控制，其中亦包含與隱私權重疊之部分，自不待言。

第二節 個人資料的定義與其使用行為之要求

法院使用卷證中個人資料之行為，同時涉及個人資料保護法與刑事訴訟法，兩個法領域均為本文討論的對象。過去即有學者指出，縱使法院調閱個資的行為涉及刑事程序，亦應注意資訊自決權之保障，然而無論個資屬於被告或第三人，

⁷⁰ 張陳弘，新興科技下的資訊隱私保護：「告知後同意原則」的侷限性與修正方法之提出，國立臺灣大學法學論叢，47卷，1期，2018年3月，頁257-264。

刑事訴訟法上幾乎沒有相關規範設防⁷¹，亦欠缺救濟管道。時至今日，現行刑事訴訟法上對於如何處理與利用出自刑事程序之個人資料，仍僅有少數例外⁷²。

有論者指出，個資法屬實體法，其注重的是個人權益之維護，內容包含公務機關使用個資的行為規範，與刑事訴訟法所設證據使用禁止及其救濟管道之相關規範，兩者之立法目的不同⁷³。就刑事審判的公共利益而言，個資法上僅得依目的拘束原則等進行控制，而未能更細緻地區分追訴犯罪或資訊公開等公益，似不宜逕將法院使用刑事卷證中個資的行為交由個資法規範處理，而仍應由刑事訴訟法規承擔，以求更貼近資料當事人之權利保護，與符合正當法律程序要求⁷⁴。本文以為，無論使用個資的行為規範於個資法或刑事訴訟法中，皆須符合個資保護之原理原則要求；在刑事卷證中個資的使用行為上，個資法與刑事訴訟法產生競合，應先適用刑事訴訟法為特別法，若有不足再尋求個資法規範。本文將先介紹個資法的具體保障範圍，再介紹個資保護的各項子原則，說明上開行為應符合何種要求。

第一項 個資法的保障範圍

欲判斷法院裁判所使用之卷證是否屬於個資，首須說明如何認定個資法的保護範圍及保護密度。在刑事訴訟法條文中，至多僅提及「卷證」作為卷宗與證物的合稱，對於其內容涉及之個人資料並無定義。依循整體法律體系解釋，個人資料的定義，仍應回到個資法探求。依個資法第 2 條第 1 款，凡得以直接或間接方式識別該個人之資料均屬個人資料，而實務上往往仰賴主管機關函釋與法院裁判

⁷¹ 何賴傑，論刑事訴訟法之傳承與變革—從我國與德國晚近刑事訴訟法修法談起，月旦法學雜誌，100 期，2011 年 1 月，頁 183。

⁷² 如刑事訴訟法第 33 條第 5 項，「持有第一項及第二項卷宗及證物內容之人，不得就該內容為非正當目的之使用」；第 33 條之 1 第 2 項，「辯護人持有或獲知之前項證據資料，不得公開、揭露或為非正當目的之使用」。參見林鈺雄，註 8 文，頁 201。

⁷³ 陳玟瑄，刑事偵查「第三人原則」與「隱私之合理期待」—以偵查機關向網路服務提供者調取非內容性通訊資料為例，國立政治大學法律學系碩士論文，2017 年 7 月，頁 4-7。

⁷⁴ 同前註。另有學者認為，違反目的拘束原則而取得之刑事證據，其證據能力應依刑事訴訟法第 159 條之 4 權衡之，然進一步而言，此類問題應交由個資法或刑事訴訟法規範，已屬立法論問題，參見李惠宗，註 7 文，頁 58-59。

之認定，諸如行車記錄器攝錄影片內容、定位資訊、通聯記錄與通話內容、車牌影像資料、自人體採集之體液等生物檢體，及電話號碼所屬之電信業者別等，均為實務判決或函釋曾認定之個人資料⁷⁵。而與刑事審判直接相關者，例如前述條文列舉之「犯罪前科」，依個人資料保護法施行細則第4條第6項，指經緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄。至於個人資料的原則性定義，本文將討論可以做為個資判斷依據的資料特性，並指出具有某些特性的資料將受到更高程度保護。

第一款 直接或間接識別/去識別化

在我國個資法的操作上，判斷個人資料的其中一個重要標準，在於該資料得否經由直接或間接識別而連結至特定個人，而無法識別個人的資料，則不在個資法保障範圍。反過來說，將資料中可連結至個人特性的部分消除，使其成為「去識別化」的資料，亦屬兼顧資訊流通與個資保護的手段。資料連結至特定人的現象，並非僅為有無之分，而是存在程度差異，其中關鍵即在於「間接識別」的意義與範圍如何界定，亦引起學說的熱烈討論。間接識別的意義，依個人資料保護法施行細則第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。實務、學說上亦各自發展出不同標準，整理如下⁷⁶。

有學者認為，所謂「以間接方式識別」，應指僅依該資料本身無法識別出特定人，但與其他資料組合比對後得以為之，而具有間接識別能力之人，可能是一般社會大眾，亦可能為與當事人關係密切之人，所掌握關於當事人資料的質與量往往差異甚大，因此宜以「社會一般多數人」為判準，以適當保持個資之合理流通使用⁷⁷。若社會一般多數人依該等資料均能推知出該個人，則該資料屬個人資料，應依法受保護。

⁷⁵ 財團法人資訊策進會科技法律研究所，個資保護 2.0，書泉，2019 年，頁 14-15。

⁷⁶ 張陳弘、莊植寧，註 55 書，頁 30-31。

⁷⁷ 范姜真嫻，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，41 期，2013 年 12 月，頁 98-99。

實務上則有以「資料蒐用者」為判準，認為應審酌蒐集或使用本身主觀條件，依個案情形認定，並無一定標準。如記名悠遊卡卡號是否屬個資，法務部曾有函釋認為應區別持卡人以外之第三人與悠遊卡公司二者討論，就前者而言，查詢上有困難，或需費過鉅方能識別特定人時，客觀上即屬無法識別的個資；就後者而言，其得藉由比對卡號與其內部資料庫而識別出個人，查詢尚無困難亦無需過多勞費，故屬於得識別之個資，仍受個資法規範⁷⁸。因間接識別的個資需與其他資料連結方得識別出個人，故同一筆資料在不同人手上將發揮不同效果，此判準似較貼近實際運用需求，然仍仰賴個案判斷，而難以建立準則，對於個資法適用的穩定性亦造成影響⁷⁹。

有論者提出，鑑於我國個資法立法過程中參酌歐盟 DPD 甚多，DPD 的相關解釋對於我國法亦有參考價值，而在個人資料的認定上，可參歐盟資料保護工作小組(Art. 29 Working Party，下稱 AWP 29)所提出之意見書⁸⁰。AWP 29 於 2007 年提出之意見書認為，個人資料的認定標準有四要件，分別為「任何資料」(any information)、「資料與個人之關聯性」(relating to)、「已識別或足資識別」(identified or identifiable)與「自然人」(natural person)，以下分別解釋⁸¹。

前兩個要件與資料相關。「任何資料」乃從寬認定的要件，舉凡任何與個人有相關的資料，無論是客觀或主觀、真實與否，均屬之⁸²。「資料與個人之關聯性」則提供進一步的篩選標準，若資料的內容(content)、目的(purpose)或結果(result)

⁷⁸ 法務部法律字第 0999051927 號函，轉引自張陳弘，註 6 文，頁 70。

⁷⁹ 張陳弘，註 6 文，頁 71。類似觀點參見陳重言，刑事追訴目的之通信（通聯）紀錄調取與使用—兼評 2014 年初通保修法，檢察新論，16 期，頁 42。

⁸⁰ 歐盟資料保護工作小組係歐盟委員會、歐洲資料保護監督聯盟委員會與各會員國之個資保護監理機關指派之代表，依 DPD 第 29 條共同組成，並在 2018 年 5 月 GDPR 正式施行後，由歐洲資料保護委員會(European Data Protection Board, EDPB)取而代之。參照張陳弘、莊植寧，註 55 書，頁 iv、20。惟須注意者，DPD 與 AWP 29 之意見書，對各歐盟會員國而言，並無強制拘束力；關於歐盟所使用之法律工具及其效力，可參照許耀明，歐盟法、WTO 法與科技法，元照，2009 年，頁 141-144。

⁸¹ Art. 29 Working Party, Opinion 4/2007 on the Concept of Personal Data, 01248/07/EN: WP 136, 20 June 2007.

⁸² 客觀的資料如血型或身分證字號，主觀的資料如對個人的評價；內容不真實的資料亦可能為個資，因個資保護賦予當事人更正其資料之權利。參照張陳弘，註 6 文，頁 72-73；張陳弘、莊植寧，註 55 書，頁 21。

任一項與個人有相關性，則滿足此要件，亦即資料之內容、資料使用目的，或資料使用結果對個人權益將造成影響時，即屬之⁸³。

後兩個要件則與個人相關。「已識別或足資識別」指的是，一位自然人在群體中可與其他人區分，或無法立即與他人區分而有可能區分，DPD 前言第 26 節 (Recital 26)⁸⁴、GDPR 前言第 26 節即指出，「足資識別」乃透過所有可能、合理的方式，考量成本、時間、技術，得辨認出個人者屬之⁸⁵。「自然人」則以現存在世者為限，惟亡者或法人之資料，與現存之自然人具有連結者，仍可能在此範圍內受個資法保護⁸⁶；另外，尚未出生之胎兒亦可能為例外受保護的對象⁸⁷。

本文認同以 AWP 29 意見書之準則作為個人資料的判斷標準。其優點在於該準則與我國個資法立法脈絡貼近，亦與 GDPR 操作一致，故其相較其他見解更符合我國立法者原意，並能與國際趨勢接軌。該準則的可操作性較高，亦降低個案適用的不穩定性。綜上言之，符合四種要件之資料屬於個人資料，應受個資保護；而若資料無法識別特定人，則不在保障範圍內。此可概分為兩種情形，其一是本來就與個人無關之資料，如天氣預報，自不屬個資法保障範圍，另一情形則為「去識別化」之資料，亦即個資法施行細則第 17 條所稱，「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」。

去識別化的技術又可分為假名化(pseudonymisation)與匿名化(anonymisation)。假名化依 GDPR 第 4 條第(5)款、2016/680 指令第 3 條第(5)款，乃指一種處理個資的方式，使該個資在不使用其他資訊時，不再能單獨識別出資料當事人，且該資料亦已被分開存放，並以技術或組織上措施確保該資料無法連結至已識別或足

⁸³ 參照張陳弘，註 6 文，頁 73-74；張陳弘、莊植寧，註 55 書，頁 22-23。

⁸⁴ Recital 乃指歐盟指令或規範條文的前言，與條文一同公布，並非法律或命令，僅為用以說明條文內容，本身並無任何強制力，或可理解為立法說明。該前言第 26 節稱為「Recital 26」，以此類推。

⁸⁵ 如一位女士罕見的名字(first name)與其 X 光片被刊登於科學期刊，其熟識者仍得由此辨認出該特定人，故該份資料屬於個資。Art. 29 Working Party, *supra* note 81, at 15. 亦參照張陳弘，註 6 文，頁 74-75；張陳弘、莊植寧，註 55 書，頁 23-24。

⁸⁶ Art. 29 Working Party, *supra* note 81, at 23. 張陳弘，註 6 文，頁 76-77。劉定基，個人資料的定義、保護原則與個人資料保護法適用的例外——以監視錄影為例(上)，月旦法學教室，115 期，2012 年 5 月，頁 44-45。

⁸⁷ 如胎兒之超音波照片、基因檢測資料等。同前註。

資識別之自然人⁸⁸。2016/680 指令的前言第 53 節指出，利用假名化方法將個資去識別化，有助兼顧資訊流通與資訊安全⁸⁹，但其亦於前言第 51 條、第 61 條指出，假名化資料若遭未經授權之回溯(unauthorised reversal of pseudonymisation)，有損於當事人利益，亦屬個人資料毀損(personal data breach)⁹⁰。假名化的方法包含編碼(coded)或永久去連結(delinked)兩種方式，前者指以特定數字或文字等代碼取代資料中可識別當事人之部分，然事實上仍保有回溯的方式與可能；後者則指一開始就放棄解碼回溯的可能，永久去除可識別當事人的部分⁹¹。以編碼方法假名化之資料，因尚具有可回溯性，仍可能屬於個資，不得將其排除於個資保護⁹²。永久去連結之資料，因不再具有可辨識性或回溯之可能，而落入匿名化個資的範疇。匿名化個資除上述的事實上不能再識別外，尚包含制度上不能，即立法禁止任何人以任何方式將其重新連結至當事人⁹³。申言之，無論以何種方法，只要將個資永久地去識別化，使之斷絕再連結回個人之可能，即屬匿名化個資，而不屬個資保護範圍。

去識別化的目的在於藉由降低個資風險而促進資訊流通，試圖在二者間取得平衡，然而在現今科技日新月異的發展下，完全斷絕回溯可能性的永久去連結將不斷受到挑戰，而該等匿名化個資亦將落入既無法制保障，又可能再被連結回當事人的風險中⁹⁴。而我國個資法及其施行細則亦無規範去識別化之方法，留下解

⁸⁸ 翻譯參考張陳弘、莊植寧，註 55 書，頁 26。所謂適當技術或組織上措施之細節，以德國個資法為例，其措施諸如確保使用紀錄、事後審查、接受主管機關監管、維護系統之可信度、完整性、可用性、持久性等，參見翁逸泓、李寧修，歐盟國家個人資料保護法制因應 GDPR 施行之調適 - 以德國與英國為例，國家發展委員會委託研究報告，2020 年 5 月，頁 97-102。

⁸⁹ 原文為：「The use of pseudonymisation for the purposes of this Directive can serve as a tool that could facilitate, in particular, the free flow of personal data within the area of freedom, security and justice.」

⁹⁰ 關於個人資料破壞所衍生之義務，見後章節說明。

⁹¹ Art. 29 Working Party, *supra* note 81, at 18-20. 邱文聰，註 28 文，頁 185，但該文獻中並未區分假名化與匿名化之差異。

⁹² GDPR Recital 28. 張陳弘、莊植寧，註 55 書，頁 27。

⁹³ Art. 29 Working Party, *supra* note 81, at 21. 亦參照張陳弘、莊植寧，註 55 書，頁 27。

⁹⁴ 翁逸泓，註 25 文，頁 15-16。Maria Cristina Caldarola、Joachim Schrey 著、趙彥清、黃俊凱譯，大數據與法律實務指南，元照，2020 年，頁 184；關於假名化與匿名化之技術操作標準，亦可參見該書，頁 176-188。

釋空間，但也可能造成個資的使用規範密度不周⁹⁵。本文認為，無論個資是否經過去識別化，檢驗資料是否應受個資保障，仍應回歸 AWP 29 提出之四要件判斷，亦即重新評估該等資料在個案脈絡中是否可被連結至特定人，方能使個資保護不致出現缺口。

第二款 一般性個資/敏感性個資

在個資法的保障範圍中，涉及「病歷、醫療、基因、性生活、健康檢查及犯罪前科」等六種個人資料因對於個人之其性質特殊，對當事人影響較大，故個資法第 6 條賦予該等資料特殊保護，明定其使用行為乃「原則禁止、例外允許」⁹⁶。在第 6 條立法理由上，承襲 DPD 在其前言第 33 節的特別說明，給予敏感性個人資料較高保護的原因在於，「此等資訊依其本質具有造成隱私或基本權侵害的能力」(data capable by their nature of infringing fundamental freedoms or privacy)⁹⁷。立法者特別列舉這類資料，因該等資料往往涉及個人私密領域，亦即與隱私權保障範圍高度重疊，且一經揭露往往將透露個人弱點或未來發展趨向、或使個人遭受歧視⁹⁸，對資料當事人之人際交往關係造成不可逆的損害，妨害其人格形成與發展，故須嚴格對待其使用行為。

第三款 後設資料

在現今的科技快速發展下，資料連結至個人的可能性逐漸提高，偵查機關與法院調查、掌握個人生活的圖像也越來越清晰。有論者指出，所謂「後設資料」(meta data)，意即用以描述資料的資料(data about data; information about information)，亦屬於國家用以監控人民的手段之一，而其可能連結至個人之特性，使得該等資料亦可能受個資保護⁹⁹。以通訊監察為例，除了通訊內容外，通訊保

⁹⁵ 邱文聰，註 28 文，頁 186。

⁹⁶ 財團法人資訊策進會科技法律研究所，註 75 書，頁 31。

⁹⁷ 邱文聰，註 28 文，頁 183-184。劉靜怡，不算進步的立法：「個人資料保護法」初步評析，月旦法學雜誌，183 期，2010 年 8 月，頁 152。

⁹⁸ 財團法人資訊策進會科技法律研究所，註 75 書，頁 30-36。

⁹⁹ 陳重言，註 79 文，頁 42。劉靜怡，通訊監察與民主監督：歐美爭議發展趨勢之反思，歐美研究，第 47 卷，第 1 期，2017 年 3 月，頁 73-74。

障及監察法第 3 條之 1 第 1 項所規範之通訊雙方電信號碼、通信時間、使用長度、位址、服務型態、信箱或位置資訊等通信紀錄，雖不能直接識別出個人，但對於具備專業知識的電信業技術人員或偵審機關而言，其有能力將該等資料與其他資料併同連結至特定人，故其使用該等資料仍應符合個資保障要求¹⁰⁰。

值得一提的是，在德國法上，有論者認為電子卷證之後設資料亦屬於卷證資料的一部份，例如資料的種類標籤(標示屬於判決書、起訴書等)、電腦系統自動產生的資料編號，以及資料上的人工註解(Annotationen)等¹⁰¹。這些附隨的資料雖屬於卷證，亦可能連結至個人，但本文以為，其實際上是否受個資保護，仍應以 AWP29 提出之前揭原則檢驗，而非一概納入保障。

第四款 個人資料檔案

依個資法第 2 條第 2 款，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。又依個資法施行細則第 5 條，其備份檔案亦屬之。只要是系統性地建立、集合、整理而可以檢索者，皆屬個人資料檔案，在管理上與使用上皆具有相當大的便利性，但反面而言其中個資亦更容易受到濫用¹⁰²。個資法就此對個人資料檔案提供較高程度保護，課予公務機關較高義務要求，如個資法第 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」；其施行細則第 24 條，「公務機關保有個人資料檔案者，應訂定個人資料安全維護規定」；第 25 條要求維護資安專業人員之能力等。

依 GDPR 第 4 條(4)款、2016/680 指令第 3 條第(4)款，將個人資料彙整建檔的行為，稱為「個人特徵描繪行為」(profiling)，意指對個資進行任何形式之自動化處理行為，包含使用個資來評量關於資料當事人的個人特徵，特別是用以分

¹⁰⁰ 同前註。或有文獻稱為「輔助資料」(auxiliary data)，本文認為應屬相同概念，參考劉定基，註 86 文，頁 48。

¹⁰¹ Nicolai Grove / Dr. Ulf Gutfleisch, Die Strafakte im Zeitalter ihrer digitalen Reproduzierbarkeit, NStZ 2020, 633 (637).

¹⁰² 財團法人資訊策進會科技法律研究所，註 75 書，頁 29。

析或預測其工作表現、經濟與健康狀況、個人偏好與興趣、可信度、行為、位置或動向¹⁰³。此二規範就個人資料檔案，特別指單純(solely)以自動化處理之行為，如有人為介入環節則不屬之，而不若我國兼含自動化與人工產生之檔案；其目的在於評量當事人之各種個人特徵面向，而我國僅強調個人資料檔案易於查詢管理的功能，並未進一步點出該等檔案對個人的影響。

依照 GDPR 第 22 條、2016/680 指令第 11 條，國家機關進行個人資料檔案的單純自動化處理時，有義務保障當事人之自由與權益，至少需賦予當事人要求人為介入的權利。相較 GDPR，2016/680 指令第 11 條就此提供更高強度的個資保護，當單純自動化處理行為將對個人造成法律上反效果(adverse legal effect)或重大影響(significantly affects him or her)時，原則禁止之¹⁰⁴。2016/680 指令之前言第 38 節亦宣示，在此情形應設置適當保護措施(appropriate safeguards)保障當事人，包含對自動化處理的受解釋權。然而有文獻指出，2016/680 指令性質上係對於歐盟會員國之建議，並無強制力拘束各國，在內國法化的過程中，各國不一定均會落實指令中的各項呼籲；且有鑑於國家與個人間的資訊落差，個人是否果能獲知必要資訊，亦殊值懷疑¹⁰⁵。不過，依 2016/680 指令第 13 條，資料控制者仍應使當事人知悉自動化處理之法律依據、資料保存期間，以及接收其個資者之屬性，依個案決定提供資訊的範圍¹⁰⁶。

總言之，相較於 GDPR 與 2016/680 指令，我國個資法對於個人資料檔案之保障，雖亦察覺到其需受較高程度管理，但僅以交由行政機關內規方式處理此問題，並不似歐盟法上對該等檔案之使用行為設置加強規範。本文以為，使用該等

¹⁰³ 翻譯參照張陳弘、莊植寧，註 55 書，頁 208-209。

¹⁰⁴ Juraj Sajfert & Teresa Quintel, Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities (December 1, 2017), at 8-9. Cole/Boehm GDPR Commentary, Edward Elgar Publishing, 2019, Forthcoming, Available at SSRN: <https://ssrn.com/abstract=3285873> 該文獻指出，所謂「法律上反效果」，乃自動化處理將造成資料當事人之法律上權利受到負面影響，而「重大影響」則指 1.顯著影響資料當事人之處境、行為與選擇；2.對資料當事人造成長期或永久的影響；3.在極端狀況下，可能造成資料當事人被排斥或歧視。相關說明亦參照 Art. 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679: 18/EN, wp251rev.01, 6 February 2018, at 21. 翻譯參照張陳弘、莊植寧，註 55 書，頁 213。

¹⁰⁵ Juraj Sajfert & Teresa Quintel, *id.*, at 9-10.

¹⁰⁶ Juraj Sajfert & Teresa Quintel, *id.*

檔案內之個人資料本須依其性質遵循一般性或敏感性個資之要求，然就個資的「集合」本身，雖現行法未對此有何進一步要求，但仍應肯認個人資料檔案亦屬個資保障範疇。

第二項目的拘束原則

有學者整理指出，任何人對於他人個人資料的取得與使用，需取得當事人同意，或明定取得、使用的正當目的，方可為之¹⁰⁷。個人資料的流向通常經過「蒐集」、「處理」、「利用」三個階段，每一階段中再分辨「得否」及「如何」為之，各環節皆必須符合法律授權與正當目的要求；另外，三個階段的目的均需相同，如有目的外之蒐集、處理、利用，則需另有獨立法律授權依據，或取得當事人同意，方為適法，而不能以概括授權條款或組織法充之¹⁰⁸。本文以「使用」合稱所有個資的蒐集、處理及利用環節，探討卷證中個資在何情形下能被使用，又以何方式使用，並討論現行刑事訴訟法、個資法與相關法規是否已有充足的規範密度，並論及其改進之處。本文將於以下討論個資保護法制的重要核心原則，說明個資使用行為合法性的內涵。

目的拘束原則，或稱為目的限定(**purpose limitation**)原則，其內涵參照我國個資法第 5 條後段，指個資使用行為不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。在 2016/680 指令中有更細緻的說明，該指令前言第 26 節指出，所有個資處理行為對資料當事人都必須公平、合法且透明，並僅得依法律授權之目的為之；該特定目的必須合法且明確，所使用的個資亦須與該目的相關¹⁰⁹。該指令前言第 29 節並宣示，「個資的蒐集行為應在本指令範圍內，

¹⁰⁷ 李建良，資料流向與管控環節—個資保護 ABC，月旦法學雜誌，272 期，2017 年 12 月，頁 26。

¹⁰⁸ 李建良，註 107 文，頁 27-28。詳言之，依個資法第 2 條第 3 款，「蒐集」指以任何方式取得個人資料；同條第 4 款，「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；同條第 5 款，「利用」指將蒐集之個人資料為處理以外之使用。

¹⁰⁹ 原文為：「Any processing of personal data must be lawful, fair and transparent in relation to the natural persons concerned, and only processed for specific purposes laid down by law.」 「In particular, the specific purposes for which the personal data are processed should be explicit and legitimate and

依特定、明確且合法的目的為之，而就與刑事預防、調查、偵查、追訴或執行，包含對於公共安全威脅的保護與預防措施之目的，不相容的(*incompatible*)其他目的，則不應依其為之。若個資依本指令範圍內之目的，由相同或其他資料控制者進行原本蒐集目的外的使用行為，則該行為須經現行法之授權，且對於新的目的而言具有必要性及合比例性¹¹⁰」。該指令第4條第1項(b)款規定，會員國應規定個資應依特定、明確且合法的目的蒐集，且不得以與前述目的不相容之行為處理或利用；同項(c)款則規定，個資與其使用行為之目的間應具合理關聯，且不得超過此範圍為之。

目的拘束原則乃個資保護法制中最核心的基本原則。只有個資使用行為之目的足夠特定與明確，個資流向中各環節之相關人等才能預見使用的方式及範圍，不僅能實踐透明性與可預見性之要求，亦有助落實資料當事人之資訊自決權¹¹¹。目的特定的程度，不能空泛到僅以如「學術研究」稱之¹¹²，而需詳細到足以確定何種使用行為在此目的下會進行或不進行，並可用以評估應適用的法規範與資料安全維護措施¹¹³。

在目的拘束原則下，目的外使用個資行為乃原則禁止，僅在新舊目的具相容性(*compatibility*)時方被允許¹¹⁴。相容性要求的意義在於，新的個資使用行為除

determined at the time of the collection of the personal data. The personal data should be adequate and relevant for the purposes for which they are processed.」

¹¹⁰ 原文為：「Personal data should be collected for specified, explicit and legitimate purposes within the scope of this Directive and should not be processed for purposes incompatible with the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. If personal data are processed by the same or another controller for a purpose within the scope of this Directive other than that for which it has been collected, such processing should be permitted under the condition that such processing is authorised in accordance with applicable legal provisions and is necessary for and proportionate to that other purpose.」

¹¹¹ 張陳弘、莊植寧，註55書，頁124。

¹¹² 李婉萍，歐盟個資小組對「目的拘束原則」之詮釋及該詮釋對界定個資法上「特定目的」之啟發，科技法律透視，第25卷，第9期，2013年9月，頁24。

¹¹³ Art. 29 Working Party, Opinion 03/2013 on Purpose Limitation 2012, 00569/13/EN: WP 203 2 April 2013, at 15. 李婉萍，註112文，頁20；張陳弘、莊植寧，註55書，頁125。

¹¹⁴ Art. 29 Working Party, *id.*, at 20-23, 40. 張陳弘、莊植寧，註55書，頁127。翁逸泓，科技人權－全民電子通訊監察與個人資料保護，臺灣民主季刊，15卷，1期，2018年3月，頁19。翁清坤，大數據對於個人資料保護之挑戰與因應之道，東吳法律學報，31卷，3期，2020年1月，頁113。

需有合法事由外，新舊目的間還需具有關聯，否則若兩個合法但無關的行為間均可任意切換，將可能架空目的限制原則，故應就個案加以評估¹¹⁵；而依 GDPR 前言第 50 節，當目的外使用行為基於當事人同意，或為確保第 23 條第 1 項所定目的，如刑事預防、調查、偵查、追訴或執行，包含對於公共安全威脅的保護與預防措施，歐盟或會員國之司法獨立性或司法程序保障等，得例外無須進行相容性判斷，以兼顧資訊流通之公共利益¹¹⁶。而就刑事程序中目的外使用個資行為而言，在 2016/680 指令中，第 9 條第 1 項揭示，「依本指令之目的蒐集之個資不得為該等目的外之使用，但另有歐盟或會員國法律授權者不在此限。該等目的外使用行為應適用 GDPR 規定，但該等行為非屬歐盟法規範內者，亦不在此限¹¹⁷。」是故個資使用目的均會落入上開範圍，新舊目的之相容性判斷在此意義不大，惟須注意使用非本案卷證資料之問題¹¹⁸。

目的外使用行為仍須遵守目的拘束原則，無論是蒐集、處理、利用等任一環節均相同，而原則上目的外使用行為本身仍應具備法律授權，且與原蒐集目的具備相容性。然而，我國個資法第 16 條規定中，公務機關的目的外使用規範僅限於「利用」階段，卻不及於「目的外處理」，造成解釋不連貫與管制漏洞¹¹⁹；且該條文亦欠缺相容性要求之設計，對於新舊目的間關聯缺少一層把關機制，在刑事審判卷證中個資挪作刑事程序外之目的使用的情形，將可能產生容許範圍難以界定的解釋問題¹²⁰。

¹¹⁵ 依 GDPR 第 6 條第 4 項，相容性的詳細操作標準包括但不限於以下五項：新舊目的間之關聯性、資料當事人對新目的有無合理預期、是否涉及敏感性個資、對資料當事人可能造成之後果、有無適當保護措施，詳參張陳弘、莊植寧，註 55 書，頁 128-129；Maria Cristina Caldarola、Joachim Schrey 著、趙彥清、黃俊凱譯，註 94 書，頁 148-151。

¹¹⁶ 張陳弘、莊植寧，註 55 書，頁 127-128。

¹¹⁷ 原文為「Personal data collected by competent authorities for the purposes set out in Article 1(1) shall not be processed for purposes other than those set out in Article 1(1) unless such processing is authorised by Union or Member State law. Where personal data are processed for such other purposes, Regulation (EU) 2016/679 shall apply unless the processing is carried out in an activity which falls outside the scope of Union law.」

¹¹⁸ 此處可能產生三種情形，分別為 1. 刑事審判中使用另案卷證資料；2. 刑事審判卷證中個資挪作刑事程序外之目的使用；3. 非因刑事目的所蒐集之個資用於刑事審判卷證中。詳見第三章之討論。

¹¹⁹ 翁逸泓，註 114 文，頁 22、30。

¹²⁰ 張陳弘、莊植寧，註 55 書，頁 134-136；亦參見註 125 之說明。

第三項 資料最小化原則

資料最小化原則，意指個資使用行為應在必要性範圍內，以最小侵害手段為之，包含使用資料的量、資料的敏感程度、使用行為之方式，均應避免過度侵害當事人權益。我國個資法第 5 條規定，個人資料之蒐集、處理或利用，「不得逾越特定目的之必要範圍」，亦肯認此原則。在歐盟法上，GDPR 第 5 條第 1 項第 (c) 款揭示，個資使用行為應「適當、相關且限於處理目的所必要¹²¹」；然而 2016/680 指令對於資料最小化原則之要求則似乎相對寬鬆，其前言第 26 節僅指出，個資蒐集行為須與其目的適當且相關，而無不得逾越其範圍之說明；該指令第 4 條第 1 項第 (c) 款則指出，「個資應與其使用目的適當、相關，且不超出其範圍¹²²」。有文獻指出，兩者差異賦予 2016/680 指令中的資料控制者與使用者更多彈性¹²³。另有文獻進一步提出，該指令中留下的彈性空間，可能造成內國法化的過程中未能落實資料最小化要求，尚須仰賴監管機關之設置與運行¹²⁴。

有學者指出，法院卷證資料之製作與處理，亦應遵守資料最小化原則要求¹²⁵。其認為無論是檢辯雙方遞交法院的起訴書、答辯狀、告訴狀等，或由法院自行製作之裁判書等文書，均應檢視其在格式與內容中是否包含根本不需要的資料，從源頭減少使用當事人之個資，另一方面亦可減少法院行政負擔；而關於卷證資料之公開，則應考量對於當事人之隱私或其他利益(如更生保護)有無重大危害，在無助於達成公益目的之情形，應禁止公開¹²⁶。本文以為，此見解之可行性有待進一步討論，但至少點出法院在使用卷證中個資時，應注意資料最小化原則要求，

¹²¹ 原文為「adequate, relevant and **limited to what is necessary** in relation to the purposes for which they are processed」。粗體與底線為本文另加。

¹²² 原文為「adequate, relevant and **not excessive** in relation to the purposes for which they are processed」。粗體與底線為本文另加。

¹²³ Juraj Sajfert & Teresa Quintel, *supra* note 104, at 6.

¹²⁴ Thomas Marquenie, The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework, 33 Computer Law & Security Review 324, 331 (2017).

¹²⁵ 劉定基，第三人近用法庭卷證資料權利與個人資料保護的調和，國立臺灣大學法學論叢，第 49 卷，第 3 期，2020 年 9 月，頁 914。

¹²⁶ 劉定基，註 125 文，頁 914-917。

在必要範圍內為之。

個資儲存行為亦屬於使用行為的一種態樣，須符合最小化之要求。個資保存期間應盡可能縮短，至少不應超過其使用目的所需期間，而在到期後應將資料永久刪除¹²⁷。2016/680 指令第 5 條亦要求歐盟各會員國，對於以儲存之個資應設置刪除與定期審查之時限規定，並應搭配程序性規範以落實該等要求。該指令前言第 26 節亦指出，各會員國對於儲存期間較長之個資，應設置適當保護措施，以達成公共利益、統計或科學上、歷史上研究目的。依該指令第 9 條第 2 項，在刑事目的以外之使用行為，應符合 GDPR 規定；而 GDPR 第 89 條重申目的拘束原則與資料最小化原則要求，說明為實踐上開目的，應遵守技術上及組織上之保護措施，例如匿名化與假名化。

第四項 透明性原則

2016/680 指令前言第 26 節中亦揭示個資使用行為應遵守透明性原則，但其對「透明性」卻未進一步定義。有論者認為，透明性要求已落實於該指令中賦予資料當事人之權利，如第 12 條至第 14 條之資訊獲知權，使資料當事人得知悉其個資有何使用行為正在進行，更及於該使用行為之目的、法律基礎、資料控制者的身分、涉及個資的種類、資料的傳遞與接收方、儲存方式與期限等，藉由這些資訊，資料當事人才能就其個資行使其他權利，以落實資訊自決¹²⁸。但本文欲指出，這些權利還須經過內國法化才能落實透明性原則，而 2016/680 指令對於各會員國對資料當事人揭露該等資訊之方式及範圍等，均可能與指令條文有所不同。在刑事程序中，優先滿足透明性原則並不實際，否則將可能干擾犯罪偵查¹²⁹。例如在要求揭露資料使用者的決策邏輯與風險評估時，GDPR 第 15 條規定資料當事人有權取得上述資訊的副本，而 2016/680 指令則僅在其前言第 43 節中，將

¹²⁷ 張陳弘、莊植寧，註 55 書，頁 65-66。

¹²⁸ Thomas Marquenie, *supra* note 124, at 332.

¹²⁹ Mark Leiser & Bart Custers, *The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680*, 5 EUR. DATA PROT. L. REV. 367, 371 (2019).

此手段作為其中一個選項，二者的強制力與規範密度存有相當差異¹³⁰。

論者亦指出，不同個資使用行為的透明性原則要求，依個案亦將存有差異，此時個資法與個案中其他規範資料使用者行為之法律間關係即十分重要，因後者可作為前者的解釋參考¹³¹。揭露資訊的方式則需考量資料當事人之個人能力，以國外使用演算法自動化形成偵查行為決策為例，對資料當事人揭露該行為邏輯時，若以揭露演算法原始碼的方式為之，將使大多數不具專業知識的當事人縱然握有此等資訊亦無法解讀¹³²，故須以合理方式解釋，始能讓當事人有效率地知悉該等資訊，契合透明性之要求。

第三節 卷證中的個人資料及其使用規範要求

本文已經說明個資保護的一般合法性原則，接下來欲指出刑事審判卷證中含有大量個人資料，其種類與應受保護的規範密度，其對資料當事人的影響，以及其需符合前述的原則性要求。

第一項 卷證中包含個人資料

論者整理美國實證研究後指出，卷證中含有大量且多樣的個人資料，其中不乏敏感性個資，且刑事案件卷證中的個資明顯多於民事、非訟等其他案件，而在所有案件類別之卷證中出現頻率最高的個資種類，分別是位置資料、身份辨識資料(如社會安全碼、出生年月日等)及刑事程序資料(如曾被逮捕、判刑、假釋之紀錄)；由我國司法院之「裁判書遮隱規則」亦可推知卷證中含有豐富的個資：須由電腦與人工遮隱的個資，包含身分證字號、住址、生日性別、護照號碼、電話、金融帳號、車牌號碼、病例號碼，以及性侵害等敏感案件中可能足資識別當事人、證人、關係人的其他資料，如地緣關係、親屬關係、學經歷關係、職稱或稱謂等，

¹³⁰ Diana Dimitrova, *The Right to Explanation under the Right of Access to Personal Data: Legal Foundations in and beyond the GDPR*, 6 EUR. DATA PROT. L. REV. 211, 214 (2020).

¹³¹ Diana Dimitrova, *id.*, at 216.

¹³² 參見 2016/680 指令第 11 條與前開第二章、第二節、第一項、第四款個人資料檔案中的說明。

裁判書中的個資尚且如此，卷證中的個資必然更加完整、更能描繪特定人的輪廓；由上可知，無論在外國或我國，卷證中的資料皆與隱私或個資保護的範圍高度重疊¹³³。

卷證中的個資並不因其經由公開審判揭露後即喪失保護必要。或有實務見解從隱私保護觀點切入，認為已公開之個資因不再屬於隱私領域，而不須再受保護¹³⁴，此一傳統觀點已在現今遭受質疑¹³⁵，現行個資法規定亦不以個人資料屬於公開或私密領域作為保護與否的判準。就資訊自決權的角度而言，雖然卷證中的個資可能是由法院或偵查機關職權調查，或由告訴人、證人提供而呈現於法院，資料當事人對此並不一定有自主權限，但並不代表資料當事人對其個資的後續利用無權控制¹³⁶。對於法院的使用行為施加法律要求與限制，即屬於對資訊流通的管制，也保障了資料當事人的自主權¹³⁷。

第二項 卷證屬於個人資料檔案

卷證中個別的個人資料，可屬於一般性或敏感性個資，而受不同規範密度保護；至於卷證資料整體，因包含大量且多樣的個資，依一定規則系統性建立，且得以自動化機器或其他非自動化方式檢索、整理，本文認為其亦可視為個資法第2條第2款之個人資料檔案。

個人資料檔案的特殊性在於，經由系統性整理後的個資，不但可以被快速搜尋，更可以與不同案件卷證中的其他個資橫向連結，對既有資料產生新的解讀，藉此得出更清晰的個人輪廓。藉由累積多樣化的資料以獲取更全面的資訊，此類以小見大的現象，在美國法上以「馬賽克理論」稱之。以 GPS 行車軌跡紀錄為

¹³³ 劉定基，註 125 文，頁 902-903。

¹³⁴ 整理參見張陳弘，註 70 文，頁 92-95。

¹³⁵ 就算是已公開之個資，亦可能與其他資料結合，進而識別出特定個人，並藉此取得更多資料，或產生新的意涵，因此仍有保護必要，其使用行為仍應遵守相應規範。參見：張陳弘，已公開個人資料的隱私保護可能－司法陽光網引發的隱私保護爭議，法令月刊，67 卷，9 期，2016 年 9 月，頁 158-160；劉定基，註 125 文，頁 904。

¹³⁶ 劉定基，註 125 文，頁 904。

¹³⁷ 邱文聰，註 28 文，頁 174。

例，美國最高法院認為 GPS 行蹤資訊足以反映資料當事人之家庭、政治立場、職業、宗教甚至性生活等社會生活大量細節的紀錄，且政府機關可能儲存與利用該等資料，造成隱私權的侵害，且侵害範圍並不明確¹³⁸。美國法乃以合理隱私期待的角度，闡述細碎資料亦得以拼貼出個人生活圖像，造成「量變導致質變」的現象¹³⁹；就資訊自決權的角度而言，個人資料檔案藉由整理零碎的個資，交相堆疊後衍生出個資的其他意涵，是否與原來蒐集目的相同或相容，或已屬於目的外使用情形，而進一步之使用規範為何，均有待釐清¹⁴⁰。

本文以為，卷證中與個人有關的資料，宜以前述「資料關聯性」判斷其是否受個資保護，以將現今科技下資料更容易直接或間接識別個人的可能性納入考量，並贊同學者以「資料可識別個人之程度高低」替代過往「系爭資料是否屬於個資」的觀點，實質上呼應個資保護需求¹⁴¹，且在資料易於堆疊拼湊的使用背景下，應廣泛將該等資料納入保護，使其使用行為亦須受一定規範要求。就卷證資料之使用行為，本文認為，法院藉由個人資料檔案彙整細碎的個資，拼湊出資料當事人在某段時間中的行為，乃至於獲得資料當事人的生活樣貌，本屬審判活動中使用卷證，對資料當事人本人與其行為加以評價的正常現象；為了發現真實，法院藉由卷證經過系統化整理的特性，有效率地快速瞭解資料當事人，並作出正確的裁判，乃正常發揮卷證資料的功能。有疑義的是，若法院依訴訟目的外使用卷證資料，則同樣需尋求法律授權才能使該等行為得到正當性，但現行法規範下該如何解釋，即生問題。

¹³⁸ 蔡彩貞，定位科技在刑事司法程序之運用與人權保障——以利用 GPS 追蹤為中心，月旦裁判時報，65 期，2017 年 11 月，頁 65-68。

¹³⁹ 張陳弘，美國聯邦憲法增修條文第 4 條搜索令狀原則的新發展：以 Jones, Jardines & Grady 案為例，歐美研究，48 卷，2 期，2018 年 6 月，頁 290-292。

¹⁴⁰ 翁逸泓，註 114 文，頁 28。該文獻以「巨量資料之再利用」稱之，說明現今科技已能夠同時處理天文數字之資料，並出現連資料當事人本人都尚未知悉、甚至無法知悉的資訊，在此技術的應用中，經常可能發生個資原本蒐集目的以外的使用行為，而須考量目的限定原則與新舊目的之間的相容性。亦參考劉定基，大數據與物聯網時代的個人資料自主權，憲政時代，42 卷，3 期，頁 276。該文獻以「個人資料的累積效果」(aggregation effect)稱之，指出資料當事人雖經告知後同意，但在此現象下，其是否能充分掌握資料經累積、組合、比對、分析後的影響而為同意，殊值懷疑。

¹⁴¹ 張陳弘、莊植寧，註 55 書，頁 40-42。

第三項 現行法就卷證或個人資料檔案並無特殊使用規範

有鑑於卷證內個人資料的多樣性，使用部分或全部的卷證，往往涉及單項、多項個資或個人資料檔案的使用行為，但在個資保護原則與現行個資法下，使用行為中涉及個資的量的多寡，與要求的嚴格程度並無直接關聯，僅在所涉資料是否為敏感性個資時，個資法制上才設有較嚴格的使用要求。因此卷證的個人資料檔案性質，僅說明了卷證內資料更容易被查詢、組合、分析等情形，而該等使用行為範圍雖廣，但其應受何規範，仍以實際上使用的資料種類、資料控制者的地位，與資料當事人得主張的權利為斷。就本文研究範圍而言，卷證資料之控制者為法院，其為實踐審判目的，能夠依職權調查證據，或決定當事人得否、如何閱覽卷證等，對於卷證內個資有幾近全面的使用權限，而就訴訟外其他目的之使用，法院的權限則有待解釋。

目前刑事訴訟法上的卷證使用規範，對於程序內之人准予閱覽卷證或獲知卷證資訊，散見於被告、辯護人、鑑定人、告訴人與被害人等閱卷規範¹⁴²；對於卷證之管理，散見於第一編第五章之文書¹⁴³，各類型強制處分¹⁴⁴，以及偵審機關間、各審級間移交卷證之規定中¹⁴⁵，然而這些規範僅為偵審機關間職務分配之規定，至於法院具體如何使用卷證中個資，則仍無明文規範，又關於法院如何在訴訟目的外使用個人資料，刑事訴訟法亦無相關規定¹⁴⁶。需注意的是，法院若於訴訟目的外使用個資，此時即非居於審判機關、而是居於司法行政機關地

¹⁴² 刑事訴訟法中提到「檢閱」一詞，且與閱覽卷證相關的條文，如第 33 條、第 33 條之 1、第 205 條、第 258 條之 1、第 271 條之 1、第 455 條之 42 等。提到「獲知」一詞，且與閱覽卷證相關的條文，如第 33 條之 1、第 93 條第 2 項、第 93 條之 2 第 4 項等，而第 101 條第 3 項但書則規定，「依第九十三條第二項但書規定，經法院禁止被告及其辯護人獲知之卷證，不得作為羈押審查之依據。」

¹⁴³ 例如刑事訴訟法第 54 條第 1 項規定，「關於訴訟之文書，法院應保存者，由書記官編為卷宗」；第 2 項，「卷宗滅失案件之處理，另以法律定之」。

¹⁴⁴ 例如刑事訴訟法第 93 條第 2 項規定，偵查中檢察官應檢附卷證向法院聲請羈押。

¹⁴⁵ 例如刑事訴訟法第 121 條第 2 項、第 3 項規定，案件在第三審上訴中，而卷宗及證物已送交該法院者，羈押、羈押替代處分、其他關於羈押事項及關於限制出境、出海之處分，由第二審法院裁定之；而第二審法院於為此裁定前，得向第三審法院調取卷宗及證物。

¹⁴⁶ 林鈺雄，註 8 文，頁 201。

位¹⁴⁷，其使用行為之要求即應回歸個資法規範，若是訴訟外第三人為瞭解、監督司法權行使而主張近用卷證資料，亦可能適用政府資訊公開法與檔案法等規範¹⁴⁸。

本文以為，法院以訴訟外目的使用卷證中個資時，依現行法規架構，在不同的對象及脈絡下，相對應的法律之規範目的亦有不同，而需適用不同的法律，然而刑事訴訟法於此情形本就具有事務相近性，在立法論上應由刑事訴訟法設置特別規範，較能契合刑事審判卷證特殊之處。不過在現行制度下，仍應探究個資法、政府資訊公開法或檔案法規範，尋找法院使用卷證中個人資料之行為的法律依據，並檢視法院之行為既然適用該等規範，其運作上對個資的保護是否充足。



¹⁴⁷ 參見本文第一章第一項法院角色之說明。

¹⁴⁸ 劉定基，註 125 文，頁 899。

第三章 法院使用卷證中個人資料之行為

卷證中包含大量且多樣的個人資料，法院使用卷證的行為即是使用個資的行為，同樣須符合個資保護的原則。法院使用卷證的行為，應如何遵守個資保護原則，涉及使用行為的態樣，與該等行為的目的，決定其應受何種程度的要求。若將資料流向，即「蒐集」、「處理」、「利用」三階段¹⁴⁹，與審判時序結合觀察，法院在審判前與審判中，均可能以准許強制處分之方式，藉由調查證據以蒐集資料，使個人資料成為卷證的一部分，在審判中，法院將採擇含有個資的卷證內容，作為裁判基礎，即屬處理、利用，而在審判後，法院將對第三人公開裁判書，甚至亦可能公開卷證資料，並將卷證資料儲存於資料庫，亦屬處理、利用行為。

由法院進行審判程序的時序觀察，法院在審判前、中、後，使用本案卷證資料，各有不同行為態樣，這些行為可能合乎審判目的，亦可能與刑事審判目的無關，而屬於卷證中個人資料的目的外使用。是故本文將法院使用個資行為依其目的分為二大類，分別為「基於審判目的使用」與「審判目的外使用」。法院的任務雖在藉由審判程序發現真實、行使國家刑罰權，但法院使用卷證的行為，並非總是與審判目的相關；為了其他與行使國家公權力相關的目的，法院在使用卷證時仍須注意個資保護要求，惟此時需遵守個資保護的程度，即與基於審判目的之使用行為有所不同。

至於兩種目的間的轉換，乃目的拘束原則之例外。新目的下的使用行為亦構成基本權干預，且須有法律授權，新舊目的間亦須具有相容性，方屬適法。法院可能將原本與刑事審判無關的資料，納入卷證中作為裁判基礎，或將原屬卷證的資料，使用於與審判無關的事務，此時針對所涉及的資料敏感程度，或新的使用行為目的，法院亦應適用不同的行為規範。

¹⁴⁹ 李建良，註 107 文，頁 27-28。

第一節 基於審判目的使用

法院基於審判目的使用卷證，本來即是法院為達成其任務所進行的必要行為。本文並未將法院所有涉及卷證的行為進行地毯式的鋪敘，而欲以三種行為切入，說明審判中法院運用卷證時，其行為已經隱含個資保護原則，也必須符合該等要求。本文所採擇之行為，乃法院就「本案」審判行為所為，至於就「另案」之審判行為，涉及目的外使用卷證資料，將於本章第二節中說明。本文選擇的法院審判行為，乃「准許閱覽卷證」、「公開法庭錄音錄影」，以及「傳輸卷證資料」。簡言之，這三種行為分別涉及將卷證內容以不同方式，交給訴訟關係人與其他法院，此時本案法院皆須處理揭露內容範圍的問題，有些情況下容許職權判斷，有些則僅能依法律規定為之。這些行為均涉及資訊傳遞，資訊流向將經由法院送往他方，法院在此作為傳遞方，應對傳遞行為之合法性負責¹⁵⁰；本文認為法院雖因本案審判目的而進行傳遞，而有更重要之權衡利益，但不必全然排除個資保護，仍可適度兼顧該等要求。

第一項 審判中閱覽卷證之准許

第一款 閱覽卷證之人：被告、辯護人、程序中與程序外之第三人

閱覽卷證是被告行使防禦權的前提，唯有得知卷證內容，藉由行使辯護人之閱卷權、被告之卷證資訊獲知權，才能進行有效防禦。在聽審原則的要求下，應運卷證獲知需求而生的權利，尚有沒收程序參與人之代理人閱卷權¹⁵¹。使訴訟參與人獲知卷證資訊，亦可能為聽審原則以外的其他目的，在協助法院發現真實

¹⁵⁰ 詹鎮榮，公務機關間個人資料之傳遞－以臺灣桃園地方法院行政訴訟 102 年度簡字第 2 號判決出發，法學叢刊，第 60 卷，第 1 期，2015 年 1 月，頁 9。

¹⁵¹ 參見刑事訴訟法第 455 條之 21 第 2 項準用第 33 條第 1 項。在德國法上，被告或受干預人的「請求資訊權」(Recht auf Information)乃滿足其聽審權的第一步，唯有使其在審判前事先受通知，才得對受干預之情事進行有效防禦，參考林鈺雄，刑事訴訟法 上冊，8 版，新學林，2017 年 10 月，頁 168；王士帆，第三人沒收程序——評釋最高法院 108 年度臺上大字第 3594 號裁定，政大法學評論，163 期，2020 年 12 月，頁 12-13。

方面，鑑定作為證據方法之一，鑑定人亦得獲知卷證內容¹⁵²，以專業領域知識使法院能釐清事實；在立法政策面，則為賦予犯罪被害人程序參與人地位，使其得以瞭解訴訟經過與維護其人性尊嚴¹⁵³，而設置被害人之代理人閱卷權¹⁵⁴。在審判程序終結後，仍有訴訟參與人可能向法院聲請接觸卷證資料，例如律師受當事人委任聲請再審或非常上訴而聲請閱卷¹⁵⁵，此時法院准駁之決定，仍與審判相關，而屬司法行為。

在訴訟外的第三人欲獲知卷證資料，原則上已非屬法院於審判中的職權。該等第三人需先向法院聲明其欲接觸本案卷證的理由為何，確定其訴訟上之地位，進入訴訟程序內，法院才能在相對應程序的規定下，依法准駁接觸卷證資料的請求。至於其他在審判程序終結後，欲再使用卷證資料的情形，通常涉及卷證資料之目的外使用，此時法院已非依審判目的使用該等資料，容後敘明。

得請求閱覽卷證之人即屬法院可能提供卷證資料的對象，同時亦將取得卷證內的個資。關於法院得以使該等訴訟參與人獲知卷證內容的方式，見下款所述；而關於該等訴訟參與人獲知卷證資料後，得否再就此進行目的外使用行為，相關規定於刑事訴訟法上幾不可尋，僅有辯護人閱卷權有「不得就該內容為非正當目

¹⁵² 參見刑事訴訟法第 205 條第 1 項。

¹⁵³ 參見刑事訴訟法第 455 條之 38 立法理由二，「審判中訴訟之三面關係為法院、檢察官及被告。被害人訴訟參與制度係在此三面關係下，為被害人設計一程序參與人之主體地位，使其得藉由參與程序，瞭解訴訟之經過情形及維護其人性尊嚴。」

¹⁵⁴ 參見刑事訴訟法第 455 條之 42 立法理由二，「訴訟參與人雖非本案當事人，然其與審判結果仍有切身利益關係，為尊重其程序主體地位，並使其得以於訴訟進行中有效行使其權益，實有必要使其獲知卷證資訊之內容」，然而其亦揭示「本條則係為提升訴訟參與人及其代理人於現行刑事訴訟制度下之資訊取得權，使其得以獲知訴訟進行程度及卷證資訊內容之政策性立法」，與被告閱卷權之概念不同，故不以準用第 33 條的方式立法，而另定其行使方式。

¹⁵⁵ 過去實務裁判見解認為其屬司法行政範圍，參照梁哲璋，註 12 文，頁 389-390；然而該文獻亦說明，最高法院 108 年度台抗字第 1170 號刑事裁定指出：「至於判決確定後之刑事案件被告，固得依檔案法或政府資訊公開法之相關規定，向檔案管理機關或政府資訊持有機關申請閱卷，如經該管機關否准，則循一般行政爭訟程序處理；惟因訴訟目的之需要，而向判決之原審法院聲請付與卷證影本，實無逕予否准之理，仍應個案審酌是否確有訴訟之正當需求，聲請付與卷證影本之範圍有無刑事訴訟法第 33 條第 2 項應予限制閱卷等情形，而為准駁之決定。」本於合目的性解釋，舊刑事訴訟法第 33 條第 2 項「審判中」與法院組織法第 90 條之 1「該案件」，於當事人為再審而聲請閱卷時，應解為包含訴訟程序終結後，亦不限於本案範圍。本文同意此見解，認為其仍涉及被告訴訟權，而屬審判行為。另需注意者，現行刑事訴訟法第 429 條之 1 第 3 項已有準用同法第 33 條規定，再審案件之辯護人亦有審判中閱卷權。

的之使用」規定¹⁵⁶，告訴代理人準用之¹⁵⁷，自訴代理人、沒收程序參與人之代理人卻未準用該限制¹⁵⁸，鑑定人接觸卷證根本亦無設置相似限制，於體系上有紊亂之嫌。違反該規範之法律效果也付之闕如，可能僅得尋求刑法上業務洩密罪等處罰，而無較細緻之補救措施或罰則¹⁵⁹。

第二款 閱覽卷證之方式：查閱卷證與提供答覆

針對不同的訴訟參與人，因其與本案訴訟的利害關係不同，刑事訴訟法上設計使訴訟參與人得以接觸卷證的方式、範圍亦有不同，可以權利區別，概分為辯護人閱卷權與其他訴訟參與人之卷證資料獲知權。就獲知方式而言，辯護人的實質有效辯護乃被告得以防禦國家追訴行為的防線，使辯護人得以直接接觸所有卷證原本；被告、沒收程序參與人與被害人則與本案訴訟存在利害關係，其生命、自由、財產或人性尊嚴可能將因判決結果而首當其衝，而僅能透過辯護人或代理人轉知，至多請求法院付與影本，以間接方式獲知卷證內容。

就獲知範圍而言，辯護人原則上依刑事訴訟法第 33 條、第 33 條之 1，得接觸所有卷證原本，惟在第 33 條第 2 項但書情形，「卷宗及證物之內容與被告被訴事實無關或足以妨害另案之偵查，或涉及當事人或第三人之隱私或業務秘密者，法院得限制之。」第 93 條第 2 項但書則涉及「有事實足認有湮滅、偽造、變造證據或勾串共犯或證人等危害偵查目的或危害他人生命、身體之虞之卷證」，檢察官得聲請法院限制或禁止被告、辯護人獲知。本文以為，辯護人閱卷權不得任意受限制，以免違背聽審原則要求，此處乃例外、列舉的限制規定，閱卷範圍除上開情形外，其餘部分仍須照常使辯護人接觸全部原本。被告、沒收程序參與人之卷證資訊獲知權，經釋字第 762 號解釋指出，亦應及於全部卷宗、證物，以避

¹⁵⁶ 參見刑事訴訟法第 33 條第 5 項、第 33 條之 1 第 2 項。

¹⁵⁷ 刑事訴訟法第 271 條之 1 第 2 項規定，審判中告訴代理人準用整個第 33 條。

¹⁵⁸ 刑事訴訟法第 38 條、第 455 條之 21 第 2 項文字中，僅規定準用第 33 條第 1 項。

¹⁵⁹ 例如辯護人閱卷後就訴訟準備、攻防目的外使用卷證資料，對外界任意公布甚至加以評論，試圖引導輿論之行為，已有害於司法運作與公正性，參見邱忠義，我國妨害司法公正罪之再建構，月旦法學雜誌，265 期，2017 年 5 月，頁 19-21。該文獻同時指出，美、日、德等國就該等行為均設有刑罰，可供我國參考。

免造成無辯護人被告之歧視待遇，落實武器平等、正當法律原則¹⁶⁰，法院僅以付與影本方式為之，但範圍仍應及於全部卷證。至於被害人之卷證資訊獲知權，規範模式與第 33 條相似，就被害人本人未委任代理人或代理人非律師的情況下，僅得請求法院付與影本，其若有代理人，方得享有與第 33 條第 1 項相同權限。有論者指出，就舊法告訴人委任代理人閱卷之目的觀之，無非在獲取有助其心理回復與充實法院量刑的資訊，所有的被害人均可能有此需求，而不僅止於告訴人；新法第 455 條之 42 雖一般性地賦予被害人卷證獲知權，惟仍有缺點，如僅適用於審判中，偵查中之被害人不得主張，且有無委任代理人亦大大影響閱卷範圍，仍存在無正當理由之差別待遇¹⁶¹。最後，就鑑定人獲知卷證的範圍及限制，現行法仍無規定。

第二項 法庭錄音錄影公開與否之決定

就法院的職務角色而言，有文獻指出，是否交付審判期日錄音檔的決定，乃法官居於審判獨立地位所為，屬於審判行為，而非司法行政行為¹⁶²。依照刑事訴訟法第 44 條之 1 第 1 項，「審判期日應全程錄音；必要時，並得全程錄影。」現行「法庭錄音錄影及其利用保存辦法」第 2 條更細部地規定，法院審理刑事案件，於法庭或其他法規規定之處所開庭時，原則上應錄音，且於必要時得以錄影設備錄影；同條亦規定，法院行遠距審理、訊問開庭，應全程使用科技設備錄製視訊過程。依同辦法第 3 條，其他在庭之人原則上不得就法庭活動錄音錄影，但經審判長許可則不在此限。

論者整理指出，審判筆錄除為法院裁判基礎，亦為上級審檢視下級審之裁判與程序是否合法的重要依據，而由刑事訴訟法第 44 條之 1 的規定與立法理由可知，法庭錄音的主要目的僅為輔助製作筆錄，提升筆錄的正確性及完整性¹⁶³。

¹⁶⁰ 許願，註 23 文，頁 131。

¹⁶¹ 吳昭億，註 22 文，頁 32、38-39。

¹⁶² 梁哲璋，註 12 文，頁 312-313。

¹⁶³ 劉定基，法庭錄音的公開及其限制——司法獨立、司法課責與隱私保護，月旦法學雜誌，245

過去實務常常緊扣此目的，僅容許為輔助筆錄製作才願意公開錄音，公開對象僅限於當事人或依法得聲請閱覽卷宗之人，不包含一般社會大眾，方式亦以播放為主，而未將錄音內容交付予聲請人，以確保其無法散佈或公開¹⁶⁴。我國個資法於 2013 年修正公布後，更有實務見解以個資保護為由，因公開法庭錄音將洩漏參與法庭活動之人的個資，構成目的外使用行為，故如非為法律明定之輔助製作筆錄目的，應不予公開¹⁶⁵。

2015 年新增之法院組織法第 90 條之 1 立法理由二指出，交付法庭錄音錄影的目的亦在於「提升司法品質，增進司法效能」，不再以輔助製作筆錄為限。於 2021 年因應 COVID-19 疫情而修正之法庭錄音錄影及其利用保存辦法，亦明示法庭活動的錄音或錄影，目的在於「強化法庭活動之公平、公正與公開¹⁶⁶」，說明了實務上對此議題態度的轉向。至於法院錄音錄影內容向第三人，亦即向一般社會大眾公開，實務目前則仍採保留態度。在司改國是會議第四分組「第三人取得審判錄影帶、光碟的法制」議題中，法務部書面回應，法院審理之個案大多涉及兩造間個人法益侵害，且現行法院組織法第 90 條之 1 與法庭錄音錄影及其利用保存辦法均未規定第三人得聲請法院交付法庭之錄音錄影，此乃立法者價值選擇，以兼顧法庭公開與保護個人資訊，避免法庭錄音錄影內容遭人惡意使用，應予尊重¹⁶⁷。

由實務判決見解可一窺法院的立場。最高法院 109 年度台抗字第 1650 號刑事裁定指出，「法院對於參與法庭活動者實施錄音或錄影之主要目的在於輔助筆錄製作，顯係出於執行審判職務之目的需要，而法庭錄音或錄影內容載有參與法

期，2015 年 10 月，頁 151-152。

¹⁶⁴ 劉定基，註 163 文，頁 153。

¹⁶⁵ 參見最高行政法院 102 年度台抗字第 202 號裁定，以此為由拒絕交付法庭錄音光碟作為評鑑法官用途之目的，轉引自前揭註。本文以為，該判決見解適用目的限定原則的邏輯固然正確，但同時亦須注意該文獻之提醒，個資法為普通法性質，在當事人或利害關係人聲請交付光碟的情形，應適用法院組織法等特別規範，無須再以個資法判斷是否提供錄音。

¹⁶⁶ 參見法庭錄音錄影及其利用保存辦法第 2 條修正理由二。

¹⁶⁷ 法務部，司改國是會議第四分組「第三人取得審判錄影帶、光碟的法制」法務部書面回應，2017 年 4 月，頁 2-3，<https://www.moj.gov.tw/Public/Files/201705/7512101813709.pdf> (最後瀏覽日：2022 年 6 月 16 日)。

庭活動者之聲紋、情感活動等內容，涉及人性尊嚴、一般人格權及資訊自決權等核心價值，為憲法保障人民基本權之範疇，故其蒐集、處理及利用，應兼顧法庭公開與保護個人資訊之衡平性，避免法庭錄音內容遭惡意使用。」¹⁶⁸「刑事案件審判中，原則上應使被告得以適當方式適時獲知其被訴案件之全部資訊。此所謂之刑事案件之全部資訊主要包括『卷宗及證物』及『法庭錄音或錄影』二大部分。」而就後者內容，「因非屬卷宗及證物之範圍，被告無從循前開刑事訴訟法第 33 條第 2 項之規定請求付與，但法庭錄音或錄影內容，同為訴訟資料之一部分，可以用以糾正或補充法庭活動之筆錄紀錄，為提升司法品質及增進其效能」，當事人及依法得聲請閱覽卷宗之人，因主張或維護其法律上利益，可依法院組織法第 90 條之 1，聲請法院許可交付法庭錄音或錄影內容。

整理現行法制與實務見解，法庭錄音錄影制度的目的，仍以輔助筆錄製作為主，並導入落實當事人資訊獲知權之思維，而未承認第三人、公眾監督司法權運作等其他目的。聲請的要件亦有嚴格解釋，當事人須具體敘明理由，說明法院審理有何程序違背或法院筆錄疏漏等等，必須藉由法庭錄音光碟之交付，始足以主張或維護其法律上利益之理由，亦即須具備正當合理關連性¹⁶⁸。交付的方式則是將影音檔案存於光碟中並交與聲請人，而對於交付後聲請人的使用行為，法院組織法第 90 條之 4 設有目的外使用之限制與其行政罰。

本文於此處欲說明兩點。第一，實務見解雖認為法庭錄音錄影不屬於「卷證」，而屬於訴訟資料，但本文以為，實務上的筆錄既為法庭活動紀錄，不如逐字稿般詳盡，卻已包含許多個資，應遵循個資保護要求，錄音錄影技術乃地毯式地記錄審判活動，其中包含的個資只可能會更多，故本文認為不應囿於卷證之概念，而使法庭錄音錄影逸脫個資保護範圍，應將此制度亦納入討論。第二，公開卷證資料與交付法庭錄音錄影有所不同。其區別實益例如刑事訴訟法第 165 條第 2 項，卷宗內之筆錄及其他文書，若有關風化、公安或有毀損他人名譽之虞者，應交當事人、代理人、辯護人或輔佐人閱覽，不得宣讀；如被告不解其意義者，應告以

¹⁶⁸ 參照 106 年度高等行政法院法律座談會提案及研討結果 提案十一。

要旨。在此類情形僅公開法庭活動紀錄，未公開卷證資料時，即可保護他人名譽權、隱私權、資訊自決權等，兩種制度亦非互斥，法院應視個案情形靈活運用。

就個資保護的觀點而言，本文認為現行制度仍有改善空間。現行刑事訴訟法規定之法院錄音錄影，是基於輔助法院審判，並充實被告或其他關係人之救濟手段的立場，本文認為第三人欲取得該等影音資料，並不符合此處制度目的，無論第三人欲取得的目的為何，均屬目的外使用，應以法律特定事由為限，然而刑事訴訟法無相關明文，留下解釋空間。就聲請交付之要件而言，現今實務見解要求聲請人需先敘明筆錄有何違誤，才考量是否准許，然而聲請人對當時的記憶可能不完全清晰，需先取得影音光碟，才能比對審判筆錄與審判期日活動有無出入，有效率地指摘筆錄記載，制度上恐形成矛盾。有論者則認為，若當事人或關係人已符合「主張、維護權益所需」之要件，其獲得法院錄音錄影的必要性較高，所受限制應較低，以免妨害其行使訴訟權；法院於高度私密性之案件，如性侵害案件、家庭暴力案件、少年刑事案件等，亦應依個案情形裁量是否准許¹⁶⁹。

第三項 卷證資料之移交

法院審判案件，往往並非由單一審級法院即可完成整個審判流程。檢察官結束偵查後，獲得被告有罪之合理懷疑者，將該案件起訴意旨與全部卷證資料移交法院；在裁判後，若經當事人合法上訴，案件即發生移審效，下級法院須將卷證送交上級法院，此時移交的卷證範圍應為全部。法院移交全部卷證的行為對於審判權運作乃屬必須，且每一審級的法院均有機會傳輸全部卷證資料至下一審級¹⁷⁰，但大量的資料傳輸，也必然牽涉到個資保護。目前關於法院間的卷證資料傳輸與保管問題，學者多以「證物監管鏈」的角度探討，認為現行法規或實務上對於卷證保管的問題意識不強，在刑事程序中對於證物滅失亦無相應的規範與法律效果，應在法律密度上或科技技術上更注重證物的管理與保存，以確保證物

¹⁶⁹ 劉定基，註 163 文，頁 165。

¹⁷⁰ 最高法院也有機會發回更審，將卷證資料傳輸給更審法院。

之真實性、同一性，否則證物滅失或內容不完整將足以影響被告防禦權利與法院判決結果¹⁷¹。有學者指出，實務上將部分書證(例如帳簿)或物證(例如錄音帶)編入卷宗內，隨卷移送，卻有其他未編入卷內，亦隨卷宗移送的「外放」證物，通常由書記官點收與保管，而非登記放入贓證物庫，雖然給予法官方便，卻也潛藏證物遺失、被竄改或受潮消磁等風險¹⁷²。

綜上言之，「證物監管鏈」的制度目的在於保全證據，其構想由確保證物同一性出發，須保持證物的真實性與完整性，才能使被告與法院得以檢驗該證據，進一步提出有效主張，或發現真實；而本文認為，此制度另一個重要的附帶功能，即是保護證物中的個人資料，使其不致毀損或外洩，而構成個人資料破壞，額外損及資料當事人權益¹⁷³。實務上「外放」證物的作法，對其中包含的個資而言並非妥善的保存措施，未將該證物編入卷宗更不利其管理，亦容易造成法院卷證內容與實際包含的資料不一致，降低法院使用該卷證的效能，而資料當事人也將難以掌握其個資的控制者與控制範圍，造成該等個資完全逸脫資料當事人自主範圍的危險。

第二節 審判目的外使用

法院在審判外使用卷證中個人資料的行為，涉及另案審判使用與司法行政使用。在個資保護之目的限定原則下，二者均構成新的基本權干預，需有法律授權始得為之。在另案審判的情形，法院可能向其他法院、行政機關或私人依職權調查，該等對象控制之個人資料，均非為本案審判目的而蒐集；法院為司法行政行為時，因卷證資料本為審判而蒐集，若為司法行政目的而使用，則必然涉及目的外使用個資。此等目的轉換的情形，除須尋求另一合法性事由外，尚須注意該等

¹⁷¹ 林裕順，臺灣與日本證物保管法制之比較研究，檢察新論，28期，2020年8月，頁109-115；李佳玟，關於刑事案件贓證物保管的三點建議(上)，司法周刊，2014期，2020年7月，2-3版。

¹⁷² 李佳玟，註172文，3版。

¹⁷³ 法院對其保管之個人資料毀損(personal data breach)所衍生之義務，如通知當事人之義務、採取必要措施防止損害擴大的義務、記錄並保存相關事故的義務等，參見張陳弘、莊植寧，註55書，頁255。亦參見第四章第一節第二項之說明。

使用行為是否合乎比例原則，且須注意新舊目的間之相容性。

第一項 新的基本權干預與其正當化基礎

人民就其個人資料有權免於國家機關無限制地使用，而對此權利的限制，依法律保留原則，應有明確的法律授權基礎，且應遵守比例原則要求¹⁷⁴。若國家機關將逾越原本的授權規定，另為原本目的範圍外的使用，則構成另一個獨立的基本權干預事由，此時原有的法律授權已不能再作為新的干預行為之基礎，需要另尋新的干預正當化事由，否則該行為即屬違法¹⁷⁵。

針對新的干預行為的法律授權，個資法第 16 條規範目的外使用的合法性事由，但這些事由得否直接作為法院於本案審判外目的使用卷證中個資的正當化基礎，則生疑問。若法院基於另案審判目的而使用卷證中個資，此時法院仍居於審判機關地位，是否應受何種規範拘束其目的外使用行為？若法院基於司法行政目的而使用卷證中個資，是否得直接適用個資法第 16 條，作為其行為之授權依據？

在第一種情形，法院居於審判機關地位時，是否屬於個資法第 2 條第 7 款「依法行使公權力之中央或地方機關或行政法人」，而為公務機關？依照該條款，司法院轄下之各級法院為達成審判任務，似乎亦屬於國家為達成其任務設立之中央機關¹⁷⁶。觀察個資法整體法制，個資法第 53 條規定，法務部應會同中央目的事業主管機關訂定特定目的及個人資料類別，提供公務機關及非公務機關參考使用，其結果即是法務部發布之「個人資料保護法之特定目的及個人資料之類別」，共編列出 182 種特定目的，以便作為公告或其他相關作業之依據。其與本文討論較有關者，例如代號「○二五」為「犯罪預防、刑事偵查、執行、矯正、保護處分、犯罪被害人保護或更生保護事務」、「○三二」為「刑案資料管理」、「○五五」為「法院執行業務」、「○五六」為「法院審判業務」、「一七四」則為「其他司法行政」。本文認為由此可以反推，實務上將這些事項均歸屬個資法作用範圍，法院

¹⁷⁴ 林鈺雄，註 8 文，頁 205；亦參見本文第二章第一節之說明。

¹⁷⁵ 林鈺雄，註 8 文，頁 206。

¹⁷⁶ 財團法人資訊策進會科技法律研究所，註 75 書，頁 40。

居於審判機關時，亦屬於個資法上之公務機關，而適用該法第二章等規定。然而，具有審判獨立地位的法院，與具有行政一體上命下從性質之行政機關，適用同一套「公務機關」之規範，將造成權力分立下的法體系紊亂，是否妥適，殊值懷疑。本文以為，關於法院審判事務應尋求訴訟法規定，但在現行法並無明文的情況下，仍須參酌個資法規定，以符合個資保護要求。

在第二種情形，法院為司法行政機關地位時，亦受到行政作用法的拘束，此時屬於個資法上所稱公務機關無疑，得適用個資法第 16 條。然而有學者指出，個資法本身應為個資保護的基本法或程序相關規定，個別使用行為不能僅依個資法規定，還需要按照各該情形，依該領域的作用法明文授權，否則光以個資法第 16 條各款事由作為依據，例如「為維護國家安全或增進公共利益所必要」等，仍嫌空泛¹⁷⁷。就法院使用卷證中個資而言，除須注意有無明確法律授權外，還須注意該等法律之解釋適用上如何遵循個資保護原則。

目的外使用行為的正當化基礎，除了合法事由外，新舊目的間還須具備相容性，亦即新目的需相容於原始目的，以免後續使用行為對資料當事人的個資保護造成過度突襲，從而架空目的拘束原則¹⁷⁸。然而，法院對刑事審判卷證中的個資進行目的外使用，是否需判斷相容性要件？相容性概念本由 GDPR 第 6 條第 4 項規定而來，但刑事偵查、執行中的個資保護，應適用 2016/680 指令¹⁷⁹，而該指令中相對應的條文，第 4 條第 2 項，並未要求判斷新舊目的間之相容性，僅規定合法性事由，似乎降低目的拘束原則之要求¹⁸⁰。惟 AWP 29 於 2013 年之意見書中說明目的外使用行為時，曾以非刑事目的蒐集之個資轉作刑事執法目的使用

¹⁷⁷ 劉靜怡發言，邱文聰、吳全峰、劉靜怡、劉定基、翁逸泓，科技防疫與個人資料保護（下），月旦裁判時報，107 期，2021 年 5 月，頁 99-100。

¹⁷⁸ 張陳弘、莊植寧，註 55 書，頁 134-135。相容性的具體判斷標準，參見註 122。

¹⁷⁹ 關於 GDPR 與 2016/680 指令適用範圍的詳細說明，參見本文第四章。

¹⁸⁰ Catherine Jasserand, Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?, 34 Computer Law & Security Review 154, 164 (2018). 該條項原文：「Processing by the same or another controller for any of the purposes set out in Article 1(1) other than that for which the personal data are collected shall be permitted in so far as: (a) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and (b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.」

為例，並仍然實質進行相容性判斷，故在此情形下，新舊目的間之相容性仍為必要¹⁸¹。但論者認為就現行規範文義解釋，2016/680 指令第 4 條第 2 項僅要求合法性(legality)與合乎比例原則(propportionality)，取代了相容性的判斷，並未強調新舊目的間的關聯，宜透過歐盟主管機關再對此條文要件的解釋發布意見書，或由歐盟會員國在將指令內國法化的過程中再加入相容性要件，以解決此問題¹⁸²。

就我國法規範而言，有論者指出，現行個資法混淆「合法性事由」與「目的相容性標準」兩種不同概念，例如個資法第 15 條第 3 款之「對當事人權益無侵害」、第 16 條第 5 款之個資已去識別化、同條第 6 款「有利於當事人權益」，均無法導出正當利益的存在，因為這些判斷要素屬於目的相容性標準，而非合法性事由¹⁸³。現行法規範這些要素只需擇一成立，目的外使用行為即屬合法，但理論上該行為須具備合法性事由並通過相容性判斷，才具有正當性基礎。

在刑事程序法領域中涉及處理個人資料的議題上，刑事訴訟法與個資法規乃特別法與普通法關係，適用順序上，應先依照刑事訴訟法規定，若無規定再尋求個資法規作為法律基礎。是故，本文在探尋法院目的外使用卷證中個資的法律基礎時，亦先由刑事訴訟法著手，再參酌個資法規定。

最後，就當事人同意是否能作為法院於本案審判外目的使用卷證中個資的正當化基礎，本文將於本節第五項中說明。

第二項 另案審判使用

依刑事訴訟法第 163 條第 2 項，法院本有依職權調查證據之權限，其範圍依實務見解，以有利被告之事項為限¹⁸⁴，且該條項立法理由稱「在強化當事人進行色彩後之刑事訴訟架構中，法院依職權調查證據僅具補充性、輔佐性」，惟法

¹⁸¹ Art. 29 Working Party, *supra* note 113, Annex 4, examples 17 to 20, at 67-69; Catherine Jasserand, *id.*

¹⁸² Catherine Jasserand, *supra* note 180, at 164-165.

¹⁸³ 張陳弘、莊植寧，註 55 書，頁 136。

¹⁸⁴ 參照最高法院 101 年度第 2 次刑事庭會議決議。

院仍有主動調查證據之可能。近期最高法院具參考價值之裁判亦指出，「法院固得依職權調查證據，但並無蒐集證據之義務。法官為保全證據、沒收、追徵，雖得親自實施扣押，但在現行加強當事人進行主義色彩之刑事訴訟架構下，法院依職權調查證據僅居於補充性、輔佐性之地位，實施扣押仍以受聲請為原則」，乃對此議題再為闡釋¹⁸⁵。依法條文義及實務見解，法院調查證據之目的為發現真實，維護公平正義，而已有利被告之證據為限，法院此行為居於補充性地位僅在被告、檢察官雙方均未主張、聲請調查，而法院認為有必要時，才主動開啟調查。雖然此行為居於補充性地位而不多見，然而法院仍有此權限，亦屬於審判中目的外使用卷證中個資之行為，而需檢視法律授權之範圍及其正當化基礎。

依刑事訴訟法第 274 條、第 277 條及第 278 條，法院得於審判期日前調取或命提出證物、為搜索、扣押及勘驗，以及就必要之事項，請求該管機關報告。法院為了進行本案審判，可能將使用原本不是為了本案審判所被蒐集之個資，本文統稱為另案審判目的之使用行為，以強調法院此時使用了來自其他案件卷證中的資料，甚或原本不是出於刑事追訴目的而被蒐集的資料。本文認為其包含刑事審判中使用另案卷證資料，以及非因刑事目的所蒐集之個資用於刑事審判卷證等兩類情形。

實務上，本案與另案之刑事法院間、乃至於民刑法院間，遇有審判需求時，往往會互相調閱卷證，而現行刑事訴訟法上對此並無授權規範，僅有法院內部規則可循。至於非因刑事目的所蒐集之個資用於刑事審判卷證，法院應如何依法調查，本文亦將探討之。

第一款 使用另案卷證資料

實務上常見法院間互相調取卷證，採為本案裁判基礎，然此行為於刑事訴訟法幾無規範。本文認為或可由刑事訴訟法上關於審判中閱卷權、卷證資訊獲知權等之限制規定，例如第 33 條第 2 項「足以妨害另案偵查」作為限制事由，觀察

¹⁸⁵ 參照最高法院 110 年度台抗字第 1371 號刑事裁定。

立法者似乎預設偵查機關另案使用卷證資料的可能；但就審判機關而言，刑事法院如何使用其他法院的卷證，則無規定。

法院調取另案卷證的相關規範，目前僅見於法院內部行政規則，即「臺灣高等法院及所屬法院調卷處理要點」，但該要點內容僅是法院間調卷的作業流程。法院以進行審判任務、發現真實、實行國家追訴權等目的，能否作為其目的外使用行為的合法性事由？本文以為，依舉輕以明重之法理，偵查機關既有另案使用卷證的權限，法院也應有此權限；另一個切入點則可從個資法第 16 條，公務機關目的外使用個資的授權規定觀察，公務機關在法定職務範圍內，依該條第 1 款，於法律明文授權情形，或第 2 款「維護國家安全或增進公共利益所必要」情形下，得為目的外使用，可知法院的角色若依本文所述，屬於個資法框架下的公務機關，則法院進行審判乃是進行憲法授權之任務，且的確為增進公益所必要，其合法性固無疑問。

法院此處行為需否審酌的相容性？GDPR 雖要求相容性判斷，但 GDPR 同時亦將刑事司法事務交由 2016/680 指令規範，二者間互為補充性地位，而 2016/680 指令亦清楚指出，審判事務並非其適用範圍，應適用各會員國內規範¹⁸⁶。本文認為，法院於本案、另案審判間轉換的目的外使用行為，因前後目的都是審判，故相容性的判斷問題不大，但法院仍須注意比例原則要求。法院調取、使用另案卷證時，應注意資料最小化之要求，盡量僅使用與本案案情相關、本案審判所需之部分，其他無關之部分則不應納入。論者已有指出，將該原則應用於法院卷證上，需考量在個資使用的各環節中，均以審理所需之必要範圍為限¹⁸⁷。進一步言之，依照 2016/680 指令關於資料最小化原則的說明，本文認為應將該範圍解釋成「不超出審判目的」，以兼顧刑事追訴目的下法院所需之彈性¹⁸⁸。

本文以為，法院使用另案卷證的合法性，雖可由法理尋得，但仍需在刑事訴訟法中設置一般性授權規範。法院對於法理之解釋與實踐容有不同，而對於法律

¹⁸⁶ Thomas Marquenie, *supra* note 124, at 330.

¹⁸⁷ 劉定基，註 125 文，頁 914-915、919。

¹⁸⁸ 該指令第 4 條第 1 項第(c)款參照，詳見本文第二章第二節第三項之說明。

解釋則相對而言較少爭議；設置一般性授權規範，亦有助於在刑事訴訟中建立個資保護規範體系，使該等原則得以明確化。

第二款 使用非刑事目的蒐集之資料：以簡訊實聯制位置資料為例

日前有偵查機關聲請法院核發通訊監察書，以調取 1922 簡訊實聯制蒐集之當事人位置資料¹⁸⁹，而為超出防疫目的使用該等位置資料。此爭議涉及三個層次的問題，第一，行政機關以簡訊實聯制蒐集位置資料，有無法律授權；第二，偵查機關調取該等資料有無法律授權；第三，法院得否使用該等資料作為裁判基礎？本文設定主要欲探討第二與第三層次的問題，即偵查機關有無法源得調取非因刑事目的所蒐集之資料，法院又如何將該等資料納入卷證，作為裁判基礎。

在第一層次，簡訊實聯制將資料當事人手機門號之位置資料主動傳送給衛福部，屬於公務機關蒐集個資無疑，而此制度運作之量能十分巨大，依照國家通訊傳播委員會(National Communication Commission, NCC)之臉書貼文，總共有超過 47 億則簡訊發送並刪除¹⁹⁰，而此數字仍在逐日上升。如此廣泛而全面地蒐集資料當事人之位置資訊，對其隱私權、資訊自決權，一般行動自由等基本權，確已造成干預，但該等使用行為之法律授權卻十分模糊¹⁹¹。

在第二層次，儘管行政機關蒐集簡訊實聯制之位置資料的法源未臻明確，偵查機關與法院依通保法第 3 條之 1、第 11 條之 1 及其職權，仍得調查上開簡訊資料，本次爭議即在於偵查機關向電信業者調取該等資料¹⁹²。有論者批評，通保法規定僅倚賴重罪原則作為控制通訊監察書核發之手段，欠缺以個資保護作為

¹⁸⁹ 行政院於 2021 年 5 月間因應 COVID-19 疫情，為加快民眾出入公眾場所登記姓名、電話等資料的速度，推行「1922 簡訊實聯制」，透過以手機掃瞄 QR 碼，即可發送簡訊給 1922 專線，內容包含該手機門號、場所代碼與簡訊發送時間，且註明「資料僅供防疫目的使用」。參考廖緯民，1922 實聯制簡訊、通訊監察與個資保護，月旦醫事法報告，60 期，2021 年 10 月，頁 28。

¹⁹⁰ 國家通訊傳播委員會每周都會在其臉書粉絲專頁上發布貼文，說明自 2021 年 5 月 19 日簡訊實聯制上路起，至當周止，累計共蒐集、刪除之簡訊數量，並附註「電信事業依規定僅能留存簡訊實聯制資料 28 日，第 29 日前之簡訊資料應予刪除」；簡訊實聯制已於 2022 年 4 月 27 日終止，而所有簡訊資料據稱已在 2022 年 5 月 27 日刪除完畢，參照國家通訊傳播委員會，取自 <https://www.facebook.com/photo?fbid=385869756916824&set=a.350511723785961> (最後瀏覽日：2022 年 6 月 16 日)

¹⁹¹ 李榮耕，註 2 文；吳忻穎，註 2 文。

¹⁹² 劉世怡，註 3 文。

考量的有效限制¹⁹³；而就行政機關與偵查機關間的個資交換，有法務部函釋見解認為，應依個資法第 16 條但書所列合法性事由判斷，該等目的外使用行為是否屬之¹⁹⁴，亦有警察機關見解認為，警方因偵辦案件而向他機關索取個資，如有個資法第 6 條之情形，並於執行法定職務必要範圍內，難謂有違反個資法之虞¹⁹⁵。上開見解均試圖為偵查機關對於行政機關蒐集之個資目的外使用行為提供正當性基礎，卻僅以「法定職務必要範圍」逕認偵查機關已有法律授權依據，本文認為此依據並不足以作為合法性事由。蒐集犯罪情資本為偵查機關的職權，若再將該等職權作為蒐集行為的依據，將陷入循環論證中；若認為偵查機關之目的外使用行為乃為增進公益，本文以為，該行為亦應有法律明確授權，方符合法律明確性要求，縱使認為未臻明確之「公益」得作為目的外使用行為之合法性事由，該行為亦僅通過比例原則下合目的性要求，就其必要性與衡平性而言，仍為一片空白，因此實務上就該行為之解釋並無法說明其正當性。

綜上，本文認為此等目的外使用行為至少應另有法律授權方得為之，以符合個資保護原則下目的拘束原則之要求，該等使用行為並應符合比例原則。在我國法尚未完備的情況下，參照 2016/680 指令較完整之架構，刑事偵查機關須有明確法律授權作為合法性事由，以及符合比例原則，在此二要件下方得進行目的外使用行為。實務上，偵查機關得以調取簡訊位置資料，必然包含法院的允許及參與。本文認為，在第三層次，偵查機關向法院聲請通訊監察書時，法院即應審查，若允許偵查機關調查該等位置資料，造成目的外使用個資，形式上雖符合通保法之程序，但仍應尋求其他授權規定，並判斷防疫目的與刑事偵查目的間之相容性，以及考量該行為是否符合比例原則¹⁹⁶。法院應審酌，在現行法授權未臻明確、充足的情況下，偵查機關欲調取該等位置資料，是否涉及證據取得或使用禁止；

¹⁹³ 廖緯民，註 189 文，頁 30。

¹⁹⁴ 法務部(105)年法律字第 10503518090 號，轉引自廖緯民，註 189 文，頁 35。

¹⁹⁵ 新北市政府警察局刑事警察大隊，警方因偵辦案件向他單位索取個資，是否違反個人資料保護法？，取自 <https://www.cic.police.ntpc.gov.tw/cp-774-1995-28.html>，2013 年 2 月 22 日(最後瀏覽日：2022 年 6 月 16 日)，轉引自廖緯民，註 189 文，頁 35。

¹⁹⁶ 參照本文第三章第二節第一項，學者 Jasserand 對 2016/680 指令之批評。

縱使法院透過偵查機關取得該等個資，但本文認為，該等個資原為防疫目的所蒐集，現為審判目的而使用，法院若將原非因刑事目的蒐集之個資，納入卷證中作為審判依據，仍屬目的外使用，法院仍需尋求該等行為之合法性事由與判斷其相容性與比例原則。

第三項 司法行政使用

當法院居於司法行政機關地位時，因其行為已逸脫審判獨立範圍，不得再以此作為與個資保護權衡的衡量因素，法院此時地位與其他國家機關類同，可能將受到較高度度的個資保護要求。在學理上，廣義司法行政包含法院行政與狹義司法行政兩種目的¹⁹⁷，本文集中討論後者，若未特別說明，均指基於狹義司法行政目的之使用行為。

卷證資料本為法院審判以追訴犯罪之目的而存在，法院居於司法行政機關地位而使用卷證，例如對第三人公開卷證資料，通常屬於目的外使用行為¹⁹⁸。這些行為的目的不一，但通常含有公眾監督、司法課責等價值¹⁹⁹。於此分類下乃法官非居於審判獨立地位所為之行為，包括法院擔任刑事執行之權責機關所為者、對第三人聲請閱覽訴訟卷宗之決定、裁判繕本對第三人之送達、判決書面之公告、法院蒐集整理裁判書類供人閱覽、法院院長安排分配法庭室等²⁰⁰。本文欲討論與個資保護直接相關的行為，即裁判書公開與第三人查閱卷證之准許。

法院此時所進行的目的外使用行為，原則上均有個別法律的授權，而個資法

¹⁹⁷ 梁哲瑋，註 12 文，頁 315-316。該文獻指出，廣義司法行政包含法院行政與狹義司法行政，本文集中討論後者，僅在此對前者作簡略介紹。法院行政乃各個法院為了履行司法審判或行政任務所對內進行之人事、設備、資材等經營管理事務，包含整體人事管理行政(例如人員培訓、職務異動、懲戒權行使等)、職務組織建立運作(例如筆錄繕打安排、檔案管理等)與經費運用、會計統計等。此等事務因與普通法院間並無事務相近性之內在關聯，其救濟管道涉及公法爭議，應歸屬行政法院管轄。

¹⁹⁸ 范姜真嫻，政府資訊公開法於臺灣之實施狀況，行政執行／行政罰／行政程序／政府資料開放／風險社會與行政訴訟，元照，2017 年 1 月，頁 255。該文獻指出，第三人向政府機關合法聲請請求提供他人個資時，政府機關依政府資訊公開法提供他人個資給第三人，常應解為目的外使用，應進一步再依個資法第 16 條但書所列事由，判斷能否提供該等個資。

¹⁹⁹ 劉定基，註 125 文，頁 909。

²⁰⁰ 梁哲瑋，註 12 文，頁 313、439、442。

第二章「公務機關對個人資料之蒐集、處理及利用」的一般性規定亦補充適用。法院使用卷證的行為，若涉及其中個人資料，則需有特定目的方可為之；若涉及個資法第 6 條之「病歷、醫療、基因、性生活、健康檢查及犯罪前科」等敏感性個資，更需法律明文規定或授權方得進行。個資使用範圍亦應限於達成目的所必要者，以遵循資料最小化原則；並應使個資當事人知悉使用之方式、範圍、期限與法律基礎，以符合透明性原則。

第一款 裁判書公開

第一目 裁判書公開之制度目的

經過審判程序後，法官終於形成被告有罪或無罪之心證，或是否沒收犯罪相關財產之決定，而從卷證中整理所需資料，作成判決。判決書公開的正當性基礎，來自法治國原則下司法權之公共任務義務、民主原則和權力分立原則；經由判決可以瞭解民主呈現的立法決定，若無裁判公開，則無法達成對司法的公眾意見形成，亦難以促成公眾討論；法院裁判深深影響法律的具體化與法律的續造，甚至可與立法決定相較，因此人民應有機會瞭解法律的核心意義內容²⁰¹。

從公開審判的觀點而言，審判程序公開對此目的的助益相對有限，因為法庭的空間、開庭的時間限制，都減少了可以參與的人數，且當事人、訴訟關係人提出的書狀、證據等，現行實務下亦不會完全在審判中重現，而有賴裁判書中的記載²⁰²。綜上，裁判書公開是司法得受監督的第一步，亦屬於法院的重要任務。

雖然裁判書公開彰顯了透明性原則、司法監督的價值，但並非所有案件之裁判書均需公開。裁判書中並不僅有被告的個人資料，舉凡被害人、證人、告訴人、沒收程序參與人等訴訟關係人，從判決書中的資料均可能連結至該特定個人，因

²⁰¹ Arndt Sinn 著、吳瑛珠譯，裁判書公開於德國之實踐(上)，司法周刊，1926 期，2018 年 11 月，2 版。

²⁰² 劉定基，註 125 文，頁 887。該文獻亦進一步指出，裁判書僅記載經過法院整理的資訊，但一方面法院的整理、記載亦應為可受監督的事項，二方面裁判書僅記載卷證資料的部分內容，完整公開卷證資料將更有助民眾獲得全面的資訊。

此公開判決書所影響的資料當事人可謂相當廣泛。法院組織法第 83 條第 1 項以公開為原則，而以其他法律規定為例外，就案件類別而言，如兒少、性侵等案件因其特別法規定而不公開外，其他案件均公開當事人姓名²⁰³。同條第 2 項則規定公開範圍，「除自然人之姓名外，得不含自然人之身分證統一編號及其他足資識別該個人之資料」，原則上公開自然人姓名，但其出生年月日、身分證字號、住居所及其他足資識別該個人之資料，得隱匿之。依該條文於 2011 年之修法理由，其乃為平衡「人民知的權利」與「個人資訊隱私權」。論者認為由此可以肯認裁判書公開有助人民理解法規落實情形，進一步監督權力機關、透過民主程序影響改變法規的不足之處等²⁰⁴。

第二目 裁判書公開之個資保護：以當事人全名為中心

裁判書公開適用何種個資保護規範？在歐盟法層級，與司法權行使直接相關的事項，屬於歐盟各會員國的立法自主形成空間，歐盟並不以 2016/680 指令或 GDPR 直接干涉；以「刑事犯罪之預防、調查、偵查或追訴或刑罰執行」為目的之事項，適用 2016/680 指令，其餘與個資使用及保護相關事項則適用 GDPR²⁰⁵。裁判書公開屬司法行政之事項，並不屬於審判事務之司法權範圍，亦不屬於犯罪追訴或刑事執行領域，故仍適用 GDPR 規定。然而，若裁判書公開時，因內國法規定，而將裁判書內容中之個人資料匿名化或假名化，而達到去識別化、無法再連結至該特定人的程度，則此一公開的裁判書將被排除在 GDPR 保護範圍外²⁰⁶。

在我國現行法院組織法第 83 條第 2 項規定下，裁判書公開自然人姓名，無論被告、證人或被害人皆然，除姓名外之「其他足資識別該個人之資料」，則「得」隱匿之。現行實務往往將上開法條中例示的出生年月日、身分證字號、住居所地

²⁰³ 裁判書公開的範圍曾隨修法而變，本文討論以現行法制為主，過去流變可參見吳瑛珠，裁判公開的個資保護，月旦法學雜誌，294 期，2019 年 11 月，頁 126-128。

²⁰⁴ 吳瑛珠，註 203 文，頁 140。

²⁰⁵ 吳瑛珠，註 203 文，頁 137。

²⁰⁶ 吳瑛珠，註 203 文，頁 138-140。

址逐字以「○」代替，即為去識別化之措施。經過我國實務去識別化的裁判書，是否已因無法連結至特定個人，而排除個資法之保護？過去常見的論點是，裁判書中個資經公開後即不再受保護，或謂其中資料經去識別化後已非個資，因此不再受個資保護，是否有據？

就裁判書內容中之個資，已經公開者不受保護，乃過往基於隱私權於公開領域不再受合理保護的論述導出的結論，現行個資法已無採納²⁰⁷。就裁判書中資料已經去識別化而逸脫個資範疇，現行實務製作之判決書，雖然遮隱當事人之住址、車牌號碼等個資，但仍公開其姓名，與案情結合後仍得連結至特定個人，因此不符合歐盟法上的去識別化定義，亦未達到我國個資法施行細則第 17 條「無從識別該特定個人」的程度，故應受到個資保護。裁判書公開制度欲同時滿足公眾監督司法與個資保護兩個目的，今日制度的這番面貌於是以公開自然人姓名滿足前者，隱匿其他資訊以滿足後者，卻衍生問題。本文認為是否公開全名的問題具有代表性，故將聚焦於此部分討論。

在監督司法與保護個資的雙重目的拉扯下，現行實務作法的去識別化措施並不完全，並非屬於匿名化或假名化，而僅是形式上遮隱部分資料，對於達成這兩個目的都還有再改善的空間，尤其在裁判書大多於司法院網站公開的情況下，亦將使裁判書更容易連結至資料當事人，進而使侵害隱私權、資訊自決權，甚而受判決人回歸社會之一般人格權等風險升高²⁰⁸。

現行裁判書公開的範圍與方式，既無法在監督司法與保護個資間取得平衡，亦無法滿足兩者，或許尚待立法者作出價值選擇以解決²⁰⁹。在此之前，就個資保護的觀點，本文認為可參照論者於實務判決之法律鑑定意見²¹⁰，作為裁判書

²⁰⁷ 張陳弘，註 139 文，頁 158-160；陳起行，台灣法律資料庫及其個人資料之保護，法令月刊，59 卷，6 期，2008 年 6 月，頁 104；亦參見本文第二章第三節第一項之說明。

²⁰⁸ 吳瑛珠，註 203 文，頁 141-143。

²⁰⁹ 李惠宗，裁判書上網公開與個人資料自決權的衝突，月旦法學雜誌，154 期，2008 年 2 月，頁 33。

²¹⁰ 張陳弘，109 年度易更一字第 10 號鑑定書，取自

<https://law.judicial.gov.tw/FJUD/data.aspx?ty=JD&id=TCDM,109%2c%e6%98%93%e6%9b%b4%e4%b8%80%2c10%2c20210820%2c1> (最後瀏覽日：2022 年 6 月 16 日)。

公開範圍的判準。該法律鑑定意見涉及撤銷緩起訴公告之效力問題，其中對於撤銷緩起訴公告若列上受處分人全名，是否侵害隱私權或違反個資法，亦作出闡釋。本文認為，該鑑定意見雖非直接針對法院之裁判書公開而發，仍具參考價值，因為其揭示兩項重要觀點：其一，刑事訴訟法及其授權規範與法院組織法為個資使用之特別法，優先於個資法之適用；其二，公告資料當事人之全名，須符合個資使用之必要性要求，若完整姓名並非公告行為所必要，應屬違反個資法²¹¹。

本文認為上開鑑定意見中所謂符合個資使用之必要性，內涵等同於目的拘束原則之判斷；而檢視裁判書公開訴訟關係人之全名，是否為監督司法所必要，例如當事人全名有利於正確檢索裁判、提升監督司法的效率²¹²，或為保護當事人個人權益，而認為不得公開，端視此制度之目的究竟為何，然而本文以為現行法院組織法第 83 條的作法矛盾，立法者應作出更明確的價值選擇，以宣示裁判書公開的目的，如此一來解釋論上方得隨之劃定其公開範疇。

最後，在現行制度公開訴訟關係人全名的前提下，若欲減少對於資料當事人權益的影響，本文認為可由法官在撰寫裁判書時，將資料最小化原則納入考量，亦即在足以清楚交代案情的前提下，不使用過多的個人資料，從源頭保護資料當事人權益²¹³。

第二款 第三人查閱卷證資料

法院得否准許第三人查閱卷證資料，或將卷證對訴訟關係人以外之人公開？本文認為，前者指的是第三人聲請法院提供其知悉卷證內容，法院提供的對象為特定人；後者指的是法院對不特定人公開，如公開線上資料庫使大眾查閱等。在我國法上並無後者情形存在，第三人欲知悉特定案件之卷證內容，應向法院聲請

²¹¹ 張陳弘，註 210 文，頁 13。

²¹² 陳起行，註 207 文，頁 105。

²¹³ 劉定基，註 125 文，頁 915。在進一步制度設計的立法論上，另有論者認為，可由資料使用者身分進行分級管理，面對一般社會大眾時，公開徹底進行去識別化後之裁判書，在以會員身分才能登入之系統中，方提供完整的數位判決，參見陳起行，註 207 文，頁 107；亦有論者認為，可由案件所涉犯罪類型著手，若犯罪涉及個人隱私法益或為告訴乃論之罪，原則上不公開，參照李惠宗，註 209 文，頁 31-32。

之，本文亦將主要討論範圍設於前者。

第一目 所適用之法律

第三人欲向法院聲請查閱某特定案件之卷證，法院應依何法律處理之？108年度高等行政法院法律座談會曾討論：「判決確定之刑事審判卷宗及證物，是否為依政府資訊公開法第9條第1項請求公開，或依檔案法第17條請求應用之標的？」經投票表決，會議結論採否定說，其理由主要有四：第一，訴訟個案非屬公共事務，卷宗亦非因施政作為而生，不生一般性公開原則問題；第二，政府資訊公開法(下稱「政資法」)規定乃由行政程序法衍生而來，不適用於司法權作用下產生的資訊；第三，檔案法僅規範行政權所生之檔案，至於法院卷證如何應用，應以訴訟法規為準；第四，若現行法對刑事卷宗的利用、閱覽、保障有所不足，應由司法權主管機關提出修法解決，而非比附援引作用性質顯然相異之行政法規及其原理原則²¹⁴。

有學者則認為應依政資法規定，考量准許向第三人公開，其認為政資法第4條第1項所稱政府機關包含司法院及其轄下各級機關，而同法第3條所稱政府資訊亦包含法院用於審判之卷證²¹⁵。學者更進一步批評，上開實務見解忽視政資法第4條及檔案法第1條之立法理由，政資法與檔案法均適用於法院檔案²¹⁶；且法院之卷證資料雖因含有個資，而涉及當事人之隱私權、資訊自決權等私益，但此僅為該等資料得否限制公開的問題，而非全然否定政資法、檔案法之適用²¹⁷；最後，學者認為訴訟法規中對於卷證的保存、閱覽與滅失之處理雖有部分規定，然其目的主要仍在保障訴訟關係人之訴訟上權利，至於訴訟外第三人若欲近用卷

²¹⁴ 劉定基，註125文，頁896-897。

²¹⁵ 劉定基，註125文，頁896。

²¹⁶ 政資法第4條立法理由：「本法所稱之政府機關，包括所有中央、地方各級機關，意即除行政院及其所屬各級機關外，尚包括國民大會、總統府及其所屬機關、立法院、司法院及其所屬機關、考試院及其所屬機關、監察院及其所屬機關及各級地方自治團體之機關」；檔案法第1條立法理由：「為統一政府各級機關檔案管理制度，以利應用，明定本法適用範圍。至各機關因業務性質特殊，其案卷之管理已另有法律規定者，例如民事訴訟法第二百四十一條，刑事訴訟法第五十四條等，仍得適用其他法令之規定」。

²¹⁷ 劉定基，註125文，頁897。

證資料，則不在上述訴訟法規的規範範圍內，應回歸適用政資法與檔案法²¹⁸。

本文認為，上開學說批評實務決議見解，實屬有據。觀察政資法與檔案法的立法理由，立法者確實將法院卷證納入政資法與檔案法的規範範疇；本文亦認為，卷證公開與裁判書公開同樣具有監督司法的制度意義，若裁判書與卷證均予公開，法院形成心證的過程與結果均可受監督，若兩者資料結合，則第三人對該特定案件將有全盤掌握，監督的力道也隨之增強。就個資使用行為之透明性要求而言，揭露法院卷證資料亦有助於資料當事人掌握其個資被使用的情形；但就第三人得否向法院聲請揭露該等資料，本文則認為需進一步討論。最後，在適用法律的順序上，本文認為訴訟卷證之公開雖屬司法行政範疇，但仍需與訴訟法規為一體考量，以顧及法一致性，是故應先尋求刑事訴訟法規定，此時政資法、檔案法即居於普通法地位。無論適用何部法律，卷證公開涉及個人資料目的外使用行為，亦應同時符合個資法規範與個資保護要求²¹⁹。

實務上對於卷證資料公開，所適用的法規範層次，亦有不同見解。就刑事、行政法院審判權劃分的問題，最高行政法院 105 年 5 月份第 2 次、6 月份第 1 次庭長法官聯席會議分別針對告訴人及被告討論，「在被告之不起訴處分確定後，向檢察機關申請閱覽、抄錄該刑事案件卷宗，遭拒絕，循序提起行政訴訟，高等行政法院有無審判權限？」該決議結論認為，若告訴人與被告乃為再度進行刑事程序之目的，如再行起訴、告訴、告發或自訴犯罪等，或作為要求更正偵查筆錄或不起訴處分書所記載理由之用，且未引用政資法或檔案法為申請依據，則「此等公法爭議本質上屬廣義之刑事司法事務，應循刑事訴訟法之規定為救濟，高等行政法院對此公法爭議無審判權」；反之，若申請案中並無前述目的存在，且申請人引用政資法或檔案法為依據，則依行政訴訟法第 2 條規定，因現行法律對此爭議救濟程序無特別規定，應依循一般行政爭訟程序解決，高等行政法院對之有

²¹⁸ 劉定基，註 125 文，頁 899。該文獻亦認為，若現行制度適用上有未盡之處，最終應由立法者制定完整的卷證使用制度，但在此之前仍不得拒絕適用現有的法律。

²¹⁹ 本文認為，前註文獻未表明所謂「完整的卷證使用制度」應規範於刑事訴訟法中，或政資法、檔案法、法院組織法中，甚或另立專法。

審判權限。

對於刑事案件之被告，於案件終結後，如何再取得卷證資料，最高法院 105 年度台抗字第 830 號裁定即認為，「法院因受理刑事訴訟案件，於職權範圍內作成或取得之各種存在於文書、磁碟等媒介內之訊息，屬政府資訊公開法所指之政府資訊。」該裁定見解認為，於訴訟進行中，被告及其辯護人自得行使閱卷權，依刑事訴訟法及其相關規定辦理；於訴訟終結、判決確定後，訴訟關係消滅，相關卷證等政府資訊之檢閱或公開，已與被告訴訟權保障無關，而與被告法律上利益或保障人民知的權利有關，而因現行刑事訴訟法就此無相關規定，關於確定刑事案件卷證資訊之公開，除其他法令另有規定外，如新修訂之刑事訴訟法 429 條之 1 第 3 項準用同法第 33 條，使再審案件之辯護人得行使閱卷權，其餘應依檔案法或政資法之規定，向檔案管理機關或政府資訊持有機關申請辦理。

臺中高等行政法院 105 年度訴字第 126 號行政判決就台中地檢署抗辯提供已確定案件之警詢筆錄，將違反個資法，指出：「倘原告(按：當事人)合於申請要件，並無檔案法第 18 條得拒絕申請閱覽或政府資訊公開法第 18 條第 1 項應不予提供之情形，則被告(按：台中地檢署)依檔案法或政府資訊公開法規定，負有提供含有該第三人個人資料之政府檔案資訊的義務，自屬個人資料保護法第 16 條第 1 款『法律明文規定』得為特定目的外利用之情形。是以，被告依檔案法或政府資訊公開法規定，據以提供系爭筆錄(按：偵查之警詢筆錄)及錄音光碟給原告閱覽、抄錄、複製，符合個人資料保護法第 16 條第 1 款情形，非不得為之，自無違反個人資料保護法之規定。」

綜上，從上開裁判、決議見解可知，實務對於卷證資料公開的態度，仍限縮於訴訟關係人方得主張，而不及於一般性、全面性的卷證資料公開請求權。關於卷證公開之請求與准駁事務，實務亦肯認其屬於廣義刑事司法範疇，且卷證資料屬於政府資訊，在法理上，應依刑事訴訟法規處理，而在現行法欠缺此等規範的情況下，才由行政法領域之規範作為普通法之依據。

第二目 第三人查閱卷證資料的類型化

第三人查閱卷證資料在我國法上確有初步的法理基礎可循，作為開放的基礎，然而卷證中亦包含大量個資，個人資料的累積效果即不容忽視²²⁰。經由交互比對裁判書與卷證資料，不僅將大幅增加資料當事人被識別的機遇，亦可能在該當事人不知情的狀況下，由此勾勒出其生活圖像，而對其資訊自決權產生干預。刑事卷證本為審判目的所使用，第三人查閱卷證為目的外使用，其身分與查閱卷證的目的、方式、範圍等，在目的拘束原則要求下，均應於法有據。

我國政資法對於卷證資料採取限制公開的態度，但其出發點卻不全然為了個資保護，而是出於權衡國家追訴犯罪利益與個人受公平審判、隱私權的立場²²¹。政資法第 18 條第 1 項第 2 款規定，政府資訊「公開或提供有礙犯罪之偵查、追訴、執行或足以妨害刑事被告受公正之裁判或有危害他人生命、身體、自由、財產者」，應限制公開或不予提供，即為執法資訊之豁免公開²²²。論者進一步指出，本款包含三種類型，第一種為公開有妨害犯罪偵查、起訴等訴訟程序進行之虞，目的在於避免犯罪嫌疑人先一步濫用政府資訊公開制度，以規避法律制裁；第二種為公開有妨害刑事被告受公正裁判之虞，乃保障某特定刑事被告受公平審判的權利；第三種為公開將危害他人生命、身體、自由、財產，其範圍較廣泛²²³。本文以為，上開規定之目的亦得透過政資法第 18 條第 1 項第 1 款「其他法律、法規命令規定應秘密事項或限制、禁止公開」達成，因刑事訴訟法與偵查不公開作業辦法等相關規範此時應優先政資法適用²²⁴。

個資保護並非完全限制卷證中個人資料的公開與否，而是試圖在兩種價值間

²²⁰ 參見註 147 之說明。

²²¹ 參照政資法第 18 條立法理由一。

²²² 劉靜怡，政府資訊公開法第十八條研究，法學叢刊，60 卷，3 期，2015 年 7 月，頁 9。

²²³ 劉靜怡，註 222 文，頁 10-11。

²²⁴ 參照政資法第 18 條立法理由二：「依法核定為國家機密或依法律、法規命令規定應秘密之事項，符合法律保留原則，本為本法之特別規定，爰明定應限制公開或不予提供，以利適用」；政資法自 2005 年立法後即未再修法，而偵查不公開作業辦法為 2012 年公布施行，取代政資法第 18 條第 1 項第 2 款的部分功能。

取得平衡，就公開的範圍及方式層面，現行法對於第三人則無類型化的公開規範，而是由實務個案式的運用法理判斷，逐步累積見解。然而，司法實務並未普遍認可第三人向法院請求查閱卷證的一般性權利²²⁵，僅及於表示此等事務的審判權歸屬，進一步無此權利的規定，申請也就無疾而終，而類型化的卷證公開授權規範亦不存在。

法律除規定特定類型之第三人查閱卷證情形外，是否適宜再為卷證資料一般性公開之規定？本文以為，就現行法制發展，第三人查閱卷證欲全面開放，恐有實踐上的困難²²⁶，且其亦為目的外使用敏感性個資，本屬例外情形，應從嚴解釋，以法律有明文規定的類型為限，而不宜設置一般性的規定。延續此脈絡，本文欲討論類型化放寬第三人查閱卷證的可能。

第三目 學術研究使用

借鏡外國法，在歐盟法上，GDPR 及 2016/680 指令均肯認以學術研究作為目的外使用個資的事由。2016/680 指令第 4 條第 3 項規定，「相同或其他資料控制者所為第 1 條第 1 項之處理，得包含基於公共利益、學術研究、統計或歷史目的之使用，且應對資料當事人之權利設置適當保護措施²²⁷」，例如警察系統之統計資料，即是將依照該指令目的所蒐集的資料，轉換為內部行政目的使用²²⁸。該指令第 9 條第 2 項則規定，「主管機關依會員國法律授權處理個資，非屬本指令第 1 條第 1 項目的者，其使用或目的外使用行為自應遵循 GDPR 規定，包含

²²⁵ 劉定基，註 125 文，頁 918。

²²⁶ 有論者認為，可參考裁判書依案件類型公開的作法，在卷證資料也做相似處理，並舉美國法為例，參照劉定基，註 125 文，頁 915-917；李惠宗，註 209 文，頁 30-33。然而另有論者認為，卷證資料公開在我國尚屬發展中的制度，刑事卷證又尤具敏感性，宜以保守方式，採用正面表列、社會矚目案件優先的方式，較為穩健，參照劉定基，註 125 文，頁 919，註 136 之審查意見。

²²⁷ "Processing by the same or another controller may include archiving in the public interest, scientific, statistical or historical use, for the purposes set out in Article 1(1), subject to appropriate safeguards for the rights and freedoms of data subjects."

²²⁸ Giving a brief example of German police crime statistics ("Polizeiliche Kriminalstatistik (PKS)"), see Tristan Radtke, The Concept of Joint Control under the Data Protection Law Enforcement Directive 2016/680 in Contrast to the GDPR, 11 J. INTELL. PROP. INFO. TECH. & ELEC. COM. L. 242, 250 (2020).

基於公共利益、學術研究、統計或歷史目的之使用²²⁹。」此規定則說明，學術研究之使用行為不再屬於刑事執行目的，此一目的外使用行為應回歸適用 GDPR，而 GDPR 第 89 條即詳細列出資料當事人之權利清單，在學術研究之使用下相對應地受到何等限制²³⁰。2016/680 指令也僅就學術研究設置這兩條規定，本身未限制資料當事人之權利，而經由歐盟立法者的事務分配與制度設計，回歸適用 GDPR 處理。值得注意的是，GDPR 及 2016/680 指令均未規定研究者需為學術研究機構，GDPR 前言第 159 節指出，就算是私人研究者，只要具備要件與實行保護措施，亦可基於學術目的而使用個資，對此採取較寬鬆的解釋。綜上，歐盟立法例已經顯示，法院得基於學術研究目的，准許第三人查閱卷證，作為其中個人資料之目的外使用事由。

相較於歐盟法上將學術研究使用作為放寬目的拘束原則的特殊類型，設有明確的授權規範與相應的配套措施，我國法上並未就學術研究設有如此密度的規範。我國個資法第 6 條第 1 項第 4 款、同法第 16 條第 5 款、第 19 條第 1 項第 4 款則分別規定例外使用敏感性個資的事由、公務機關與非公務機關基於學術研究得例外使用之規定，「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」，文字幾乎相同。我國個資法僅將規制對象二分為公務機關與非公務機關，並未另外定義學術研究機構，有論者認為，學術研究機構應包含大學及其他以研究為專職之組織、機構，以免資料使用者、控制者藉學術研究名義規避個資法²³¹；另外，無論是資料提供者已經將個資去識別化，或由學術研究者取得原始資料，並

²²⁹ “Where competent authorities are entrusted by Member State law with the performance of tasks other than those performed for the purposes set out in Article 1(1), Regulation (EU) 2016/679 shall apply to processing for such purposes, including for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, unless the processing is carried out in an activity which falls outside the scope of Union law.”

²³⁰ 詳細整理與表格，參見楊智傑，歐盟、美國與臺灣個資保護法規中之研究利用，興大法學，26 期，2019 年 11 月，頁 30-36。

²³¹ 李寧修，個人資料合理利用模式之探析：以健康資料之學術研究為例，國立臺灣大學法學論叢，49 卷，1 期，2020 年 3 月，頁 18-19。本文欲指出，與 GDPR 規定相較，我國個資法雖規定學術研究之使用行為僅限於公務機關與學術研究機構，但並未將學術研究機構限定於公務機關，非公務機關之學術研究機構亦可屬之。然而我國法依照學術研究機構屬於公務機關與非公務機關，令其分別適用兩套規範，恐有違平等原則。

將個資去識別化後再發表，最終發表的研究成果必須符合前述個資法要求，即「依其揭露方式無從識別特定之當事人」²³²。

我國法律學術研究使用的實證資料，大多是以依法院組織法公開的裁判書、起訴書，以及其相關統計資料，例如「司法院及所屬各級法院之終結案件資料」即為司法院定期更新的統計資料²³³。至於卷證資料，如審判筆錄、偵查筆錄、甚至是被告之犯罪前科紀錄表等敏感性個資，得否作為學術研究素材，本文有如下意見：第一，刑事訴訟法、個資法與政資法在此均有適用，但僅有個資法對此有明文，而政資法將妨害執法、刑事被告受公平審判權利納入公開與否的權衡因素，應一併考量。第二，另有論者批評，基於學術研究使用行為要求去識別化，此任務原應由個資的原始蒐集者負擔，現行法放寬由原始蒐集者及學術研究者均得為之，增加洩漏風險²³⁴，而卷證資料往往包含大量敏感性個資，容易連結至特定個人，甚至勾勒出其生活圖像，其目的外使用行為應謹慎為之，法院若將卷證中的個資提供給學術研究機構，提供之範圍、方式皆應有特別授權、明文規定。第三，學術研究作為目的外使用之事由，並非完全豁免此使用行為，法院與學術研究機構仍應具備個資使用的正當化基礎，並為適當保護措施²³⁵，而最終亦應達成我國法上去識別化之要求。

第四項 已確定案件之卷證中個資之使用與保護

第一款 論題聚焦

本文至此已經初步整理法院使用卷證中個資行為之態樣，以及該等行為之授

²³² 李寧修，註 231 文，頁 19-20。

²³³ 林常青，台灣法律經濟學實證的探掘資料——介紹與應用，經濟論文，47 卷，4 期，2019 年 12 月，頁 536-539。

²³⁴ 翁逸泓，開放全民電子健康資料加值應用之個資保護問題——以英國經驗為例，月旦法學雜誌，285 期，2019 年 1 月，頁 152。

²³⁵ Art. 29 Working Party, *supra* note 113, at 28. 楊智傑，註 230 文，頁 16。另有論者指出，此要求在我國法上相對應者，乃個資法施行細則第 12 條所稱「公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，而採取技術上及組織上之措施」，參見樓一琳、何之行，個人資料保護於雲端運算時代之法律爭議初探暨比較法分析：以健保資料為例，國立臺灣大學法學論叢，46 卷，2 期，2017 年 6 月，頁 375。

權規範，並觀察其中存在規範密度不足的問題。本文欲再聚焦法院於審判目的外之使用，居於司法行政機關地位，提供第三人查閱卷證之部分，進行深入的論述。本文選擇此區塊的理由如下：第一，法院在審判目的下使用卷證，本為其職權，亦屬憲法所賦予之重要任務，無論是在本案或另案審判中使用卷證皆然，雖然法院行為需要更細緻的授權規範，但實務以解釋現行法規的方式為之，本文以為尚不屬於法律漏洞，故為節省篇幅，暫不處理此問題。第二，本文已經交代裁判書公開制度的核心問題，不在制度設計的缺失，而在於公開裁判與保護個資兩種價值未能達到平衡，使現行制度左支右絀，故不再更深入評析裁判書公開之制度，但在概念體系上仍會在後續論述中提及。第三，本文認為現行文獻多著重於以政府資訊公開的角度分析卷證資料之公開²³⁶，與分析敏感性個資，特別是健保資料，應如何公開²³⁷，二者間交集較少²³⁸；本文由法院作為司法行政機關時，在需依法揭露卷證資料的情況中，討論現行法制賦予法院哪些揭露方式，以有效踐行卷證中的個資保護。

法院揭露尚未確定案件之卷證資料，是否於法有據，尚有疑問，且同時涉及法院作為審判機關與司法行政機關兩種地位之切換，為使討論更加聚焦，本文將討論範圍限於已確定之案件，法院原則上對此不再具審判機關地位，討論重心較能集中於法院的司法行政機關角色。於本章中，本文將先說明法院居於司法行政機關地位時，得適用哪些法領域的授權規範；本文將再說明已確定案件之卷證，更精確的範圍為何；之後梳理前一章中提及依法需公開卷證之情況，並依揭露對象為訴訟關係人、學術研究單位及一般大眾之第三人分別說明；最後評析法院依法公開卷證時，現行法制如何同時兼顧個資保護要求，及其不足之處。

第二款 法院對已確定案件卷證之角色

在我國法上，刑事訴訟法對於卷證中個資之使用，僅有未臻完整的閱卷權規

²³⁶ 如劉定基，註 125 文；劉靜怡，註 222 文。

²³⁷ 如邱文聰、吳全峰、劉靜怡、劉定基、翁逸泓，註 177 文；楊智傑，註 230 文；李寧修，註 231 文。

²³⁸ 如劉定基，註 125 文。

定，且缺乏對於已確定案件卷證使用之規範，而需尋求法院組織法、政府資訊公開法、個人資料保護法等公法領域規範。然而，已確定刑事案件之卷證有其特殊性，其中包含大量敏感性個資，例如被告之全國前案紀錄表，或證人之驗傷證明等，即屬個資法第 6 條所稱「犯罪前科」、「病歷、醫療、健康檢查」等個資，再加上卷證經過系統性的整理、編碼，具有能夠在同一案件之卷證中，甚或在不同案件之卷證中交互比對之功能，而屬於個資法第 2 條第 2 款所稱「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」，屬於個人資料檔案。個資法或政資法關於資料公開之設計，立基於行政機關之政府資料公開²³⁹，對於司法機關之資料公開，則屬於其邊陲地帶，多透過解釋或實務見解累積的方式為之，而法院組織法關於公開裁判書與法庭錄音錄影之規定，又未見與前述法規有整合的跡象，而是各行其政，亦無法回應制度上的空白。

綜上，法院考量已確定案件卷證中之個資使用，本文認為雖然就該案件而言，已卸下審判者地位，惟該等事務仍涉及法庭活動，乃至於法院形成心證、作出裁判的外在過程，與審判高度相關，一般性的法規適用於此將有不足之處，宜透過特別法完整規範，提供法院明確的授權規定。

第三款 卷證之範圍

已確定案件之偵查、審判活動業已結束，其卷證資料範圍原則上也不會再變動。卷證於刑事訴訟法中無明確定義，其範圍相當廣泛，除了書面的卷宗與實體證物外，實務見解曾認為檢警偵訊時之錄音錄影、法院庭期中之錄音錄影等法庭紀錄，亦屬卷證²⁴⁰。

裁判書不屬於卷證，然其內容乃本於卷證所產生，故本文亦納入討論。裁判書內容的範圍比卷證小，但裁判書中的個人資料經由法官揀擇，呈現出案情經過，

²³⁹ 在政資法上，一般行政機關的資訊公開與執法機關的資訊公開，即屬原則與例外關係，參照劉靜怡，註 222 文，頁 9-11。

²⁴⁰ 參照第三章第一節第二項之說明。需注意的是，實務此見解乃基於「交付法庭錄音錄影予訴訟關係人屬於審判行為」而作，但關於訴訟外第三人聲請獲知法庭紀錄時，是否仍為相同解釋，實務則未說明。

相較於龐大的卷證，更加容易交互比對其中的個資，是故本文認為，裁判書公開對資料當事人之影響，並不亞於卷證公開。

第四款 卷證資料公開與個資保護

實務見解認為，已確定案件之法庭紀錄屬於卷證，其公開涉及法院組織法、個資法、政資法、檔案法等法領域，其中法院組織法應屬特別法，而優先適用；在判斷是否公開時，還需進一步考量聲請人是否屬於該案件之訴訟關係人，或僅為一般大眾之第三人；就現行法上制度與評析，本文前已說明，不再重複²⁴¹。本文於此欲再補充說明的是，卷宗與證物公開的方式。對於已確定案件的卷證，如何分層提供資料供第三人查閱，又卷宗與證物公開方式有無不同，以下說明之。

第一目 卷宗公開之方式

就審判中之案件而言，我國現行刑事訴訟法上公開卷宗的方式，本文依公開的範圍，分為全卷或部分公開，依公開之客體，則可分為卷宗原本或影本，而法律則依照各該訴訟關係人獲知卷證的需求強弱、與本案判決結果的利害關係等，就範圍與客體進行排列組合。例如就辯護人之閱卷權而言，原則上為全卷、原本之公開，而例外遭限縮時則可能為部分、影本之公開；就被告或被害人之卷證資訊獲知權而言，則可能為部分、影本公開。

就已確定之案件而言，在我國現行法上，實務認為其卷宗公開之方式可能因受判決人欲聲請再審或非常上訴等救濟，而準用或類推適用刑事訴訟的閱卷權規定；至於其他訴訟關係人或學術研究單位，地位則與一般大眾之第三人相同，實務並未肯認其請求卷證公開之權利。

已確定案件卷證資料公開的空間雖然有限，但仍有此可能。本文從資訊分層的角度說明「全卷或部分」、「原本或影本」兩組公開方式的差異，仍有實益。法

²⁴¹ 參照第三章第一節第三項第二款之說明。

院考量卷宗公開之方式時，卷證中的個資保護往往不是主要因素，充其量僅為一項反射利益。然而，法院使用卷證資料，在達成其目的的前提下，亦應注意以最小干預手段為之，符合目的拘束原則、資料最小化原則。

第三人聲請近用卷證的目的不同，法院亦須審酌卷證公開之範圍。有學者從類型化的觀點切入，認為卷證公開首須於法有據，並適宜依照不同情形分別規範全部或部分公開，例如依案件類型、或採正面表列的規範模式等²⁴²。本文欲再進一步補充，刑事卷證中包含大量敏感性個資，不僅屬於被告，亦可能屬於證人、被害人等，法院審酌是否提供第三人卷證時，就第三人取得卷證後是否可能進行不當之目的外使用，雖非法院主要考量的原因，但本文認為，亦應將此因素納入考慮，第三人聲請近用卷證，是否有何特別重要的利益，並與卷證中資料當事人之利益進行權衡。

提供原本或影本，所考量者應為保全卷宗，而限制與本案具利害關係之聲請人接觸卷宗原本。本文以為，在現行實務已漸漸推廣使用電子卷宗的情況下，卷宗的潛在危險不僅有原本滅失，卷宗之影本或副本具有易複製、改動的特性，進而導致其真實性可能受質疑。雖然這些問題在技術上可被克服，但對於卷證中個資遭第三人再為目的外使用，現行法上缺乏有力的監督或處罰機制，亦造成實務上對於提供第三人卷證資訊採取保守態度。

綜上所述，本文認為公開卷證的方式應保持一定彈性，並非全有或全無，而得藉由全卷或部分、原本或影本的操作，使法院得以在個案中運用較多手段靈活裁量。

第二目 證物公開之方式

本文認為，證物公開的方式，與卷宗公開大致相同。然而，證物因其自身特性，可能具有不能長期保存的特質，例如刑事訴訟法第 140 條、第 141 條所稱，

²⁴² 參照第三章第二節第三項第二款第二目之說明；劉定基，註 125 文，頁 915-917；李惠宗，註 209 文，頁 30-33。

扣押物有不便搬運、易生危險、有喪失毀損或減低價值之虞、或不便保管、保管需費過鉅等情形；或依沒收制度，於案件確定後，依刑法第 38 條之 1 第 5 項、刑事訴訟法第 473 條發還被害人等情。此時證物原件在事實上或法律上不能留存於國家機關，而僅可能查閱該等證物在卷宗中之描述或紀錄，以取得其外觀、數量、特徵等資訊。

在直接審理原則下，考量法院直接接觸證物以獲得較強心證的需求，證據替代品乃居於例外地位，僅在原件無法近用等法定特別情況下，方得使用。然而，在提供第三人近用卷證資料時，證據替代品是否仍屬原則禁止，本文認為與前述卷宗公開的考量相同，不再重複。

案件確定後，我國法上對於證物如何管理幾乎無明文規範，僅於刑事訴訟法第 317 條設有扣押物發還之相關規定。除應依法沒收者外，其餘證物是否、如何留存，是一個值得探討的技術問題。本文於此欲探討的是，若證物有提供原件供聲請人查閱的可能，其前提則為我國有運作完善的證物監管制度，不僅是在案件進行中原則需留存原件，在案件確定後，於可供檢證的程度內，仍視情況留存原件或書面、電子紀錄，以供聲請人查閱。

第五項 資料當事人之告知後同意

在個資法的架構下，資料控制者若欲就資料當事人之個資進行目的外使用，可告知該當事人後取得其同意，以此「告知後同意」作為合法性事由。是故在法有明文規定下，資料控制者負有告知義務，同時需取得資料當事人的真摯同意，其使用行為方屬適法。涵攝至本文研究主題，法院目的外使用卷證中的個資時，尤其是已確定案件之卷證，是否負有向資料當事人之告知義務？法院在何種情況下，得以取得當事人之同意？本文將嘗試從現行法與原理原則提出解釋與看法。

第一款 告知後同意的意義與適用範圍

在特定情形下，告知後同意可以作為個資使用行為的正當化基礎。歐盟基本

權利憲章第 8 條第 2 項明定，「個人資料僅得基於當事人同意或其他法律規定的合法原因，為特定目的，公平地被蒐集、處理與利用²⁴³。」其最主要的意義與功能在於落實資料當事人之資訊自決權，當事人得自由決定其個資是否交由他人使用、交由何人使用、使用之目的、方式、範圍等，資料控制者就此需事前取得當事人同意²⁴⁴。

相較於其他合法性事由，還需加上使用行為之「必要性」要件，方成為正當化基礎，當事人同意本身即可作為正當化基礎，無須再考量個資使用行為的必要性，因當事人已行使其資訊自決權²⁴⁵。資料控制者使用個資時，若無其他法律授權，亦得尋求資料當事人之同意，作為使用行為的正當化基礎。同意與其他法律授權之正當化基礎並非互斥關係，而得以並存，但每一種個資使用行為都需考量其使用目的、個別事由之適用範圍等，選擇合適的法律基礎，不宜逕以取得當事人同意作為優先手段²⁴⁶。

有學者指出，同意的機制在公私部門扮演的角色不同，在私部門規範體制下，當事人同意居於核心地位，例如消費者的個資保護機制，即賦予當事人較多協商空間；但在公部門規範體制下，其較少依賴取得當事人同意作為正當性基礎，而較依賴立法者設置例外之強制規定，賦予公務機關得不經當事人同意而使用個資之權限²⁴⁷。實際上，取得當事人同意相對而言亦將阻礙公務進行，並增加公務成本，當公務機關無法適用任何一項除外條款之授權，或欲強調取得民眾「共識」時，才會尋求當事人同意²⁴⁸。

在刑事追訴的脈絡下，尤其是在 2016/680 指令的規範目的範疇，資料當事人之同意並不能單獨作為個資使用行為的正當化事由。依據該指令第 8 條第 1 項，個資使用行為的合法性事由僅有「執行刑事追訴之必要」，意即符合該指令

²⁴³ 翻譯參照劉定基，註 51 文，頁 148。

²⁴⁴ 洪家殷，註 7 文，頁 49；劉定基，註 51 文，頁 148、162。

²⁴⁵ 張陳弘、莊植寧，註 55 書，頁 85-86。

²⁴⁶ 劉定基，註 51 文，頁 149；張陳弘、莊植寧，註 55 書，頁 90。

²⁴⁷ 翁清坤，告知後同意與消費者個人資料之保護，臺北大學法學論叢，87 期，2013 年 9 月，頁 245-246，註 103。

²⁴⁸ 同前註。

第 1 條第 1 項之規範目的，才得作為該行為之依據²⁴⁹。該指令第 8 條第 2 項亦重申目的拘束原則，揭示在刑事目的下，會員國法律應至少清楚規範使用行為的目的、欲達成的結果，及所涉及個資的範圍。2016/680 指令在其前言第 35 節中更詳細說明，「預防、調查、偵查或追訴刑事犯罪或執行刑罰，乃法律賦予主管機關的制度性權力，使其得以要求或命令自然人。在此情況下，GDPR 中規範之資料當事人同意，不應成為主管機關使用個資的正當化基礎。當資料當事人被要求遵循一項法律義務時，其並無真摯、自由的選擇餘地，故資料當事人的反應並不能被認為是出於自自由意志表示同意²⁵⁰。」其前言第 37 節說明敏感性個資之使用，亦指出當資料當事人明確同意會對其造成侵擾的個資使用行為時，該等行為亦為法所許，但其同意本身不得作為主管機關使用其敏感性個資的正當化基礎²⁵¹。有學說亦指出，依刑事目的而為之個資使用，在本質上即難以取得資料當事人同意，因當事人不僅難以掌握偵查機關使用其個資之情形，就算其得掌握，於法律上也難以行使其權利，故實際上難以取得有效的當事人同意²⁵²。

然而，若為刑事目的外使用之行為，則應回歸適用一般性之個資使用規範，依一般性或敏感性個資之使用規範分別處理，當事人同意此時即得作為正當化基礎。法院使用已確定卷證中個資之行為，尤其是考量是否、如何提供予第三人，已與刑事目的之使用不同，屬於審判目的外之使用，二種行為亦應適用不同規範；在歐盟法上，該等行為將適用 GDPR，而在我國法上，則可能為個資法與政資法的交互適用，惟刑事訴訟法規若有特別規定，應優先從之，本文將進一步討論。

²⁴⁹ Mark Leiser & Bart Custers, *supra* note 129, at 374.

²⁵⁰ “The performance of the tasks of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them to require or order natural persons to comply with requests made. In such a case, the consent of the data subject, as defined in Regulation (EU) 2016/679, should not provide a legal ground for processing personal data by competent authorities. Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the reaction of the data subject could not be considered to be a freely given indication of his or her wishes.”

²⁵¹ “The processing of such data should also be allowed by law where the data subject has explicitly agreed to the processing that is particularly intrusive to him or her. However, the consent of the data subject should not provide in itself a legal ground for processing such sensitive personal data by competent authorities.”

²⁵² Mark Leiser & Bart Custers, *supra* note 129, at 374. Paul De Hert & Vagelis Papakonstantinou, The New Police and Criminal Justice Data Protection Directive: A First Analysis, 7 NEW J. EUR. CRIM. L. 7, 11 (2016).

第二款 告知後同意的合法性要件

本文欲先說明當事人之告知後同意之要件，以及撤回同意之要件，再於下一節中說明法院使用卷證中個資時，得否以已得同意作為正當化基礎。然而本文欲探究的重點仍限縮於法院使用卷證中個資的行為，於以下說明中除了介紹同意與其撤回之合法要件外，進一步之說明均將圍繞本文研究主題。

我國個資法上針對公務機關使用個資，及其目的外使用行為規範，規定於第 15 條及第 16 條，此二條文均將當事人同意設為合法性事由。我國個資法上因無必要性要件之明文，故當事人同意與其他合法性事由並列；相較於此，GDPR 中的一般合法性事由，需再加上必要性要件，方得作為使用行為的正當化基礎²⁵³，而當事人同意有別於其他正當化基礎，本身即為個資使用行為的正當化基礎。

為刑事目的而使用個資的情形，於我國法上除刑事訴訟法中零星規範外，其餘未規範事項均以個資法第 15 條、第 16 條作為概括、可能的法律基礎，其中刑事訴訟法並無直接規定當事人同意以使用個資之規範，個資法第 6 條、第 15 條、第 16 條，一般性或敏感性個資、目的內或外之使用規範，均設有當事人同意之事由；而 2016/680 指令中無當事人同意的條文，惟指令前言第 35 節最末說明，儘管資料當事人於刑事目的使用下之同意並非真摯、自由，「此現象並不排除歐盟會員國得以法律規定，資料當事人得同意依本指令之規範目的而使用其個資，例如犯罪調查中之 DNA 檢驗，或為執行刑法而以電子裝置監控其所在地點²⁵⁴。」

本文將介紹之當事人同意要件，乃以規範較完整之 GDPR 為主，GDPR 第 4 條第 11 款規定，資料當事人之同意，係指當事人「出於自由意志、針對具體特定目的，在已受充分告知下，透過聲明或其他清楚肯定的行動，表示其內心同意使用其個資之想法²⁵⁵。」資料當事人就一般性個資使用為同意的要件，即為「出

²⁵³ 張陳弘、莊植寧，註 55 書，頁 104。

²⁵⁴ “This should not preclude Member States from providing, by law, that the data subject may agree to the processing of his or her personal data for the purposes of this Directive, such as DNA tests in criminal investigations or the monitoring of his or her location with electronic tags for the execution of criminal penalties.”

²⁵⁵ “[A]ny freely given, specific, informed and unambiguous indication of the data subject's wishes by

於自由意志」(freely given)、「受充分告知」(informed)、「針對具體特定目的」(specific)，以及「清楚的同意行為」(unambiguous indication of wishes)等四項²⁵⁶。GDPR 第 7 條、其前言第 32、33、42 節則說明資料控制者如何達到這些要件要求。其中在透明性原則下，資料控制者的告知義務可謂資料當事人主張其權利的重要前提，蓋資料當事人需先知悉自己的個人資料正在依何目的、被誰、以何種方式，在何範圍下使用，才能決定是否主張，而無論資料當事人是否行使其知情權，資料控制者都負有主動告知之義務²⁵⁷。AWP 29 意見書對此亦有闡釋，以下說明之。

第一目 出於自由意志(freely given)

AWP 29 意見書中對此要件解釋採反面描述，認為若資料當事人受不當影響或壓力，或不為同意將招致不利後果時，當事人同意乃於不自由的情境下作成，不符此要件要求，因而無效²⁵⁸。GDPR 前言第 43 節亦說明，公務機關與自然人之間通常存在明顯的權利不對等情形，資料當事人就其個資為公務機關使用，現實上亦難以尋得替代方案，故公務機關不太可能以當事人同意作為正當性基礎，AWP 29 意見書亦認為公務機關應尋求更加合適的正當性基礎²⁵⁹。然而，在 GDPR 的框架下，公務機關並非全然不得取得有效之當事人同意。GDPR 欲排除的是權力不對等下之當事人同意，若雙方不存在權力不對等關係，資料當事人對於公務機關使用其個資，仍有出於自由意志同意之空間²⁶⁰。反面而言，在資料當事人無法自由選擇的情況下，不得以當事人同意作為正當化基礎，而需另尋其他更合

which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her[.]”

²⁵⁶ Art. 29 Working Party, Guidelines on Consent under Regulation 2016/679: 17/EN, WP259rev.01, 10 April 2018, at 5. 張陳弘、莊植寧，註 55 書，頁 87-89。

²⁵⁷ 張陳弘、莊植寧，註 55 書，頁 64、71、177。

²⁵⁸ Art. 29 Working Party, *supra* note 256, at 5.

²⁵⁹ Art. 29 Working Party, *supra* note 256, at 6.

²⁶⁰ Art. 29 Working Party, *id.* 張陳弘、莊植寧，註 55 書，頁 88。該二文獻均舉例，如某市政府欲興建道路，主管機關提供興建進度報告供沿線居民參考，居民只要上網註冊，並輸入電子郵件，主管機關就會寄送報告至其電郵信箱，由於居民提供電郵與否，並不會使市政府不提供其任何核心服務，或影響其權利義務，故可認為居民提供電郵係出於自由意志所為。

適的法律依據；例如為刑事目的而使用個資時，2016/680 指令為 GDPR 之特別規定。該指令延續 GDPR 所謂「權力不對等情形下，資料當事人無法自由為同意」觀點，指出在其規範目的下，當事人被課予一定法律義務，且國家機關與自然人間亦存在懸殊的權力不對等情形，故資料當事人此時處於不自由的狀態，無法為有效同意²⁶¹。

整理 GDPR 與 2016/680 指令之前言與規定，公務機關使用個資，得否取得當事人同意，在刑事目的方面，因公務機關主導刑事追訴，自然人有時甚至依法負有忍受或協助之義務，二者間始終存在權力不對等關係，故當事人同意原則上至少不得單獨作為使用行為的正當化基礎；在刑事目的以外之使用，若公務機關與當事人間存在權力不對等關係，原則上同於前述，當事人同意至少不得單獨作為使用行為的正當化基礎；若公務機關與當事人間無權力不對等，當事人同意才能作為單獨之正當化基礎。此處「權力不對等」在 GDPR 條文、前言或 AWP 29 意見書中均無清楚定義，目前應個案認定²⁶²。

更進一步而言，考量到卷證中蘊含大量敏感性個資，其使用往往牽涉當事人權利義務關係，法院與資料當事人間普遍存在權力不對等情形，是故，為刑事審判目的而使用卷證中個資時，法院居於審判機關地位，應優先尋求刑事訴訟法規之規範，此時法院不得僅以當事人同意作為正當化基礎，尚需尋求其他具備必要性之合法性事由，以為授權；而法院為審判外目的而使用卷證中個資，居於司法行政機關地位時，則屬目的外使用個資，需再度考量其正當化基礎，此時除應適用各該相關法律授權外，亦應個案認定法院與當事人間有無權力不對等情形。

需特別說明的是，第三人學術單位出於學術研究目的，請求法院准許查閱卷證之情形。此情形涉及敏感性個資之目的外使用行為，卻符合 GDPR 所設之例外，而得以進行該等使用。在 2016/680 指令設計下，學術研究使用出於刑事程序之個資，回歸 GDPR 處理²⁶³，而 GDPR 第 5 條關於一般性個資之使用、第 6

²⁶¹ 劉定基，註 51 文，頁 156。

²⁶² Art. 29 Working Party, *supra* note 256, at 5-6.

²⁶³ Tristan Radtke, *supra* note 228, at 250.

條規定敏感性個資之使用、第 14 條規定個資目的外使用時資料控制者之告知義務內容，各條規定均將學術研究列為豁免事由，當提供相關資訊予當事人顯有困難或需耗費顯不相當之努力，且資料控制者已符合第 89 條之要求時，毋庸再取得當事人同意²⁶⁴。GDPR 前言第 33 節亦對學術研究採取寬鬆態度，說明符合該研究領域之倫理規範下使用個資，可視為已得當事人同意，惟當事人仍得隨時撤回同意²⁶⁵。我國現行法上對法院得否准許學術單位查閱卷證，於刑事訴訟法規尚無明確授權規範，於個資法第 6 條第 1 項第 4 款規定敏感性個資得為學術研究使用、第 16 條規定公務機關得為學術研究而目的外使用個資，在體系上與當事人同意並列，同為合法性事由，有別於 GDPR 以同意作為正當化基礎的設計。本文以為，在現行法下，學術研究目的本身即可作為法院目的外使用之依據，毋庸取得當事人同意；而法院或學術單位若欲以當事人同意作為其個資用於學術研究之合法性事由，因當事人此時並未受法律義務拘束，就算拒絕法院或學術單位亦無不利益，不生權力不對等問題，得為自由判斷，故本文肯認當事人同意於此單獨作為正當化基礎之可能。

綜上，法院在刑事目的範疇中使用個資時，當事人同意幾乎無餘地作為正當化基礎；若將由刑事目的蒐集而來之資料，轉作非刑事目的之使用，如前述學術研究目的，資料當事人才可能有自由選擇的可能，法院也才有適用當事人同意的空間。

第二目 針對具體特定目的(specific)

此要件要求資料控制者需基於具體特定之目的，告知資料當事人，並取得當事人針對此目的下進行個資使用之同意。此要件的意義在於重申目的拘束原則，確保個資使用過程中受到管控，並遵循透明性原則²⁶⁶。AWP 29 意見書中進一步指出具體特定目的之三項要求，以下介紹之。

²⁶⁴ 楊智傑，註 230 文，頁 41-43。

²⁶⁵ Art. 29 Working Party, *supra* note 256, at 28-29.

²⁶⁶ Art. 29 Working Party, *supra* note 256, at 11.

第一項要求是預防「功能潛變」(function creep)²⁶⁷，指個資使用的範圍在過程中逐漸擴張或模糊，因而逸脫當事人最初同意的範圍。論者認為在大量資料交互比對的情況下，較易發生此現象，尤其是採用大數據技術進行分析，或個資已經過系統化整理，更易於交互比對的情形²⁶⁸。本文以為，明確界定使用行為的目的，也就同時劃定了使用的範圍。若資料控制者欲進行目的外使用，應再就新目的，重新取得當事人同意，方得為之²⁶⁹。

第二項要求是，若資料控制者基於多種目的使用個資，應就每一種目的個別取得同意，資料當事人原則上不得概括同意²⁷⁰。然而，在本文研究範疇內，學術研究之使用乃此要件之例外。GDPR 前言第 33 節說明，「為學術研究目的，在資料蒐集階段時，通常不可能完整地界定出個資使用的目的。因此，資料當事人在行使同意權時，只要符合該研究領域中被認可的倫理規範，可以對特定領域之研究給予同意。資料當事人應有機會只對特定領域的研究，或只對部分的研究計畫給予同意²⁷¹。」依照此見解推論，雖然 2016/680 指令與 GDPR 前言第 50 節都將學術研究列為例外無須再取得當事人同意之情形，但仍未完全排除法院以取得當事人同意作為傳輸個資的正當化基礎，此時法院得取得概括同意，在後續的研究使用中，毋庸再一一取得當事人同意。

第三項要求是，資料控制者需提供明確的資訊，使資料當事人知悉其同意與否將如何影響其權利²⁷²。有論者指出，同意是否符合此要件，一般而言取決於資料控制者所告知資訊的詳細程度，因而與告知義務具有內在連結²⁷³。

本文認為，上述三項要求並非涇渭分明，而有重疊的可能，例如單一使用目的的可能發生功能潛變，而成為多重目的之使用，是故只要個資使用之範圍超出當事人同意之範圍，即屬目的外使用，而需另外取得當事人同意。然而，針對已確

²⁶⁷ 譯名參照翁逸泓，註 25 文，頁 36。

²⁶⁸ 參照本文第二章第三節第二項之說明。

²⁶⁹ 劉定基，註 51 文，頁 156。Art. 29 Working Party, *supra* note 256, at 12.

²⁷⁰ Art. 29 Working Party, *supra* note 256, at 12.

²⁷¹ 翻譯參考楊智傑，註 230 文，頁 38，再經編輯以符合本文用語。

²⁷² Art. 29 Working Party, *supra* note 256, at 12.

²⁷³ 劉定基，註 51 文，頁 156。關於告知義務之內容，參見下款說明。

定案件之卷證使用，以學術研究使用為例，本文認為，若原本蒐集個資的目的即是為了學術研究使用，則資料當事人得僅為概括同意；若個資先因刑事目的蒐集，而後轉作學術研究之目的外使用，在我國現行法下，法院本可以個資法第 16 條作為正當化基礎，亦得以當事人同意作為正當化基礎，而此處之同意，本文考量學術研究範圍不易在研究初始界定之特性，從寬解釋，認為取得概括同意即可。

第三目 受充分告知(informed)

GDPR 第 14 條規定資料控制者在蒐集個資前對資料當事人之告知義務，我國個資法第 8 條、第 9 條亦設有告知義務之規定。告知雖然屬於同意的要件，但並非所有取得當事人同意的情形均需進行告知，在某些特定情形下，法律規定可免除資料控制者之告知義務，例如資料當事人已能知悉、告知不可能、法律基於其他利益維護考量規定不能告知等情形²⁷⁴。有論者觀察，告知義務與同意的關係乃「拆離的雙重結構」，指同意與告知義務不必然相伴，而存在「須告知，但不須取得同意」與「不須告知，但取得之同意仍有效」兩種情形²⁷⁵。前者情形較無問題，乃個資法原理原則下之透明性要求²⁷⁶，資料控制者之告知義務本得單獨存在；後者情形則受到學者批評，認為未經告知即取得之當事人同意，有違透明性要求與告知後同意制度之精神，該同意是否有效殊值懷疑²⁷⁷。

本文整理後以為，前述論者批評主要立基於討論告知後同意與其他個資使用之正當化基礎間關係，該論者認為告知後同意應優先適用，例外在取得同意將妨礙其他更重要的利益追求時，或僅取得當事人同意無法完整保護資訊隱私利益時，才以其他法定事由與必要性考量，作為正當性基礎²⁷⁸。不少學說亦主張，現行個資法將當事人同意與其他法定使用事由並列，未凸顯其原則性地位，已實質架

²⁷⁴ 張陳弘、莊植寧，註 55 書，頁 183-184。

²⁷⁵ 張陳弘，註 70 文，頁 279。

²⁷⁶ See generally GDPR Recital 39; Art. 29 Working Party, Guidelines on Transparency under Regulation 2016/679: 17/EN, WP 260rev.01, 29 November 2017, at 6-7.

²⁷⁷ 張陳弘，註 70 文，頁 279。

²⁷⁸ 張陳弘，註 70 文，頁 274、280-281。

空個人資訊自主的精神²⁷⁹。

本文以為，告知後同意雖在學說上居於原則性地位，但在法院因刑事目的使用卷證中個資時，本質上無法先告知當事人並徵得其同意再行使用，故此類行為毋庸取得當事人同意，也排除同意作為其正當化基礎，其需依法律授權方可進行；至於本文所欲探討的範圍，即法院非依刑事目的使用卷證中個資時，則需考量該等事務的性質，並權衡法院行為背後的公共利益與當事人利益。在此體制下，告知後同意反而是在法律未授權時，或法院欲尋求資料當事人的共識以增強其使用之正當性時，退而求其次地選擇的正當性基礎。在現行法對於法院之授權規範未臻細緻的情況下，法院的各種行為均需透過個資法第 15 條第 1 款「執行法定職務必要範圍內」、第 16 條第 1 至 5 款目的外使用之法定事由等解釋，取得使用個資的授權。

本文認為，法院使用已確定案件卷證中的個資，以當事人同意作為正當性基礎的情形，應十分限縮。首先，管理已確定案件之卷證亦屬法院司法行政之職責，乃依法授權而為，原則上無須再取得當事人同意。第二，縱然肯認得以當事人同意作為正當性基礎，惟卷證中資料往往涉及被告、證人、被害人等人之個資，難以截然擷取部分²⁸⁰，理論上需取得卷證中的訴訟關係人同意²⁸¹，但所牽涉的當事人層面廣泛，而造成實際操作的困難。

就算告知後同意難以作為正當化基礎，法院是否仍應負告知當事人義務？現行個資法對於告知義務的設計，重在蒐集資料階段，而就後續之處理、利用，如傳輸資料予他方，則另由資料的接受方，即下一階段中個資之蒐集者，負告知義

²⁷⁹ 邱文聰，註 28 文，頁 182；劉靜怡，不算進步的立法：「個人資料保護法」初步評析，月旦法學雜誌，183 期，2010 年 8 月，頁 147-164。

²⁸⁰ 附帶言之，在 2016/680 指令中，則有將被告、證人等訴訟關係人之個資予以類型化後，分別使用、儲存及管理的要求，但學者亦批評其可行性不高。參照 2016/680 Directive Art. 6; Celine C. Cocq, EU Data Protection Rules Applying to Law Enforcement Activities: Towards an Harmonised Legal Framework, 7 NEW J. EUR. CRIM. L. 263, 267-269 (2016).

²⁸¹ 參照法務部法律字第 10603509640 號函釋，其指出「為達到『明確告知』之目的，蒐集者仍應以個別通知之方式使當事人知悉，不得以單純擺設(張貼)公告或上網公告之概括方式為之，而須足以使當事人知悉或可得知悉該公告內容之方式(例如：須直接向當事人提示公告內容所在位置，並請其閱讀瞭解)始屬之」。

務。例如依個資法第 8 條第 2 項，依刑事目的使用卷證資料時，無須告知資料當事人，否則將妨礙法院執行職務，而卷證的原始使用目的並不包含提供第三人查閱，法院若以刑事以外目的提供，即屬目的外使用²⁸²；而使用已確定案件卷證中的個資，則須視第三人之身分個別而定，在學術研究使用方面，由於學術研究單位直接請求法院提供其卷證屬於個資的蒐集者，需考量由該學術單位負告知義務或免為告知²⁸³，而與法院無關。是故法院作為傳遞方，不須再負告知當事人義務。

附帶言之，至於原來資料控制者需告知當事人之基本資訊，以 GDPR 第 14 條第 1 項為例，AWP 29 意見書整理其內容包含：資料控制者的身分、個資使用行為之目的、所使用的個資種類、當事人撤回同意之權利、資料傳輸中因當事人的不充分決策可能產生的風險及保護措施、以及若將個資用於演算法自動化決策中需告知之資訊等²⁸⁴。就告知的方式，原則上應以當事人得容易瞭解的方式為之，例如以簡明的語言，或輔以圖示說明等²⁸⁵。

第四目 清楚的同意行為(unambiguous indication of wishes)

依照 AWP 29 意見書的說明，當事人同意的最後一個要件是清楚的同意行為。此要件的要求相對容易達成，依 GDPR 前言第 32 節，口頭、書面、電子化的同意行為皆可屬之。需注意的是，在使用敏感性個資的情形，GDPR 第 9 條提高其要求程度，需資料當事人的明確(explicit)同意，如書面同意，或電子簽章等，並應由資料控制者事後證明²⁸⁶。

²⁸² 楊智傑，註 230 文，頁 75。該文獻以建置全民健康資料庫為例，法理與本文此處相同。

²⁸³ 在比較法上，依 GDPR 第 14 條第 5 項第 b 款，若告知當事人屬無法達成或需費過鉅時，可免除同條第 1 至 4 項之告知義務，學術研究即屬此類在蒐集時難以完整告知使用範圍的情形，故在符合該領域之學術倫理的前提下，得免除告知。參照李寧修，註 231 文，頁 30-31。惟該文獻亦指出，學術研究單位原則上仍應取得當事人同意，方符 GDPR 對研究倫理之期待。

²⁸⁴ Art. 29 Working Party, *supra* note 256, at 13. 關於演算法自動化決策需告知之資訊，因與本文研究範圍較無關，故不於此詳述，可參黃子潔，論人工智慧演算法時代的解釋權－歐盟 GDPR 與我國個人資料保護法之比較研究，國立臺灣大學科際整合法律學研究所碩士論文，2019 年 6 月。

²⁸⁵ Art. 29 Working Party, *supra* note 256, at 14-15.

²⁸⁶ 張陳弘、莊植寧，註 55 書，頁 145。Art. 29 Working Party, *supra* note 256, at 18.

鑒於卷證包含大量敏感性個資，法院使用已確定案件之卷證時，若欲以當事人同意為正當性基礎，原則上應取得明確同意。

第三款 現行告知後同意制度的不足之處

我國刑事訴訟法中關於「告知後同意」的規範模式，可見於被告受訊問時同意於夜間訊問、受搜索扣押之人的自願性同意，以及當事人於審判中同意使用傳聞證據等，多為強制處分及證據使用層面；至於當事人個資使用的告知後同意，則與司法行政處分同未規定。在法理解釋的層面，法院使用已確定案件之卷證資料，已有其他正當化基礎可循，雖然法律規範未臻明確，但仍適用個資法作為普通法位階之授權規範²⁸⁷。

然而，現行告知後同意制度本身仍有不足之處，本文欲以兩點說明之。第一，告知後同意制度的定位在我國個資法上，與其他合法性事由相同，並無優先適用的原則性地位，亦與 GDPR 或 2016/680 指令中獨立作為正當性基礎的地位不同。學者已經指出，從資料當事人的角度而言，如此制度設計將架空其資訊自決權²⁸⁸。第二，學者指出，現行告知後同意要件解釋未排除默示同意，造成當事人同意行為的明確程度不清²⁸⁹。我國個資法第 7 條第 1 項僅定義當事人同意為「當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示」；個資法施行細則第 14 條則說明其得以電子文件方式為之。法律層級的規範僅有如此，留下相當大的解釋空間。惟本文從自身研究範圍看來，未將告知後同意置於原則地位，以及制度內部的要件模糊，對法院適用不同正當化基礎的影響不大，故不再深入批評。

本文認為，現行告知後同意制度，對於法院使用已確定案件中卷證之個資，

²⁸⁷ 實務函釋數度說明個資法為普通法位階，參照法務部 108 年 9 月 16 日法律字第 10803512600 號、107 年 2 月 13 日法律決字第 10703500220 號、106 年 6 月 19 日法律字第 10603508500 號等函釋，轉引自楊智傑，註 230 文，頁 97。另有不同見解指出，個資法僅為合法性基礎的描述，不得作為授權依據，參照謝碩駿，行政機關蒐集個資之法律依據，月旦法學教室，198 期，2019 年 4 月，頁 16。該文獻亦提醒，組織法並不能作為個資使用行為的授權依據。

²⁸⁸ 參見前述本章第二節第二項第三款之說明。

²⁸⁹ 楊智傑，註 230 文，頁 97-98。

具有較直接影響的缺陷，應是法院既不負有再度告知之義務，又欠缺配套措施。在雙元授權基礎的構造下，法院僅需法定事由即可傳輸資料，毋庸再取得當事人同意，而可能產生的告知義務則由蒐集方負擔，使法院在傳輸個資時無須告知當事人。我國制度設計由蒐集方告知當事人，與 GDPR 設計相同，並無太大問題，但我國制度並未如 GDPR 設置其他要件或配套措施，造成法院的正當化基礎模糊。舉例而言，傳輸已確定案件中之個資，屬於目的外使用行為，法院僅需在具備法定事由時為之即合法，並無如 GDPR 之相容性要件的把關。現行個資法第 16 條將「法定事由」、「當事人同意」與「去識別化」並列為個資目的外使用的合法性要求，且只需符合其一即合乎此要求，使實務發展出資料去識別化後即無須再取得當事人同意之見解²⁹⁰。此制度設計不僅落入「已公開之個資即無保護必要」之窠臼，忽視當事人之資訊自決權，同時亦將當事人同意與其他法定事由置於同一地位，使得任何法定事由均可用於傳輸，而不需考量其與刑事目的之關聯性²⁹¹。

本文以為，與刑事目的之相容性判斷，對於法院使用已確定案件之卷證資料，其重要性在於，當授權規範較為模糊或寬泛時，得適度縮減法院使用行為，以求其中個資使用不過度偏離目的拘束原則。儘管使用已確定案件之卷證資料似已脫離刑事目的之範圍，但仍需符合目的拘束原則，考量卷證本為刑事目的而生，此一刑事使用轉作非刑事使用之行為²⁹²，仍須具備相容性。

第三節 小結：授權規範的缺乏

綜上，法院使用已確定案件之卷證中個資時，往往居於傳輸機關地位，提供或不提供其資料予第三方。學說上有認為，公務機關間的資料傳遞行為，乃「傳遞機關之個資利用行為」與「接收機關之個資蒐集行為」共同組成，而具有「行

²⁹⁰ 張陳弘，國家建置全民健康保險資料庫之資訊隱私保護爭議－評最高行政法院 106 年度判字第 54 號判決，中原財經法學，40 期，2018 年 6 月，頁 248。

²⁹¹ 張陳弘、莊植寧，註 55 書，頁 136。另關於相容性的判準，詳參本文註 122 之說明。

²⁹² 相較之下，2016/680 指令中規定非刑事目的來源之資料，轉作刑事目的使用，則無相容性要件要求，參照第二章第二節第二項、第三章第二節第一項之說明。

為評價之雙元性」，應分別適用不同授權規範²⁹³。本文在此基礎之上，欲集中討論法院一方的授權規範，暫不深究接收方的授權規範或請求之基礎，對於接收方身分的討論，也僅在與法院的授權規範相關的範圍內為主。

本文整理法院基於本案審判中使用、與本案審判外使用卷證中個資的架構，並輔以司法行為與司法行政行為區分，說明法院使用卷證中個資的情境不同，適用之行為規範亦不同。

法院在本案審判中，基於審判目的使用卷證資料，乃法院的憲法任務，亦為卷證資料使用最原始的目的，刑事訴訟法就此已有明文及相關制度設計，如訴訟關係人的卷證資訊獲知權、法庭錄音錄影光碟之交付、法院間的卷證資料傳輸等，而個資保護在此為法院踐行正當法律程序時，所需衡量的其中一項要素。上開制度的目的都已穩定且明確，本文認為此處應考量的是，該等制度之規範是否已落實目的拘束原則與資料最小化原則要求，亦即在能使訴訟關係人準確知悉其所需資訊的前提下，法院將卷證中個資提供給訴訟關係人時，其提供的範圍與方式，不應揭露過多的個人資料；資料的儲存與轉移亦應具備監督機制。上開原則之要求在刑事訴訟法規中均應有完整規範。

法院在本案審判中，基於司法行政目的使用卷證資料，乃為履行其他公法上的重要任務，如裁判書之公開即為法治國原則與民主原則之要求。此等行為性質上屬於審判目的外之使用，因此法律就新目的、公開之方式、範圍，均應有明文授權規範。然而，現行法院組織法及其相關規範未能貫徹裁判書公開的目的，亦未在兩種價值間取得平衡，除了部分類型案件的裁判書不予公開外，其餘公開者之範圍與方式又未貫徹去識別化，並未達到個資保護要求。

法院在本案審判中，使用其他案件的卷證資料，或非因刑事目的蒐集之個人資料，對於該等個資而言，法院行為亦屬目的外使用。雖然法院本就具有調查證據權限，但其目的外使用個資行為對資料當事人已構成基本權干預，法院仍需尋求其行為之合法性事由、判斷相容性與比例原則。

²⁹³ 詹鎮榮，註 150 文，頁 10。

最後，法院在考量是否准許第三人查閱卷證時，由於法院此時居於司法行政機關地位，應適用個資法第 6 條第 1 項，公務機關目的外使用敏感性個資的授權規定，並從嚴解釋，需有明確法規授權，並依法定權限為之，此授權應按照個資被使用的不同背景，為類型化的規範，例如以學術研究使用；其還需具備適當的保護措施，以維護資料當事人權益。

在法規的適用順序上，本文認為刑事卷證中的個資保護屬於訴訟法規之範疇，應優先適用刑事訴訟法，當刑事訴訟法無明文時，再適用居於普通法位階的個資法、政資法等法律。綜觀法院使用卷證中個資之行為，本文認為法院的行為規範並不完整，往往需尋求適用普通法位階的規範，而由此產生解釋上問題，須由實務、學說累積見解解決。雖有論者觀察提出，法院使用已確定案件卷證之個資，得適用個資法與政府資訊公開法²⁹⁴，但亦有論者指出，個資法第 15 條關於公務機關的使用個資規範，僅指出使用行為的合法性要求，本身並不能直接作為授權依據，而應先探詢是否有特別法存在²⁹⁵。本文認為，第一，政府資訊公開法僅規範公務機關對非公務機關的資料傳遞，且法院是否適用，尚存爭議，本文對此亦採保守態度；第二，現行刑事訴訟相關法規缺乏對於已確定刑事案件卷證的使用規範，造成法院無所依循，本文除檢討此現象外，亦將於後續章節中，由法規面切入，提出立法建議。

實務、學說上考量個別情況，適用不同行為規範、不同類型的近用方式，須注意個資保護原則要求。法院應遵循目的拘束原則，進行目的外使用應有特別授權，亦即針對資料當事人之基本權干預，應有法律授權之合法性事由；在達成使用目的之前提下，法院需遵循資料最小化原則，個人資料被揭露的範圍、方式，諸如提供全部或部分卷證原本或副本、或另外提供答覆等，應有類型化的區分。法院亦應考量比例原則，綜合判斷若提供該等個資，對資料當事人之影響，尤其是在資料的累積作用下，是否容易連結至資料當事人，甚或描繪出其生活圖像。

²⁹⁴ 劉定基，註 125 文，頁 896；參照本文第三章第二節第三項第二款之討論。

²⁹⁵ 謝碩駿，註 287 文，頁 16。

最後，法院應確保踐行適當的保護措施，無論是在技術上對資料使用施加限制，或在法律上課予下一個資料使用者義務與責任，每種使用行為都應該具備相應的配套措施，其嚴謹程度依使用行為的性質而定。



第四章 卷證中個人資料保護之比較法制探討：

以歐盟及德國為對象

本文將由歐盟法及德國法切入，說明在外國法制上，較為完整的卷證個資使用制度之面貌。本文將聚焦於法院使用已確定案件之卷證的授權規範，討論這些規範如何落實個資保護。本文已經在前開章節中，論述我國法制現狀時，輔以歐盟 GDPR、2016/680 指令說明，於本章中，將再度完整介紹該二規範之適用範圍與配套措施；考量該二規範屬於歐盟法層級，本文再選擇德國法制，探討將歐盟規範內國法化後，所呈現的個資保護制度面貌，以供我國法借鏡。

第一節 歐盟法制之發展

第一項 GDPR 與 2016/680 指令之適用範圍

在刑事訴訟法規與個資保護法規的適用順序上，就歐盟法的角度，GDPR 乃適用範圍最廣泛的規範，涵蓋公法及私法領域；2016/680 指令適用於與刑事目的相關之事務，二者範圍互有重疊²⁹⁶。各會員國的刑事訴訟法規適用於審理事務，乃各國主權核心範圍之一，無論是 GDPR 或 2016/680 指令都將其排除於規範範圍外²⁹⁷。法院在刑事案件確定後，居於審判者之任務已告一段落，為刑事執行而使用個資，則可能適用 2016/680 指令。依 GDPR 第 55 條規定，為保持司法機關進行司法任務及決策之獨立性，資料保護監督機關(data protection authority,

²⁹⁶ GDPR 前言第 20 節指出：「主管機關為達預防、調查、偵查及追訴刑事犯罪或執行刑罰之目的所為當事人受保護之個人資料處理，包括為維護及預防此等資料對公共安全及個人資料自由流通造成之威脅，乃係特定歐盟法之主要議題。因此，本規則不適用於有關上開目的所為之個人資料處理。惟公務機關依本規則處理個人資料時，如其使用係為上開目的，則應受更為具體之歐盟法案之拘束，即歐洲議會及歐盟理事會所制定之歐盟第 2016/680 號指令。」翻譯參照吳瑛珠，註 203 文，頁 137。亦參照財團法人金融聯合徵信中心編，歐盟個人資料保護規則，財團法人金融聯合徵信中心，2017 年 7 月，頁 41。

²⁹⁷ Thomas Marquenie, *supra* note 124, at 330.

DPA)對司法目的下之資料使用行為並無管轄權，而應交由成員國司法體系中之特別單位進行內部監督²⁹⁸。法院若欲以刑事以外目的使用卷證，除各國刑事訴訟法規有特別規定外，則回歸適用 GDPR 之其他規定²⁹⁹。

第二項 個資保護之其他具體措施

在 GDPR 與 2016/680 指令中，尚有其他保護個資的具體措施，就資料當事人的角度而言，歐盟規範與指令均提供其詳盡的權利清單，例如資料更正權、資料可攜權、被遺忘權、限制處理權等³⁰⁰，本文偏重於研究法院之行為規範，對於資料當事人之各項權利在此不欲一一引介，但欲指出，在刑事與非刑事目的之脈絡中，資料當事人均享有這些權利，但也引來學者批評，於 2016/680 指令目的下，資料當事人的權利往往流於理論，使內國法化的過程充滿困難³⁰¹。

在管理、傳輸卷證資料的流程中，法院負有另一項重要的資料控制者義務，即為個人資料毀損(data breach)衍生之義務。在卷證資料處於法院的控制下，若其中個資遭受未經授權的篡改、毀損，或無法取得之破壞，則屬於個人資料毀損，法院負有修復義務及通報義務。就較重要之通報義務而言，原則上應依 GDPR 第 33 條、第 34 條規定，向資料保護監督機關及受影響之資料當事人通報，惟在法院涉及司法行為範圍內，依 GDPR 第 55 條，資料保護監督機關並無管轄權；為保持司法機關進行司法任務及決策之獨立性，該等情形應交由成員國內司法體系中之特別單位處理³⁰²。惟就不涉及司法權之範圍，如審判外目的下使用已確定案件之卷證資料，則仍適用 GDPR 中通報之規定，就通報主管機關而言，應優先適用內國法較詳盡之規範，就通報資料當事人而言，則應同時考量有無例外

²⁹⁸ Arndt Sinn 著、吳瑛珠譯，裁判書公開於德國之實踐(下)，司法周刊，1928 期，2018 年 11 月，2 版。

²⁹⁹ 論者指出，參照 GDPR 前言第 20 節、第 9 條第 2 項第 f 款，第 37 條第 1 項第 a 款，第 55 條第 3 項等意旨，GDPR 所排除的是司法機關行使司法權與刑事訴追、執行刑罰目的下使用個人資料，屬於司法行政的裁判公開仍在 GDPR 的適用範圍內，參照吳瑛珠，註 203 文，頁 137。

³⁰⁰ 劉靜怡，註 37 文，頁 7-12。GDPR 與 2016/680 指令中對於資料當事人權利的比較整理，參見 Mark Leiser & Bart Custers, *supra* note 129, at 373.

³⁰¹ Paul De Hert & Vagelis Papakonstantinou, *supra* note 252, at 12-13.

³⁰² Arndt Sinn 著、吳瑛珠譯，註 298 文，2 版。

無須通報之事由。

另一項屬於資料控制者的個資保護措施，則是資料保護風險評估(data protection impact assessment, DPIA)，在進行個資使用行為前³⁰³，本文以為法院宜先踐行此一事前評估。DPIA 旨在協助資料控制者、資料使用者檢視其使用行為之合法性，這項程序得以協助劃定使用行為範圍，檢視其必要性與是否合乎比例原則，以及衡量該行為對資料當事人之基本權利帶來之風險³⁰⁴。GDPR 對公務機關使用個資行為，設有事前進行 DPIA 之要求，依 GDPR 第 35 條，特別是在「藉由個人資料的自動化蒐集、處理或利用，包括個人特徵描繪行為(Profiling)，對自然人之私人領域進行系統性及大規模的分析，並據以對特定個人作成具有法律效果的決定或產生類似影響；大規模蒐集、處理及利用第 9 條第 1 項的敏感性個人資料或第 10 條的犯罪資料；大規模且系統性地監控公眾得以進出之場所」等情形³⁰⁵。在刑事目的範疇，2016/680 指令亦要求執法機關進行 DPIA³⁰⁶，但其適用情形較 GDPR 限縮，僅在「該等個資使用行為採用新興科技，且考量其本質、範圍、背景、目的，可能對自然人之自由或基本權利造成高風險時」，方有義務為之³⁰⁷。

DPIA 的進行方式僅有 GDPR 之細部規範，2016/680 指令則無。依 GDPR 第 35 條第 7 項，其內容應包含所擬進行使用行為之系統性描述及其目的之說明；使用之必要性、適當性及與目的間關係之評估；對資料當事人之權利及自由可能造成風險之評估；為防範該等風險而預計採行之相應保護措施；考量當事人與其

³⁰³ GDPR Recital 90; GDPR Art. 35 (1); Art. 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679: 17/EN, WP248rev.01, 10 October 2018, at 13.

³⁰⁴ Art. 29 Working Party, *id.*, at 4.

³⁰⁵ GDPR Art. 35 (1); (3). 翻譯參照李寧修，註 231 文，頁 35。

³⁰⁶ Juraj Sajfert & Teresa Quintel, *supra* note 104, at 12; Paul De Hert & Vagelis Papakonstantinou, *supra* note 252, at 17.

³⁰⁷ EU Directive 2016/680 Art. 27 (1): “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, Member States shall provide for the controller to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data.”

他關係人權利與合法利益，確保所採取之個資保護機制符合 GDPR 之要求等³⁰⁸。有論者指出，相較於傳統的隱私影響評估(privacy impact assessment, PIA)，DPIA 能就資料當事人除隱私權外之其他權利進行通盤考量，實屬制度上的進步³⁰⁹。

附帶言之，我國現行法上並無類似 DPIA 之程序可供比較，在規範文字上相似的制度，見於個資法施行細則第 12 條第 3 款「適當安全維護措施」其中之「個人資料之風險評估及管理機制」，然此僅為適當安全維護中一種建議採行之措施，並非如同 DPIA 乃特定前提下之強制要求，二者之規範目的、密度均相異³¹⁰。最後，DPIA 於歐盟法層級尚屬普遍性、一般性之指引，與個案實際應用情況存有落差³¹¹，法院如何進行 DPIA，亦有賴更詳細的內國法規範。

第二節 德國刑事訴訟法上相關規定

隨著 2016 年歐盟通過 GDPR 與 2016/680 指令，德國也展開一連串修法，使其內國法制能與歐盟接軌，甚至採取比歐盟更嚴格的標準。德國於 2017 年修訂其「聯邦資料保護法」(Bundesdatenschutzgesetz, BDSG)，條文數量擴充至舊法的近乎兩倍，體系上也分為總則、GDPR 目的下之資料使用行為規範、2016/680 指令目的下之資料使用行為規範、以及其他補充條款等四個章節，並配合 GDPR，於 2018 年 5 月間生效，完全與歐盟法接軌³¹²。

在此修法趨勢之前，德國刑事訴訟法已有相對完整的個資保護規範與專章³¹³，而未如聯邦資料保護法般整體翻新制度，僅於 2017 年隨電子卷證制度新增相關規定與章節，並個別修正部分條文，最後造成刑事訴訟法中的條文與新修

³⁰⁸ 何之行、廖貞，AI 個資爭議在英國與歐盟之經驗——以 Google DeepMind 一案為例，月旦法學雜誌，302 期，2020 年 7 月，頁 150-151；李寧修，註 231 文，頁 35。

³⁰⁹ Atanas Yordanov, Nature and Ideal Steps of the Data Protection Impact Assessment under the General Data Protection Regulation, 3 EUR. DATA PROT. L. REV. 486, 489 (2017).

³¹⁰ 張陳弘，註 64 文，頁 350-351。

³¹¹ 張陳弘，註 64 文，頁 350。

³¹² Dominic Broy, Germany: Starting Implementation of the GDPR - Brief Overview of the Government Bill for a New Federal Data Protection Act, 3 EUR. DATA PROT. L. REV. 93, 95 (2017).

³¹³ 德國刑事訴訟法第 8 編的立法歷程，參見林鈺雄，註 8 文，頁 205；本文第二章第一節第一項之說明。

訂之聯邦資料保護法未能完全吻合³¹⁴。然而，聯邦資料保護法與刑事訴訟法間，仍屬普通法與特別法之關係，兩者法條用語亦為互通³¹⁵。雖然 GDPR 與 2016/680 指令並未對德國刑事訴訟法帶來直接改變，卻也衍生各規範間如何解釋適用的問題。GDPR 與 2016/680 指令均說明其範圍不涉及刑事審判，由各國刑事訴訟法自行規範之，而德國刑事訴訟法不僅就刑事審判目的下使用，而就使用刑事卷證中個資均設有相對完整的規範。本文將聚焦於引介已確定案件之卷證的相關使用規範，以供我國法借鑑。

第一項 刑事程序法與個資保護要求

在德國刑事訴訟法中，卷證資料之使用規範集中於第 8 編，其共分四章，分別為「提供答覆及查閱卷證、逾越程序目的將資訊移作他用」、「資料規則」、「跨邦檢察機關程序登記資料庫」、以及「電子卷證之個人資料的保護與使用」³¹⁶。本文欲探究的個資使用之總則性規定，集中於第 1 章、第 2 章，主要於 2000 年時生效，部分條文於 2015 年、2018 年細部修正，距今已有二十年以上歷史³¹⁷。

第 8 編第 1 章包含第 474 條至第 482 條，規定了管理卷證之機關由卷證內容提供答覆(Erteilung von Auskünften)及提供卷證本身給其他法院、檢察機關、公務機關、私人、學術研究機構等不同主體之法律授權基礎；這些條文屬於本案刑事目的外使用卷證資料的授權規範，亦補充刑事訴訟法中既有的閱卷相關規定³¹⁸。第 2 章則包含第 483 條至第 491 條，主要規定資料使用的細項流程規則，資料的更正與刪除，以及資料當事人得請求答覆之權利等³¹⁹。

延續 1983 年「人口普查法」判決中確立資訊自決權屬憲法所保障基本權之

³¹⁴ 有文獻指出，德國刑事訴訟法當時並未隨聯邦資料保護法修訂，前者中引用的條號乃是後者的舊法，參見林鈺雄，註 8 文，頁 207，註 2。

³¹⁵ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO Vor §§ 474 Rn. 3.

³¹⁶ 翻譯參見連孟琦譯，德國刑事訴訟法：附德國法院組織法選譯，元照，2016 年，頁 445 以下；林鈺雄，註 8 文。

³¹⁷ 林鈺雄，註 8 文，頁 205-207。

³¹⁸ 林鈺雄，註 8 文，頁 206。

³¹⁹ 林鈺雄，註 8 文，頁 216。

脈絡，若國家機關以資料當事人無法掌握的方式使用其個資，從而危及其人格發展，則其基本權利應受保障，是故國家使用個資時，應基於授權規範為之；在執行政府任務而進行個資傳遞時，資料的傳輸與接收均構成基本權干預，如同兩扇大門，傳輸方與接收方均應個別取得法律依據，如同兩扇門均開啟時，才能合法進行資料傳遞，此即所謂「雙門模式」³²⁰。進一步而言，若資料的傳遞分為不同的干預處分來規範，則明確性的要求也適用於各該階段，逾越原目的使用資料之行為即單獨構成基本權侵害，必須單獨檢視其合法性要件，或需取得當事人同意，方可為之³²¹。

第二項目的外使用行為之依據

聚焦於本文主要研究範圍，法院對已確定案件卷證之使用，其授權規範與實際運用時之資料規則，乃本文欲探究的對象。德國刑事訴訟法第 8 編第 1 章即設有「本案程序目的外使用卷證資料」之授權規範，以下介紹之³²²。需先說明的是，第 8 編中所稱「卷證資料」，原則上與第 199 條第 2 項第 2 句「卷證應連同起訴書一併呈交法院³²³」相同，包含法院可使用之資料與起訴書中所含資料，涵蓋第 163 條第 2 項第 1 句，從「警察機關與警察官員應立即將調查所得之材料送交檢察官³²⁴」開始的所有資料，包含首次取證後的所有證據資料，以及其後送交至檢方，用以在起訴審查程序中對抗被告，與最終成為起訴書內容的資料，但檢方原有的制式資料除外³²⁵。

需注意的是，在德國法上，依第 480 條第 1 項第 1 句規定，關於由卷證內容提供答覆及閱覽卷證，在案件確定終結後，由檢察官決定之；在程序進行中，則由受訴法院審判長決定之。在案件終結後，法院就已確定案件之卷證，並無直接

³²⁰ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO Vor §§ 474 Rn. 1b. 詹鎮榮，註 150 文，頁 9-10；廖緯民，註 189 文，頁 31-34。

³²¹ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO Vor §§ 474 Rn. 1c.

³²² 為求行文簡潔，此章節中條文若未特別說明，均指德國刑事訴訟法。

³²³ 翻譯參考連孟琦譯，註 316 書，頁 237。

³²⁴ 翻譯參考連孟琦譯，註 316 書，頁 219。

³²⁵ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 474 Rn. 1.

決定是否傳遞其中資料的法律授權，惟就此決定之救濟，依第 480 條第 3 項或法院組織法施行法(Einführungsgesetz zum Gerichtsverfassungsgesetz，下稱 EGGVG)第 23 條等規定，仍由法院裁判，故法院仍作為最終的裁量者。

第一款 一般性授權規範

第 474 條乃總則性、一般性授權規範，其第 1 項授權「為司法目的所必要時，法院、檢察官及其他司法機關得查閱卷證³²⁶」；同條第 2 項第 1 句則授權公務機關，若具備各款事由之一，得以獲得卷證內資訊。本條第 1 項說明，為了刑事司法的重大公益，以及對於司法審判程序的信賴，容許查閱卷證資料是原則；法院包含所有法院，如民事法院³²⁷。所謂「司法目的」乃指「本案程序以外」之目的，可能為另案程序，但實際運用情形相當限縮，且若將相同事實用於追訴另一個被告，則不能主張目的外使用合法³²⁸。

第 474 條第 2 項規定中有「必要」要件，說明其適用上須考量比例原則³²⁹。其第 1 款之容許情形為確定、行使或防禦與犯罪有關聯之權利，例如追索與補償之請求³³⁰。第 2 款為基於職權或特別規定，由刑事程序中傳遞卷證資料給其他公務機關，而不需闡明或證明其有查閱卷證資料的必要性存在³³¹。第 3 款則為準備其他處分或措施，有傳遞卷證資料之必要，經由特別規定之授權，得依職權傳遞至請求機關；與第 1 款情形不同的是，在第 3 款下，所傳遞的資訊範圍由請求機關決定，因為傳遞機關通常不比請求機關清楚所需資料的範圍，故請求機關應為適當說明，再由傳遞機關為合理裁量(pflichtgemäßem Ermessen)³³²。在個案

³²⁶ 翻譯參考連孟琦譯，註 316 書，頁 446。

³²⁷ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 474 Rn. 2.

³²⁸ 對於另案，第 474 條的資料傳輸僅發生於資料當事人同時屬於「第 264 條第 1 項之判決對象、第 200 條第 1 項第 1 句之起訴書所載之人、第 409 條第 1 項第 1 句第 3 款之處刑令所載被告所犯罪名、行為時地、犯罪法定構成要件、以及基本法第 103 條第 3 項之一罪不二罰之主體」，實際上相當難達成，參見 *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 474 Rn. 1.

³²⁹ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 474 Rn. 3.

³³⁰ 具體如專業機構向其前任 CEO 請求違反競業禁止之補償與不正經營行為之賠償，或健保機構向偽造處方箋詐領健保費的醫師求償，參見 *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 474 Rn. 4a.

³³¹ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 474 Rn. 3.

³³² 關於傳遞與接收個資的責任歸屬，另外可對照第 477 條第 4 項第 1 句「只要接收者是公務機關或律師，則傳遞合法性之責任由其負擔」；同條第 2 句「在此情形中，除存在進一步審查傳遞

中，傳遞資料的必要性與傳遞範圍原則上均由請求機關先行審查，但傳遞機關亦須考量其傳遞行為是否屬於其法定職權範圍³³³。

第 474 條第 3 項則規定，若符合第 2 項之要件，但由卷證中資訊提供答覆所需耗費不成比例，或僅得到答覆不足以完成請求機關之任務時，得准許請求機關直接查閱卷證；第 4 項、第 5 項則規定，在第 1 項、第 3 項之要件下，亦得查閱證物或紙本卷宗。

在依第 474 條傳遞卷證中個資之前，傳遞機關尚須考量是否符合第 477 條第 2 項與第 478 條第 2 項的限制³³⁴，且有優越於個人資訊自主基本權的利益存在，或至少有具體原因可供嗣後審查其傳遞行為之正當性，例如保護租稅秘密、執行法定職務、履行法定義務，或請求機關之目的與資訊自決之基本權並不衝突³³⁵。例如使用鏡像副本方式(“gespiegelte” Kopie)全盤複製之被告硬碟內資料，只能經由保障個人資訊自決之基本權的方式給予請求機關；若檢察機關所請求之被告硬碟內資料包含被告與其配偶或其他將受到影響之第三人等幾乎完整的私人生活內容，則在利益權衡時，德國實務認為將該個資保密的利益，優於供作請求機關偵查的利益³³⁶。

承上所述，第 474 條是公務機關、司法機關之間傳遞卷證資料的授權規範，其中又以「必要性」要件作為第一道把關，所有的卷證資料使用行為，均須符合必要性原則³³⁷。在使用已確定案件之卷證的情形，檢察官作為傳遞機關，此時若接收者為公務機關或司法機關，即需適用第 474 條。在審查傳遞卷證中個資之決定時，法院是否需如 GDPR 與 2016/680 指令之要求，同時考量新舊目的間之相容性？在德國刑事訴訟法中，並無要求個資目的外使用需具備相容性之明文，

合法性之特殊緣由外，傳遞機關僅審查傳遞請求是否在接收者之職務範圍內」。KK-StPO/Gieg, 8. Aufl. 2019, StPO § 474 Rn. 4c. 翻譯參考連孟琦譯，註 316 書，頁 451-452。

³³³ KK-StPO/Gieg, 8. Aufl. 2019, StPO § 474 Rn. 3.

³³⁴ 詳見第四章第二節第二項第三款之說明。

³³⁵ KK-StPO/Gieg, 8. Aufl. 2019, StPO § 474 Rn. 3. 此處所謂保護租稅秘密(Steuergeheimnisses)，意指依德國會計法第 30 條，在調查個人所得稅繳納之情形，調查結果與犯罪行為之關聯尚不明確時，不得要求傳遞不特定範圍之個資。

³³⁶ A. a. O.

³³⁷ 林鈺雄，註 8 文，頁 208。

觀察第 474 條各項要件，亦屬於以法律規定得進行目的外使用之事由，而不同於 GDPR 第 6 條第 4 項之相容性要件。此問題的解答，需回到居於普通法位階之聯邦資料保護法³³⁸，由公務機關目的外使用個資之相關規範中探詢。

參酌聯邦資料保護法，其雖跟隨歐盟法修正，但在聯邦資料保護法中，相容性概念卻未見於與 GDPR 接軌章節中之條文，包含該法第 23 條關於公務機關目的外使用個資之一般性規定，以及同法第 25 條關於公務機關間傳遞個資之規定，也因此被學者認為其較 GDPR 第 6 條第 4 項寬鬆，並未成功採納 GDPR 規定，其本身不足以為具體的授權規範³³⁹。

在與 2016/680 指令接軌章節中之條文中，亦浮現相似的模式。德國刑事訴訟法第 500 條規定，刑事訴訟法優先適用於聯邦資料保護法，但後者在刑事訴訟法未規定時，仍有適用³⁴⁰。聯邦資料保護法第 47 條乃依 2016/680 指令目的下使用個資之一般性規範。同法第 49 條則為將依第 47 條目的蒐集之個資，進行目的外使用之規定，其第 1 句規範仍依第 47 條目的使用之情形，例如將犯罪預防目的所得個資改用於刑事偵查程序³⁴¹，此時仍需其他具體授權規範方得為之，不得僅以第 49 條充之³⁴²，該等行為同時還需具備必要性，並符合比例原則³⁴³。該法第 49 條第 2 句則為將依第 47 條目的蒐集之個資，進行目的外使用，且新目的不屬於第 47 條範圍之情形，此時第 49 條亦不能單獨作為授權規範，該等行為之合法性要件應參照其他具體授權目的外使用之各該規定³⁴⁴。學者也指出，聯邦資料保護法並未引入新概念，僅將此等不同法律間之適用關係明文化³⁴⁵；在跨越刑事與非刑事目的轉換的情形，考量傳遞行為的合法性時，因為該等行為此時

³³⁸ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 474 Rn. 3. 林鈺雄，註 8 文，頁 207。

³³⁹ *Gola/Heckmann/Heckmann/Scheurer*, 13. Aufl. 2019, BDSG § 23 Rn. 3; § 25 Rn. 17. 相同見解參照謝碩駿，註 287 文，頁 16。

³⁴⁰ *BeckOK StPO/von Häfen*, 42. Ed. 1.1.2022, StPO § 500 Rn. 6. 另外，聯邦資料保護法第 1 條第 2 項規定，其他關於個資保護之規定優先於本法適用，亦定調其居於補充性地位，參見吳瑛珠，註 203 文，頁 136。

³⁴¹ *Gola/Heckmann/Heckmann/Scheurer*, 13. Aufl. 2019, BDSG § 49 Rn. 10.

³⁴² *Gola/Heckmann/Heckmann/Scheurer*, 13. Aufl. 2019, BDSG § 49 Rn. 11-12.

³⁴³ *Gola/Heckmann/Heckmann/Scheurer*, 13. Aufl. 2019, BDSG § 49 Rn. 13-14.

³⁴⁴ *Gola/Heckmann/Heckmann/Scheurer*, 13. Aufl. 2019, BDSG § 49 Rn. 12; 16.

³⁴⁵ *Safferling/Rückert: Europäische Grund- und Menschenrechte im Strafverfahren – ein Paradigmenwechsel?*, NJW 2021, 287, 291.

已屬於 GDPR 目的範圍，應一併考量同法第 25 條、2016/680 指令第 9 條第 1 項與 GDPR 規定³⁴⁶。

綜上，聯邦資料保護法中關於個資傳遞的規定，學者認為僅屬傳遞行為合法性之描述，實際上的正當性基礎尚需由各規定中尋求。德國刑事訴訟法第 474 條，正屬於特別法位階中的授權規範，法院得引用之。惟使用行為之正當性基礎，除須符合第 474 條要件外，尚須具備新舊目的間相容性，方符合聯邦資料保護法、GDPR 及 2016/680 指令建構之個資保護完整架構。

第二款 個別情形之授權規範

延續前揭架構，依照學者見解，法院使用已確定案件卷證中個資，其正當性基礎，由德國刑事訴訟法中之具體授權規範，以及相容性判斷兩部分構成。第 474 條屬於一般性之授權規範，主要針對公務機關間之資料傳遞，而對於其他種類之接收方，則存在不同要件之授權規範，以下介紹之。

第一目 對私人及其他機構提供卷證資料

第 475 條乃對私人及其他機構提供卷證資料之授權規範，其所提供之個資理論上無論屬於進行中或已確定之案件均可，惟僅得提供給該等私人或其他機構之律師；該等私人乃指程序外之第三人，若為被告、自訴人(Privatkläger)、附加訴訟人(Nebenkläger)、被害人、沒收參與人、鑑定人等，均適用各該閱卷特別規定，而不適用本條³⁴⁷。

第 475 條第 1 項第 1 句要求，聲請人需「就卷證訊息說明存在正當利益³⁴⁸」，且學說認為，聲請人需說明對所請求的資料有何利益及其範圍，並證明該等利益存在之事實，但對此證明程度之要求則不高，僅低於表面證據(Glaubhaftmachung)，

³⁴⁶ Gola/Heckmann/Heckmann/Scheurer, 13. Aufl. 2019, BDSG § 49 Rn. 16-17. 參照本文第二章第二節第二項、第三章第二節第三項第二款第三目之說明。

³⁴⁷ KK-StPO/Gieg, 8. Aufl. 2019, StPO § 475 Rn. 1. BeckOK StPO/Wittig, 42. Ed. 1.1.2022, StPO § 475 Rn. 2, 4. 林鈺雄，註 8 文，頁 209-210。

³⁴⁸ 翻譯參考連孟琦譯，註 316 書，頁 447。

以避免濫行聲請³⁴⁹。司法機關審酌是否提供卷證資料時，則應考量到卷證中含有關於犯罪行為人或被害人的人身或犯罪事實等相關資訊，仍屬於個資，提供答覆或允許查閱卷證都構成對個人基本權之干預，反面而言，基本權保護將對接觸卷證資料造成阻礙與限制，在利益權衡時，法院應於第 33 條之程序中保障將受影響之人的法定聽審權，聽取其意見³⁵⁰。若相關參與人的聽審權未受法院保障，訴訟程序具有瑕疵(schwerwiegenden Verfahrensfehler)，應透過上訴救濟³⁵¹。

法院於個案中仍須權衡提供之利益與保密之利益，並考量是否可使聲請人查閱經過匿名化之資料，若資料當事人有優於聲請人之利益，諸如隱私秘密、商業秘密、營業秘密、租稅秘密等，則法院不應提供卷證資料³⁵²。需注意的是，第 475 條並非法院向新聞媒體提供資料的法律依據，在德國基本法第 5 條第 1 項第 2 句所保障之新聞自由下，法院亦應依個案考量新聞自由與其衝突的利益，媒體報導內容亦應考量是否將對受判決人的再社會化造成阻礙等因素，並依各邦特別規定為之³⁵³。若聲請人為有理由，接觸卷證資料的方式亦相當限縮，其範圍僅為涉及該聲請人個資之決定、涉及秘密偵查如何進行，與關於該聲請人之調查結果的部分，且方式原則上為提供答覆，並不能直接閱覽卷證³⁵⁴。

依第 475 條聲請近用卷證資料的合法性，雖然門檻不高，但法院就本條正當利益要件，需綜合資料當事人之利益、傳遞行為是否將危害刑事程序目的，或是否與其他法律規定牴觸等諸多因素進行權衡，因此適用結果上，聲請人的正當利益就算確實存在，往往也未優位於其他利益，較難以由此獲取卷證中個資³⁵⁵。本條之聲請人的特殊救濟程序，依第 480 條為之³⁵⁶。

³⁴⁹ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 475 Rn. 4.

³⁵⁰ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 475 Rn. 2; § 474 Rn. 1. 此處指於案件進行中提供卷證內個資的情形。

³⁵¹ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 475 Rn. 2; § 478 Rn. 3.

³⁵² *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 474 Rn. 3; § 475 Rn. 5-6; § 477 Rn. 3.

³⁵³ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 475 Rn. 10. 舉例而言，下薩克森邦對於新聞報導的現行方針，參照 Arndt Sinn 著、吳瑛珠譯，裁判書公開於德國之實踐(中)，司法周刊，1927 期，2018 年 11 月，2-3 版。

³⁵⁴ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 475 Rn. 1b, 2.

³⁵⁵ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 475 Rn. 1a; § 477 Rn. 3.

³⁵⁶ *BeckOK StPO/Wittig*, 42. Ed. 1.1.2022, StPO § 475 Rn. 17.

第二目 為學術研究目的提供卷證資料

第 476 條則為學術研究目的之使用提供法律基礎。本條所稱科學研究之範圍相當廣泛，只要符合本條第 1 項第 1 句各款之大專院校、其他學術研究機構以及公務機關，甚至博士候選人，所進行之獨立研究均屬之³⁵⁷。此處資料接收方亦屬私人或其他機構，與第 475 條相同，惟基於促進科學研究發展等目的，並尊重德國基本法第 5 條第 3 項之學術研究自由，本條對於學術研究另設合法性要件，依本條第 1 項第 1 句第 3 款及第 2 項，「研究工作之公共利益、學術利益，顯然優於受干預人對於不予傳遞數據所值得保護之利益時³⁵⁸」，則認為進行研究的公共利益值得保護，亦屬德國基本法中學術研究自由與一般人格權的平衡；惟在其所進行之研究主題僅為大眾科學或偽科學、研究方法明顯在事實上不能執行、假借研究名義而刺探個資、或可預見研究結果將用作商業競爭之工具等情形，學者認為該等研究之利益不如資料當事人之利益，故該等傳遞行為將不具合法性³⁵⁹。附帶言之，若研究機構已取得當事人同意，則法院不需再進行利益衡量，但研究機構應循其領域之研究倫理取得當事人同意，而不得規避之³⁶⁰。

第 476 條僅涉及學術研究目的，關於檔案管理、統計、歷史目的之使用，則未規範於德國刑事訴訟法，而見於聯邦資料保護法第 50 條。聯邦資料保護法第 50 條乃將 2016/680 指令第 4 條內國法化之規範，但與歐盟指令不同的是，德國法要求檔案管理、學術研究、統計、歷史目的下之個資使用，需同時具備公共利益，而歐盟指令僅對檔案管理目的有此要求³⁶¹。然而，就該等目的使用卷證資料時，研究機構仍須遵循聯邦資料保護法、2016/680 指令及 GDPR 規範中，對於個資使用之相關限制與踐行保護措施，以保障資料當事人之權利³⁶²。

³⁵⁷ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 476 Rn. 2.

³⁵⁸ 翻譯參考連孟琦譯，註 316 書，頁 449。

³⁵⁹ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 476 Rn. 2.

³⁶⁰ A. a. O.

³⁶¹ *Gola/Heckmann/Kroh*, 13. Aufl. 2019, BDSG § 50 Rn. 7.

³⁶² 參見本文第三章第二節第三項第二款第三目之說明；另須注意，聯邦資料保護法第 50 條亦對資料當事人之權利保護有所要求，包含技術上與組織上之措施，特別是匿名化，參見本文註 95

第 476 條多規範研究機構使用卷證資料所負之義務，包含保密義務³⁶³、再用於其他研究之限制³⁶⁴、接受主管機關之監管等³⁶⁵；法院審查傳遞行為之合法性時，亦將依循本條第 1 項要件，對研究機構進行考量，若法院准許提供卷證資料，依本條第 2 項，應優先考量由卷證資料提供答覆，而不直接准許查閱卷證³⁶⁶。

第三款 一般性之限制

對於卷證資料使用的一般性限制，規定於第 479 條，本條亦為第 474 條至第 476 條之總結性規定，依該等條文進行傳遞行為時，亦須符合本條，而第 8 編其他條文亦有準用³⁶⁷。本條為傳遞卷證資料之限制，乃刑事訴訟的證據使用規則，與證據使用禁止之法則不同，前者涉及執法機關是否得使用證據資料、用於何目的之問題，後者則是關於在哪些情況下某些證據具有證據能力，法院得採為裁判基礎的問題³⁶⁸，本文研究聚焦於前者。

本條第 1 項第 1 句規定，「若傳遞抵觸刑事程序目的，包含危及其他刑事程序調查目的，或特別之聯邦法或相應之邦法使用規定，則不由卷證資料提供答覆或查閱卷證³⁶⁹。」學者認為，此處刑事程序之目的主要為發現真實，惟發現真實的利益，並不優於證人之證言不受影響之利益(unbeeinflussten Zeugenaussage)；反面而言，若將發現真實置於證人陳述任意性之利益之前，則不僅將抵觸閱卷權之規定，甚至將侵害證人的不自證己罪權利³⁷⁰。例如在偵查中揭露警詢筆錄內容，可能將使法院過早形成心證而產生預斷危險，亦可能因此阻礙證人行使拒絕證言權³⁷¹。

之說明。亦參見 *Gola/Heckmann/Krohm*, 13. Aufl. 2019, BDSG § 50 Rn. 8-11.

³⁶³ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 476 Rn. 4.

³⁶⁴ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 476 Rn. 5.

³⁶⁵ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 476 Rn. 6.

³⁶⁶ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 476 Rn. 3.

³⁶⁷ 舊法版本參見 *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 477 Rn. 1. 林鈺雄，註 8 文，頁 213。

³⁶⁸ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 477 Rn. 3.

³⁶⁹ 舊法版本翻譯參考連孟琦譯，註 316 書，頁 451；本文此處所指的 2021 年新法僅變更條號次序，內容與舊法相同。參照 *BeckOK StPO/Wittig*, 42. Ed. 1.1.2022, StPO § 479 Rn. 2, 2.1.

³⁷⁰ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 477 Rn. 3. *BeckOK StPO/Wittig*, 42. Ed. 1.1.2022, StPO § 479 Rn. 3; 3.1.

³⁷¹ A. a. O. 證人依第 475 條聲請閱覽卷證，也常因此理由而遭駁回，參見 *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 475 Rn. 1a.

第 479 條第 2 項第 1 句規定，「若某項處分依本法僅在特定犯罪嫌疑情況下得實施，則根據該處分所獲得之個人資料，在其他刑事程序中使用時，應受第 161 條第 3 項拘束³⁷²。」本句所指條文則規定，「若依本法限於具有特定犯罪嫌疑才得為某項處分，對於依其他法律所為之同類處分蒐集之個人資料，僅在為查明依本法得命該處分之犯罪時，方得不經處分受干預人同意，在刑事程序中為證據目的而使用³⁷³。」需注意的是，此處「為證據目的」不一定得推導出，附帶的調查結果也得作為證據，例如附帶搜索、另案扣押等情形，即使該等處分並不涉及本句所指處分要件中之罪名清單；學者強調，在未徵得資料當事人同意的情況下，在其他刑事程序中使用該等個資作為證據時，新的使用目的也需與允許使用該刑事程序措施的罪名有關，故應回歸蒐集個資時所採取的強制處分要件，判斷該等個資得否進行目的外使用；另外，在原程序中合法取得的個資，在該處分要件之罪名清單中，同一犯罪的不同實施行為類型、構成要件，或其他廣義共犯，只要仍屬程序法上同一罪名，仍得使用該等個資作為證據資料³⁷⁴。第 479 條第 2 項第 2 句各款則授權，依前句取得之個資，用於刑事程序以外之目的，其中第 4 款即明訂第 476 條之學術研究目的使用屬之³⁷⁵。

針對已確定案件之卷證資料，證人若欲取得卷證資料內容，是否仍受第 479 條第 1 項、第 2 項之限制，需考量同條第 3 項，在「被告受無罪宣告、拒絕開啟審判程序或程序終止」或「有罪判決未被記錄在機關之刑事記錄證明中，且自裁判確定時起已逾 2 年」，「僅於釋明獲知資訊之法律上利益，且先前之被告對於拒絕答覆無值得保護之利益時，方得對非公務機關由卷證資料提供答覆或查閱卷證³⁷⁶」。學者認為，本條第 3 項對依第 475 條提出聲請之私人設下嚴格要求，使其必須說明其理由與提出其正當利益的表面證據，且必須排除被告具有值得保護

³⁷² 舊法版本翻譯參考連孟琦譯，註 316 書，頁 451。

³⁷³ 舊法版本翻譯參考連孟琦譯，註 316 書，頁 216。此處新法僅改變項次。

³⁷⁴ 學說上以「假設性的替代干預」(hypothetischen Ersatzeingriffes verwertet)稱呼此現象，參見 *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 477 Rn. 3; *BeckOK StPO/Wittig*, 42. Ed. 1.1.2022, StPO § 479 Rn. 5a; *BeckOK StPO/Sackreuther*, 42. Ed. 1.10.2021, StPO § 161 Rn. 16.

³⁷⁵ *BeckOK StPO/Wittig*, 42. Ed. 1.1.2022, StPO § 479 Rn. 8.

³⁷⁶ 本條項之翻譯參考連孟琦譯，註 316 書，頁 451。新法未修訂之。

之利益，乃正確的立法³⁷⁷。法院居於傳遞機關，依本條第4項第2句，原則上僅審查傳遞請求是否屬於接收方之職務範圍；依本條第4項第1句，只要接收方是公務機關或律師，則傳遞合法性之責任由其負擔³⁷⁸。

綜上，第479條對於個資傳遞之限縮，可視為目的拘束原則之落實³⁷⁹。進一步而言，本文認為本條重視出於刑事目的之來源的個資使用，與後續目的外使用之相容性。本條規定目的外使用卷證中個資之行為，除須符合第474條至第476條等規範外，尚須符合本條限制，考量在何種情形下，出於刑事目的之卷證資料才能轉作其他目的使用。本文以為，德國刑事訴訟法雖未明文繼受歐盟指令，但在制度架構上仍與其十分相似，均以合法性要件加上相容性之模式，作為個資目的外使用行為之正當化基礎。

第三項 其他資料使用規則

前述第8編第1章乃卷證資料使用之授權條款，規範法院使用該等資料之正當性與應受之限制；第2章則為使用卷證資料之規則，但不涉及儲存卷證或使用電子檔案的合法性³⁸⁰，而為「刑事程序中個資可能被處理的受干預人之個資保護規定³⁸¹」。本章中的授權規範用語為「資料」而非前章所稱「卷證」，暗示依本章規定下之使用行為，涉及但不限於卷證資料，其他來源之個資亦可屬之。例如第484條第2項、第3項所稱之「其他資料」³⁸²。本文將介紹第483條至第487條規定，說明一般性之資料使用規則。

第一款 資料使用規則

第483條規定為現在之刑事程序使用資料，其第1項規定，「只要為刑事程序目的所必要，法院、刑事追訴暨執行機關、觀護人、行為監督之監督機構及司

³⁷⁷ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 477 Rn. 4.

³⁷⁸ 本條項之翻譯參考連孟琦譯，註316書，頁451。新法未修訂之。

³⁷⁹ 林鈺雄，註8文，頁213。

³⁸⁰ *BeckOK StPO/Wittig*, 42. Ed. 1.1.2022, StPO § 483 Rn. 1, 3.2.

³⁸¹ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 483 Rn. 1. 林鈺雄，註8文，頁217。

³⁸² 林鈺雄，註8文，頁218-219。

法輔助機構，得儲存、更改及利用資料中之個人資料³⁸³。」惟蒐集個資行為仍需另由法律授權³⁸⁴。學者認為，本條項對於檢察實務的意義重大，賦予其為刑事程序目的而儲存、更改及使用個資的權限，並填補聯邦憲法法院人口普查判決以來的授權條款空缺³⁸⁵。對法院而言，本條項亦賦予法院相同權限，在刑事程序進行中，亦即由偵查開始至執行程序終結³⁸⁶，得以使用資料。惟本文認為，依院檢與其他司法機構間之任務分配不同，以及本條項之一般性條款地位，法院仍不得恣意使用個資，故本條項在適用上仍相對嚴格。就本文研究範圍而言，為符合目的拘束原則，在被告最終無罪釋放、未開啟審判程序、或訴訟程序終結確定後，法院若欲繼續儲存其資料，則需進行第 489 條之特殊個案審查³⁸⁷。第 483 條第 1 項各款則明定使用卷證資料時，必須指明所涉及的程序、法律基礎、所涉罪名、資料當事人之資訊獲知權、儲存與刪除的期間等³⁸⁸。

第 484 條則為將來刑事程序目的而使用個資之規範，其第 1 項具體規定可供儲存、更改及利用之個資的範圍，在此之外的其他個資，則由第 3 項所稱之法規命令進一步界定細部範圍，並於第 2 項要件下方可使用³⁸⁹。本條規範目的在於保留曾在刑事程序中出現的資料，而非以存檔形式在實質上進行蒐集資料行為，故本條純然規範未來的、壓制犯罪之活動(repressive Tätigkeit)，而非屬危險預防之警察任務(präventiv-polizeiliche Aufgabe)³⁹⁰。

第 484 條第 1 項各款明定為將來刑事程序目的得使用個資之範圍，包含「被告個人資料，以及只要有必要，其他適合識別之特徵；管轄機構及案號；犯罪之詳細描述，尤其是犯罪時間、犯罪地點及大約損害額；犯罪指控，以表明法律規

³⁸³ 舊法版本翻譯參考連孟琦譯，註 316 書，頁 456。新法就此未更動。

³⁸⁴ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 483 Rn. 2.

³⁸⁵ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 483 Rn. 1. 林鈺雄，註 8 文，頁 217。

³⁸⁶ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 483 Rn. 2.

³⁸⁷ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 483 Rn. 3; *BeckOK StPO/Wittig*, 42. Ed. 1.1.2022, StPO § 483 Rn. 4.

³⁸⁸ *BeckOK StPO/Wittig*, 42. Ed. 1.1.2022, StPO § 483 Rn. 5.

³⁸⁹ 林鈺雄，註 8 文，頁 218。

³⁹⁰ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 484 Rn. 1.

定之方式為之；在檢察機關及法院之程序始末，並附上法律規定³⁹¹」。本條項主要適用於檢警機關，學者認為立法劃定之資料範圍相當寬泛，也賦予其較大的裁量空間³⁹²。同條第2項則規定，被告或犯罪參與人之其他個資儲存、更改及利用之前提，第2項第1句之合法性要件要求需對「犯罪方式或實施情況及被告或犯罪參與人性格或其他知悉情狀」進行全面評估，並須具備必要性，始得使用該等個資，法院的角色即是對此要件及必要性進行司法審查³⁹³。第2項第2句則由立法者限縮該等個資之使用，若在被告受無罪判決確定等情形，而資料當事人並未犯罪，則亦不得依第1句之規定儲存、更改及利用³⁹⁴。第3項則授權由聯邦司法部、消費者保護部及各邦政府依其職權，以頒布法規命令方式細部界定該等各資範圍；由於其範圍具有高度不確定性，所涉及之資料當事人亦不限於曾受正式偵查者，故應符合上述要件方得使用之³⁹⁵。

第485條為檔案管理目的使用卷證資料之規範，屬於司法行政範疇³⁹⁶。其第1句規定，「只要為檔案管理目的所必要，法院、刑事追訴暨執行機關、觀護人、行為監督之監督機構及司法輔助機構，得儲存、更改及利用資料中之個人資料³⁹⁷」，條文中僅設下「必要性」要件，並未明定管理卷證的具體目的，亦未區分使用何種資料，學者批評授權過於寬泛³⁹⁸。「檔案管理」指的是建立檔案，記錄現有的檔案與檔案材料，尤其是整理行政紀錄與從收到卷證或調查開啟的各程序階段的時序性紀錄³⁹⁹。本條第2句、第3句則分別規定第483條為現在程序目的、第484條為將來程序目的，均可使用本條之資料。

³⁹¹ 翻譯參考連孟琦譯，註316書，頁457。

³⁹² *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 484 Rn. 2; *BeckOK StPO/Wittig*, 42. Ed. 1.1.2022, StPO § 484 Rn. 1. 本條項劃定之資料範圍，也與第492條第2項第1句所規定，聯邦司法局(Bundesamt für Justiz)之中央檢察機關程序登記資料庫(Zentrales staatsanwaltschaftliches Verfahrensregister)應登記之資料相同。

³⁹³ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 484 Rn. 3.

³⁹⁴ 林鈺雄，註8文，頁218-219。

³⁹⁵ 同前註。

³⁹⁶ 林鈺雄，註8文，頁219。

³⁹⁷ 翻譯參考連孟琦譯，註316書，頁458。

³⁹⁸ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 485 Rn. 1; *BeckOK StPO/Wittig*, 42. Ed. 1.1.2022, StPO § 485 Rn. 1.

³⁹⁹ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 485 Rn. 2.

第 486 條乃建立「共同資料」(gemeinsame Dateien)管理權責之規定，該等資料可能由多個檢察機關間、甚或跨邦之間共同管理，而由保管機關共同承擔其責任⁴⁰⁰。第 487 條則為資料之「開放條款」(“Öffnungsklausel”)，規範為了第 483 條至第 485 條之目的，以及本條第 1 項第 1 句「為赦免程序、剝奪行動自由措施之執行或刑事案件國際司法互助目的所必要⁴⁰¹」，得傳遞至儲存機關外之管轄機構，使得刑事司法系統內出現一個全面的資料傳輸網絡⁴⁰²。

綜上，本文認為，第 484 條至第 487 條之資料使用規則，已經總則性地說明為不同程序或司法行政目的使用個人資料的限制，該等規範之射程範圍亦包含已確定案件之卷證資料，而其授權之使用行為不限於原本刑事程序，亦屬目的外使用之授權規範。本文以為，第 8 編第 1 章各條文乃法院審酌不同對象之聲請，考量是否提供卷證內個資的授權規範；第 2 章則主要為法院主動依職權儲存、更改、傳遞、利用卷證等資料之授權規範，惟對於傳遞行為的不同對象，仍須注意第 8 編第 1 章各條文，與本章交互適用。

第二款 對受干預之資料當事人之義務

在法院等司法機關使用資料之過程中，資訊自決之基本權受干預之資料當事人，得就此對司法機關主張其權利；而法院等司法機關除須遵守授權規範使用資料外，對於因而受干預之資料當事人，依法亦負一定義務。本文欲舉司法機關之更正、刪除資料義務，及對資料當事人之告知義務為例，說明該等義務。

第 489 條規定，依第 483 條至第 485 條儲存資料時，對於其中個資，資料當事人有要求更正、刪除之權利；資料控制者，即司法機關，則基於維護資料之真實性、完整性原則，負更正之義務，而基於目的拘束原則，負有屆期刪除之義務，無待當事人請求⁴⁰³。由司法機關義務的角度，個人資料毀損發生時，將資料回復原狀的法源即是本條。本條舊法第 8 項規定，「當儲存機構確定，不正確或應

⁴⁰⁰ BeckOK StPO/Wittig, 42. Ed. 1.1.2022, StPO § 486 Rn. 1-4.

⁴⁰¹ 翻譯參考連孟琦譯，註 316 書，頁 459。

⁴⁰² KK-StPO/Gieg, 8. Aufl. 2019, StPO § 487 Rn. 1.

⁴⁰³ KK-StPO/Gieg, 8. Aufl. 2019, StPO § 489 Rn. 1-2.

刪除或應封鎖之個人資料已被傳遞時，若為維護受干預人值得保護之利益有必要，應通知接收者予以更正、刪除或封鎖⁴⁰⁴」，新法刪除後，回歸聯邦資料保護法規定，儲存機構仍負該等義務⁴⁰⁵，此亦屬於法院等司法機關之義務。最後，當事人欲對司法機關更正、儲存其個資行為提起救濟，其管道為依 EGGVG 第 23 條以下，向法院請求⁴⁰⁶；原儲存機關在刪除期間屆至後，不得保留任何資料、甚或其副本⁴⁰⁷。

第 491 條規範司法機關提供資料當事人答覆義務，原則上保障人民獲知其個資是否被用於刑事程序之權利，落實一般人格權及資訊自決之基本權⁴⁰⁸，然而刑事訴訟法之其他特別規定亦應優先適用，例如第 475 條向私人或其他機構提供已確定案件之資訊⁴⁰⁹。本條第 1 項規定，若有數個機關均使用個資，而資料當事人無法辨別任一機關當責，當事人得向任一機關請求，由該機關決定是否提供資訊，以簡化程序⁴¹⁰。本條第 2 項明文準用聯邦資料保護法第 57 條，若未抵觸刑事訴訟法，則須落實資料當事人之資訊獲知權⁴¹¹。聯邦資料保護法第 57 條在體系上屬於繼受 2016/680 指令章節之條文，繼受 2016/680 指令第 15 條而來⁴¹²，規定當事人受告知權所能取得之資料範圍。第 491 條提供資料之範圍見於聯邦資料保護法第 57 條第 1 項各款，包含所儲存個資之來源、種類、傳遞與接收方之身分、以及儲存之目的⁴¹³。資料當事人對於其資訊獲知權之救濟，則依 EGGVG 第 23 條以下之程序為之⁴¹⁴。

綜上，就本文研究範圍而言，在更正、刪除義務方面，德國刑事訴訟法配合

⁴⁰⁴ 翻譯參考連孟琦譯，註 316 書，頁 463。

⁴⁰⁵ *BeckOK StPO/Wittig*, 42. Ed. 1.1.2022, StPO § 489 Rn. 12.

⁴⁰⁶ *BeckOK StPO/Wittig*, 42. Ed. 1.1.2022, StPO § 489 Rn. 13.

⁴⁰⁷ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 489 Rn. 7.

⁴⁰⁸ *BeckOK StPO/Wittig*, 42. Ed. 1.1.2022, StPO § 491 Rn. 1. 本條舊法版本參見連孟琦譯，註 316 書，頁 464-465；學者批評舊法並未全面準用 BDSG 規定，與 2016/680 指令之要求不符，新法已修正此問題，參照 *BeckOK StPO/Wittig*, 42. Ed. 1.1.2022, StPO § 491 Rn. 1.1.

⁴⁰⁹ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 491 Rn. 1.

⁴¹⁰ *BeckOK StPO/Wittig*, 42. Ed. 1.1.2022, StPO § 491 Rn. 10.

⁴¹¹ *BeckOK StPO/Wittig*, 42. Ed. 1.1.2022, StPO § 491 Rn. 1.

⁴¹² *Gola/Heckmann/Werkmeister*, 13. Aufl. 2019, BDSG § 57 Rn. 5-6.

⁴¹³ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 491 Rn. 4.

⁴¹⁴ *BeckOK StPO/Wittig*, 42. Ed. 1.1.2022, StPO § 491 Rn. 9.

其固有之 EGGVG 救濟制度，對於資料當事人之保護相當完善；在當事人之資訊近用方面，德國刑事訴訟法雖無規定司法機關負直接告知義務，但明文採取與 2016/680 指令程度相同的保護措施，使欲了解自己個資使用情形的資料當事人，原則上均可向司法機關請求該等資訊，法院亦透過 EGGVG 救濟制度審核該等決定。

第四項 救濟途徑與法院之審核

本文業已介紹德國刑事訴訟法上，關於司法機關傳遞卷證中個資之相關規範，而在刑事訴訟法本身與 EGGVG 中，也為了欲查閱卷證之聲請人設有針對該等規範的救濟管道。就本文研究之角度，法院縱然在德國法下，對於已確定案件卷證資料之傳送，不總是居於傳遞機關地位，但在救濟程序中，事後審查傳遞機關之決定時，亦須通盤考量傳遞行為是否完整具備正當化基礎。本文將介紹德國法上兩種對於傳遞已確定案件之卷證中個資的救濟程序。

第一款 刑事訴訟法中之救濟

德國刑事訴訟法第 8 編之救濟規定，見於第 480 條第 3 項，其第 1 句「在第 475 條之情形中，不服檢察官第 1 項之決定，得向依第 162 條有管轄權之法院聲請法院裁判⁴¹⁵」，即屬於欲取得卷證資料之私人的救濟程序。若依第 475 條聲請獲得已確定案件之卷證資料，在案件進行中，尤其是偵查尚未終結時，此時不得對受命法官之決定提起抗告⁴¹⁶。此屬審判權歸屬之特別規定⁴¹⁷，在該等程序中，刑事訴訟法中有關救濟之一般性規定、抗告、裁判費用等規定準用之⁴¹⁸。第 480 條第 3 項並無規範依據第 474 條或第 476 條使用已確定案件之卷證資料的情形，此時聲請人應依 EGGVG 第 23 條以下提起訴訟，由刑事法院審理⁴¹⁹。在該等程

⁴¹⁵ 舊法版本翻譯參考連孟琦譯，註 316 書，頁 452-453。新法僅變更條次。

⁴¹⁶ BeckOK StPO/Wittig, 42. Ed. 1.1.2022, StPO § 480 Rn. 7.

⁴¹⁷ A. a. O. KK-StPO/Gieg, 8. Aufl. 2019, StPO § 478 Rn. 5.

⁴¹⁸ 實際準用之條文清單為第 297 條至第 300 條、第 302 條、第 306 條至第 309 條、第 311a 條及第 473a 條，參見第 480 條第 3 項第 2 句。

⁴¹⁹ KK-StPO/Gieg, 8. Aufl. 2019, StPO § 478 Rn. 5; BeckOK StPO/Wittig, 42. Ed. 1.1.2022, StPO §

序中，亦應注意保護資料當事人之聽審權，否則屬程序之重大瑕疵⁴²⁰。

法律未明文規定的是，在案件已確定後，第 475 條之聲請人就檢察機關之決定，是否仍適用第 480 條第 3 項第 1 句及第 162 條第 1 項等規定進行救濟？本文以為，因第 162 條第 1 項雖規定偵查中檢察官向法官聲請為「法官調查行為」(richterliche Untersuchungshandlung)，目的乃為保全訴訟或為保全、預先進行將來判決時所預期之處分⁴²¹，然第 480 條第 3 項第 1 句僅為審判權分配之規定，其後程序之規定在制度設計上已準用刑事訴訟法中關於救濟之規範，且第 480 條第 1 項亦指出，在案件中終結後，由檢察機關決定卷證資料之傳遞，故就體系上觀察，第 475 條之特別救濟程序，無論是在案件起訴前或終結後，均得適用⁴²²。

綜上，在傳遞卷證資料的三種情形，傳遞對象為私人之第 475 條，其救濟途徑適用刑事訴訟法內規定，取代原本的行政訴訟程序。傳遞對象為其他司法機關、公務機關之第 474 條，及對象為學術研究機構之第 476 條，則適用 EGGVG 救濟，乃司法行政處分之一般救濟管道。

第二款 法院組織法施行法之救濟

在本文研究範疇內，欲取得卷證資料的聲請人，針對檢察機關決定的救濟途徑，依照聲請人的身分不同，在德國法上分為雙軌。其一是刑事訴訟法第 475 條與第 480 條，針對訴訟外私人，依刑事訴訟法內規定救濟；另一是第 474 條與第 476 條，針對司法機關等公務機關，以及學術研究機構，由 EGGVG 第 23 條以下規定救濟⁴²³。

由於 EGGVG 第 23 條以下規定之救濟範圍相當廣泛，橫跨刑事法與行政法

480 Rn. 8.

⁴²⁰ *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 478 Rn. 3; *BeckOK StPO/Wittig*, 42. Ed. 1.1.2022, StPO § 480 Rn. 9.

⁴²¹ 參照連孟琦譯，註 316 書，頁 218。

⁴²² 梁哲璋，註 12 文，頁 318 中說明，就司法行政處分設有特別規定可向普通法院救濟者，如刑事偵查程序有關強制處分的權利侵害，於刑事訴訟法中設有即時救濟機制，例如(舊法)第 478 條第 3 項(現行德國法第 480 條第 3 項)；該文獻第 301-302、313 頁亦指出，法官非基於審判獨立下之行為，如對第三人聲請閱覽卷證之決定，屬司法行政行為。本文以為，對於第三人聲請閱覽卷證之決定，無論在偵查中、案件進行中或審判後，本質上應無太大區別，其適用之救濟管道亦應相同。

⁴²³ *BeckOK GVG/Köhnlein*, 14. Ed. 15.2.2022, EGGVG § 23 Rn. 90, 91.

等各大法領域，德國註釋書亦以龐大篇幅一一介紹幾乎所有適用此一管道的案件類型⁴²⁴。然而，並非所有類型均屬本文在此關注的對象，本文將簡介 EGGVG 第 23 條等規定，說明何謂司法行政處分，並就刑事法院審核已確定案件之卷證資料部分進一步說明。

司法行政處分在德國法上，意指「司法行政機關就規制民法、商事法、民事訴訟、非訟事件及刑事司法之個別事件，所為之命令、處分或其他措施⁴²⁵。」該等行為在法律上並無明確定義，單方高權行為均可屬之，而不限於行政法領域之行政處分概念，惟該等行為以 EGGVG 列舉之法領域事項為限⁴²⁶。司法行政處分概念乃是為了救濟途徑之審判權劃分而創設，具有一定的工具性質，並隨德國行政法院審判權規定而演進，本身與組織法或作用法上既有的法律相關概念並不完全相同⁴²⁷。此制度基於「事務相近性」之考量，將原本由行政法院審理，但與民刑事或非訟法領域具有緊密實質關聯的案件類型，改由本較為熟悉此等事務之普通法院審理，以簡化救濟體系，並減少裁判紊亂等情形⁴²⁸。司法行政處分可分為三要件：「司法行政機關」，任何從事 EGGVG 第 23 條第 1 項列舉之司法事務，從事高權行政任務者屬之；「法定列舉司法事務領域之特別事件」，與民商事、民事訴訟、非訟事務、刑事司法領域事務相關；「單方高權行政行為」，直接對外發生一定法律上或事實上效果⁴²⁹。在實務上，個案是否屬於司法行政處分，仰賴學說及實務的累積，針對本文研究範圍，對於已確定案件卷證資料之傳遞屬之⁴³⁰。

對於司法行政處分之救濟，依 EGGVG 第 23 條至第 30 條規定為之，其細部規定乃在普通法院審判體系中，建立一套「袖珍版」、較為簡便的行政訴訟程序，

⁴²⁴ *KK-StPO/Mayer*, 8. Aufl. 2019, EGGVG § 23 Rn. 54-115; *BeckOK GVG/Köhnlein*, 14. Ed. 15.2.2022, EGGVG § 23 Rn. 79-185.

⁴²⁵ 翻譯參照梁哲瑋，註 12 文，頁 290。亦參照本文第一章第三節第一項之說明。

⁴²⁶ *BeckOK GVG/Köhnlein*, 14. Ed. 15.2.2022, EGGVG § 23 Rn. 16. 梁哲瑋，註 12 文，頁 305-306。

⁴²⁷ 梁哲瑋，註 12 文，頁 299。此制度之演變亦參照該文獻，頁 290-295。

⁴²⁸ 梁哲瑋，註 12 文，頁 294-295。

⁴²⁹ 梁哲瑋，註 12 文，頁 299-317。

⁴³⁰ 參照本項前款之說明。

其內容涵蓋聲請救濟之權利保護要件、審判權、實體裁判要件、對第一審裁判不服之救濟等⁴³¹。與德國刑事訴訟法中第 475 條、第 480 條第 3 項等救濟規定比較，本文認為，就審判權劃分，第 474 條至第 476 條之救濟均由刑事法院審理，似無太大差別；但第 474 條、第 476 條乃資料當事人聲請救濟，第 475 條乃欲取得卷證資料之聲請人為之，前者屬於個人對抗國家機關之傳統行政爭訟，後者亦屬聲請人與國家機關間紛爭，準用刑事訴訟法中抗告規定，另亦重視資料當事人於程序中之聽審權保障⁴³²，二者情形在程序上的需求不同，也適用不同救濟管道。

第五項 小結：卷證中個資保護的基本體系

本文整理德國刑事訴訟法第 8 編第 1 章、第 2 章等規定，說明卷證中個資使用與保護的規範情形。本文認為，德國在 2016 年 GDPR 與 2016/680 指令公布後之修法，使刑事訴訟法第 8 編規定至少符合歐盟規範，或比歐盟規範更嚴格，展現出重視卷證資料中個資保護的趨勢。爬梳德國法的條文與體系後，本文觀察到，德國法於體系上將司法機關等公務機關傳遞卷證資料與其救濟規定，置於第 1 章，而將卷證資料的其他管理規則置於第 2 章；第 1 章中的第 474 條至第 476 條，規範不同主體要求傳遞卷證資料時，傳遞機關之授權規範；第 2 章中的第 483 條至第 485 條則規定卷證資料之控制者在不同目的下，得主動使用卷證資料。本文以為，第 1 章與第 2 章規定中，卷證資料、司法機關等規範主體雖然重疊，但所指脈絡不同，因而有分別設置條文的必要。然而這兩組條文也並非平行規定，司法機關使用卷證資料時，亦可能同時涉及第 1 章與第 2 章規定，而均需遵守之；若有刑事訴訟法未規定的情形，則以聯邦資料保護法規定作為補充；資料當事人亦可能尋求 EGGVG 第 23 條以下規定之救濟。

⁴³¹ 詳參梁哲瑋，註 12 文，頁 298。

⁴³² 文獻指出受干預之資料當事人此處之聽審權保障應類推適用第 33 條，法院對於程序參與人之聽詢(müssen die Betroffenen analog § 33 regelmäßig angehört werden)，參照 *KK-StPO/Gieg*, 8. Aufl. 2019, StPO § 478 Rn. 3; *BeckOK StPO/Wittig*, 42. Ed. 1.1.2022, StPO § 480 Rn. 4, 5. 連孟琦譯，註 316 書，頁 17。

與我國法相較，德國刑事訴訟法對於卷證中個資的使用與保護，從授權規範到救濟管道一應俱全，體系較為完整。就其救濟途徑與補充性法源依據而言，德國法亦可援引固有的完善規定，如EGGVG與聯邦資料保護法，作為其配套措施。我國刑事訴訟法尚無關於此的授權規範，而在補充性法源方面，個資法或政府資訊公開法亦無明確規範或配套措施，留下許多解釋空間。本文以為，我國現行法對此領域的規範密度不足，根本的解決之道並非再由現有規範擴充解釋，而為制定新的規範，令卷證使用與個資保護的法制體系完整發展，同時亦能兼顧法律明確性與個資保護基本原則，如目的拘束原則的要求。在此背景下，本文認為歐盟法與德國法屬於良好的借鏡對象。



第五章 對現行實務之建議及立法構想

本文已經回顧個人事訊自主權之理論發展，並嘗試分析法院使用卷證中個資的行為態樣，再引介比較法上相應規範，希望做為我國法制發展的參考對象。本章將對於前述論述中所點出之問題，提出現行法下可能的應對措施，以及立法論上的建議。針對已確定案件之卷證中個資使用，現行法欠缺對於司法機關的授權規範，後續如使用行為的配套措施、救濟管道等，亦無相關規定。本文以為，現行法已不敷個資保護需求，另訂法律才是根本解決之道，本文進一步認為，基於刑事事務之相近性，應於刑事訴訟法中訂立特別規定，方能與固有規範接軌，形成完整的卷證使用及個資保護體系。

第一節 現行法欠缺及應補足之規範

在卷證中，個資保護的界線要從何畫起，是一個值得探討的前提問題。本文認為，個資的定義並不會隨著其來源而改變，此處的重點應為，在「刑事卷證中」的個資，與其他來源的個資相比，有何特殊之處，因而需要受到何等特別規範，故刑事訴訟法中毋庸再特別定義何謂個人資料，而由個資法規範即可。

至於我國法上個人資料的定義，於個資法第 2 條第 1 款已有規定，但此規定是否完善，則純然屬於個資法領域的問題。本文欲指出，以歐盟個資工作小組之資料關聯性(*relating to*)為判準，擴大保護範圍，使卷證中的資料納入個資保護的討論範圍，更能有效保障卷證中資料當事人之個人資訊自決權；惟本文旨在探討刑事訴訟法與個資法之交錯，在此不再深究。

刑事卷證中包含大量個人資料，而在司法系統中，卷證資料經由偵查、審理程序的整理，而產生容易與其他卷證資料連結的特性，屬於個人資料檔案。這些卷證中的個資與個人資料檔案，需要受到個資法與刑事訴訟法規範的保護，應無疑問。然而，個資法乃居於普通法地位的法律，在更專業的法領域需要更加細緻、

具體的授權規範⁴³³，但現行刑事訴訟法上卻幾乎沒有對於卷證中個資的保護及使用規範⁴³⁴，本文以為此等空缺應透過立法解決；而在此之前，從法院的角度，在適用現行法上有何需注意之處，亦為本章的核心。

依照整體法律體系，法院使用個資時，應先適用刑事訴訟法上的特別規定，但在此層次的規範付之闕如時，在現行法下，法院需適用個資法上的一般性規範。與法院有關的個資使用規範，乃個資法第 6 條關於敏感性個資的使用規範，第 7 條至第 14 條關於資料當事人告知、資訊近用等措施，以及第 15 條、第 16 條關於公務機關使用及目的外使用一般性個資的行為規範，前均已述及。

這些一般性的規範並不全然吻合刑事卷證的使用情況，因此在修法前有待學說、實務的發展補充。本文欲提醒的是，在大原則上，若使用卷證的行為涉及個資，則需遵守個資保護的重要原則，此亦體現於個資法第 5 條，「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。」本條強調個資使用應將資料當事人之權益納入考量，並尊重其權益，亦應遵守目的拘束原則。在個資法的體系上，本條亦列於所有使用規範之前，顯見其為個資使用行為的依歸。

第二節 建立事前評估及事後審核機制

本文以為，在現行法下，仍得嘗試建立卷證中個資使用之事前評估機制，並可運用現存制度作為事後審查機制。就事前層面，本文將介紹 GDPR 與 2016/680 指令中的資料保護影響評估制度(Data Protection Impact Assessment, DPIA)，並建議以 DPIA 之審查框架作為事前評估之內容。就事後層面，本文認為現有司法救濟程序足以擔負審查之責，惟仍須注意個資保護原則之要求。

⁴³³ 參照註 287。

⁴³⁴ 何賴傑，註 71 文，頁 183。

第一項 事前評估之建立

第一款 資料保護影響評估制度(DPIA)制度介紹

第一目 歐盟法上之 DPIA 制度

DPIA 乃比較法上之歐盟制度，見於 GDPR 第 35 條與 2016/680 指令第 27 條。兩個條文在其第 1 項中說明進行 DPIA 的前提時，使用了相同的文字：「在處理資料，特別是使用新興科技的情形，考量該處理方式之本質、範圍、脈絡、目的，認為該處理方式可能造成自然人之權利及自由之高度風險⁴³⁵」，而 GDPR 直接要求資料控制者在此前提下進行 DPIA，2016/680 指令則要求會員國應立法規定資料控制者進行 DPIA。就刑事目的使用而言，由於現實上往往難以提供資料當事人事前告知及資訊近用，以免與刑事程序目的衝突，由資料控制者，通常亦為國家機關進行 DPIA，即成為一種補救方式⁴³⁶。

DPIA 為「事前」的措施，亦即資料控制者須在處理個資前，先就 GDPR 或 2016/680 指令中所要求的事項進行預先評估，以掌握並試圖減輕使用之風險⁴³⁷。在使用已確定案件卷證中個資的情形，此時的資料控制者為檢察機關，其除了依法裁量是否提供該等資訊外，本文認為也適宜考慮加入 DPIA 的架構。

在 GDPR 與 2016/680 指令下，並非所有個資使用行為均須先進行 DPIA，而是當該等行為可能造成自然人之權利及自由的「高度風險」(high risk)時，資料控制者方有義務為之。GDPR 前言第 75 節、第 76 節，以及 AWP 29 之意見書均說明，高度風險應由該事件與後果切入，並以其嚴重性與發生可能性(severity and

⁴³⁵ “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[.]” See GDPR Art. 35 (1); EU Directive 2016/680 Art. 27 (1).

⁴³⁶ Paul De Hert & Vagelis Papakonstantinou, *supra* note 252, at 17.

⁴³⁷ Art. 29 Working Party, *supra* note 303, at 14. 何之行、廖貞，註 308 文，頁 150。張陳弘，註 64 文，頁 363-364。

likelihood)兩者，同為判斷標準⁴³⁸。進一步言之，GDPR 第 35 條第 3 項中例示三種須進行 DPIA 的情形，分別為「以自動化方式處理個資而對自然人的個人特質進行系統性及廣泛性的評估，包括個人特徵描繪行為(profiling)，以及基於該評估作成對該自然人產生法律影響或其他相似的重大影響之決定；大規模蒐用敏感性個資或前科及犯罪個資；大規模、系統性監督公眾得出入之區域⁴³⁹」。AWP 29 於意見書中則提出十項具備高度風險而須進行 DPIA 的判斷因子，若同時具備兩項以上，則需進行 DPIA；這些判斷因子中，與司法機關使用已確定案件卷證中個資相關的有：「為了對自然人剖繪所進行的資料蒐用，尤其是關於自然人的工作表現、經濟狀況、健康、個人偏好、個人行為模式等；蒐用敏感性個資；不同資料庫間的連結使用；資料當事人與資料控制者間存在不對等的權力關係⁴⁴⁰」。本文因而認為，司法機關使用該等個資前，應先進行 DPIA。

DPIA 應包含的內容，比較 GDPR 第 35 條與 2016/680 指令第 27 條，可發現兩者間存有差異。2016/680 指令要求應至少包含「對於該處理行為的概述、對於資料當事人權利及自由之風險評估、應對該等風險所採之保護措施、為遵循本指令所採之措施，並考量資料當事人及其他有關之人的權利與合法利益⁴⁴¹」。GDPR 第 35 條第 7 項各款則對其內容列舉出更詳細的規範，包含「系統性描述所預定的資料蒐用行為與目的；該蒐用行為與蒐用目的達成間之必要性與合比例性的評估；對於本條第 1 項規定之對於資料當事人之自由權利所生風險之評估；應對蒐用行為所生風險的方法，包括保護與安全措施、確保個資保護之機制，以及將資料主體與其他人相關之權利與正當利益納入考量後，證明蒐用行為符合 GDPR

⁴³⁸ Art. 29 Working Party, *id.* Katerina Demetzou, Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'highrisk' in the General Data Protection Regulation, 35 Computer Law & Security Review 1, 5 (2019).

⁴³⁹ Art. 29 Working Party, *supra* note 303, at 8. 翻譯參照張陳弘，註 64 文，頁 359。

⁴⁴⁰ Art. 29 Working Party, *supra* note 303, at 9-12. 翻譯參照張陳弘，註 64 文，頁 359-360。

⁴⁴¹ "[DPIA] shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Directive, taking into account the rights and legitimate interests of the data subjects and other persons concerned." See EU Directive 2016/680 Art. 27 (2).

要求⁴⁴²」。比較兩者，以刑事目的使用為背景所進行之 DPIA，不須考量新舊目的間之關聯性與相容性，此亦為在 2016/680 指令目的下之相容性判斷例外，前已述及⁴⁴³，除此之外，兩者實質上評估的內容一致。在資料控制者的不同使用目的下，則應分別適用其領域所屬的 DPIA 內容。

第二目 德國法上之 DPIA 制度

德國學者認為，在 2016/680 指令的範圍內，進行 DPIA 更顯重要，因為可以即時設置保護措施，避免未經授權者接觸個資⁴⁴⁴。在德國法上，刑事訴訟法中並未對 DPIA 設有特別規定，而由聯邦資料保護法第 67 條將 GDPR 第 35 條、2016/680 指令第 27 條此二關於 DPIA 的規範內國法化；該條文在架構上未如 GDPR 例示需進行 DPIA 的情形，因此學者認為其留下較廣的解釋空間，而涵蓋了 GDPR 第 35 條適用的所有情形，在 GDPR 與 2016/680 指令下關於 DPIA 的解釋，亦適用於聯邦資料保護法第 67 條⁴⁴⁵。

就 DPIA 之內容而言，學者認為，個資使用行為除需合法，還需符合比例原則，特別是手段目的間之衡平性原則，在刑事目的方面，例如依刑事訴訟法第 81h 條進行 DNA 群眾檢測，或依第 98a 條進行自動化資料比對，均屬應進行 DPIA，並應符合衡平性原則之情形⁴⁴⁶。

附帶言之，聯邦資料保護法第 67 條第 3 項重申 GDPR 第 35 條第 4 至 6 項，在進行 DPIA 時需同時通知外部監管之獨立機關，但 2016/680 指令第 27 條中並無此要求，學者亦認為，本條項並非一體適用於所有 DPIA，而需依不同目的背景下，決定是否須有外部獨立監管機關之介入⁴⁴⁷。

⁴⁴² 翻譯參照張陳弘，註 64 文，頁 357。

⁴⁴³ 參見本文第二章第二節第二項之說明。

⁴⁴⁴ *Gola/Heckmann/Nolte/Werkmeister*, 13. Aufl. 2019, BDSG § 67 Rn. 1.

⁴⁴⁵ *Gola/Heckmann/Nolte/Werkmeister*, 13. Aufl. 2019, BDSG § 67 Rn. 2.

⁴⁴⁶ *Gola/Heckmann/Nolte/Werkmeister*, 13. Aufl. 2019, BDSG § 67 Rn. 26.

⁴⁴⁷ *Gola/Heckmann/Nolte/Werkmeister*, 13. Aufl. 2019, BDSG § 67 Rn. 18.

第二款 我國相似制度

第一目 個資法施行細則第 12 條第 2 項第 3 款個人資料之風險評估及管理機制

我國法上與 DPIA 制度文字相近的規範，可參酌個資法施行細則第 12 條第 3 款規範之「個人資料之風險評估及管理機制」，屬於「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」之一，就其內涵亦無進一步的規定。就其性質而言，相較於 GDPR、2016/680 指令對於造成資料當事人自由及權利高度風險的情況，課予資料控制者進行 DPIA 之義務，我國個資法施行細則所規定者僅為適當維護安全措施的其中一項建議措施，二者在本質上與規範密度上均相異，我國法上並未如歐盟或德國法設有 DPIA 規範⁴⁴⁸。

第二目 於司法機關之裁量中加入 DPIA

本文認為，我國法上雖無 DPIA 制度，但在使用已確定案件之卷證中個資時，司法機關宜在其裁量中加入 DPIA 的內容，亦即在其理由中呈現其使用個資行為的概述、對於資料當事人權利及自由之風險評估、應對該等風險所採之保護措施、為遵循個資法所採之措施，以及考量資料當事人及其他有關之人的權利與合法利益。例如在檢察機關決定是否准許第三人或學術研究機構近用卷證資料時，即能依此架構，使其理由更為完備。而在可能的事後救濟程序中，法院也能在此基礎上建立較穩定的審查框架，針對先前決定的實質理由作出說理豐富的裁判。

第二項 法院之事後審查

第一款 個資使用之事後審查是否應受外部監管

在 GDPR 的制度設計下，原則上公務機關或私部門之個資使用行為須受外

⁴⁴⁸ 張陳弘，註 64 文，頁 350-351。

部獨立機關之監管⁴⁴⁹，但在司法領域，為了保持司法權之獨立性，即產生司法權下之個資使用，受監管之例外及解釋問題⁴⁵⁰。在歐盟及德國法架構下，審判相關事務因司法獨立性之保障，由法院內部自我監管，監督機關就此無管轄權限；而就司法行政相關事務，因已不屬審判權範圍，故可受獨立機關監管，德國法院中就此類事務亦設有個資保護官員⁴⁵¹。

就我國法而言，現行法上個資法之主管機關為國家發展委員會，其是否適格作為監管個資保護之獨立機關，或由其他機關充任，在法制面與政策面均尚未明朗⁴⁵²。本文認為，在我國缺乏此等機關的情況下，貿然採用與歐盟相同的監管框架並非好的作法。本文以為，在使用已確定案件卷證中個資之事後審查方面，應先利用現有之救濟管道，由法院審查司法機關使用行為之正當性基礎，其優點有二：第一，無論是基於審判權或司法行政而使用，資料控制者均為司法機關，由法院進行事後審查，比起經由另一外部機關審查，更有效率；第二，在司法程序中的事後審查，得以借助現有制度的嚴謹性，法院之裁判亦具有較強的既判力、執行力等法律效果，使事後審查更加有效。

第二款 事後審查之內容

延續前述觀點，法院在司法程序中，就檢察機關之決定進行事後審查，本文認為其實質判斷內容，可檢視檢察機關依 DPIA 架構所為之理由，並逐項評價其判斷之風險是否得當，所提出之保護措施是否適切、是否已落實等，最後以裁判之作用調和個資使用與保護。

除此之外，法院作成決定前，亦應注意個資保護之原則要求，諸如該等使用行為是否具備授權規範，是否已滿足資料當事人之資訊獲知權利，以及個資法第

⁴⁴⁹ GDPR 第 35 條第 1 項 a 款規定，除法院行使其司法權外，公務機關進行個資使用行為者，資料控制者應指定資料保護官(data protection officer, DPO)。就 DPO 及獨立機關地位之個資使用監管機關的詳細介紹，亦參見：GDPR 第 37 條至第 39 條、第 52 條；達文西個資暨高科技法律事務所，個資保護專責機關與資料在地化之法制研究，國家發展委員會委託研究報告，2018 年 5 月，頁 27-38。

⁴⁵⁰ Arndt Sinn 著、吳瑛珠譯，註 298 文，2 版。

⁴⁵¹ 同前註。

⁴⁵² 張陳弘，註 64 文，頁 392。達文西個資暨高科技法律事務所，註 449 文，頁 201-207。

5 條、第 11 條揭示之誠信原則、比例原則、目的拘束原則、資料最小化原則等⁴⁵³。雖然在事前評估中亦須注意符合這些原則，本文認為在事後評估中，同樣需檢驗該等使用行為是否遵循之，是故就需判斷的要素而言，並無本質上的不同。

第三節 立法建議

本文考察至此，亦將對現行刑事訴訟法就卷證中之個資使用規範提出立法建議。本文之建議分為三部分，第一部分建議立法增訂卷證中個資使用的一般性規範，令司法機關使用卷證中個資時有特別法位階之授權規範可循；第二部分建議增訂授權規範之配套措施，即司法機關相對應地須對資料當事人所負之義務，並以告知義務為例說明；第三部份則建議增訂關於司法機關使用卷證中個資行為的救濟程序。最後，本文試提出我國刑事訴訟法之修正構想，為未來可能的修法方向拋磚引玉。

第一項 已確定案件卷證中個資之使用規範

針對已確定案件卷證中個資之使用規範，有三種立法方向可考慮，分別為制定專法、修訂個資法或法院組織法等法律，以及修訂刑事訴訟法。有論者說明，專法為特別規範某種人事物之特別法律，適用於特殊狀況，而刑事訴訟法則是規範刑事程序中會面臨的一般情形⁴⁵⁴。本文以為，於刑事訴訟法中修訂卷證中個資使用的相關規定，比制定專法更為合適，理由有三：第一，由刑事程序產生之卷證資料，與刑事訴訟法之規範領域最為相近，在刑事訴訟法中設置規範，在法律體系上較為一貫，而若是在個資法等其他法律中設置卷證使用規範，則又增加與民事、行政法領域重疊之解釋空間；第二，在體系解釋上，關於刑事卷證之事務，於同一部法律中統一規定，可免除不同法律間交錯解釋可能產生之歧義，在實際適用上亦可避免規範於其他法律而漏未適用之困擾；第三，於刑事訴訟法中

⁴⁵³ 張陳弘，註 64 文，頁 378-382。該文獻以「臺灣社交距離 App」作為事前遵法之分析對象，本文則取其判斷框架。

⁴⁵⁴ 吳昭億，註 22 文，頁 189-190。

修訂，亦具有政策宣示作用，可宣示立法者對刑事程序中個資保護此領域之重視。

第二項 對於資料當事人之義務：以告知義務為例

過往刑事訴訟法著重於平衡被告與國家機關間不對稱權力，以及保障被害人之程序參與權利，而對於卷證中資料當事人之個資保護，幾乎無著墨。雖然卷證中出現的個資，大抵不脫訴訟關係人的資料，但本於其資訊隱私、個人之資訊自決等基本權，在與刑事程序目的不衝突的前提下，仍應設置規範，於一定程度保障該等權利，而非一概認為該等權利在所有情形中均劣於刑事程序背後的公共利益。

在現行法律與實務上，較接近本文討論者，乃法庭錄音錄影是否及如何公開的爭議。有實務見解認為，法院應審酌當事人聲請交付法庭錄音光碟之主張是否具有正當性及必要性，亦即為「主張或維護其法律上利益所必要」，但其中是否應考量資料當事人同意，或納入徵詢、表達意見之程序環節，尚無定見⁴⁵⁵。

本文以為，對於資料當事人之事前告知，縱然與刑事訴訟之目的及實務運作有所扞格，但在案件已確定後，使用卷證中個資之司法機關亦得負告知義務；而在事後或救濟程序中，亦應使資料當事人知悉其個資之使用狀況，並給予其表達意見之機會。

第三項 救濟程序

本文認為司法機關使用已確定案件卷證中個資，屬於司法行政處分，並於比較法章節中參考德國 EGGVG 第 23 條以下之法院組織法特別救濟程序。雖然我國法現無如同德國法制的司法行政處分與其救濟制度⁴⁵⁶，本文亦無意主張全盤仿效德國法，但欲指出，此類救濟程序乃為審判權分配而設，本身並未額外開放

⁴⁵⁵ 臺中高等行政法院 105 年抗字第 4 號裁定，轉引自吳志光，行政法上利益衡量方法論，台灣法學雜誌，411 期，2021 年 3 月，頁 6-7。

⁴⁵⁶ 梁哲瑋，註 12 文，頁 297，註 35。

權利保護功能⁴⁵⁷。本文僅欲說明本文認為較理想的審判權分配方式。

就現行法與實務而言，已確定刑事案件之卷證資料是否、如何公開，乃行政法院之管轄範圍⁴⁵⁸；惟本文認為，基於刑事卷證之使用，與刑事法院之作用範圍具有事務相近性，若該等事務由刑事司法機關進行決定，則救濟管道亦應留存於刑事司法系統中。刑事訴訟法規範刑事程序內的相關事務，但在程序終結、案件確定後，卷證使用之問題仍需透過刑事司法系統解決，故本文亦贊同立法修訂之。

第四項 立法構想之提出

本文參考歐盟規範與德國刑事訴訟法架構，提倡於我國刑事訴訟法最末接續增訂第十編「個人資料使用與保護」，其下設置二章，分別為卷證使用之授權規範，及資料使用規則。礙於能力與本文篇幅，本節在此並未擬出第十編的所有草案條文，而僅提出與司法機關使用已確定案件卷證中個資範疇內，第一章中部分的一般性卷證使用規範，及第二章中部份的資料規則；因此，以下提及之條號僅為依循現存刑事訴訟法而編輯，整體法律體系仍以本節之說明為主。

第十編第一章內容為卷證使用之總則性授權規範，包含一般性及目的外使用之規範。我國第 513 條規定得參考德國刑事訴訟法第 474 條，司法機關為司法目的所必要時，得查閱卷證，並依職權對其他公務機關由卷證資料提供答覆。惟僅提供答覆可能需要不成比例之耗費，或不足以履行其任務時，亦得使該公務機關直接查閱卷證。

我國第 514 條規定得參考德國法第 476 條，為研究目的，司法機關得將卷證資料傳輸予學術研究機構，且應一併規範其配套措施，包含：該學術機構之保密義務；學術機構對卷證中個資的保護措施要求，例如將個資使用行為與行政任務、商業目的之實現，於空間上、組織上分離；發表時之匿名化要求等。

⁴⁵⁷ 梁哲璋，註 12 文，頁 296-297。

⁴⁵⁸ 參見 108 年度高等行政法院法律座談會之結論、本文第三章第二節第三項第二款第一目之說明。

我國第 515 條規定得參考德國法第 479 條，設置傳遞資訊之方式及使用限制，並引入目的外使用之相容性要件：若提供卷證副本或僅提供答覆即可達成卷證使用之目的，則司法機關得僅提供副本或答覆；若卷證使用之目的或結果牴觸刑事程序目的，則司法機關不應准許之。此外，若卷證中部分資料乃由強制處分取得，則目的外使用於另案證據時，亦應於另案亦得為同類強制處分時，方得使用之。

最後，我國第 516 條規定得參考德國法第 480 條或德國法院組織法施行法第 23 條規定，設置審判中及審判後卷證資料聲請人之救濟管道，由刑事法院裁判，並準用抗告規定。

第二章內容為資料規則，包含為現在或將來刑事程序、檔案管理目的處理卷證資料之授權規範，以及資料當事人受告知之權利。

我國第 517 條規定得參考德國法第 483 條，我國第 518 條規定則得參考德國法第 484 條，分別規定為現在、將來刑事程序目的，刑事司法機關得使用已確定案件之卷證資料。需注意的是，為將來刑事程序而使用個資時，當被告受無罪判決確定，且裁判理由中說明受干預之資料當事人未犯罪，刑事追訴機關則不得再使用其個資。我國第 519 條規定得參考德國法第 485 條，為檔案管理之司法行政目的，法院亦得使用卷證資料。以上三個條文乃針對刑事司法系統內之個資使用，相對應的授權規範。

我國第 520 條規定得參考德國法第 489 條，當事人有要求管理卷證資料之機關更正、刪除其個資的權利，該機關亦負有主動更正以維護資料正確性，及儲存期滿主動刪除資料之義務。

我國第 521 條規定得參考德國法第 491 條，使用機關原則上應使受干預人，即資料當事人知悉其個資被使用的情形，並準用我國個資法第 7 條至第 9 條，關於告知義務的規定。惟若其他法律另有規定，或進行告知將有害於刑事程序進行，則例外毋庸為之。

第六章 結論

總結本文論述，本文欲指出現行法規的不足之處，並就現行法下法院如何使用已確定刑事案件卷證中個資提出裁量內容上的建議以及立法構想。對於已確定刑事案件卷證中個資，就整體法律體系以觀，由個資法作為司法機關使用行為的普通法，在解釋上過於寬泛而留下較多解釋空間，而現行刑事訴訟法幾乎沒有特別授權規範，出現法制上的空缺。本文將於以下整理各章內容，並作成結論。

本文在第一章、第二章中說明研究範圍，與卷證中個資保護所涉及的基本權之理論背景，結果如下：

1. 本文界定研究範圍時，已經指出法院除了擔負審判任務外，也兼具司法行政機關的角色，因而依據其不同任務角色，應適用不同規範作為授權基礎。
2. 刑事卷證中包含個人之病歷、醫療、基因、性生活、健康檢查及犯罪前科等一般性、敏感性個人資料，且經過偵查、審判程序的系統性整理，容易與其他卷證資料連結，而屬於個人資料檔案。
3. 關於我國資訊隱私權、個人資訊自決權等基本權利的理論及實務發展，本文認為無論釋憲實務或學說採用何種名詞，資料當事人對其個資均有自主權，受憲法第 22 條保障，而得決定使用或不使用之範圍及方式。

本文在第三章中以法院為觀察重心，整理司法機關使用刑事案件之卷證中個資的行為，分為基於審判目的使用與審判目的外使用兩大種類，並以較宏觀角度檢視法律體系，找尋這些行為背後的授權規範，並整理如下：

1. 卷證資料本為進行刑事程序而蒐集，就基於審判目的使用而言，法院使用卷證資料乃進程序之必要行為，依循刑事訴訟法中關於法院調查證據、作成裁判等訴訟行為規定，均得使用之。
2. 然而，在審判目的下，法院需傳遞卷證資料時，依照所傳遞的對象與內容，即生不同問題。例如閱卷權規定僅及於被告與被害人，但其他訴訟參與人則

無明文；又如審判程序終結後，法院考量是否交付法庭錄音錄影，仍屬審判事務，惟現行法院組織法中對此立法態度仍屬曖昧，凡此均應透過立法解決。

3. 在審判以外的目的下使用卷證資料，本文探討另案使用與司法行政使用兩種類型，並聚焦於後者。本文整理學說文獻，指出另案使用已與個資保護之目的拘束原則衝突，然而現行法幾無限制。
4. 本文亦探討個資當事人之告知後同意得作為個資使用行為的正當化基礎，並說明歐盟法上要件及我國法之制度現況。雖然事前告知制度與刑事程序發現真實之目的衝突，可能將妨害偵查、審判程序之進行，是故刑事程序屬於告知後同意制度的例外，司法機關因刑事目的使用卷證中個資，無庸取得資料當事人之同意。歐盟 GDPR、2016/680 指令及我國個資法均有此等設計。
5. 本文欲再進一步指出，在刑事程序目的外，例如將卷證中個資供作學術研究使用等司法行政範疇之使用，已經不屬於刑事審判範疇，則回歸一般情形之處理，而有尋求當事人合法同意作為正當化基礎的空間。
6. 本文於第三章後半聚焦司法行政領域，從兩個切入點說明問題：其一，現行裁判書公開制度下，遮隱資訊之方式與個資保護尚有落差；其二，關於是否開放訴訟外第三人查閱卷證資料，現行法並無規定，而學說與實務見解存有歧異，本文認為不應開放一般第三人查閱，但可有條件使學術研究機構查閱卷證資料。

在第四章中，本文整理歐盟 GDPR、2016/680 指令與德國刑事訴訟法、聯邦資料保護法、法院組織法施行法(EGGVG)等法律，作為我國法參考對象，所得結果如下：

1. GDPR 和 2016/680 指令的關係，在刑事目的外及刑事目的中使用個資時互為特別法而交錯適用，但二者均排除刑事審判，由各會員國內國法自行規劃其審判權行使。
2. 本文將重點放在 GDPR 和 2016/680 指令設置的配套措施，以個人資料毀損

伴隨的義務與資料保護影響評估為主。為維護資料完整性及正確性，當個人資料毀損發生時，資料控制者應負回復原狀之義務，並善盡平時保存、更正、刪除資料的義務。資料保護影響評估則可提供資料控制者事前思考框架，對於所擬進行使用行為、使用之必要性、適當性及與目的間關係、對資料當事人之權利及自由可能造成之風險、預計採行之相應保護措施進行評估。

3. 本文亦觀察德國法制，以刑事訴訟法為主，加上聯邦資料保護法、法院組織法施行法中相關條文，闡述德國法上對於司法機關使用卷證中個資的授權規範、資料規則及救濟管道較全面與詳盡的規劃。
4. 德國刑事訴訟法第 8 編設有卷證資料使用的一般性規定及配套措施，本文介紹由以一般性授權規範與司法機關義務切入，呈現其法律體系，再聚焦說明司法機關將卷證資料傳遞給訴訟外第三人之要件，就私人與學術研究機構兩者寬嚴不同，且均須符合相容性要件，最後說明資料當事人之配套權利，與 2016/680 指令相近，以及德國司法行政體系下之救濟途徑。

本文於第四章中比較歐盟、德國法及我國法，提出司法機關於現行法下適用法律的建議，以及未來修法構想，供作參考：

1. 本文先回顧我國刑事訴訟法，說明其目前欠缺已確定案件之卷證中個資使用授權規範，亦無相關配套措施，如更正、刪除資料、資料當事人之資訊近用權等，而全盤需找尋個資法中的相近規範，再加以解釋適用。
2. 針對此困境，在現行法下，本文建議司法機關在使用卷證中個資前，得在其裁量中加入資料保護影響評估(DPIA)之思考框架，於其決定中概述其使用行為，並說明對於資料當事人權利、自由所造成的風險，以及所採取的保護措施；法院在事後救濟程序中審查該決定時，亦可就資料保護影響評估內容審視個資使用機關的描述是否與實際使用情形相符、是否落實保護措施等，並藉由個案累積，有助建立更明確的審查標準。
3. 就資料當事人之權利而言，本文認為至少在案件確定後，刑事程序發現真實等目的已不會再與個資使用透明性等原則產生衝突，此時司法機關再使用卷

證中個資，需給予資料當事人表達意見之機會。

4. 在立法論上，本文則建議我國刑事訴訟法增訂第十編，就個人資料之使用與保護設置授權規範與配套措施。在刑事訴訟法內設置特別授權規範，得使刑事司法機關使用卷證資料的目的、範圍、方式皆有法可循而更為明確，亦可減少跨法規解釋的模糊空間，若有不足之處，再尋求個資法規定處理，而免於全盤由個資法解釋適用。本文基於事務相近性及訴訟經濟的考量，亦提議將救濟程序交由刑事法院處理。
5. 藉由上述實務建議與立法構想，本文嘗試使刑事訴訟法與個資法得以接軌，令整體個資保護法律體系更加完備。



參考文獻

一、中文文獻

(一)專書

1. Maria Cristina Caldarola、Joachim Schrey 著、趙彥清、黃俊凱譯，大數據與法律實務指南，元照，2020 年。
2. 王玉葉，歐洲聯盟法研究，元照，2015 年。
3. 王泰銓，歐洲聯盟法總論，台灣智庫，2008 年。
4. 財團法人金融聯合徵信中心編，歐盟個人資料保護規則，財團法人金融聯合徵信中心，2017 年 7 月。
5. 財團法人資訊策進會科技法律研究所，個資保護 2.0，書泉，2019 年。
6. 李震山，多元、寬容與人權保障：以憲法未列舉權之保障為中心，2 版，元照，2007 年。
7. 李震山，人性尊嚴與人權保障，元照，2011 年。
8. 林鈺雄，刑事訴訟法 上冊，8 版，2017 年。
9. 許耀明，歐盟法、WTO 法與科技法，元照，2009 年。
10. 連孟琦譯，德國刑事訴訟法：附德國法院組織法選譯，元照，2016 年。
11. 張永明等 10 人，行政執行／行政罰／行政程序／政府資料開放／風險社會與行政訴訟，元照，2017 年。
12. 張陳弘，莊植寧，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，新學林，2019 年。
13. 蕭文生，「一九八三年人口普查案」判決－德國聯邦憲法法院裁判選集(一)，司法院，1991 年 5 月。

(二)期刊論文

1. Arndt Sinn 著、吳瑛珠譯，裁判書公開於德國之實踐(上)，司法周刊，1926 期，2018 年 11 月，2-3 版。
2. Arndt Sinn 著、吳瑛珠譯，裁判書公開於德國之實踐(中)，司法周刊，1927 期，2018 年 11 月，2-3 版。
3. Arndt Sinn 著、吳瑛珠譯，裁判書公開於德國之實踐(下)，司法周刊，1928 期，2018 年 11 月，2-3 版。
4. 王士帆，第三人沒收程序——評釋最高法院 108 年度臺上大字第 3594 號裁定，政大法學評論，163 期，2020 年 12 月，頁 1-48。
5. 何之行、廖貞，AI 個資爭議在英國與歐盟之經驗——以 Google DeepMind 一案為例，月旦法學雜誌，302 期，2020 年 7 月，頁 127-156。
6. 何賴傑，論刑事訴訟法之傳承與變革——從我國與德國晚近刑事訴訟法修法談

- 起，月旦法學雜誌，100期，2011年1月，頁172-183。
7. 李佳玟，關於刑事案件贓證物保管的三點建議(上)，司法周刊，2014期，2020年7月，2-3版。
 8. 李婉萍，歐盟個資小組對「目的拘束原則」之詮釋及該詮釋對界定個資法上「特定目的」之啟發，科技法律透析，25卷，9期，2013年9月，頁18-24。
 9. 李惠宗，裁判書上網公開與個人資訊自決權的衝突，月旦法學雜誌，154期，2008年2月，頁21-34。
 10. 李惠宗，個人資料保護法上的帝王條款－目的拘束原則，法令月刊，64卷，1期，2013年1月，頁37-61。
 11. 李寧修，預防性通信資料存取之憲法界限－以歐盟儲備性資料存取指令（2006/24/EG 之發展為借鏡），興大法學，17期，2015年5月，頁87-140。
 12. 李寧修，個人資料合理利用模式之探析：以健康資料之學術研究為例，國立臺灣大學法學論叢，49卷，1期，2020年3月，頁1-50。
 13. 李建良，資料流向與管控環節－個資保護ABC，月旦法學雜誌，272期，2017年12月，頁25-31。
 14. 李建良，訴訟程序與起訴要件（中），月旦法學教室，189期，2018年7月，頁33-55。
 15. 李震山，來者猶可追，正視個人資料保護問題－司法院大法官釋字第60三號解釋評析，台灣本土法學雜誌，76期，2005年11月，頁222-234。
 16. 林素鳳，卷宗閱覽之請求與救濟，月旦法學教室，89期，2010年2月，頁12-13。
 17. 林常青，台灣法律經濟學實證的探掘資料——介紹與應用，經濟論文，47卷，4期，2019年12月，頁533-546。
 18. 林裕順，臺灣與日本證物保管法制之比較研究，檢察新論，28期，2020年8月，頁109-122。
 19. 林鈺雄，初探醫療秘密與拒絕證言權－從歐洲人權法院之 Z v. Finland 判決（愛滋病患案）談起，月旦法學雜誌，127期，2005年12月，頁5-27。
 20. 林鈺雄，刑事程序中的個資保護——德國刑事訴訟法第8編 (§§474-499 StPO) 逐條釋義，刑事政策與犯罪研究論文集，22期，2020年10月，頁201-233。
 21. 吳志光，行政法上利益衡量方法論，台灣法學雜誌，411期，2021年3月，頁1-18。
 22. 吳瑛珠，裁判公開的個資保護，月旦法學雜誌，294期，2019年11月，頁125-143。
 23. 邱文聰，從資訊自決與資訊隱私的概念區分－評「電腦處理個人資料保護法修正草案」的結構性問題，月旦法學雜誌，168期，2009年5月，頁172-189。
 24. 邱文聰、吳全峰、劉靜怡、劉定基、翁逸泓，科技防疫與個人資料保護(下)，月旦裁判時報，107期，2021年5月，頁88-104。
 25. 邱忠義，我國妨害司法公正罪之再建構，月旦法學雜誌，265期，2017年5

- 月，頁 5-35。
26. 范姜真嫩，個人資料自主權之保障與個人資料之合理利用，法學叢刊，225 期，2012 年 1 月，頁 69-103。
 27. 范姜真嫩，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，41 期，2013 年 12 月，頁 91-123。
 28. 洪家殷，公務機關資料之蒐集與個人資料之保護，東吳法律學報，30 卷，4 期，2019 年 4 月，頁 29-68。
 29. 翁清坤，告知後同意與消費者個人資料之保護，臺北大學法學論叢，87 期，2013 年 9 月，頁 217-322。
 30. 翁清坤，大數據對於個人資料保護之挑戰與因應之道，東吳法律學報，31 卷，3 期，2020 年 1 月，頁 79-159。
 31. 翁逸泓，OTT 發展之隱私與個人資料保護問題初探，世新法學，10 卷，1 期，2016 年 12 月，頁 25-85。
 32. 翁逸泓，科技人權—全民電子通訊監察與個人資料保護，臺灣民主季刊，15 卷，1 期，2018 年 3 月，頁 1-43。
 33. 翁逸泓，開放全民電子健康資料加值應用之個資保護問題——以英國經驗為例，月旦法學雜誌，285 期，2019 年 1 月，頁 144-173。
 34. 翁逸泓，資訊委員的時代角色——以 GDPR 及英國 2018 年資料保護法為中心，月旦法學雜誌，286 期，2019 年 3 月，頁 32-50。
 35. 涂偉俊，建構刑事 DNA 資料庫之合理界限，法學新論，35 期，2012 年 4 月，頁 157-182。
 36. 陳起行，台灣法律資料庫及其個人資料之保護，法令月刊，59 卷，6 期，2008 年 6 月，頁 99-109。
 37. 陳重言，刑事追訴目的之通信（通聯）紀錄調取與使用—兼評 2014 年初通保修法，檢察新論，16 期，頁 40-59。
 38. 張陳弘，個人資料之認定—個人資料保護法適用之啟動閥，法令月刊，67 卷，5 期，2016 年 5 月，頁 67-101。
 39. 張陳弘，已公開個人資料的隱私保護可能—司法陽光網引發的隱私保護爭議，法令月刊，67 卷，9 期，2016 年 9 月，頁 143-164。
 40. 張陳弘，隱私之合理期待標準於我國司法實務的操作—我的期待？你的合理？誰的隱私？，法令月刊，69 卷，2 期，2018 年 2 月，頁 82-112。
 41. 張陳弘，新興科技下的資訊隱私保護：「告知後同意原則」的侷限性與修正方法之提出，國立臺灣大學法學論叢，47 卷，1 期，2018 年 3 月，頁 201-297。
 42. 張陳弘，國家建置全民健康保險資料庫之資訊隱私保護爭議—評最高行政法院 106 年度判字第 54 號判決，中原財經法學，40 期，2018 年 6 月，頁 185-257。
 43. 張陳弘，美國聯邦憲法增修條文第 4 條搜索令狀原則的新發展：以 Jones, Jardines & Grady 案為例，歐美研究，48 卷，2 期，2018 年 6 月，頁 267-332。

44. 張陳弘，GDPR 關於蒐用一般個人資料之合法事由規範——臺灣個人資料保護法遺漏的正當利益權衡條款，月旦法學雜誌，285 期，2019 年 2 月，頁 174-190。
45. 張陳弘，科技智慧防疫與個人資料保護：陌生但關鍵的資料保護影響評估程序，國立臺灣大學法學論叢，第 50 卷，第 2 期，頁 337-400。
46. 葉俊榮，探尋隱私權的空間意涵——大法官對基本權利的脈絡論證，中研院法學期刊，18 期，2016 年 3 月，頁 1-40。
47. 詹鎮榮，公務機關間個人資料之傳遞——以臺灣桃園地方法院行政訴訟 102 年度簡字第 2 號判決出發，法學叢刊，60 卷，1 期，2015 年 1 月，頁 1-27。
48. 楊智傑，歐盟、美國與臺灣個資保護法規中之研究利用，興大法學，26 期，2019 年 11 月，頁 1-91。
49. 廖緯民，1922 實聯制簡訊、通訊監察與個資保護，月旦醫事法報告，60 期，2021 年 10 月，頁 25-37。
50. 樓一琳、何之行，個人資料保護於雲端運算時代之法律爭議初探暨比較法分析：以健保資料為例，國立臺灣大學法學論叢，46 卷，2 期，2017 年 6 月，頁 339-422。
51. 劉定基，個人資料的定義、保護原則與個人資料保護法適用的例外——以監視錄影為例（上），月旦法學教室，115 期，2012 年 5 月，頁 42-54。
52. 劉定基，析論個人資料保護法上「當事人同意」的概念，月旦法學雜誌，218 期，2013 年 7 月，頁 146-167。
53. 劉定基，法庭錄音的公開及其限制——司法獨立、司法課責與隱私保護，月旦法學雜誌，245 期，2015 年 10 月，頁 149-167。
54. 劉定基，大數據與物聯網時代的個人資料自主權，憲政時代，42 卷，3 期，頁 265-308。
55. 劉定基，第三人近用法庭卷證資料權利與個人資料保護的調和，國立臺灣大學法學論叢，49 卷，3 期，2020 年 9 月，頁 881-928。
56. 劉靜怡，說故事的自由？——從歐洲人權法院近年隱私權相關判決談起，台灣法學雜誌，146 期，2010 年 2 月，頁 59-77。
57. 劉靜怡，不算進步的立法：「個人資料保護法」初步評析，月旦法學雜誌，183 期，2010 年 8 月，頁 147-164。
58. 劉靜怡，大法官保護了誰？釋字第 689 號的初步觀察，月旦法學雜誌，197 期，2011 年 10 月，頁 47-61。
59. 劉靜怡，政府資訊公開法第十八條研究，法學叢刊，60 卷，3 期，2015 年 7 月，頁 1-64。
60. 劉靜怡，通訊監察與民主監督：歐美爭議發展趨勢之反思，歐美研究，47 卷，1 期，2017 年 3 月，頁 43-106。
61. 劉靜怡，淺談 GDPR 的國際衝擊及其可能因應之道，月旦法學雜誌，286 期，2019 年 3 月，頁 5-31。

62. 蔡彩貞，定位科技在刑事司法程序之運用與人權保障——以利用 GPS 追蹤為中心，月旦裁判時報，65 期，2017 年 11 月，頁 62-78。
63. 謝碩駿，政府資訊公開請求權在德國的憲法基礎，法學新論，3 期，2008 年 10 月，頁 49-88。
64. 謝碩駿，行政機關蒐集個資之法律依據，月旦法學教室，198 期，2019 年 4 月，頁 15-16。
65. 蘇凱平，2018 年刑事程序法回顧：刑事被告憲法上防禦權的新篇章，國立臺灣大學法學論叢，第 48 卷特刊，2019 年 11 月，頁 1703-1732。
66. 蘇慧婕，歐盟被遺忘權的概念發展—以歐盟法院 Google Spain v. AEPD 判決分析為中心，憲政時代，第 41 卷，第 4 期，2016 年 4 月，頁 473-516。

(三)學位論文

1. 林宛怡，以犯罪偵查為目的之 DNA 資料保存—以歐洲人權公約第八條為中心，國立政治大學法律學系碩士論文，2009 年 12 月。
2. 吳昭億，犯罪被害人之資訊獲知權—以刑事程序為中心，國立政治大學法律學系碩士論文，2018 年 7 月。
3. 許願，刑事被告與辯護人獲悉卷證資訊之探討，國立政治大學法律學系碩士論文，2019 年 2 月。
4. 陳玟瑄，刑事偵查「第三人原則」與「隱私之合理期待」—以偵查機關向網路服務提供者調取非內容性通訊資料為例，國立政治大學法律學系碩士論文，2017 年 7 月。
5. 黃子潔，論人工智慧演算法時代的解釋權—歐盟 GDPR 與我國個人資料保護法之比較研究，國立臺灣大學法政學院法律學研究所碩士論文，2019 年 6 月。

(四)研討會紀錄與研究報告

1. 高愈杰，「司法行政處分」概念與其救濟實務之探討 與談(三)，105 年度第 2 次行政訴訟實務研討會實錄，最高行政法院，2017 年 12 月，頁 437-449。
2. 梁哲璋，「司法行政處分」概念與其救濟實務之探討，105 年度第 2 次行政訴訟實務研討會實錄，最高行政法院，2017 年 12 月，頁 287-419。
3. 翁逸泓、李寧修，歐盟國家個人資料保護法制因應 GDPR 施行之調適—以德國與英國為例，國家發展委員會委託研究報告，2020 年 5 月。
4. 達文西個資暨高科技法律事務所，個資保護專責機關與資料在地化之法制研究，國家發展委員會委託研究報告，2018 年 5 月。

(五)網路資源

1. 李榮耕 (2021 年 6 月 20 日)，警察，我在這裡—簡訊實聯制的法律依據何在？，風傳媒，取自 <https://www.storm.mg/article/3770196> (最後瀏覽日：2022 年 6 月 16 日)。
2. 吳忻穎 (2021 年 6 月 21 日)，法官吹哨「簡訊實聯制」遭不當利用，問題

在於台灣防疫蒼白的法制面，聯合新聞網，取自

<https://opinion.udn.com/opinion/story/12626/5547273> (最後瀏覽日：2022年6月16日)。

3. 法務部，司改國是會議第四分組「第三人取得審判錄影帶、光碟的法制」法務部書面回應，2017年4月，頁1-5，取自
<https://www.moj.gov.tw/Public/Files/201705/7512101813709.pdf> (最後瀏覽日：2022年6月16日)。
4. 張淵森 (2021年6月19日)，我必須成為吹哨者：「簡訊實聯制」資訊遭利用，指揮中心請儘速反應，聯合新聞網，取自
<https://opinion.udn.com/opinion/story/120701/5542571> (最後瀏覽日：2022年6月16日)。
5. 新北市政府警察局刑事警察大隊，警方因偵辦案件向他單位索取個資，是否違反個人資料保護法？，取自
<https://www.cic.police.ntpc.gov.tw/cp-774-1995-28.html>，2013年2月22日(最後瀏覽日：2022年6月16日)
6. 劉世怡 (2021年6月24日)，實聯制簡訊遭誤解用於辦案 法務部：研議修法保障個資，中央社，取自
<https://www.cna.com.tw/news/asoc/202106240357.aspx> (最後瀏覽日：2022年6月16日)。

二、英文文獻

(一)期刊論文

1. Aidan Forde, The Conceptual Relationship Between Privacy and Data Protection, 1 CAMBRIDGE L. REV. 135 (2016)
2. Catherine Jasserand, Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?, 34 Computer Law & Security Review 154 (2018)
3. Celine C. Cocq, EU Data Protection Rules Applying to Law Enforcement Activities: Towards an Harmonised Legal Framework, 7 NEW J. EUR. CRIM. L. 263 (2016)
4. Diana Dimitrova, The Right to Explanation under the Right of Access to Personal Data: Legal Foundations in and beyond the GDPR, 6 EUR. DATA PROT. L. REV. 211 (2020)
5. Dominic Broy, Germany: Starting Implementation of the GDPR - Brief Overview of the Government Bill for a New Federal Data Protection Act, 3 EUR. DATA PROT. L. REV. 93 (2017)
6. Juraj Sajfert & Teresa Quintel, Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities (December 1, 2017). Cole/Boehm GDPR

Commentary, Edward Elgar Publishing, 2019, Forthcoming, Available at SSRN:
<https://ssrn.com/abstract=3285873>

7. Katerina Demetzou, Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'highrisk' in the General Data Protection Regulation, 35 *Computer Law & Security Review* 1 (2019)
8. Maria Tzanou, Data Protection as a Fundamental Right next to Privacy? "Reconstructing" a Not so New Right, 3 *INTERNATIONAL DATA PRIVACY LAW* 88 (2013)
9. Mark Leiser & Bart Custers, The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680, 5 *EUR. DATA PROT. L. REV.* 367 (2019)
10. Norberto Nuno Gomes de Andrade, "Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights," in *Privacy and Identity Management for Life*, ed. Simone Fischer-Hübner et al., vol. 352, *IFIP Advances in Information and Communication Technology* (Berlin, Heidelberg: Springer Berlin Heidelberg, 2011), 90–107, https://doi.org/10.1007/978-3-642-20769-3_8
11. Orla Lynskey, Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the EU Legal Order, 63 *INTERNATIONAL & COMPARATIVE LAW QUARTERLY* 569 (2015)
12. Paul De Hert & Serge Gutwirth, Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power, in *PRIVACY AND THE CRIMINAL LAW* 61 (E. Claes, A. Duff & S. Gutwirth eds., 2006), https://works.bepress.com/serge_gutwirth/5/
13. Paul De Hert & Vagelis Papakonstantinou, The New Police and Criminal Justice Data Protection Directive: A First Analysis, 7 *NEW J. EUR. CRIM. L.* 7 (2016)
14. Thomas Marquenie, The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework, *Computer Law & Security Review*, Volume 33, Issue 3, 2017, Pages 324-340.
15. Tristan Radtke, The Concept of Joint Control under the Data Protection Law Enforcement Directive 2016/680 in Contrast to the GDPR, 11 *J. INTELL. PROP. INFO. TECH. & ELEC. COM. L.* 242 (2020)

(二) 歐盟出版品

1. Art. 29 Working Party, Opinion 4/2007 on the Concept of Personal Data, 01248/07/EN: WP 136, 20 June 2007
2. Art. 29 Working Party, Opinion 03/2013 on Purpose Limitation 2012, 00569/13/EN: WP 203 2 April 2013
3. Art. 29 Working Party, Guidelines on Transparency under Regulation 2016/679: 17/EN, WP 260rev.01, 29 November 2017
4. Art. 29 Working Party, Guidelines on Automated individual decision-making and

Profiling for the purposes of Regulation 2016/679: 18/EN, wp251rev.01, 6 February 2018

5. Art. 29 Working Party, Guidelines on Consent under Regulation 2016/679: 17/EN, WP259rev.01, 10 April 2018
6. Art. 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679: 17/EN, WP248rev.01, 10 October 2018

三、德文文獻

(一) 註釋書

1. *Gola, Peter/Heckmann, Dirk*, Bundesdatenschutzgesetz 13. Aufl., 2019.
2. *Graf, Jürgen Peter (Hg.)*, Beck’scher Online-Kommentar StPO mit RiStBV UND MiStra, 42. Ed., 1.1.2022.
3. *Hannich, Rolf (Hg.)*, Karlsruher Kommentar zur Strafprozessordnung, 8. Aufl., 2019.
4. *Graf, Jürgen Peter (Hg.)*, Beck’scher Online-Kommentar GVG, 14. Ed., 15.2.2022.

(二) 期刊論文

1. *Growe, Nicolai/Gutfleisch, Ulf*, Die Strafakte im Zeitalter ihrer digitalen Reproduzierbarkeit, *NStZ* 2020, 633-639.
2. *Safferling, Christopher/Rückert, Christian*, Europäische Grund- und Menschenrechte im Strafverfahren – ein Paradigmenwechsel?, *NJW* 2021, 287-292.
3. *Warg, Gunther*, Der Begriff der Akte und ihre Vorlage im Strafverfahren, *NJW* 2015, 3195-3200.