《歐美研究》第四十七卷第一期 (民國一〇六年三月)，43-106
© 中央研究院歐美研究所
http://eurамerica.org

通訊監察與民主監督：歐美爭議發展趨勢之反思

劉靜怡
國立臺灣大學國家發展研究所
10617 臺北市大安區羅斯福路四段 1 號
E-mail: cytahr@gmail.com

摘 要

本文從民主社會應如何監督政府通訊監察行為出發，檢視歐洲人權法院的相關判決，並與美國相關爭議比較，以探究歐美通訊監察法制爭議之發展趨勢，對我國有何啟示，藉此探討通訊監察法制應有的民主監督形貌。本文認為：歐洲人權法院在資訊隱私權領域已累積豐富的判決，往往決定締約國通訊監察或監控法制的改革。值得注意的是，歐洲人權法院在適用歐洲人權公約第 8 條規定時，經常把重點放在「依法」的解釋與分析上，而非「民主社會所必需」要件。此一趨勢可能導致締約國僅以內國立法表面回應，民主社會所需的資訊隱私保護架構仍有改進空間。

關鍵詞：通訊監察、資訊隱私、歐洲人權法院、後設資料、巨量資料

投稿日期：104.12.23；接受刊登日期：105.12.23；最後修訂日期：106.1.6
責任校對：蔡旻芳、林碧美、曾嘉琦

壹、前言

在現代社會中，各種監控措施或通訊監察 (surveillance) 手法，例如電話監聽或網路活動監控等，可說已經深入我們的社會生活中，而且，這些監控措施的目的，大多和所謂國家利益或公共利益互相連結在一起，因而，正如知名的監控研究者所說的，也就導致政府習於宣傳的「如果無可隱藏之事，便無所畏懼」(If you have nothing to hide, you have nothing to fear) 此種想法，深植於一般大眾心中 (Lyon, 2009)。

然而，是否真的該「無所畏懼」，或許不該遽下結論。當今不但許多國家採取廣泛的通訊監察或監控措施，而且，此一監控網絡恐怕仍處於方興未艾、不斷創新演進的階段 (James, Lin, & Millett 2007: 88-97)，同時，資訊科技的研發趨勢和使用方向，使得過往至今分析隱私權概念的「公領域」和「私領域」兩分的概念逐漸遭受挑戰：私領域是創意、異議和向傳統挑戰的搖籃，倘若個人知悉自己所處的社會是無時無刻不受到國家監控的社會，那麼可以算是私領域已經實質消滅的社會，個人也就會因此失去自我的特性 (Cohen, 2012: 107-115; 2013)。換言之，國家監控隱含高壓性質，無論其監控活動是如何運作，對於自由所產生的限制，實質上已經無可忽視，甚至已經逐漸掏空「資訊自決權」的實質內涵，[1] 對於民主生活來說，和過去任何時代民主治理模式下的政府通訊監察活動一樣，都暴露出必須嚴肅處理的權力監督問題。

---

[1] 「資訊自決權」是指，每個人基於其自主意志，都有權自行決定，是否將其個人資料交付與提供給他人（包括政府部門在內）利用與處理。參見李震山 (2000: 277-318)。關於資訊自主權的實踐及其近年來相關爭議之討論，參見李惠宗 (2013: 37-61)；范姜真媺 (2016: 61-106)；許炳華 (2015: 125-163)；劉定基 (2013: 146-167)；劉靜怡 (2016: 73-84)。

此一民主監督的迫切性，在 2013 年美國國家安全局 (National Security Agency; NSA) 長年以來的各種監控作為，遭到承包聯邦政府資訊業務廠商的離職員工 Edward Snowden 以大量文件的形式揭露之後 (Hardin, 2014)，更顯重要。當然，即使是類似美國國安局這種採取全面監控措施的機關，不可能一一檢視每一個電話通訊或電子郵件的內容，也不可能追蹤每一個人的活動，但是，監控系統之所以能夠有效控制個人的行為，本不在於國家監控措施是否涉及內容的讀取，而是在於受監控者認為自己的一言一行都受到監視，因此限縮了個人自主發展的人格 (Lyon, 2007)，這就是「圓形監獄」(panopticon) (Bentham & Božovič, 2010) 的概念核心。正因為如此，司法判決必須更正視和傳統偵防手法不盡相同的通訊監察或監控措施對於隱私權保護領域所帶來的衝擊。本文的目的，在於檢視歐洲人權法院針對歐洲各國通訊監察或監控法制所衍生的訴訟，究竟採取怎樣的判決立場，同時比較美國通訊監察法制相關爭議的發展趨勢，並且及於最近數年來備受矚目的大型監控與後設資料爭議，以探究歐美國家通訊監察法制運作中所出現的爭議及其發展方向，對於思考我國通訊監察法制的興革，究竟可以帶來怎樣的啟示，嘗試描繪出現代通訊監察法制下的民主監督形貌。

歐洲的司法者在資訊隱私權此一領域中，可謂已經累積堪稱豐富的判決經驗，無論是在資訊隱私權的重要價值方面，或者是資訊隱私權的實際適用方面，均有值得其他國家的法制借鏡之處。歐洲人權公約第 8 條在歐洲各國通訊監察法制實踐上，對於政府所進行的秘密監控，是最為重要的制約機制 (林鈺雄，2008: 109-152)，而且，由歐洲人權法院相關判決的內容，往往可以看出歐洲法制和目前美國法制實踐現狀差異甚大之處。

歐洲人權法院的判決，往往決定歐洲各國在通訊監察立法或者

監控相關法制的改革。歐洲人權公約第 8 條，是歐洲人權公約各條規定中和政府監控 (government surveillance) 行為之間相關性最高的規定。尤其值得注意的是，歐洲人權法院在適用公約第 8 條的規定時，往往會把重點放在「依法」(in accordance with the law) 的解釋分析上，法院並不是將司法審查重點放在「民主社會所必需」(necessary in a democratic society) 此一要件上 (Murphy, 2013: 66-67)。此一趨勢，對於民主社會就通訊監察或監控行為進行監督，究竟帶來怎樣的影響，不無探究之價值。

換言之，不難想見的是，歐洲人權公約的締約國，為了避免遭受歐洲人權法院違憲判決的結果，在其通訊監察或監控相關法制之型塑過程中，歐洲人權公約第 8 條的規定和歐洲人權法院的判決取向，自然是重要參考對象。而且，歐洲人權法院將審查焦點放在「依法」此一要件上的結果，是否使得歐洲人權公約締約國僅願意透過內國立法予以表面回應而已，因而導致民主社會所需的資訊隱私保護架構仍然闕漏處處。同時，由於通訊監察活動的國際化本質使然，比較歐洲和美國的通訊監察法制發展，勢在難免，因此，在本文行文過程中，亦將適度引用美國法制的發展與爭議概況，以為比較參照之用，併此說明。

貳、隱私保護的資訊面向

隨著數位科技在資訊傳遞、處理、儲存等方面的功能不斷快速提升，關於數位科技使用者的身分、活動、位置和習慣等面向的資訊蒐集和處理，已是常態，而這些「個資常態」可以具體勾勒出十分詳盡的個人面貌，甚至推估出個人和特定群體之間的關係 (Desai, 2014)。

同時，隨著數位科技的發展，各國政府執行情報行動、通訊監察或各種監控措施的方式，也因此產生改變。尤其是 911 事件發生之後，不少國家以反恐為名規避法治基本要求，漠視國家安全政策中也應該注意人權保障問題的需求，國家安全到底該不該是人民享有自由的前提，也成為 911 事件後的辯論焦點之一 (Davis, 2003)。在此一辯論中，通訊監察措施所衍生的人權侵害議題，如何在民主社會應有的監督體制下降到最低程度，不僅是法學對話領域的重點之一，也凸顯出法院在此一領域中所扮演的重要角色。

究其實際，數位時代的「資訊隱私」(informational privacy) 問題，至少具有兩個資訊特色，一是無論是公部門或者私部門，對於個人資訊的蒐集，其數量幾無上限，一是一旦資訊公開揭露，那麼其傳播速度之快將難以想像 (Hoppin, 2012: 1957-1961)。

大致上說來，歐洲人權法院不但對隱私權中的「資訊隱私」此一權利面向做了相當程度的澄清，歐洲人權公約締約國絕大多數也將其納入內國法制之中予以落實，甚至已經將個人隱私應受保護的權利適用範圍，解釋成不僅限於國家義務而已，甚至，各國法院也認為資訊隱私應該對私部門的企業甚或個人同樣可產生規範效力。[2] 簡言之，歐洲基於「資訊隱私」在自我決定自由和個人主體發展方面的重要性，提供比較完整的資訊隱私保護 (Lemmens, 2003: 383-384)，和美國法制現狀頗有差異。有鑒於此，本文以下便以歐洲人權法院的判決為核心，說明「資訊隱私」中有關「通訊監察」此一重要議題的歐洲發展歷史與目前趨勢。

[2] Mosley v. News Grp. Newspapers Ltd., [2008] EWHC 1777 [QB].

參、歐洲人權法院判決下的通訊監察法制

歐洲人權公約第 8 條要求成員國保障個人隱私權，該條第 1 項規定「所有人的隱私、家庭生活、家庭與信件有應受尊重的權利」，第 2 項則規定政府機關不應干預前項權利之行使，除非其干預依法為之，而且，在民主社會中，該干預應該具有維護國家安全、公共安全、經濟福祉、防免社會失序與犯罪、保護健康或道德價值、或保障他人權利行使之必要者。本條規定展現了歐洲人權公約嘗試平衡「個人權利保護」與「國家採取保護民主體制措施之必要性」兩者的努力。同時，值得注意的是，歐洲人權法院的判決發展至今，法院並未清楚地界定該條第 1 項所規定的四種隱私權利，究竟範圍如何，但也正因為此一判決態度使然，所以提供了歐洲人權法院隨著社會與科技的發展趨勢，得以詮釋該等權利內容的空間。[3]

一、歐洲人權公約第 8 條的權利屬性

歐洲人權公約第 8 條第 1 項規定個人私生活的權利應受尊重，此一關於隱私權利的規定，是各國在歐洲人權公約下應履行之國家義務的根據。此處的國家義務，包括消極義務和積極義務在內 (Harris, O'Boyle, & Warwick, 1995: 284-285, 302-304)，在通訊監察的領域中，歐洲人權公約第 8 條所保障的隱私權利在歐洲人權法院的判決中，則是著重於如何劃定秘密監控的程序要求，[4] 以及著重於國家消極義務的面向，也就是要求國家不得干預隱私權利，而非從積極義務的面向，要求如何確保隱私權利行使 (Harris et al., 1995: 284)。然而，無論如何，歐洲人權法院目前判決發展趨勢，對於第

[3] 關於歐洲人權公約第 8 條的內容分析，參見翁逸泓、廖福特 (2014: 152-154)。
[4] 可與 Dutertre (2003) 比較。

8 條個人私生活應受尊重的權利是否以及如何產生強化保護的功能，乃是值得重視的分析對象之一。

雖然歐洲人權公約第 8 條的規定並未特別提及當代通訊方式，但是，電話、傳真、e-mail 這幾種類型，已被歐洲人權法院確認為乃屬於「個人私生活」與「通訊自由」的保障範圍內。[5] 整體而言，歐洲人權法院對於秘密通訊監察或監控措施的分析，例如針對信號情報或以個人為對象的監聽所為的分析，相對而言尚稱豐富，正如同其對於私人生活與家庭生活不採狹義解釋，[6] 可以想見歐洲人權法院對於任何新興通訊方式是否被納入歐洲人權公約第 8 條的「通訊自由」範圍內，應該也會採取比較接近於正面肯定的開放態度。此種態度，也就是學者所稱的「Strasbourg 案例法的動態憲章」(the dynamic charter of the Strasbourg case law) (De Hert, 2005: 74)，在歐洲人權法院落實公約的過程中，算是相當重要的詮釋方法。

二、啟動權利保護程序的相對容易特性：從 *Klass* 案的當事人適格談起

個人資訊的儲存與揭露模式，是保護資訊隱私的基本門檻，其受到何種程度的保障，就判斷隱私權保護周全與否而言，可謂具有指標意義，而歐洲人權法院長期以來的判決立場，均認定單純涉及個人隱私資訊蒐集或處理等行為，即足以啟動歐洲人權公約第 8 條的適用。[7] 例如，在 *Leander v. Sweden* 這個判決中，原告遭到某祕密的警方系統蒐集資訊，而且原告無權近用此一系統，然而，此一

---

[5] Liberty and Others v. the United Kingdom, application no. 58243/00, para. 56; Sottiaux, 2008 (275-276).

[6] Niemietz v. Germany, application no. 13710/88, paras. 29-32.

[7] Leander v. Sweden, application no. 9248/81, paras. 1 & 18

資訊蒐集的結果，卻導致原告喪失一個在海軍基地獲得工作的潛在機會，因此法院認定適用歐洲人權公約第 8 條。[8] 同樣地，在 *S. & Marper v. the United Kingdom* 此一判決中，歐洲人權法院也認為，單純「儲存」DNA 這類涉及個人隱私的資訊，便構成歐洲人權公約第 8 條所規定的干預隱私權行使。[9]

歐洲人權法院在通訊監察領域第一個重要判決，應該是 1978 年的 *Klass and Others v. Germany*。[10] 本案原告基於以下列兩個理由，在歐洲人權法院挑戰當時德國通過的通訊監察法違反歐洲人權公約：第一個主張是系爭規定未要求政府在通訊監察結束之後，通知受通訊監察的對象；第二個理由，則是系爭立法排除了利用內國普通法院進行訴訟的救濟途徑。歐洲人權法院的判決結果，認為德國在本案中並未違反原告受歐洲人權公約第 8 條所保障的隱私權，但是，值得注意的是，在本案中，法院同時也列出檢視內國政府行使通訊監察權力時是否違反歐洲人權公約的審查標準，因此本判決被視為指標判決。

本案原告 Klass 等人由於懷疑自己的通訊遭到政府的通訊監察行為干預，所以提起訴訟挑戰系爭通訊監察的合法性。儘管 Klass 等人無法證明他們確實是受到國家監控的被害人，但是當時的歐洲人權委員會 (European Commission on Human Rights) 仍然認為本案合乎原告適格的要件，可以向法院起訴。雖然，一般而言，只有歐洲人權公約所保護的權利受侵害者，方能起訴，但是，歐洲人權委員會特別指出：所謂秘密監控，其本質就是受監控者通常不會明

---

[8] *Leander*, paras. 4-5.

[9] S. & Marper v. the United Kingdom, application nos. 30562/04 and 30566/04, Eur. Ct. H.R. 1, 20-21 [2008].

[10] Klass and Others v. Germany, application no. 5029/71.

確得知自己已經遭到監控，所以，在此一先天條件下，不可能要求原告證明自己的權利確實受到侵害。[11] 接著，歐洲人權法院也在其判決中同意人權委員會的見解，並且進一步指出，倘若嚴格要求起訴的原告必須證明自己為確實遭受秘密通訊監察的受害人，無疑將會架空歐洲人權公約第 8 條的真正意旨。[12]

在此一判決中，歐洲人權法院在肯定原告合乎適格要件之後，進一步檢視德國系爭立法是否違反公約第 8 條規定時，首先指出，系爭立法本身的存在，確實已經對人民造成了「遭受監控的威脅」。[13] 接著，法院審查德國系爭通訊監察立法是否具有正當性時，指出兩個重點：第一，德國政府所從事的通訊監察行為，具有內國法律依據，因此合於公約第 8 條規定之「依法」要求；第二，歐洲人權法院認為，在系爭法律規定下，德國政府所從事的通訊監察行為乃是為了達成保護國家安全或預防犯罪的目的，此乃具有正當性的合法目的。[14] 在本案中，比較困難的問題在於，如何判斷德國系爭通訊監察措施，是否為民主社會所必需。[15]

針對「民主社會所需」此一問題，歐洲人權法院認為，在某些特殊狀況下，秘密監控確實可能符合民主社會所需的要件，尤其是在當代社會中，由於通訊技術的快速發展，使得國家必須不斷面對越來越防不勝防的犯罪手法或恐怖主義時，尤其如此。因此，歐洲人權法院認為各國立法機關應就此享有一定程度的裁量權。不過，由於秘密監控也相當可能藉保衛民主之名，導致侵蝕民主的結果，

[11] *Klass and Others*, at para. 27.
[12] *Klass and Others*, at para. 34.
[13] *Klass and Others*, at para. 41.
[14] *Klass and Others*, at para. 46.
[15] *Klass and Others*, at para. 46.

所以法院認為仍然必須對各國所享有的裁量權加以限制，也就是透過對國家監控立法的裁量空間予以限制，方能避免權力濫用，達到適當且有效確保通訊或資訊隱私。[16]

歐洲人權法院在本案中判決德國並未違反公約第 8 條的規定，其理由在於系爭立法僅授權政府將秘密監控適用於「有具體事證足以懷疑犯罪嫌疑人正在計畫、進行或已經犯下嚴重犯罪」的案件，而且，歐洲人權法院也認為，由於系爭立法並未授權政府可以進行試探性 (exploratory) 或者全面性 (general) 的通訊監察，這也構成其不違反歐洲人權公約第 8 條的原因。此處值得注意的是，歐洲人權法院在本案中所建立的判斷標準，是其後續案件中一再遵循並適用的標準，只是這個判斷標準的內涵也隨著時間的經過及歐洲人權法院判決的發展，不斷有所修正，甚至，連「依法」此一要件的內涵，也出現漸趨嚴格的傾向。

總之，在原告適格方面，歐洲人權法院長期以來一直維持 *Klass* 案的見解，認為由於通訊監察先天上具有秘密進行的不透明本質，因此，只要是內國法律或措施允許通訊監察，就算原告無法證明自己確實是受監控的對象，仍然有提起訴訟的原告當事人適格。[17] 由於法院並未針對原告當事人適格此一要件予以嚴格限制，因此，歐洲人權法院就涉及秘密通訊監察的案件所做成的判決，通常認為只要有系爭立法存在，即構成歐洲人權公約第 8 條所規定的「干預」，可以進一步從事後續的分析和審查。

三、歐洲人權法院審查架構

歐洲人權法院針對涉及公約第 8 條所保護的隱私權利侵害的案

16 *Klass and Others*, at paras. 48-50.

17 Iordachi and Others v. Moldova, [2009] ECHR 256.

件，歸納起來，其所援用的審查步驟，可以分成幾個部分：(一) 權利干預之有無；(二) 國家干預之「合法性」要件；(三) 民主社會所需：「必要性」要件與「判斷餘地」。然而，究諸實際，近年來也逐漸出現「合法性」與「必要性」兩者之審查並進的趨勢。關於上述審查步驟的詳細內容，分述如下：[18]

(一) 權利干預之有無

在審查涉及通訊監察或監控措施的案件時，首須確定系爭權利範圍與干預之有無。歐洲人權法院首先會分析在系爭事實中，是否有公約第 8 條的權利受到限制，[19] 在確定國家的干預涉及公約第 8 條的權利時，不僅包括政府積極透過通訊監察或監控措施限制或剝奪人民行使權利，[20] 若是消極不作為是發生在具有積極義務的情況下，同樣也會構成權利的干預。

國家有無干預個人權利，由原告負擔舉證責任 (Harris et al., 1995: 335)，而歐洲人權法院是否決定審查系爭案件，則是取決於當事人是否主張其權利遭到歐洲人權公約締約國的侵害 (The Council of Europe's for the Protection of Human Rights and Fundamental Freedoms [the European Convention], Art. 34, 先前的 Art. 25 及 46)。然而，由於絕大部分的通訊監察和監控措施是在秘密狀態下執行，因此，歐洲人權法院指出，只要合乎一定的條件，則系爭立法架構即可構成干預。[21]

發生於瑞典的 *Kopp* 案，便在這方面點出了兩個重點：一是國

---

[18] Case of A. and Others v. the United Kingdom, [2009] ECHR 301.
[19] A. v. France, application no. 14838/89, paras. 34-37.
[20] Segerstedt-Wiberg and Others v. Sweden, application no. 62332/00, para. 73.
[21] Klass and Others v. Germany, application no. 5029/71, paras. 34-37.

家進行干預的時間點，二是程序發展過程的重要性。[22] 在這個涉及電話通訊監察的案件裡，由於透過通訊監察手段所取得的數據並未傳送，而且隨後已經銷毀，因此，做為被告的瑞典政府所提出的爭執重點之一，即是對於個人隱私權產生侵害的國家干預是否存在。[23] 針對此一主張，歐洲人權法院認為，如何使用通訊監察所得之資料，並不影響國家干預的成立。[24] 甚至，即使系爭通訊監察或監控措施並未造成損害，也仍然可能構成侵害，例如沒有法律授權的非法干預，即屬之。[25]

總之，凡是締約國的法律架構授權政府進行通訊監察或監控措施，則在系爭個案中即須分析受通訊監察的對象，是否落在公約第 8 條隱私權利所保障的範圍內，倘若答案是肯定的，那麼，系爭法律架構的存在，便可能涉及公約第 8 條權利的限制問題。至於國家的干預是否存在和何時存在此一問題，則應該從系爭行為的角度出發來進行分析。換言之，由於通訊監察或監控措施此種行為的本質，通常具有秘密特性，所以很難從個人觀點去理解自己是不是已經成為受通訊監察或受監控對象。正因為如此，歐洲人權法院認為，只要締約國的法律架構授權就通訊進行秘密監控，那麼，就是對此一法律架構所有適用對象構成妨礙通訊自由的威脅。換句話說，只要具有可採行秘密監控措施的法律架構，便構成對公約第 8 條權利的干預，無論實際上是否針對特定個人採取任何具體的通訊監察或監控措施，皆在所不問。[26]

---

22 Kopp v. Switzerland, application no. 13/1997/797/1000, para. 72.

23 *Kopp*, at para. 51.

24 *Kopp*, at para. 53.

25 Huvig v. France, application no. 11105/84, para. 35.

26 *Liberty and Others*, para. 56; *Weber and Saravia*, para. 78; *Klass and Others*, para. 41.

總之，歐洲人權法院上述見解認為，可能會限制個人權利的通訊監察或監控系統，由於潛藏了對個人通訊隱私的威脅，所以本身就構成對公約第 8 條權利的干預。[27] 甚至，即使締約國在法院審理程序中證明並未有具體出現的通訊監察或監控措施，但是法院仍然認定原告乃是處於遭受通訊監察或監控的危險當中，因此准許原告起訴並進行實質審理。[28] 除此之外，因為歐洲人權法院後來的判決立場進一步擴張的結果，法院已經確認不管是否針對通訊監察或監控所得資料予以使用，都不會影響公約第 8 條所保護的權利受到干預的認定。[29]

(二) 國家干預之「合法性」要件

歐洲人權公約第 8 條的規定，在歐洲人權法院審理涉及通訊監察和國家監控的案件裡，扮演相當重要的角色，不過，即使系爭案件涉及國家干預的事實，但只要合乎對第 8 條的權利乃是進行「依法」(in accordance with the law) 且出於「民主社會所必需」之正當目的進行干預時，則為歐洲人權公約所容許。

「合法」此一要件，乃是歐洲人權公約第 8 條第 2 項的核心，歐洲人權法院審查「合法性」要件時，除了要求必須循著「法律保留」原則，根據法律規定為之，並具有正當之目的外，進而則是要求必須合乎「民主社會所需」此一「必要性」要件。此一審查結構，與歐洲人權法院大部分案件的分析步驟相同，[30] 只要不符合任一要件，便極可能構成權利侵害。本文以下將先針對歐洲人權法院關於

---

27 *Liberty and Others*, para. 57; *Klass and Others*, para. 41.

28 *Klass and Others*, para. 37.

29 *Klass and Others*, para. 53; Rotaru v. Romania, application no. 28341/95, para. 46.

30 *Klass*, paras. 43-60; Liberty and Others v. the United Kingdom, application no. 58243/00, paras. 58-59.

公約第 8 條第 2 項之「依法」要件，以及相應的比例原則要求，進行分析。

歐洲人權公約第 8 條所規定的「依法」此一要件，其重要特徵之一就是不僅涉及內國法，同時也與法律的品質有關。換言之，通訊監察或監控相關立法不僅必須符合依法而治 (rule of law) 原則，而且必須具有可被理解性 (accessibility) 及可預見性 (foreseeability)。[31]

就內國法律此一面向而言，內國法必須確保受歐洲人權公約第 8 條保護的權利不受公權力機關的任意干預，由於政府在行使通訊監察或國家監控這種本質上在秘密狀態中行使的權力時，附隨的是更為專斷恣意的風險，因此透過內國法的立法保障來降低專斷恣意的風險，就顯得格外重要。

在前述 *Klass* 判決中，法院對於公約第 8 條規定的「依法」要件的詮釋，非常寬鬆，只要系爭通訊監察措施具有內國法當做依據，便可以被認定為符合「依法」的要件。但是，到了 1984 年的 *Malone v. the United Kingdom* 判決，歐洲人權法院轉而認為「依法」要件所要求的，不應該僅限於政府通訊監察措施對於個人通訊隱私的干預與「國內法」相符，具有內國法的授權，系爭內國法還必須具備一定的「法律品質」，方可通過審查。[32] 此處所謂的法律品質，對於受規範者而言，除了系爭立法必須是具有前述的可理解性和可預見性之外，還必須與法治精神相符。[33] 這些要求，在歐洲人權法院後續關於通訊監察的判決中，也成為審查「依法」此一要件時所適用的判斷標準。

---

31 Malone v. the United Kingdom [1984] ECHR 10 at para. 67.
32 *Malone*, at para. 66.
33 *Malone*, at para. 66.

在 *Malone v. the United Kingdom* 這個涉及電話監聽的判決中，歐洲人權法院雖然同意可預見性這個要件，在秘密監控的脈絡下，應該有不同的適用方式，[34] 但是，法院同時也明確指出，政府應該負起確保正確執行法律的義務：不管是在何種背景或條件下，當法律授權公權力機關以訴諸秘密因而具有潛在危險性的手段，針對個人私人生活或通訊應受尊重的權利進行干預時，法律應就此對人民提供充分的資訊，使人民明確知悉在何種情況下會遭到此種依法進行的干預。[35] 換言之，由於通訊監察或監控措施通常未能受到個人或一般大眾的監督，[36] 因此，授權公權力機關從事通訊監察或監控行為的法律，其規定必須明確，且系爭通訊監察或監控措施必須具有正當目的，為個人提供免於受國家任意干預的充分保護。[37]

接著，在 *Huvig* 和 *Kruslin* 這兩個判決裡，歐洲人權法院進一步詮釋「依法」此一要件。法院認為，「依法」所追求的避免法律遭到濫用此一目標，其重點不僅僅是「民主社會之所需」而已，同時也因為電話監聽或者任何其他對通訊內容的監控，對個人私人生活與通訊造成嚴重干預，所以，此等干預必須基於相當明確的法律，方得為之。[38] 截至目前為止，在衡量通訊監察或監控系爭措施所依據的法律是否充分且明確時，*Huvig* 與 *Kruslin* 這兩個判決出現於 1990 年代初期的判決，一直扮演相當重要的指引角色。

在 2006 年 *Weber & Saravia v. Germany* 的判決裡，[39] 歐洲人權

---

[34] *Malone*, at para. 66.
[35] *Malone*, at para. 66.
[36] *Malone*, at para. 68.
[37] *Malone*, at para. 68.
[38] Huvig v. France [1990]12 EHRR 528 at para. 30 & para. 32; Kruslin v. France 12 EHRR 547 at para. 32; Cameron (2000: 103).
[39] [2006] ECHR 1173.

法院便再次基於上述兩個判決，針對通訊監察立法應該規定哪些最低限度的保障，表達立場，法院在 *Weber & Saravia v. Germany* 判決中指出，授權公權力機關從事通訊監察或監控行為的立法，至少必須就以下事項明確規定之：[40]

1. 據以取得通訊監察票之違法行為性質為何；
2. 明確定義哪些類型的對象可以成為受通訊監察之對象；
3. 通訊監察之期間限制；
4. 檢查、使用及儲存通訊監察所得資料時應遵守之程序；
5. 將通訊監察所得資料傳遞給他人時應採取的防護措施；
6. 在哪些情況下可以或者必須消除通訊監察錄音所得資料，或者銷毀通訊監察所得影音資料。

在本案中，原告起訴爭執的系爭立法與 *Klass* 案所涉及者一樣，都是德國的通訊監察法。*Weber & Saravia v. Germany* 的原告在本案中所爭執的，是德國政府針對其通訊進行「策略性監控」(strategic monitoring) 以取得資訊並予以使用，侵犯其受歐洲人權公約第 8 條保護的隱私權。[41] 法院在本案中仍然認為系爭監控具有內國法依據，自己不該代替內國法院解釋內國法律，除非是在極度明顯違反法治要求的情形下，才有例外可言，[42] 而且，法院認為本案並未構成自己應該代替內國法院解釋內國法的例外。

不過，值得注意的是，「可理解性」與「可預見性」這兩個要求，往往互相糾結在一起，不容易切割處理，整體而言，在歐洲人權法院的判決中，前者所獲得的關注，往往低於後者所獲得的關

40 *Weber*, at para. 95.
41 *Weber*, at para. 4.
42 *Weber*, at para. 90.

注。[43] 在 *Liberty v. the United Kingdom* 這個案件中，[44] 原告是一個非營利組織，起訴主張英國國防部操作一套足以同時攔截 10,000 個倫敦、都柏林和歐洲大陸之間的跨境電信頻道，以及可以攔截在英國兩個電信業者之間互相傳輸的相當數量的電話、傳真和電子郵件的設施。[45] 英國政府對於原告指控的事實，採取既不承認也不否認的不置可否態度，在本案訴訟進行中，英國政府承認在當時的情報蒐集計畫下，原告確實有可能落入其通訊資料會遭到攔截的法人類型範圍內，不過，基於涉及國家安全機密此一理由，英國政府拒絕針對上述情報蒐集計畫揭露更多和搜索令有關的資料，也不願意提供據以監督這些情報蒐集計畫進行的相關手冊和指令資料。[46] 同時，英國政府還主張，和上述情報蒐集計畫相關的資料，均經由一委員會進行獨立審查，而根據該委員的報告，其審查過程相當注意人權保障之要求。[47]

在本案中，法院同意可理解性與可預見性這兩個要件的落實，並不一定要求必須透過嚴格意義的國會立法為之，若是以行政命令或者其他訴諸「軟法」的模式，落實可理解性和可預見性這兩個要件，也可接受。[48] 不過，即使如此，法院在本案中依然認定英國政府的作為違反歐洲人權公約第 8 條的要求，主要理由如下：首先，法院指出：雖然系爭法規符合可理解性的要求，但是，到底哪些非屬英國境內的外部通訊，才可以納入通訊監察票的範圍內，並未加

---

[43] *Weber*, at para. 92; Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, [2007] ECHR 533 at para.73.

[44] [2008] ECHR 568.

[45] *Liberty and Others*, at para. 5.

[46] *Liberty and Others*, at para. 48.

[47] *Liberty and Others*, at para. 48.

[48] *Liberty and Others*, at para. 61.

諸任何限制，如此一來，實際上等於是完全放任行政機關恣意裁量。[49] 其次，英國系爭立法授權給上述執行通訊監察機關的權限相當廣泛，上述機關就哪些蒐集所得資料實際上會進行實質檢視，也可行使裁量權，亦即系爭部會可以發出描寫哪些資料會成為檢視對象的許可，在許可文件中使用諸如「國家安全」這類意義空泛的條件及理由，便核准對通訊內容進行檢查。[50] 除非該機關首長認定攔截從英國境內特定地址發出的訊息乃是預防或偵查恐怖主義行動所必需，也應該予以適用，否則，原則上這些許可適用於除了從英國境內特定地址所發出的通訊以外的所有通訊。[51] 此外，系爭立法也授權機關首長在其認定必要時，採取確保不在上述許可範圍內的資料不受檢查的措施，以及確保許可進行檢查的資料只在必要範圍內揭露和複製的措施。[52]

不過，更重要的是，關於上述措施之安排，其細節乃是處於一般大眾無從接近取得的秘密狀態，[53] 雖然上述委員會的委員每年定期向部長提出報告，說明系爭安排乃是合乎歐洲人權公約第 8 條「依法」的要件，不過，即使如此，法院依然指出，雖然年度定期報告有其正面幫助，但對一般大眾而言，並未因此將上述措施之安排以更為清楚明確或更具有接近可能性的方式表現出來，因為提出報告的委員並不具有在公開報告中揭露措施安排細節的權力可言，[54] 所以其無法滿足歐洲人權法院所要求的「特別是關於檢查、使用和儲存攔截資料的程序，應該以開放給公眾檢視和知悉的形式為之」的

49 *Liberty and Others*, at para. 64.
50 *Liberty and Others*, at para. 65.
51 *Liberty and Others*, at para. 65.
52 *Liberty and Others*, at para. 66.
53 *Liberty and Others*, at para. 66.
54 *Liberty and Others*, at para. 67.

標準。[55]

換言之，歐洲人權法院在本案中無法接受英國政府所提出之公開這類資訊會傷害政府情報行動的效能此一主張。而且，相對於前述 *Weber* 案中的德國政府，已經將有關通訊監察時的指引和限制都規定在可以公開接近取得的立法當中，英國政府在本案中的作法，相形之下顯不具有說服力。於是，歐洲人權法院的本案判決結論是：英國內國法未提供避免通訊監察權力濫用的適當保障，因為其內國法賦予政府過度廣泛的裁量權，尤其是在檢查、分享、儲存和銷毀遭攔截資訊的程序方面，也不是一般公眾所能理解和預見者，所以英國系爭措施違反歐洲人權公約第 8 條的規定。[56]

最後，在 *Iordachi and Others v. Moldova* 案中，歐洲人權法院基於以下三個理由，宣告系爭立法違反公約第 8 條的要求：一是針對通訊監察票的聲請欠缺司法控制，二是依據系爭立法的規定內容，可能遭到攔截的通訊範圍過於廣泛，三是允許進行通訊監察或攔截資料的要件未臻精確。[57] 即使後來 *Moldova* 修正了系爭法律，規定通訊監察票的聲請應受司法審查，並且列出可以啟動通訊監察的犯罪類型，法院還是認定 *Moldova* 的法律仍未達成法院要求。[58] 此外，歐洲人權法院也指出系爭法律針對政府如何過濾蒐集所得的情報以找出有用的資訊，如何維護其完整性和機密性，以及如何保存和銷毀這些通訊監察所得資料，也都欠缺充分明確的細節規定。甚至，法院還特別指出，由於幾乎所有該國檢察官提出的通訊監察票聲請，法官均予以核准，所以可見 *Moldova* 這個國家的政府秘密

---

55 *Liberty and Others*, at para. 67.
56 *Liberty and Others*, at para. 69.
57 Iordachi and Others v. Moldova, [2009] ECHR 256, at para. 41.
58 *Iordachi and Others*, paras. 43-44.

監控系統有遭到過度濫用的傾向，而且，從該國法院每年核發的通訊監察票數量來看，可以說是系爭法律內並未提供充分保障，未適當保護人民的通訊隱私。

總結而言，歐洲人權公約第 8 條所要求的不僅限於「依法」，還包括相對廣義的法治原則。例如，在上述 *Weber* 案中，歐洲人權法院認為德國系爭法律已經針對免於恣意干預的權利提供充分保障，[59] 而在 *Ekimdzhiev* 案中，法院則是認為保加利亞系爭法律在核准階段便已經規定了充分的權利維護措施，所以，如果嚴格遵守該規定的話，那麼應該只有相當特定類型的通訊會成為攔截對象。[60] 但由於保加利亞系爭立法未能針對該國情報機關執行系爭法律的後續措施規定獨立審查機制，因此無法有效防止通訊監察權力濫用的現象出現。[61] 法院也認為，縱然本案系爭立法欠缺事後應該通知受通訊監察者的規定，並非不合理，亦即可以基於正當理由不告知受通訊監察者，然而，毫無限制的永久保密卻不合法治原則，是法院不能接受的作法，除非事後已經基於秘密通訊監察所得資料起訴受通訊監察者，或是因為資訊洩露而使當事人知悉，否則相關個人無從知悉自己是否曾經受到通訊監察，因此無從主張自己受到違反歐洲人權公約第 8 條的不法干預，尋求救濟。[62]

關於通訊監察保障措施的內容，歐洲人權法院不但敘述得相當詳盡，其高度描述性的要件要求，也使內國立法機關必須以非常特定的方式進行立法，方能符合其要求。歐洲人權法院對內國立法機

---

59 *Weber*, at para. 101.

60 Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, [2007] ECHR 533 at para. 84.

61 *Ekimdzhiev*, at para. 93.

62 *Ekimdzhiev*, at para. 91.

關提出如此詳盡的指示，其要件嚴密程度以及其偏重程序的特性，正可顯現出其深知通訊監察領域爭議的特質：由於通訊監察或監控行為本質上的秘密特性使然，受通訊監察者不可能知道自己正處於受通訊監察或受監控狀態中，而且這也正是從事通訊監察的公權力機構有意確保的秘密狀態，和其他比較具體可見的個人隱私干預相較之下，顯然難以監督，或者監督效果不彰。再者，因為通訊監察和監控措施，往往涉及國家安全和特定重大犯罪這類敏感情境，所以對個人權利保護所產生的威脅，也就更形惡化。因此，如何在要件層次和程序層面「依法」拘束公權力機關，就成為關鍵，也就不難想見何以歐洲人權法院對於如何適用「依法」此一要件，格外重視。

綜合以上所述，就合法性要件來說，該要件乃是要求必須有授權干預的法律依據，雖然要求法律依據確需存在，但是，不同位階的法律，包括判例法在內，均可當做授權依據，因此整體而言，歐洲人權法院對於合法性要件的要求，實屬寬鬆。[63]

不過，系爭通訊監察或監控措施之法律依據，依然必須通過三個實質標準的審查，亦即公眾得以理解 (accessible)、可預見性以及符合法治要求，三者缺一不可。[64] 倘若以上三個合法性要件的元素均具備，方進一步進行正當目的此一要求的審查。此處所謂的正當目的，基本上是要求國家行為須有國家安全、公共安全、經濟體發展、預防失序或犯罪、保護健康與道德價值，以及保障他人權利等正當目的，以上雖為列舉規定，然而，實際上歐洲人權法院通常不會在案件中質疑締約國所主張之正當目的。

---

63 Sunday Times v. the United Kingdom, application no. 6538/74, paras. 47-49; Barthold v. Germany, application no. 8734/79, para. 46.

64 *Liberty and Others*, paras. 69-70.

(三) 民主社會所需：「必要性」要件與「判斷餘地」

究其實際，歐洲人權公約第 8 條規定的「民主社會所需」此一「必要性」要求，是指為限制基本權利的「手段」與其所追求的「目的」之間的比例關係，亦即強調「合比例性」(proportionality) 的「比例原則」的要求。與前述強調「法律保留」的合法性要件相較之下，此處的必要性審查已非如合法性要件所要求的一般性抽象審查，而是針對特定具體立法或干預，進行評價。然而，即使如此，由於關於比例性的要求，內國法仍享有一定的「判斷餘地」(margin of appreciation)，[65] 所以，嚴格說來，歐洲人權法院對於必要性要求的門檻不算高，各國政府仍享有一定程度的裁量權。在必要性的審查中，最重要的判斷標準在於必須有足以有效地、適當地防制通訊監察權力濫用的機制，而且最終必須允許法院進行徹底的審查。例如在 *Weber* 案中，歐洲人權法院便認為德國政府的通訊監察計畫乃是基於防範國際恐怖主義所必須，而且因為其通訊監察涵蓋範圍，及通訊監察要件等方面都受到相當的限制，因此並不違反歐洲人權公約第 8 條的要求。[66]

根據歐洲人權法院的判決立場，「必要性」要件的內涵，包括系爭干預具有急迫的社會需求 (pressing social need)，[67] 而且該干預必須和其所欲追求的正當目的之間具有比例合致的關係，也就是必須符合「比例原則」。[68] 不過，關於「民主社會所需」此一必要性要件，事實上欠缺具體定義，歐洲人權法院也特別強調必須視個案情形而異其詮釋，甚至表示「民主社會所必需」並不等同「不可

---

65 關於歐洲人權法院如何適用「判斷餘地」原則，參見王玉葉 (2007: 485-511)。

66 *Weber*, paras. 106-110.

67 Dudgeon v. the United Kingdom [1981] ECHR 5 at para. 51.

68 Handyside v. the United Kingdom, application no. 5493/72, paras. 48-49.

缺少」或者「合理」此種意涵。[69]

歐洲人權法院也容許締約國的立法者與行政機關可以擁有判斷通訊隱私的權利限制必要性的裁量空間。此一裁量空間同樣並非固定不變，而是取決於系爭案件與限制目的的性質而定，例如，若是基於國家安全目的，則其裁量空間相當廣泛。不過，法院仍然強調自己對於此一裁量空間仍具有最終決定權，各締約國依然必須受到監督。[70]

以 *Leander v. Sweden* 這個判決為例，雖然該判決結果認定干預為合憲，但歐洲人權法院清楚描繪出歐洲人權公約第 8 條第 2 項應該如何解釋適用：[71] 首先，就干預正當性而言，所謂干預應該依法為之，其內容廣於表面所示，不僅要求必須有干預的授權依據，還要求系爭干預的潛在受規範對象必須知悉並具有預見可能性。[72] 因此，歐洲人權法院擴張第 8 條的文意，要求應該事先讓人民知悉，使其對自己的資訊將遭到蒐集或公開的情況有所預知，以便決定是否採取某些行為，避免其個人資訊遭到揭露，或者促成個人資訊公開的結果。至於必要性此一要件，則是要求在正當干預目的、干預手段及避免權力濫用數者間應具比例關係，不要求國家僅能在無其他選擇可能性時，才可以進行干預。[73]

相對地，在 *S. & Marper v. the United Kingdom* 此一判決中，法院則是認為，在警方資料庫中無限期保留 DNA 和指紋資料的全面

---

69 *Silver and Others*, application no. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, para. 97; Handyside v. the United Kingdom, application no. 5493/72, para. 48.

70 Leander v. Sweden, application no. 9248/81, *Weber and Saravia*, para. 106.

71 *Leander*, paras. 18-21.

72 *Leander*, paras. 19-20.

73 *Leander*, at para. 21.

性政策，即使是該資料庫僅開放給具有特定器材的專業人員方能取得資料，但因為此一全面性政策是絲毫不區分重罪輕罪，無論是無罪開釋者或遭到起訴者均一體適用，因此被認定不符合必要性的要求。[74]

在討論歐洲人權法院通訊監察領域判決立場的學術文獻中，有認為歐洲人權法院審查系爭通訊監察措施是否符合歐洲人權公約第 8 條要求時，是將重點放在是否「依法」此一要件，而非「民主社會所需」此一要件的判斷上者 (Sottiaux, 2008: 276)。而究諸實際，在通訊監察案件中，「依法」此一要件的審查，往往比較容易判斷，不難想見審查重點偏向「依法」此一要件的現象何以出現 (Ruiz, 1997: 181)。不過，歐洲人權法院的法官對於上述審查傾向，並非完全沒有異議。舉例而言，早在 1980 年代 *Malone* 案中，Louis-Edmond Pettiti 法官在該判決的協同意見書當中表達反對立場，Pettiti 法官指出：如果歐洲人權法院不僅是將審查重點限制在審查系爭干預是否依法上而已，那麼該就此做出更為清楚而明確的判斷。Pettiti 法官進一步認為：該案系爭措施的重要性，已經到達應該對被告國家英國所採取的措施和實際作法進行全面性審查的地步，因此，法院本應進行更為完整的論證而且應該做出未滿足必要性此一要件的結論，但是卻未循此途，此乃是 Pettiti 法官認為歐洲人權法院未善盡審查職責之處。[75]

歐洲人權法院對於「依法」此一合法性要件的重視，對於比較具有爭議性的法律領域，的確也發揮了某程度的具體性和一致性功能。不過，即使如此，仍不乏論者認為，歐洲人權法院此種審查傾

---

74 *Marper*, application nos. 30562/04 and 30566/04 ECHR at paras. 207-209.

75 Malone v. the United Kingdom [1984] ECHR 10, Louis-Edmond Pettiti J. concurring opinion.

向，導致只關注課責性 (accountability) 和可預見性這種相對而言比較安全的爭議此一結果，對於目前正在歐洲內外發展出來的監控措施這類新興警察權 (new police powers)，到底是不是歐洲人權公約可接受者，未能明確表態，殊為可惜 (De Hert & Gutwirth, 2005: 63)。

平心而論，歐洲人權法院若能更為重視何為民主社會所需的必要性要件審查，針對民主社會中可接受哪種通訊監察權力的行使，不可接受哪種通訊監察權力的行使，劃出分界線，一方面確保個人私人生活應受尊重的權利獲得確保，他方面也對通訊監察必要性此一議題所涉及的「效率」問題深入分析，尤其是在全面監控 (mass surveillance) 措施逐漸普遍的當下，對於保護個人自主性來說，應該是更具有迫切性的重點發展方向。

更進一步言之，歐洲人權法院身為確保歐洲人權公約在各締約國能夠落實的主要機關，[76] 雖然無法肯定其判決具有全面的對世效力 (Ress, 2005: 374)，但是歐洲人權法院判決的實質效果，已經不是僅僅限於系爭個案而已，該法院也數度在其判決中主動指出，該法院的判決，不僅止於解決當前系爭個案所引發的爭議而已，同時也具有闡明、確保和發展歐洲人權公約規定的功能。[77] 所以，締約國內國機關應該遵從歐洲人權法院的判決，包括其內國立法機關在內，應無疑問。

然而，歐洲人權法院的判決若要實質上有效拘束締約國，就必須確保其判決能影響各締約國的內國實踐。由於歐洲人權法院本身並無執行機關，所以，如何在避免僭越其權限，導致各締約國內國

[76] Article 19, ECHR.

[77] Ireland v. the United Kingdom [1978] ECHR 1 at 239-240; Karner v. Austria [2004] 38 EHRR 24 at para. 26.

政府普遍遵從歐洲人權法院每一判決主要意旨的意願降低，便成為關鍵之一。「判斷餘地」原則，雖然是賦予各國在內國法上享有一定程度的合比例性判斷空間，不過，同時值得注意的是，儘管歐洲人權法院基於善意，透過判斷餘地理論的運用，賦予各締約國的內國政府一定空間的裁量權，此一理論的運用也遭致例如過於相對主義之類的批評。[78] 不過，平心而論，由於歐洲人權法院仍扮演最終審查者的角色，從另一個角度來看，判斷餘地原則所扮演的收放調節功能，其實也具有確保歐洲人權公約締約國落實歐洲人權法院判決的作用 (Gerards, 2012: 200)。

就通訊監察領域而言，適用「判斷餘地」原則的主要意義在於：由於內國政府對國內實際狀況的知悉程度最高，所以原則上比國際法院的法官更適於決定某個具體措施是否為「民主社會所需」。[79] 就通訊監察和國家監控行為而言，由於其往往事涉國家利益等敏感議題，而且也涉及行政機關的專業判斷，所以，即使是法院在通訊監察和大型監控案件中大量運用判斷餘地原則，應該並不是太令人意外之事。然而，如前所述，歐洲人權法院已經指出「民主社會所必需」並不等同「不可缺少」或者「合理」，因此容許國家干預通訊隱私權，在法院的判斷上，仍屬例外情形，依然必須從嚴解釋，再加上歐洲人權法院對於「合法性」要件的審查，並非寬鬆，因此，或許毋庸過度擔心判斷餘地原則掏空歐洲人權法院在通訊監察相關案件上對於比例原則的堅持。

---

78 Z. v. Finland [1998] 25 EHHR 371, Jan de Meyer J. partly dissenting opinion, part 3.

79 Handyside v. the United Kingdom [1976] ECHR. 5 at para. 48.

(四)「合法性」與「必要性」審查的並進

如前所述，除了「依法」要件的審查之外，近年來歐洲人權法院的判決逐漸連同民主社會所需此一「必要性」要件，也當作實質審查對象。[80] 歐洲人權法院此一判決取向的轉變，是否乃意識「依法」此一要件與「必要性」此一要件兩者之間難免常有重疊，難以強行區分兩者，所以採取此一判決取向，或許尚有爭論，無論如何，只有當歐洲人權法院開始對通訊監察法制必須滿足的要件進行整體分析，才能夠真正改善現況。不過，此一判決新趨勢，是否會成為歐洲人權法院未來確定的判決立場，似乎仍待觀察。

在歐洲人權法院此一脈絡下，分析 *S. & Marper v. the United Kingdom*，[81] 此一近年來歐洲人權法院明顯同時考量「依法」要件和「必要性」要件兩者的判決，而且是有可能成為各國立法者重要參考對象的判決，應該有其意義。

歐洲人權法院在本案中做成英國違反歐洲人權公約規定的結論，並且要求英國必須在 2009 年 3 月之前提出銷毀現有資料庫內相關樣本和資料的計畫，或者針對必須保留部分樣本和資料的特別原因，提出解釋。此一判決起因於英國當局採集、儲存所有犯罪嫌疑人的指紋與去氧核糖核酸 (DNA) 的立法授權，[82] 而建立這類刑事 DNA 資料庫的理由，則大都不外乎認為其在犯罪偵查過程中，可以發揮相當程度的輔助效能。在本判決中，有兩位原告，其中一位在 2001 年因騷擾伴侶遭到逮捕，並且被採集指紋和 DNA 樣本，

---

80 Kvasnica v. Slovakia [2009] application no. 72094/01; Kennedy v. the United Kingdom [2011] EHRR 4.

81 [2008] ECHR. 158.

82 詳細授權內容參見系爭英國立法，Section 61, Section 63 & Section 64 of the Police and Criminal Act of 1984 (the PACE)。關於英國刑事 DNA 資料庫之介紹，參見王勁力 (2009: 67-68)。

但是 3 個月後夫妻兩人回復和好狀態，因此撤銷告訴；另一位原告則是在 2001 年時被控搶劫而遭到採集指紋和 DNA 樣本，但最後也獲判無罪。在上述司法程序結束之後，兩人均要求銷毀其指紋和 DNA 樣本，以及從資料庫中刪除相關資料，但均遭挫。兩人在英國國內法院敗訴之後，訴請歐洲人權法院保護其權利，歐洲人權法院 17 位法官一致認為，在歐洲國家中唯一有系統地保留未被定罪者指紋和 DNA 紀錄的英國，侵犯歐洲人權公約第 8 條所保障的「隱私與家庭生活受尊重」(right to respect for private and family life) 的權利。

根據英國系爭法律之規定，上述指紋和 DNA 資料，可以保留到指紋和 DNA 所有人死亡或年滿百歲為止。相對地，許多歐洲國家則是允許暫時儲存刑事案件相關的 DNA 樣本，在案件終結之後，通常會銷毀樣本，例如芬蘭、瑞典、法國、德國等國，便是規定嫌犯獲無罪開釋後，應將 DNA 樣本銷毀、將相關資料刪除。至於美國，最近也出現了可以針對犯罪嫌疑人蒐集 DNA 樣本和建立相關資訊，且可以無限延長保留期限的趨勢，但是許多州仍未達成共識，甚至拒絕採取這種作法。

究其實際，英國此一資料庫內儲存了超過 430 萬人以上的 DNA 相關紀錄 (指紋資料庫包含數量則更大，根據新聞報導，約涵括 730 萬人的指紋資料)，英國這個資料庫，是法國類似資料庫的 50 倍，是歐洲同類型資料庫中規模最龐大的。但是，其中卻有 86 萬人從未有犯罪定罪紀錄，但是該資料庫仍可依法永久儲存這些資料 (Lyall, 2008)。在本案爭訟過程中，英國政府一直以此一刑事犯罪嫌疑人 DNA 資料庫有助於打擊犯罪為由，堅持其立法內容和實務作法不違反歐洲人權公約，但是，歐洲人權法院卻認為：任何人未受定罪之前，都該享有「受無罪推定的權利」(entitled to the pre-

sumption of innocence)，保留未犯罪者的 DNA 樣本和紀錄，等於要求未犯罪者承擔被污名化的風險，會令無犯罪紀錄的當事人被當做和罪犯同等看待而感到終日不安。

換言之，歐洲人權法院在本判決裡，對於所謂「偵查犯罪所需」的公共利益與個人權益兩者做了這樣的權衡：歐洲人權法院認為英國系爭作法，逾越了可接受的尺度，是以「概括全面且不加區別」(blanket and indiscriminate nature) 的掌握個人資料的權力、不成比例地侵害犯罪嫌疑人私人生活領域的權利，不應該被當做是民主社會必要的作為。雖然歐洲法院並未否認指紋、DNA 樣本和 DNA 資料等在犯罪偵查過程中的功用，但是，「偵查犯罪」、「維護治安」是不是還能夠繼續當做採集人民指紋和 DNA 樣本與建立成資料庫，而不容質疑的正當性基礎，或許歐洲人權法院這個判決帶來的訊息，就是重新思考此一正當性基礎的可能空間。

在本判決中，歐洲人權法院認為英國系爭立法和警察實務的作法，已經遠超過上述思考個人資料保護的比例原則所能容忍的範圍，因此，歐洲人權法院才會在本判決中明確指出：如果我們容許在刑事程序裡，以不惜任何代價的方式使用現代科技，以及不謹慎衡量使用現代科學技術所得的利益和因此所犧牲的個人隱私利益，那麼，歐洲人權公約第 8 條的宗旨將蕩然無存。同時，歐洲人權法院也特別在本判決中提醒大家，任何主張運用新興科技來執法的政府，都必須承擔在科技運用和個人隱私權利保護兩者之間，找出適當平衡點的責任。

換言之，在 *Marper* 案中，歐洲人權法院指出，英國政府取得 DNA 資料的作為，具有當時英國內國法授權當做基礎，不過，歐洲人權法院同時也指出，個人 DNA 資料的取得，就和取得個人的電話通訊錄音一樣，至少必須有最低限度的保障。然而，就本案系爭

事實而言，關於 DNA 此種個人資料儲藏和使用，包括取得個人資訊的目的，儲存期間及刪除資訊的法定標準等，其法律基礎均不充分 (Nardell, 2010: 49-50)。在這個判決裡，雖然歐洲人權法院其實大可像過去的判決態度一般，直接將審查重點聚焦在「依法」此一要件上，但是，在 *Marper* 這個判決裡，法院卻選擇把審查焦點放在「必要性」此一要件的審查上，並且明確地指出：在 *Marper* 這個案件的脈絡下，「合法性」要件和「必要性」要件兩者之間具有密切關係，無從分割處理。[83]

歐洲人權法院在本案中針對「必要性」此一要件的審查，乃是從系爭英國立法的立法目的著手分析，法院指出：英國系爭立法針對尚未受確定判決的未定罪嫌疑犯進行範圍廣泛而且絲毫無差別地蒐集指紋、細胞樣本和 DNA 資料等等，未能在追訴犯罪的公共利益與人民隱私保障兩者間取得平衡。換言之，英國內國法未考量尚未受確定判決的犯罪嫌疑人所犯之罪名輕重，而且所蒐集之資料保存期間沒有限制，也沒有考慮少數族群可能因此遭受怎樣的傷害，事後判決確定無罪者難以要求銷毀其先前遭到蒐集的個人資料，而且系爭立法規定中也欠缺獨立審查機制，因此，最後歐洲人權法院判決英國系爭立法未能尊重個人應受尊重的私人生活，而且並非民主社會所必需，不符合「必要性」此一要件。[84]

歐洲人權法院在此一判決中探究 DNA 資料庫建置所產生的實際影響，並且審查英國政府所主張的政策目標是否合於歐洲人權公約第 8 條要求，應該算是比較適當的審查模式，因為如此一來可以讓內國立法者在立法過程中，有更充分的參考資料可稽。雖然，法院的個案判決往往不免附隨零碎且僅針對個案予以回應的先天限

83 *Marper*, at para. 99.
84 *Marper*, at paras. 119, 122-124.

制，但是，歐洲人權法院長期以來的實踐，已經讓自己在歐洲人權公約的權利解釋方面建立起權威地位，儘管歐洲人權法院仍然相當尊重各內國政府的判斷餘地，但是，如果歐洲人權法院可以勇於提供更為全面性的比例原則審查標準，對於各國的行政權、立法權和司法權之權力行使，應該都能提供更有實質意義的參考依據。

整體而言，歐洲人權法院自 *Malone* 案此一判決後所確立程序保障模式，相當程度算是有效地針對各國政府在通訊監察領域是否妥善行使其權力，提供了指引方向，有助於改善通訊監察的秘密特性所帶來的流弊。但是，如本文以上所述，歐洲人權法院在通訊監察領域中採取此一審查模式，對於保護個人資訊隱私或通訊隱私來說，依然是不足的，雖然比例原則的審查並非用來取代程序保障審查模式，但是，若能更為強調比例原則的審查在通訊監察領域的案件中的重要性，那麼，應該會讓歐洲人權法院在通訊監察領域中呈現出更為通盤的思考邏輯，並且對各國通訊監察法的品質，帶來更明顯的正面影響。以 *Marper* 案判決做成以後，英國制定新法以資因應的經驗為例，英國新法的內容及其國會辯論過程所呈現的重點，都顯示出歐洲人權法院將審查重心挪移至比例原則的新審查模式，對於內國立法者所帶來的影響。

四、後設資料與巨量資料趨勢下的通訊監察

(一) 後設資料與大型監控引發的通訊監察爭議

所謂的後設資料 (metadata)，其通俗易解的定義便是「資料的資料」(information about information)。詳言之，在數位通訊的脈絡下，後設資料的類型至少包括：通訊的時間、延續期間、地點，以及通訊雙方的電話號碼或電子郵件，這些後設資料都會在個別使用者使用數位設備或數位服務之際自動產生，在大部分情況下，這些

後設資料也可以直接連結到特定個人。不過，同時值得一提的是，後設資料並不僅只存在於數位通訊的場域裡，舉例來說，自動車牌辨識系統可以記錄交通工具在某一特定時間的位置，文書處理軟體可以記錄某份文件的主要編輯者及編輯時間，以及更多不勝枚舉的例子，都是後設資料。

各國政府系統性蒐集甚至運用後設資料的作為，本就行之久遠，同樣地，大型監控 (mass surveillance) 在通訊監察領域中，並不是個新穎的議題，但是，隨著科技的進步，政府能夠以更有效率的方式進行規模更大的監控，蒐集數量更多的資訊，再者，另一方面，跨國界的情報活動及資訊共享現象，雖然不乏規範層面的爭議 (Donohue, 2014)，但也早是存在已久且不曾間斷的事實，以近年來美國國家安全局解密的檔案為例，其實就已經揭露出許多過去一直有類似行動 (Greenwald, Poitras, & MacAskill, 2013)。事實上，美國與英國兩國之間的情報合作，至少可以回溯到 1940 年代，從當時起，兩國之間就開始針對國際性信號情報 (signals intelligence; SIGINT) 和通訊情報 (communications intelligence; COMINT) 兩者協商並建構起一連串的情報共享協議，最後則正式發展成一個正式的 United Kingdom-United States of America (UKUSA) 協定，同時也將加拿大、澳洲和紐西蘭三國納入，建立起俗稱的「五眼情報聯盟」(Five Eyes，或稱 Echelon)，[85] 在 UKUSA 協定下，美英兩國互相同意並保證雙方的情報機關可以共享許多種通訊相關的資料，除此之外，美國也陸續和許多其他國家達成法律互助協定 (mutual legal assistance treaty; MLAT)，以便共享資訊和相互協助調查、追訴

[85] 該協議稱為 UKUSA Agreement，詳見 http://www.nsa.gov/public_info/_files/ukusa/new_ukusa_agree_10may55.pdf；另參見 Cox (2012)。

犯罪和恐怖主義活動，[86] 在此一架構下所建立的，其實就是跨國性的大型監控網絡。進一步追究之下，其實更不難發現，從 911 事件發生到 Snowden 解密事件出現之間的十多年之間 (Greenwald, 2014)，本已存在的國際通訊和情報網絡所追求的，其實已經從「需要知道」(need to know) 發展到「需要分享」(need to share)，究其實際，各國政府機關現在也的確開始大量地分析各種「後設資料」和其他線上活動資料 (Swire, 2006: 951)。[87]

自從 Edward Snowden 在 2013 年揭露 NSA 機密文件，並且經媒體大幅報導美國政府長年執行範圍廣及國外的監控計畫之後，國家蒐集後設資料此一作法，便在國際間引發不少爭論。究其實際，過去多年來，美國各種民權組織針對政府監控計畫提出訴訟挑戰者，所在多有，但是，從過去判決所展現出來的發展趨勢，卻已經清楚地告訴我們，當政府以國家安全或國家機密當做抗辯理由時，美國的司法者大多會傾向尊重行政機關的自制態度，採取不予干預的判決立場，此一趨勢和歐洲人權法院的判決取向，可以說是完全不同的態度。依照美國聯邦最高法院的判決見解，NSA 蒐集後設資料的行為，由於不涉及通訊內容，很可能根本不至於違反合理隱私期待，因此不至於構成違憲結果。例如，在 *U.S. v. Miller* 此一判決中，聯邦最高法院即認為人民不得對於已經交給第三方的資料主張合理隱私期待，[88] 同樣地，在 *Smith v. Maryland* 這個判決裡，聯邦最高法院也認為人民對自己所撥打出去的電話號碼，沒有合理隱私

---

[86] 如 Treaty between the Government of Canada and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters, E101638-CTS 1990 No.19, March 18, 1985，詳見 http://www.treaty-accord.gc.ca/text-texte.aspx?id=101638

[87] 關於跨國情報活動所涉及之監控和隱私爭議發展趨勢，可參見 Donohue (2016)。

[88] U.S. v. Miller, 425 U. S. 435 [1976].

期待可言。[89] 在這樣的司法解釋脈絡下，個人的隱私權利是否受保障的關鍵其實在於「政府的資訊蒐集行為是否構成搜索」此一問題(Kerr, 2012)，雖然「內容」及「非內容」這種二元對立的區分模式，本身並沒有太大問題，但是，如果直接將這個嚴格區分兩者的原則套用到目前快速發展的數位科技情境下，對於個人通訊隱私權利的保障，顯然會出現捉襟見肘的不足現象。而且，率爾認定政府監控電話通訊後設資料並未違反憲法保障隱私權之要求，事實上可能忽略了美國聯邦最高法院的 Samuel Alito 大法官和 Sonia Sotomayor 大法官兩位在 *U.S. v. Jones* 這個判決中針對隱私權利的保護所提出的最新見解：這兩位大法官的協同意見書，都特別指出人民對於「空間位置後設資料」(location metadata) 具有合理隱私期待，[90] 從兩位大法官的立場來看，「後設資料」在通訊隱私中之地位，已經看見了曙光，不再處於不受肯定的境地。

以 Jones 這個判決的兩份重要協同意見書對於後設資料的相對友善態度，來比較 Edward Snowden 在 2013 年所揭露的 PRISM (稜鏡計畫)，更足以彰顯後設資料法律地位的重要性。稜鏡計畫之揭露之所以重要，是因為如今全世界有幾十億人利用網路當做溝通工具，留下無數雖非屬通訊內容但仍具有一定程度隱私價值的後設資料，而美國國安局則透過此一計畫，從網路公司取得其所想要的一切後設資料。美國國安局之所以可以進行如此大規模的通訊隱私干預作為，是因為 911 恐怖攻擊發生之後的國會立法授權以及一再延長擴張立法授權所致，而美國政府有些監控計畫雖然表面上看來是針對恐怖行動的嫌犯而設，但是實際上卻很可能跟國家安全絲毫無

89 Smith v. Maryland, 442 U. S. 735 [1979].

90 U.S. v. Jones, 132 S. Ct. 945 [2012], Sotomayor J. concurring opinion; Alito J. concurring opinion.

關，難怪有論者認定美國政府其實是透過一個由多個計畫所組成的大型監控體系，達成消滅全球電子隱私的目標 (Greenwald, 2014: 73-75, 93-95)。

Snowden 當時所揭露的美國政府各種監控計畫的內容，非常明確地向世人展示了以國家為後盾的大型監控系統是如何建置和如何運作，以及個人通訊自由遭到干預的程度，已經惡化到怎樣嚴重的程度。由於監控本身向來被認為對民主憲政社會的治理是相當大的威脅來源，因此，Snowden 事件才會引發舉世對於美國政府監控作為的嚴重憤慨。更重要的是，只要是關切通訊監察及監控措施改革方向，和網路自由所代表的價值，我們必然要面對的問題是：做為一個民主憲政社會的公民，究竟應該如何看待幾乎毫無限制的全面性監控 (Greenwald, 2014: 169)？

究諸實際，大量蒐集後設資料，並且埋下爭議引信，對於大西洋對岸的歐洲來說，也不陌生 (Newell, 2014)，因此，從後設資料的蒐集處理進而建置大規模監控架構的角度，來看歐洲法制的發展，同樣有值得關切的類似趨勢及爭議出現 (Reidenberg, 2014)。2006 年歐盟通過了 2006/24/EC 指令，亦即「資料保存指令」(Data Retention Directive; DRD)，[91] 揚棄過去「容許」成員國之內國法要求儲存電信通聯資料模式，轉而強制成員國必須立法規定電信業者儲存電信通聯資料的立場，以儲存期間至少 6 個月，至多不超過 24 個月為期，[92] 供公權力機關調取利用，各成員國相關執法機關並得基於重大刑事犯罪之偵查、起訴等目的而調取上述通聯資料，各成員國應於其內國法中針對調取目的與範圍等事項予以明確規定。[93]

---

91 2006 O.J. [L 105] 54 [EC].

92 Directive 2006/24/EC, Art. 6 & 12.

93 Directive 2006/24/EC, Art. 1 & 4.

至於電信業者應該儲存的資料，則包括所有得追索並辨識通訊之發話端與接收端的資料、通訊之日期、時間、長短、通訊類型、通訊設施、得以特定出行動通訊設備之位置的資料等等，幾乎涵蓋所有通訊方式的後設資料。[94] 除了合法性要件之外，各成員國且必須基於必要性與比例原則的前提訂定國內法，各國國內法並應遵守歐盟法以及歐洲人權公約等國際公約的相關規定。[95]

此一歐盟指令自草擬時期開始，便充滿侵害通訊隱私的爭議。不難想見的是，透過上述後設資料所建立的生活體制，其實跟所謂的大型「拖網國家」(dragnet nation) 無異 (Angwin, 2014)，個人資料無時無刻不處於被國家支配的狀態下。然而，由於各成員國負有依據指令內容進行內國立法的義務，在此一架構下，歐盟國家事實上已經形成了一個幾乎可謂全面監控的網路，未來各歐盟成員國國內將引發怎樣的憲法訴訟，加上目前歐盟國家的討論方興未艾的「被遺忘的權利」(the right to be forgotten) 崛起 (Tsesis, 2014)，更深化了這個全面監控網路所涉問題的複雜程度。那麼，歐洲人權法院將如何依據歐洲人權公約及其過往在通訊監察領域中所累積來的判決立場，針對可能在歐洲人權法院起訴的案件，針對後設資料和大型監控的爭議做成決定，或許是目前歐洲人權法院最值得關切的指標之一。

當代通訊科技的演進結果，已經發展到可以透過精確的通訊流量分析方法，以及可以利用各種軟體檢視通訊模式的地步。透過流量和軟體分析這類手段，不但可以據以建立起個人的通訊行為圖像，更可以進一步建立個人與特定群體之間的連結關係。這類資料管理的現象，對於 *Malone* 案判決產生之後的歐洲人權法院所帶來

94 Directive 2006/24/EC, Art. 1[2], 3[2] & 5.
95 Directive 2006/24/EC, Art. 15.

的衝擊，便是涉及歐洲人權法院已經明示歐洲人權公約的解釋適用必須順應當代科技發展情況為之，以確保公約第 8 條所保障的權利能夠務實且有效地受到應有的保護。[96] 那麼，歐洲人權法院究竟應該如何順應「後設資料的通訊世界」此一科技演變所帶來的必然挑戰，我們自然也沒有等閒視之的道理。

換言之，通訊過程中所累積的後設資料，不僅可以當做通訊流量分析的基礎，在科技層面上，針對這類資料進行管理的效能不斷提高，對於通訊自由的影響其實極為深遠。進一步言之，由於後設資料所提供的是關於通訊內容的脈絡，片段的資訊內容，若是沒有使用者、位置、通訊方式等後設資料的輔助，其實不容易達成通訊監察和監控措施所追求的真正效能，因此，後設資料等於是具有強化公約第 8 條所要規制之權利干預效果的作用。

再者，*Malone* 案中所涉及的自特定電話號碼取得其所撥出的號碼和通話時間等資料的監控計算機制，將後設資料和通訊內容兩者予以區分，然而時至今日，在許多情況下，尤其是在網路通訊情況下，要清楚區分後設資料及通訊內容兩者並不容易。換言之，後設資料與通訊內容的概念，不得不與時俱進，兩者分開保護的法理或許亟待修正。

歐洲人權公約起草於六十年前，當時不僅通訊傳播科技和今日大不相同，目前各國政府所採行的通訊監察和監控設備及其效能，和六十年前的情報活動或通訊監察作為也難以比擬。整體而言，從歐洲人權法院主張歐洲人權公約的解釋適用應該務實且有效地保護隱私權利的基本立場來看，可以說法院其實清楚意識到科技發展對隱私權所帶來的影響，乃是處於不斷變化的狀態，而其動態性解

---

96 Christine Goodwin v. the United Kingdom, application no. 28957/95, para. 74; Rees v. the United Kingdom, application no. 9532/81, para. 47.

釋的判決立場，對於個人的通訊隱私和資訊隱私保障來說，無疑也是強化歐洲人權架構的重要來源。在此一理解下，歐洲人權法院若能不再堅持區別「後設資料」和「通訊內容」兩者對於通訊隱私的影響此一立場，應該更能展現出歐洲人權架構對於科技變化的認知，為個人通訊隱私免於國家干預的基本要求立下另一個時代里程碑，讓科技所帶來的通訊隱私不保危機成為轉機。

(二) 巨量資料趨勢下的歐洲法院新判決啟示

「巨量資料」(big data) 近年來蔚為風潮之後，成為許多國家的政府與民間企業頗為重視的科技發展領域，期待其在促進經濟成長，提升服務品質、醫療研究突破、國家安全應用與維護等方面，得以成為關鍵助力。以美國為例，2013 年 3 月白宮提出「巨量資料研究與發展倡議」(Big Data Research and Development Initiative)，宣布集合數個部會、機構 (國家科學基金會、國家衛生研究院、國防部、能源部、地質調查局) 之力，投入兩億美金推動巨量資料的基礎研究與教育，以及在醫療、國防、氣候變遷、地震研究等領域的應用 (Office of Science and Technology, Executive Office of the President, 2012)，然而，「巨量資料」的應用，在資訊隱私權上可能帶來的衝擊，卻也不可忽視。2014 年 1 月歐巴馬總統則進一步指示其顧問 John Podesta 領導一個高層、跨部會 (商務部、能源部、總統科學顧問、總統經濟顧問等) 小組，進行一項為期九十天的研究，探討巨量資料科技對經濟、社會及政府活動可能造成的影響 (Executive Office of the President, 2014)；同時，總統科學技術顧問委員會也組成工作小組，針對巨量資料所帶來的隱私衝擊進行研究 (President's Council of Advisors on Science and Technology, Executive Office of the President [PCAST], 2014)。

上述兩者的研究結論，均認為巨量資料分析技術，以及進一步配合開放政府資料和物聯網科技，雖然將帶來各領域前所未見的發展前景，但也無可避免地會對憲法所欲保護的既有價值，包括隱私價值與平等價值，造成重大衝擊，甚至，對於長期以來已經逐漸穩定發展成型的個人資料保護法律架構 (包括：個人資料定義、告知同意模式)，帶來莫大挑戰。因此，如何在隱私等價值之保護，以及個人資料保護法制方面謹慎處理 (PCAST, 2014: 13-14)，[97] 甚至必須從根本的科技及法律規定層面進行檢討以為回應，才是民主體制發揮監督作用以保護個人權利的正途。

相對於美國上述發展趨勢，歐洲的法院近幾年對於通訊監察和個資保護領域作出的判決，也頗具參考價值，例如，歐盟法院 (European Union Court of Justice; ECJ) 在 2014 年 4 月 8 日做出了一則關於數位時代人權保障的指標性裁判——*Digital Rights Ireland* 案。[98] 本案涉及前述「資料保存指令」(DRD) 的解釋適用問題。系爭指令要求所有電信服務提供者保留全部歐盟公民電子郵件、簡訊、電話之數據資料兩年，且在保存期間應開放予國家安全單位以供調查之用，ECJ 在本案中判決認定系爭指令違反歐盟基本權利憲章 (European Union Charter of Fundamental Rights) 的隱私與資料保障權。

ECJ 在本案中明確提出的質疑是：由電信服務提供業者保存個人資料，其實並不會降低濫用資料的風險。ECJ 認為：如果國家對個人資料的直接掌握會讓人聯想到 George Orwell《1984》這本書中所描寫的景象 (Orwell, 1949)，那麼，在 ECJ 眼中，私人部門保

[97] 關於巨量資料發展趨勢所帶來的社會衝擊與法律爭議，可參見 Pasquale (2015)。

[98] Joined Cases C-293/12 & C-594/12, Digital Rights Ir. Ltd. v. Minister for Commc'n, 2014 ECR I-238.

存個人資料，一樣會對私人生活造成干擾，而這個干擾，並非民主社會的必然成本，也不是保護國家安全所需的手段。在此一觀點下，ECJ 這個判決其實開啟了一個算是新穎的問題：在民主憲政體制下，是否真的允許對個人資料進行系統性的蒐集？

如前所述，在歐洲，隱私權受到各國法律與憲法、歐洲人權公約 (European Convention on Human Rights; ECHR)、歐盟條約與立法之保障。在國家的層次上，大部分歐盟成員國的憲法都有明文保障隱私權，甚至許多國家的憲法法院均長期將國內法朝保障隱私權的方向解釋。同時，所有歐盟成員國均受到歐洲人權公約拘束，而歐洲人權公約第 8 條保障所有人「私人及家庭生活、居所與通訊受到尊重的權利」，歐洲人權法院在其判決中也一再擴張歐洲人權公約第 8 條的範圍，承認個人資料之保障也在歐洲人權公約第 8 條的範圍內。然而，值得注意的是，在隱私權與國家安全衝突時，歐洲人權法院往往會擴張國家的裁量權限。

另一方面，歐盟立法對於隱私權的保障，似乎更為顯著，尤其是 2000 年制定、2009 年生效的歐洲聯盟基本權利憲章，在其第 7 條中保障私人及家庭生活，規定「人人有權享有使自己的私人和家庭生活、住所和通信獲得尊重的權利」。[99] 而第 8 條則是保障個人資料，規定「1. 人人均有權享有個人資訊之保護。2. 此等資訊應僅得於特定明確目的，且於資訊所有人同意或其他法律規定之正當依據下，公平地被處理。人人均有權瞭解其個人資訊，並有權要求銷毀其個人資訊。3. 應由獨立之主管機關監督這些原則之確實遵

99 Charter of Fundamental Rights of the European Union [2000/C 364/01], Art. 7: Everyone has the right to respect for his or her private and family life, home and communications.

守」。[100] 其次，與里斯本條約一同制定，在 2009 年生效的歐盟運作條約 (Treaty on the Functioning of the EU; TFEU) 第 16 條，則是強調每個人均有其個人資料受到保護之權利，並且賦予歐洲議會等歐盟立法權機關權限，令其就歐盟組織、機關及成員國對個人資料之處理，以及個人資料之流通建立規則。[101]

歐盟在 1995 年開始就個人資料的近用進行規範，並發布了 1995 年第 46 號指令 (即一般所稱的「資料保護指令」[Data Protection Directive; DPD])，[102] 該指令規定成員國在處理個人資料時，有義務保障國民的基本權利，尤其是隱私權。而個人資料的處理，則必須建立在「質的原則」(qualitative principle) 上，包括個人資料的取得就其所欲追求的目的必須符合比例，且原則上必須取得當事人同意。[103] 同時，此一指令也禁止成員國處理種族、宗教、政治傾向等敏感資料。另外，此一指令也規定當事人必須知悉其個人資料的蒐集，而且當事人擁有近用、要求修改甚至封鎖資料的權利。2001 年歐盟成立歐洲資料保護監察官 (European Data Protec-

---

100 Charter of Fundamental Rights of the European Union [2000/C 364/01], Art. 8:
1) Everyone has the right to the protection of personal data concerning him or her.
2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3) Compliance with these rules shall be subject to control by an independent authority.

101 Consolidated Version of the Treaty on the Functioning of the European Union, May 9, 2008, 2008 O.J. [C 115] 47, Art. 16.

102 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. [L 281] 31.

103 DPD, Art. 6[1].

tion Supervisor)，該監察組織與其他歐盟機關的運作，都應該遵守上開原則。[104]

究其實際，歐盟其他部門的立法，更進一步將隱私保護與個人資料保護延伸到新興敏感領域或者高科技領域。2002 年歐盟第 58 號指令將 DPD 所揭櫫的原則納入電子通訊的規範中，要求各成員國在處理電子通訊時所涉及的個人資料時，必須注意個人基本權利的保障。歐盟理事會 (EU Council) 也曾在 2008 年就警察或司法合作刑事案件時的個人權利保護作出個人資料保護的相關決定，[105] 同時，就其他警察執法的情形，也有制定了許多個人權利保護準則。[106]

不過，值得注意的是，歐盟的個人資料保護框架，在遭遇國家安全問題時，也例外允許成員國限制 DPD 內所揭櫫的權利。儘管歐盟有權對於成員國執法與反恐作為進行統一的立法規定，但是，基於國家主權的原則，國家安全仍然屬於個別成員國的主權範圍，因此，DPD 也將國家安全、國防、公共安全、刑案或一般性道德違反之預防、調查、偵查及追訴、成員國或歐盟的重大財經利益等等，當作例外領域來處理。[107]

在 911 事件發生之後，部分歐盟成員國希望增加資料保護規定的例外，其中包括要求網路與電信服務提供者保存電子通訊的資料，並允許執法單位於必要時取用。部分成員國甚至將這些例外納入內國規定，如此一來，自然影響了歐盟法規對於個人資料的保護

104 Commission Regulation 45/2001/EC, The Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data, 2001 O.J. [L 8] 1.

105 Council Decision 2008/615/JHA, 2008 O.J. [L 210] 1 [EC].

106 Council Decision 2009/371/JHA, 2009 O.J. [L 121] 37 [EC].

107 DPD, Art. 13.

密度 (Bignami, 2007)。

為了調和歐盟國家這些不同的內國法規，歐盟於是在 2006 年施行了前揭判決認定違反隱私與資料保障權的 DRD，針對部分成員國以「刑案之預防、調查、偵查及起訴」為例外要求電信服務提供者保存數據資料，而這些內國規定彼此並不相同的現象，予以規範(李寧修，2015: 87-140)，[108] 如此一來，這些內國規定就會阻礙歐盟內部市場的資訊流通，蓋各個服務業者在處理不同的個人資料時也必須面對不同的資料保存規定。

為了緩解這個狀況，DRD 要求所有成員國以內國管制手段保存電子通訊所生的數據資料。其中第 5 條要求成員國制定法律，強制電信服務提供者保存電子通訊的來源、位址、時間、長度以及種類等資料(但不包括通訊內容在內)。[109] 第 6 條則規定系爭資料保存期間最短不得低於 6 個月，最長不得高於 2 年。[110] 又依據第 4 條之規定，成員國必須以內國法規定使用這些資料的條件，而且必須符合必要性與比例性，且不得違反歐盟法或歐洲人權公約。[111] 但是，DRD 仍然給予成員國很大的裁量權限，只要其使用資料的條件規定合於該指令第 1 條的「刑事重罪的調查、偵查與追訴」即可。[112]

DRD 對個人資料應受保護的權利，造成極大衝擊，尤其是對那些已經在內國憲法提高隱私保護標準的國家，例如羅馬尼亞、捷克、德國等等。其中尤以德國所引發的爭議，特別引人注意：德國聯邦憲法法院長期認同資訊自決權是受到德國基本法保障的基本

108 DRD, Art. 3.
109 DRD, Art. 5.
110 DRD, Art. 6.
111 DRD, Art. 4.
112 DRD, Art. 1.

權利，並且判決德國國會依循 DRD 的立法違憲，蓋系爭立法會造成「受監視的感受」，且未對保存資料的使用設立足夠的限制 (Zoller, 2016: 223-235)。[113] 但是，由於德國聯邦憲法法院無法直接挑戰 DRD，所以僅要求國會提供更多的保護措施以確保人民的隱私保障。

愛爾蘭也曾經直接在 ECJ 的法庭上挑戰 DRD，但是，當時愛爾蘭的主張是聚焦在指令制定程序的技術性問題，並未處理 DRD 與個人資料保護間的相容性。[114] 事實上，愛爾蘭之所以要挑戰 DRD，是因為愛爾蘭的個人資料保護程度是當時最低的，若遵循 DRD 的規定，將會使愛爾蘭被迫提高其對電子通訊的保障。最後 ECJ 駁回愛爾蘭的主張，但同樣沒有處理個人隱私權保障的問題。[115]

在歐盟的權利保障體系下，個人有權直接挑戰歐盟立法，但由於歐盟立法大多透過成員國內國法律具體化，因此個人通常必須先經過內國法院程序，方能進而挑戰歐盟立法。而且，若在內國法院程序中，關於歐盟立法的效力有爭執，則內國終審法院必須先將案件提交給 ECJ 徵詢意見。2012 年愛爾蘭最高法院與奧地利憲法法院因為國內有人民爭執歐盟 DRD 違反隱私保障與資料保護的基本權利，因此將系爭案件提交 ECJ，請求 ECJ 裁判 DRD 在歐盟基本權利憲章第 7、8、11 條的規定下，是否有效。[116]

由於兩案的類似性，ECJ 遂將之結合為一。2013 年 12 月佐審員 [117] Cruz Villalón 提出意見，首先從歐盟基本權利憲章第 52 條著

113 BVerfGE 125; BVerfGE 261.

114 Case C-301/06 Ir. v. Parliament and Council of the Eur. Union, 2009 E.C.R. I-95.

115 Case C-301/06 Ir. v. Parliament, §93.

116 Joined Cases C-293/12 & C-594/12, Digital Rights Ir. Ltd. v. Minister for Commc'n, 2014 E.C.R. I-238, §23.

117 Advocate General (AG) 在 ECJ 法庭中扮演提供獨立法律意見供法官參考的角色。

手，強調該條文所揭櫫之基本權利限制要件的重要性。接著區分隱私權與個人資料保護權，認為後者是前者廣義權利的一部分。最後佐審員建議 ECJ 裁判 DRD 整體違反歐盟基本權利憲章第 52 條，或者推翻 DRD 第 6 條關於資料保存最長可達 2 年的規定，理由則是該條文已違反歐盟基本權利憲章第 7 條。此後 ECJ 決定以大法庭進行聽審，並在 2014 年 4 月 8 日宣判。[118]

ECJ 的 *Digital Rights Ireland* 案此一判決，首先分析歐盟基本權利憲章第 7、8、11 條與 DRD 之間的關係，指出 DRD 要求蒐集並保存電子通訊所生的數據資料，而這些資料彼此間結合在一起後，可能精確地描繪出個人的私人生活狀況。因此，儘管 DRD 並未允許保存通訊內容資料，但 ECJ 認為並不難想像該指令仍然會對歐盟基本權利憲章第 11 條的表意自由造成影響，更不用說系爭資料的蒐集、保存會直接牽涉到憲章第 7、8 條的隱私權與個人資料保護。[119]

接著，ECJ 開始檢視 DRD 中有哪些規定，可能違反歐盟基本權利憲章的要求，尤其是第 7 條和第 8 條的內容，是 ECJ 的檢視重點。ECJ 在本判決中所採用的取徑，與歐洲人權公約的取徑相似，是採取分成兩個層次進行探討的處理模式：首先探討 DRD 是否構成對於歐盟基本權利憲章第 7 條、第 8 條的干預，接著討論系爭干預是否具有正當理由。就第一個問題而言，ECJ 很快就得到肯定的結論，ECJ 認為 DRD 要求的保存資料義務當然構成對憲章第 7 條所保障的權利的干預，再加上這些資料可能會被政府機關使用，又是更進一步的權利干預。同樣地，ECJ 也認為 DRD 會對憲章第 8 條所保障的權利造成干預，而且還特別強調這個權利干預是「廣泛」

118 *Digital Rights Ir. Ltd, §23*. 大法庭(Grand Chamber)，針對具有高度重要性的案件，由 15 位法官組成的特別法庭。

119 *Digital Rights Ir. Ltd*, §27.

而且「特別嚴重」的干預。ECJ 此一判決並引用上述佐審員的意見，指出通訊資料會被保存的事實，而且嗣後的進一步使用用戶並不知情，將使得用戶產生其私人生活一直受到監視的感受。[120] 值得注意的是，同樣的論點，也出現在德國聯邦憲法法院的前述判決中。

就第二個問題而言，ECJ 並不採部分論者認為 DRD 侵害隱私權核心的主張。ECJ 承認 DRD 所欲達成的「對抗嚴重犯罪」以及「對抗全球性恐怖主義」兩個目標，是正當理由，但是，即使如此，ECJ 還是認為 DRD 對於隱私的干預，不符比例原則的要求。[121] ECJ 在該判決的此一部分，引用歐洲人權法院的判決，指出：考量到個人資料保護相對於私人生活保障的重要性，以及有鑒於系爭干預的嚴重性，所以 ECJ 會採取更嚴格的標準來檢視 DRD。[122]

ECJ 認為 DRD 合於比例原則中的適合性原則，因為其確實有助於增加各國政府發現重大犯罪的機會。但是，ECJ 認為 DRD 無法達到必要性原則的要求。換言之，ECJ 認為，對抗組織犯罪和恐怖主義確實是重大的政府利益，可以正當化某些現代化偵查手段，但是，無論多麼重大的政府利益都不可能正當化 DRD 所規定的方式。

ECJ 判決在這個部分的說理，尤其著重在 DRD 所設立的規範體系，並未對隱私權之干預設立足夠的限制。另一方面，卻又使得幾乎全歐洲的人口都受到基本權利干預。

依據 ECJ 的觀點，DRD 有下列五大缺失，而且因為這些嚴重的缺失，ECJ 判決歐盟立法機關逾越了比例原則，宣告 DRD 應立即失效：[123]

---

120 *Digital Rights Ir. Ltd*, §37.
121 *Digital Rights Ir. Ltd*, §41-44.
122 *Digital Rights Ir. Ltd*, §48-49.
123 *Digital Rights Ir. Ltd*, §§58, 60-62, 63, 66, 68.

1. DRD 就人的適用範圍而言，毫無設限，對使用電子通訊的人產生全面性的影響，而未區分通訊與嚴重犯罪或恐怖主義間可能的關聯。
2. DRD 並未限制國家機關使用個人資訊的條件，反之僅有指令第 1 條的籠統規範，而且沒有規定法院等其他中立機關扮演把關角色。
3. 資料保存時間未有足夠限制，不需區分資料類型而一律以 6 個月為保存期間下限。
4. DRD 對於被私人公司保存下來的個人資料，也沒有建立足夠的保障。
5. DRD 未要求資料僅被保存在歐盟範圍內，因此無法確保歐盟基本權利憲章第 8 條第 3 項的規範要求。

從宏觀的角度來看，ECJ 這個判決若能成為歐盟個人資料保護法制長遠發展的趨勢，必然會成為數位時代中人權保障的歷史分水嶺，而且很有可能會重塑歐盟對抗恐怖主義的策略，同時影響法院和政治部門在自由與安全間達致平衡的方式。

ECJ 的 *Digital Rights Ireland* 案判決所闡述的重點，無非是：當有一個規範體系會將所有人民的每一次數位通訊資料都儲存起來以供未來偵查或執法之用，將會對人際關係產生寒蟬效果，並在極度影響每個人的私人以及家庭生活。ECJ 認為這些資料總和在一起，可以精確地描繪出一個人的個人生活，包括每天的生活習慣、永久或暫時居所、日常移動路徑、進行的活動、與他人的社會關係以及周遭的社會環境等等。其實，這樣的見解，也與美國聯邦最高法院 Sotomayor 法官在 *United States v. Jones* 案中的協同意見書相呼應。[124]

[124] United States v. Jones, 132 S.Ct. 945, 956 [2012), Sotomayor J. concurring opinion:

從這個觀點來看，ECJ 注意到了數據資料蒐集計畫所帶來的普遍效應，並否決了「個人在與電信通訊提供者交換資訊時已經放棄隱私保障」的主張。ECJ 的判決，可以說是傾向德國聯邦憲法法院的見解，即使是在公共領域的政府全面監控，也必須保障人民隱私權。其結果在數位時代下擴張並強化了隱私與個人資料的保障。

ECJ 並未否認對抗犯罪和保護國家安全的重要性，而是採取了嚴格的比例原則，要求任何對隱私或個人資料的干預，都必須是達成政府目的所嚴格必須的，方能通過審查。這樣的觀點不僅對歐盟行政及立法部門課予極高負擔，事實上也排除了任何對國家、對個人資料的短期、針對性蒐集。當然 DRD「對全歐洲所有人民產生影響」這個因素某程度上影響了 ECJ 的決定，但是，真正的關鍵在於 ECJ 在比例原則第二階段審查時所提出的批評：蒐集範圍過廣、政府對資料的使用條件太寬鬆、保存期間過長，也因而限制了歐盟決策者再次使用全面性資料保存規範的可能性。換言之，ECJ 判決對於國家機關「全面監控」的行為模式，採取了相當保留甚或否定的態度。

從表面上看來，*Digital Rights Ireland* 案這個判決僅對愛爾蘭和奧地利產生效力，然而由於各國的資料保存措施都是 DPD 的例外，也都必須通過歐洲人權法的檢驗，而由於 ECJ 明確表示資料保存措施與歐盟基本權利憲章相扞格，不難想像各成員國的措施可能也無法倖免，任何成員國內國法院遇到類似案件之後，也都可以不需再提交 ECJ，而是可以逕行撤銷各國的資料保存措施。因此 ECJ 裁判

. . . surveillance . . . by making available at a relative low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, choses to track—may alter the relationship between citizen and government in a way that is inimical to democratic society.

所產生的效應可能就此順勢外溢，促使歐盟達成全新的隱私與個人資料保護規範。更有甚者，其外溢效果可能不僅限於歐盟境內。

ECJ 這個判決，正好出現在美國社會也激烈爭執政府監控計畫的期間，自從 Snowden 揭露美國政府的監控計畫後，關於隱私與國家安全間應該如何達致平衡，也在美國產生激烈爭辯。尤其當 Snowden 揭露 NSA 依據愛國者法，以流刺網式的方式蒐集美國公民以及外國人之電話、簡訊以及電子郵件的數據資料之後，更使得美國政府內外要求重新檢討監控政策的強大聲浪。而出現於大西洋隔岸的這個 ECJ 判決，對於針對任何「全面監控」式的科技架構應該如何規範的思考，具有相當高的參考價值。換言之，ECJ 這個判決，更偏向強調隱私與個人資料保護的制度設計，強調若是人民覺得自己隨時受到監控，將會對隱私價值及民主價值造成威脅，因此，人民在透過新興科技溝通時，也應該獲得保障。再者，ECJ 認為即使在國家安全的目的下，對於隱私或個人資料保護的干預，也必須以嚴格標準之比例原則檢視。比對近年來美國聯邦最高法院的判決，似乎也有類似的趨勢出現。然而，整體而言，美國聯邦最高法院截至目前為止依然保守地認為一旦個人將其資料分享給電子服務提供者，也就同時放棄就該些資料的隱私權主張，則是隱私和個資保護的障礙。正因為如此，在上述的 Jones 案判決當中，Alito 大法官在協同意見書中認為數位科技會降低隱私期待，而反恐調查也可能正當化隱私權的犧牲，以換取國家安全，[125] 也就不足為奇了。

在科技發展下，政府擁有監控人民更強大的能力，*Digital Rights Ireland* 案對美國司法者來說正是強化隱私保障的強力依據。而我們可以從 ECJ 判決所學到的，至少是：在數位時代裡，對隱私及個人

[125] 132 S. Ct. 945, 962, Alito J. concurring opinion.

資料的保障必須強化，而非減弱，而法律理論也必須隨之進化而非停滯不前。

其次，ECJ 這個判決，也可以讓我們認真思考，到底是應該由政府部門或私人部門負責保存個人資料。在歐盟的 DRD 之下，個人資料是由私人部門進行蒐集並予以保存，情資與執法單位並無法直接使用這些資料，而是只能間接向私人部門取得這些資料。相反地，在美國前述監控計畫下，則是直接由政府進行個人資料的蒐集與儲存，也因此激起大眾的關注，產生了是否應該將此一權限從 NSA 移轉到私人部門的辯論。而歐巴馬總統最終也表示其願意交由網路及電話公司執行這項權限，國會亦以此作為處理 NSA 監控問題的方向之一 (Keller, Parlapiano, Sanger, & Savage, 2014)。

但是，ECJ 的 *Digital Rights Ireland* 案判決，卻是認為私人與政府的區分並無意義，真正對隱私權造成侵害的，其實正是資料保存本身。換言之，ECJ 指出了更尖銳的問題：對個人數據資料的廣泛蒐集、儲存是否可以作為政府反恐的政策工具？正如 David Cole 所說的，較大的問題不是誰保有這些資料，而是政府以流刺網式的做法蒐集所有人的資料這件事 (Cole, 2014)。從這個角度來看，ECJ 的判決也有助於質疑這種大規模監控計畫的有效性。換言之，ECJ 的 *Digital Rights Ireland* 案，不但提供了美國反思其監控政策方向的機會，也可能有助於美國更強化其隱私保障，使雙方未來在反恐合作上有更深入的檢討空間。尤其是此一判決出現之後，足以證明過去區分個人資料蒐集由私人或政府為之的界線已經不再重要，因為，其實是「資料保存」這件事本身，而非保存資料的機關，影響了人民與政府的關係，並且對民主社會造成威脅，因此，如何對「資料保存」進行程序面與組織面的雙重控制，應是通訊監察的民主監督時，值得關切的重點。

肆、結論

我國通訊監察相關事務，雖然歷經演變，並且已經受到正式立法的規範，但是，無論是立法前後，都不乏質疑之聲 (朱敏信，2003)，即使是通訊監察之授權正式立法之後，其法律規定內容及其執行，近年仍因為監聽引發的政治風波而備受爭議、眾說紛紜 (李榮耕，2014: 148-175；林鈺雄，2013: 25-39；陳妍婷，2014；許家源，2014: 95-113；張麗卿，2014: 25-45)。歐洲人權法院的判決，對於臺灣的通訊監察法律實務而言，雖然比較遙遠，然而從比較法制的觀點來看，歐洲人權法院在通訊監察或通訊隱私領域中關於如何有效監督通訊監察作為，以保障個人基本權利的判決發展方向，或許值得我們在討論臺灣法制的興革方向時特別注意，並且可以引為如何填補我國法制現行缺漏的參考。

根據本文以上分析，歐洲人權法院在通訊監察或通訊隱私領域中的判決，對於合法性要件的要求，有兩個方向的發展值得特別注意。首先，法院事實上要求各國必須符合歐洲人權公約所設下的最低限度要求，而在最低限度的要求下，法院判決也發展出法治原則此一要件，也就是認為國家立法的目的，應該在於避免歐洲人權公約所保障之隱私權利遭到恣意干預侵害。就此而言，法院也進一步明確指出，關於秘密通訊監察或監控措施的授權規定，應該規定裁量範圍及其行使方式。

其次，第二個發展方向，則是著重於從適用對象的角度來擴張歐洲人權公約第 8 條的保障範圍。換言之，從歐洲人權法院的判決來看，其實已經將適用於保護個人通訊隱私的原則，擴張到無特定個別對象的一般性通訊監察也應適用的地步。*Liberty and Others* 案可以說是確認了這項見解的判決。在該判決中，歐洲人權法院認為英國政府系爭一般性監控計畫，也應該適用對個別對象採行通訊監

察或監控措施的要件，即可得知。在歐洲人權法院這個將以個人為對象的通訊監察要件擴張適用的趨勢下，即等於透過法院判決見解擴大歐洲人權公約第 8 條對通訊隱私權的保護範圍。而這個發展方向，或許也是未來處理後設資料與大型監控計畫爭議時可以仰賴的重要判決前例。

從以上歐洲人權法院判決的發展方向來檢視我國通訊監察法制，不難探知其不足之處：首先，在我國現行法制上，對於通訊隱私的地位，雖然已經透過憲法第 12 條與第 23 條的規定，以及通訊監察及保障法的規定，保障人民通訊隱私，並且要求公權力機關干預通訊隱私時必須先獲得法律授權，就「合法性」要件而言，表面上與歐洲人權公約的要求和歐洲人權法院的實務差異不大，然而，在法律授權密度的要求方面，以及在如何有效控制公權力機關實質上難以避免的濫權傾向方面，我國法制事實上仍有相當程度之不足(林鈺雄，2014: 55-65)。相對地，基於歐洲人權公約之規定乃最低限度的要求，歐洲人權法院認為國家立法的目的，應該在於避免歐洲人權公約所保障之隱私權利遭到恣意干預侵害，因此，法院進一步明確指出，關於秘密通訊監察或監控措施的授權規定，應該規定裁量範圍及其行使方式。而這個發展趨勢所指向的，則是更為嚴密、更具有實質意義的合法性要求。

其次，相較於歐洲人權法院的判決已經將適用於保護個人通訊隱私的原則，擴張到無特定個別對象的一般性通訊監察也應適用的地步，亦即透過法院判決擴大歐洲人權公約第 8 條對通訊隱私權的保護範圍，透過司法權強化通訊監察領域的民主監督功能，我國通訊監察相關實務作法與判決，截至目前為止，對於後設資料與大型監控所涉及的通訊隱私威脅與侵害，尚未有具體個案出現，然而，由於我國通訊監察及保障法等相關立法在後設資料與大型監控這

方面的規範頗為模糊，因此，不難想像此一類型的問題終將成為潛在爭議。在此一理解下，歐洲人權法院上述關於無特定個別對象的一般性通訊監察的立場及其判決發展方向，或許可以當作我國實務未來處理後設資料與大型監控計畫爭議時可以仰賴的重要比較法判決前例。

然而，即使是在上述兩個發展趨勢下，更值得注意的是，雖然歐洲人權法院的判決同時在「要件」和「範圍」兩個發展方向上，落實且擴張了歐洲人權公約第 8 條保障個人通訊隱私免於干預的要求，甚至也對目前各國方興未艾的一般性監控措施表達了基本立場。不過，由於「國安通訊監察程序」與「刑事偵查程序」兩者之間的界線，在常態性大型監控計畫的盛行下，極可能出現模糊化的傾向，加上各種資料庫的建立和運用逐漸成為同時出現在公部門與私部門的常態，以及一般個人的通訊活動隨時隨地均可留下數位足跡，在數位資訊取得易如反掌的情況下，到底在何種條件下，才算啟動國安通訊監察程序，以及才算啟動刑事偵查程序，即不免產生爭議，再加上在數位時代裡，上述程序可能對任何人均可隨時實質上秘密發動，但卻絲毫未受注意，這對於維持、發展民主與多元社會所必需的隱私權保護來說，可以說是充滿危機的發展趨勢，因此，也就需要更多的法院判決和法學辯論，方能釐清通訊監察和民主監督之間的關係。

只要允許國家以全面性或大規模監控模式從事治理，等於是政府掌握了至高無上的權力，可以去強迫人民的網路或通訊活動必須在國家能夠使用與控制的科技和資料範圍內受到監控，如此一來，便很容易會造成一種治理上的道德危機：蒐集、分析和儲藏資料變得太過於容易，並且往往超越了預定執法目標所需，自然就會對人民的各種基本自由權利造成極大威脅。而且，幾乎無限量的資料，

等於執法者創建了一個吸引力驚人的蜜罐，實際上就是一個引誘政府無限制使用人民資料的陷阱。政府一旦取得資料，以目前的科技而言，只要願意花費經費，無論是在完整儲存或徹底檢索資料方面，都是不難達成的目標，而且只要防護措施完善，這些資料理論上都不至於遭到刪除或破壞，於是，上述誘惑也就永遠不會消失。若再加上組織面和程序面的規範鬆散，那麼這些資料幾乎都是隨時可用的資料，可以任由執法者自由處理。因此，重新思考在資訊時代究竟應該建立怎樣的管制架構，才能無損於我們應享有的基本自由，是思考通訊監控措施時難以迴避的重要議題。換言之，究竟如何因應目前通訊監察執法技術的發展，要求國家必須提供與時俱進的規範架構，區分不同類型的資料蒐集行為和不同類型的儲存式資料庫，以及其對人民基本自由權利的威脅程度，決定通訊隱私的未來，其實可以說是舉世所有司法者的任務，歐洲人權法院應該也非例外。

政府監控對於個人自由具有潛在威脅，幾乎是無人反對的主張，然而即使如此，國家往往會以維護民主生活之名 (Heymann, 2003: 87-113)，以對抗間諜或者恐怖活動為理由，採行通訊監察或監控措施，以一般人難以察覺的幽微方式，侵害個人的隱私權利 (Richards, 2013: 1934-1935)。傳統觀點下強調免於干預的消極自由，雖然是指個人不受干預或侵害的自由，但是，另一方面，若是將自由理解為「反權力」(anti-power) 的憑藉，也就是免於權力者支配的依據，那麼，在民主憲政體制下，則必須強調對於權力應該施以適當節制，保護個人不在非自願的情況下成為他人手段或支配對象。因此，在民主憲政體制下，如果能夠強調政府的通訊監察或監控措施必須合乎一定法定程序要件，以及達成一定的透明化目標，也就是強化政府和人民之間的「相互監控」，增加人民對政府

監控活動資訊的理解可能性和理解管道，就應該更能確保原本在秘密之幕後從事通訊監察和監控行為的政府，不會恣意濫用其裁量權力和監控權力，而這可以說正是我們可以看出的歐洲人權法院在通訊監察此一領域的判決向來的努力方向。舉例來說，歐洲人權法院認為，以當事人適格為由，駁回個人對於政府秘密通訊監察或監控措施的司法挑戰，已經對個人自由造成一定程度的干預，就是為政府與個人之間的「互相監控」，保留一個監督政府權力行使的基本入口。和歐洲人權法院以上基本立場互相比較之下，美國實務不願實質審查政府秘密監控計畫內容的傾向，將會使得政府對人民通訊活動的恣意支配欠缺約束，也是反對政府監控權力陣營的努力在美國的挫敗。而美國法制上對於通訊監察領域中政府恣意支配人民通訊活動的現象，顯得輕忽且無力的態度，及其可能導致的出現 Snowden 事件之類的反彈後果，或許是討論我國通訊監察法制興革方向時，值得戒慎恐懼的比較法教訓。

「資訊就是權力」這句耳熟能詳的話，原意固然是指掌握資訊者往往是權力擁有者，但是更重要的是，資訊的掌握可以促進權力更有效率的運作，對人民發揮更強的控制效能。相對地，從民主監督的角度來看，透過司法權的運作，得以近用和取得與通訊監察計畫及措施相關的資訊，則往往是人民對抗來自於政府之潛在權利侵害的前提要件。資訊不對稱以及資訊接近使用權限不平等的結果，將使得政府權力與人民權利兩者之間產生嚴重失衡結果，因此，歐洲人權法院的判決要求政府所從事的通訊監察或監控措施必須符合一定程度以上的資訊公開要求，以及其認為個人通訊隱私權利遭到侵害與否的決定，並非取決於人民是否意識或理解到政府所從事的通訊監察或監控措施，而人民可以尋求的救濟，也不限於其可以具體證明或已經遭到揭露的政府通訊監察或監控作為，也都在在提

醒我們，對於通訊監察進行民主憲政社會應有的監督，當然不該把焦點放在政府的非祕密監控上，相對地，如何從立法嚴密程度和司法監督有效性雙管齊下，促成政府各種監控計畫與措施對於一般人民的透明化，才是真正的民主監督戰場，唯有如此，才是人民足以促使政府的通訊監察體制真正「去支配化」的正確方向。

參考文獻

王玉葉 (2007)。〈歐洲人權法院審理原則——國家裁量餘地原則〉，《歐美研究》，37, 3: 485-511。(Wang, L. Y. Y. [2007]. The national margin of appreciation doctrine in the dynamics of European human rights jurisprudence. *EurAmerica*, 37, 3: 485-511.)

王勁力 (2009)。〈淺論刑事 DNA 資料庫之擴建與人權保障——以我國去氧核醣核酸採樣條例修正方向探究〉，《月旦法學雜誌》，167: 65-81。(Wang, C. L. [2009]. On the criminal DNA database expansion and protection of human rights: An inquiry through the course of the amendment of the DNA Sampling Act of Taiwan. *The Taiwan Law Review*, 167: 65-81.)

朱敏信 (2003)。《論我國監聽制度設計之源起、演化及未來——以電話監聽為中心》。臺北：臺灣大學法律學研究所碩士論文。(Chu, M. S. [2003]. *On the origin, development and future of the surveillance system of Taiwan: Centered around the surveillance of telecommunications.* Unpublished master's thesis, Department of Law, National Taiwan University, Taipei.)

李惠宗 (2013)。〈個人資料保護法上的帝王條款——目的拘束原則〉，《法令月刊》，64, 1: 37-61。(Lee, H. T. [2013]. The emperor term in the Personal Information Protection Act: The principle of purpose-specification. *The Law Monthly*, 64, 1: 37-61.)

李榮耕 (2014)。〈簡評二〇一四年新修正的通訊保障及監察法——一次不知所為何來的修法〉，《月旦法學雜誌》，227: 148-175。(Li, R. G. [2014]. The curious case of the 2014 amendment to the Communication Security and Surveillance Act: A critique. *The Taiwan Law Review*, 227: 148-175.)

李寧修 (2015)。〈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/EC) 之發展為借鏡〉，《興大法學》，17: 87-140。(Lee, N. H. [2015]. Constitutional boundary on preventive retention of communication data: Taking the development of 2006/24/EC Directive as example. *Chung-Hsing University Law Review*, 17: 87-140.)

李震山 (2000)。《人性尊嚴與人權保障》。臺北：元照。(Li, C. S. [2000]. *Human dignity and protection of human rights*. Taipei: Angle.)

林鈺雄 (2008)。〈論通訊之監察——評析歐洲人權法院相關裁判之發展與影響〉，《東吳法律學報》，19, 4: 109-152。(Lin, Y. H. [2008]. Interception of communications – Critiques on judgments of European Court of Human Rights. *Soochow Law Review*, 19, 4: 109-152.)

林鈺雄 (2013)。〈通訊監察之修法芻議——通訊保障及監察法之部分修正條文〉，《萬國法律》，192: 25-39。(Lin, Y. H. [2013]. On the amendment to the Law of Surveillance: Selected amended provisions of the Communication Security and Surveillance Act. *FT Law Review*, 192: 25-39.)

林鈺雄 (2014)。〈法官保留原則與干預處分專庭——以通訊監察之修法芻議為例〉，《月旦法學教室》，136: 55-65。(Lin, Y. H. [2014]. The principle of exclusive authority of judges and the specialized court for compulsory measures: On the amendment to the Law of Surveillance. *Taiwan Jurist*, 136: 55-65.)

范姜真媺 (2016)。〈網路時代個人資料保護之強化——被遺忘權利之主張〉，《興大法學》，19: 61-106。(Fan Chiang, C. M. [2016]. The enforcement of protection of personal data in internet era: The claim of the right to be forgotten. *Chung-Hsing University Law Review*, 19: 61-106.)

翁逸泓、廖福特 (2014)。《私生活之權利——探索歐洲，反思臺灣》。臺北：新學林。(Weng, W. Y. H., & Liao, F. F. T. [2014]. *The right to private life: Reflections on Taiwan through the inquiry into Europe*. Taipei: New Sharing.)

陳妍婷 (2014)。《通訊監察「相關性原則」之探討》。臺中：東海大學法律學研究所碩士論文。(Chen, Y. T. [2014]. *A study on the relevance requirement in the Communication Protection and Surveillance Act*. Unpublished master's thesis, Department of Law, Tunghai University, Taichung.)

許炳華 (2015)。〈被遺忘的權利：比較法之觀察〉，《東吳法律學報》，27, 1: 125-163。(Hsu, P. H. [2015]. Right to be forgotten: Observations from the perspectives of comparative law. *Soochow*

Law Review, 27, 1: 125-163.)

許家源 (2014)。〈論通訊保障及監察法「調取票」之創設〉，《靜宜法學》，3: 95-113。(Hsu, C. Y. [2014]. A study of the "access warrant" in the Communication Security and Surveillance Act. *Providence Law Review*, 3: 95-113.)

張麗卿 (2014)。〈通訊保障及監察法之修正與評析〉，《月旦法學雜誌》，229: 25-45。(Chang, L. C. [2014]. The Communication Security and Surveillance Act: Amendment and critique. *The Taiwan Law Review*, 229: 25-45.)

劉定基 (2013)。〈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: 146-167。(Liu, T. C. [2013]. On the notion of "consent of the parties" within the meaning of the Personal Information Protection Act. *The Taiwan Law Review*, 218: 146-167.)

劉靜怡 (2016)。〈監視科技設備與交通違規執法〉，《月旦法學雜誌》，248: 73-84。(Liu, C. Y. [2016]. Monitoring technology equipments and traffic enforcement. *The Taiwan Law Review*, 248: 73-84.)

Angwin, J. (2014). *Dragnet nation: A quest for privacy, security, and freedom in a world of relentless surveillance*. New York: Times Books.

Bentham, J., & Božovič, M. (Eds.) (2010). *The panopticon writings*. London: Verso Books.

Bignami, F. (2007). Privacy and law enforcement in the European Union: The data retention directive. *Chicago Journal of International Law*, 8, 1: 233-255.

Cameron, I. (2000). *National security and the European Convention on Human Rights*. The Hague, the Netherlands: Kluwer Law International.

Cohen, J. E. (2012). *Configuring the networked self: Law, code, and the play of everyday practice*. New Haven, CT: Yale University Press.

Cohen, J. E. (2013). What privacy is for. *Harvard Law Review*, 126, 7: 1904-1933.

Cole, D. (2014, March). Can privacy be saved. *The New York Review*

of Books. Retrieved from http://www.nybooks.com/articles/2014/03/06/can-privacy-be-saved/

Cox, J. (2012). *Canada and the Five Eyes intelligence community*. Retrieved from http://cdfai.org.previewmysite.com/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf

Davis, R. N. (2003). Striking the balance: National security vs. civil liberties. *Brooklyn Journal of International Law,* 29, 1: 175-238.

De Hert, P. J. A. (2005). Balancing security and liberty within the European human rights framework: A critical reading of the court's case law in the light of surveillance and criminal law enforcement strategies after 9/11. *Utrecht Law Review,* 1, 1: 68-96.

De Hert, P. J. A., & Gutwirth, S. (2005). Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. In E. Claes, A. Duff, & S. Gutwirth (Eds.), *Privacy and the criminal law* (pp. 61-104). Mortsel, Belgium: Intersentia.

Desai, D. R. (2014). Constitutional limits on surveillance: Associational freedom in the age of data hoarding. *Notre Dame Law Review,* 90, 2: 579-633.

Donohue, L. K. (2014). Bulk metadata collection: Statutory and constitutional consideration. *Harvard Journal of Law & Public Policy,* 37, 3: 757-900.

Donohue, L. K. (2016). *The future of foreign intelligence: Privacy and surveillance in a digital age.* New York: Oxford University Press.

Dutertre, G. (2003). *Key case law extracts: European Court of Human Rights.* Strasbourg, France: Council of Europe Publishing.

Executive Office of the President. (2014, May). *Big data: Seizing opportunities, preserving values*. Retrieved from http://www.statedu.ntu.edu.tw/bigdata/big_data_privacy_report_may_1_2014.pdf

Gerards, J. (2012). The prism of fundamental rights. *European Constitutional Law Review,* 8, 2: 173-202.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. New York: Picador.

Greenwald, G., Poitras, L., & MacAskill, E. (2013, September 11). NSA shares raw intelligence including Americans' data with Israel. *The Guardian*. Retrieved from http://www.theguardian.com

Hardin, L. (2014). *The Snowden files: The inside story of the world's most wanted man*. London: Vintage.

Harris, D. J., O'Boyle, M., & Warwick, E. (1995). *Law of the European Convention on Human Rights*. Oxford, UK: Oxford University Press.

Heymann, P. B. (2003). *Terrorism, freedom, and security: Winning without war*. Cambridge, MA: The MIT Press.

Hoppin, M. B. (2012). Overly intimate surveillance: Why emergent public health surveillance programs deserve strict scrutiny under the Fourteenth Amendment. *New York University Law Review*, 87, 6: 1950-1995.

James, W., Lin, H. S., & Millett, L. I. (2007). *Engaging privacy and information technology in a digital age*. Washington, DC: The National Academies Press.

Keller, J., Parlapiano, A., Sanger, D., & Savage, C. (2014, January 17). Obama's changes to government surveillance. *The New York Times*. Retrieved from http://www.nytimes.com

Kerr, O. S. (2012). The mosaic theory of the Fourth Amendment. *Michigan Law Review*, 111, 3: 311-354.

Lemmens, K. (2003). The protection of privacy between a rights-nased and a freedom-based approach: What the Swiss example can teach us. *Maastricht Journal of European and Comparative Law*, 10, 4: 381-404.

Lyall, S. (2008, December 4). European Court Rules against Britain's policy of deeping DNA databases of suspects. *The New York Times*. Retrieved from http://www.nytimes.com

Lyon, D. (2007). *Surveillance studies: An overview*. Cambridge, UK: Polity.

Lyon, D. (2009). Surveillance, power, and everyday life. In C. Avgerou, R. Mansell, D. Quah, & R. Silverstone (Eds.), *The Oxford handbook of information and communication technologies* (pp.

449-467). Oxford, UK: Oxford University Press.
Murphy, M. H. (2013). The relationship between the European Court of Human Rights and national legislative bodies: Considering the merits and the risks of the approach of the court in surveillance cases. *Irish Journal of Legal Studies,* 3, 2: 65-91.
Nardell, G. (2010). Levelling up: Data privacy and the European Court of Human Rights. In S. Gutwirth, Y. Poullet, & P. J. A. De Hert (Eds.), *Data protection in a profiled world* (pp. 43-52). Dordrecht, the Netherlands: Springer.
Newell, B. C. (2014). The massive metadata machine: Liberty, power, and mass surveillance in the U. S. and Europe. *I/S: A Journal of Law and Policy for the Information Society,* 10, 2: 481-522.
Office of Science and Technology, Executive Office of the President. (2012, March 29). *Obama administration unveils "big data" initiative: Announces $200 million in New R&D Investment.* Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2015/11/19/release-obama-administration-unveils-big-data-initiative-announces-200
Orwell, G. (1949). *Nineteen eighty-four*. London: Secker & Warburg.
Pasquale, A. F. (2015). *The black box society: The secret algorithms that control money and information.* Cambridge, MA: Harvard University Press.
President's Council of Advisors on Science and Technology, Executive Office of the President. (2014, May). *Big data and privacy: A technological perspective*. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf
Reidenberg, J. R. (2014). The data surveillance state in the United States and Europe. *Wake Forest Law Review,* 49, 2: 583-608.
Ress, G. (2005). The effect of decisions and judgments of the European Court of Human Rights in the domestic legal order. *Texas International Law Journal,* 40, 3: 359-382.
Richards, N. M. (2013). The dangers of surveillance. *Harvard Law*

Review, 126, 7: 1934-1965.

Ruiz, B. R. (1997). *Privacy in telecommunications: A European and an American approach*. The Hague, the Netherlands: Kluwer Law International.

Sottiaux, S. (2008). *Terrorism and the limitation of rights: The ECHR and the US Constitution.* Oxford, UK: Hart.

Swire, P. P. (2006). Privacy and information sharing in the war on terrorism. *Villanova Law Review,* 51, 4: 951-980.

Tsesis, A. (2014). The right to erasure: Privacy, data brokers, and the indefinite retention of data. *Wake Forest Law Review*, 49, 2: 433-484.

Zoller, M. A. (2016).〈處在德國法與歐洲法緊張氛圍下的通信紀錄調取〉(王士帆譯)，《月旦法學雜誌》，252: 223-235。(Zoller, M. A. [2016]. Inquiries concerning telecommunication traffic data between the challenges of German and European law [Wang, S. F., Trans.]. *The Taiwan Law Review*, 252: 223-235.)

Surveillance and Democratic Supervision —Reflections on Tendencies in Developments in Europe and the United States

Ching-Yi Liu
Graduate Institute of National Development
College of Social Science, National Taiwan University
No.1, Sec. 4, Roosevelt Rd., Taipei 10617, Taiwan
E-mail: cytahr@gmail.com

Abstract

Pursuing an inquiry into how a democratic society is supposed to monitor government surveillance, this essay examines the attitude of the European Court of Human Rights (ECtHR) towards litigation derived from laws on surveillance in European nations, and juxtaposes the findings with relevant disputes in the United States; the purpose of this inquiry is to explore how these traditions might shed light on the situation in Taiwan and how the landscape of democratic supervision is to be shaped under modern surveillance law. This essay argues that the European judiciary is well-experienced in the realm of informational privacy, and that reforms to surveillance law in European nations is generally determined by ECtHR case-law. Of particular significance is the emphasis that the ECtHR lays on the interpretation and analysis of Article 8 of the European Convention on Human Rights (ECHR), specifically the focus on the notion "in accordance with the law" rather than "necessary in a democratic society." Such tendency might lead to the fact that the State Parties to the ECHR are merely willing to introduce domestic legislation. Accordingly, there is still plenty of room for improvement in the protective framework of informational privacy essential for a democratic society.

Key Words: surveillance, informational privacy, European Court of Human Rights, metadata, big data