# 南　　華　　大　　學

## 歐洲研究所碩士論文

# 歐洲個人資料保護之研究

## --以歐洲經驗反思我國作爲

# The Study of Personal Data Protection in Europe

## --An Introspection of Taiwan's Conduct from European Experience


指導教授：　廖福特　　博士

研 究 生：　翁逸泓


中華民國九十四年十二月五日

# 南　華　大　學

## 碩士學位論文

歐洲研究所

歐洲個人資料保護之研究

The Study of Personal Data Protection in Europe

研究生：[redacted]

經考試合格特此證明

口試委員：[redacted]

指導教授：[redacted]

所　　長：[redacted]

口試日期：中華民國　92　年　10　月　6　日

# 謝辭

終於，論文的進展階段已經到了要寫謝辭的時候了，在過去的幾年裡，夢想著要打出這份謝辭已經好多次了，但是卻驚覺，真正要開始動筆時，還真的有點不知所措。

這篇論文的完成，當然要先感謝指導教授廖福特教授的悉心指導與協助。老師在沒有心裡準備的情況下，居然敢收我爲門下的研究生，真是令人敬佩當時他答應指導的勇氣；當然，我也希望這篇論文的提出不會令他失望。老師在指導的過程中，真的花了很多心力，從資料的借閱、觀念的啓發、論文的寫作，一直到許多行政過程上的幫助，真的讓我十分感動！對於老師在論文專業上的指導，更是令我感到完整而確實的指導方式應當若是，在此獻上我的無限感激！

論文的完成當然也感謝李孟玢教授、鍾志明教授兩位口試委員的指導。兩位教授在本論文的寫作上提供的諸多觀點與啓發，對於整個視野的開闊與文字的表達正確性著墨甚深，當然也是對我有極大的貢獻的。另外，在歐研所求學過程中，吳東野老師對於整體歐洲概念的詳細傳授與用功的態度，帶給了我無比的震撼，讓我能進一步瞭解做學問的應有態度；而前任所長林信華老師、前任所長許仟老師、前任所長洪美蘭老師、沈玄池老師、蘇宏達老師、鍾志明老師等師長的諄諄教導，也都讓我有許多收穫，從而能夠在原本所學的法律學科之外，多方面的涉略社會科學各學科的知識。

室友欣杰、振峰、乃維、林鴻、智良帶給我在學期間許多幫助與歡樂，在搞笑的日子裡我們一同學習了許多無論是課業或生活上的歡愉；同學威鍇、芸瑋、怡伶、孟秋、林蔚、茜荻、毓清、世豐、彥平、倫彰常適時給我幫助與鼓勵，當然還有令我感動的同學間情誼的提供。另外，學弟妹佳玲、明螢、子妤等等也都給了我許多鼓勵；歐所助教淑娟姐給的我許多行政作業上之莫大幫助，大學時代學姐佩宜、航代；摯友明志、宗諭、志揚經常的關心，在此也一併致謝。

在口試完成後休學服替代役則是另一段美好的回憶，在台灣高等法院台中分院的服役期間，民六庭吳庭長火川、饒法官鴻鵬、吳法官惠郁、陳法官繼先以及陳書記官如慧、林書記官育德、柯書記官夢伶都給我很多司法實務上的學習機會，也讓我服役期間獲益匪淺。當然，檔案室林豔雪阿姨對替代役男們的照顧也讓我銘感五內。謝謝他們陪我度過充實的服役期間！

當然，論文完成最大的功臣是我的父母親。他們提供了我無虞的生活與求學環境，在日常的生活上，也能讓我處處的感受到他們對我的愛與溫暖，讓平常不常在家的我有了可以依靠的慰藉，真的非常感謝他們不遺餘力的讓我完成學業。

**論文名稱：**歐洲個人資料保護之研究—以歐洲經驗反思我國作爲
**校（院）所組別：**南華大學歐洲研究所碩士班
**畢業時間暨提要別：**九十四學年度第一學期碩士學位論文提要
**研究生：**翁逸泓　　**指導教授：**廖福特 博士
**論文提要內容：**

歐洲之人權傳統向來極其重要，在隱私權概念下的個人資料保護相關理論與概念，於歐洲即爲此悠久人權傳統下的新頁。在歐洲理事會（Council of Europe）所締之「個人資料保護公約」與歐洲聯盟（European Union）之「個人資料保護指令」確立法中心規範下，歐洲對於個人資料保護與資訊之自由流通之態度便形成所謂以法規範爲主核心的「歐洲模式」，並落實至其後之實際執行層面與相關法院判決上。

至於個別領域的案例方面，由於個人之醫療資料與警察資料均爲具敏感性之特種資料，則其公益與私益之平衡顯然較其他領域爲困難與重要，故而本文提出討論，並發現歐洲在此二領域之實際法規範與執行上均有所成就與值得學習之處，並於法院實際裁判上也歸納了相關之基本原則；另方面，由於網際網路發展之趨勢變化快速，傳統之相關個人資料保護理論或有不足之處，歐洲模式之處理下，也能發現其能夠與時並進的獨到之處。

對照歐洲之相關作爲，我國在立法與實際之執行上明顯未有與時並進之現象，又由於該「電腦處理個人資料保護法」本身原本之保守性格，遂使相關之作爲在實際運用上，出現許多窒礙難行或保護不全之處。面對快速的全球資訊化影響，實應加快腳步迅速立法修正，以符人權立國之信念。對於諸多政策在實施或考慮時，除了考量國家之整體經濟或行政效率之發展外，更應對於人權之事項多加注意，以避免淪爲過去帝制或專制時期思考方式之延續。

**關鍵詞：**個人資料保護、人權、隱私權、全民健保 IC 卡、全民指紋建檔、網際網路個人資料保護、歐洲理事會、歐洲聯盟

**Title: The Study of Personal Data Protection in Europe**
**--An Introspection of Taiwan's Conduct from European Experience.**

**Name of Institute: Graduate Institute of European Studies, Nan Hua University**
**Graduate date: Dec. 2005** **Degree conferred: LLM**
**Name of Student: WONG, Yi-Hung** **Advisor: Dr. Liao, Fu-Te**

**Abstract:**

The tradition of human rights in Europe is always important. The theory and the idea of personal data protection, which belong to the idea of right of privacy, then become a new page of this European human rights tradition. Under the norm of Council of Europe's "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" and "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" of European Union, the position of the personal data protection and the free movement of such data in Europe then become the "European way". Moreover, these data become practicable on the actually enforcement and related judgments.

In the specific sector, owing to the potential sensitivity of medical data and police data, the balance of public welfare and private rights then obviously become more important than other kinds of personal data. Therefore, this thesis will discuss these two sectors and finds that the importance in Europe. On the other hand, due to the fast change of Internet trend, the tradition researches of personal data protection have become a defect. Hence, that is another sector we will discuss in this thesis.

In Taiwan, the conduct is not as advanced as that in Europe---both to legislation and carrying out. In addition, because of the conservative character of "Computer-processed Personal Data Protection Law" in Taiwan, the conduct in our country becomes less practicable and does not have enough protection. Taiwan should pay more attention to human rights besides considering the entirety economy or administration efficiency when making policy in order to avoid becoming the last of the past imperialism or autocratic period.

**Key words:**
personal data protection; human rights; right of privacy; National health-care IC card; establish of loops and whorls on fingers; personal data protection on internet; Council of Europe; European Union.

# 目錄

# 圖表目錄

# 第一章　緒論

## 第一節 研究動機暨研究目的

### 一、　研究動機

觀諸歐洲歷史，人權之脈動，未曾一刻停歇；時至新世紀之開展以來，新興之人權議題亦不曾間斷出現。在網際網路已經充分改變許多人際與國際關係常態之今日，關於個人資料隱私之自決[1]，即成爲一項重要之當代人權指標。

在全球個人資料保護理論與法規範中執世界牛耳者，當爲歐洲區域之相關研究與發展。在歷史上，1949 年成立之歐洲理事會（Council of Europe, COE）於 1981 年便已經有「關於個人資料自動化處理保護個人公約」（Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data[2]，以下簡稱「個人資料保護公約」）之出現，乃是世界上最早的一份專門關於個人資料保護之法律文件，爲隱私權開拓了劃時代之新里程碑，並且由於該公約具有約束性之效力，故而影響甚大；另一方面，也因爲歐洲理事會在人權方面保障之傳統在世界上備受尊崇，故而個人資料保護之種子便於焉開散。

其後歐洲區域最重要之個人資料保護法律文件，當屬由歐洲最具代表性組織－－歐洲聯盟（European Union, EU）於 1995 年所制定之「個人資料處理及自由流通保護指令[3]」（Directive 95/46/EC of the European Parliament and of the

[1] 關於資訊自決權及此一名詞之詳細定義與介紹，參：李震山，《人性尊嚴與人權保障》，第七章「論資訊自決權」，台北：元照出版，2000，頁 275-318。至於人權架構上與個人資料保護之研究，請參本文第二章第一節。

[2] Opening for signature: 1987/01/28; Entry into force: 1985/01/10.

[3] 關於 Directive 之中文翻譯一般均翻譯爲「指令」，惟國內法律學者有翻譯爲「準則」者，如王泰銓，《歐洲共同體法總論》，台北：三民書局，1997，頁 204 以下。吾人亦覺其所持理由較佳，然爲顧及國內學習歐洲事務者多數爲政治或國際關係學者，又其多數均以「指令」爲名，爲免於混淆，仍從之。關於歐盟名詞之一般對照，詳參歐洲聯盟研究論壇之「歐盟名詞

European 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[4]，以下簡稱「個人資料保護指令」)，其承接前述「個人資料保護公約」之精神，對於個人資料保護在法規範之開展與基本原則之揭示上，有著無比之影響力。更有甚者，其關於第三國與之資料流通上，也有一定之限制，以維個人資料之安全[5]。由於該指令挾著歐盟整合以來之強大之經濟與政治能力，更迫使其他國家對之不得不有相關之因應作爲。

在實際之落實上，歐洲也出現了此方面之重要案例。在這些案例中也都出現一個在人權架構上必須要討論到的面向－－資訊自由流通權與個人資料隱私保護之競合。在歐洲的個案研究中，可以發現其對於此方面之處理結果並不像表面般看到的淨是爭端與矛盾，相反的，卻有相輔相成之效果發生，而這也是個人資料保護理論發展至今的一項重要爭點，亦即，究竟應採取如同歐洲模式般的嚴格規範作爲個人資料保護之方式？或是採取較爲偏重於個人資料自由流通面向去思考的美國模式？吾人相信，這將會是關於個人資料保護理論在未來持續爭議的重點議題。

另一方面，我國對於個人資料保護之法規範當然也深深受歐洲之思維影響，「電腦處理個人資料保護法」便是我國針對個人資料保護需求所制定之專法。制定之初已算是全球先進之法規範的「電腦處理個人資料保護法」，卻很可惜的並未追上歐洲與時並進切合新科技發展的腳步，在相關法規上始終原地踏步；甚至在實際之實行層面與落實上，有相對消極與保守之情況出現，則歐洲之相關經驗實在值得吾人借鏡。

環顧我國現狀，更有值得筆者作爲本文研究動機之處：在我國之許多新近

中英文對照表」(URL：http://iir.nccu.edu.tw/eurf/歐盟名詞對照表.xls)。

[4] Official journal of the European Communities, No. L281, 23/11/1995 P.0031.

[5] 主要規範在第廿五條，至於詳細之論述，參本文第二章。

之政策議題或政策焦點上，一再追求實體正義或是行政經濟效率的我國政府，在推動許多政策時，大多未對於程序正義或是人民之基本權利多加注意與提供足夠保護，特別是本文所欲論述的全民健康保險 IC 卡政策與全民指紋建檔議題，其對於個人資料保護之爭議性尤大，我國已有許多論著與團體持續對該議題表達關注與焦慮，甚至出現專爲個人資料保護發聲之團體[6]，足見我國關於個人資料保護之視野已經於焉開闊。

然觀諸我國國內之相關論述，少有專門以個人資料保護重鎮的歐洲爲源，去反思我國現況者。在法律學領域裡的論文或著述，大多以我國自有之法制與相關作爲爲論述之中心，間或出現以美國經驗或僅以歐洲單一國家如德國等爲焦點之著述，並且在關於個案之研究上，也尚未有專門以歐洲經驗之相關案例爲研究基礎之論文。故而筆者爲本文相關之研究，期能以不同之切入面向，對於我國個人資料保護之研究與發展有所助益。

## 二、 研究目的

承上述，本文之研究目於法規範之焦點方面爲透過對於歐洲經驗的研究，對於我國個人資料保護法規在法制的完備性上，發現現行之可能盲點，並提出相關之建議。

另外對於個別領域之研究上，則以較具敏感性之個人醫療資料與個人警察資料爲論述主體，透過歐洲實際在法規範或執行層面與法院判決上之研究，對於我國在該領域上所遭遇之個人資料保護問題，以明白得失並更積極的提出建議；又個人資料保護由於網際網路之發展已然進入嶄新時代，故而本文在個別之觀察領域中，加入網際網路線上個人資料相關保護議題研究，期能對於新世

[6] 參：全民個人資料保護聯盟： URL: http://www.tahr.org.tw/PDPA/index.htm.

紀個人資料保護問題，能以他山之石的經驗而對我國之相關作爲能有所幫助。

## 第二節 研究方法

本文由於需參酌歐洲之相關法制與作爲以爲我國之參考，故而除了必要之**文獻分析方法，**以國外之相關論述與歐洲理事會及歐洲聯盟官方文件爲經緯之外，尚須對照我國國內之相關文獻，以收對照與切合國內運用之效。故在專有名詞之翻譯上，力求與我國法制或學術習慣相符。並且由於在論述時會牽涉法制之沿革與理論之脈絡，故而部分使用**歷史回顧**之方法。

另外，本文也必須有**比較法制**上之方法，對於歐洲經驗之法規範與吾國之法規範做一比較之研究與處理；又對於個案領域之研究方面，則透過歐洲相關法院之**判決分析**，找尋出研究上之脈絡，並對我國之作爲提出建議。

當然，本論文在社會科學的研究方法上，也應用了**歸納法**及**演繹法**之精神，以符合社會科學方法之需要。

## 第三節 研究範圍暨研究限制

### 一、 研究範圍

本文之研究並無法針對所有歐洲地區之國際區域性組織，或是所有之國家之個人資料保護相關作爲逐一之研究，因爲那將使本文在篇幅上無限量之增加，並且不易集中而完整地表達所欲論述之焦點，故而僅將焦點集中於素以人權爲核心的歐洲理事會，與在歐洲最有影響力之歐洲聯盟二者，研究其對於個人資料保護領域的相關法規範與作爲。但如有論述上必要之時，仍會兼論部分

需要之歐洲國家或區域組織相關法典，甚或其他區域、國家之相關作爲。

其中歐洲聯盟部分，由於「個人資料保護指令」乃是歐洲聯盟時期方公布之指令，因此大部分論述範圍並未兼及於歐洲共同體（European Community, EC）時代之相關問題，僅於論述到歐體法之一般法律原則時，方會有所觸及。

其次在實際案例之研究上，歐洲理事會與歐洲聯盟本應有歐洲人權法院（Eueopean Court of Human Rights）與歐洲法院（European Court of Justice）二者各爲裁判，但由於歐洲聯盟在 1995 年方公布「個人資料保護指令」，並直至 1998 年各國之指令落實期限方結束，又況且直至 2003 年，仍有部分國家未有立法，乃招致歐盟執委會提出訴訟[7]，故而歐洲法院對此所爲判決並未如歐洲人權法院般完整與精細。特別是當本文在實例之研究上，僅對於個人醫療資料、個人警察資料與網路線上服務之個人資料爲個論之觀察，歐洲法院近來對個人資料保護之訴訟卻多是針對會員國未履行歐體法之訴，故此部分之判決分析僅以歐洲人權法院爲焦點；至於歐盟部分，則於適當時機補充歐盟官方之研究報告或官方舉辦之研討會論文。

至於我國之部分，則以「電腦處理個人資料保護法」爲法規範之中心，並於個論研究時納入全民健保 IC 卡政策、全民指紋建檔之議題與網路線上個人資料保護於我國實際網站之執行實況三者。

## 二、 研究限制

在本文研究之限制上，由於筆者時間上之限制，並無可能對於所有歐洲個人資料保護之文獻逐一收集閱覽，僅於能力所及部分盡量加以擴充延伸。主要資料之來源除歐盟之官方公報（Official Journal, OJ）外，乃以我國國家圖書館

[7] 關於此部分之詳細情形，詳參本文第二章第五節。

與中央研究院歐美研究所兩處國內研究歐洲法律圖書與期刊論文文獻最多之圖書館爲主，另兼及網路上所能取得之期刊論文等爲輔，爲本文研究上之最重大限制所在。

另外，國內參考資料方面在既定已形成政策部分當然以官方之說明或宣導文件爲中心，但未形成實際政策或議題部分者（全民指紋建檔與線上個人資料保護）均僅以相關既有之法規範爲經緯，旁徵部分時事報導與研究論述等，加以討論。

## 第四節 相關文獻回顧

在專門論著方面，關於個人資料保護與資訊自由流通之間之關係的代表性論著爲 David Brin 所著《*The transparent Society: Will technology force us to choose between privacy or freedom?*》[8]，其中有著精彩之論述與相關實例之介紹，並揭示對於兩者間之衝突性與互補之可能性，其並提出相當創新的「相互透明」理論對於資訊隱私與自由做一詮釋，對於吾人基本理論與思想上之建構有著相當大之助益。

另外，Lawrence Lessig 所著之《*Code: and other Laws of Cyberspace*》[9]與 Andrew L. Shapiro 著之《*The control revolution- How the internet is putting individuals in charge and changing the world we know?*》[10]則在網際網路之個人隱私權方面也有部分之相關論述，強調隱私權理論及其在新資訊社會下所扮演之

[8] David Brin, *The transparent Society: Will technology force us to choose between privacy or freedom?*, New York: Addison-Wesley Longman, Inc., 1998. 中文翻譯本：蕭美惠譯，《透明社會－個人隱私 vs. 資訊自由》，台北：先覺出版社，1999。

[9] 勞倫斯・雷席格（Lawrence Lessig）著，劉靜怡譯，《網路自由與法律》（*Code: and other Laws of Cyberspace*），台北：商周出版，城邦文化發行，2002。

[10] Andrew L. Shapiro 著，劉靜怡譯，《控制權革命－新興科技對我們的最大衝擊》，台北：城邦文化發行，2001。

角色。而在實際歐洲的個人資料保護法規與實際各領域之案例分析研究上，則在 David Bainbridge 之著作《*EC Data Protection Directive*》中有著基礎之介紹。但殊爲可惜的是，在 David Bainbridge 氏著中，只簡單對個人資料保護之相關歷史與法律之運作爲一簡要之介紹，並未就個案例之詳細判決法理爲說明，但是其卻創新的將各領域之個人資料保護爲個案式之研究，已踏出新的一步。

另方面歐洲理事會與歐洲聯盟本身對於個人資料保護方面亦有諸多研究之報告，但由於偏向於官方之文件，故相較之下多對歐盟之個人資料保護架構採取較爲積極面向之思考。在批判或較爲理論性之檢視方面，則並不如諸多美國相關期刊論文來的具有批判性[11]。不過在新進之研討會議中，則也有學者提出了較爲折衷之混合模式[12]，顯見個人資料保護之方式在未來仍然有許多討論與發展之空間。

在我國專門論著方面，許文義教授之《個人資料保護法論》爲目前唯一專門以個人資料保護爲中心之專門論著，其主要以我國「電腦處理個人資料保護法」爲出發點對於該法有詳盡之釋義，並提出了關於當事人權利個人資料之蒐集處理利用傳遞之原則等。至於在比較法制上面，其也將德國之相關法規提出比較，對於我國個人保護法制的基礎理論方面著墨甚深，惜對於較爲特殊領域之面向上未有進一步之論述。另外劉靜怡教授近來多篇論文，則對於歐洲與美國之個人資料保護相關法制之競合有著相當完整之介紹，亦使吾人在比較法制上收穫良多，在本文的許多觀念中，筆者亦加以利用。

於個人資料保護之相關論文中，國內方面最有代表性之論文爲台大熊愛卿博士之論文「網際網路個人資料保護之研究」。該論文完整清楚的交代個人資料

[11] 例如 Joel R. Reidenberg 便在柏克萊大學之科技法期刊中對美國自身之個人資料保護之業者自律模式做出相關批判。See Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 Berkeley Tech. L.J. 771, spring, 1999.

[12] See Jason Albert, *Privacy on the Internet: Protecting and Empowering Users*, COVINGTON & BURLING, Brussels, 2002/10/01.

保護之基礎理論與學理，在關於國際相關文件之網羅上也著墨最多。文中從解釋相關之名詞與歷史發展爲開端，進一步蒐羅國際性之相關文獻與文件並對台灣之相關法治提出建議，對筆者啓發甚大。

另外，陳宏達碩士之＜個人資料保護之研究＞；洪榮彬碩士之＜資訊時代之資料處理與資料保護—以德國聯邦個人資料保護法爲中心＞；林建中碩士之＜隱私權概念之再思考----關於概念範圍,定義及權利形成方法＞;葉淑芳碩士之＜行政資訊公開之研究-以隱私權益之保障爲中心＞;陳志忠碩士之＜個人資訊自決權之研究＞；簡榮宗碩士之＜網路上資訊隱私權保護問題之研究＞；紀佳伶碩士之＜電子化/網路化政府資訊內容隱私權之研究＞;李瑞生碩士之＜電子商務交易安全法制之研究＞等之相關研究，均對個人資料保護之基礎研究有一定之精闢論述，惟相關論文均以研究國內法爲中心，論及國際性文件尤其是歐洲之文件方面著墨較少，並且甚少對專門領域之個人資料保護加以申論。

又，曹昌棋碩士之＜從警察權之行使論個人資料保護＞；林振智碩士之＜資訊公開法制之研究－以警察機關爲例＞；吳全峰碩士之＜全民健康保險制度與醫療人權相關之分析＞；劉坤旺碩士之＜從憲法觀點論警察處理個人資料法制＞；張裕榮碩士之＜論資訊公開與個人資料保護之界線~以少年非行資料爲中心＞;吳昊碩士之＜由醫療資訊隱私之觀點論全民健保 IC 卡政策＞;蔡佳婷碩士之＜台灣醫療資訊安全之立法與實踐研究－由個資法的經驗到推動 HIPPA 之可行性＞等之論文，雖各自從特別領域對個人資料保護加以觀察研究，惜對於國外之相關案例或是比較法規範上較少著墨，大多專對我國相關法規範領域爲論述，而這也是我國法學上往往僅以國內法爲出發點時常見之現象。

## 第五節 研究架構

本文共分爲六大部分，除第一章緒論與最末章結論外，分爲四大部分：

第二章部分，本文主要以歐洲理事會與歐盟爲出發，對歐洲個人資料保護之理論法規範與相關實際作爲爲研究重心。該章首先釐清個人資料保護在歐洲整個人權保護理論體系之定位，並釐清其與資訊自由流通之關係。其後對於「個人資料保護公約」與「個人資料保護指令」二者爲立法沿革上與整個法規範體系架構內涵上之論述，並歸納個人資料保護之基本原則，作爲理論之核心。本章最末則對於「個人資料保護公約」與「個人資料保護指令」之後續法規與歐洲之實際執行狀況加以觀察，以瞭解法規範與實際執行時是否存在落差。

承續第二章對於個人資料保護之基礎研究部分，第三章爲個論部分之探究。本章分別以個人醫療資料、個人警察資料與網路線上服務之個人資料等三個面向，對個人資料保護在不同領域中的落實做一分析研究。在該三面向中，並各以法規範配合實際之法院判決互相印證，並歸納出其較爲特殊之處，以使吾人明白個人資料保護在實際之落實上之成效與對人權保障之真實反映。

於第四章中，則反觀我國之相關作爲，以歐洲之法規範模式與實際之案例的經驗，與台灣做一縱軸上之比較。在法規範的橫切面上，主要以我國「電腦處理個人資料保護法」與歐洲理事會「個人資料保護公約」及歐盟「個人資料保護指令」做一對照；在實際個別領域之案例的橫切面上，則以前章之個人醫療資料、個人警察資料以及網際網路線上服務個人資料對照我國之全民健保 IC 卡政策全民指紋建檔議題與我國網站之個人資料隱私權保護問題分別做一比較，以爲呼應。

第五章部分則是於前述幾章的研究之後，於該章中則具體分別對於我國之相關作爲在法規範上與在實際執行上所能有之加強之處，做一建議。該章中準此對於「電腦處理個人資料保護法」的中心規範與個人醫療資料個人、警察資料與網路線上服務之個人資料等個別之領域，以歐洲經驗爲師，期能對我國在未來之修法與實際執行個人資料保護時有所助益。

# 第二章　歐洲個人資料保護之規範及執行

對於個人資料保護之理論來說，歐洲區域對其相關之研究乃是一領導之先驅，也因此對於要探討個人資料保護理論來說，「歐洲經驗」是相當重要且不可或缺的。本章重點即以歐洲區域組織爲出發點，研究個人資料保護之基礎理論及其實行部分之成效，並提出個人資料保護與資訊流通之間之競合關係加以佐證，以強化個人資料保護理論之研究可行性。

## 第一節　個人資料保護之重要性：人權及隱私權之架構

本節中，筆者試圖找尋出爲何個人資料保護的理論在歐洲是最重要且最先進的？是否歐洲的個人資料保護值得研究？又，其定位爲何？亦即，其在整個人權保障架構中的位置？等等都是筆者欲釐清之所在，亦可作爲解釋吾人爲何以歐洲爲論述之中心。

首先，歐洲之整合由經濟之整合起步，已經進展至政治之整合甚或文化之整合，此時即需要各國間之文化合作，並且此等合作乃是建立在認知並尊重文化多樣性及差異性之上。此時歐洲聯盟的整合便會得到社會的正當性及合法性，而其中，歐洲文化的一個核心面向，即關於人權之問題，即不得不被重視。因爲，人權與民主不論是歐洲文化傳統中或是經歷兩次世界大戰後，均造成了

其爲極度核心的部分，也只有在此點建立認知並尊重人權保障的多樣性及差異性[1]，方有文化整合[2]之基礎。由此，歐洲的人權保障系統乃是全球最爲完整的，也是全球最先進的[3]。

其次，人權保障架構（參：圖 2-1）下的隱私權概念[4]，也在歐洲佔有重要之角色。不僅在「歐洲保護人權和基本自由公約」（the European Convention for the Protection of Human Rights and Fundamental Freedoms（1950），簡稱「歐洲人權公約」）中第八條明白列舉爲其保障項目；另於「歐洲聯盟基本權利憲章[5]」（Charter of Fundamental Rights of the European Union）中第七條：「人人均有權要求尊重其私人與家庭生活、住居及通信。」也可窺見立法者保障隱私之意涵。而隱私權之定義依廣義而言，乃是「對於個人領域內事務之控制權，其具體內容包括有三部分，即個人空間隱私權、個人資訊隱私權及個人自主權。在權力之定位上，隱私權是個人權利整體中，屬於完全涉己之部份。」[6]，在此定義之下，又可以導引出一項在今天資訊社會中不可或缺之隱私權能－－個人資訊隱私權。

而所謂的「個人資訊隱私權」，於法律名詞中與「個人資訊自決權[7]」相當[8]。

---

[1] 在消極的的意義上，文化合作乃是建立歐洲人民交往或互動的質料空間，例如制度、法律程序、科技網路、文化電子傳播等等。它爲歐洲整合提供了範圍最廣的文化概念意義，例如科技就是文化 (Technology is culture) 、所有的東西都是文化 (all is culture) 等等的訴求。在積極的意義上，文化合作提供行爲者 (agency) 的職能 (competence) ，包括人民個體參與社會與文化生活的能力，以及歐洲聯盟機制在各種生活領域中的決策與執行能力。參閱：林信華，《文化政策新論－建構台灣新社會》，臺北：揚智文化，2002，頁 178。

[2] 同上註，頁 15。

[3] See Fort Fu-te Liao, <European Human Rights: Often the first in the world>, The 21st century Seminars Cultural Exchange Programme Europe-Taiwan, Agenda of the 8th seminar, Oct. 20, 2001 (Sat.),
（URL:http://eusa-taiwan.org/seminar/taieuro/thesis/European%20Human%20Rights%20Often%20the%20First%20in%E2%80%A6.pdf.）

[4] 於 1890 年 Warren 與 Brandeis 二人即在哈佛法學中提出 The Right of Privacy 一文，咸認爲隱私權最早的論著，對美國之影響其實也相當巨大。See Edward J. Bloustein, *Individual & Group Privacy*, New Brunswick: Transaction publishers, 2003, pp.1-46; 67-121.

[5] 國內文獻對於該「歐洲聯盟基本權利憲章」之詳細分析，請參：廖福特，＜人權宣言？人權法典？--「歐洲聯盟基本權利憲章」之分析＞，《歐美研究》，2001，12 月。

[6] 此定義主要參：詹文凱，＜隱私權之研究＞，台灣大學法律學研究所博士論文，1998 年 7 月，頁，132-145；頁 291 以下。而對於隱私之概念，重要學者間亦有不同，例如 Warren 與 Brandeis 當初即認爲是所謂「獨處的權利」；而「幽靜生活」、「自身資訊」、「自身領域」、「個人生活經驗和行事」等等均分別有國外權威學者主張之，詳參詹文凱，前揭文，頁 132，註 32-39。

[7] 資訊自決權係指每個人基本上有權自行決定是否將其個人資料交付與提供利用。關於資訊自決

由於資訊社會下對於個人資料之保護，具有異於其他同屬隱私權保護客體之特性、需求及限制之條件，因此有必要將其特別挑出而加以論述。在歐洲，最早確定特別加以獨自出來成爲保護客體之時點，應爲 1983 年德國聯邦憲法法院之「人口普查案（Volkszählung）[9]」判決，其謂：個人原則上有權自行決定，是否將其個人資料公開及使用之「個人資訊自決權」（Recht auf informationelle Selbststimmung）。也因此，個人資訊自決權自此獨立成爲一項新的保護客體，而建構於個人資訊自決權基礎上的個人資料保護之理論，在資訊時代的衝擊下也進入了一個全新的時代。

爲此，歐洲個人資料保護之理論基礎係建基於歐洲人權保障架構之下，獨立且特別發展之重要領域－－在資訊社會之衝擊之下尤是。綜合以上論述，筆者歸納其架構應如（圖 2-1）所示：

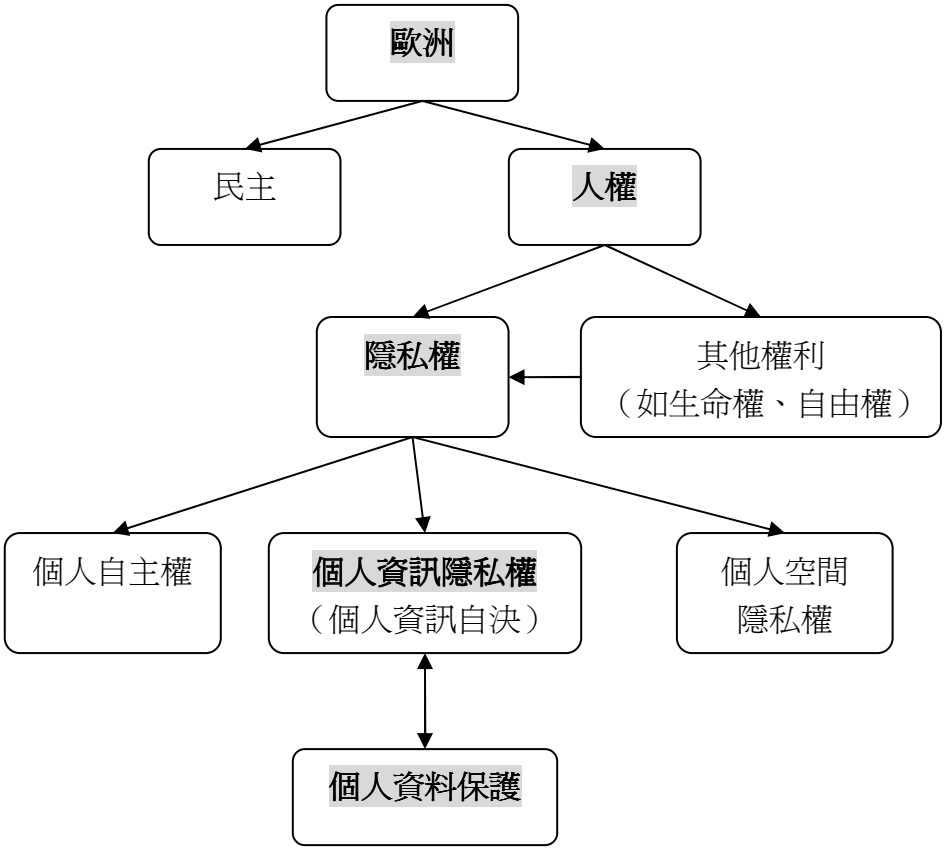
（圖 2-1）歐洲個人資料保護所屬架構：

製圖：作者自繪。

權之詳細論述，參：李震山，前揭註 1，頁 277-318。

[8] 參：陳志忠，＜個人資訊自決權之研究＞，東海大學法律學研究所碩士論文，2000 年 1 月，頁 47。

[9] 判決全文請參：蕭文生譯，《「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），司法院印行，1991 年 5 月，頁 288 以下。




另一方面，網路上侵害隱私權，造成個人資料受不當侵害之情形，在歐洲已經引起不僅歐洲各國國國內甚且是該區域間廣泛之不安及注意，此由各國紛紛制定個人資料保護之相關法律及發生相關之判決即可得知。但在另一方面，就網路上個人資料保護之議題而言，由於各國所採取之政策，莫衷一是，且由於網路無國界的特性，使得對個人資料保護嚴格之國家擔心其資料若經由網路移至其他未對個人資料加以保護或僅有寬鬆標準之國家，將使其對個人資料之保護無法落實。因此，其將可能對資料之流通採行日益嚴格之標準，而影響到人民資訊權之行使及國家科技、文化之進步。而對個人資料保護寬鬆之國家，在面對他國採行嚴密的保護政策，不許資訊流通時，亦或多或少對該國經濟產生影響，尤其是在經過歐盟整合後，此行為可能間接造成四大流通目的之達成發生困難。此種過與不及之現象，當非歐洲各國所樂見，是以，如何在兩者間求得平衡，調合互相衝

突的立場，即爲刻不容緩的工作[10]。此時便有賴歐洲區域國家間共同或各國間彼此加以協調，在區域組織之架構下制定公約、雙邊協定或多邊協定，或是以歐盟的制定共同體法規範之方式，來達成跨國個人資料保護之共識，縮短國與國之法律差異，並輔以程度相當之內國隱私權法令，以因應資訊社會之需要。因此，個人資料保護的跨國性規範之制定，實有其必要性。

於前述文中均可大略窺見，個人資料之保護可以作爲一系統化理論之主體；惟，相對地，以另一角度觀之，個人資料之保護也可能是一種例外之情形。例如，在政府資訊公開或是資訊快速流通之要求下，個人資料之保護反而是該種面向之下的一種例外地應用上之限制情形，然而此時兩者之關係究爲相互排斥或是互爲因果，則值得加以討論，以下便以上述面向對個人資料保護理論應用上之限制加以處理。

一個在邏輯上對於研究個人資料保護理論所不得不提出的一個問題，即：到底資料之蒐集是錯在哪裡？而公開展示所蒐集而得之個人資料又錯在哪裡[11]？由這個問題所延伸而出之問題亦即：到底應支持資訊之自由流通，或是個人資料之保護？

支持資訊流通可在不牴觸最低限度之隱私而全面開放之論點以爲：假定個人已公開揭示自己資訊，於公共場所進行交易之行爲之時，便放棄了隱私之權利，便得以適當之方式處理這些個人資料進，而加以流通。其原因可包含例如：此處之傷害不會太大；強迫他人忽略已公開展示之個人資料是不公平之負擔；此等個人資料可帶來許多益處；並且，蒐集個人資料者之目的並不一定是想要藉此真正了解該個人，而可能只是業者想藉此進行分類下差別待遇，以傳銷其商品或

[10] 參：簡榮宗，＜網路上資訊隱私權保障問題之研究＞，東吳大學法律研究所碩士論文，1999，頁 109-110。

[11] 這個議題之討論是借用了 Lawrence Lessig 的思考。參前揭著 9，頁 378。

服務而已[12]。

而在此議題中，支持個人資料保護之論點則認爲，應保護無辜因個人資料外洩而受害者之利益[13]。對上述兩難問題，便有學者提出了不同的解決之道：諸如 Davis Brin 認爲可以用監視[14]之方式，亦即其認爲要解決你暗中監視我的方法，並非阻止你窺探我而是讓我也能監視你，也就是讓你負起該有的責任。據此而認爲，政府及有能力蒐集個人資料之單位應負起責任；而 Lawrence Lessig 則認爲可以透過財產權規則[15]之方式，也就是認爲可以將個人資料便成爲財產權架構下之一環，在別人取得你的「財產」之前，必須和你協商這些財產之價值究竟有多高，也同時可以保護那些比其他人珍惜他們隱私的人，以及認爲其隱私並無價值之人，加以解決。

在前文中所提到之人權保障架構中，毫無懷疑的由「自由權」所引申而出之各項權利，包含資訊之自由流通權利，也是人權系統中相當重要之一環。甚至我們可以發現，其所出現的時間點及所受重視之程度，絲毫不輸給由「隱私權」概念所出之權利。在「歐洲人權公約」中，此二項權利當然也未有缺席，分別於第十條與第八條中加以規範。但是不禁令人質疑的是，此二權利究竟是否有矛盾與衝突之處[16]？乍看之下，隱私權之概念－－尤其是個人資料保護之概念似乎明顯的排斥了資訊自由，因爲限制了個人資料之存取必定需要相當程度地限制資訊之流通。

但是，其實自由與隱私在人權架構邏輯上，乃是分屬於不同之主題，並且此二邏輯之間並無互斥之二分觀念在其中，相反的，這兩個觀念應該是互爲因果

[12] 同前註，頁 378-380。
[13] 同前註，頁 380-381。
[14] 參前揭註 8，頁 126-135。
[15] 參前揭著 9，頁 400-401。
[16] See Michael Tugendhat QC, and Iain Christie (eds.), *The Law of Privacy and the Media*, Oxford University Press, 2002, pp.155-156.

的[17]。在具有隱私保障的環境之下，資訊自由反而因爲更容易使人安心而可能得以更快速之擴張，而另一方面，資訊之流通也相對地可以使個人資料在一更完整之體系之下受到保護，例如，個人資料之錯誤或缺漏可以更快速地被更正或補充，因此，這兩項命題並無衝突之處[18]。

況且，在資訊爆炸式流通的今日，資訊之公開與流通是不能也不可能被禁止的。在公領域方面，政府爲達成施政之目標與國家統治權之行使，獲得資訊以滿足其知之必要性（government's need to know），已經成爲不可或缺之手段，而其之所以需要強化資訊流通之功能，原因可能有三：其一爲蒐集資訊以決定現存之法令是否被違反，或新法令之實行與否有無必要；其二爲經濟與社會發展之所需，爲達統計目的而有取得之必要；其三則爲認許之目的，以發予執照或認可文件之目的，對於商品或服務之規範[19]。另一方面在私領域部分，若市場上之交易資訊不流通，則易導致不公平競爭發生之可能，而進一步阻礙了商業交易之發展，並且由於私人無法透過資訊之自由流通獲取所需要之資訊，則會阻斷人民知的基本權利。

準此，歐洲理事會在保護個人資料方面當然也不可能阻擋了資訊之自由流通，故而在歐洲理事會「個人資料保護公約」前言中，即稱其立法目的乃是爲了重申對資訊自由之承諾（reaffirming at the same time their commitment to freedom of information regardless of frontiers），並應協調尊重隱私之基本價值與個人間資訊之自由流通（to reconcile the fundamental values of the respect for privacy and the

---

[17] See David Brin, *op. cit.* pp.289-290.。

[18] 在我國法制上對於該自由權之限制即以不逾越必要程度爲界線，故而可推知自由權與隱私前之間並非絕對衝突。參：大法官解釋釋字第 327 號，楊建華大法官一部不同意見書：「按依憲法應受保障之自由權利，依同法第二十三條之意旨，爲防止妨礙他人自由、避免緊急危難、維持社會秩序或增進公共利益所必要者，固得以法律限制之。惟其限制應不得逾越『必要』程度，此即與所謂『比例原則』有關。在『比例原則』下，國家爲達一定目的，不得不限制人民自由權利時，如有多種方法，能達相同之目的者，應選擇損害人民權益最少之方 法行之，否則，即逾越必要之範圍，而與首開憲法意旨有違。…」。

[19] 詳參：葉淑芳，＜行政資訊公開之研究－以隱私權之保障爲中心＞，中興大學法律研究所碩士論文，1999 年 7 月，頁 154-155。轉引註自楊富強，＜資訊取得之公法研究－以私人與政府之關係爲中心＞，政治大學法律研究所碩士論文，1989 年 6 月，頁 34-38。

free flow of information between peoples），並且在跨國資料傳輸中亦強調不會妨害資訊之自由流通，若非如此，則該公約即很有可能會違反「歐洲人權公約」第十條中所規範之表意自由不受侵犯之權利[20]。

同樣地在歐洲聯盟 1995 年「個人資料保護指令」中之個人資料保護架構乃放置於其關於內部市場政策中之保障自由流通項目之下，其前言亦提到其對於本指令之立法目的，乃是在於爲了保護個人資料之處理與個人資料之流通。於該指令第一條第二款中也特別提到：「會員國不得以第一款有關保護之規定爲理由，限制或禁止會員國間個人資料之自由流通」之明文規範，此條文之目的明顯可看出立法者並不願意發生舉著保護個人資料之大旗，以對抗資訊自由流通等「因噎廢食」之情形出現。另外，於該指令第九條中也規範有表意自由應不受拘束之條款，規範有會員國應訂定有關因新聞之文學或藝術表現目的，進行個人資料處理之例外或排除條款，「以平衡隱私權利及表現自由原則」。

其後「電信事業個人資料保護指令[21]」（97/66/EC）之立法理由第一項中，亦表明本指令乃是承接「個人資料保護指令」之立法精神而來，故而對資料之自由流通（free movement of such data）並不生衝突之處；繼而，對此指令加以取代之「電信事業個人資料保護指令[22]」（2002/58/EC）中前言亦稱其目的乃是在確保「個人資料保護指令」中個人資料之隱私與流通二者，於電子通訊（electronic communication）部分，之個人資料保護應不妨礙會員國內部市場之流通，並應促進電子通訊之進步與發展[23]。

另外，規範個人資料保護相關架構之目的，係爲了要預防資料受蒐集及處理之危險，旨在保障個人資料受公務或非公務機關之濫權所造成之傷害，與確保

[20] 關於「歐洲人權公約」第十條與第八條之衝突可能性，詳參 Madeleine Colvin(ed.), *Developing Key Privacy Rights*, Hart Publishing, 2002, pp. 13-44.其中較爲著名之案例如 *KVN v. Sweden* (1987, 50 D & R 173.)等。

[21] Official Journal L 024, 30/01/1998 P. 0001 – 0008.關於本指令詳細內容參下文。

[22] Official Journal L 201 , 31/07/2002 P. 0037 – 0047.關於本指令詳細內容參下文。

[23] 參該指令說明理由第八項。

個人能控制其本身之資料，及限制或排除特定之蒐集或運用。其中心意義是在於在未通知當事人並獲得其書面同意前，資料持有者不可將當事人爲某特定目的所提供之資料運用於另一目的上。

故在本章第三節中，筆者即以兩個歐洲區域組織爲例，對歐洲的個人資料保護規範做一法律上之分析。附帶一提，筆者之所以以歐洲理事會與歐洲聯盟此二機構爲例，而不選擇其他之歐洲區域組織加以敘述，除了因爲限於篇幅之外，主要之原因，其一歐洲理事會乃是歐洲處理關於人權議題歷史最悠久[24]，同時也是最完整的歐洲區域組織，其所轄之「歐洲人權法院[25]」（European Court of Human Rights）同時也是處理相關議題的最重要司法單位；其二，歐洲聯盟爲現今歐洲最重要之區域組織[26]，其影響力不容忽視，因此必須加以論述。

## 第二節　定義及立法歷程

### 一、　定義及相關概念

欲對個人資料保護理論有一概括式之理解，則對其相關字辭之定義即爲不可或缺之先決要素。以下便分別對「資料（Data）」、「個人資料（Personal data）」、

[24] 歐洲理事會於 1950 年通過並於 1953 年生效的歐洲人權公約所建立的人權保護制度，是目前國際性和區域性人權保護制度中最爲有效的。另外，歐洲人權公約的正式名稱爲「歐洲保護人權和基本自由公約」，爲第一個區域性人權公約（「歐洲人權公約」）。

[25] 歐洲人權法院設立於 1959 年，由同歐洲理事會成員相等數目（至 2003 年 7 月止共 45 國）的法官組成，其中不得有兩名法官爲同一國家的國民。法官由歐洲理事會成員國提名（3 名候選人，其中 2 人爲國民），由諮詢議會以多數票選出。候選人應具有「高尚的道德品質」並具有高級司法職位之任命資格或者公認的法學家。法官獨立，任期 9 年，可連任。法院選舉一名院長，一至兩名副院長；法院制訂其內部規則並確定審判程式。本文第五頁所引歐洲人權法院同此註。See Brice Dickson (ed.), *Human Rights and the European Convention- the effects of the convention on the United Kingdom and Ireland*, London: Sweet & Maxwell Ltd, 1997, pp. 17-21.

[26] 對於歐洲聯盟是否即爲傳統國際關係定義上之「區域組織」尚非有一確切定論，惟此處非本文討論重點，故姑且先以此名詞爲之。

「資料處理（Processing of personal data）」等較基礎之用語之定義加以敘述，以便其後行文：

（1）「資料」：

此一詞彙在電腦學上，係指任何可以用電腦加以處理之物，包含各種可能形態之數字、文字、圖表等等[27]。另外須注意的一點是有文獻[28]指出其與「資訊（Information）」之不可混同性，因爲就個人資料保護而言，「資料」此一用語顯較「資訊」此一用語對當事人之隱私權，更能有較周全之保障。由於通常稱「資訊」時，表示已經將「資料」做一有系統之歸納或整理，故吾人認爲在大部分談到個人資料保護之時區分並無實益，因爲當保護個人「資料」之時，其範圍當然包括已經處理之資訊或未處理之資料。

（2）「個人資料」：

依據「個人資料保護指令」第二條 a 項之規定，所謂「個人資料」是指「有關識別或足以識別[29]自然人（資料當事人）之任何資訊」；另外，在「個人資料保護公約」中，「個人資料」乃是指「關於得確定或得確定個人之資訊[30]」 ；而德國「聯邦個人資料保護法」（Bundesdatenschutzgesetz ，BDSG）第二條則將個人資料規定爲「涉及特定或可得特定之自然人之所有屬人或屬事之個別資料」，其均大同小異，採概括式[31]之規定。

（3）「資料處理」：

---

[27] 參：潘大連/黃小魏，《電腦辭典》，台北：貓頭鷹出版社，1997，頁 57-58。轉引自：許文義，《個人資料保護法論》，台北：三民書局，2001，頁 18，註 55。

[28] 參：許文義，前揭書，頁 18-22。另有主張區分與否並無大礙者，參：陳志忠，前揭文，頁 7，註 8。

[29] 足資識別之人指直接或間接能與識別者，特別是以參考識別數字或以其身體、生理、經濟、文化或社會歸屬之一項或多項特定因素。See Directive 95/46/EC, Art.2.(a).

[30] 參「個人資料保護公約」第二條 a 項。

[31] 相較於歐洲聯盟及歐洲理事會的概括式立法，我國電腦處理個人資料保護法第三條第一款：「個人資料，指自然人之姓名、出生年月日、身分證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病例、財務情況、社會活動及其他足資識別該個人之資料。」則是採例示性及概括性並列之立法方式。

於歐盟「個人資料保護指令」中的第二條 b 項「資料處理」被定義爲：「不論是否以自動化之方式，而對個人資料所進行之操作或一組操作，如：蒐集、紀錄、組織、儲存、改編或變更、檢索、諮詢、利用傳輸揭露、傳播或其他任何產生效用、排列組合、凍結、刪除、銷毀等」；而歐洲理事會之「個人資料保護公約」第二條 c 項，則只有對自動傳輸之部份作出規範。總之，資料處理是指從資料被觀測或蒐集時起，直到其遭破壞爲止，這段期間之內對資料所進行之任何操作行爲而言。

## 二、 立法歷程

在簡略地對相關名詞加以定義之後，本文將簡單地介紹上述提到的兩個歐洲區域之法律文件，即歐洲理事會的「個人資料保護公約」及歐洲聯盟的「個人資料保護指令」二者。

首先，在歐洲理事會部分，1980 年歐洲理事會完成了有關保護個人資料之「個人資料保護公約」，並於次年供會員國簽署。該公約並已於 1985 年 10 月 1 日正式生效，現今（2005 年 12 月止）已有三十四個國家加入[32]或批准，另有六國簽署尚未批准，爲目前世界第一個有拘束力之關於隱私權保護之國際公約，但是其在適用範圍上，乃僅限於經自動化處理之個人資料，而不包括人工處理之個人資料，惟其所指個人資料之範圍，尚可及於法人資料。另外，歐洲理事會並有四十四國同意讓歐體加入該公約。

復次，於歐洲聯盟部分，對於隱私權與個人資料保護之議題，歐盟以其經由歐洲共同體法所確立的高度法制化之社會背景下，並基於保護個人資料之立場，率先訂定各項指令以維個人資料之安全。其中，最重要者爲 1995 年的「個

[32] 本公約亦開放予非歐洲理事會之會員國加入。See URL: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=&CL=ENG

人資料保護指令」，於 1995 年 12 月由歐盟部長理事會（Council of the European Union）及歐洲議會（European Parliament，EP）通過，並於 1998 年 12 月 25 日正式生效，由十五個會員國據以修訂其資料保護立法[33]。本指令也確立了歐盟保護自然人基本人權及自由之立場，尤其是關於其個人資料隱私權保護之立場。

## 第三節　法律基礎及基本原則

### 一、 歐洲理事會個人資料保護

（一） 法律基礎－「個人資料保護公約」

歐洲理事會乃是歐洲區域組織中對人權保障著墨甚深者，其對個人資料保護也是處於領先者之姿態。其中的一份國際條約「個人資料保護公約」是最重要的關於個人資料保護的基礎條約。本節以降即以本條約爲中心，討論其立法目的及過程，並分析其規範內涵及所確立之原則，最後並敘及相關的後續發展及「個人資料保護公約」之影響[34]。

1. 立法目的

歐洲理事會「個人資料保護公約」之立法目的，根據其前言所述，約有三點：（1）對人權、基本自由及對法治之尊重，以達成會員國間更臻統一之目的；（2）鑒於經過自動化處理之個人資料跨國之流通量增加，實有必要對個人權利、基本自由，尤其是隱私權加以尊重；（3）重申對資訊自由之承諾，並應協調尊重

[33] 此即關於指令之間接效力，亦即關於應達成之目標具有拘束力但會員國得自行選擇達成目標之形式與方法，規定於歐洲共同體條約第二四九條。參：王泰銓，前揭著，頁 204 以下。

[34] 至於歐洲理事會之「個人資料保護公約」與歐洲聯盟的「個人資料保護指令」在基礎原則與其他見解上之異同的比較，詳參本論文下節，本節僅分別對此二法規範圍扼要之說明，合先敘明。

隱私之基本價值與個人間資訊之自由流通。

然而上述僅爲條約所載之立法目的，其實當時之背景因素眾多，並非僅此三點。例如[35]：

（1） 就原有的歐洲人權公約中，其第八條所規範之隱私權[36]與第十條中所規範之表意自由權[37]所引申而出之資訊自由流通權，具有潛在性之衝突之處。當其中的一項權利行使之時，會多少地造成另一項權利行使之限制，也因此，需要制定相關之規範加以調和。在此，需加以說明的一點是資訊自決

（2） （資料保護）與資訊自由之間，應非僅具有典型的衝突關係存在，反應爲兩種相輔相成之權利。蓋人民基於資訊自由，只得向國家請求具有一般得接近之訊息，故其範圍是有限制的；但是在另一方面，根據資訊自決權所衍生之受告知請求權[38]則可以相當程度地補充前述資訊自由權上之限制；此外，資訊公開之目的在增進行政透明，個人資料保護之目的則是透明化公務或非公務機關對人民個人資料所擁有之檔案，而可以對其加以監督，從而兩者並無牴觸之處[39]，也因此歐洲理事會認有必要有一明確之法律基礎對此二者加以調和。

（3） 六〇年代之後電子資訊開始加速度地快速流通，值此同時，各國政府公務部門資料庫（database）或非公務部門資料銀行（data bank）

[35] 參：歐洲理事會個人資料保護背景說明，(URL: http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Background/。)

[36] 「歐洲人權公約」第八條：人人有權於其私人與家庭、家居生活及通信受到尊重。

[37] 「歐洲人權公約」第十條：人人有不被公共機關阻撓且不論國界，而得接收與傳送資訊或意識之自由。

[38] 即受告知請求權原則，下述之「個人資料保護公約」及「個人資料保護指令」均可歸納出此原則。

[39] 關於此二權利之調和，詳參：陳志忠，前揭文，頁 132-136。另參：葉俊榮、許宗力主持，＜政府資訊公開制度之研究＞，行政院研考會，1996 年 8 月，頁 249。另外，在兩者理論上是否有衝突之處，詳參本章「應用上限制」一節。

之出現，雖然使得政府管理行政之效果增加，卻對人民之個人隱私造成相當程度之傷害，故極需促成一管理之架構，加以保障之。

（4） 個人電腦發達及社會暨經濟之快速發展，造成個人成爲資訊社會之積極角色，亦即，個人參與資料流動的程度提高，故更需要一個相關之機制加以控制。

凡上敘述，均可作爲其立法理由之參考。

2. 規範內涵

本公約條文共有二十七條，分爲七個章節。首先第一章爲總論之部份，規範有相關之目的（第一條）、相關定義（第二條）、範圍（第三條）等；次章爲個人資料保護之基礎原則（第四條至第十一條）；第三章爲跨國資料流通之規範（第十二條第一項），並同時要求簽約國不得僅因純粹保護隱私權之目的，而限制資料跨國界之流通，除非簽約之他國家未訂定法律提供相同之保護，或其移轉係以簽約國爲媒介，且將再移轉至其他非簽約之第三國（第十二條第二、三項）；第四章爲會員國之間，關於個人資料保護之相互協助（第十三至十七條），分別規定有：各簽約國應指定一官署主管有關資料保護之規定，及向他簽約國提供該國有關法律及行政執行之資訊（第十三條），對僑居人民之協助（第十四條），一國官署由他國所取得之資料不得做其他目的之使用（第十五條），受請求協助官署得拒絕他國之情事爲：請求不合法、不符合本公約條款，或若答應之，則受請求之一方之統治權、安全或公共行政政策目的將有所違背，或其與管轄權範圍內個人之基本權利與自由相衝突（第十六條）；第五章爲管理此事務之委員會（諮詢委員會）及其相關功能（第十四至二十條）；第六章爲修正案之條款（第廿一條）；最末章爲附則，規範有執行時間（第廿二條）、非會員加入方法（第廿三條）、領域條款（第廿四條）、保留及其他條款（第廿五至廿七條）等。

本條約爲達成序言中及前述所稱之目標，從而有上述之相關規範，希望藉此建立起資料保護方法之基本原則、跨國資料流通之資料原則及審議機制等。而其在內涵上因爲必須區分不同領域[40]而有不同之保護方法，解決之道便是以建議（recommendations）之方式，交由各國政府分別以國內立法之方式加以處理。在相關審議機制方面，該公約設有「諮詢委員會」（Consultative Committee，T-PD）及「資料保護計畫研議小組」（Project Group on Data Protection，CJ-PD）二者，雖然二者工作乃是相輔相成的相互協調，然其內容上仍有區別，前者乃是公約的守護者及促進者，職司解釋疑義及確保與促進公約之執行；後者乃是規劃不同領域的技術面與細節面的指導原則。

並且，此公約雖與「經濟合作與開發組織」（Organization for Economic Cooperation and Development, OECD）於 1980 年所通過之「關於個人資料之國際流通暨隱私權保護指導原則」（Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data）之內容及所持之基本原則雖然大同小異[41]，然仍有不同[42]之處，例如「個人資料保護公約」所有之可排除他人主張權利之情況，如國家安全（第九條二項二款）等，便爲該指導原則所無；況「個人資料保護公約」爲第一個在國際法上具有約束力之國際資料保護條約，對各會員國具法律拘束力，效果遠勝該經濟合作與開發組織之指導原則[43]。

（二） 所確立之原則

「個人資料保護公約」條文中所建立之基礎原則，相當具有指標性及開拓

[40] 關於個人資料保護中的領域理論，大意約略爲：將受保護之私人生活形成領域，放置於一同心圓之模型上，並加以區分爲不同層級而受到不同強度之保障，及具有不同程度之對抗干預能力。詳參：陳志忠，前揭文，頁 56-58。

[41] 關於經濟合作與開發組織之「關於個人資料之國際流通暨隱私權保護指導原則」部份之基本原則，詳參：熊愛卿，＜網際網路個人資料保護之研究＞，台灣大學法律研究所博士論文，2000 年 7 月，頁 131-132。

[42] 參：紀佳伶，＜電子化/網路化政府資訊內容隱私權之研究＞，政治大學公共行政學系碩士論文，2000 年 7 月，頁 108-111。

[43] See Julia M. Fromholz, *Data Privacy: The European Union Data Privacy Directive*, 15 Berkeley Tech. L.J. 461, 2000.

性，約略有下列數點：

1. 立約國義務原則（Duties of Parties）

指簽約國至遲於公約就該公約國生效之時，即應採取履行公約中的保護基本原則之措施（第四條），並且，各簽約國應採取適當之制裁及救濟之措施，以對抗關於個人資料保護原則國內法之破壞行爲（第十條）。

2. 資料品質原則[44]（Quality of data）

該原則含有下列五項子原則，規範蒐集、處理、儲存及消除個人資料之方式，以確保資料之品質合乎各子原則之標準（第五條）：

A. 蒐集與處理之公平性與合法性原則（fairly and lawfully）。

B. 目的性原則：資料之儲存應有特定及合法之目的，並禁止不符合資料儲存目的之利用。

C. 必要性原則：應爲適當（adequate）適切（relevant）及不過度（not excessive）地逾越資料目的之儲存。

D. 內容正確原則：個人資料內容應準確（accurate），且於必要時應進行更新。

E. 儲存逾期禁止原則：以一種准許確認所儲存個人資料是否已逾其目的上之需要之形式，加以保存個人資料。

3. 特種資料處理原則（special categories of data）

[44] 有學者翻譯爲「處理個人資料之限制」，且將資料品質概念下的其他原則分別獨立出，而成爲個別之原則，參許文義，前揭書，頁 163-164。筆者以爲，若依照其所歸納之原則加以分類，則恐怕吾人不能完全掌握該條約中法條之原有體系，故本文另以其原本之法條體系加以歸納出原則，以釐清原本「個人資料保護公約」所欲建立之體系架構，並推論出該公約立法者之思考邏輯方向。

除國內法提供適當之保護外，有關健康、性生活、種族、政治意見、宗教信仰之個人資料，不得予以自動化之處理（第六條）。

4. 安全確保原則（data security）

爲防止個人資料被非法地蒐集、變更或傳遞、銷毀或滅失，須採取必要之保護措施，以維護其安全（第七條）。另，於特殊領域之安全，亦需要特別加強保護（第八條）。

5. 排除原則（exceptions and restrictions）

亦即對個人資料品質原則之例外與限制，指上述之資料品質原則，於依據簽約國之法律規定，並爲保持民主社會之利益之時，於以下二要件之下，得排除之（第九條）：

A. 保衛國家安全、公共社會福祉、國家金融利益之健全，或防止犯罪行爲之發生。

B. 保護資料主體或他人之權利與自由。

6. 延伸保護原則（extended protection）

指上述所列之各種規範並非個人資料保護之最上限，亦即各簽約國得以國內立法之方式，對個人資料保護有更完善之規範（第十一條）。

## 二、 歐洲聯盟個人資料保護

由於歐洲聯盟是歐洲乃至於全球發展最完備的一個區域組織，故相對地其所觸及的任何議題，不免地需要更加深入地討論，並且，也通常吸引了較多的關注。同樣地，在個人資料保護方面，歐洲聯盟也可以說是歐洲最重要而不可或缺

的討論面向。經過不斷地深化與廣化的整合，歐體的法律架構爲共同體會員國所一致尊重與遵守，故其在這方面所頒布的指令，也成爲影響會員國最深的一項法律文件。相對於歐洲理事會對於個人資料保護的「老資格」，歐洲聯盟關於個人資料保護之作爲，則可稱爲最有「影響力」的，這不僅是在歐洲區域部分，在全球亦有其舉足輕重之地位。以下，本節即以歐洲聯盟最重要的 1995 年的「個人資料保護指令」爲中心，敘述其相關之立法目的、規範內涵、所確立之原則及其後續之發展及影響。

（一） 法律基礎－「個人資料保護指令」

1. 立法目的

就歐盟「個人資料保護指令」中前文所羅列之所依據要點[45]而言，歐洲共同體創立目的之一，係爲確保人民基本權利、維護並強化和平及自由暨促進民主。而資料處理系統係爲服務人類而設計，此時即應抱持尊重個人基本權利與自由，尤其是尊重隱私權之態度，故當其建立內部市場 （internal market）[46]時，隨著經濟與社會之整合，必然會發生因爲會員國間公務與非公務的密切交流，而使個人資料交換傳遞之需求量大增，從而使個人資料受侵害之情形益增，此時，不僅是要求個人資料於會員國間得以自由流通，同時亦需要保障個人基本權利。

另外，由於會員國間對個人之權利與自由，尤其是隱私權部分之認知，並不完全相同，故保護之水準也不盡相同，規範不一，形成會員國間資料傳輸之障礙，例如：在人員自由流通方面，常需伴隨著個人資料之一併流通，若會員國間個人資料流通之規範不同，便造成該人員之自由流通造成限制，在勞務方面亦同，而成爲經濟活動之阻力。因此，爲了達到內部市場四大（人員、貨物、勞務、

[45] 參：本指令前文（1）-（10）。

[46] 關於內部市場之資訊，詳參：（URL: http://europa.eu.int/comm/internal_market/en/index.htm.）。值得注意的是，因爲個人資料保護是爲滿足建立內部市場後，所可能發生問題之因應，故歐盟個人資料保護之網頁，是建立在該內部市場網頁之子目錄之下的，這也同時可以讓吾人更清楚地釐清該架構。

貨幣）自由流通之目標，必須要縮減各國之法律差異，並希望能在縮減各國法律差異，達成相當程度保護之後，會員國能不再以保護權利及個人隱私爲由，禁止個人資料於歐盟內部自由流通，從而達到內部市場自由流通之目標[47]。

上述兩個主要的立法目的－－其一，會員國應保護自然人（法人非本公約範圍）之基本人權與自由，特別是有關個人資料保護之隱私權；其二，會員國不得以上述之相關保護規定爲由，限制或禁止會員國間之資料自由流通，也因爲是立法上的最終目的，故也分別成爲本指令之第一條的第一、二款。

2. 規範內涵

在歐洲聯盟，不論是「條約」這種主要的歐體法源，或是「指令」、「規章」等等的次要法源均爲歐盟決策過程[48]中政治妥協下的產物，如「個人資料保護指令」中，便涉及了資訊隱私與資訊自由流通之緊張關係，各會員國間側重之方向不一，也有各自不同之利益，加上各壓力團體之遊說，故本指令實有許多需要折衷之處，故在其指令的前文中，便分別加以釐清。也因爲需妥協之處繁多，故前文中共羅列有 72 點要點，可謂相當繁多。

「個人資料保護指令」之內容共分爲七章，第一章總論中就本指令的目的（第一條）、定義（第二條）、範圍（第三條）與會員國國內法之適用（第四條）加以規範。在此，值得注意的是「個人資料保護指令」與前述歐洲理事會「個人資料保護公約」在適用範圍上有所不同，蓋歐盟「個人資料保護指令」中，除了保護「個人資料保護公約」所敘及的「自動化」所處理之個人資料外，並兼及以「部分自動化及非自動化方式處理之個人資料」，惟人工處理部份，則僅限於結

[47] 論者也有謂主導歐洲統合的法德二國對於個人資料保護之規範的影響，乃是爲了更加速內部市場之統一。See John C. O'Quinn, BOOK NOTE: *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (By Peter P. Swire & Robert E. Litan), 12 Harv. J. Law & Tec 683, summer, 1999.

[48] See Helen Wallace and William Wallace, *Policy-Making in the European Union, fourth edition*, Oxford University Press, 2000, Chapter II, The Policy Process, pp.39-64.

構化之建檔系統[49]。另外，於範圍部分應注意者，因爲本指令爲一政治妥協文件，故觸及國家敏感部分範圍者，並不適用，即「爲共同體法律範圍以外之活動者」（第三條第二項第一款）非爲本指令適用範圍，而「自然人單純爲個人或家計活動者」，也不適用；第二章（第五至第廿一條）則確立了其個人資料保護之基本原則，爲本指令核心，詳參以下敘述。

第三章（第廿二至第廿四條）則規範個人得向該會員國司法機關提起訴訟之法律救濟，且會員國應先有法律救濟之相關措施（第廿二條）、損害賠償（第廿三條）及罰則（第廿四條）等等；第四章（第廿五至第廿六條）規範個人資料向第三國傳遞之原則（第廿五條）與例外規定（第廿六條），原則上個人資料向第三國傳遞，僅限於該第三國具有相當於本指令之對個人資料保護之水準，至於水準是否相當，則須依據整體狀況加以評估，特別是應該要考量資料之性質、目的及持續處理之時間、來源國及最終目的國、該第三國之法律規範及專門之保護措施等等[50]。例外於當事人明示同意、爲契約履行所必須而有利於當事人、增進重大公共利益、維護當事人重大利益所必須、登記處依法所爲等等，於有相當條件之保護措施之下，亦可傳遞。

第五章（第廿七條）爲相關管理規則之規範，第六章（第廿八至第三十條）爲個人資料權益保護之主管機關及工作小組，規定各會員國應有一主管個人資料保護之機關（第廿八條），並且歐盟應有一關於個人資料處理之個人權益保護工作小組，此即「第二十九條資料保護工作小組（Article 29 data Protection Working Group）」。至於該工作小組之職權及義務，則規範於第三十條內。本指令最末章爲關於共同體之施行措施（第三十一條），即執委會與該指令之諮詢委員會的相

[49] 參「個人資料保護指令」前言第二十七項。

[50] 歐盟對外之貿易等契約因此可享受資料保護指令之下的歐洲當局完整保護。See Michael W. Heydrich, *A brave new world: complying with the European Union directive on personal privacy through the power of contract*, 25 Brooklyn J. Int'l L. 407, 1999.另外，個人資料向第三國傳遞之契約範例詳參：URL: http://europa.eu.int/comm/internal_market/en/dataprot/modelcontracts/index.htm。

互關係；指令最末則有附則（第三十二條至第三十四條），規範指令之技術性事宜。

（二）　所確立之原則

「個人資料保護指令」所建構之基本原則爲往後共同體相關議題處理時的基本指導原則，而此等原則因爲有相當程度之保護作用，故常被其他區域組織或國家加以仿效，往往成爲國際間關於個人資料保護之「範本」，以下便分別敘述之：

1. 資料品質原則（data quality）

「個人資料保護指令」要求各會員國必須立法規範關於個人資料之原則（第六條），如：公平及合法地處理、以特定、明確且合法之目的蒐集，且不得以該等目的以外之目的處理、其處理必須適當、相關聯且不超越目的範圍、該等資料必須確保正確且隨時更新，以及以該個人資料所有人允許之形式保存。各該子原則與歐洲理事會之「個人資料保護公約」的第五條大致相同，茲不贅述。

2. 資料處理之正當性原則（criteria for making data processing legitimate）

個人資料必須於特定條件下始得合法地被處理（第七條），包括：資料當事人之明確同意、爲履行契約之需要（基於契約或契約前之關係）、爲履行法定義務、爲保護個人之重大利益、爲維護公益、爲資料保管人或爲第三人（資料收受人）合法權益之所需。惟，若違反本指令第一條第一款，危害當事人基本人權及自由者，則爲不可。

3. 特種資料處理原則（special categories of data）

本指令規定（第八條）有關種族血緣、政治意向、宗教或哲學信仰、商會會員、健康或性生活等皆屬於敏感資料，原則上禁止處理，與歐洲理事會「個人

資料保護公約」的第六條大致相同。

惟，特種資料之處理原則亦有例外[51]，如：

A. 當事人明示同意（第八條第二項 a 款）者，但會員國得以該國法律排除之[52]。

B. 與公共利益有關（第八條第二項 b 款）或與當事人利益有關（第八條第二項 c 款）者。

C. 涉及特種非營利性組織，如基金會、協會等，基於政治、哲學、宗教或商會目的之法定活動之會員事項（第八條第二項 d 款）者。

D. 相關資料已顯然公開，或爲成立行使或防禦其法律上之主張所必要（第八條第二項 e 款）者。

E. 與健康及醫療資料有關（第八條第三項）者。

F. 涉及重大公共利益（第八條第四項）者。

另外，對於刑事或保安措施等敏感性較高之個人資料，則限由公務機關控制下進行，然會員國法律若已有相當之保護者，得例外之。並且，會員國也可以擴大範圍至行政罰、民事裁判資料等領域，亦需要由公務機關加以監控（第八條第五項）。而爲了平衡隱私權與表現自由原則之間的衝突，於第九條中亦明文會員國應制定排除關於新聞目的、文學目的、藝術表現等之資料處理於上述之規範之外。

4. 資料當事人之相關權利（data subject’s right）

[51] 需注意者，下列之例外乃是「特種」資料之例外，而非一般處理原則之例外。關於一般資料處理之例外，爲第十三條（與「個人資料保護公約」第九條相似）相關規範之射程，併此敘明。

[52] 在此也可看出所謂「政治妥協」之影子，常常伴隨著出現在各條文的但書之中，而使得各會員國仍有一定程度之主導力量。

A. 當事人受告知權（information to be given to data subject）

除資料當事人就以下應告知事項已本爲知悉者外，應當告知其：資料保管人及其代表人之身分、資料處理之目的、資料收受者或其類別、所可能發生後果、得享查詢與更正之權利等。於特種資料處理時，並應就該種資料提供更充分之資訊，向資料當事人保證公平處理（第十條）。惟，若所蒐集之資料非爲當事人所提供之時，則適用第十一條之規範。

關於第十一條與第十條之間適用情形之分野，歐盟執委會之研究報告[53]做出下圖 2-2 之區別標準：

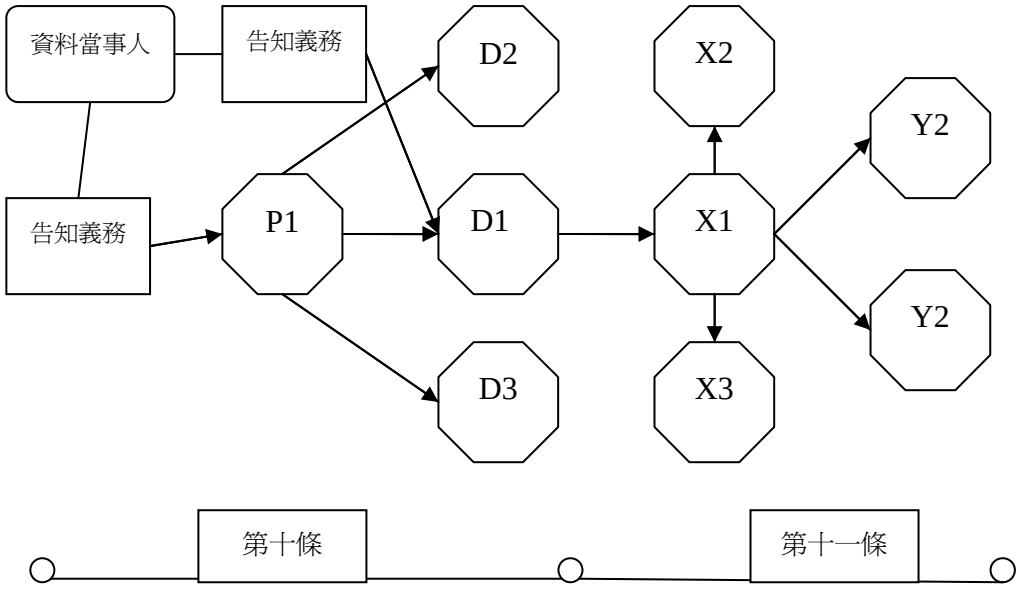
（圖 2-2）「個人資料保護指令」第十條與第十一條之區別：

P= 主要之資料取得者（Primary Obtainer）

D= 第一手接收資料者（First Recipient）

X+Y= 第二手以下之後手接收資料者（Subsequent Recipients）

[53] See Masons Study, Handbook on Cost Effective Compliance with Directive 95/46/EC, Study for Commission of EC (DG XV), 1998/08, pp.45-49.




資料來源：

歐洲聯盟執委會對「個人資料保護指令」研究報告（Directorate General XV ）--Handbook on Cost Effective Compliance with Directive 95/46/EC, P.48.

於上圖中，包括了資料當事人、主要之資料取得者（P）以及第一手之接收資料者（D）等均在第十條之規範範圍之內，而相對的，第二手接收資料者（X）及其後手（Y）以後之後首資料者，則是第十一條之範圍。之所以區分爲此二種不同範圍之實益爲：當適用第十條向資料當事人收集資料時，雖然應告知其相關資訊，但是當告知之資訊當事人已知者，則毋須再行告知；換句話說，此例外只適用於資料當事人、主要之資料取得者（P）以及第一手之接收資料者（D）之間，除此之外的其他獲取或接收個人資料者（即第二手接收資料者（X）及其後手（Y）以後之後首資料者），均無此例外之適用，且需依第十一條「於最遲於初次揭露個人資料前」提供相關應告知事項之資訊。

B. 當事人查詢請求權（right of access to data）

資料當事人於合理期間、無過度延遲與費用之限制之下，得請求查詢以確認資料處理之目的、資料收受者或其類別及資料之類別等，取得之方式並應以當事人得明瞭之方式爲之。

C. 當事人確定及凍結資料權（right to ensure and blocking）

資料當事人於發現處理之資料不符「個人資料保護指令」時，特別當資料不完整或不正確之時，得向資料保管人要求適當更正、刪除或凍結資料（第十二條 b 款）；保管人於爲上述情事之時，並應通知資料當事人（第十二條 c 款）。

D. 當事人異議權（right to object）

異議權包括二方面（第十四條），其一爲依據本指令第七條第五款及第六款之情形處理個人資料時，即基於增進公共利益，或爲執行法令，或爲第三人權益而爲之資料處理之異議權，如當事人有正當理由，得反對處理其特定資料；其二爲資料管理人爲直接行銷目的處理之資料，或爲直接行銷目的，初次傳遞於第三人者，當事人得反對此項目的之利用與傳遞。

E. 當事人拒絕資料自動化處理權（automated individual decisions）

個人有權拒絕僅以自動化之方式，處理個人特定事項之資料，如工作表現、信用、可靠程度、品行等爲評量而作成，對其具有法律效果或重大影響之決定（第十五條）。

5. 資料保管人之相關義務與責任[54]（obligations and duties to the data controller and processor）

A. 資料保密與安全義務（confidentiality and security of processing）

資料保管人及處理人須確保個人資料之隱密性與安全性。在隱密性方面（第

[54] 關於本原則的歸類方法，主要是參考：熊愛卿，前揭文，頁 167-169，筆者另爲細部修正。

十六條），當保管人授與他人代理時，除法律規定外，未經保管人指示，不得處理個人資料；而在安全方面（第十七條），保管人應設置適當技術及組織設施。

B. 登記義務（notification）

於自動化處理個人資料時，資料保管人有義務將資料之處理事項向主管機關登記，登記後主管機關於其處理資料作業開始之前，應檢查並決定該處理作業對資料當事人權利與自由所可能產生之風險，該處理作業並應該公開化（第十八至廿一條）。

C. 損害賠償責任（liability）

資料保管與處理人因非法處理資料，或違反依本指令所規定之國家法規，致生他人損害者，應負損害賠償之責任。惟，其若能證明造成損害非可歸責於其之事由者，免除其全部或部分之責任（第廿三條）。

6. 例外與限制原則（exceptions and restrictions）

此處之例外與限制原則與「個人資料保護公約」第九條之排除原則稍有不同，「個人資料保護公約」第九條包括有：保衛國家安全、公共社會福祉、國家金融利益、防止犯罪行爲之發生、保護資料主體或他人之權利與自由等，然「個人資料保護指令」第十三條 e 款的部分則規範爲「會員國或『歐洲聯盟』之重大經濟或金融利益，包括貨幣、預算及稅捐事務」，即增加保護歐盟之部份，以促進歐洲聯盟之發展。

並且，本原則乃是僅適用於第六條第一款（公平及合法地處理）第十條（當事人受告知權）第十一條第一款（資料蒐集不屬當事人提供者應告知事項）第十二條（當事人查詢請求權）及第二十一條（處理作業之公開化）之部份，前述之特種個人資料並非其範圍。

## 第四節　歐洲理事會與歐洲聯盟對個人資料保護規範之異同

由上節分別對歐洲理事會與歐洲聯盟對於個人資料保護法規範之檢視後，本節將對之做進一步之分析，試圖找尋出該二國際區域組織間對個人資料保護法規範之異同，俾做一比較。在瞭解其共通處後，能使吾人對個人資料保護理論有一更確定性之解釋；而找出相異之點，則不論在實質內容或程序上，均可提供作爲未來台灣修改相關法律時的參考及選擇依據，以明白其利弊得失。

### 一、 相同之處

（一）首先，此二區域組織對於個人資料保護均立有一中心法規範，在歐洲理事會方面即爲 1981 年「個人資料保護公約」；而歐洲聯盟則爲 1995 年「個人資料保護指令」。而由此一中心規範爲出發點，該二區域組織後續對個人資料保護之其他法律基礎，均以其爲架構或核心。

（二）該兩份法律基礎文件均以確立基本的個人資料保護原則爲內容，且在立法形式上，也都是以先確立大方向原則之方式，先架構若干主要原則，再做其他較細部之處理。又，該二文件之基本原則在內涵上大多是相通的，也就是說，有很大一部份之保障條文在個人資料保護之理論上是相通的，而這部分的條文通常是個人資料保護價值的核心所在。

（三）在後續之法規範上均重視個別之領域，而爲專門立法之方式分別處理，但原則上均依循原有中心規範之架構。

（四）由於歐洲理事會與歐洲聯盟有重疊之會員，現有十五個會員國重

疊，於 2004 年後應增爲二十五個，即爲過半數歐洲理事會之會員國均爲歐洲聯盟之成員國，故而對於個人資料保護之觀念相當近似，在立法精神上也有若干相似之處。

## 二、 相異之處

（一）就立法目的言：「個人資料保護公約」之立法目的不外乎對人權、基本自由及對法治之尊重，尤其是隱私權加以尊重以及協調尊重、隱私之基本價值與個人間資訊之自由流通等主要以人權爲出發點之立法；但是在歐洲聯盟的「個人資料保護指令」中除了上述爲保障人權之目的以外，爲了達到歐盟內部市場四大流通之目標，必須要縮減各會員國之法律差異，從而達到內部市場自由流通之目標亦是一項重要之立法目的，整體而言「個人資料保護指令」具備有較大之功能性。

（二）就法規範本質言：「個人資料保護公約」爲一國際性之法律公約文件，需受國際法體系之限制，換句話說，該公約需會員國加入、簽署或經其他相關國內立法之動作後方生效，且可有保留之條款。而歐盟由於歐體法具有直接效力[55]，指令生效後會員國即便不採用其他措施加以履行，對該會員國國民仍直接有效，故「個人資料保護指令」即使會員國怠於執行仍爲直接有效。

[55] 關於歐體法直接效力原則，在 1962 年 *Van Gend en Loos* 案後，即爲通說，該案所代表之直接效力原則略爲：歐體法直接效力不須經由國內法制定確實的法律案履行，因而在會員國及其國民合法關係間產生直接效力。歐體建立了一個新的國際法上的規律，而此新法律上的規律好處在於會員國限制其部分主權，而在此限制的範圍內，其對象包含會員國及其國民，歐體法不只增加個人法律上的義務並且給予個人同等保障其法律上權利，歐體法條文應詮釋爲其產生直接效力並且創設一個國家應保護之個人權利。再如 1990 年 *Andrea Francovich v. Italian Republic* 案中也指出，指令雖授權國家完成立法，但國家不論用何種方式完成指令，立法目的均不可牴觸個人的權利；指令即使因爲國家之怠惰轉換，仍然具有直接效力。

（三）就法體系言：歐洲理事會之「個人資料保護公約」經歐洲理事會會員國同意歐體得加入該公約之 1999 年 6 月 15 日之修正案，故歐體也必須遵守「個人資料保護公約」[56]；但反之歐洲理事會之其他會員國則無遵從「個人資料保護指令」之義務。另外，歐洲理事會同時也開放「個人資料保護公約」供其他非會員國加入，也是較爲特殊之處。

（四）就執行法院言：由上述法體系延伸，「個人資料保護公約」同時爲歐洲人權法院與歐洲法院[57]之判決依據；而「個人資料保護指令」僅爲歐洲法院之判決依據（歐洲人權法院理論上只可將「個人資料保護指令」列爲裁判時之參考文件而類推適用）。

（五）就人權架構言：「個人資料保護公約」之上位法規範爲「歐洲人權公約」，亦即當歐洲人權法院判決時，均以是否違反「歐洲人權公約」（主要是第八條）爲依據；而「歐洲人權公約」本身在第一節所說明之人權架構上，本即爲一專門之人權法律文件，但是「個人資料保護指令」卻是依據歐體條約第二八六條，並非一專門之人權法律文件，所以在歐洲法院判決時常常會另外引用「歐洲人權公約」或「個人資料保護公約」爲依據。

（六）就範圍言：「個人資料保護公約」並不包括人工處理個人資料之情形（第三條第一項）；但是「個人資料保護指令」則包括全部或部分自動化方式處理，以及非自動化方式處理（僅限於結構化之建檔系統）而建立之個人資料，所以在範圍上「個人資料保護

[56] See http://conventions.coe.int/Treaty/EN/searchsig.asp?NT=108&CM=8&DF=。事實上，歐盟國家均爲歐洲理事會成員國，並均加入「個人資料保護公約」，故於 1995 年「個人資料保護指令」通過後，本即有同時遵守二規範之義務。

[57] 歐洲法院於 2000 年尼斯條約中明文以每一會員國出任一法官爲原則，詳細之組織內容參照：王玉葉，＜歐洲法院＞，收錄於黃偉峰主編，中央研究院歐美所，《歐洲聯盟的組織與運作》，台北：五南圖書出版，2003，頁 327-374。

指令」顯然較爲廣泛。

## 第五節　歐洲個人資料保護之執行

### 一、 歐洲理事會之實施

（一）「個人資料保護公約」之相關後續發展

於「個人資料保護公約」之後，歐洲理事會便又數度通過針對不同領域的資料保護之建議，例如：「關於自動化醫療資料庫規則之建議[58]」；「關於科學及統計之個人資料保護之建議[59]」；「關於直銷之個人資料保護之建議[60]」；「關於社會安全之個人資料保護之建議[61]」；「關於警察部門之個人資料保護之建議[62]」；「關於就業之個人資料保護之建議[63]」；「關於薪資及其他作業之個人資料保護之建議案[64]」；「關於公務單位所有之個人資料保護之建議[65]」；「關於電子通訊服務尤其是電話部分個人資料保護之建議[66]」；「關於醫療個人資料保護之建議[67]」；「關於爲統計目的所蒐集與處理之個人資料保護之建議[68]」；「關於網路隱私之個人資料

[58] Recommendation No. R (81) 1 on regulations for automated medical data banks (23 January 1981).
[59] Recommendation No. R (83) 10 on the protection of personal data used for scientific research and statistics (23 September 1983).
[60] Recommendation No. R (85) 20 on the protection of personal data used for the purposes of direct marketing (25 October 1985).
[61] Recommendation No. R (86) 1 on the protection of personal data for social security purposes (23 January 1986)
[62] Recommendation No. R (87) 15 regulating the use of personal data in the police sector (17 September 1987)
[63] Recommendation No. R (89) 2 on the protection of personal data used for employment purposes (18 January 1989)
[64] Recommendation No. R (90) 19 on the protection of personal data used for payment and other operations (13 September 1990)
[65] Recommendation No. R (91) 10 on the communication to third parties of personal data held by public bodies (9 September 1991)
[66] Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services (7 February 1995)
[67] Recommendation No. R (97) 5 on the protection of medical data (13 February 1997)
[68] Recommendation No. R (97) 18 on the protection of personal data collected and processed for

保護之建議[69]」；及最近通過的「爲保險目的所蒐集與處理之個人資料保護之建議[70]」等。

另外，值得重視的一個部分，是 2000 年所召開的歐洲理事會相關會議中，針對「個人資料保護公約」提出了相關之附加議定書的草案[71]（Draft additional Protocol to Convention ETS No. 108 on Supervisory Authorities），並且本草案於 2001 年 11 月 8 日通過成爲正式之條約，即「自動化處理資料個人資料保護公約就主管機關暨跨國資料流通之附加議定書[72]」（Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows,，簡稱「資料跨國流通附加議定書」）。

該附加議定書如其名稱一般，將焦點放在兩方面：其一爲在各簽約國內建立一超然獨立（第一條第二項款）之個人資料保護主管機關（supervisory authority[73]），並賦予該機關調查權及訴訟程序介入權（第一條第二項 b 款），及接受個人資料當事人爲保護其基本人權與自由所提申訴之途徑（第一條第二項 c 款），當事人對該主管機關之決定不符得至該國法院請求救濟（第一條第二項 d 款），且各簽約國之主管機關應依「個人資料保護公約」中第十三條之精神相互合作（第一條第二項 e 款）；其二爲對個人資料跨國傳遞至非簽約國境內（transborder data flows[74]）之相關規範（第二條），其要求簽約國規定個人資料之傳遞予非簽約國或組織時，該非簽約國或組織須能提供相當之保護水準（adequate level of protection）（第二條第一項），並且提出兩種上述規定之例外情形，允許個人資料跨國傳遞與非簽約國或組織，即：簽約國國內法基於維護資料當事人之

---

statistical purposes (30 September 1997)

[69] Recommendation No. R (99) 5 for the protection of privacy on the Internet (23 February 1999)

[70] Recommendation No. R (2002) 9 on the protection of personal data collected and processed for insurance purposes.

[71] 參：熊愛卿，前揭文，頁 142-144。

[72] Opening for signature: 2001/11/08.

[73] 參「資料跨國流通附加議定書」第一條。

[74] 參「資料跨國流通附加議定書」第二條。

特定利益或較具優勢之正當利益，特別是重大公共利益之時（第二條第二項 a 款），或該次傳遞之負責保管人能提供特別是以契約條款約束之安全措施，且該措施已經由有權機關依據國內法認定其適當者（第二條第二項 b 款）之時。

故，歐洲理事會的「個人資料保護公約」實爲歐洲乃至於全世界對個人資料保護影響最早也是影響最深之條約，並且其後之相關建議案及修正，往往具有指標性之影響，而能對其他相關之組織或國家對個人資料保護的相關議題，起一個帶頭性之作用。惟，其仍有缺點存在，例如其缺乏超國家（supranational）之法律架構，監督其對個人資料保護之最低標準之確切執行[75]；並且由於其範圍僅及於透過「自動化」處理之個人資料，因之，其他非自動化處理之部份，便成爲其死角。

（二）實行部份

歐洲理事會關於個人資料保護方面之相關公約由於較早制定，且歐洲理事會本身之成員國數目於歐洲區域亦較歐洲聯盟爲多，故相對的較其他歐洲區域組織在執行個人資料保護方面之執行範圍較爲廣泛。

在各國簽署並批准歐洲理事會的「個人資料保護公約」方面，共有包括阿爾巴尼亞、奧地利、比利時、保加利亞、克羅埃西亞、塞浦路斯、捷克、丹麥、愛沙尼亞、芬蘭、法國、德國、希臘、匈牙利、冰島、愛爾蘭、義大利、拉脫維亞、列支敦士登、立陶宛、盧森堡、馬爾他、荷蘭、挪威、波蘭、葡萄牙、羅馬尼亞、塞爾維亞與蒙地內哥羅（Serbia and Montenegro）、斯洛伐克、斯洛伐尼亞、西班牙、瑞典、瑞士、英國等共三十四國；另外，簽署卻尚未批准之國家分別有：波赫（Bosnia and Herzegovina）、喬治亞、摩達維亞、俄羅斯、土耳其、烏克蘭等國，詳參表 2-1[76]：

[75] David Bainbridge, *EC Data Protection Directive*, London：Butterworths, 1996, p.17.

[76] 由於歐洲理事會成員國包含歐洲聯盟廿五國，故本表扣除之，以避免與歐洲聯盟個人資料保

（表 2-1）：歐洲理事會各國執行「個人資料保護公約」法律架構概況

| 會員國 | 入憲年份 | 特別法存在與否 | 生效年份 | 主管機關 |
|---|---|---|---|---|
| 阿爾巴尼亞 | 1998 | ○ | 1999 | ○ |
| 波赫* | 1995 | ○ | 2001 | ○ |
| 保加利亞 | 1991 | ○ | 2002 | ○ |
| 克羅埃西亞 | 1990 | ○ | 2005 | ○ |
| 塞浦路斯 | 1960 | ○ | 2001 | ○ |
| 捷克 | 1992 | ○ | 2001 | ○ |
| 愛沙尼亞 | 1992 | ○ | 1997 | ○ |
| 喬治亞* | 1995 | ╳ | ╳ | ○ |
| 匈牙利 | 1949 | ○ | 1993 | ○ |
| 冰島 | ╳ | ○ | 2000 | ○ |
| 拉脫維亞 | 1992 | ○ | 2000 | ○ |
| 列支敦士登 | ╳ | ○ | 2002 | ○ |
| 馬爾他 | ╳ | ╳ | 2003 | ╳ |
| 立陶宛 | 1992 | ○ | 2000 | ○ |
| 摩達維亞* | 1994 | ╳ | ╳ | ╳ |
| 挪威 | ╳ | ○ | 2000 | ○ |
| 波蘭 | 1997 | ○ | 1998 | ○ |
| 羅馬尼亞 | 1991 | ○ | 2001 | ○ |
| 俄羅斯* | 1993 | ╳ | ╳ | ╳ |
| 塞爾維亞與蒙地內哥羅 | 1992 | ○ | 1998 | ╳ |
| 斯洛伐克 | 1992 | ○ | 1998 | ○ |
| 斯洛伐尼亞 | 1991 | ○ | 1999 | ○ |
| 瑞士 | 1999 | ○ | 1993 | ○ |
| 土耳其* | 2001 | ╳ | ╳ | ╳ |

作者自繪。本表中，○代表該項目存在，x表示未有規範、未生效或未存在，數字代表生效年代，＊表示該國已簽署但未批准。

護部份重複。

資料來源：歐洲理事會法律事務總署（Directorate General of Legal Affairs – DG I ）（2005/11/22）；URL：http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/National_laws/

由上表中得知，除了部分前蘇聯之加盟共和國與土耳其以及少數歐洲聯盟之會員國（參下表 2-2）之外，大部分歐洲理事會之會員國均已加入或批准「個人資料保護公約」，並大多已生效。另外，由生效日期觀之，大部分國家之生效日期均集中在 1998 年之後，這可能的原因應該是由於歐洲聯盟之「個人資料保護指令」規定會員國須於 1998 年之前完成各會員國之國內立法，而根據歐洲理事會之「個人資料保護公約」第二十二條之規定，有超過五個批准生效後的三個月內，其他各會員國便須相對地對之加以生效；又，歐盟會員國均爲歐洲理事會之會員國，故於 1998 年之後，歐洲理事會之會員國便紛紛對之加以生效了，這也是歐洲聯盟之法律效力影響其他國際公約或其他國家立法之最佳佐證。

## 二、 歐洲聯盟之實施

### （一）「個人資料保護指令」之相關後續發展

承前所述，歐盟的「個人資料保護指令」爲影響整個歐洲聯盟關於個人資料保護基礎來源，其後的許多相關指令均以其爲基礎而加以建構，並且，於其後所新增之歐體條約關於個人資料保護部份，亦多建立於此基礎之上。

首先，在相關指令部分，歐盟通過了數份與個人資料保護息息相關之指令，例如 1997 年的「電信事業個人資料處理及隱私保護指令[77]」（簡稱「電信事業個人資料保護指令」）便是緊接其後而加以規範的。前述之「個人資料保護指令」

[77] Directive 97/66/EC of the European Parliament and of the Council of 15, December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, Directive 97/66/EC, Official Journal L 024, 30/01/1998 P. 0001 – 0008.

並未區隔特定行業規範，亦即適用對象並未限制，然由於在此同時數位技術不斷精進，且已適用於公眾電信網路（public telecommunications networks），有鑑於新型態電信服務對使用者之個人資料及隱私必須特別予以注意，尤其對整合服務數位網路(Integrated Services Digital Network; ISDN)，因此歐盟於 1997 年 12 月 15 日制定了「電信事業個人資料保護指令」，並指出該指令除就「個人資料保護指令」之補充外，並特別保護用戶之合法利益。在「電信事業個人資料保護指令」中，用戶(subscriber)係指與提供公眾電信服務之業者訂約之自然人或法人（第二條 a 款），而使用者(user)則係指爲私人或商業目的使用公眾電信服務之使用者，而未簽訂契約者（第二條 b 款）。本指令特別強調係適用於在共同體內經由公眾電信網路(public telecommunications services)之公眾電信服務相關之個人資料處理，尤其是經由整合服務數位網路(Integrated Services Digital Network, ISDN)及公眾數位行動網路(public digital mobile networks)者（第三條第一項）。

關於「電信事業個人資料保護指令」與「個人資料保護指令」相較，「電信事業個人資料保護指令」所涉及的特殊之議題包括：（1）要求公眾電信服務提供者，且必要時連同公眾電信網路提供者，應採取適當之技術方法防衛其所提供服務之安全，若其網路有特別之危險時，公眾電信服務之提供者必須將危險及可能之損害通知用戶（第四條）；（2）要求各會員國必須確保公眾電信網路及公眾電信服務之通訊秘密(the confidentiality of communications)，特別是國內法規必須禁止除法律允許情形以外之第三者未經相關使用者同意就通訊之監聽、錄音、儲存或其他形式之截取或監視（第五條）。（3）除了爲用戶帳務及互連付費之目的或得用戶同意等例外情形之外，用戶及使用者之關於通話之記錄應於通話結束時即予消除；就分項列舉之帳務記錄，會員國應注意調和發話使用者與受話用戶之權利（第六條、第七條）。（4）對於提供來話顯示之服務而言，必須提供發話之使用者一種免費之方式就個別之通話得除去來話顯示，對受話之用戶亦同（第八條）。（5）會員國必須確保任何一位用戶有權停止來自第三者之通話自動轉接（第

十條）等等[78]。

在「電信事業個人資料保護指令」其後，歐盟最近又有 2002 年的「隱私及電子通訊個人資料保護指令[79]」（簡稱「電子通訊個人資料保護指令」）之通過，依其前言第四點所示，本指令將個人資料保護由前述「電信事業個人資料保護指令」的「電信」（telecommunications）範圍擴大爲「電子通訊」（electronic communications），並明文將前述的「電信事業個人資料保護指令」加以撤銷及取代。其取代之原因爲隨著現今資訊科技之進步，數位行動網路（digital mobile networks）已發展成爲不可或缺的重要生活領域之一（如：手機、衛星電話、行動網路、PDA 等），重要性不亞於前述之傳統電信通訊方式（如：有線電話、有線傳真等），且範圍上亦包括傳統之通訊方式，故加以取代之[80]。其特殊之處在於，其不僅保障自然人之個人資料隱私法益，也同時保障法人之相關法益（第一條第二款）。

於規章（Regulation）方面，則有「共同體機構及部門間個人資料自由流通之規章[81]」（簡稱「共同體機關間資料流通規章」）之出現，其目的乃是爲了落實下述歐體條約第二八六條之相關要求。其範圍並同時包括「個人資料保護指令」與「電信事業個人資料保護指令」兩者，而對共同體轄下之各機關與組織的個人資料相互流通作一規範。

復次，歐洲聯盟於 1997 年訂定阿姆斯特丹條約（Treaty of Amsterdam, ToA）時，亦將個人資料保護由原第二一三之 b 條轉換爲第二八六條，其規定：「自 1999 年 1 月 1 日起，於處理個人之相關資料與自由流通資料時，關於保護個人之共同

[78] 詳參：簡榮宗，前揭文，頁 121-123。

[79] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Directive 2002/58/EC, Official Journal L 201 , 31/07/2002 P. 0037 – 0047.

[80] 關於「電子通訊個人資料保護指令」之詳細內容，詳參本文第三章第三節第二項第二目。

[81] Regulation (EC) 45/2001 of the European Parliament and of the Council of 18. December 2000 on 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, Official Journal L 008, 12/01/2001 P. 0001 – 0022.

體法（指「個人資料保護指令」）適用於由本條約或以本條約爲依據而設立之機關與機構，並且於前述時間內，理事會依第二五一條之程序決議設立一獨立之主管機關，以負責監督之，必要時，並得公佈其他相關規定。」

甚至於最近的重要文件「歐洲聯盟基本權利憲章」（Charter of Fundamental Rights of the European Union[82]）第八條中亦明文規範有對個人資料保護之規定，其曰：「人人均有權享有個人資訊之保護」（第一項）、「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。」（第二項）、「應由獨立之主管機關監督這些原則之確實遵守。」（第三項），均揭櫫「個人資料保護指令」之原則，並將其具體體現於條文之中。

另外，歐盟執委會於 2003 年 5 月 15 日也首此提出了針對「個人資料保護指令」之執行報告（First report on the implementation of the Data Protection, from the Commission），且於 2002 年 9 月 30 日至 10 月 1 日在布魯塞爾舉行關於個人資料保護之論壇與會各國專家學者及相關政府官員紛紛發表論文[83]。

由前述可知，歐洲聯盟對個人資料保護領域之重視已經由傳統「個人資料保護指令」的基礎上，更加以仔細區分各領域之個人資料，而分別加以特別規範。也由此可知，個人資料保護之領域的議題正不斷地擴大及更新，隨著資訊科技的愈加發達與進步，個人資料保護正受到來自各種新領域之侵害，傳統的「個人資料保護指令」除了提供基本原則外，已漸趨不敷使用，因此個人資料保護之研究，也就需要與時並進地隨時對科技發展加以追蹤。

（二）實行部份

按照歐盟「個人資料保護指令」第三十二條之規定，歐盟之會員國應該於

[82] 2000/C 364/01.

[83] See Data Protection Conference, Brussels, 30.9./1.10.2002, at URL: http://europa.eu.int/comm/internal_market/privacy/lawreport/data-conference_en.htm.

該指令通過之日起三年內，依據該指令而訂立相關必要之法律規則以及行政規章施行之，即應當於 1998 年 10 月 25 日時便應已備妥相關法令。惟並非歐盟所有之會員國均遵從此指令所訂之期限，關於歐盟會員國落實「個人資料保護指令」之法制狀況可參下表（表 2-2）：

（表 2-2）：歐盟會員國落實「個人資料保護指令」之法制狀況：

| 會員國 | 相關立法 | 生效及後續 | 關於歐洲理事會「個人資料保護公約」狀況[84] |
|---|---|---|---|
| 奧地利 | 經由 2000 年所執行的「2000 資料保護法案（ Datenschutzgesetz 2000 . DSG-2000）」對本指令加以落實。 | 其後有七個邦紛紛加以立法並加以落實生效。 | 1981 年簽訂，1988 年批准。 |
| 比利時 | 國會於 1998 年通過立法，1999 年公佈於官方公報。 | 於 1999 年並透過網路公開諮詢之方式完成二次修法之草案，於 2001 年 2 月 13 日通過，2001 年 3 月 13 公佈於官方公報，2001 年 9 月 1 日生效。 | 1982 年簽訂，1993 年批准。 |
| 賽浦路斯 | 國會 2001 年通過 The Processing of Personal Data Law。 | 2003 修正案。 | 1986 年簽訂，2002 年批准。 |
| 捷克 | 國會於 2000 年四月通過 Personal Data Protection Act 101。 | 仍有修正案研議中。 | 2000 年簽訂，2001 年批准。 |
| 愛沙尼亞 | 國會於 2003 年 2 月通過 Data Protection Act | 2003 年 10 月生效。 | 2000 年簽訂，2001 年批准。 |
| 丹麥 | 國會於 2000 年 5 月通 | 2000 年 7 月生效。 | 1981 年簽訂，1989 年 |

[84] 當該會員國已執行歐盟 1995 年之「個人資料保護指令」的同時，當然也意味著已經對歐洲理事會的「個人資料保護公約」加以落實。故，本表格不另對落實歐洲理事會的「個人資料保護公約」之日期加以贅述，請參「個人資料保護指令」之生效日期。

| | | | |
|---|---|---|---|
| | 過 Act. No. 429 of 31.05.2000 on processing of personal data。 | | 批准。 |
| 芬蘭 | 於 1999 年 4 月通過 The Finnish Personal Data Act (523/1999)。 | 1999 年 6 月生效。 | 1991 年簽訂 1991 年批准。 |
| 法國 | 僅於 2001 年 7 月完成草案。 | 議會仍討論立法中。 | 1981 年簽訂，1983 年批准。 |
| 德國 | 於 2001 年 3 月方通過聯邦資料保護法 The Federal Data Protection Act (Bundesdatenschutzge-setz)。 | 2001 年 5 月生效。其後大部分的邦均通過資料保護法案[85]。 | 1981 年簽訂，1985 年批准。 |
| 希臘 | 於 1997 年 4 月通過 Law 2472 on the Protection of individuals with regard to the processing of personal data 並生效。 | 1997 年 4 月生效。 | 1983 年簽訂，1995 年批准。 |
| 匈牙利 | 1992 年通過 Act LXIII on the Protection of Personal Data and Public Access to Data of Public Interest。 | × | 1993 年簽訂，1997 年批准。 |
| 愛爾蘭 | 於 1988 年 7 月提出草案（屬出版法之部份）送交國會。2003 年 4 月通過。 | 2003 年 7 月生效。 | 1986 年簽訂，1990 年批准。 |
| 拉脫維亞 | 2002 年通過 Personal Data Protection Law。 | × | 2000 年簽訂 2001 年批准。 |
| 立陶宛 | 2003 年 1 月通過 Law on Legal Protection of Personal Data。 | 2003 年 1 月生效。2004 年 4 月修正案。 | 2000 年簽訂 2001 年批准。 |
| 義大利 | 1996 年 12 月完成立法 Protection of individuals and other subjects with regard to the processing of personal data Act no. 675。 | 2000 年 5 月生效，現正討論該法案之更新。 | 1983 年簽訂，1997 年批准。 |
| 盧森堡 | 2002 年 8 月通過 Act Concerning the Use of | 2002 年 12 月生效。 | 1981 年簽訂，1988 年批准。 |

[85] 除 Sachsen（薩克森）及 Bremen（布來梅）兩邦之外。

| | | | |
|---|---|---|---|
| | Nominal Data in Computer Processing。 | | |
| 馬爾他 | 2001 年通過 Data Protection Act。 | 2002 年修正後逾 2003 年生效。 | 2003 年 2 月簽訂，2003 年 3 月生效。 |
| 荷蘭 | 2000 年 7 月通過 Personal Data Protection Act。 | 2001 年 9 月生效。 | 1988 年簽訂，1993 年批准。 |
| 葡萄牙 | 1998 年 10 月通過'Lei da protecçao de dados pessoais。 | 1998 年 10 月生效。 | 1981 年簽訂，1993 年批准。 |
| 波蘭 | 1997 年通過 Act on the Protection of Personal Data。 | 2004 年修正之。 | 1999 年簽訂，2002 年批准。 |
| 斯洛文尼亞 | 1999 年通過 Personal Data Protection Act。 | 2001 年修正之。 | 1993 年簽訂，1994 年批准。 |
| 斯洛伐克 | 2002 年七月通過 Act No.428 on personal data protection。 | × | 2000 年 4 月簽訂，2000 年 9 月批准。 |
| 西班牙 | 1999 年 12 月通過 Protección de Datos de Carácter Personal。 | 2000 年 1 月生效。 | 1982 年簽訂，1984 年批准。 |
| 瑞典 | 1998 年 4 月與 9 月分別通過指令與規則。 | 1998 年 10 月生效。 | 1981 年簽訂，1982 年批准。 |
| 英國 | 1998 年通過 Data Protection Act 1998。 | 2000 年 3 月生效。 | 1981 年簽訂，1987 年批准。 |

資料來源：

歐盟執委會「內部市場」總署（Internal Market Directorate General of the European Commission）：URL：http://europa.eu.int/comm/internal_market/privacy/law/implementation_en.htm 及歐洲理事會法律事務總署（Directorate General of Legal Affairs – DG I）（2003/3/19）；URL：http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/National_laws

由上表得知真正於期限內將「個人資料保護指令」加以完整落實並通過立法的國家僅有比利時、希臘、葡萄牙、瑞典、義大利等國家，其餘國家均未於期限內完成立法，因此執委會於 1999 年 8 月便行文德國、法國、荷蘭、盧森堡、

英國、愛爾蘭、丹麥、西班牙、奧地利等九國說明遲緩原因[86]，並且於 2000 年 2 月對法國、盧森堡、荷蘭、德國及愛爾蘭於歐洲法院以違反歐體條約第 266 條之規定，提出訴訟[87]。

## 三、 對其他區域之影響

由於歐洲的上述「個人資料保護公約」及「個人資料保護指令」，使得歐洲大部分區域均對個人資料之保護有著相當之重視，然而相對地其他區域在全球化趨勢下的今日，也不得不面臨到一個問題－－其他區域及國家該如何去面對這些立法趨勢對其之影響。

在此一問題的處理之中，必須要先處理到的是歐洲理事會以及歐洲聯盟如何能夠影響到第三國之問題？又受影響最重者如何因應之？另外，台灣之態度又爲何？以下，本節便分別對此三問題作一處理。

首先，爲何歐洲區域關於個人資料保護之行爲會影響到，同時，也必須影響到非歐洲理事會或歐洲聯盟之第三國？關於這方面之問題，最重要之關鍵點便是在資訊快速流通得全球化資訊社會之下，若單只有對內生效之「個人資料保護公約」及「個人資料保護指令」，則透過全球快速的資訊流通－－尤其是藉著高速資訊公路的網際網路之流通，「個人資料保護公約」及「個人資料保護指令」對於個人資料保護之完整保護之意圖及標準將形同具文，也因此，歐盟之「個人資料保護指令」需要去處理到與非歐盟國家之間資料流通之議題。

況且，就另一角度而言，歐洲區域之國家對於電子商務[88]重視之程度並不輸

[86] 其中，芬蘭已於 1999 年 4 月通過，故未對之警告。

[87] IP/00/10, Brussels, 11 Jan. 2000.
（http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/00/10|0|AGED&lg=EN&display=）

[88] 所謂電子商務，係指：經由網際網路媒介，合致完成商品交易、資訊服務、金融匯兌、市場

予其他地區之國家－－尤其是美國。而在美國不斷地大力倡言資訊自由流通之下，由於兩者切入面向不同，歐洲區域顯然地較重視其古老重視人權之傳統，因而對個人資料保護之問題希望架構一完整之法律體系，以促使一般交易者對於電子商務之交易產生信賴感及隱私感，進而使電子商務之交易更爲流暢，故在此觀念之下，個人資料之保護不得不擴張至與歐洲地區交易之第三國，以保護歐洲區域國家之交易者及其相對人，以及可能受此行爲所影響者之權利。

準此，在歐盟「個人資料保護指令」第廿五條中，即規定有個人資料向第三國傳遞之原則，其中第一項規定：會員國應當規定，個人資料在不違依本指令其他規定，而制定之國其他法律之下，僅限於第三國於個人資料之保護，「確有相當於本指令規定之水準時」，方得傳遞至該第三國。並且，歐洲理事會亦加以採納之，故歐洲聯盟及歐洲理事會之會員國，便依此項原則能夠去影響其他第三國與該區域之間之個人資料流通。

其次，歐洲區域組織對於個人資料流通至第三國之規定，衝擊影響最大的自是資料流通量最大的美國。在美國，雖然隱私權在 Samuel D. Warren 以及 Louis D. Brandies 所發表之”The Right to Privacy”於 1980 年代即已獲得大力之倡言，並強調：任何人均有生活之權利（Right to Life），及不受他人干擾之權利（general right of the individual to be let alone），此二種權利在其立論基礎之下乃用以對抗「日益瘋狂與科技化之社會壓力」[89]。然而，在個人資料保護方面的隱私權活動，其保護標準卻遠遠不及歐洲區域之國家，甚至有論者以爲，歐盟資料保護之指令是強加外國文化於美國之企業，而其中部分之強制規定也未必符合當今之科技潮流，並認爲，在既有一個集中式電算主機之世界中或許可以運作順利，然卻不適

情報交換、電信服務、藝文影視節目提供等等商務活動，且其創造空間無限寬廣。關於此定義，詳參馮震宇，網路法基本問題研究（一），台北：學林文化出版，1997，頁 232。

[89] David Brin, *The transparent Society: Will technology force us to choose between privacy or freedom?,* （Addison-Wesley Longman, Inc., 1998）中文翻譯本：蕭美惠譯，《透明社會－個人隱私 vs. 資訊自由》，台北：先覺出版社，1999，頁 112-113。

用於分散處理模式之世界[90]。甚至認爲，限制各人資訊之流通使用，便是對於個人資訊自由之「人權」帶來危害，並將會嚴重影響經濟之發展[91]。但是，美國爲了貿易之利益，終究還是與歐洲聯盟妥協，期望能透過其於 1998 年所提出之「隱私保護國際安全港原則」（International Safe Harbor Privacy Principles），使歐盟認可其保障標準。惟，歐盟加以審視之後並不認爲美國方面所提出的該項標準能夠「令人滿意」，並建議應當加以改進之處。於 1999 及 2000 二度協商之後，於加入相關條件之後，方認可美國對於個人資料保護已達最低之流通標準[92]。

另一方面，對台灣而言，由於過去歷史上不論是受中國帝制時期、日本統治時期乃至於國民黨白色恐怖統治時期，個人之資料均長期的成爲統治者之利器，而此等隱私權之侵害，往往也變成箝制其他權利之手段，例如：於 1950 年代當時台灣省政府僅憑一紙行政命令[93]，即逕行收集役男之個人資料及指紋即爲適例。當 1995 年歐洲聯盟通過「個人資料保護指令」之時，我國政府亦恰巧地於該年（民國八十四年）公佈「電腦處理個人資料保護法」，並保護我國之電腦處理之個人資料，可見個人資料之保護不但在歐洲受到重視，連台灣也察覺到其重要性[94]；就此方面來說，台灣在個人資料保護方面近幾年來所受之重視與發展也可算是相當進步的－－雖然仍有許多有待改進與新危機（例如全民指紋建檔與健保 IC 卡等）的發生。至於台灣方面對之的對應態度，詳參本文第四章，茲不贅述。

---

[90] 參熊愛卿，前揭文，頁 200。

[91] Solving Singleton, Privacy and Human Rights: Comparing the United States to Europe (Dec. 1, 1999), 轉引注自：熊愛卿，前揭書，頁 201。

[92] 關於歐美對於次事件之發展及詳細內容，詳參：熊愛卿，前揭書，頁 200-207。

[93] 民國 45 年 10 月 26 日公布之「徵兵規則」第廿七條，即稱：兵役單位辦理徵兵及及齡男子體格檢查之資料，包含每一部隊檢查之結果及指紋資料等，係爲供體格檢組判定體位之用，縣市政府應予妥爲保存，而司法調查或警察機關得向兵役單位借調歷年徵兵及及齡男子體格檢查之資料，包含每一部隊檢查之結果及指紋資料，以供比對。該條文殘害役男權利甚巨，已於民國 89 年 12 月 27 日修正後刪除。

[94] 我國「電腦處理個人資料保護法」係參照經濟合作開發組織（OECD 揭示的保護個人資料八大原則）所制定。

## 第六節　結語

本章在討論歐洲地區，尤其是在歐洲理事會與歐洲聯盟兩方面個人資料保護之理論時，首先試圖去尋找整個個人資料理論之架構與內涵，發現在歐洲所倡導多時的人權架構下所謂的隱私權保障與個人資料保護之概念早已存在多時，只不過個人資料保護之種子直到最近在歐洲方開花結果。而在這當中，也發生了與人權觀念下資訊自由流通觀念之可能產生的齟齬，但是筆者透過法學甚至是法律社會學之驗證後發現，其實在這兩個人權大架構之下的觀念乃是可以相輔相成的。

在法律基礎方面，首先兩個歐洲組織均先確立一個中心的法規範，亦即「個人資料保護公約」與「個人資料保護指令」二者，之後圍繞著此二中心法規範分別發展出相關之建議或後續性之法律文件，或是以另一種做出定期報告以及成立相關機構專責處理個人資料保護事務；並且，在中心法規範中先確立基本原則之方式，在往後個別之領域中即可以依循著既有之基本原則在針對特殊領域之需求作一「對症下藥」之處理，由於個人資料保護之範圍是有其擴張性與持續發展性的，所以在有了基礎原則後對後續之發展也較能有效地處理。在此研究了中心法規範之後，必須分別處理一些實際上的個別領域問題，在本文第三章中也反映了這種對個別領域之探究也必須從基本之中心法規範出發的模式。

另外，在所確立原則方面，則重心大多擺在保護資料當事人權益方面，並進而衍生諸如資料品質原則、正當性原則等規範資料保管人之原則；另一方面，跨國之傳遞則是另一重點，關係到了國際間對個人資料保護問題之相互態度及處理模式，而歐洲區域組織尤其是歐洲聯盟對此之態度可說是影響全球最為重大

的，不但迫使美國訂立了相關之安全港法規，也迫使欲與這新興貿易體進行貿易或其他互動之國家，需要就此方面與歐盟做出妥協，並進一步使個人資料保護延伸至國際。

於比較歐洲理事會與歐洲聯盟對於個人資料保護之不同規範上，發現了其根本上之相同點在於整個「歐洲」對於人權保障之長遠堅持的理想，而歐盟會員均爲歐洲理事會會員，也使其在於思考邏輯上本即相似，故在兩大體系之個人資料保護規範上有著諸多的相似之處；但是，由於二組織在成立目的上及功能上有所不同，歐洲理事會明顯的較爲鬆散，而爲一般類型的國際組織，其法院或公約依照一般國際法之體系架構爲之，而相對的，歐洲聯盟則有部分新功能主義之嘗試，其整合之過程已跳脫一般國際法或國際組織之體系與概念，故而在對於個人資料保護之內容或程序上，有著明顯的差異。

至於在執行層面，歐洲各國尤其是歐洲聯盟各國大多已在國內有相關之立法，甚至已經入憲，並且在後需相關之立法上也持續分別就相關個別領域之議題做進一步之規範。至於執行面的另一個層次，也就是在實際案例中的判決結果是否均符合個人資料保護前述所歸納之理論與原則，則在下一章中有更進一步之說明與敘述。

# 第三章　歐洲個人資料保護案例研究

## 第一節　概說

個人資料保護就一般基礎理論暨歐洲區域之執行部份，已若前章所述。但是，若要對個人資料保護之整體有一較完整且深入之了解，則必須個別地就不同之領域（sector）加以分別觀察之，此即爲一種以分別領域去探究理論整體之方法（sectoral approach[1]），以符合相關特殊領域之特別要求。但是國內大部分之文獻均只針對本文前章部分，就個人資料保護之基礎總論部分爲一申論，少有就個別領域之資料保護做一較深入而具體之論述者，故筆者本章即擬透過個別案例之分析研究，分別對歐洲區域之醫療資料（medical data）、警察資料（police data）等特種（敏感性）資料之問題，做一討論。另外，對於新興之網路線上個人資料（on-line data），由於關係到未來整個個人資料保護發展之重大變化，且爲使本論文能在未來發展上能夠有一進一步延伸之空間，故將其納入本章第三節加以一併討論。

按，個人資料之分類依法務部「電腦處理個人資料保護法之個人資料之類別[2]」之區分，約可分爲十類：辨識個人者；個人描述；家庭情形；社會情況；教育、技術或其他專業；受僱情形；財務細節；商業資訊；健康與其他（含刑事資料）；其他各類資訊等等，並且各大類別之下，又有細目，分類繁多。爲顧及將歐洲區域之特別領域部分與次章之台灣現狀中最值得重視的兩項議題－－全民健保 IC 卡與全民指紋建檔能加以配合，又限於筆者能力及論文篇幅所限，僅將歐洲理事會之「個人資料保護公約」與歐洲聯盟之「個人資料保護指令」

[1] Explanatory Memorandum of recommendation No. R (87) 15 regulating the use of personal data in the police sector, 17 September 1987, p.1 sec. 2.

[2] 參：法務部，「電腦處理個人資料保護法之個人資料之類別」。

均認爲特別敏感資料，而應受特別保護之個人醫療資料及警察資料兩類特別之領域，另加入新興科技下之個人線上資料保護之領域，以案例研究之方式敘述，以符合未來之潮流，合先敘明。

又由於歐洲聯盟之「個人資料保護指令」乃於 1995 年方公布之，故相關案例於歐洲法院發生者本即甚少，且大多爲關於基本原則之案例，如執委會控告各會員國怠於執行 1995「個人資料保護指令」之案例（例如 *Commission of the EC v. Grand Duchy of Luxembourg*, Case C-450/00），或是關於涉及商業利益之個人資料保護訴訟（例如 *Adidas AG Case*, Case C-223/98）等，所以以下所敘述之判決部分，主要是以歐洲人權法院之相關判決爲中心，併此敘明。

## 第二節　個人醫療資料

### 一、 概說

凡人均有生老病死，而不論是生、老、病、死中的任一樣情事均會接觸到健康及衛生單位，故而在出生的那一刻起，個人資料也均會在該健康及衛生單位加以儲存紀錄－－不論該種單位是國營的或私營的；是大型的教學醫院、區域醫院乃至於地區醫院或小診所，均會對個人之病歷或醫療資料加以儲存，並相當地有可能會加以流通，或進而匯整成一種或多種之資訊，並加以形成一統計之數據。

並且，由於此種醫療個人資料[3]通常是最貼近一般個人之身體的，又是一種必須且不可能排除其存在之個人資料，且其通常最能代表一人之身心理狀況，故而個人之醫療資料無疑的在大部份之情形下是一種相當敏感而需要受到

[3] 醫療個人資料一般而言，指包括在醫療實踐之過程中由病人被動或主動提供，以及由醫療專業團體依醫學知識主動生產，與病人個人有關之相關資料。

保護之個人資料種類。也因此，不論是歐洲區域的各種資料保護法令，或是美國[4]、台灣甚至是只要有個人資料保護相關法令之規範，均會將其納入敏感性個人資料之範圍中，因爲，無論是該資料當事人之疾病如 HIV[5]、其他種類之性傳染病、遺傳疾病、心理疾病，或是最近流行之嚴重急性呼吸道症候群[6]，甚至是個人的基因資料（Genetic data）或是其他之長、短期病史，均有可能會影響該個人之就學、就業、信用、保險等方面之待遇，故而不論何種醫療資料，均爲相當具有特殊性之敏感個人資料，而須特別受到重視。

個人醫療資料除了會被儲存之外，該種資料之複製、流通、更新與刪除也是需要被討論之議題。該等資料之流程可能是經過多手而複雜的，例如有學者提出如下（圖 3-1）之標準醫療資料流通模式[7]，吾人將之移用，以爲理解個人醫療資料之高度散佈可能性之所用。

（圖 3-1）：標準醫療資料流通模式[8]：

[4] 關於美國的個人醫療法令與相關研究理論，可參考：Paul M. Schwartz, and Joel R. Reidenberg , *Data Privacy Law*, Virginia: MICHIE Law Publishers, 1996, pp.153-203.

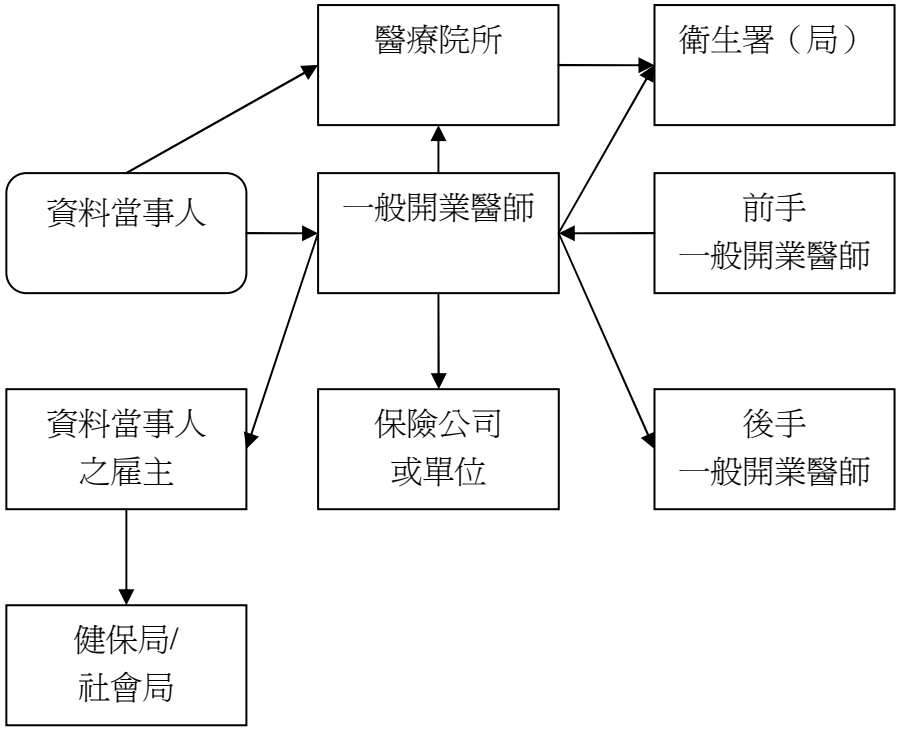
[5] 愛滋病毒(HIV)是一種能夠破壞人體免疫系統的病毒，全名爲人類免疫力缺乏病毒，英文名爲 Human Immunodeficiency Virus，簡稱 HIV，與愛滋病（Acquired Immunodeficiency Syndrome ,AIDS，後天免疫缺乏症候群）並非等同。

[6] Severe acute respiratory syndrome (SARS)爲 2003 年來台灣所遭受之最重大突發傳染性疾病，由於其傳染途徑尚未確定，只知乃是主要經由飛沫傳染或直接接觸患者體液傳染，因而造成一般民眾恐慌，深怕一遇見帶原者即遭感染，故而人口一罩。若此時該病例之個人資料一經外洩，即被視爲瘟神一般，迭遭歧視，故此等個人資料乃是最具有敏感性質的。關於 SARS 之資訊，詳參中華民國行政院衛生署疾病管制局 SARS 資訊網站：http://www.cdc.gov.tw/sars/（2003/5/20）。

另外，關於急性傳染病之防止是否即一定符合社會重大公益而應爲優先之處理，則尚須討論，詳見本節下述。

[7] See David Bainbridge, *op. cit.*, pp.170-172.

[8] 原資料圖表以英國之政府單位爲主，爲適應台灣情狀筆者將部份翻譯爲切合台灣現狀之名詞，請查照。




資料來源：David Bainbridge, *EC Data Protection Directive*,（London：Butterworths, 1996）, p.171, Figure 8.1: data flows- health care.

在該流程圖中，吾人可觀察出若資料當事人發生轉診及新病史發生，或原有疾病已痊癒之時，個人之醫療資料便需要加以更動改變，發生前後手開業醫師之個人醫療資料流動，則該特種之資料便必須依照個人資料保護之基本原則去加以保護，否則，可能會發生之後果並不一定會比被儲存該等資料來的輕微。試想，當個人醫療資料未被及時更新而轉診至他衛生單位時，則醫護人員誤判斷該病徵之機率便會大大增加；而當該病症已痊癒，卻又未被及時更新之時，該資料當事人之投保公司（單位）卻可能仍沿用該舊資料加以超收超額之保險費用，甚至拒絕保險[9]；另外，若該等資料經開業醫師手中經雇主之手輾轉流入健保局或社會局手中，導致一些當事人所可能不希望發生之「關切」也足以招

[9] See: Paul M. Schwartz, , and Joel. R. Reidenberg, , *Data Privacy Law*, Virginia: MICHIE Law Publishers, 1996, pp.155-165.

致該當事人之困擾；又該個人資料任意流通，則可能會使該資料當事人之隱私權遭受侵害，例如曾有性病之病史，縱使已經治癒，但一旦該等個人資料遭受散佈，則對該資料當事人之隱私權即可能有重大之傷害。凡此種種，均可驗證出該個人之病歷資料均須遵守嚴格之保護原則與規範，方爲妥適而不違背人權保護及隱私權保護之觀念。

另需說明的一點，本文以下均以個人「醫療」資料（medical data）涵蓋如基因資料（genetic data）、健康資料（health data）、病歷資料（disease history data）及其他相關之屬於醫療領域之個人資料，作爲一概括性之統稱。

準此，本節依上述概念，即先對歐洲區域組織之個人醫療資料保護之法律基礎先加以說明，隨之以歐洲重要法院之一的歐洲人權法院之判決結果加以佐證，以加強法實證之基礎，對醫療個人資料之保護理論做一論述。

## 二、 法律基礎

### （一） 歐洲理事會

於歐洲區域組織的歐洲理事會部份，有關個人資料保護最基礎之法律文件自然爲前章所述之「個人資料保護公約」，而其中所延伸之建議文件（Recommendation）中，專門關於醫療資料之保護者，爲 1981 年之「關於自動化醫療資料庫規則之建議[10]」與 1997 年之「關於醫療個人資料保護之建議[11]」（下均簡稱：醫療個人資料保護建議）二者。但是由於該 1981 年之「關於自動化醫療資料庫之建議」年代稍嫌久遠，並且已不符合現今將個人資料予以電子

[10] Recommendation No. R (81) 1 on regulations for automated medical data banks (23 January 1981). Adopted by the Committee of Ministers on 23 January 1981, at the 328th meeting of the Ministers' Deputies.

[11] Recommendation No. R (97) 5 on the protection of medical data (13 February 1997). Adopted by the Committee of Ministers on 13 February 1997, at the 584th meeting of the Ministers' Deputies.

化處理之趨勢與要求，故而歐洲理事會後來於 1997 年即研擬「關於醫療個人資料保護之建議」對之加以取代，俾符合醫療科學及資訊技術之發展與進步，並使會員國能夠確保尤其是包含隱私權在內的個人基本自由與權利，故在此本文對關於「自動化醫療資料庫規則之建議」之內容即不再敘述。

就結構及內涵言，該 1997 年「醫療個人資料保護建議」共分爲十二部份，第一部份爲對「個人資料」、「醫療資料」、「基因資料」之定義。其中重要者，乃係定義「醫療資料」爲有關個人健康之所有資料，而「基因資料」則是個人遺傳性徵或有關係之一群人的相關遺傳性徵之資料，並包含所有有關該個人之健康或疾病之基因資訊及基因鏈[12]（genetic line）；第二部份係範圍之確定，將其限制於電腦自動化處理醫療資訊之範圍內，惟會員國可自行將其擴張至非自動化處理之範圍；第三部份係宣示隱私權之尊重；第四部份則是醫療資料之蒐集與處理，原則上應直接由資料當事人取得，例外如有重大公共利益或另有特別法規定者，不在此限。另外，基因資料則僅限於預防性治療診斷，或爲科學研究之需要而蒐集或處理。又本建議亦對未出生之胎兒爲資料之保護，乃是一相當進步之立法例；第五部份係資料當事人資訊之告知，如個人醫療資料之存在、使用目的、存於何處、由誰負責管理、如何取得、得否拒絕存取等。在此特別值得注意的一個重點是，於基因資料部份，需告知該當事人可能有無法預料而超出預期之發現。另外，關於無行爲能力人，則由法定代理人依該無行爲能力人之最佳利益爲之。

該建議第六部分爲資料當事人之同意，應於自由狀況下而爲表意；第七部份爲關於個人醫療資料之流通之禁止原則，例外於該資料爲顯而易之者、依法得流通者（如基於重大公益或保護他人重大利益）、國家因怠於立法而未保護該資料當事人利益，或依比例原則得流通者，不在此限；第八部份乃資料當事

[12] 基因鏈於本文件中，係指由兩人或兩人以上之個人所生殖或分享所產生之基因相似之結果，所組成之鏈結（See Art.1）。

人之權利，如獲取該資料之權或更正權等，原則上均須准許之，例外如公益大於私益、知之則對其健康有嚴重損害、該筆資料含他人之資料，或其基因資料會損及父系或母系或其他相關之人、或用於統計或科學研究，而不致損及個人隱私，或非針對特定之個人者，不在此限；第九部份是資料安全之維護，如需提供適當之組織機關或技術加以維護之，並且此一部份之條文也提供了一些需定期檢視之方法[13]；第十部份爲資料管理之相關原則；第十一部份係料傳遞（至第三國）；該第十二部份爲利用個人醫療資料之科學研發，應以匿名爲原則。

綜觀上述法規之架構可以發現，其大體上主要是依循「個人資料保護公約」之架構，而在有關於醫療資料方面之特點另外爲特別之規範，相當符合其以分別領域去探究理論整體之方法，以符合相關特殊領域特別要求之觀念。

而歐洲理事會在專門關於「基因資料」的研究與對於其個人資料保護方面，另外有「關於生物與醫學方面保障人權與人性尊嚴公約：人權暨生物醫學公約[14]」（以下簡稱「人權暨生物醫學公約」），其前言特別提到立法精神之一即爲「個人資料保護公約」其第十條便明言保障個人對於其健康狀態之隱私生活與知的權利（private life and right to information），並在其第五章關於生物醫學的科學研究中，對於個人資料保護與個人人性尊嚴加以規範：對於個人基因資料之研究行爲，例如蒐集與分析等，除了需依一般個人資料保護原則，經當事人明確同意之外（第十六條），「人權暨生物醫學公約」第十七條也規定當事人如無行爲能力足以行使同意權時，則必須於所期待之研究成果對於當事人健康有事實上與直接之助益方得爲之（第十七條第一項），如無如上之「有事實上與直接之助益」要件時，則必須在最後就成果將有助於獲得人類疾病或障礙之資

[13] 如進入個人資料存取設備之控制（ See Art. 9.2.a）、資料媒體之控制（ See Art. 9.2.b）、記憶體之控制（ See Art. 9.2.c）、利用該等資料之控制（ See Art. 9.2.d）、取得之控制（ See Art. 9.2.e）、流通之控制（ See Art. 9.2.f）、資料前手之控制（ See Art. 9.2.g）、資料傳遞之控制（ See Art. 9.2.h）、及獲取該資料之控制（ See Art. 9.2.i）等。

[14] Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, adopted at Oviedo on 4 April 1997.

訊，且該資訊可能對於當事人或其他同年齡層罹患相同疾病或障礙者，及處於相同狀況之人有益者（第十七條第一項第一款），或是該研究對於當事人造成的結果是最小風險與最小負擔[15]（第十七條第二項第二款）之時，方得爲之。

（二） 歐洲聯盟

歐盟對於個人醫療資料保護有別於上述歐洲理事會之做法，其並無專門之建議或準則對之加以特別規範，僅於 1995 年之「個人資料保護指令」做一總則性之規定。其於前言（立法目的）中的第三十四項與第四十二項中，則有特別針對健康及醫療資料之領域分別加以敘述。

其中，第三十四項係爲規範關於個人敏感性資料之立法目的，乃謂「依重要公共利益之合理需要，應授權會員國放寬敏感性資料類別禁止處理之規定。公共利益之合理重要理由，包括：『公共衛生』及社會保護，特別在健康保險制度請求給付及服務程序方面，爲保證其品質及成本效益之所需、學術研究及政府統計之所需；爲保障基本權利與個人隱私，提供特定適當保護措施者」。由此點得知，個人之醫療資料如有涉公共利益者，即有可能成爲敏感性個人資料受到特別保護之例外，亦即如於公共利益之合理需要範圍內，可於公共健康方面有限度地放寬規定。

---

[15] 「人權暨生物醫學公約」第十七條第二項原文爲：

Exceptionally and under the protective conditions prescribed by law, where the research has not the potential to produce results of direct benefit to the health of the person concerned, such research may be authorised subject to the conditions laid down in paragraph 1, sub-paragraphs i, iii, iv and v above, and to the following additional conditions:

i. the research has the aim of contributing, through significant improvement in the scientific understanding of the individual's condition, disease or disorder, to the ultimate attainment of results capable of conferring benefit to the person concerned or to other persons in the same age category or afflicted with the same disease or disorder or having the same condition;

ii. the research entails only minimal risk and minimal burden for the individual concerned.

，惟學者李震山教授對於「該研究對於當事人造成的結果是最小風險與最小負擔」此一要件，認爲乃是與「有事實上與直接之助益」並列的對於當事人如無行爲能力足以行使同意權時，而例外能對之進行研究之要件之一，似乎誤認該要件爲「人權暨生物醫學公約」第十七條第一項之內涵，事實上該要件爲該條第二項第二款，併此敘明。參：李震山，＜論個人資料保護－以人體基因資訊爲例＞，《月旦法學雜誌》，台北：元照出版，第 75 期，2001 年 8 月，頁 19。

次之，第四十二項爲「會員國得爲當事人之利益，或爲保障第三人之權利與自由，限制當事人查詢權利與資訊。例如：查詢醫療資料（medical data），得規定應僅限由醫療專業者爲之」此亦爲關於個人醫療資料保護之一項例外情形，與上述不同者，此項規定專爲保護當事人或第三人利益，與上述保護公共利益之射程範圍有所不同。

另，「個人資料保護指令」於第八條關於特種資料禁止處理原則中，第一項規定：「凡揭示…個人醫療或性生活之資料，會員國原則上應禁止處理之」，故可由此得知歐盟將其列入敏感的特種資料中，予以特別之保障。但是該等醫療個人之特種資料仍有例外情形不適用上述之規定，而仍得處理之者，如：於資料當事人明示同意處理其醫療資料、當事人病重已不能爲意思表示時，爲保護該當事人或第三人之重大立即之利益、爲預防醫療、診斷之目的與看護或治療或醫療服務管理之規定所要求資料之處理，以及由醫療事業依國家法律或國家主管機關訂定之規則遵守專門職業保密規定，或由第三人遵守同等保密義務而爲資料處理者。不過在處理上述例外情況之時，仍應特別注意個人資料之保護並非符合上述例外規定即可任意地加以處理流通，因爲即使是已非特種資料限制之範圍內之資料，也依然有可能會有其他方面之利益（比如說商業上之利益，像是該等資料遭直銷藥品商之不當使用之情形），若隨意處理之仍會使該資料當事人之權利受侵害。

值得特別注意的一點是，於該指令第十八條之登記義務中規定，會員國應規定資料保管人或其代表有向主管機關登記之義務。其中的例外情形（第十八條第二項第二款）之一，謂「保管人依循其國家授權之法律，得任命一爲資料保護『專員[16]』（官員）專門負責（特定事項）」者，於對資料當事人之權利與

[16] 該原文爲"officer"一詞，國內翻譯大多翻成「官員」（參：熊愛卿、詹文凱合譯：歐盟 1995 年資料保護指令，收錄於熊愛卿前揭博士論文附錄）或「資料保護人」（參：何金鍾編譯，歐洲資料保護綱領，台北：財團法人金融聯合徵信中心，1997 年 6 月，頁 62。），但是管見以爲，當個人資料之保管人爲私人部門時，則翻譯爲「官員」似有未妥，蓋「官員」一詞多用於政府之公部門，於此處例如該保管者爲私人醫療院所時，則似應譯爲「專員」，意即對

自由不致有負面影響之情形之下，得簡化或免除登記。此點於醫療資料流程中（圖 3-1），除非該等資料保管人是大型之醫療院所、保險公司或政府相關單位，否則可能會無能力指定一專門人員處理此事，則政府之對口單位則會因此缺乏經驗而不能完整照顧到此一需求，實際案例中歐盟之德國即爲適例[17]，是本指令可能有不足的地方。

## 三、 案例研析

本小節主要以歐洲理事會所轄之歐洲人權法院[18]，對於個人醫療資料方面相關之判決做出回顧，並加以整理出一些規則，以檢視其是否對相關之法律基礎有所呼應，甚或作出更進一步之解釋，以彌補上述相關法律基礎之不足之處。

歐洲人權法院主要乃是依據該案例事實有無違背「歐洲人權公約」而爲判決之依歸，故而在裁判上均以「歐洲人權公約」之違背與否爲主要論點，佐以其他相關之歐洲理事會法令規範加以裁判，所以下列有關個人醫療資料之判決大多以是否違背「歐洲人權公約」之第八條爲主，而以「個人資料保護公約」爲輔。因此，在作本章以下分別對歐洲人權法院判決分析之論述前，有必要先針對「歐洲人權公約」第八條之內涵加以論述。

「歐洲人權公約」第八條爲保障隱私及家庭生活之條款，該條第一項規範：「人人均有於其隱私及家庭生活與通信方面受到尊重之權利」，上述原則之例外則規定於第二項中。歐洲人權法院常以是否符合下列三要件，作爲是否構成第八條第二項要件之判斷依據[19]：

---

此事項專門處理之代表人爲妥，至於「資料保護人」則語意不清，亦未見妥適。

[17] See David Bainbridge, *op. cit.*, p.173.

[18] 關於歐洲法院之相關個人醫療資料案例並未發生，故未能一併敘述。

[19] See European Court of Human Rights, M.S. v. Sweden, Judgment of 27 August 1997, *Reports of Judgments and Decisions* 1997.

1. 需有法律依據。其下又有兩項標準，分別爲是否有法律基礎及是否有可預見性。

2. 合法之目的性。公約列舉有：爲國家安全、公共安全、國家經濟之健全、防止犯罪及違反國家秩序、保障身心健康及保障他人之權利與自由之利益等。

3. 需爲民主社會之所需（necessary in a democratic society）。

依上述對於「歐洲人權公約」第八條之闡釋，歐洲人權法院關於個人醫療資料保護之相關判決歸納出一些原則及例外，就與「個人資料保護公約」言均有所切合。

首先，在直接肯定個人醫療資料保護原則方面，歐洲人權法院對於該等資料之資料當事人之相關權利予以正面之肯定，並以相當積極之態度加以確保資料當事人有相關權利，例如在 *M.G v. The United Kingdom*[20] 案中，歐洲人權法院即認爲當事人有當事人接近資料權（right of access to data）而判決英國政府敗訴。

於該案例中，案例事實爲 Mr. M.G.兒時因爲其母親患有精神方面之疾病，而父親則與家中之小孩有相處上之困難，甚至有虐待兒童之況出現，因此 Mr. M.G.分別於五段時期受到國家社會服務單位之照顧，並製作相關之社會服務及醫療紀錄。在 Mr. M.G.長大後，向該社會服務機構要求該等資料，希望得知其小時後是否有被父親不當對待（ill-treatment）及其父親是否有虐童之刑事資料，但社會服務單位卻拒絕提供完整之資料，而採提供其認爲「已足夠」之個人相關醫療與社會福利資料而已，且認爲於個人資料保護相關法規立法完成前所製作之個人資料，並不在個人資料相關法規之規範範圍之內，因此 Mr. M.G.向歐

[20] See European Court of Human Rights, M.G v. The United Kingdom, Judgment of 24 September 2002, *Reports of Judgments and Decisions* 2002.

洲人權法院提出訴訟。該案件爭點爲個人能否完整的得到其個人之資料，以及於個人資料保護相關法規立法完成前所製作之個人資料是否亦受到規範。

歐洲人權法院對此認爲：資料現仍存於政府機關之中，即應受相關個人資料保護法規之規範，不論其原始之紀錄時點爲法規生效之前或之後；又，相關政府單位應有積極之義務，提供完整而無遺漏之當事人所要求之個人資料，而並非由該單位決定提供資料之多寡，故而歐洲人權法院判決英國違反「歐洲人權公約」第八條[21]。

至於在以反面判決該案例是否爲個人資料保護之例外方面，歐洲人權法院大多以公益大於私益爲理由，對個人資料保護之特種資料處理原則（special categories of data）加以排除。例如在 *M. S. v. Sweden*[22]案中歐洲人權法院即以此種公益大於私益之排除法則，對資料品質原則（Quality of data）加以排除。

在 *M. S. v. Sweden* 案中，案例事實是 Ms. M. S.本來即患有椎關節粘連[23]（Spondylolisthesis）之疾病，而造長久性背痛，故其之前即有看過醫生。後來，有了一份工作之後，Ms. M. S.背痛舊疾復發又去看了醫生，再向社會保險局（Social Insurance Office, Försäkringskassan）依該國職業傷害賠償法（Industrial Injury Insurance Act, Lagen om arbetsskadeförsäkring）申請職業災害補助（理由爲因其教師之工作長久坐於椅上而造成背痛），社會保險局則向該醫院所屬醫師索取 Ms. M. S 之醫療資料，以進行查核。但是，查核後發現 Ms. M. S.並非是因爲工作而受職業傷害，故駁回其申請。Ms. M. S.則向歐洲人權法院提出訴訟，認爲該醫師及所屬醫院未經 Ms. M. S.同意，而隨意洩漏個人醫療資料予社會保險局。該案件之爭點爲：爲了公益（避免職業傷害賠償之浮濫）所需，是否個

[21] 於 *M.G v. The United Kingdom* 案中，判決另指出之類似案例爲 Gaskin v. the United Kingdom, 7 July 1989（Series A no. 160）and Martin v. the United Kingdom, 28 February 1996（Application no. 27533/95）兩案。

[22] See European Court of Human Rights, M.S. v. Sweden, Judgment of 27 August 1997, *Reports of Judgments and Decisions* 1997-IV.

[23] 乃一脊椎與骨椎間關節之退化性疾病，多見於頸椎或腰椎。

人醫療資料可在公共機關之間互相流通，而不必有資料當事人之明示同意。

歐洲人權法院對此認爲，就「歐洲人權公約」第八條第二項言，瑞典政府社會保險局之行爲：

1. 有法律依據。其下兩項標準，分別爲是否有法律基礎及是否有可預見性均有所符合。

2. 合法之目的性存在，乃是爲國家經濟之健全之所需（避免職業傷害賠償之浮濫而造成經濟失衡）。

3. 爲民主社會之所需。因爲第一，該醫療資料是由一公家單位轉到另一公家單位，就保管者言均爲政府機關，未發生主體之改變；其次，該查核之行爲乃社會保險局職務之所需，並且爲其義務；第三，此行爲有防止濫用補助之法定目的，故爲民主社會之所需。

故，歐洲人權法院判決瑞典政府不違反「歐洲人權公約」第八條，當然也就不違反相關之個人資料保護規範。

另一個關於當事人得否以訴訟之方式阻止或檢視公共機關間個人醫療資料之傳遞之案例也值得注意，在 *Anne-Marine Andersson v. Sweden*[24]案中，就是有關當事人得否阻止其個人資料傳遞之案例，該案例並可看出排除個人醫療資料保護之另一要件－－爲第三人之利益。在本案中，事實部份係 Mrs. Anne-Marine Andersson 爲一精神疾病患者，瑞典社會局（Social Council, Socialnämnden）爲保護 Mrs. Anne-Marine Andersson 兒子之利益，請診斷 Mrs. Anne-Marine Andersson 之精神科醫師傳遞 Mrs. Anne-Marine Andersson 之個人醫療資料予社會局，而當 Mrs. Anne-Marine Andersson 要求此份資料於公家機關間之傳遞需使其得以訴訟方式阻止之時，卻遭拒絕，故向歐洲人權法院提起訴

[24] See European Court of Human Rights, Anne-Marine Andersson v. Sweden, Judgment of 27 August 1997, *Reports of Judgments and Decisions* 1997-IV.

訟。爭點爲瑞典是否缺乏一供病人於其醫療資料由醫療單位傳遞至社會服務機構前，能得知其病歷，並於該國法院中以訴訟方式阻止（或檢視）其個人資料傳遞之規範，該爭點主要之訴訟標的爲「歐洲人權公約」第六條第一項之公平公開審判權。

歐洲人權法院判決結果認爲該醫生傳遞 Mrs. Anne-Marine Andersson 個人醫療資料與社會局之行爲由於：

1. 有向社會局報告精神疾病患者之義務。

2. 乃係爲了保障第三人（Mrs. Anne-Marine Andersson 之子）之利益。

3. 醫生於疾病之診斷與應如何處理該個人醫療資料有相當廣泛之決定權，係爲其專業之所在，且其並無先與病患溝通後再決定其診斷結果爲何之義務。

所以並無以訴訟方式先行加以審視是否得傳遞予社會局之必要，也未違反「歐洲人權公約」第六條第一項，當然在個人資料保護原則中，得以保護第三人利益爲理由加以排除。

又關於個人醫療資料中性別資料亦包含於健康資料之中，尤其是在精神與心理上之性別認同與身理上之變性手術，爲最敏感之性別資料之一。在 ***Sheffield and Horsham v. the United Kingdom***[25]案中即針對個人之性別資料等關於個人身體健康之醫療資料作出闡明。該事實部份由於是屬於兩案合併（爭點同一），故有兩件事實存在。在 Ms. Sheffield 方面，其出生時本爲男性，已婚，有一女，且有刑事資料，之後因爲長期性別認同障礙之關係，經心理醫生診斷確定其心理上爲女性，故而准許其變性，其後與元配離婚，英國法院法官認該變性人無法提供子女最佳利益，故裁定由其元配扶養女兒。Ms. Sheffield 變性後，其護

[25] See European Court of Human Rights, Sheffield and Horsham v. the United Kingdom, Judgment of 30 July 1998, *Reports* 1998.-V.

照與駕照之性別均已更改，並有改名（first name），但是其他之資料如出生證明及社會與安全警政之資料（含刑事資料）等均未更改，Ms. Sheffield 認爲政府未更動其個人資料之行爲違反英國之個人資料保護法（Data Protection Act 1984）而，向歐洲人權法院提起訴訟；至於 Ms. Horsham 部份，其出生時亦爲男性，爾後與 Ms. Sheffield 同樣理由而變性，且其因爲雖然護照上已經改爲女性，但是其他文件如出生證明等仍維持爲男性，故而無法與其另一男性伴侶於英國結婚，故向歐洲人權法院提起訴訟。由於該二案之爭點均爲國家是否有積極之義務去認知二原告變性之後之新法定性，故合併爲一案共同製作判決。

本案歐洲人權法院認爲，「歐洲人權公約」第八條中的應「尊重」（respect）隱私及家庭生活與通信一詞，定義並非明確，在本案中即出現會員國政府是否應有主動積極之義務，去認知到個人醫療資料或其他相關之資料有無改變之義務，並加以更改之爭議。法院對此認爲，在此處由於該等變性爲特別之新醫療科技之個別案例，非具有一般性，且未具嚴重性而能使國家需要重新認知，且若需一一就個案加以重新認知，則需要相當大之費用與人事成本，況且英國已經盡最大之能力於原告通知更改時，即行更改其護照與駕照上之個人資料，以減低其困擾；又，Ms. Sheffield 主張之一爲希望能於變性後刪除其過去之刑事資料，歐洲人權法院認並無法律依據，所以判定英國無該等認知個人醫療資料改變，進而更動其他種類個人資料之積極義務，故不違反「歐洲人權公約」第八條之規定。

## 四、 小結

由上述論述中，筆者歸納出一些特點，茲臚列如下：

1. 基因資料之重要性：隨著時代之進步，個人基因資料庫有著其相當之進展及必要性存在，但是由於科技之進步如今已是一日千里，故而雖然規範相關科技之法律性文件不斷追趕，但是仍有許多跟不上「時代的腳步」之時。例如，本文件中規範個人基因資料部份常有「無法預期」（unexpected）之文字出現，雖然充滿了不確定性，但是面對科技日新月異之衝擊，尤其在生物科技（biotech）領域等牽涉基因資料之研發中，此種採取較爲預先性之立法例卻也不能避免，但於執行上似仍應有一確切之規範，以符合法律確定性原則爲佳。

2. 對於未出生胎兒及無行爲能力人之保護：該建議中有對該二者爲一定之保護，已堪爲先進之立法例。

3. 範圍侷限於自動化處理之個人醫療資料：歐洲區域性之醫療資料保護文件均未強制性規範其範圍亦包含未經自動化處理之個人醫療資料。雖然電腦已十分普及，但是有許多私人診所所擁有之該等個人資料，因許多理由而尚未完全電子化或自動化處理，卻也以非自動化之方式儲存了貼近人身之個人醫療資料，甚至是基因資料，則該部份之遺漏可能會使部份之資料儲存機構故意遲遲不將其資料加以電子化，反而可能會有礙科技研發及管理上之發展。

4. 歐洲人權法院在對個人醫療資料保護方面，除了該被告明顯之違法之外，多以「公益大於私益」或「第三人利益保護」之角度思考去判定是否符合排除原則之標準，似乎略嫌保守，惟其均有一定之理由證明該等公益的確「大於」私益，故而仍在合理之處理範圍之內。

## 第三節　個人警察資料

### 一、 概說

凡人均生而可能犯錯，於法治國情況下，個人若所犯錯誤構成違法之行爲、有責任能力之人所爲之行爲、基於故意或過失及需以刑法爲制裁之行爲等條件，即成立所謂「形式意義之犯罪[26]」；另外，在社會上被認爲是犯罪之行爲（實質意義之犯罪），則需要有具備某種違反社會道義之因素，致侵害社會共同生活之安寧與利益的反社會行爲[27]。當該個人之行爲構成犯罪，甚至乃是有嫌疑而已，均會有警察資料存於警政系統或相關司法檢調系統之相關資料庫中。此等資料對個人之隱私來說相當重要，因爲不僅可以招致犯罪嫌疑之認定，且若未保管或處理妥當則可能傷害該個人之隱私甚巨，故而通常被認定爲敏感性之個人資料，需要特別加以處理。

關於個人警察資料之部分，由於其可能包含於關於警察部門所擁有之個人資料中，故而下文中部分敘述與法律文件，將範圍設定在警察部門所有之個人刑事資料之保護。另外，在警察部門之資料中另有「警政資料」一項，乃是指關於警察行政需求下所擁有之個人資料，該資料內容爲關於警察人員自身之個人資料，牽涉職等、薪俸等人事，與刑事資料並無相關，則應回歸適用相關之基礎法律規範如「個人資料保護公約」或「個人資料保護指令」等，並非本部分所要討論之面向，併此敘明。

在警察資料方面最需要注意之焦點在於如何平衡公益與私益，也就是說，在打擊犯罪維護社會秩序等等之公益裡與治安與保障個人隱私之個別私益之間，需要找尋到一個平衡點。在一個專制國家，或許維護社會秩序至上，故爲了更有效率地維持治安，必定會犧牲個人之隱私權，將個人資料尤其是相關之

[26] 參：張甘妹，《犯罪學》，台北：三民書局，十二版，1998 年，頁 2。
[27] 同上註。

警察資料加以濫用，以收預防犯罪與威嚇之效果；但是另一方面，當然，過猶不及，若將維護個人隱私無限上綱而危害整體社會治安亦爲吾人所不樂見，故而在此方面關於個人警察資料可能有諸多之限制，但是此等限制應該是在干涉個人隱私之最小範圍之內，且能執行維持社會治安之功能爲足夠。

## 二、 法律基礎

### （一） 歐洲理事會

於歐洲理事會部份，關於「個人資料保護公約」所延伸之建議文件（Recommendation）中，關於個人警察資料之保護最有相關性者，爲 1987 年通過之「關於警察部門之個人資料保護之建議[28]」 ：

該建議只簡單分爲三個部分，分別爲前言、範圍及定義與基本原則三個單元。在前言中，除了與其他相關建議一般，提到其目的乃是爲了符合「個人資料保護公約」之精神，並加以於專門領域中規範外，主要提到了前文所述，本建議乃著重於公益與私益之平衡。

在定義與範圍方面，該建議限於自動化處理個人警察資料之範圍，且此部分之個人資料指確定或可得確定之個人相關資訊。當然，除此之外會員國亦可以國內立法或其他之方式將範圍擴大至人工處理之範圍[29]，但若以改用非自動化處理警用資料之目的，乃是爲了避免本建議者無效。而所謂「爲警察目的」（for police purposes）之意含，則是指一切警方用以防止犯罪及維護公共秩序任務之資料言，故而在此定義上可看出，本建議其實與個人之警察資料之範圍密不可分。

[28] Recommendation No. R (87) 15 regulating the use of personal data in the police sector, adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies.
[29] See Council of Europe, committee of ministers, Explanatory Memorandum of R(87)15, sec. 38-39.

在主要結構的基礎原則部分，共有八個原則加以規範：

1. 關於控制與登記之相關原則。較特殊之處爲其規定以新科技方法去收集或處理個人資料，應符合現有之資料保護精神。

2. 資料收集原則警察資料之收集。限於防止真正危險或制止個別犯罪，若有例外則應該嚴格限制之；應盡告知義務；以科技方法或其他自動化之方法應以特別規定立法之方式爲之；收集關於特別宗教喜好、種族、性行爲嗜好、政治意見、特別社團活動或組織除有「絕對必要」之外，應禁止之。

3. 資料之儲存，警用資料應精確地被儲存，且需真正爲警方法定任務之所需；應予以區分種類；警察資料應與個人之其他行政資料加以區分。

4. 警察資料之使用應只限於警方於警察用途使用。

5. 資料之流通。警方於法定架構下且有法利益之下方可使用個人警察資料；不同警察體系間個人資料之流通，限於有明確法令授權或由監督單位授權，或爲完成其任務之不可或缺或是處理之原資料方爲完整且不違法定任務；個人之警察資料可流通於明顯爲當事人利益之所需或於當時有必須允許之情事發生，或於爲防止立即而嚴重之危險發生之時；流通至私人部門除上述情形外，尚需要有明顯之法定義務或於監督單位監督下爲之；個人警察資料之國際流通應被限制，除非國際法或國內法有明顯之法律規定或防止立即嚴重之危險，並爲防止嚴重犯罪之所需；於國際法或國內法下之跨國流通應秉持互惠原則；以上流通條件應盡量確定其爲屬實，若以不

被確定或爲更新則不應流通因故必須流通則應告知對方其不確定性；不同目的間個人資料之流通應於特別防止犯罪之目的下爲之，並應有法依據或監督單位之監督；線上資料之流通應符合上述相關跨國流通之規範及本國法。

6. 公開化、知曉個人警察資料之權利、修正與接近之權利。其例外爲爲完成警方之法定義務，或保護當事人或第三人；拒絕予以當事人資料應以書面爲之，並告知理由；被拒絕者可有救濟途徑。

7. 儲存資料之時間與更新。當不需要該個人警察資料之時，即應刪除之；刪除時應該就最後法律意見，尤其是不起訴處分、復職、定罪、特赦、當事人年齡等加以考量；會員國國內法並應有修正該等資料規則之法規。

8. 主管機關應確保該個人警察資料之安全。

歐洲理事會針對於該建議並且分別於 1994[30]、1998[31]、2002[32]年舉行三次對個人警察資料方面之評估並做出報告，並於 1999 年於法國史特拉斯堡（Strasbourg）舉行關於關於個人警察資料之區域研討會[33]，希望能對相關之條文規範提出報告與更新。

對於歐洲理事會該關於「關於警察部門之個人資料保護之建議」，筆者歸納出下列較爲特殊之處：

[30] First evaluation of the relevance of Recommendation No. R (87) 15 regulating the use of personal data in the police sector.
[31] Second evaluation of the relevance of Recommendation No. R (87) 15 regulating the use of personal data in the police sector.
[32] Report on the third evaluation of Recommendation N° R (87) 15 regulating the use of personal data in the police sector.
[33] Regional Seminar on Data Protection in the Police Sector, Strasbourg 1999.

1. 個人警察資料之收集處理及儲存應較其他特別種類之個人資料更受到嚴格之保護程度，因爲警察資料所牽涉之內涵關係著刑事法規範下之個人資料，其中心內涵直指人權之核心價值，亦即可能牽涉了包含生命權自由權等基本權利，故而需要特別的慎重處理，所以「關於警察部門之個人資料保護之建議」不論於收集、儲存或處理之相關原則上，均有較一般個人資料保護更爲嚴格之限制。

2. 公益與私益之平衡顯然不易！本建議中即出現保護私益之例外（公益）又出現例外（私益之平衡）之情形，且這些例外，甚至是例外的例外也有許多嚴格之限制，故而可發現立法者希望能完整兼具公私益之用心。

3. 法規範雖然尚稱完整，卻出現許多不確定之法律概念，例如所謂「警方完成法定任務之所需」、「防止嚴重犯罪之所需」等何謂警方之法定任務？何謂嚴重之犯罪？並無規定，則可能仍然出現警方違法濫權之行爲。

歐洲理事會之「關於警察部門之個人資料保護之建議」對於個人警察資料與個人警察資料之保護，可稱是相當先進與完整，在這方面所出現之判決也堪稱經典，至於相關之判決將於下小節中加以敘述，此不贅述。

（二） 歐洲聯盟

關於歐洲聯盟個人警察資料之保護可以從兩個角度之觀點加以切入，其一爲從 1995「個人資料保護指令」之本身加以觀察之；另一方面，由於警察及刑事目的之個人資料保護牽涉到了歐洲聯盟第三支柱之司法與內政合作方面（Justice and Home Affairs cooperation, JHA）的警察合作，故本小節論述方別以

此二角度加以分析，合先敘明。

首先，在「個人資料保護指令」方面，其前言第四十三項中謂會員國在訂定相關對限制資料當事人查詢相關資訊之規範的理由中，其中一項原因即爲刑事偵察及檢查，並於防制犯罪項目中應有監視、檢查及相關必要之管制措施。可見關於犯罪之個人資料保護項目中，常有可能形成排除或限制個人資料保護指令原則之原因存在，也在在證明了此處常涉及公益之衡平。另外，在「個人資料保護指令」本文中，較爲相關之條文爲第八條第五項：「關於犯罪刑事判決或保安處分等資料之處理，限由公務機關監管下爲之，若國家法令已提供適當特定之安全維護措施者，會員國即得訂立例外之條款」，「但關於刑事有罪判決之完整記錄應限由公務機關監管下方得處理」。準此，個人之警察資料在「個人資料保護指令」規範下是得出現例外之排除條款的，並且即便個人之警察資料得由私人部門處理，但仍應在公務機關之監督之下爲之。

另方面，在歐盟本身司法與內政合作之架構中於刑事方面所進行之合作方式，其一即爲關於個人警察資料之交換流通，這主要是在「歐洲司法小組[34]」（European judicial Co-operation Unit, Eurojust）之架構下運作，歐洲司法小組在歐盟一份「針對加強對抗嚴重犯罪之意見」（Council Decision of 28 February 2002 setting up a view to reinforcing the fight against serious crimes[35]）中被授權可經由會員國提供一切之相關資料，以完成其對抗嚴重犯罪之任務[36]，這當然包括了提供相關不論是由自動化方式或人工方式之犯罪者或嫌疑人之個人資料在內[37]。

在此，關於第三支柱之關於個人警察資料之相關保障即透過該意見之第十

[34] 其主要功能在於涉及兩個重大犯罪之調察與起訴時促進與改善相關機關之間之協調工作與改善會員國彼此之間特別是促進執行國際相互法律協助及引渡要求上之合作。詳參：鄧衍森，＜歐盟第三支柱與人權保障＞，中研院歐美所，《歐洲聯盟人權保障研討會》論文集，2002 年 12 月 10 日，頁 15。

[35] Council Decision O. J. L63/1, 2002/187/JHA, 28, 12, 2002.

[36] *Ibid*, Art. 6. (a). (v).

[37] *Ibid*, Art. 14.1.

四條第二項，而準用歐洲理事會之「個人資料保護公約」之原則及相關之後續條約或是建議，故而在個人警察資料之處理（process）上之原則上均適用上一章所敘述之 1981 年「個人資料保護公約」與前小節所論及之「關於警察部門之個人資料保護之建議」；在處理個人警察資料之限制上，則依該意見第十五條僅能於該當事人涉及該意見第四條所規定之重大犯罪類型，而受偵察或起訴者之包括[38]：A. 姓名與任何假名或替代名稱；B. 出生日期、地點；C. 國籍；D. 性別；E. 住、居所；F. 社會保險號碼、駕照、護照、身份證；G. 與受司法調查或起訴確定或可得確定之自然人有關法人之消息；H. 銀行帳戶與其他財務機關之帳戶；I. 所指稱犯罪之敘述、性質、目的、類別與調查進度；J. 指向國際發展之事實；K. 有關犯罪組織會員之細節等之個人資料上加以處理。

該意見第十六條並要求應製作關於上述十五條之自動化處理之索引與臨時之檔案資料；十七條則規定歐洲司法小組應指定一特定之資料保護專員（data protection officer）管理相關事項；十八條規定歐洲司法小組得授權他單位或機關接近相關之個人警察資料；十九條規定有當事人之接近權；廿條為修正及刪除權；廿一條為資料儲存期限；廿二條則是資料之安全之相關規定。

因此，基於政府合作關係以進行偵查自由與起訴自由之歐洲司法小組，在對相關犯罪之個人資料之使用與處理上，有關於基本權利與自由，特別是在隱私權及個人資料保護上，似乎可謂已兼具實體與程序上之保障[39]。

[38] *Ibid*, Art. 15.1.A-K.
[39] 參：鄧衍森，前揭著，頁 20。

## 三、 案例研析

關於歐洲人權法院相關之刑事個人資料或是警察個人資料之判決，最爲具有代表性的即爲 *Case of Klass and others*[40]與 *Malone Case*[41]二者，這在歐洲理事會「關於警察部門之個人資料保護之建議」的解釋備忘錄中亦有提出[42]該二判決，作爲解釋理由的依據之一，足可見其重要性故本文以下以此二判決爲實例，對個人警察資料之保障作一分析[43]：

首先在 *Case of Klass and others* 方面，其案例事實爲 MR. Gerhard Klass 等五原告均爲從事法律相關工作之人士如律師或法官等，於向德國[44]（西德）憲法法庭控告該國基本法（Grundgesetz）第十條第二項有關政府當局得監視人民，並將其監視結果記錄爲個人刑事之相關記錄資料，違背了基本人權之保障及「歐洲人權公約」之第八條[45]於憲法法庭敗訴後，向歐洲人權法院提起本訴訟。另外，其訴訟之標的並非爲政府是否有權力監視人民，而是當局並無義務於監視行爲後，告知被監視之當事人，且無任何訴訟途徑得救濟之。

對此，西德憲法法院認爲其基本法已經有提醒人民注意之條文存在，且該五原告並無直接訴之利益，因爲西德當局並未對該五人進行監視或監聽之行爲。另外，西德政府對此也向歐洲人權法院抗辯，謂該法已盡一切可能除去所有之不確定因素，且未對原告等人爲監視或誤爲監視之行爲。西德政府會立該

---

40 *European Court of Human Rights, Klass and others v. Federal Republic of Germany*, Judgment of 6 September 1978, *Series A, No. 28.*

41 *European Court of Human Rights, James Malone v. the United Kingdom*, Judgment of 2. August, 1984, *Series A, No, 82.*

42 Explanatory memorandum of recommendation No. R (87) 15 regulating the use of personal data in the police sector (17 September 1987), para. 18.

43 至於新進相似之案例，如 European Court of Human Rights, P.G.. And J.H. v. the United Kingdom, Judgment of 25 Septmber 2001, *Reports of Judgments and Decisions s* 2001.與 European Court of Human Rights, Amann v. the Switzerland, Judgment of 16 February 2000, *Reports of Judgments and Decisions s* 2000 等乃與警方監視或監聽所得資料有關，請自行參照。

44 當時兩德尚未統一，本案發生之一造乃是當時之德意志聯邦共和國，即西德，在 *Case of Klass and others* 中本文以下均簡稱西德。

45 本案原告另控西德政府違背「歐洲人權公約」第廿五條、第六條、第十三條等，由於與本文欲論述主題較無關連，故不贅述。

法條之原因，乃是因爲於二次戰後西德爲美英法三強所控，尤其是在監視郵政或通訊方面，西德身不由己，故希望建立該法條將相關權力收回於西德本身，又西德已經對該條文作嚴格之限制，以避免人民基本權利受侵害，故應無違反「歐洲人權公約」之事實存在。

歐洲人權法院對本案認爲：爭點應該在西德之基本法第十條第二項之監視方式，是否符合「歐洲人權公約」第八條第二項之例外規定。依本文前節對於該第八條之判斷標準所做之敘述，法院認爲西德政府之作爲符合所謂「依法（有可預見性、明確性等）」、「爲一民主社會之所需」、「爲防止公共秩序混亂或犯罪」以及「保護第三人基本權利與自由」等要件，且事實上，當時西德有兩件應該加以考慮之事實現狀需考慮：第一，科技發展造成之間諜或監視行爲乃不可避免；第二，恐怖份子於歐洲之活動明顯日趨頻繁。故西德所做之行爲乃屬必要，此時公益明顯較私益爲重大，而基本法第十條也有其存在必要性，故法院判決西德並不違背「歐洲人權公約」第八條。

至於在 *Malone Case* 方面，案例事實略爲 Mr. Malone 爲一英國人，於 1977 年被控以不誠實擁有贓物罪，並開始於法院中訴訟。於訴訟開庭期間，英國警方爲證明其爲有罪而提出一份警方某警官之筆記，筆記中記載有 Mr. Malone 之電話記錄，且該電話記錄詳細記載其談話內容，並以此爲其刑事犯罪之個人資料，並將其建檔於法院當成證物。Mr. Malone 就此認爲其通訊遭受非法之中途攔截（interception），且警方非法持有其個人犯罪資料，並以自動化儲存之方式取得其個人之資料，而未經其同意。英國政府則抗辯其乃依該國分別於 1957 年、1980 年與 1981 年所通過之本國法之程序，而爲相關之蒐集證據之行爲，乃是依照「歐洲人權公約」第八條第二項之要求「依法（in accordance with the law）」而爲上述之行爲，故並不違背「歐洲人權公約」之相關隱私權規範。

歐洲人權法院對此認爲：所謂「依法」對隱私權保護原則加以限制，除了

乃是指相關公布之本國法以外，最重要的其實是該法之法律品質合乎相關公約之規範，[46]而英國所通過之三項法案並不具備有可預知性（foreseeable）、精密（precision）與確定（certainly）等三項嚴格之品質判斷標準，故雖然英國警方之行爲是依英國之本國法，但是由於該法案並不符合歐洲人權公約第八條之例外情形所要求之標準，故法院判決英國警方之行爲對歐洲人權公約第八條有所違反。

## 四、 小結

綜觀歐洲該二組織對於個人警察資料之保障，筆者嘗試歸納出以下小結：

1. 由於個人之警察資料常有可能涉及一國之警察事務或甚至是檢調事務，所以常常直指該國重要之主權或公益中心之所在，因而在此方面，個人資料隱私之保護上常常可能會居於弱勢。相對於世界上大多數國家的並未重視個人資料保護之議題來說，不論是歐洲理事會或是歐洲聯盟在這方面所建立之相關法規都算是相當進步的，並且其立法目的也都說明兼顧公益與私益之平衡是其重要之立法精神，可謂是相當成熟之立法例，足堪其他區域或是國家借鏡。

2. 如上所述，由於警察權之行使常會攸關一國之主權，故而歐洲聯盟在此方面不但於超國家(supranational)色彩濃厚之第一支柱中，於內部市場的議題內對個人資料保護之通則加以規範，並於政府間合作(inter-governmental)色彩的第三支柱之中對特別之警察方面之個人資料保護予以處理，以求會員國之

[46] *James Malone v. the United Kingdom*, para. 67.

間之協調。由此觀之，在個人警察資料保護的議題中可能會使超國家主義與政府間主義之間產生某種程度之激盪，而這激盪之源頭應回歸到上述之平衡公益與私益之基本面去加以處理。

3. 歐洲人權法院對這方面判斷標準之認定，主要還是透過判決中所謂「歐洲人權公約」第八條第二項之相關判別標準[47]加以認定，故在除了理解個人警察資料保護之相關法規外，對於基本的人權保障基本文件也應有相關之理解，方可對本問題有完整之瞭解。

## 第四節　線上服務個人資料

### 一、 概說

凡人均需學習與時並進，在二十世紀以降，最重要的發明之一莫非網際網路之發明與運用。透過網路之運用，自由的思想與行爲不須大眾媒體即能於全球迅速傳遞，並且由於其難以封閉之特性，導致其必須被分享的結果出現[48]，而隱私權－－包括了所謂線上服務[49]之個人資料之保護，則原本可以透過被網路中的匿名性與追蹤訊息來源的困難度所保護，因爲在技術上，無限制的網路

[47] 詳參本文第三章第一節第三項之論述。

[48] See A. Michael Froomkin, *Cyberspace and Privacy: A New Legal Paradigm? The Death of Privacy?* , 52 Stan. L. Rev. 1461, May, 2000; Mark A. Lemley, *Cyberspace and Privacy: A New Legal Paradigm? Private Property*, 52 Stan. L. Rev. 1545, May, 2000.

[49] 所謂的「線上」服務（on-line service）傳統上指的是透過網際網路（Internet）進行所進行資料之傳輸所達成之服務，此種服務有可能是私人之商業服務或公共單位之服務。但是由於科技之飛快進步，傳統的網際網路已經能夠透過電子通訊（electronic communications）之方式進行線上資料之處理，例如最近 Intel 公司之 Intel® Centrino™行動運算技術即爲此例。故筆者以下所提到之線上資料包含所有透過電子通訊科技所傳遞之資料，當然主要之焦點還是擺在網際網路上，合先敘明。

結構與網路的全球化特色[50]，使網路應當是難以控制的。

但是，由於政府在這方面因爲失去了主導掌控之優勢權而可能造成某部分國家主權或秩序之鬆動，因此也在技術上研發了許多「識別[51]」、「監視[52]」與「調查[53]」的方法對網路秩序加以管理與控制。在全球網路中，從任何地方到任何地方都實踐著入侵和破解，這顯示出源自於國家邊界內官方之權力的傳統型式管制的無力，這也因此提高了世界各地政府的焦慮，因爲他們沒有能力去遏止通訊的流動，只能取締在其國境內的通訊，就如同中國對法輪功訊息之取締一般[54]。政府也通常試著藉由約束或取締加密技術來消解人民手中加密的權力，其大量的擴張政府在竊聽和阻礙資料交流的權力，並且爲了網路服務供應者對他們的使用者設置可追蹤的技術建立了契約，也強迫使用者的身分在政府的要求下必須告知。這完全相當於削減了通訊在網際網路中的隱私權，使網際網路從一個自由的區域變爲一個玻璃屋。通訊將仍自由在的流動不息，因爲這是網際網路的結構。但是經由網路供應者的控制對使用場域的重新定義，以及對於特定的網路設置監視的特別通訊協定，控制或懲罰或許會在往後的法律中

---

[50] See Joel R. Reidenberg and Paul M. Schwartz, *Data protection law and on-line services: Regulatory responses*, study project commissioned from ARETE by DG-XV of the commission of the EC, 1998/02, p. 2.

[51] 識別的科技包括了密碼的使用、「Cookies」、以及辨認的程序等。「Cookies」乃指網站自動放入電腦磁碟來連接它們之數位標籤。 倘若「Cookies」被放入電腦，該電腦所有的線上活動都將自動被置入「Cookies」之網站之伺服器所紀錄。辨認的程序使用能夠允許其他電腦查證互動通訊者原點與特徵的數位簽證。其通常依賴編碼的技術。識別通常是分層工作，隨著個別使用者被伺服器所識別，伺服器本身又被網路所辨識。網路上最早安全協定的例子之一，是 Netscape 所制定的「secure socket layer(SSL)」。其它許多標準的安全協定已被信用卡公司和電子商務公司所採用。See Manuel Castells, *The Internet Galax: Reflections on the internet, business and society*, New York: Oxford University Press Inc., 2001, p.171.

[52] 監視的科技通常依賴於辨識的科技來找出個別使用者。監視之科技可以攔截訊息（放置能追蹤來自特定電腦位置之訊息的標籤）並監視機器的運作。監視的科技可以在訊息的原點辨識一個已知的伺服器。於是，靠著說服或強迫，政府、公司、或法院將可以透過辨認的科技來辨認潛在的犯罪，或者當資訊允許時，能輕易地查到它們的清單（例如：將伺服器之客戶的電子住址比對真實住址）。Ibid, pp.171-172.

[53] 調查的科技涉及來自於監視與資料取得的結果之資料庫的建構。一旦資料以數位的形式收集，資料庫中的所有資訊項目可以被加總、相減、結合、以及依據目的和產能來分辨。有時候，它可能僅僅是資料的加總（例如在市場的研究）。其乃爲個人化的追蹤，例如一個人可能被電子紀錄（來自於信用卡的網路付款、電子郵件、電話紀錄）所辨識。在現今的科技環境，所有電子化的訊息傳送都將被紀錄，可隨時被處理、辨識。Ibid, pp.172.

[54] Ibid., p.178.

加以規範。新的網際網路結構、新的規範、變成了控制的基本工具，使之可能藉由傳統形式的國家權力去實行管制與監督[55]；而在另一方面，相關之私人企業業者也一直不斷嘗試透過彼等科技試圖由網路中獲取控制之權力[56]，這其中也包括了對線上個人資料之覬覦[57]，因爲透過快速而豐富完整的個人資料之快速蒐集與儲存，其中所可能隱藏的無限商機是絕對具有相當大的吸引力的。

所以，不論是政府或私人企業[58]對線上隱私權來說，都有可能是一種侵害之來源，此時當然就需要一套完整之立法與司法制度對之加以平衡。因此，在法規面方面需要制訂有相關之規範，即便是可能會因爲該線上資料之技術發展飛快而使法規來不及與時並進，但是制訂基本之通則與讓民眾瞭解其相關權利卻是最基本之需要[59]。另一方面，在司法制度上除了要使法官們能對網路上新科技能即時地吸收與理解，故在職相關訓練不能缺少外，對相關之法律工作人員如律師、檢、調人員等，均需有一般性之推廣使之能趕上瞬息萬變的網路發展。

在線上資料的個人資料保護方面可由兩個面向切入，其一爲由整個網際網

---

[55] Ibid, p.178-179.

[56] 參：＜歐洲企業試圖爲電子郵件保留資訊痕跡＞，2002/09/25，歐洲日報（聯合報）：
…歐洲企業本身已開始試圖建立可同時儲存和過濾收發的郵件的方式。在意外事件後或司法調查時需要還原資料的環境下，「資訊痕跡」的概念正蓄勢待發。

[57] 例如，微軟公司(Microsoft)即可能以此種方式快速收集線上之個人資料，參：＜歐盟保護隱私權 盯上微軟 Net. Passport＞，2002/05/28，歐洲日報（聯合報）:
微軟公司自網際網路蒐集使用者個人資料的系統是否觸犯隱私權保護法，已引起歐洲聯盟執行委員會的調查，爲軟體巨人在歐洲面臨的反托辣斯案調查增添麻煩。
在回應歐洲議會荷蘭籍議員梅桀（Erik Meijer）質詢的書面答覆中，歐盟執委會宣布，已針對微軟 Net. Passport 免費服務展開調查。執委會歐盟區內市場委員柏克斯坦（Frits Bolkestein）寫道：「委員會正與各國資料保護當局聯合調查此案，查明該系統是否遵守歐盟的資料保護法。」 。

[58] 在私人企業中，勞工與雇主之間在企業內部網路之個人資料保護也是一重要之議題，諸如雇主是否看監看員工之電子郵件或相關屬於該企業電腦中的電子軌跡等，也是一種可能之侵害態樣。關於這部分之論述參：Hammond Suddards Edge, *Privacy and Communications*, London: CPID, 2001, pp.36-42.

[59] 針對此觀點，國際知名的隱私權保護團體 EPIC（Electronic Privacy International Center）便特別認爲歐盟的「電子通訊個人資料保護指令」能符合線上隱私保護之法制需求。參：http://www.epic.org/privacy/intl/data_retention.html.

路的線上技術面爲焦點切入，在此面向上主要以一般線上之隱私保護技術[60]（Privacy-Enhancing Technologies, PETs），如 Anonymiser 或 Cookie Pal 等較爲偏向網際網路本身技術之方式，對個人資料以及線上隱私加以保護；另一方面，則可以法治社會面之方式對個人線上資料加以保障[61]。本節以下主要針對法治社會之面向，對歐洲個人資料保護之相關法律規範與實際執行層面以及案例之探討爲主[62]。

本節以下即先以歐洲理事會與歐洲聯盟之相關法規範爲基礎，對個人線上資料之保護做一整體性之認識；另外，由於該等基礎規範均爲近年來所公布，故而相關之法院均未對個人線上資料保護有所判決之先例存在，因此筆者以相關組織之研究報告或政策作爲實際上案例之分析研究方式，合先敘明。

## 二、 法律基礎

### （一） 歐洲理事會

歐洲理事會對於線上個人資料之個別建議爲「關於網路隱私之個人資料保護之建議－－保護個人於資訊高速公路[63]收集與處理個人資料之指導方針[64]」

---

[60] 該技術涉及以保護個人識別爲目的之技術上與組織上之概念，通常涉及加密之技術，詳參熊愛卿，前揭文，頁 53。

[61] 網路影響生活至大，故論者認爲需有規範加以約束。See Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, April, 1998.而該面向又有學者細分爲兩面向，其一爲從強化資訊社會基礎架構與軟、硬體設計者之社會責任著手；其二爲從網際網路社會中之企業經營者之自律爲約束。前者似較偏向法律面；後者偏向社會面，但整體來說均以人文面向作爲思考的出發點，與前項以科技爲出發點之技術面有所差異，故筆者爲此分法。參熊愛卿，前揭文，頁 56-57。

[62] 至於較爲技術面之議題可參考熊愛卿，前揭文，頁 58-60。

[63] 「資訊高速公路」（Information superhighway）指作爲提供資訊傳輸之資訊基礎架構，是由電腦及各種電信管道所組成之廣闊資訊網，包括所有之公共、商業、私人網路之電腦及相關之周邊設備，參熊愛卿，前揭文，頁 14-16。

[64] Recommendation No. R (99) 5 for the protection of privacy on the Internet—guidelines for the protection of individuals with regard to the collection and procession of personal data on information highways, adopted by the Committee of Ministers on 23 February 1999, at the 660th meeting of the Ministers' Deputies.

（下簡稱「個人資料保護指導方針」），該建議文件是以一種「指導方針」之形式寫成，內涵上透過一種類似宣導方式之文字，提供了包括了網路使用者（users）與網路服務提供者（Internet service providers, ISP）雙方面對於個人線上之資料保護應注意之事項的資訊。之所以會以此種有別於其他建議採取法條式規範形式之方式爲其內容架構，究其原因，可能是因爲網路之發展性過於快速而難以預料，以法條方式爲之難免缺乏一般原則性之不足；另外，以此種方式爲之可方便一般民眾更加容易閱讀與瞭解該建議之內容，並進一步提醒使用者與 ISP 業者所應負起之責任與相關之權利，故必須採較爲「平易近人」之方式爲之。較爲特殊的一點，本建議因爲採特殊之指導方針式立法，所以是唯一一個沒有解釋備忘錄或相關會議報告的建議文件。

於「個人資料保護指導方針」前言中提及，由於體認到新科技與線上通訊服務之發展會影響到社會關係－－尤其是國內或國際之資訊通訊與交換，以及其所可能帶來之危機，其依循整個由「歐洲人權公約」第八條乃至「關於薪資及其他作業之個人資料保護之建議案」、「關於公務單位所有之個人資料保護之建議」與「關於電子通訊服務尤其是電話部分個人資料保護之建議」等立法之脈絡，而有本建議之出現。

內容架構上本建議（指導方針）共分四部分，分別爲總論、對網路使用者（for users）、對網路服務提供者（for Internet service providers, ISP）與聲明及救濟。總論中聲明以下兩部分之基本原則係基於對網路使用者與 ISP 業者之公平對待與保護隱私所設定，而網路使用者除了注意攸關本身權益與義務之第二部分外，對於 ISP 業者所應有之義務與責任也應一併瞭解，反之 ISP 業者亦然。

在對網路使用者部分該建議共歸納出十三項指導方針，爲避免流於繁瑣本文摘錄其重要者如下：

1. 網路是不安全的，往往有許多危險存在，但其實有許多方法

可以對之加以預防，其中，「加密（encryption）」是一項很好用之工具。

2. 任何到過之網站或瀏覽之信件均會留下「電子痕跡（electronic tracks）」，鼓勵安裝相關電子追蹤系統以瞭解到過之網址。

3. 盡量對網路身份「匿名化」，若礙於法規或事實無法爲之，則應盡量採用假名或筆名等非真正資料。

4. 注意己身之敏感性資料如信用卡資料或帳號資料等；電子郵件住址乃是一種個人資料，可要求對方刪除或保密。

5. 線上所處理之資料網路使用者需對之負責，故勿寄發有惡意之信函（如病毒信件或涉及毀謗、詐欺內容等）。

6. 網路使用者之 ISP 業者有責任管理網路使用者之資料使用目的；反之，網路使用者亦可對 ISP 業者做出篩選之動作。

7. 資料之跨國傳輸應注意對方國家之個人資料保護標準。

至於對 ISP 業者言，所規範者大多爲與上述互爲相對之內容，其他較爲特殊者如：

1. 勿進一步要求網路使用者提供必須之個人資料以外之資料或資訊－－除非有對方之明確同意。

2. 對資料之使用應有責任並公布隱私權政策（privacy policy），若需公布資料於網站上則需「三思而後行」。

3. 若需提供個人資料則提供之資料需確保其準確與即時。

至於在最末的聲明與救濟部分，則是指出包括 ISP 之範圍可能含有：提供

網路路徑者、提供內容者、網路架構提供者、軟體設計者及電子布告欄操作者等；另外，網路使用者與 ISP 業者均需確定本建議之相關權利受到尊重，並可要求官方之協助；並且，本指導方針可提供全部種類之資訊高速公路做爲參考。

（二） 歐洲聯盟

在「個人資料保護指令」中專門關於網際網路方面，僅在其前言中第四十七項稱「以電信或以電子郵件之方式，以傳遞包括個人資料之訊息爲單一目的者，原則上，該原始訊息應屬於個人資料之初始管理人，而非訊息傳遞之服務者。但爲提供其服務作業之所必須而處理額外之個人資料者，視爲管理人。」本項所要表達者，筆者認爲應擴張解釋爲：透過電子通訊科技所傳遞之個人資料均在範圍之內；也就是說，應包含所有之「線上」個人資料。因爲該前言之立法精神應該是希望將所有透過新興科技而非傳統方式之資料傳遞（例如文書或簡單之電腦磁碟片交換）都納入保護，蓋透過該等新興科技之資料傳遞常常會發生資料之原始所有人無法掌控之事實，故希望該等資料仍應屬於個人資料之初始管理人之所有，以保護其權利以及避免個人資料不當外流也。

「個人資料保護指令」其餘並未特別在該指令正文中特別標明專爲網際網路線上流通之個人資料所規範者，但由於該「個人資料保護指令」爲原則性之中心基礎規範，故關於網際網路或其他以電子通信方式之線上個人資料原則上均應該有所適用。其後歐盟由於察覺電子通訊新科技之進步以及網際網路之普遍化，故也分別公布了 1997「電信事業個人資料保護指令[65]」、2001「共同體機關間資料流通規章[66]」以及 2002「電子通訊個人資料保護指令[67]」等以爲因應。

[65] Directive 97/66/EC of the European Parliament and of the Council of 15, December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, Directive 97/66/EC, Official Journal L 024, 30/01/1998 P. 0001 – 0008.

[66] Regulation (EC) 45/2001 of the European Parliament and of the Council of 18. December 2000 on 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, Official Journal L 008, 12/01/2001 P.

應注意的是，1997 年之「電信事業個人資料保護指令」其範圍大多侷限在傳統之有線電話電信服務，與本文所討論核心線上個人資料略有出入，但其後對之加以取代之「電子通訊個人資料保護指令」則將範圍擴大，故應認爲其範圍擴張至包含線上之個人資料。關於這些指令或規章之內涵本文已在前章[68]中有所敘述之部分，在此不另外贅述，僅特別將對「電信事業個人資料保護指令」加以取代的「電子通訊個人資料保護指令」提出，加以詳細討論，並將焦點聚於關於網際網路之線上服務之個人資料部分。

在歐盟「電子通訊個人資料保護指令」前言中，除表明係依照「個人資料保護指令」之精神而爲規範之外，另外相當特殊的一點是首次提到其係遵照「歐洲聯盟基本權利憲章」第七條與第八條之精神而立法，筆者認爲是否透露了歐盟制憲化的希望雖不得而知，但是至少透露出了歐盟以後關於基本權利或人權之相關法規範應該也會對「歐洲聯盟基本權利憲章」加以呼應之事實[69]。另外，本指令前言特別關於網際網路者，例如在第六項中指出：網際網路以提供一普遍而廣泛之全球性電子通訊服務建設之方式，顛覆了傳統的市場架構，雖帶來了許多的新希望，卻也爲個人資料及隱私帶來許多新的危險；而第廿四項中則指出除了依合法目的並使使用者（users）能對之知悉外，網路之各種間諜軟體（spyware, web bugs, hidden identifiers）乃是禁止使用的；第廿五項則是關於 cookies 之管控，該指令認爲 cookies 仍有必要存在，但需要加以管理，並讓使用者能有對之加以拒絕存取至使用者自身之權利。

至於在「電子通訊個人資料保護指令」本文方面共有廿一條，筆者認爲對於網際網路方面之重要者大略敘述如下：

---

0001 – 0022.

[67] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Directive 2002/58/EC, Official Journal L 201 , 31/07/2002 P. 0037 – 0047.

[68] 詳參本文第二章第五節第一項第一目。

[69] 關於歐盟之制憲問題與人權議題之可能競合，See J. H. H. Weiler, *The Constitution of Europe-'Do the New Clothes have an Emperor' and Other Essays on European Integration*, Cambridge University Press, 1999, pp.102-129.

在定義上需說明的是，除特別在第二條中說明者外，均以「個人資料保護指令」爲準；「電子通訊資料（traffic data）」指在以電子通訊網路上傳送通訊爲目的而處理之各種資料（第二條 b 款）；「位置資料（location data）」任何在電子通訊網路上傳遞之資料能指出電子通訊服務之使用者地理上終端位置者（第二條 c 款）；而「通訊（communication）」在本指令定義中則是指以公開可得知之電子通訊網路服務所爲之在有限數目對象之間的資訊交換或傳輸，並且所謂之通訊的範圍，不包括除可確定通訊端外之公開廣播或傳播（第二條 d 款）。

在網路安全方面，則規定電子通訊服務之提供業者應提供適當之技術及組織化之方法，以保障其所提供服務之網路隱私安全（第四條第一項）；並且在用戶有可能發生安全上之危險時，必須盡告知義務，包括告知各種可能之救援方法及所需之花費等（第四條第二項）；在隱密性方面，則是會員國政府應對電子通訊服務之通訊網路加以確保（第五條），若需以科技或其他方法獲得用戶終端設備之資料時，用戶端需依「個人資料保護指令」之相關要求，獲得明白且確定之告知（第五條第三項）。

電子通訊資料於毋須使用時，必須由電子通訊服務網路提供者加以刪除或予以匿名化（第六條第一項），但若用戶需使用之則得依法加以保留（第六條第二項），用戶明確同意者亦得爲之（第六條第三項）；而除了電子通訊資料外，使用者之位置資料則只准許在匿名或用戶於加值服務需要下，經同意方得爲之，並且該使用者並得有隨時撤回之權利（第九條第一項）。

總之，在「電子通訊個人資料保護指令」規範下可以歸納的一點是，歐盟希望各會員國透過政府之力量，對電子通訊服務及網際網路之線上個人資料之傳遞用法律規範之方式加以掌控，此種管理網際網路之方式在下文中會有較詳細之說明。

## 三、 相關研究

對於網際網路上的隱私權保障以及個人資料保護之觀念來說，歐洲本身與美國之間在觀念上是有所歧異，而並非如同在個人資料保護中的其他領域（例如警政或醫療領域）一般的理念相近。就理論上言，網際網路之興起由於有一種打破既有秩序，甚至是「控制權革命[70]」之態樣，所以相對的對此種新興科技的態度也可能產生不同的觀念。而在線上隱私方面，由於網際網路之快速發展而造成了許多衝擊，在對這種情況的處理態度上，隱私權提倡者們有著不同的看法。在自由風氣與資本主義興盛的美國，漸有輿論要求應該是由消費者（使用者）而非各國政府應該被賦予權力去控制個人資訊之流向，而爲達此一目的，甚至其主張應該創造一個所謂的「隱私權市場[71]」。在這種理念下，其目的在於讓個人能夠對個人資訊取得更多自主性之控制權，而非將其交由政府所控制；甚至，其倡議可將之交與產業自律來解決。

但是，過份將隱私權保護私人化之結果，期待個人在沒有政府之協助下去完成隱私權之保護，卻相當可能產生許多不利的困境[72]，例如：不合乎效率要求、對於個人資訊交換所產生之無法預測結果的視若無睹、不平等談判力量之出現、使裁量和平衡之空間變的侷促而有限、隱私權商品化而發生諸多問題等等。

也因此，由政府去適當主導隱私權架構相關規範則是另一種主要之觀點，而這種觀點則相當程度地反映在歐洲上[73]，這也是本論文之所以在論述歐洲觀

---

[70] 關於所謂「控制權革命」之概念，筆者主要是參考 Andrew L. Shapiro 的*"The control revolution-How the internet is putting individuals in charge and changing the world we know?"* 一書，中文翻譯詳參前揭著 10，第一篇，頁 27-107。

[71] 所謂的「隱私權市場」是指一個和逐漸成長的個人資訊市場處於競爭或互補關係之市場。關於其詳細之解釋以及例證，詳參同上註，頁 245-246。

[72] 同上註，頁 246-252。

[73] 歐洲對個人資料隱私採較嚴格之規範，對於網路之隱私也形成獨特之法領域體系。See: Joel R.

點的個人資料保護理論時，均不斷地輔以提出相關之法規範依據之原因。在歐洲的觀念中，不論是歐洲理事會或歐洲聯盟均認爲隱私權與個人資料保護是人權架構中不可或缺的一環，當然在網際網路線上服務的個人資料保護上亦若是，所以不論是歐洲理事會或是歐盟本身均對於此議題有著重要之關注，而由於網路科技之發展快速，雖然歐洲理事會或是歐洲聯盟均以積極立法之態度加以面對[74]，但是仍追趕不上其發展速度，故對於網際網路線上服務之個人資料議題便不斷地以提出研究報告或圓桌論壇會議之方式去討論，並常常將其結果規範於未來之法規範上。觀察該報告或會議結論常常可以瞭解歐洲未來對網際網路個人資料保護之觀點與發展趨勢，因此本文以下便分別對近來歐洲理事會以及歐洲聯盟對於網際網路線上服務個人資料之相關報告或會議做一論述。

在歐洲理事會部分至目前爲止一共召開三次有關個人資料保護之相關會議，其中與線上個人資料較有關連之會議爲 2001 年在波蘭華沙所召開之歐洲資料保護會議[75]，該次會議主題爲討論「個人資料保護公約」之現狀與未來（Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data: Present and Future）而會議中主要之議題爲：個人資料保護法規－現在與未來對資訊社會挑戰之回應，其中一篇核心的報告「全球資訊世界下之個人定位：權利與義務（The individual's position in a globalised information world: rights and obligations）[76]」一文中提出對於網際網路領域中應

Reidenberg, *Cyberspace and Privacy: A New Legal Paradigm? Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 Stan. L. Rev. 1315, May, 2000.

[74] 這便是所謂的「歐洲模式」，乃採取嚴格之立法規範去保護個人資料。相對的「美國模式」對此則強調自由與開放主要係以業者自律與市場機能之調節，來達個人資料保護之目的。關於美國在電子通訊個人資料保護方面之態度與立法，詳參：Paul M. Schwartz and Joel. R. Reidenberg, *Data Privacy Law*, Virginia: MICHIE Law Publishers, 1996, pp. 219-259.

[75] European conference on data protection on Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data: Present and Future, organized by the Council of Europe and the Inspector General of Poland for Personal Data Protection, Warsaw(Poland), 19-20 November, 2001.

[76] Nathalie Mallet- Poujol, *The individual's position in a globalised information world: rights and obligations*, report of European conference on data protection on Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data: Present and Future, 19-20 November, 2001 proceedings, p.69-90.

如何於個人資料保護方面加以因應之方法：

首先，對線上個人資料處理之預先告知，是個人資料檔案處理過程盡量透明化的保證，但是在實際執行上常常窒礙難行。對此之解決方法應以追本溯源之方式加以解決，盡量去追查初始或前手資料之來源，以達到能夠預先告知當事人之能力；復次，能有得接近當事人個人資料之權利也是重要指標之一，但是當事人卻常常甚少使用該權利，在全球資訊社會下若不能保證使個人對自動處理之資料能夠「有跡可尋（tracking）」，則此種得接近個人資料之權利將會走入死胡同中而無法實際有效果。弔詭的是，網際網路正有此項所謂「留下足跡」之功能存在；另方面，其認爲應該在未來的立法上促使當事人更積極地對其權利行使，並鼓勵當事人有反饋（feedback）之行爲。

有趣的一點是，在該報告中認爲當事人之同意之權利在全球資訊社會中常常最受到矚目，但是應將其視爲最後之防線而應該由其他方法先防止侵害，且需要有程度上之區別，例如，在網路上對於經濟利益上個人資料之同意與對於醫療個人資料上之同意必定有不同程度之差異，而當事人在經濟利益上個人資料之同意應是較對於醫療個人資料上之同意爲優先之選項的。

對於此觀點，管見以爲此乃是因爲當事人同意是相當程度具有自主性的，其精神與上述「隱私權市場」概念中，希望讓個人能夠對個人資訊取得更多自主性之控制權，而非將其交由政府所控制之觀念不謀而合，則此種概念與歐洲模式的由政府主導個人資料保護之觀念有所差異，當然應該限縮其使用之態樣，但是，當事人同意之觀念也反映了個人自主之人權概念而不能拋棄，故在歐洲方面應該是抱持著一種審慎使用該權利的態度。

在歐洲聯盟部分[77]，則是在布魯塞爾於 2002 年 9 月 30 至 10 月 1 日舉辦了

[77] 歐盟部分對於線上個人資料之研究報告另有 Joel R. Reidenberg and Paul M. Schwartz, *Data protection law and on-line services: Regulatory responses*, study project commissioned from ARETE by DG-XV of the commission of the EC, 1998/02 與 Serge Gauthronet and Frédéric

資料保護會議[78]，其中第二個研究會議（workshop）主題即爲「資訊社會之發展：網路及線上隱私保護技術（Developments in the Information Society: Internet and Privacy Enhancing Technologies (PETs)）」，可見網際網路以及線上之隱私與個人資料保護議題相當受到歐盟重視。

於該會議報告中提到之對於線上服務個人資料保護以及隱私權政策之看法，則有相當重要的一種不同方向的思考方式出現[79]。其認爲網路線上服務將會收集使用者之生活習慣，而可能造成個人資料遭到任意收集之情況，例如知名網路書店亞瑪遜網路書店（Amzaon.com）會根據該線上服務使用者之消費歷史所形成之購書消費習慣而推薦相關之書目，此種作爲就正面言可收方便消費者，省去搜索書目之時間成本，且易發現自己有興趣之書籍進而購買之效；但是相對的，卻也容易限制了該消費者閱讀之範圍，並且可能一此而洩漏個人閱讀習慣，甚至是政治立場與宗教思想等等，所以需要對於網際網路上的隱私權保障以及個人資料保護之觀念加以處理。而解決之道卻不應該侷限於歐洲傳統模式的由政府主導整個法令之方式[80]，或是加強企業者（資料管理者）之責任，而應該是強化消費者（使用者）之權力[81]。

該份研究報告認爲歐洲傳統對於個人資料之保護方式可能會發生一些缺憾，例如：資料管理者可能會因此而轉嫁其因個人資料保護政策所生之成本予消費者（資料當事人），或者當保管人制訂了「單一定型化（one-size-fits-all）」之選項時，則相對的使用者在選擇上會發生僵化之現象，若發生此種僵化選項

---

Nathan, *On-line services and data protection of privacy*, study project commissioned from ARETE by DG-XV of the commission of the EC, 1998/12 兩篇，由於篇幅所限，未能一併論述，請自行參考。

[78] Data Protection Conference and Report on the implementation of Directive 95/46/EC, Brussels, 30.9./1.10.2002, IP/02/1373.

[79] See Jason Albert, *Privacy on the Internet: Protecting and Empowering Users*, COVINGTON & BURLING, Brussels, 2002/10/01.

[80] 關於歐洲與美國兩方面政府所扮演角色之不同，參考 Fred H. Cate, *Privacy in the information age*, Washington D.C.: Brookings Institution, 1997, pp.121-128.

[81] 例如在美國模式的安全港原則中，即有強調消費者之個人選擇權如「選擇退出」（opt out）之型態，選擇其個人資料是否向第三人揭露及是否願接受與原先目的不同之使用等；另「選擇加入」則賦予當事人更高度之積極選擇機會。See Fred H. Cate, *op. cit.*, p.117.

之現象時，則可能產生消費者消費了過剩之服務的情形。換句話說，若消費者有選擇可能的話，其並不一定會多花錢去選用該項個人資料保護之措施（不論是因爲其本身對於該項個人資料並不那麼在意，或是因爲經濟之因素），則這種情形可能會使低消費能力者就此退出網際網路線上服務，而使資訊社會造成不平等之現象；另一方面，選擇上會發生僵化之現象若發生，也可能產生使用者之特殊需求無法反映在單一定型化選項中之情形。

並且在傳統的歐盟模式中，雖由各會員國政府主導之態勢相當強硬，也因此而使諸如美國等其他國家或貿易體屈服，進而與歐盟訂立隱私權條約，但是在未來並非所有之相對國家皆會如此作爲，特別是當遇到了堅持個人自由或國家自主立場堅定之國家或貿易對象時，歐盟是否仍會因爲對方之隱私權保護政策與歐盟不同而拒絕與之貿易，是有相當疑問的；況且，姑不論國際情勢，就歐盟本身而言，內部也不時傳來雜音[82]，顯見由完全由政府主導之政策在執行上是顯有困難的。

因此該份會議報告中主張用一種較爲折衷之混合模式，以加強使用者選擇權限，而非只單一增加資料管理者責任之方式，例如透過「隱私選擇平台[83]（the Platform for Privacy Preferences Project, P3P）」之技術或「線上隱私保護技術（PETs）」，混合以法規範規定個人資料保護之模式加以保護線上個人資料，而由於該等技術已經針對不易使用加以改善，並且已經引入兩大知名瀏覽器（Microsoft Internet Explorer、Navigator）中，故應該更加強其使用之可能性。

對於此種觀念，筆者認爲此種混合模式應只限於在較爲非敏感性之個人資料領域中（例如純粹商業目的之線上服務個人資料）強化使用者之選擇權，而於敏感性個人資料領域仍應強化政府主導以及增加線上服務提供者責任，否則

[82] 例如愛爾蘭等國至今並未將「個人資料保護指令」國內法化，另外由於歐盟於 2004 年即將增加 15 國，則可以預料的雜音也會因此增多之可能性相對地提高許多。
[83] 關於 P3P 之詳細內涵，參：熊愛卿，前揭文，頁 66-69。

過度強化個人選擇權之結果可能會有諸多缺點，已若上述。

## 四、 小結

由上述論述中，筆者歸納出一些論點，茲臚列如下：

1. 線上服務其實是一種工具，其目的是有著相當廣泛領域的，從一般的商業買賣、傳播行銷，乃至於敏感的信用資料、醫療服務、警政作業等，均可透過網際網路之方式達成，甚至其不斷地有新的擴張，因而確立基本原則乃勢必要的趨勢；另一方面，由於其跨領域之特性，筆者認爲未來針對特定領域之線上服務的個人資料加以立法有極大之可能性。

2. 歐洲對於網際網路線上服務個人資料保護之處理依目前情勢看來，乃是以政府用法規範之方式加以主導，透過歐洲的區域組織的相互合作，歐洲整體間對於網際網路線上服務個人資料保護較能有相近似之制度。但由於該種保守且嚴格之法規範相較於網路世界的自由趨勢是相當存在著矛盾的，因此歐洲在整個網際網路線上服務個人資料保護上的方式，是仍有討論空間的。

3. 網際網路線上服務個人資料保護不但在法規面需要加以重視，在實際的執行面向上顯然更需透過向人民之直接推廣，例如歐洲理事會關於網路隱私之個人資料保護之建議即以此種淺顯易懂之方式加以規範，避免以法條之艱澀文字而使之推廣不易，藉由此方面使人民快速瞭解線上服務應有之權利與義務，方能進一步避免糾紛及不當侵害。畢竟，由於網際

網路線上服務之形態日新月異，若能使民眾對基本原則有認識，方爲治本之法。

## 第五節　結語

本章個別地就不同之領域加以分別觀察歐洲個人資料保護之面向，以符合相關特殊領域之特別要求。透過個別案例之分析研究，分別對歐洲區域之醫療資料（medical data）、刑事資料（criminal data）等敏感性資料之問題，做一討論，並且對於新興之網路線上個人資料（on-line data），由於關係到未來整個個人資料保護發展之重大變化也一併加以論述。

首先在個人醫療資料保護方面，透過相關之醫療流程之驗證，發現個人之醫療資料爲相當重要之敏感性之個人資料領域，因而歐洲區域組織對之也特別加以立法。個人醫療資料保護之法律基礎透過歐洲理事會 1997 年「醫療個人資料保護建議」與「生物醫學公約」以及歐洲聯盟「個人資料保護指令」本身，均是針對該特別領域所訂立之專法，對於個人醫療資料之領域做出專門之保障。隨之以歐洲人權法院（ECHR）之判決結果加以佐證，以加強法實證之基礎，對醫療個人資料之保護理論做一論述，在分析歐洲人權法院判決之後，歸納出包括基因資料之重要性不容忽視、對於未出生胎兒及無行爲能力人之保護十分重視以及範圍侷限於自動化處理之個人醫療資料之情形。並進而發現在關於個人資料保護方面歐洲人權法院經常以「法依據」、「合法之目的性」與「爲民主社會之所需」三要件對個案加以檢驗，足供吾人參考。

至於在個人警察資料之保護方面，筆者發現最需要注意之焦點在於如何平衡公益與私益，並且因該資料非常可能影響個人之刑事記錄，故亦爲敏感性之特種資料之一。在法基礎層面的處理上，透過歐洲理事會之「關於警察部門之

個人資料保護之建議」，發現不論於收集、儲存或處理之相關原則上，均應有較一般個人資料保護更爲嚴格之限制；在歐洲聯盟個人警察資料之保護，則從兩個角度之觀點加以切入，其一爲從 1995「個人資料保護指令」之本身加以觀察之；另一方面，則從歐洲聯盟第三支柱之司法與內政合作方面的「針對加強對抗嚴重犯罪之意見」加以論述，並發現在個人警察資料保護的議題中，可能會使超國家主義與政府間主義之間產生某種程度之激盪，而這激盪之源頭應回歸到上述之平衡公益與私益之基本面去加以處理。隨之以 Case of Klass and others 與 Malone Case 兩個在個人警察資料領域中的經典判決對之加以做實際上案例之研究，並印證公益與私益之衡平在個人之警察資料方面是最重要之關鍵所在。

最後在網際網路線上服務的個人資料保護領域方面，筆者發現由於網路以及資訊社會之秩序對傳統的其他領域來說是一種全新的體驗，不論是政府或私人企業對線上隱私權來說，都有可能是一種侵害個人資料之來源，此時當然就需要一套完整之立法與司法制度對之加以平衡，這也是所謂「歐洲模式」的觀念。在「歐洲模式」中，歐洲理事會以獨特的指導方針模式規範有「關於網路隱私之個人資料保護之建議」，堪稱創舉；而歐洲聯盟對此，則以「電子通訊個人資料保護指令」加以因應。至於在實際的論壇以及會議上，歐洲的學者激盪出不同於美國自由派模式的思考方式，認爲仍應由政府加以主導管控，但卻也不同的反向思考，認爲應該適當地加入混合式的思考方向。對此，筆者也提出看法，認爲應僅限於在較爲非敏感性之個人資料領域中，去強化使用者之選擇權，方爲妥適。

# 第四章　我國與歐洲對個人資料保護作爲之比較

個人資料保護在歐洲方面之理論與實際，在前二章已有相關論述；由前二章亦可觀察到歐洲區域對於此議題之重視與發展之成熟度。本章以下則以前述歐洲經驗反觀台灣對於個人資料保護之相關作爲，以歐洲之法規範模式與實際之案例的經驗，與台灣做一平行式之比較。而在法規範的切面上，主要以我國「電腦處理個人資料保護法」與歐洲理事會「個人資料保護公約」及歐盟「個人資料保護指令」做一對照；在實際個別領域之切面上，則以前章之個人醫療資料、個人警察資料以及網際網路線上服務個人資料分別做一比較，以作爲呼應。

## 第一節　電腦處理個人資料保護法暨相關法規

### 一、 概說

個人資料保護之權利在我國憲法中並未於第二章明文規定，但由於所謂的個人資訊隱私權[84]已經是一項公認之基本權利，故應可以憲法第二十二條爲概括之保護依據[85]。而我國之民法第一百九十五條第一項規定：「不法侵害他人之身體、健康、名譽、自由、信用、隱私、貞操，或不法侵害其他人格法益而情節重大者，被害人雖非財產上之損害，亦得請求賠償相當之金額。其名譽被侵害者，並得請求回復名譽之適當處分。」即已經將個人之隱私納入保障之權利之中，又刑法第三百五十九條：「無故取得、刪除或變更他人電腦

[84] 關於個人資訊隱私權之論述，詳參本文第二章第一節。

[85] 參：李震山，《人性尊嚴與人權保障》，第七章 論資訊自決權，台北：元照出版，2000 年，頁 295-296；另參：李震山，＜論個人資料保護－以人體基因資訊爲例＞，《月旦法學雜誌》，台北：元照出版，第 75 期，2001 年 8 月，頁 18。

或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」亦對違法蒐集電腦或電磁設備中之個人資料爲相關規範，但真正關於個人資料保護在我國之專法乃是「電腦處理個人資料保護法」。

又，我國最新進之人權基本大法「人權基本法草案」，對於我國未來之人權保護用力甚深，其中第十九條則是與本文主題直接相關之個人資料保護問題。其曰：「個人資料應受法律保護（第一項）。個人資料之取得、處理及使用，非依法律規定或當事人之同意，並基於特定之目的，不得爲之（第二項）。人人有權知悉及更正其個人資料，並要求銷毀不法或不當取得之個人資料（第三項）。」，亦明白揭示我國近來對於個人資料之基本保護的重視。

我國對於個人資料保護之核心法規範即爲民國八十四（1995）年所公布之「電腦處理個人資料保護法」，該法乃係最早於民國七十九（1990）年因爲行政院明確函示法務部對於資料保護法加以制定[1]，而在制定該資料保護法前先參考經濟合作開發組織（OECD）所規範之八大個人資料保護原則，訂定職權命令；法務部也在八十（1991）年成立審議小組起草委員會加以討論；八十一（1992）年完成「個人資料保護法草案」初稿，經多次折衝將草案名稱修正爲「電腦處理個人資料保護法」，於民國八十二（1993）年送立法院審議，方於八十四（1995）年通過[2]，並且由總統公布。

但是由於該「電腦處理個人資料保護法」公佈施行後因爲有諸多缺點，例如不能追上時代潮流，無法因應網際網路世界之快速改變；而在內容上，學者也對之有諸多批評，諸如規範之行政程序過於繁瑣、條文內容不明者所在多有[3]，故而呼籲改革之聲不斷，所以法務部針對「電腦處理個人資料保護法」正進行修

[1] 關於更早期對於科技法律之重視，詳參：＜中華民國立法院公報＞，第八十三卷，第四十五期，頁 521；另參：許文義，前揭書，頁 95。

[2] 中華民國八十四年八月十一日華總（一）義字第五九六０號令公布。

[3] 參：許文義，前揭書，頁 97。

正草案之研擬，希望能對這些缺憾加以補救，本文也對此加以追蹤，並加以論述評析。

另方面，若「電腦處理個人資料保護法」爲我國保護個人資料之中心法規範，則在其他個人資料處理上的特別領域，則亦有相關法規存在，即爲特別法與一般法之關係。在個人資料保護領域特別法中，較重要的例如「檔案法」、「通訊保障與監察法」二者。由於檔案是政府各級機關行使公務之書面或電子記錄，具有相當多諸如行政稽憑法律證據之功能，另一方面也是學術或教育研究之重要憑藉，而其中可能隱含相當大比例之個人資料在內，故而具重要性；另外，通訊秘密之保障也是個人隱私與個人資料中相當重要的一環，歐洲理事會之「電子通訊個人資料保護指令」、「電信事業個人資料保護指令」的立法精神即與此相若，故而特別提出加以說明。最後，由於本章欲呼應前章所討論之特別領域，亦即關於個人醫療資料、個人警察資料以及網際網路線上服務個人資料等，故也會討論相關國內之法規範。

## 二、 電腦處理個人資料保護法

### （一） 架構與內涵

我國「電腦處理個人資料保護法」全文分六章共四十五條，依照其章節架構，可分成：總則、公務機關之資料處理、非公務機關之資料處理、損害賠償及其他救濟、罰則與附則等。其中非常特殊的一點，就是該法將公務機關與非公務機關做一區別，並分別在不同章節中加以規範對於個人資料之蒐集，這在全世界的相關立法例中，是相當「特殊」的，因爲事實上在歐洲不論是「個人資料保護公約」、「個人資料保護指令」或是各國之相關法規範如：奧地利[4]、丹麥[5]、義大

[4] Federal Act concerning the Protection of Personal Data -Implementation of Directive 95/46/EC.
[5] The act on processing of personal data.

利[6]、西班牙[7]，甚至是全球其他諸如加拿大[8]、香港[9]、智利[10]等國之國內法規範均鮮少有特別將此項區別[11]作爲架構上之判斷依據，大多不分公務或非公務機關均一體適用，只在較特殊例外之處另爲規定，僅德國之「聯邦個人資料保護法」（BDSG）爲如上之區分，可見我國「電腦處理個人資料保護法」受德國「聯邦個人資料保護法」影響頗大。

但是在另一方面，「電腦處理個人資料保護法」卻未有如同其他大多數個人資料保護法規範一般的關於基礎原則之專章，而是散落在各章之中，就算是德國之「聯邦個人資料保護法」也在其總則之章節中對於各基礎原則做一說明（第3a 條至第十一條），在這點上，我國「電腦處理個人資料保護法」才算是真正的「突出」與「特殊」。

在條文內涵上，第一條規定了「電腦處理個人資料保護法」之立法目的乃是爲了「規範電腦處理個人資料，以避免人格權受侵害，並促進個人資料之合理利用」等，就此可知本法之重要目的之一即在防止人格權受侵害。另範圍應僅限於電腦所處理之自動化資料，並不包含人工處理之個人資料。不過在次條中卻規定「個人資料之保護，依本法之規定。」頗令人不解，因爲所謂個人資料之保護文義上似應包含自動化處理與人工處理二者，則又如何在非自動化處理個人資料保護方面依本「電腦處理個人資料保護法」加以規範？故而筆者認爲，若仍欲依本法之現行範圍爲規範，則第二條文字上亦應限縮於電腦處理之個人資料。而由於本「電腦處理個人資料保護法」爲關於個人資料保護的一般法規定，所以第二條但書稱「但其他法律另有規定者，依其規定」。

[6] Protection of individuals and other subjects with regard to the processing of personal data act.
[7] Organic Law 15/99 on the Protection of Personal Data.
[8] The Personal Information Protection and Electronic Documents Act.
[9] Personal Data (Privacy) Ordinance.
[10] Act on the Protection of Personal Data.
[11] 以下關於法規架構上，對於「電腦處理個人資料保護法」之建議，詳參本文第五章。

第三條則爲相關定義之規範，規範有包括個人資料、電腦處理、蒐集、利用、公務機關、非公務機關、當事人、特定目的等名詞之定義，較爲特殊的是在個人資料的定義上面採取了列舉自然人之姓名、出生年月日、身分證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社會活動及其他足資識別該個人之資料等，而非僅區別是否足資識別特定個人。另一項重要定義則是所謂的「非公務機關」是指非上述公務機關且需滿足下列三者之一：1.徵信業及以蒐集或電腦處理個人資料爲主要業務之團體或個人；2.醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業；3.其他經法務部會同中央目的事業主管機關指定之事業、團體或個人。

第四條則就當事人權利加以規定，謂「查詢及請求閱覽、請求製給複製本、請求補充或更正、請求停止電腦處理及利用、請求刪除等權利，不得預先拋棄或以特約限制之」，其中隱含了個人資料保護之許多基本原則，將於次節中詳述。第五條規定處理資料人之範圍；第六條則是誠信原則及必要性原則之揭示。

第七至十七條爲公務機關資料處理之相關規定在第七條（收集資料之原則）、第八條本文（特定目的原則）、第九條（依法原則）、第十二條本文（資料品質原則）、第十三條（資料品質原則；安全確保原則）、第十四條（公告）、第十五條（期限與書面）第十七條（安全確保原則）爲公務機關對於個人資料處理上之限制與處理之原則；而相對地，第八條但書、第十一條、第十二條但書、第十三條第二項但書、第十三條第三項但書則爲這些原則上處理個人資料限制的例外。

值得注意的是，這些例外所佔的篇幅與規定之多樣以及所隱含的不確定法律概念相當的多，例如所謂「爲維護國家安全者」、「爲增進公共利益者」、「爲防止他人權益之重大危害而有必要者」、「爲學術研究而有必要且無害於當事人之重大利益者」、「有利於當事人權益者」等其他國家相關法規常見的不確定法

律概念之外，尚有「關於公務機關之人事、勤務、薪給、衛生、福利或其相關事項者」、「爲公務上之連繫，僅記錄當事人之姓名、住所、金錢與物品往來等必要事項者」等，在比例上甚至比處理個人資料所應有之基本原則多。

另外甚至在基本原則的構成要件上，也有不利於資料當事人之構成要件，例如有學者[12]即認爲第七條第三款「對當事人權益無侵害之虞者」，其判斷及認定顯然有利於公務機關，這點相當令人不解，甚至可能造成公務機關權力較被蒐集資料之當事人大上甚多。對照之下，與我國同樣區分公務與非公務機關專章的德國「聯邦個人資料保護法」則亦與我國「電腦處理個人資料保護法」相反之方式，對於公務機關蒐集或處理個人資料採取相當嚴謹之態度，例如「聯邦個人資料保護法」第十三條關於資料之蒐集，以該條第二項所列舉九項事項爲限，且並無所謂利於公務機關判斷之不確定法律概念，其第十四條對於個人資料之儲存變更利用亦同，並對於各種例外規範之比例並不若我國「電腦處理個人資料保護法」來的多，相較之下，我國「電腦處理個人資料保護法」相當具有可以檢討的空間。本章除上述條文外，「電腦處理個人資料保護法」第十六條爲當事人向公務機關查詢或復本之費用之規定。

第十八至廿六條爲非公務機關之資料處理相關規範，與上章相反的是，「電腦處理個人資料保護法」在本章多是禁止規定。第十八條爲非公務機關對於個人資料之蒐集或電腦處理之原則，需有特定目的，並符合經當事人書面同意、與當事人有契約或類似契約之關係而對當事人權益無侵害之虞、已公開之資料且無害於當事人之重大利益、爲學術研究而有必要且無害於當事人之重大利益，以及依本法第三條第七款第二目有關之法規及其他法律有特別規定等要件之一。該條之例外規定於第廿三條，於爲增進公共利益、爲免除當事人之生命、身體、自由或財產上之急迫危險、爲防止他人權益之重大危害而有必要，以及當事人書面同意

[12] 參：莊庭瑞，＜個人資料保護在台灣：誰的事務？＞，《國家政策季刊》，行政院研考會，第二卷第一期，2003 年 3 月，頁 57。

等要件之一時，得於特定目的外之利用。

第十九至廿二條爲登記之相關事項；第廿四條則規定非公務機關第三國之國際個人資料傳遞，對照第九條公務機關跨國傳輸之「應依相關法令爲之」的簡單規定，其規定有涉及國家重大利益、國際條約或協定有特別規定、接受國對於個人資料之保護未有完善之法令，致有損當事人權益之虞，及以迂迴方法向第三國傳遞及利用個人資料規避本法時，目的事業主管機關即得限制之，顯得相當之「精細」。第廿五條爲檢查與扣押非公務機關持有之個人資料的規定，並由目的事業主管機關爲之；廿六條爲準用之規定。

第四章中第廿七至第三十二條規定損害賠償與其他救濟。其中筆者想提出一有趣問題：試問，公務機關侵害個人資料致生損害何價？依第廿七條規定：被害人雖非財產上之損害，亦得請求賠償相當之金額，其名譽被侵害者，並得請求爲回復名譽之適當處分。至於「價碼」方面，不待法官認定，本法第廿七條第三項已然規定「前二項損害賠償總額，以每人每一事件新臺幣二萬元以上十萬元以下計算」，所以個人資料平均價碼爲此。雖然能證明其所受之損害額高於該金額者，不在此限（第廿七條第三項），不過第四項卻規定「基於同一原因事實應對當事人負損害賠償責任者，其合計最高總額以新臺幣二千萬元爲限」，對於牽連可能甚廣的個人資保護案件來說，顯的相當「便宜[13]」，對此草案也有相關之修正，詳後述。

第五章第三十二條至第四十一條爲有關罰則之規定，其中重要者第三十六條：本章之罪，需告訴乃論。第六章爲附則由第四十二條知法務部爲「電腦處理

[13] 與個人資料保護同屬牽連甚廣的消費者保護案例或是公平交易案例動輒數千萬罰款來說，個人資料保護相關案件非但無專屬之主管機關如消基會或公平會，連「價碼」都輸了許多，當然顯的微不足道。參：記者林淑玲／台北報導，＜老鼠會負責人廖文志無視公權力囂張吸金　公平會罰 5000 萬＞，2003/07/24，東森新聞報：
喧騰一時的「共享人生」、「超越世紀」公司網路老鼠會吸金案，去年年初遭公平會重罰 2500 萬元，並於今年 4 月遭起訴後，不僅未改正反而改頭換面成立新公司持續吸金，甚至還成立富民黨，擺明挑戰公權力，公平會 24 日認爲負責人廖文志惡行重大，爲避免他一犯再犯，決定重罰 5000 萬元，罰金創紀錄。

個人資料保護法」所設最重要之公務機關因爲法務部辦理協調連繫本法執行之相關事項；其協調連繫辦法，由法務部定之（第一項）；依本法規定應由目的事業主管機關辦理之事項，如無目的事業主管機關者，由法務部辦理之（第二項）。並且，本法之施行細則乃是由法務部定之（第四十四條），法務部除了訂定施行細則外，並依第四十二條第一項訂定「執行電腦處理個人資料保護事項協調聯繫辦法」。

（二） 修正草案

由於「電腦處理個人資料保護法」有著諸多學界所論述之缺失，故法務部也對此做出相關修正草案以爲因應，在民國 92 年 4 月 10 日即發表新聞稿，研擬「電腦處理個人資料保護法部分條文修正草案」，其指出「…因電腦科技的日新月異，尤其網際網路的蓬勃發展，現行電腦處理個人資料保護法對個人資料隱私之保護，確有不周延之處，實務上亦發生許多窒礙難行之困難。」有鑑於此，法務部從 90 年度起，即將修正電腦處理個人資料保護法納入重要政策之一。該草案迭於 90 年 3 月間，由法務部分別函請各公務機關、適用該法之民間業者，就實務上之問題與修法建議提供意見並彙整研究。90 年 10 月、11 月邀請專家學者、各公務機關與民間業者舉行四場公聽會，聆聽各界意見。91 年 3 月蒐集德國、奧地利、荷蘭、丹麥、西班牙、日本、澳大利亞及紐西蘭等八國有關保護個人資料立法例，以作爲修法之參考。91 年 9 月，法務部完成「電腦處理個人資料保護法部分條文修正草案」初稿條文，並邀請專家學者開會就該草案條文進行討論。經過十二次研商會議後，於 92 年 4 月 9 日修正確定該初稿條文內容。並於 92 年 5 月 20 日公布該草案之修正總說明。法務部也計畫於 92 年 12 月前，將該修正草案陳報行政院審查。草案修法重點如下：

首先第三條第一項將資料當事人之範圍擴大爲不論直接或間接識別個人均在保護之列取代原本「足資識別該個人之資料」之不確定解釋而改爲「足資直接

或間接識別該個人之資料。」以確實保障個人資料。

在非公務機關之範圍部分草案第三條第八項做出更清楚之界定，將原本限縮在八大行業的非公務機關擴張爲公務機關以外之自然人、法人、機構、或其他團體。草案認爲由於利用電腦蒐集個人資料之情形已經日益普遍故而原本限制行業別之作法已經不合時宜且易疏漏故將其範圍擴大。並且也在第二條的部分，做了將自然人單純爲個人或家庭之活動剔除在外之配套措施，而在原本第十九至第廿二條的部分也配合非公務機關範圍之修改而刪除。

另外在個人資料的蒐集方面，則有較以往詳盡許多之新增規定，諸如在第六條之一便規定有個人資料蒐集之書面同意相關規定及定義。在定義上，第六條之一第一項「書面同意，指當事人經蒐集機關以書面明確告知依本法應告知之事項後，在自由選擇下所爲之意思表示。」對之加以釐清，並將特定目的之外之個人資料收集另行規定爲「特定目的外利用個人資料需當事人書面同意者，應於書面中特別表明其利用目的、範圍及同意與否對其權益之影響，並就該利用單獨取得同意。（第二項）」也特別於第三項中對於資料當事人爲兒童（未成年人）時，對之加強保護，應由法定代理人爲書面同意。

而在第六條之二與第六條之三則增訂蒐集資料時不論是直接或間接蒐集，均須明確告知當事人蒐集目的；蒐集機關名稱；個人資料之類別；個人資料利用之期間、地區、對象及方式；當事人依第四條規定得行使之權利、方式及其對象；當事人提供資料係基於自由選擇或義務，及提供或不提供資料時對其權益之影響等等，並規範相關之例外情形，如依法規規定得免告知者；依法規規定，資料之蒐集、電腦處理或利用係公務機關之法定職務者；依法規規定，資料之蒐集、電腦處理或利用係非公務機關之法定義務者；告知將有損國家安全或公共利益者；告知將妨害公務機關執行法定職務者；告知有妨害第三人之重大利益之虞者。當事人明知或可得而知應告知之內容者等。

草案也增訂犯罪前科、健康、醫療及基因四類資料爲特種資料[14]，不符合「法規明文規定者；經當事人書面同意者。但法規禁止蒐集、電腦處理或利用者，不在此限；依法規規定，公務機關執行法定職務或非公務機關履行法定義務所必要者；當事人自行公開者；爲統計或學術研究之目的，且資料經電腦處理後或依其公布方式無從識別特定當事人者」之法定要件時，不得蒐集、電腦處理或利用之規定（第六之四條）。

而由於現行條文僅規定公務機關應維護個人資料之正確，但是卻對於違法蒐集與利用之個人資料並未規定應如何補救與處理，故而在草案第十三條第四項明訂「違反本法規定蒐集、電腦處理或利用個人資料者，公務機關應依職權或當事人之請求，刪除或停止電腦處理及利用該資料。」。

在公告方式中，草案第十四條也新增「公開於電腦網站，供公眾查閱。」以符合目前網際網路普遍應用之趨勢便利民眾查閱。

至於在目的事業主管機關權責部分，草案第廿五條則賦予目的事業主管機關檢查權，「發現非公務機關違反本法規定有侵害當事人權益之虞或認有必要時，得派員攜帶證明文件，進入該非公務機關檢查，並得命相關人員爲必要之說明、配合措施或提供資料，必要時並得扣留或複製非公務機關電腦處理之個人資料或其檔案。（第一項）」；第廿五條之一則賦予其必要之處分權：「目的事業主管機關爲前條檢查時，發現非公務機關有違反本法規定之情事者，除依本法規定課處罰鍰外，並得爲下列處分：一、禁止蒐集、電腦處理及利用個人資料。二、沒入違法蒐集之個人資料。三、命刪除經電腦處理之個人資料檔案。四、公布姓名、名稱及違法情形。（第一項）」，並規定有最小侵害之比例原則於第二項。

在損害賠償部分，草案第廿七條規定違反本法規定蒐集、電腦處理或利用

[14] 此即所謂特種資料處理原則。

個人資料，侵害當事人權利者，雖不能證明非財產上之損害，亦得請求新台幣二萬元至十萬元之金額，並對同一侵害原因事實，將賠償總額提高爲新台幣五千萬元，而行政爭訟也明文以第三十一條規範。

至於救濟程序方面第三十二條則規定有向目的事業主管機關之舉發權且該目的事業主管機關接獲前項舉發後，應依第二十五條規定處理，並將處理結果以書面通知當事人。而第三十二條之一也鼓勵民眾多利用公益法人代爲主張集體訴訟之權利：「以公益爲目的之法人，保護個人資料事項，係其章程所定設立目的之一者，得接受當事人之委任，代爲行使當事人依據本法可得主張之權利、提起相關訴訟或救濟。（第一項）」，以提高行政效率與節省資源，並得免除相關訴訟費用：「法人依前項規定，就同一原因事實，接受二十人以上之委任者，對公務機關行使本法規定之各項權利，應免除費用；提起民事訴訟，第一審免裁判費，第二審其標的價額超過新台幣六十萬元者，超過部分免繳裁判費。（第二項）」。

而爲了加強非公務機關行爲人與負責人之守法以保障個人隱私，草案第三十八至四十條則對之加以更重之罰則，併予裁處行政罰鍰。

總計本次草案一共刪除五條，修正廿九條，增訂六條，共四十條，修改幅度相當之大，更可發現我國原「電腦處理個人資料保護法」已難以符合現狀。

至於較舊版本之修正草案內容與上述新版之修正草案有許多差異，舊版本可參考法務部編印「檢討電腦處理個人資料保護法實施狀況公聽會會議實錄彙編[15]」之附錄三[16]，茲不贅述。

[15] 法務部法律事務司，《檢討電腦處理個人資料保護法實施狀況公聽會會議實錄彙編》，台北：法務部，2002 年 2 月。
[16] 同上註，頁 173-184。

## 三、 相關法規

### （一）檔案法與通訊保障及監察法

「電腦處理個人資料保護法」乃係專門規定有關保護個人資料之基本法規範已如上述，在相關特別法中與個人資料保護最有關係者，應當爲「檔案法」與「通訊保障及監察法」二者，蓋檔案者，依照「檔案法」第二條第二項乃是指各機關依照管理程序，而歸檔管理之文字或非文字資料及其附件，其中當會包含「電腦處理個人資料保護法」第三條第二項所稱之「基於特定目的儲存於電磁紀錄物或其他類似媒體之個人資料之集合」的個人資料檔案；另外，隱私權保障除了個人資料之保護以外，秘密通訊之保護則由「通訊保障及監察法」加以規範，而透過通訊之監察可蒐集許多個人資料並加以儲存利用，故而吾人稱「通訊保障及監察法」爲相關重要之特別法。

檔案是政府機關的一種重要知識資產，如何予以妥適管理與有效運用，將是建制現代化檔案管理制度不可或缺的議題。尤其資訊化及知識經濟時代已然來臨，知識成爲政府組織的關鍵資源之一，所以檔案之相關規範愈形重要，並且由於前述檔案中可能含有大量涉及個人隱私之個人資料，所以其管理上更需加以重視。「檔案法」於民國 88 年 12 月 15 日公布，民國 90 年 11 月 2 日施行爲檔案管理之特別立法立法目的爲健全政府機關檔案管理，促進檔案開放與運用，發揮檔案功能（第一條），相關名詞定義於第二條。其餘法條內涵由於篇幅所限，詳參「檔案法」此不贅述。值得注意者，該法主管機關爲行政院國家檔案局，該局並已經建置了全國民眾查詢檔案資訊系統，並已經上網[17]供民眾直接或申請查詢。該法另有子法「檔案電子管理儲存實施辦法」共計廿條，於民國 90 年 12 月 12 日公布，爲與「電腦處理個人資料保護法」較有關連性之子法。

[17] 全國檔案目錄查詢網： URL: http://near.archives.gov.tw/index.html.

在「通訊保障及監察法」方面，「通訊保障及監察法」於民國 88 年 7 月 16 日公布，共三十四條。因爲通訊科技的日益發達，在政府與人民間或私人關係之間的秘密通訊隱私已經與個人資料隱私一般，遭受空前之侵害可能性，並且由於通訊之監察常可能成爲犯罪之證據，涉及相當多個人犯罪資料以及相關之個人警察資料（police data），在透過通信科技結合電腦後，更加可怕，故而需透過「通訊保障及監察法」之制定，作爲保障個人隱私以及個人資料手段之一，以保障人民秘密通訊之自由，維護社會治安及奠定國家安全。

而由於「通訊保障及監察法」原本賦予檢察關於偵查中有核發通訊監察書之權，但是因該核發權爲影響人民基本權利甚大之強制處分權，理應由法院行使，故於「通訊保障及監察法」修正草案中將該核發權修正爲由法官行使。

在該修正草案中除上述修正外，也並行修正得實施通訊監察之罪名、情報監察之窒礙難行處、通訊監察書應記載之內容、通訊監察期間屆滿前停止監察之程序、電信郵政事業協助執行監察之規定、通訊監察結束後通知受監察人之規定、通訊監察監督之規定、通訊監察免責事由之規定、電信郵政事業之罰則規定、軍事審判機關通訊監察準用之規定與施行日之規定等；並增訂檢察官向法院聲請通訊監察書經駁回者不得抗告之規定、得實施緊急通訊監察之事由、「監察處所」與「執行機關」之定義規定、得於私人住宅裝置通訊監察器材之規定、通訊器材製造商關聯廠商之義務等等。

（二）醫療資料相關法規

在我國個人資料保護相關法規範中，與個人醫療資料有關之專法爲「醫院電腦處理個人資料登記管理辦法[18]」。該辦法乃係依照「電腦處理個人資料保護法」第十九條第三項、第二十條第五項、第二十六條第二項及「電腦處理個人資

[18] 中華民國八十五年十二月四日行政院衛生署 (85) 衛署醫字第 85067270 號令訂定發布全文 14 條。

料保護法施行細則」第八條第二項規定所訂定。扣除程序上以及收費上等條文，「醫院電腦處理個人資料登記管理辦法」與個人資料保護實質上有相關者爲第八條[19]、第九條[20]與第十一條[21]等；其中第八條與第九條爲接近原則（right to access）之原則與例外規定，第十一條則是安全原則之揭示。

另外在其他醫療相關法規中「醫療法」爲最重要基本規範之一，其中對於個人醫療資料之保護大多集中於病歷資料部分[22]在第四十八至第五十二條中爲相關之規定而「醫療法施行細則」第四十四條、第四六至四八條亦有相關規定。「醫療法」第四十八條[23]爲病歷之保管以及內容之資料品質原則的實踐；四十九條[24]則爲保密義務；第五十至五十二條[25]爲轉診或出院時應提供病歷之義務。又「醫師法」第十二條[26]則規定個人病歷資料之內容；「傳染病防治法」第三十一

[19] 當事人就其個人資料依本法（『電腦處理個人資料保護法』）第四條規定向醫院請求查詢、閱覽及製給複製本，應提出身分證明文件，並檢具費用及申請書申請（第一項）。前項之申請，醫院應於三十日內處理之；未能於該期間內處理者，應將其原因以書面通知請求人（第二項）。當事人查詢、閱覽其電腦處理病歷，應於醫院指定之地點，並由醫院人員陪同下爲之（第三項）。

[20] 前條之請求，除有下列情形之一者外，醫院不得拒絕：一 、 有妨礙業務執行之虞者。二 、 有妨害第三人重大利益之虞者。三 、 申請書件未齊備者。四 、 其他與法令規定不符者。

[21] 醫院保有之個人資料檔案，應指定專人依相關法令辦理安全維護事項，防止資料被竊取、竄改、毀損、滅失或洩漏。

[22] 學者有謂「醫療法」及施行細則對於病歷隱私分爲檔案管理（「醫療法」第四十八至五十二條）品質管理（「醫療法施行細則」第四六至四八條）與疾病分類（「醫療法施行細則」第四十四條）三類。詳參：陳楚杰，《病歷管理》，台北：宏翰出版社，1995，頁 10-15，轉引自：吳昊，＜由醫療資訊隱私權之觀點論全民健保 IC 卡政策＞，台灣大學法律學研究所碩士論文，2001 年 7 月，頁 143-144。

[23] 醫院、診所之病歷，應指定適當之場所及人員保管，並至少保存十年（第一項）。病歷內容應清晰、詳實、完整。醫院之病歷並應製作各項索引及統計分析，以利研究及查考（第二項）。

[24] 醫療機構及其人員因業務而知悉或持有他人之秘密，不得無故洩露。

[25] 第五十條：醫院、診所因限於設備及專長，無法確定病人之病因或提供完整治療時，應建議病人轉診。但危急病人應依第四十三條第一項規定，先作適當之急救處置，始可轉診。前項轉診，應填具轉診病歷摘要，交予病人，不得無故拖延或拒絕。

第五十一條：醫院、診所診治病人時，得依需要，並經病人或其配偶、親屬之同意，商洽病人原診治之醫院、診所，提供病歷摘要及各種檢查報告資料。原診治之醫院、診所不得拒絕；其所需工本費，由病人負擔。

第五十二條：醫院對出院病人，應依病人要求，掣給出院病歷摘要。醫院對尚未治癒而要求出院之病人，得要求病人或其關係人，簽具自動出院書。

[26] 醫師執行業務時，應製作病歷，並簽名或蓋章及加註執行年、月、日。

前項病歷，除應於首頁載明病人姓名、出生年、月、日、性別及住址等基本資料外，其內容至少應載明下列事項：

一 、 就診日期。二 、 主訴。三 、 檢查項目及結果。四 、 診斷或病名。五 、 治療、處置或用藥等情形。六 、 其他應記載事項。

病歷由醫師執業之醫療機構依醫療法規定保存。

條[27]對於傳染病歷資料則規定不得無故洩漏；「後天免疫缺乏症候群防治條例」第六條[28]亦有相似之規定，併此敘明。

最後，我國關於個人基因資料之強制收集，則與個人警察資料相結合。我國「去氧核醣核酸採樣條例」第五條規定，下列之人應接受去氧核醣核酸之強制採樣：一、 性犯罪[29]或重大暴力犯罪案件[30]之被告；二、 性犯罪或重大暴力犯罪案件之犯罪嫌疑人；並且，依本法建置去氧核醣核酸資料庫去氧核醣核酸人口統計資料庫（第十一條第一項）。而本條例關於個人資料保護條文在第十一條第二項「前項樣本、紀錄及資料庫，主管機關（內政部）非依本條例或其他法律規定，不得洩漏或交付他人；保管或持有機關亦同。」及第十二條「依本條例採樣、儲存之去氧核醣核酸樣本、紀錄，前者至少應保存十年，後者至少應保存至被採樣人死亡後十年（第一項）。依本條例接受採樣之人，受不起訴處分或經法院無罪判決確定者，得檢具確定證明文件及第八條第一項之證明書，申請主管機關刪除其去氧核醣核酸樣本及紀錄（第二項）。第八條第一項之證明書，應記載被採樣人前項之權利（第三項）。」

（三）警察資料相關法規

在國內警察相關法規中涉及個人資料者如「警察職權行使法」，於民國九十二年六月公布同年十二月方施行，乃是較爲新進之法律。其第二章爲有關警察行使身份查證及資料蒐集之事項，於個人資料方面，第九至十一條爲個人犯罪資料

[27] 各級主管機關、醫療 (事) 機構、醫事人員及因業務知悉傳染病病人之姓名及病歷有關資料者，對於該資料，不得無故洩漏。

[28] 各級衛生主管機關、醫療機構、醫事人員及因業務知悉感染人類免疫缺乏病毒者之姓名及病歷有關資料者，對於該項資料，不得無故洩漏。

[29] 依「去氧核醣核酸採樣條例」第三條第七項指刑法第二百二十一條至第二百二十九條及其特別法之罪。

[30] 依「去氧核醣核酸採樣條例」第三條第八項指刑法第二百七十一條至第二百七十三條、第二百七十七條第二項、第二百七十八條、第三百二十五條第二項、第三百二十八條至第三百三十四條、第三百四十七條、第三百四十八條及其特別法之罪。

之蒐集，第九條[31]是對集會遊行或其他公共活動參與者之行爲之資料之收集；第十條[32]則是所謂最容易侵犯個人的隱私「老大哥條款」：對於經常發生或經合理判斷可能發生犯罪案件之公共場所或公眾得出入之場所，爲維護治安之必要時，得協調相關機關 (構) 裝設監視器，或以現有之攝影或其他科技工具蒐集資料；而十一條[33]乃對於犯罪行爲之防止而得蒐集個人資料之規範。第十二條至第十三條[34]則對俗稱線民的警察以外第三人收集個人資料加以規範。第十六條[35]爲資料傳遞之目的性原則；十七條[36]爲資料利用之目的性原則；第十八條[37]則是對於個

[31] 警察依事實足認集會遊行或其他公共活動參與者之行爲，對公共安全或秩序有危害之虞時，於該活動期間，得予攝影、錄音或以其他科技工具，蒐集參與者現場活動資料。資料蒐集無法避免涉及第三人者，得及於第三人。
依前項規定蒐集之資料，於集會遊行或其他公共活動結束後，應即銷毀之。但爲調查犯罪或其他違法行爲，而有保存之必要者，不在此限。依第二項但書規定保存之資料，除經起訴且審判程序尚未終結或違反組織犯罪防制條例案件者外，至遲應於資料製作完成時起一年內銷毀之。

[32] 警察對於經常發生或經合理判斷可能發生犯罪案件之公共場所或公眾得出入之場所，爲維護治安之必要時，得協調相關機關 (構) 裝設監視器，或以現有之攝影或其他科技工具蒐集資料。
依前項規定蒐集之資料，除因調查犯罪嫌疑或其他違法行爲，有保存之必要者外，至遲應於資料製作完成時起一年內銷毀之。

[33] 警察對於下列情形之一者，爲防止犯罪，認有必要，得經由警察局長書面同意後，於一定期間內，對其無隱私或秘密合理期待之行爲或生活情形，以目視或科技工具，進行觀察及動態掌握等資料蒐集活動：
一　有事實足認其有觸犯最輕本刑五年以上有期徒刑之罪之虞者。
二　有事實足認其有參與職業性、習慣性、集團性或組織性犯罪之虞者。
前項之期間每次不得逾一年，如有必要得延長之，並以一次爲限。已無蒐集必要者，應即停止之。
依第一項蒐集之資料，於達成目的後，除爲調查犯罪行爲，而有保存之必要者外，應即銷毀之。

[34] 第十二條：警察爲防止危害或犯罪，認對公共安全、公共秩序或個人生命、身體、自由、名譽或財產，將有危害行爲，或有觸犯刑事法律之虞者，得遴選第三人秘密蒐集其相關資料。
前項資料之蒐集，必要時，得及於與蒐集對象接觸及隨行之人。
第一項所稱第三人，係指非警察人員而經警察遴選，志願與警察合作之人。經遴選爲第三人者，除得支給實際需要工作費用外，不給予任何名義及證明文件，亦不具本法或其他法規賦予警察之職權。其從事秘密蒐集資料，不得有違反法規之行爲。
第三人之遴選、聯繫運用、訓練考核、資料評鑑及其他應遵行事項之辦法，由內政部定之。
第十三條：警察依前條規定遴選第三人秘密蒐集特定人相關資料，應敘明原因事實，經該管警察局長或警察分局長核准後實施。蒐集工作結束後，警察應與第三人終止合作關係。但新發生前條第一項原因事實，而有繼續進行蒐集必要且經核准者，得繼續合作關係。
依前條第一項所蒐集關於涉案對象及待查事實之資料，如於相關法律程序中作爲證據使用時，應依相關訴訟法之規定。該第三人爲證人者，適用關於證人保護法之規定。

[35] 警察於其行使職權之目的範圍內，必要時，得依其他機關之請求，傳遞與個人有關之資料。其他機關亦得依警察之請求，傳遞其保存與個人有關之資料。
前項機關對其傳遞個人資料之正確性，應負責任。

[36] 警察對於依本法規定所蒐集資料之利用，應於法令職掌之必要範圍內爲之，並須與蒐集之特定目的相符。但法律有特別規定者，不在此限。

[37] 警察依法取得之資料對警察之完成任務不再有幫助者，應予以註銷或銷毀。但資料之註銷或銷毀將危及被蒐集對象值得保護之利益者，不在此限。
應註銷或銷毀之資料，不得傳遞，亦不得爲不利於被蒐集對象之利用。
除法律另有特別規定者外，所蒐集之資料，至遲應於資料製作完成時起五年內註銷或銷毀之。

人相關之資料之銷毀。

另外「警察機關資訊安全實施規定」第六條第五款則稱：「警察機關要求整批方式查詢資料或非警察機關請求查詢資料時，均應備文，經該電腦資料業務單位同意，並符合『電腦處理個人資料保護法』之規定；所查資料屬於『機密』等級以上者，應依『警察機關維護公務機密實施要點』規定簽報機關首長核准。」

（四）電腦電信資料相關法規

與個人資料相關之我國電信電腦法規計有下列[38]：「行政院暨所屬各級行政機關電腦處理個人資料保護要點」(80/07/25) 、「金融業申請電腦處理個人資料登記程序許可要件及收費標準」(85/07/24)、「保險業申請電腦處理個人資料登記程序及收費標準」(85/07/27)、「保險業接受個人資料查詢閱覽製給複製本之程序及收費標準」(85/07/27)、「保險業個人資料檔案安全維護計畫標準」(85/07/27)、「金融業個人資料檔案安全維護計畫標準」(85/08/12)、「金融業接受個人資料查詢閱覽製給複製本之程序及收費標準」(85/08/15)、「證券業暨期貨業申請電腦處理個人資料登記程序及收費標準辦法」(87/01/15)、「證券業暨期貨業個人資料檔案安全維護計畫標準」(87/01/15)、「證券業暨期貨業接受個人資料查詢閱覽製給複製本之程序及收費標準辦法」(87/01/15)、「私立學校及學術研究機構電腦處理個人資料管理辦法」(88/06/29)、「執行電腦處理個人資料保護事項協調連繫辦法」(89/12/20)、「電腦處理個人資料保護法之特定目的」(85/08/07)、「徵信業電腦處理個人資料辦法」(88/06/30)、「電信業電腦處理個人資料管理辦法」(86/09/08)、「行政院新聞局電腦處理個人資料管理要點」(90/11/30)、「大眾傳播業電腦處理個人資料管理要點」(90/12/13)等。

[38] 以下法規後之括號內數字爲公布之日期，以民國爲單位。

### 四、 小結

縱觀本節我國個人資料相關法規可謂琳瑯滿目，按理說應當對於個人資料保護有相當程度之助益，惟以「電腦處理個人資料保護法」爲例，其法規內涵仍有諸多缺失，最明顯者爲對於公務機關之權力仍有過重過大之嫌，另外對於基本原則之確定並未明示餘條文之中等等。

由於我國立法上對於個人資料保護有如上缺憾，故而本文即希望能以歐洲立法之相關經驗對於我國法制之改進做一建議，詳參本章第四節。

## 第二節　與歐洲法制之契合與銜接

### 一、 概說

我國「電腦處理個人資料保護法」等相關個人資料保護規範已論述如上節。本節將對於我國法制與歐洲法制之間的契合問題與銜接問題做一討論，在法規範契合方面，檢視我國「電腦處理個人資料保護法」與「個人資料保護公約」及「個人資料保護指令」在立法意旨、架構以及對基本原則之闡述上之異同，觀察是否法規之間有足夠之契合度，以評量我國對個人資料保護法制與國際相關法規是否有過大落差抑或已有長足進步。

至於在本文所謂的銜接面部分，則將焦點集中於個人資料之國際傳遞問題上，檢視我國「電腦處理個人資料保護法」與「個人資料保護公約」及「個人資料保護指令」，觀察在傳遞上之法規是否有抵觸或障礙之處，以及我國相關法規

在保障上是否能符合歐洲之要求與標準，期望能進一步達到國際資訊自由流通以促進包括貿易、經濟、社會文化等各方面之交流發展與個人資料隱私保護之平衡。

## 二、 與歐洲理事會相較

### （一） 法規契合面

首先在立法目的方面，「個人資料保護公約」由於是屬國際性之文件，故而含有相當濃厚促進資訊跨國流通之個人資料隱私保護之著眼點，而我國「電腦處理個人資料保護法」由於是國內法，故重心偏向規範法律基本保障之人格權等人權議題之規範，這是在法律本質本有之上不同處。但是我國「電腦處理個人資料保護法」立法目的並未明確說明在促進資訊流通與資料保護之橫平上所持觀點，僅簡單說明「促進個人資料之合理利用」，此與「個人資料保護公約」明確對資訊自由之承諾，並應協調尊重隱私之基本價值與個人間資訊之自由流通略有不同，顯見我國對於個人資料保護之層次與觀念仍落後國際潮流甚多。

較爲重要之部分應當爲基本原則之相關規定方面，我國「電腦處理個人資料保護法」因爲並未明白條列如「個人資料保護公約」般關於個人資料保護之基本原則，故若以「電腦處理個人資料保護法」爲個人資料保護之中心規範，則需要透過實務上或學理上之解釋，以釐清相關基本原則。

在「個人資料保護公約」資料品質原則的各子原則方面，蒐集與處理之公平性與合法性原則出現於我國「電腦處理個人資料保護法」第七條第二款與十八條第五款的「經當事人書面同意」、第六條之「尊重當事人權益」、「依誠實及信用方法」等，另外第四條之當事人相關權利不得預先請求拋棄或特約限制之相干權利，如查詢及請求閱覽、請求製給複製本、請求補充或更正、請求停止電腦處理及利用、請求刪除等，均包含於資料品質原則之中，故可視爲對於資料品質原

則的一種體現；目的性原則出現於「電腦處理個人資料保護法」第七條與第十八條；必要性原則出現於第六條後段；內容正確原則出現於第十三條與第廿六條；儲存逾期禁止原則則規定於第十三條第三項。

至於特種資料處理原則，並未規範於「電腦處理個人資料保護法」上，然於該法之修正草案中第六條之四則規定特種資料包含犯罪前科、健康、醫療及基因等四類資料，但與「個人資料保護公約」之健康、性生活、種族、政治意見、宗教信仰等分類有範圍較小之差異，尤其我國過去受政治迫害之歷史可謂「淵遠流長」，則此修正草案似有未盡全功之憾。另安全確保原則於「電腦處理個人資料保護法」亦未規定，但於舊版修正草案第十七條中則規定「公務機關保有個人檔案資料者，應指定專人依相關法令辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失、販賣或洩漏」。

在排除原則方面，我國「電腦處理個人資料保護法」則相對「精細」的多，包括第八條但書、第十一條、第十二條但書、第十三條第二項但書、第十三條第三項但書等，詳細列出相當多限制與例外之情況，幾乎所有可能情況均已納入，並多有不確定法律概念，造成有所謂「例外變原則」之現象出現。

最後在立約國義務原則與延伸保護原則方面，由於「電腦處理個人資料保護法」本質上並非如「個人資料保護公約」般爲國際性文件，故並無存在。

（二） 法規銜接面

「個人資料保護公約」對於跨國之國際個人資料傳遞由於其本質上是屬於公約之形式，故而僅對簽約國發生效力。在其第三章（第十二條）對於資料跨國流通之規定中，規定締約國不論經由任何媒介，凡經過自動化處理或基於自動化處理目的而收集之個人資料跨國傳遞之時，不得純粹爲保護隱私而禁止或限制個人資料之跨國流通，必須顧及兩者間之平衡；締約國於其本國立法已就特定類型

之資料設有特別規定，且其他締約國無相同程度之保護時，或有規避締約國關於個人資料保護之情形時，方可對資料跨國流通加以限制。

對照我國「電腦處理個人資料保護法」之相關規定，則有若干與該「個人資料保護公約」銜接上之問題。首先我國資料跨國傳遞仍區分公務機關以及非公務機關兩大類，而非如「個人資料保護公約」般一體適用。在公務機關方面，「電腦處理個人資料保護法」第九條規定「公務機關對個人資料之國際傳遞及利用，應依相關法令爲之」；非公務機關方面第廿四條規定「非公務機關爲國際傳遞及利用個人資料，而有左（下）列情形之一者，目的事業主管機關得限制之：一、涉及國家重大利益者；二、國際條約或協定有特別規定者；三、接受國對於個人資料之保護未有完善之法令，致有損當事人權益之虞者；四、以迂迴方法向第三國傳遞及利用個人資料規避本法者」，及其施行細則第十三條所謂「本法第九條及第二十四條所稱國際傳遞及利用，指利用有線電、無線電、光學系統或其他電磁系統等經由通信網路傳遞及利用，不包括利用郵寄、攜帶傳輸微縮膠片、打孔卡片、電腦報表、電磁紀錄物傳遞之情形」。

綜合以觀，我國跨國個人資料傳遞之傳播媒介受規範者爲用有線電、無線電、光學系統或其他電磁系統等經由通信網路傳遞及利用，不包括利用郵寄、攜帶傳輸微縮膠片、打孔卡片、電腦報表、電磁紀錄物傳遞之情形，範圍較「個人資料保護公約」相對縮小，於我國與「個人資料保護公約」締約國間利用郵寄、攜帶傳輸微縮膠片、打孔卡片、電腦報表、電磁紀錄物傳遞個人資料之情形時則由我國則發生範圍不一致而出現銜接之問題。在此，非公務機關之目的事業主管可援引第廿四條第二款（國際條約或協定有特別規定者）加以限制，而擴張傳播媒介之範圍，但公務機關由於僅規定「應依相關法令爲之」，則銜接上較爲有疑問。

另者，於第廿四條中第三款之「接受國對於個人資料之保護未有完善之法

令，致有損當事人權益之虞者」對「個人資料保護公約」締約國完成國內法化者，由於歐洲理事會與歐洲聯盟國家已有相對完善法令對個人資料加以保護，故解釋上目的事業主管機關不得援引本款限制我國與該等歐洲區域組織之國家之個人資料傳遞。

又，第四款「以迂迴方法向第三國傳遞及利用個人資料規避本法者」中的「以迂迴方法」與「個人資料保護公約」第十二條第三項 b 中的「以國家領土爲媒介傳遞至另一非立約國領土以避免相關規則者」之規範目的相同，均爲避免跨國傳遞個人資料以迂迴方式迴避個人資料保護相關規定，故而我國「電腦處理個人資料保護法」與歐洲理事會「個人資料保護公約」的締約國間之跨國資料傳遞在不得迂迴規避的部分，是有其銜接性的。

## 三、 與歐洲聯盟相較

### （一） 法規契合面

歐盟的「個人資料保護指令」內涵、架構與基本原則大多與「個人資料保護公約」雷同，本文以下僅比較「個人資料保護指令」與「電腦處理個人資料保護法」較不相同之處，與「個人資料保護公約」雷同處不再贅述。

首先就最明顯的範圍言，「個人資料保護指令」包括了自動化處理與非自動化人工處理之個人資料（僅限於結構化之建檔系統），但我國「電腦處理個人資料保護法」則僅規範經「電腦處理[39]」之個人資料的保護，並未及於其他非經電腦處理之個人資料。但「電腦處理個人資料保護法」第二條則因爲規定「個人資料之保護，依本法之規定」，未明言必需經「電腦處理」，但在解釋上由於「電腦

[39] 所謂「電腦處理」依照「電腦處理個人資料保護法」第三條第三款，是指使用電腦或自動化機器爲資料之輸入、儲存、編輯、更正、檢索、刪除、輸出、傳遞或其他處理。

處理個人資料保護法」立法目的範圍僅限於電腦自動化處理之個人資料，且立法時乃係鑑於立法當時認爲如果全面對所有個人資料予以保護，恐太過廣泛，所以明訂透過電腦處理之個人資料方有「電腦處理個人資料保護法」之適用[40]，故而由立法目的解釋，「電腦處理個人資料保護法」範圍並未包含非電腦自動化處理部分。

在基礎原則方面，「電腦處理個人資料保護法」無所謂特種資料處理原則已若上述，當然也就沒有所謂特種資料處理原則之例外存在；另方面，本文在此欲討論者爲歐盟「個人資料保護指令」基本原則中的一項重點－－當事人相關權利[41]（data subject's right）則或多或少散見於「電腦處理個人資料保護法」中：

在「個人資料保護指令」所包含的當事人相關權利方面，首要者爲當事人受告知權，其所規範之目的應爲積極告知當事人而有所主動作爲，對照我國「電腦處理個人資料保護法」，較接近者似應爲第十條以及第廿一條，在公務機關以公告或適當之方式[42]，在非公務機關以由公務機關公告之方式告知當事人。但是與「個人資料保護指令」比較起來，似乎並不夠積極主動，且我國實務上資料當事人鮮有爲此查閱政府公報之習慣。另外，在範圍上我國「電腦處理個人資料保護法」規定爲個人資料檔案名稱、保有機關名稱、個人資料檔案利用機關名稱、個人資料檔案保有之依據及特定目的、個人資料之類別、個人資料之範圍、個人資料之蒐集方法、個人資料通常傳遞之處所及收受者、國際傳遞個人資料之直接收受者、受理查詢、更正或閱覽等申請之機關名稱及地址等，並未包含「個人資料保護指令」中最重要的「所可能發生後果、得享查詢與更正之權利[43]」等。又，

[40] 參前揭註 203，頁 4。

[41] 對於我國「電腦處理個人資料保護法」之當事人權利，學者許文義教授於其著作中有極詳細之論述，參：許文義，前揭著，頁 113-156。惟，本文此部分所論述之當事人相關權利係以歐盟「個人資料保護指令」爲出發點，部分權利內容爲我國「電腦處理個人資料保護法」未及規範，併此敘明，以資對照。

[42] 指「電腦處理個人資料保護法施行細則」第十五條第一項，以利用電視、新聞紙、雜誌或其他可供公眾知悉之傳播媒體爲公告，解釋上應包含利用網際網路爲公告之態樣。

[43] 參「個人資料保護指令」第十條。

「電腦處理個人資料保護法」並無「個人資料保護指令」第十一條若所蒐集之資料非爲當事人所提供之時的相關規範，似嫌不夠精細。

當事人查詢請求權方面，則規定在「電腦處理個人資料保護法」第十二條、第十四條與第廿二條；當事人確定及凍結資料權於第四條第三至五款中規範。另，當事人異議權與當事人拒絕資料自動化處理權解釋上似可包含於第四條第四款、第十三條第二、三項之「請求停止電腦處理及利用」中，但當事人之凍結資料權、異議權與拒絕自動化處理權有本質上之不同，雖均可以「請求停止電腦處理及利用」做爲達成不同權利目的之相同手段，惟如此不分權利種類，概以相同文句加以規範似嫌粗糙。且「電腦處理個人資料保護法」中非公務機關部分無相關三項權利之規定，僅於「電腦處理個人資料保護法施行細則」第三十五條規定「（施行細則）第二十四條第一項、第二十五條及第三十四條規定，於非公務機關準用之」，但該施行細則第廿四條第一項爲「公務機關依本法第十三條規定爲更正、補充、刪除或停止電腦處理、利用該資料時，應通知其所知悉已收受該個人資料之機關、團體或個人。」，解釋上應爲第十三條之告知義務履行之規定，並非上述凍結資料權、異議權與拒絕自動化處理權等三項權利本身，則吾人以爲可能造成非公務機關無該等義務之錯誤。

（二） 法規銜接面

「個人資料保護指令」在個人資料跨國傳遞方面規定於第廿五條，原則上個人資料向第三國傳遞，除了有第廿五條第二款之例外以外，僅限於該第三國具有相當於本指令之對個人資料保護之水準；至於水準是否相當，則須依據整體狀況加以評估，特別是應該要考量資料之性質、目的及持續處理之時間、來源國及最終目的國、該第三國之法律規範及專門之保護措施等等，而保護水準是否足夠歐洲議會授權歐盟執委會予以認定。目前歐盟執委會認定通過該相當程度保護水

準者，包括匈牙利[44]、瑞士[45]、美國的安全港協定[46]、加拿大[47]、以及阿根廷[48]等國，我國則尚未取得認可。

該條之適用結果不但對歐盟會員國有影響，相對的也對與其有貿易上或其他方面往來的國家有所影響，影響當然及於我國，故而我國之「電腦處理個人資料保護法」應及早提供給歐盟執委會，以獲得其認定通過「個人資料保護指令」之相關規範，以利我國與歐盟之貿易以及其他方面之交流。

## 四、 小結

經由本節對於我國「電腦處理個人資料保護法」與「個人資料保護公約」、「個人資料保護指令」兩者所爲法規範之契合面與銜接面方面之比較，得知我國「電腦處理個人資料保護法」在許多方面尚差強人意。在契合面方面，最大之問題應當是在於「電腦處理個人資料保護法」在基本原則的建立上相當模糊，缺乏其明確性；並且，區分公務機關與非公務機關的結果，除了容易失去其一致性的先天性缺點之外，我國「電腦處理個人資料保護法」反而更多了公務機關權力大、責任小的重大缺點，對照「個人資料保護公約」與「個人資料保護指令」兩者，其一體適用性不論公務機關或非公務機關僅在例外時區別的立法方式，值得我國參考借鏡，至少在公務與非公務機關之間的平衡方面，應有所改進以符合個人資料保護之精神。

至於契合現方面，除了我國對於跨國個人資料傳遞規範不盡詳盡以及媒介

[44] Commission Decision 2000/519/EC of 26.7.2000 - Official journal of the European Communities, No. L 215, 25/8/2000, P.0004.
[45] Commission Decision 2000/518/EC of 26.7.2000 - Official journal of the European Communities, No. L 215, 25/8/2000, P.0001.
[46] Commission Decision 2000/520/EC of 26.7.2000 - Official journal of the European Communities, No. L 215, 25/8/2000, P.0007.
[47] Commission Decision 2002/2/EC of 20.12.2001 on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act - Official journal of the European Communities, L 2 , 4/1/2002, P.0013.
[48] Commission Decision C (2003) 1731 of 30 June 2003.

限縮之外，盡快與歐盟「個人資料保護指令」銜接，並通過歐盟執委會之認可，相信能使我國除了在個人資料保護方面向前邁進一大步之外，更能在國際資訊交流與貿易及其他方面發展上有長足之進步。

## 第三節　與歐洲案例研究之比較

### 一、 概說

本節透過台灣現今關於個人資料保護最廣受關注的兩項焦點－－全民健保 IC 卡與全民指紋建檔兩項政策性之個案議題，對照以「個人資料保護公約」與「個人資料保護指令」爲中心規範的歐洲理事會及歐洲聯盟二組織對於個人資料保護，在個人醫療資料、個人警察資料方面之相關作爲。其後並以我國同樣面臨之網際網路快速發展所帶來立法不及的問題，與上述歐洲組織做一對照，期能對於將來相關立法以歐洲經驗提出相關建議。

我國關於個人資料保護之法規係以「電腦處理個人資料保護法」爲中心已若上述，在新政策關係到個人資料保護時，當然應以該「電腦處理個人資料保護法」爲法規範中心加以適用，「電腦處理個人資料保護法」第二條本文亦爲如上之規定。另外，本文前述之我國相關個人資料保護法規在這些個案中也應有所適用，但由於該個案並未有相關個人資料保護之專法加以配套，故而在許多問題之處理上不免疑義，尤其全民健保 IC 卡已然匆促上路，許多關於個人資料保護問題已逐漸浮現；而全民指紋建檔更牽連廣泛，不應只爲單一增加行政或刑事效率而忽略程序之正義，故我國更應加緊相關立法之腳步。在未有專法出現以前，「電

腦處理個人資料保護法」應爲圭臬之所在，理應對不合時宜之部分加以改正，以符合現狀與未來發展之因應。

## 二、 醫療資料與全民 IC 健保卡

我國在個人醫療資料領域方面進來最受矚目者，當推全民 IC 健保卡[49]之相關政策，其所受爭議接連不斷，筆者對此嘗試以歐洲之經驗加以檢視。首先有必要對該政策做一概要之分析；其次，以本文第三章中所討論之歐洲相關案例以及法規範對之找出在個人資料保護方面可能之盲點。

在我國全民健保 IC 卡政策目的方面，主要官方資料[50]顯示其目的[51]包括整合現行醫療憑證、一卡到底免換卡、明白個人醫療費用記錄、即時登錄醫療費用、提醒民眾在保及繳費狀況、促進醫療院所電腦化、帶動國內資訊工業發展，以及避免重複利用昂貴儀器及檢查等八項。其內涵大約爲鑑於我國之全民健康保險現行之制度以紙卡爲主使用起來可能產生諸多不便利健保 IC 卡，於是預計將現在的健保紙卡、兒童健康手冊、孕婦健康手冊和重大傷病證明卡等四種卡冊的看病與證明功能都放在同一張卡片上，如此一來，不論身份在看病時都僅需攜帶同一張憑證，並且五到七年都不用再換健保卡；此外，這張健保 IC 卡欄位內容一旦完全實施後，除可記載持卡人的個人醫療費用、在保與繳費狀況外，保險對象也可以知道自己花費的部分負擔，醫院可以由累計的部分負擔，收到規定之全年住院部分負擔上限，即可不再收取，除了減少民眾負擔，也避免民眾必須先繳交部

---

[49] 所謂的 IC 卡，就定義上爲一種含有積體電路或晶片，並具資料儲存或處理能力之標準尺寸塑膠卡片。參：王濟民，＜智慧卡（Smart Card）之推廣與應用分析＞，台灣大學商學研究所碩士論文，民國 88 年 6 月，頁 4。至於 IC 卡之詳細整體介紹以及製作發給流程，詳參：吳昊，前揭論文，頁 13-56。另，全民健保 IC 卡之英文的簡稱爲 HCC(Health Care Card)或 NHI IC Card(National Health Insurance IC Card)。

[50] 參照：行政院衛生署中央健保局，《中華民國國民健保卡實施計畫》，民國 88 年 11 月 24 日；行政院衛生署中央健保局，《健保 IC 卡建置計畫徵求建議書文件》，民國 89 年 8 月 1 日等；另參：吳昊，前揭文，頁 20，註 25。

[51] 參吳昊，前揭文，頁 20-22。

分負擔，等到次年再向健保局核退超過上限的麻煩，中央健保局並宣稱其爲一張功能完整的多用途健保卡[52]。

而該 IC 卡片之存放內容涉及多項相關個人資料，更是必須關注之焦點，依中央健保局宣稱，在健保 IC 卡上所嵌的 IC 晶片內規劃有「個人基本資料」、「健保資料」、「醫療專區」及「衛生行政專區」等四種不同類別資料存放區段，各區段預定存放之內容說明如下（表 4-1）：

（表 4-1）：全民健保 IC 卡資料存放區段：

| 資料區段名稱 | 存放內容 |
|---|---|
| **個人基本資料** | 卡片號碼、姓名、身分證號或身分證明文件號碼、出生日期、性別、發卡日期、照片、卡片註銷註記 |
| **健保資料** | 保險人代碼、保險對象身分註記、卡片有效期限、就醫可用次數、最近一次就醫序號、就醫資料登錄、就醫累計次數、就醫累計費用、總累計費用、部份負擔累計費用、個人保險費、重大傷病註記、保健服務、新生兒依附註記、孕婦產前檢查(限女性)、最後月經開始日期、預產期 |
| **醫療專區** | 過敏藥物、重要醫令項目、長期處方箋、門診處方箋 |
| **衛生行政專區** | 預防接種資料項目、器官捐贈資料項目 |

資料來源：中央健康保險局，健保 IC 卡宣導網站，＜認識你的 IC 健保卡＞，URL: http://www.enhi.com.tw/（2005/11/22）

上（表 4-1）中，包括保險對象（資料當事人）的姓名、身分證號、出生日

[52] 參：行政院衛生署中央健保局，健保 IC 卡宣導網站，＜健保 IC 卡的意義與功能＞，URL: http://www.enhi.com.tw/（2003/8/7）.

期、卡片號碼及照片等均爲顯性資料[53]外觀上可以辨識，而其他隱性資料則需透過醫療院所之讀卡機或所謂公共資訊服務站[54]方可使當事人知悉該內容。

至於在健保 IC 卡相關對於個人資料之安全機制政策方面，中央健保局將之區分爲整體安全機制與個人資料及隱私權保護機制二者[55]前者內容爲：

（一） 契約規範：健保局與立約商東元電機公司簽訂之契約條款，第一條即明確規範立約商於履約期間所知悉或持有之健保局機密，均應保密不得洩漏。並要求立約商應與其員工及協力廠簽訂保密契約，使其對健保局負有與本約內容相同之保密義務。又於契約條款第十一條明訂在契約有效期間，立約商如將卡片或保險對象基本資料外流，健保局得沒收保證金並終止或解除全部或部分契約，並請求立約商賠償。另在投標須知第四條明訂健保 IC 卡、安全模組、讀卡設備、應用系統、軟硬體設備，如係國外產品必須提出國外原廠出具之授權經銷代理證明文件及連帶保固證明文件。

（二） 整體安全計畫：健保局要求立約商必須針對本專案提供整體系統安全政策，以建立完善之管理機制。依據這項規定，立約商（東元電機公司）提供了「整體安全計畫書」、「整體安全機制設計文件」與「整體安全政策管理使用者手冊」等文件，委請學者專家審定，並據以執行。

（三） 成立健保 IC 卡資料安全防護小組：爲防止健保 IC 卡建置計劃資料外洩或被不當使用，健保局成立健保 IC 卡資料安全防護小組，監督一切安全相關事務。

---

[53] 所謂顯性資料指在健保 IC 卡卡片表面看得到的資料皆稱爲顯性資料，諸如姓名、身分證號、出生年月日、卡片號碼與照片等。相對的隱性資料則爲隱藏在健保 IC 卡 IC 晶片裡的資料，在健保 IC 卡裡存放的隱性資料包括：基本資料段、健保資料段、醫療專區及衛生行政專區，未來並視實際需要增加存放內容。

[54] 健保 IC 卡專案的讀卡機款式之一，可提供民眾（資料當事人）密碼變更的服務，且是唯一可讓民眾直接選取列印功能的讀卡機。

[55] 參：行政院衛生署中央健保局，健保 IC 卡宣導網站，＜健保 IC 卡安全機制＞，URL: http://www.enhi.com.tw/（2005/11/22）.

後者關於個人資料及隱私權保護機制，則區分爲下列各機制：

（一）政策配套：1.不作健康保險與醫療保健目的以外之用途：健保 IC 卡的主要功能係在提供保險對象就醫時辨識身分之用，以便於醫療處置之正確判斷，目的單純明顯，並不作爲衛生行政及保健醫療服務等特定目的外之使用。2.不存放完整的病歷資料：健保 IC 卡現階段開放使用之欄位內容，僅限於取代紙卡原有功能，並不涉及隱私。部分社會團體對於 IC 卡是否會侵犯個人隱私權，極爲關切，健保局已積極與各相關人權及病友團體開拓對談平台，持續溝通，以利未來存放用藥、檢驗、檢查等資料，保障民眾對醫療知的權益與自主管理權。大家所關切之個人就醫隱私資料，係記錄並存放在各醫療院所製作之病歷中。健保 IC 卡之記憶容量，包含內建程式與必要欄位規格，僅有 32K 位元之空間，無法存放病人於各醫療院所就診之所有病歷資料及檢驗檢查影像資料。設計之存放欄位內容僅止於健保業務中有利於民眾就診作業，能提升醫療照護品質與具有費用節流功能。

（二） 卡片操作安全機制：1. 卡體精密防僞印刷：健保 IC 卡除卡片有扭索狀設計、彩虹紋、細微字、紫外線隱形印刷及光學變色油墨等多重防僞設計外；另照片背景亦有防僞處理，以防照片被取代冒用，較諸一般信用卡並不遜色。2.多重保密安全機制保護個人隱私（1） 晶片內儲存資料均加密處理。（2） 讀卡機加安全模組(SAM)卡：須具有健保局自己製作發行的讀卡機安全模組卡(SAM)才能讀取晶片內資料，採嚴謹授權及相互認証機制。（3） 醫師卡：具有醫師卡始能讀取醫療資料。（4） 個人密碼：IC 卡設有密碼功能(Pin code)，以個人密碼優於醫師卡之讀寫授權，民眾可選擇是否輸入密碼解密，一旦設定密碼，一般人或掛號人員即使有讀卡機及安全模組，亦無法讀取基本資料段以外之欄位資料，必須民眾同意輸入密碼，醫護人員始能開啓資料。

（三）資通安全機制：1. 採最高安控標準及規格，三道防火牆，並不定期

模擬駭客入侵，以期發現安全缺失，如駭客已入侵，亦可立即更換密碼阻絕。2.採用 VPN 封閉性專屬網路，不與網際網路連結，駭客無從由外部入侵。同時，以 VPN 爲骨幹網路，中華電信股份有限公司公司各地分公司均可互相備援，而網路頻寬隨使用量自動調整，以確保網路傳輸品質，有效減低網路塞車機率。3.代碼傳輸，IC 卡僅儲存必要之慢性病用藥、某些特定疾病名稱或昂貴之檢驗檢查醫令，各該項目均以數字代碼登載（code），亂碼傳輸，而非以中文記載。

（四）電腦病毒防治：1. 本局使用完善之病毒防治機制。2. 使用端輔導使用防毒軟體（1） 主機端提供使用者端之病毒碼及程式更新機制。（2） 建置與病毒防治公司(如 Trend、Norton)間之 Gateway。（3）勸導使用防毒軟體。

（五）危機處理及應變計畫：研訂危機處理應變計畫，明定危機種類、等級、認定與啓動程序，並組織危機應變小組，作爲緊急應變及危機處理機制之事前防範措施，於緊急危機(如天災、停電)發生後，亦建置有事後應變機制，如：1.卡片遺失或被竊，得立即註銷卡片。2.遇有全省大規模停電，因建置有 UPS 不斷電系統，得以確保系統能完全關閉，避免軟、硬或資料之流失與損害。3.如網路駭客侵入，除建置有三道防火牆、封閉式自屬網路加以阻決外，並不定期模擬駭客入侵，以期發現安全缺失；如駭客已入侵，亦可立即更換密碼阻絕。4.人員接觸資料設有權限劃分，任何接觸使用健保 IC 卡資料者，均會留存電子紀錄，便於追查，防止人員洩密情事發生。

在以上初步對於全民健保 IC 卡政策說明過後，本文以下部分擬提出對於個人資料保護方面該政策之可能發生問題。在關於個人資料保護面向上，一般來說，最受關注之癥結包括個人不能決定其晶卡片上的記載項目及其內容正確性、個人無法控制其個人醫療資料在系統中的私密性、個人別無選擇只得任政府和承

作業者[56]擺佈的無奈[57]等。縱觀該政策，不難發現許多在個人資料保護面向上受到爭議的地方。

本文則另歐洲相關經驗而不同於以往之切入點，分別用三個面向對於此政策加以切入，其一爲政策目的方面，探討其是否兼顧歐洲相關案例中最重視的「法律基礎」、「合法之目的性[58]」與「公益大於私益」原則；其二爲 IC 卡本身資料存放方面，探討其所存放之個人資料是否爲資料當事人所能接近（access），又是否已盡其告知義務等關於當事人的相關權利；其三則是在其所宣稱之安全機制中，是否足以符合安全原則之需求。

在法律基礎之面向上，該政策之主要直接相關法規範爲「健保 IC 卡管理須知[59]」與「全民健康保險特約醫事服務機構試辦健保ＩＣ卡就醫須知」其中「健保 IC 卡管理須知」第九條第一項規定「健保ＩＣ卡不需設定密碼即可使用；但保險對象如爲避免就醫資料爲非授權人員讀取，可於讀卡設備設定健保ＩＣ卡密碼，以維護個人隱私。」爲與個人隱私唯一相關之處，但不盡詳細，故而對於個人資料之保護仍回歸至「電腦處理個人資料保護法」，而如此涉及個人資料保護權益甚巨之政策，居然沒有以保護個人隱私之專法做爲法基礎，是相當令人不解的。

在政策目的面向上，觀察中央健保局對於效益之評估，大多集中在所謂經濟之效益方面做思考，諸如整合現行醫療憑證、一卡到底免換卡等乃節省相關效益支出費用；明白個人醫療費用記錄、即時登錄醫療費用、提醒民眾在保及繳費狀況、可在保費收入上達到快速明白收支及減少保費呆帳；促進醫療院所電腦

[56] 我國 IC 健保卡之承作業者爲東元電機公司智慧卡事業部，關於其相關介紹，參：http://www.smartcard.teco.com.tw/cht/aboutus.html.

[57] 參：莊庭瑞，＜從健保ＩＣ卡談個人資料保護＞，自由時報，自由廣場版，2002 年 8 月 6 日。

[58] 法律基礎與合法之目的性爲「歐洲人權公約」第八條中，歐洲人權法院三大判別依據之二。See M.S. v. Sweden, Judgment of 27 August 1997, *Reports of Judgments and Decisions* 1997.

[59] 公告日期：91 年 11 月 4 日，健保承字第 0910011258 號。該規範目的爲配合健保 IC 卡實施，訂定健保 IC 卡請領、換發、更新等相關規定。

化、帶動國內資訊工業發展，以及避免重複利用昂貴儀器及檢查等，更是直接明顯係爲增加國家及健康保險整體經濟效能。其合法之目的性上之重心明顯放在國家經濟之健全方向，此時對於公益（國家經濟健全）與私益（當事人個人資訊自決權）之衡平便顯的重要。

由歐洲經驗觀之，關於個人醫療資料保護之例外之主要要件，於歐洲人權法院通常爲「公益大於私益」，對照我國健保 IC 卡政策顯然會有問題。例如該政策之爲健全國家經濟之公益目的，但由於健保 IC 計畫耗資龐大，僅在民國 89-91 年，政府爲規劃及發放兩千萬張 IC 卡，已支出高達 41 億元的經費（相對紙卡一年 8 千萬元）；而更改現行健保行政管理作業程序、讀卡機、網路線路設備、資訊系統軟硬體、改進防火牆等，仍有賴後續追加預算，則該政策中所求之公益是否能確實達成即有疑義。且就另一方向言，我國人權團體也提出[60]：中央健保局何不加強目前的稽核機制，卻要建制新的 IC 卡系統，擾民傷才？如果相關單位無法改善本身行政效率，我們又何以期待未來更換系統後，醫療資源的控管效率就能夠獲得提升？等問題。但相對的另一方面之個人資料隱私權益卻未見確實保護而遭致犧牲，吾人不禁疑問，該等公益是否在真正執行面上會大於私益？則在此面向上思考公益相當可能不大於私益，就歐洲人權法院 ***M. S. v. Sweden***[61]判決中看來，本 IC 卡政策之合法目的性一旦消失，即違背「歐洲人權公約」第八條，而有違背人權價值之可能。

另就 IC 卡個人資料存放區段角度來看，依（表 4-1）觀之 IC 晶片內規劃有「個人基本資料」、「健保資料」、「醫療專區」及「衛生行政專區」等四種不同類別資料存放區段，其中資料當事人可直接知悉其個人資料之顯性資料區段爲小部分，比例上較隱性資料明顯爲少，而該等隱性資料卻需透過相對不便利之方式方

[60] 參：全民個人資料保護聯盟，＜健保 IC 卡侵犯隱私權但便利遭誇大--相關問題未獲充分討論前應停止發卡＞，全民個人資料保護聯盟呼籲健保 IC 卡中止發卡說明，2005/11/22。URL: http://www.tahr.org.tw/PDPA/index.htm.（2005/11/22）

[61] 參本文第三章第一節第三項。

得使資料當事人得知內容，在實際執行面上，會使資料當事人耗費較多成本去知悉己身隱性資料而招致不公平現象發生，明顯是對於當事人資料接近權（access）之阻礙。倘依歐洲理事會「醫療個人資料保護建議」，則明顯違背第八部分之醫療資料當事人權利，且依上述並無公益大於私益之例外。另綜合 *M.G v. The United Kingdom* 案[62]中法院之認定，相關政府單位應有積極之義務，提供完整而無遺漏之當事人所要求之個人資料，而並非由該單位決定提供資料之多寡，則我國對於隱性資料方面之告知義務明顯不夠積極。

另 IC 卡存放區段具有擴充性，而可能在未來逐步擴張[63]此時牽涉一卡多用，等於將資料當事人的一切個人資料赤裸裸呈現於有權、有管道讀取卡片資料者眼前，其具強制性且大規模地侵犯國民隱私，更將導致人民與政府間的權力嚴重失衡[64]，當然違背個人資料保護之各項基本原則，且由於 IC 卡乃透過電腦處理，故而也會違背「電腦處理個人資料保護法」之相關規定。

最後就安全機制之方向觀察，於該政策中稱健保 IC 卡之記憶容量，包含內建程式與必要欄位規格，僅有 32K 位元之空間，無法存放病人於各醫療院所就診之所有病歷資料及檢驗檢查影像資料。但其實於該 32K 位元之空間內已經可以儲存相當多欄位之個人資料，單單是最簡單明顯之就醫記錄次數或孕婦產前檢查等，便可能成爲垃圾資訊強迫推銷之騷擾，甚或遭受個人保險與工作權可能因雇主、保險業者獲悉個人就醫紀錄與病史之衝擊，故而以該 IC 卡存放內容並不完整爲立論中心並不可取。另外所謂 IC 卡設有密碼功能(Pin code)之安全機制，並非本即如同一般提款卡般，完全必須經資料當事人明確同意下方能使用該卡片。事實上在特約院所中，使用健保 IC 卡看診時是不需輸入個人密碼的，故而

---

[62] 同上。

[63] 事實上健保 IC 卡發行時便打算納入未來之國民年金與身份證資料等，而以「社會福利卡」之名發行，詳參：行政院資訊發展推動小組「IC 卡規劃與推行小組」編印，《「國民身份健保和一智慧卡」專案徵求建議書文件》，民國 87 年 6 月 10 日。另參：吳昊，前揭文，頁 9-13。

[64] 但關於此點中央健康保險局及相關行政機關則對此並不多加解釋，造成諸多人權團體反彈。參：全民個人資料保護聯盟，前揭文。

該特約院所之相關醫護甚至行政人員均可得知該 IC 卡內容，而個人密碼卻僅在查詢卡片內容時使用，或資料當事人僅能使用讀卡機或公共資訊站時，更改個人密碼，既然特約院所不需使用密碼，則如何防止一般側錄 IC 卡資料之行爲？在安全原則上既然上述該政策在「公益大於私益」上之檢驗是有疑問的，則更應相對加強安全機制及個人資料隱私保護之功能，但該政策實際推行結果爲方便民眾於特約醫院就醫等理由卻對於許多安全機制大打折扣，似乎於安全原則上並未能符合要求。

## 三、 警察資料與全民指紋建檔

我國於個人警察資料方面近來最受矚目之議題當爲全民指紋建檔[65]議題之提出，相對於上述全民健保 IC 卡政策之倉促上路，所幸全民指紋建檔並未即刻實行[66]。本節以歐洲對於個人警察資料之相關法規範與實際案例爲經驗，試圖對於我國對於全民指紋建檔議題或政策之提出，借他山之石，對之加以討論。

該全民指紋建檔議題行政院本已因人權顧慮（國家機器藉此監控人民、個人資料蒐集、流向、管理安全非個人能掌握），於 2001 年 7 月 19 日邀集各部會會商，會中決議「請領國民身分證應捺指印指紋作業不宜貿然實施，請內政部及時進行修法。」同年 12 月 31 日，立法院內政委員會初審行政院所提「戶籍法」第八條修正案，並同意將捺指紋與身分證換發脫鉤。但是行政院內政部卻聲稱因多國駐台使館、中央與地方各級機關認爲國民身分證屢傳僞造情形，且立院朝野

[65] 指紋建檔在我國由於有供刑事事件使用之用途，故當然爲個人警察資料之一環。

[66] 但我國在實際公共行政上卻已有相關類似之措施，惟並非用於警察資料。參＜指紋建檔 補換身分證有優惠＞，聯合報，第 04 版，92/07/03：
台北市民政局推動指紋建檔，預計九月起，於十四處戶政事務所規畫快速通關窗口，指紋已建檔者補換身分證時，可享有免費數位拍照服務，不必再帶傳統照片來辦理戶政事務。民政局表示，指紋建檔與戶籍法規範的全民指紋建檔不同，戶籍法不但規定要擷取建檔者的十指全指紋，還須採取掌紋；北市的指紋建檔，市民只要將左右手食指平面指紋按壓，系統即可辨識，而且戶籍法收集指紋是爲了警察機關犯罪偵防，北市指紋建檔是爲了方便民眾辦理戶政相關業務，同時避免民眾的身分證被不肖人士冒用。

黨團咸認全民指紋建檔有助維護治安，不願意刪除戶籍法中請領身分證應捺指紋規定，因此內政部研擬「全面換發國民身分證並建立指紋識別檔」，並於 2003 年 3 月 14 日召開相關公聽會，以因應國內證件僞造情況並加速換發身分證[67]。

事實上對於全民指紋建檔議題一直以來即有很大爭議，支持者[68]大多將之放在警察行政之有效性及效率性上觀察，謂之指紋建檔不止有助於偵察犯罪，並可運用在防止民眾詐領社會福利金，以及確認情報員、教師及幼兒工作者身份等；在台灣，指紋也不僅用於刑案偵辦，如 2002 年 5 月華航空難發生後，罹難者屍體辨認工作，指紋比對跟牙齒及基因鑑定都有所助益，至於日常的協尋失蹤人口、指認無名屍體或防止販售嬰兒等，雖有基因鑑定可用，但都不如指紋比對方便可行云云。

另外支持全民指紋建檔者，亦提出相關立論[69]，稱全民指紋建檔並不會侵害隱私及個人資料。例如強制指紋建檔，早有戶籍法的規定，並非不法。其次，指

---

[67] 參：全民個人資料保護聯盟，＜指紋建檔，全民公敵! 民間團體反對內政部「換發身分證並建立全民指紋檔」新聞稿＞，2003 年 3 月 14 日。

[68] 例如，司法院大法官解釋釋字第六零三號解釋理由書中，略謂行政院支持指紋建檔之理由：…二、戶籍法第八條第二項與比例原則、法律保留原則及明確性原則無違：（一）指紋爲受人格權、隱私權及資訊自決權保護之個人資料，國家對之蒐集與利用，於公眾有重大利益，而符合比例原則之前提下，得以法律爲之。（二）戶籍法第八條之立法目的係在建立全民指紋資料，以「確認個人身分」、「辨識迷失民眾、路倒病患、失智老人及無名屍體」，並可防止身分證冒用，爲明確且涉及重大公益之立法目的。（三）指紋因其人各有別、終身不變之特性，可以有效發揮身分辨識之功能，爲確保國民身分證正確性之要求之適當手段；指紋爲經濟且可靠安全之辨識方法，與其他生物辨識方法相比，爲侵害較小而有效之手段；其立法可以保障弱勢、穩定社會秩序，有重大立法利益，與可能造成之侵害相較，尚合比例。（四）以按捺指紋爲請領國民身分證之要件，爲戶籍法第八條所明定，符合法律保留原則之要求。且法條文義並非難以理解，並爲受規範者所得預見，事後亦可由司法加以審查確認。至於指紋資料之傳遞、利用與管理，則有「電腦處理個人資料保護法」規定補充，符合法律明確性原則。（五）按捺指紋爲多數民意所贊成…三、戶籍法第八條第三項，並不違憲：（一）按捺指紋爲國民身分證明之要件內涵，與身分證上顯性身分證明基本資料，均屬於辨識之基礎。國家在法律要件合致時，應依法發給國民身分證，若國民身分證之人別辨識基礎欠缺，則不具規定之要件，自應不予發給，以落實按捺指紋規定之執行，爲適當之手段。不發給身分證爲不踐行程序要件之附隨效果，並非處罰。其對人民生活或權利行使產生不便利，乃人民選擇不履行相對法律義務之結果，並非主管機關侵害人民權利。且指紋爲電腦處理個人資料保護法所規範之個人資料之一，其處理運用有相關法律規範，與比例原則無違。（二）國民身分證爲個人身分識別之重要憑證，國家發給時應確認領證人與該身分證所表彰之身分相符，而指紋因其無可變造之特性，可以輔助身分辨識功能之發揮並確保身分之正確性，二者具合理關聯等語。

[69] 參：尤英夫，＜全民指紋建檔 個人隱私並未遭侵犯＞，自由時報，自由廣場，2002 年 9 月 12 日。

紋固爲人體之一部分，但正如每個人皆有其姓名一樣，叫每個人，並不就是侵犯其隱私權。何況，一個人在社會群體中生活，不可能遺世而獨立，怎可能不與人發生各種關係，不有一個代號或姓名？留下指紋檔就像代號或姓名一樣，只是易於辨識張三或李四，不會混淆在一起。所以說強制捺指紋，不會侵害他人的隱密或寧靜（人跟人見面，面孔的隱密都不可能，而指紋還要大費周章用機器或人工辨識才能認出），誰說強制捺指紋，就是侵犯他人隱私？又強制捺指紋，只是建檔供行政機關於必要時加以利用而已，並不在於報導或公開；何況指紋建檔並不必然會侵害人權，只有當指紋檔案遭到濫用或誤用，指紋建檔才有侵犯人權或隱私的顧慮等等。

吾人針對上述支持全民指紋建檔議題之立論，則嘗試以歐洲經驗以及基礎的個人資料保護理論對之加以討論：

首先必須釐清的一點，全民指紋建檔議題由於牽涉犯罪刑事偵察，故而其所蒐集之個人資料－－指紋，當然是個人警察資料之範圍。事實上，個人警察資料之範圍可包括刑事資料、人事資料、戶口查察資料及個人忠誠資料[70]等，而相對的，全民指紋建檔議題所牽涉之範圍雖主要以刑事資料爲主，但是在其他方面個人警察資料之運用上亦有可能牽涉，甚至該全民指紋建檔議題範圍在未來實際之利用上，更可能超越個人警察資料之範圍而成爲諸多辨識工具方法之一，故對於個人資料保護之影響層面甚廣，也相當的深入。在強調其正面效能之同時，當然亦必須兼具保護個人資料隱私之效果！

並且全民指紋建檔議題最重要可能影響個人資料之癥結所在，爲透過資料庫電腦自動化之大量且快速交叉比對處理，並結合其他基本之個人資料所帶來之

[70] 參：劉坤旺，＜從憲法觀點論警察處理個人資料法制＞，中央警察大學行政警察研究所碩士論文，民國 89 年 6 月，頁 113-125。另外，個人警政的「資訊系統」則可分爲八大類：1. 犯罪管理資訊系統。2. 治安管理資訊系統。3. 安檢管理資訊系統。4. 入出境管理資訊系統。5. 交通管理資訊系統。6. 後勤管理資訊系統。7. 勤務管理資訊系統。8. 警察行政支援管理資訊系統。參：李震山，前揭著，頁 311，註 67。

後果，該可能之侵害後果與我國「電腦處理個人資料保護法」之立法目的中欲防止之侵害態樣極其相似。故而支持該議題立論之所謂「留下指紋檔就像代號或姓名一樣，只是易於辨識張三或李四，不會混淆在一起。所以說強制捺指紋，不會侵害他人的隱密或寧靜（人跟人見面，面孔的隱密都不可能，而指紋還要大費周章用機器或人工辨識才能認出）」乃可能有見樹不見林之憾，蓋不但人終其一生不可能跟全民指紋建檔所收集於電腦資料庫中之全部人口總數均親自見面，況留下代號或姓名本即可能侵害個人隱私，所以全民指紋建檔議題實需仔細討論對於個人資料隱私之侵害可能性。

本文對此全民指紋建檔議題循歐洲經驗分別以下列三個面向加以觀察：其一爲在個人警察資料中最重要的必要性原則方面觀察；其次則是對於個人警察資料所應有之特別保護原則，探討其法基礎是否則足夠；最後則以歐洲對於個人警察資料之流通與安全面向之解釋，對我國全民指紋建檔議題加以探究[71]。

就個人警察資料收集的最重要原則－－必要性原則，觀察我國全民指紋建檔議題，吾人由歐洲理事會「關於警察部門之個人資料保護之建議[72]」中得知，個人警察資料之收集處理及儲存應較其他特別種類之個人資料更受到嚴格之保護程度，因爲警察資料所牽涉之內涵關係著刑事法規範下之個人資料，其中心內涵直指人權之核心價值（此即特別保護原則），所以警察資料之收集，限於防止真正危險或制止個別犯罪，若有例外則應該嚴格限制之，除有「絕對必要」之外，應禁止之。對照我國「憲法」第廿二與廿三條所揭櫫之比例原則－－需選擇對人民基本權利侵害最小之首對達成目的來看，此種敏感性之個人資料種類更應加以

[71] 對照近來大法官解釋之態度，對於指紋建檔明顯採保留之態度。於司法院大法官解釋釋字第六零三號文中「維護人性尊嚴與尊重人格自由發展，乃自由民主憲政秩序之核心價值。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，並爲保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃爲不可或缺之基本權利，而受憲法第二十二條所保障（本院釋字第五八五號解釋參照）。其中就個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。」即開宗明義表達相關見解。

[72] 參本文第三章第二節第二項。

嚴格保護。

準此，我國相關全民指紋建檔之議題是否有該絕對之必要乃是一大疑問，蓋並非所有犯罪均會留下指紋，在包括毀謗罪、背信罪等犯罪中不但指紋證據出現機率不高，即便在許多侵害身體法益之犯罪中，也不必然會有指紋證據存在，況於全民指紋均建檔後，犯罪者留下指紋證據之機率勢必大幅降低，蓋其已知其個人指紋證據已然建檔，又如何會如此粗心留下證據？更況最極端之例子：該犯罪者以他人指紋按捺於凶器或其他證據上，企圖誤導刑事偵察之情形，則此時指紋建檔反成誣害他人之有利武器！並且指紋建檔後之比對率對調查雖有幫助，但我國實際上來說比對率是偏低的，所以吾人認爲，該全民指紋建檔之提議並非犯罪偵察之絕對必要，況其他作用方面亦非必要，則不符合應對個人警察資料收集與處理之必要性原則。

另延續上述特別保護原則之概念，對於該等資料之收集，必須要有嚴格之法律基礎，對照我國全民指紋建檔議題，該政策提出之主要法律依據爲現行「戶籍法」第八條[73]，「人民年滿十四歲者，應請領國民身分證；未滿十四歲者，得申請發給（第一項）。依前項請領國民身分證，應捺指紋並錄存。但未滿十四歲請領者，不予捺指紋，俟年滿十四歲時，應補捺指紋並錄存（第二項）。請領國民身分證，不依前項規定捺指紋者，不予發給。（第三項）」。該戶籍法之相關規定只規定個人資料之收集，並未規範其他完整之個人資料保護相關規定，若全民指紋資料依自動化方式處理，只能回歸「電腦處理個人資料保護法」之規範，則於

[73] 對於該法條，經大法官解釋後已有清楚規範，即不再適用。參照大法官解釋釋字第六零三號「…指紋乃重要之個人資訊，個人對其指紋資訊之自主控制，受資訊隱私權之保障。而國民身分證發給與否，則直接影響人民基本權利之行使。戶籍法第八條第二項規定：依前項請領國民身分證，應捺指紋並錄存。但未滿十四歲請領者，不予捺指紋，俟年滿十四歲時，應補捺指紋並錄存。第三項規定：請領國民身分證，不依前項規定捺指紋者，不予發給。對於未依規定捺指紋者，拒絕發給國民身分證，形同強制按捺並錄存指紋，以作爲核發國民身分證之要件，其目的爲何，戶籍法未設明文規定，於憲法保障人民資訊隱私權之意旨已有未合。縱用以達到國民身分證之防僞、防止冒領、冒用、辨識路倒病人、迷途失智者、無名屍體等目的而言，亦屬損益失衡、手段過當，不符比例原則之要求。戶籍法第八條第二項、第三項強制人民按捺指紋並予錄存否則不予發給國民身分證之規定，與憲法第二十二條、第二十三條規定之意旨不符，應自本解釋公布之日起不再適用。…」

紙上按指紋後方存入自動化設備時，該仍留存於紙上之非自動化處理資料即不受任何相關法規之拘束，頂多只能類推適用「電腦處理個人資料保護法」之法理，與歐洲個人警察資料經驗中特別強調的特別保護原則未盡相符，故而其對於保護個人隱私之法基礎並非完整，實需另訂專法爲之，不能逕以「戶籍法」第八條爲其法律之基礎[74]。不惟如此，在制定專法時尚須考量盡量能符合歐洲人權法院的 *Malone Case* 所判定之具備有可預知性（foreseeable）、精密（precision）與確定（certainly）等三項嚴格之品質判斷標準，以俾符合個人警察資料之保護。

末就個人警察資料之流通與安全問題觀察，在個人警察資料方面依據「內政部警政署電子計算機作業保密安全實施規定」，警察資料所存放之警用小型隨

[74] 對此法律基礎，司法院大法官解釋釋字第六零三號解釋理由書已有見解：「…戶籍法第八條第二項規定：依前項請領國民身分證，應捺指紋並錄存。但未滿十四歲請領者，不予捺指紋，俟年滿十四歲時，應補捺指紋並錄存。第三項規定：請領國民身分證，不依前項規定捺指紋者，不予發給。對於未依規定捺指紋者，拒絕發給國民身分證，顯然形同強制按捺並錄存指紋，以作爲核發國民身分證之要件。指紋係個人身體之生物特徵，因其具有人各不同、終身不變之特質，故一旦與個人身分連結，即屬具備高度人別辨識功能之一種個人資訊。由於指紋觸碰留痕之特質，故經由建檔指紋之比對，將使指紋居於開啓完整個人檔案鎖鑰之地位。因指紋具上述諸種特性，故國家藉由身分確認而蒐集個人指紋並建檔管理者，足使指紋形成得以監控個人之敏感性資訊。國家如以強制之方法大規模蒐集國民之指紋資料，則其資訊蒐集應屬與重大公益之目的之達成，具備密切關聯之侵害較小手段，並以法律明確規定之，以符合憲法第二十二條、第二十三條之意旨。查戶籍法就強制按捺與錄存指紋資料之目的，未有明文規定，與上揭憲法維護人民資訊隱私權之本旨，已有未合。雖有以戶籍法第八條修正增列第二項與第三項規定之修法動機與修法過程爲據，而謂強制蒐集全體國民之指紋資料並建庫儲存，亦有爲達成防範犯罪之目的云云，惟動員戡亂時期終止後，回復戶警分立制度（本院釋字第五七五號解釋參照），防範犯罪明顯不在戶籍法立法目的所涵蓋範圍內。…蓋就「加強國民身分證之防僞」及「防止冒用國民身分證」之目的而言，錄存人民指紋資料如欲發揮即時辨識之防止僞造或防止冒用功能，除須以顯性或隱性方式將指紋錄存於國民身分證上外，尚須有普遍之辨識設備或其他配套措施，方能充分發揮。…次就「防止冒領國民身分證」之目的言，主管機關未曾提出冒領身分證之確切統計數據，是無從評估因此防範冒領所獲得之潛在公共利益與實際效果。…則以現有指紋資料以外之資訊，既能正確辨識人民之身分，指紋資料之蒐集與「防止冒領國民身分證」之目的間，並無密切關聯性。末就有關「迷途失智者、路倒病人、精神病患與無名屍體之辨認」之目的而言，…然而就目前已身分不明、辨識困難的國民而言，於換發國民身分證時一併強制按捺並錄存指紋資料對其身分辨識並無助益，而須著眼於解決未來身分辨識之需求。惟縱爲未來可能需要，並認此一手段有助前開目的之達成，然因路倒病人、失智者、無名屍體之身分辨識需求，而強制年滿十四歲之全部國民均事先錄存個人之指紋資料，並使全民承擔授權不明確及資訊外洩所可能導致之風險，實屬損益失衡、手段過當，難以符合比例原則之要求，侵害人民受憲法第二十二條保障之資訊隱私權。揆諸上揭說明，戶籍法第八條第二項、第三項形同強制人民按捺指紋並予錄存，否則不予發給國民身分證之規定，已侵害人民受憲法保障之資訊隱私權，而就達到加強新版國民身分證之防僞功能、防止冒領及冒用國民身分證及辨識迷途失智者、路倒病人、精神病患與無名屍體之身分等目的而言，難認符合比例原則之要求，與憲法第二十二條、第二十三條意旨均有未符，應自本解釋公布之日起不再適用。至依據戶籍法其他相關規定換發國民身分證之作業，仍得繼續進行，自不待言。…」

身電腦不得與一般個人電腦相連結，並應設簿登記專人保管操作，以避免資料外洩。另在資料保密規定方面，則規定非基於法令規定及職掌權限不得使用警用電腦查詢任何資料，查詢資料應填寫查詢記錄簿查詢人取得或列印資料應取得確認，而非警察機關或人員要求提供資訊服務時，各該機關應該備文經業務單位核可後，始可提供服務[75]。但我國實務上警察常有爲爭取績效而忽略正當法律程序原則之要求，而使非警察人員取得警用電腦使用之可能，並利用儲存於該電腦之資料[76]，更況上述「內政部警政署電子計算機作業保密安全實施規定」之行政命令所謂「非警察機關或人員要求提供資訊服務時，各該機關應該備文經業務單位核可後，始可提供服務」所規範之使用時程，應非爲經常性所使用，則若干非警察人員經常性持有警用電腦之行爲即有不妥。退萬步言，若有欲使非警察人員持有警用電腦之必要，亦必須有相關完整規定，以防止個人警察資料外洩之可能。由上述，我國全民指紋建檔議題若真正推行時，則在實際執行層面上即需防止上述爲爭取績效而便宜行事之行爲，方足以符合個人警察資料流通保護之相關原則。另就資料安全面觀察，個人警察資料之濫用、盜用或誤用之情形則相對較其他一般性個人資料之安全更形重要，則全民指紋建檔之個人資料是否於我國能有足夠能力對相關安全措施加以維護，也是亟需加以考慮的[77]。

---

[75] 參：劉坤旺，前揭文，頁 115。

[76] 參：記者周盈成，＜查贓車專家 幫警方作績效＞，2003/08/10 聯合報：

…五十二歲的胡榮文像平日一樣，**拿著警用小電腦**在台北縣新店市巷弄中遊走，眼光掃過路邊成排或零散停放的機車，偶爾動動大姆指，熟練地在電腦上鍵入車牌號碼查詢是不是贓車。

**胡榮文不是警察**，曾當過七年的義警。…**員警查贓車績效被上級逼得緊，但各種勤務繁重，沒時間查贓**；如果認識胡榮文，事情就好辦多了。

**他找車的利器，就是那台警用小電腦。據他表示，是台北市某分局員警買給他用的。裡面所含的失車資訊，必須每天在「公司」或其他警察單位更新。**記者隨行採訪一個多小時，胡榮文果真當場打出一部報竊的機車，他隨即打電話回「公司」確認，請「公司」聯絡失主。

…胡榮文說，**自己是台北市唯一非警察而持用警用小電腦查贓車的**。對此，台北市警局保安科也證實。（黑體字部分爲作者強調處自行改變字體）

[77] 此部分另一立論可參考司法院大法官解釋釋字第六零三號解釋理由書中，聲請釋憲人之立論「…二、戶籍法第八條第二項強制十四歲以上國民於請領身分證時按捺指紋，因侵犯人性尊嚴、人身自由、隱私權、人格權及資訊自主權等基本權利，並違反比例原則、法律保留、法律明確性及正當法律程序原則而違憲：（一）指紋資料構成抽象人格一部分，爲人格權之保障範圍，且基於指紋資料可資辨識個人身分等屬性，其公開與提供使用爲個人有權決定事項，應受憲法上隱私權及資訊自主權之保障。戶籍法第八條第二項強制採集人民指紋，建立資料庫，不僅侵入個人自主型塑其人格之私人生活領域，侵犯人民人格權，並限制人民對其個人資訊之自

## 四、 個人線上服務資料

我國由於在全球化影響下，網際網路之使用相當普遍，也因此在先進國家網際網路使用上會發生之獨特議題，在我國同樣也會發生。而關於網際網路相關線上服務所處理之個人資料之保護，在台灣也成了一件新興的話題，在未來的發展上相關類似之問題，只會更加突顯其嚴重性，因爲網際網路相關資料之處理必定全部或部分涉及自動化之電腦設備，則相對於其個人資料之收集與處理上必定更加廣泛與快速，故而本節提出第三項我國出現之實際案例，即關於網際網路之個人線上服務資料，同樣以本文前述提到之歐洲相關經驗對之加以評析。

本文以下對於我國個人線上服務資料之相關討論將聚焦於對我國國內相關網際網路之網站在線上服務時，所收集與處理之個人資料提出討論，觀察其是否歐洲經驗有所差異。在關於國內網站個人線上服務資料部分，需先加以討論的是我國網站所收集之線上服務個人資料及會員資料，是否受我國「電腦處理個人資料保護法」之規範？由於「電腦處理個人資料保護法」範圍限於自動化處理而網站屬之，故而原本照常理言，其所處理之個人線上服務資料當然是在「電腦處理個人資料保護法」之射程內，但是弔詭的是，我國「電腦處理個人資料保護法」

---

主權、隱私權。（二）戶籍法第八條第二項要求所有十四歲以上國民按捺指紋，卻未明定蒐錄指紋之目的，違反限制基本權利之法律須於法律中明示其目的之原則。…亦非達成目的之最小侵害手段，其所能達成之效益與所造成之損害間不合比例，違反比例原則。（三）強制人民按捺指紋並錄存爲影響人民權利重大之公權力行爲，應以法律爲明確之規定。現行戶籍法第八條之立法目的、按捺並錄存指紋之用途不明確。且戶籍法第八條第二項之規定，…違反法律保留原則。（四）強制按捺指紋性質上屬於強制處分，須依憲法第八條及刑事訴訟相關法律始得爲之，現行法使行政機關得事前逕予蒐錄人民指紋資料，違背正當法律程序原則。（五）世界各國要求指紋與證件結合之實例，往往限定於特定用途之證件，用來便利查核身分或資格之有無，即使在蒐集和使用國民生物特徵資料的國家，對於是否建立集中型的生物特徵資料庫，通常採取否定的態度。…三、戶籍法第八條第三項之規定因違反不當連結禁止原則、比例原則及平等保護原則而違憲：（一）戶籍法第八條第三項以發給身分證爲條件強制人民按捺指紋，然國民身分證與指紋錄存間無實質關聯，以不捺指紋爲由拒絕發給國民身分證，違反不當連結禁止原則。（二）爲達到強制人民按捺指紋之手段中，有較不發給身分證侵害更小之手段，且以按捺指紋作爲發給身分證之條件，所欲追求之利益與人民因此造成之不利益間，不合比例。（三）在身分識別文件發給事項上，國家基於憲法所不許之理由拒絕部分國民領取身分證，違反憲法平等保護原則等語。」

另將適用對象分爲公務機關與非公務機關二者，則姑且不論公務機關之網站當然是「電腦處理個人資料保護法」之範圍，但真正的焦點在於私人之非公務機關網站是否受到「電腦處理個人資料保護法」之規範？

對此國內相關論述[78]認爲其雖非明文將其列入，但解釋上仍應認爲其在「電腦處理個人資料保護法」之範圍內，蓋「電腦處理個人資料保護法」第三條第七款對於非公務機關之定義爲：徵信業及以蒐集或電腦處理個人資料爲主要業務之團體或個人（第一目）或醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業（第二目）或其他經法務部會同中央目的事業主管機關指定之事業、團體或個人（第三目）。則網站最有可能落於電信業之範圍，但依「電信法」第十一條[79]，並未對於電信事業之範圍明確規定，則依交通部電信總局所公布之經營第二類電信事業申請書附件「經營業務申報表」中，相關數據類之業務與網站業務多有雷同，故仍會落於電信業之範圍。

但電信法於中華民國九十一年七月十日公布增訂第廿條之一[80]後，應已經有較確定之法規範將網站經營者歸類於電信業第二類之內。依該第廿條之一第六項規定，「從事電信網際網路位址及網域名稱註冊管理業務之監督及輔導事項，由電信總局辦理之；其監督及輔導辦法，由電信總局訂定之。」，另依該第廿條之一所定之「網際網路位址及網域名稱註冊管理業務監督及輔導辦法[81]」第三條，相關監督與輔導從事網際網路位址及網域名稱註冊管理業務之主管機關爲交通部電信總局，此時網站之相關業務既爲電信總局所監督輔導，當然解釋上屬於電

[78] 參：賴文智，＜網站會員資料與隱私權之保護＞，《網路資訊》，2001 年 2 月號，頁 105-107。
[79] 「電信法」第十一條：
電信事業分爲第一類電信事業及第二類電信事業（第一項）。
第一類電信事業指設置電信機線設備，提供電信服務之事業（第二項）。
前項電信機線設備指連接發信端與受信端之網路傳輸設備、與網路傳輸設備形成一體而設置之交換設備、以及二者之附屬設備（第三項）。
第二類電信事業指第一類電信事業以外之電信事業（第四項）。
[80] 中華民國九十一年七月十日華總一義字第０九一００一三六一八０號令公布。
[81] 中華民國九十二年二月十一日交通部電信總局電信公字第 09205005800 號令訂定發布全文十七條。

信業，所以我國網站所收集處理之個人線上服務資料應受我國「電腦處理個人資料保護法」之規範應無疑問。

不過我國電信業採登記之方式，而我國網站之數目如天上繁星之極其繁多，根本難以一一登記，故而實際在我國交通部電信總局依法登記者，其實僅佔小部分[82]，但在解釋上，於有經營所謂第二類電信業務時，當然應受「電腦處理個人資料保護法」法之規範。

在我國實際情況，各主要之入口網站大部分均有其所謂的「隱私權政策」或「隱私權聲明」[83]，其中有簡單說明其對於個人資料之收集與處理原則者，亦有鉅細靡遺詳加敘述者，但大多有共同之特色－－免責之聲明。在個人資料之處理方面（參：表 4-2），各網站之隱私權政策或聲明均會告知該網站有收集與處理個人資料之情形，並均告知有 cookies 之存在與功能，以及與第三者資料原則上不會交換之說明，其中微軟 MSN 入口網站與台灣新浪網並有關於兒童個人資訊的升級與使用之相關隱私權政策。本文以下以（表 4-2）爲中心，討論國內主要入口網站線上服務個人資料之隱私權政策或聲明，是否即符合「電腦處理個人資料保護法」之規範及較高標準之歐洲相關規範或學說。

[82] 參：賴文智，前揭文，頁 106。

[83] 筆者主要觀察之對象爲我國五大入口網站，其隱私權政策或聲明網址分別爲：

1. YAHOO！奇摩：http://privacy.yahoo.com/privacy/tw。2005/11/22。
2. PCHOME 網路家庭：http://event.pchome.com.tw/profile/copyright.html。2005/11/22。
3. 蕃薯藤：http://help.yam.com/policy/privacy.html。2005/11/22
4. 微軟 MSN：http://privacy.msn.com.tw/default.asp。2005/11/22。
5. 新浪網：http://www.sina.com.tw/service/privacy/privacy.html。2005/11/22。

（表 4-2） 我國主要入口網站關於隱私權政策與聲明範圍：

| | 是否告知個人資料之收集與方式 | 是否告知個人資料之分享與方式 | 是否告知COOKIES之存在與功能 | 是否告知得拒絕COOKIES與後果 | 提供聯絡管道之方式 | 與第三者之連結 |
|---|---|---|---|---|---|---|
| **YHAOO！奇摩** | ○ | ○ | 另有主題網頁 | 另有主題網頁 | 電子郵件 | 容許在網頁上放置橫幅廣告的其他公司在電腦中設定並存 cookie |
| **MSN 台灣微軟** | ○<br>有兒童升級之保護 | ○ | 最完整 | 最完整 | 電話、電子郵件或郵件[84] | 部份網路廣告會在電腦中放置一個永久的 Cookie； |
| **PCHOME ONLINE 網路家庭** | ○ | ○ | 相對較簡單 | 相對較簡單 | 電子郵件 | 可能包含其他網站或網頁的連結不論關於其內容或隱私權政策，均與其無關。 |
| **YAM 蕃薯藤** | ○ | ○ | ○ | ○ | 電子郵件;但於線上服務則另有國內電話與傳真 | 使用者連結至第三者網站進行線上購物，對方應有其個別的隱私權保護政策，其不負任何連帶責任。 |
| **SINA 新浪網** | ○<br>有兒童升級之保護 | ○ | ○ | ○ | 電子郵件 | 使用者連結至第三者網站進行線上購物，對方應有其個別的隱私權保護政策，其不負任何連帶責任。 |

[84] 但電話及郵件聯絡方式均爲國外之（微軟總部）通訊方式。

作者自繪。資料來源：各入口網站關於隱私權政策或聲明網頁；瀏覽日期：2005/11/22。

首先在「電腦處理個人資料保護法」方面，第十八條第一款的「經當事人書面同意者」即有疑問，蓋一般網頁上「點選之同意」是否爲書面是有疑問的。解釋上，若僅依「電腦處理個人資料保護法施行細則」第三十條「當事人書面同意，指依書面之記載，足認當事人已有同意之表示者（第一項）。非公務機關基於特定目的，爲取得當事人書面同意，於初次洽詢時，檢附爲特定目的蒐集法定代理人收受，而未於所定期間內爲反對之意思表示者，推定其已有同意之表示（第二項）。」觀之其仍僅限於基本之書面形式，但若對照刑法第二百廿條第二項「錄音、錄影或電磁紀錄，藉機器或電腦之處理所顯示之聲音、影像或符號，足以爲表示其用意之證明者，亦同。」與第三項「稱電磁紀錄，指以電子、磁性或其他無法以人之知覺直接認識之方式所製成之紀錄，而供電腦處理之用者。」則該網站之同意似可解釋爲書面同意。另外，「電子簽章法」第六條第一項「文書依法令之規定應以書面保存者，如其內容可完整呈現，並可於日後取出供查驗者，得以電子文件爲之。」亦爲相同之解釋。

但由於上述解釋乃透過其他立法體系加以解釋，並非由「電腦處理個人資料保護法」直接闡明，故在我國實務上各網站爲規避可能之責任，於將其所有之個人線上服務資料與第三者廠商合作時，會以其會員（資料當事人）資料擁有者之名義對會員發出第三者之廣告，使會員不能主張該網站違法外洩資料，並均先有相關之免責聲明（參：表 4-2）。

另外亦有論述指出[85]，該等網站之相關隱私權政策或聲明均非採取積極的主動告知方式，而是在各首頁底下有一不盡顯目之連結，使用者必須自己積極搜尋

[85] 參：戴皖文；邱建勳，＜個人資訊隱私由誰來把關＞，台灣人權促進會企畫，李茂生主編，《2001年台灣人權報告》，台北：前衛出版社，2002 年 9 月，頁 53-55。

並閱讀多頁之相關政策與說明方能對之理解；其次，雖如上（表 4-2）中各網站均有關於 COOKIES 之相關介紹，但都僅說明其設置原因與所帶來之好處，並且在說明得拒絕存取時，卻告知將不得享有部分之服務，故論者以爲有間接誤導消費者（資料當事人）之嫌。

事實上，對照歐洲也有相同之問題，並且歐洲方面也對之加以關切[86]。由本文第三章之論述中不難發現，歐洲對於網際網路之個人線上服務資料保護，其實投注相當多的注意焦點與辯論，故而其關於個人線上服務資料之保護在法規範架構上是相當先進的，若以其經驗觀察我國網站之上述可能缺失，則至少會發現以下問題：

1. 未有專門之法律對目前嚴重之網際網路個人線上服務資料加以保護[87]：「電腦處理個人資料保護法」由上述之書面等問題，並無法對個人線上服務資料直接而有效的處理，相較於歐洲聯盟之指令的專門性，我國甚至連歐洲理事會之建議性指導方針官方文件都沒有，在現行「電腦處理個人資料保護法」修正草案遲遲未通過前，對於個人線上服務資料保護之漏洞大開。

2. 業者消極之態度：相關網站業者對於隱私權責任雖均有提出相關說明，唯並未有如歐洲理事會「個人資料保護指導方針」指出之積極的對資料之使用應有責任並公布隱私權政策之態

[86] 參：＜歐盟保護隱私權 盯上微軟.Net Passport＞，2002/05/28 ，歐洲日報：
微軟公司自網際網路蒐集使用者個人資料的系統是否觸犯隱私權保護法，已引起歐洲聯盟執行委員會的調查，爲軟體巨人在歐洲面臨的反托辣斯案調查增添麻煩。
在回應歐洲議會荷蘭籍議員梅桀（Erik Meijer）質詢的書面答覆中，歐盟執委會宣布，已針對微軟.Net Passport 免費服務展開調查。執委會歐盟區內市場委員柏克斯坦（Frits Bolkestein）寫道：「委員會正與各國資料保護當局聯合調查此案，查明該系統是否遵守歐盟的資料保護法。」
微軟.NET Passport 系統透過電子郵件地址或其他網站，在使用者上網購物、玩遊戲或與銀行交易時，蒐集用戶的個人資料。梅桀質疑此服務的合法性。他並指出，未向.Net Passport 註冊，會遭許多網站拒絕存取，但一旦註冊使用，就不可能退出。

[87] 事實上，網路之相關科技法律本來就較難去立法釐清，論者有謂其如急奔中的馬之法律，謂其經常混亂而難釐清，但細究之下仍如現實生活般有一定規律可供釐清。See: Lawrence Lessig, *The Law of the horse: what cyberlaw might teach*, Harvard Law Review, 113 Harv. L. Rev. 501, December, 1999.

度，相反的採取一種較爲消極且不明顯之方式公布其隱私權政策。另外這種消極性也出現在與業者之聯絡方式上面，君不見在一般事項上業者大多僅以電子郵件方式爲聯絡管道，於關係商業利益之線上購物方面，才有較能迅速得到回應之其他管道，甚至有些網站對此僅有相對之下顯的消極的單一電子郵件聯絡方式。（參：表 4-2）

3. 未明白表示使用者有「加密」、「安裝相關電子追蹤系統」、「匿名化」等權利。

4. 相對於歐洲區域組織對於相關學術會議或圓桌會議召開後即有確實之執行動作，我國的「電腦處理個人資料保護法」從民國八十四年公布至今，明顯已經追不上科技潮流，雖已經出現修正草案，卻也未真正修訂完成。至於各別領域之個人資料保護完整法律，卻大多限於程序上或收費之標準問題，實質上問題並未解決，在網際網路個人線上服務資料方面尤是！

## 五、 小結

本節舉出三個我國已發生（IC 健保卡）、正發生（網際網路線上服務個人資料）與即將要發生（全民指紋建檔）之案例與歐洲之相關經驗加以對照後發現，不論在哪一方面都有許多缺失之處，顯見我國關於個人資料保護之問題並不若歐洲一般受到重視。

問題之癥結所在，筆者認爲在政府相關政策方面，不論是健保 IC 卡政策或

是全民指紋建檔議題之拋出，似未將個人資料保護視爲一項人民重要之基本權利之一，這單就我國「電腦處理個人資料保護法」觀之即爲以足。蓋雖然我國之「電腦處理個人資料保護法」在世界上算是相當先進的，但是卻未有後續重要的與時並進。須知個人資料保護之所以在這個網路世紀被重視，就是因爲其所擁有的快速發展與不可預知性，對於個人資料隱私在自動化設備大量交叉比對分析後，有著嚴重的潛在威脅，故而不論是歐洲的相關法規範模式或美國式的業者自律自由模式，均保持著所謂「與時並進」的腳步；反觀「電腦處理個人資料保護法」，雖增修草案已然出現，但卻已經推出多年而未立法，也無相關替代措施，則吾人以爲歐洲模式的相關法規經驗實在值得我國在發生相關案例時加以思索。

## 第四節　結語

本章先以我國之個人資料保護之法規範中心「電腦處理個人資料保護法」論述，其次對於相關之法規諸如「通訊保障及監察法」與「檔案法」以及個人醫療資料、個人警察資料與網際網路線上服務之個人資料相關法規，並發現歐洲模式能對之加以比較的主要立論點，即在於發現我國之以「電腦處理個人資料保護法」爲中心法規範之立法方式，與歐洲理事會以「個人資料保護公約」爲中心；歐洲聯盟以「個人資料保護指令」爲中心之規範方式，有相通之處，故而認爲歐洲經驗的實際相關案例，對我國亦應可以有相當程度的啓發作用。

在仔細驗證之後，發現我國不論在現行「電腦處理個人資料保護法」本身之規範上可能有許多漏洞，且在個人醫療方面之法規範與關於已實施之全民健保 IC 卡政策方面，著實有許多缺憾。而這些缺憾也對人民的個人資料保護造成許

多潛在之危機。不僅如此，甚至在爭議中的全民指紋建檔議題與相關個人警察資料之保護，或是未爲相關立法的網路個人線上服務資料與網站管理也好，均未能跟上資訊快速進步腳步之法規出現。

在今年（2005）年，由於身份證即將全面重新換發而由戶籍法第八條所引起的全民指紋建檔一案[88]，再度受到各方與媒體之重視。在這波換發風波中，行政機關以種種理由希望能建立全民的指紋檔案，但是遭受各界質疑與批評，在大法官做出相關解釋之後，風波暫時告一段落[89]，卻也讓人不得不深思，個人資料保護的重要性難道在行政機關的便宜與經濟原則、強調打擊犯罪（卻不一定能治標治本的達到目的！）口號下，會被整個的犧牲掉[90]。

故而，本文在下一章節裡面，便提出一些以歐洲經驗爲出發點之觀察，供我國在相關立法或實際案例發生時改進之建議，期能對我國個人資料隱私保障有所助益，也驗證我國對於個人資料保護相關作爲是否與領導人權區是的歐洲之潮

---

[88] 參：東森新聞報，＜侵犯人權！　拒按指紋社團發起連署　聲請大法官釋憲＞：
記者邱瓊平／台北報導
按了指紋、治安不一定會更好！包括 56 個團體、立委、學者所組成的「拒按指紋 524 行動聯盟」24 日舉行記者會指出，他們無法認同政府以「維護治安」的理由推動這項政策，這明顯違憲，侵犯人權和自由人權，因此，要求立法院就戶籍法第 8 條聲請大法官釋憲與暫時處分。拒按指紋 524 行動聯盟指出，86 年 5 月 21 日修訂公布的戶籍法第 8 條規定「人民年滿 14 歲者，應請領國民身分證，未滿 14 歲者，得申請發給。依前項請領國民身分證，應捺指紋並錄存。但未滿 14 歲請領者，不予捺指紋，俟年滿 14 歲時，應補捺指紋並錄存。請領國民身分證，不依前項規定捺指紋者，不予發給」。 也就是說，戶籍法第 8 條引發人權的爭議，幾乎已經確定違憲，這也是行政院法規委員會在內的多數法律人的專業見解。因此，24 日站出來的社團與立委、學者要求「我不捺指紋，給我身分證」，並展開連署，目前已有近百團體連署，以個人名義連署的則有 380 人，目前人數還在持續增加。拒按指紋 524 行動聯盟也說，該條文法律問題重重，甚至沒有包括強制全民換發身分證必須按捺指紋的明文授權。因此，該聯盟認爲立法院應該善盡國會監督責任，對行政院矛盾作爲提出質疑與譴責。同時也要就戶籍法第 8 條向大法官申請釋憲，並聲請停止按捺指紋執行的暫時處分。（2005/05/24）
URL： http://www.ettoday.com/2005/05/24/10844-1794608.htm。

[89]參：東森新聞報，＜按指紋才能請領或換發身分證　行政院暫緩執行＞：
記者鄧若寧／台北報導
針對大法官作出戶籍法第八條第二項及第三項規定，以按捺指紋始得請領或換發身分證之規定，在本案解釋公布之前，暫時停止適用，行政院發言人卓榮泰表示，會遵守大法官決議，按指紋始得請領換發身分證政策暫緩實施。
卓榮泰說，在大法官釋憲結果出爐前，7 月 1 日起，滿 14 歲請領身分證或換發身分證的民眾，將會領取到舊版身份證。（2005/06/10）
URL： http://www.ettoday.com/2005/06/10/301-1801943.htm。

[90] 對此，我國相關人權團體也提出了許多呼籲。例如，台灣人權促進會即提出許多相關的意見。參：URL： http://www.tahr.org.tw/index.php/categories/tw/campaigns/privacy/paper/。

流相切合。

# 第五章　對台灣個人資料保護之建議

## 第一節 概說

在前幾章中本文已對於歐洲對於歐洲之個人資料保護經驗從法規範層次一直討論到實際執行上的案例層次，並且已經對歐洲與我國相關個人資料保護之間進行了法規範與實例上之比較，並進而發現我國相關做爲之諸多可能缺憾。故於本章中，分別對於我國之相關作爲在法規範上與在實際執行上所能有之加強之處，做一建議。

事實上，對於我國對於個人資料保護法制或是實施面向的之諸多缺失，已有部分相關論述加以建議其應有之改進方向，惟其大多以純法律面或純資訊面加以觀察比較，而較缺乏以對於歐洲從人權傳統以來整個實際發展之系統化觀點來討論之後，方對我國與歐洲經驗銜接之比較法上之整體觀察，由於前文已經提到歐洲對於個人資料保護之發展一向能影響其他區域或國家甚劇，這在其經過了歐洲聯盟的半世紀多的整合之路[1]後，更加可能因爲其在國際關係上之政治影響力去影響其他國家或區域組織，所以本文以歐洲之出發點對我國相關作爲提出建議。

我國雖然未必要全盤接受歐洲對於個人資料保護之全部觀點與作爲，但是由於資訊全球化之趨勢已經難以阻擋個人資料之跨國傳輸，更不可能去略過貿易實力在 2004 後增爲 25 國的歐洲聯盟或是其他歐洲國家，故而強化我國對於個人資料保護之能力實有其必要性[2]，特別是若能對於歐洲相關作爲能有多一點

[1] 關於歐洲統合的歷史以及相關重要理論之介紹，詳參：張亞中，《歐洲統合：政府間主義與超國家主義之互動》，台北：揚智出版，1998。

[2] 其實政府之相關單位也已經注意到了歐盟在這方面所佔有之重要角色，並亦希望能有相關之意見。參：法務部法律事務司，《檢討電腦處理個人資料保護法實施狀況公聽會會議實錄彙

銜接的話，對於我國與歐洲聯盟或其他歐洲國家乃至於受到歐洲影響之其他國家或地區之貿易或其他交流，想必能更加順利。除此之外，我國對於人權中的資訊隱私與個人資料保護權所提升，進而真正走向民主法治。

## 第二節　法制層面之建議

### 一、 關於「電腦處理個人資料保護法」

我國之「電腦處理個人資料保護法」已經未能跟上時代腳步，不需贅述。以下僅就前章中發現與歐洲法規範[3]無法銜接之處爲相關之建議：

（一）　範圍方面的問題：

關於範圍之問題又可細分爲二類：其一爲我國「電腦處理個人資料保護法」究應採如歐洲理事會「個人資料保護公約」僅限於自動化處理之個人資料，抑或如歐盟「個人資料保護指令」般除自動化處理外並及於非自動化處理，但建立全部或部分檔案系統均爲保護對象之問題；其二爲我國區分公務機關與非公務機關後，非公務機關之範圍問題。

1. 將範圍擴大至非人工處理但系統化建檔之個人資料：

在第一個問題中，吾人以爲在歐洲理事會「個人資料保護公約」中雖規定僅限於自動化處理之個人資料方爲規範對象，但亦鼓勵會員國得將範圍擴大至其他非自動化處理之資料部分。又歐洲聯盟之「個人資料保護指令」雖將該範圍擴大至非自動化處理之資料，但又限制爲需爲系統化建檔方屬規範對象，此

編》，台北：法務部，2002 年 2 月，頁 78，法務部林錫堯次長發言。

[3] 事實上對於我國之「電腦處理個人資料保護法」在法規範上迭有批評，並不只限於以歐洲相關作爲爲出發點者，舉凡在我國法制本身、歐洲、美國與其他外國立法例之間，都可以比較發現出缺失之處，但本文既以歐洲爲研究範圍尤其只將焦點集中於歐洲理事會與歐洲聯盟二者，以避免範圍過大而失焦，合先敘明。

種立法方式能將一些雖非經由電腦處理，卻可能更直接侵犯個人資料隱私之行爲加以保護，例如我國鄉下地方或許多較爲老字號之中小型醫療院所並未將病歷均全部自動化處理，仍有維持以人工方式系統化建檔者；又如傳統小型婚友社亦有習慣以傳統方式人工建檔者，能得到許多包括財力、學歷、健康等敏感性資料，若任意流傳買賣更會對該資料當事人造成相當大之困擾。

則在上述理由下，依「個人資料保護指令」之見解顯然也不違背「個人資料保護公約」之規範範圍之本意，則我國「電腦處理個人資料保護法」也應當考慮將範圍擴至如「個人資料保護指令」般，以真正體現個人資料保護之精神，並避免資料處理者依其他迂迴或規避之方式將資料分爲數小部分，再分別以非自動化方式存檔；甚至爲避免非自動化處理規範可能帶來過大衝擊，可以使之適用簡化登記之行政程序[4]。

2. 非公務機關之範圍不以列舉式規範[5]：

不論是「個人資料保護公約」或是「個人資料保護指令」，均未有如「電腦處理個人資料保護法」般區分公務機關與非公務機關已若前述。我國雖仿德國之立法例將其區分開來，但是卻將非公務機關加以列舉。其立法之本意乃爲考量將所有非公務機關種類全部規定保護在當時恐怕衝擊過大，因此僅將最容易大量收集處理個人資料之行業納入，但是事實上近來之發展已經發現不僅此八大行業會有大量個人資料，諸如電子商務等其他行業均會觸及之，則似應轉換爲如德國「聯邦個人資料保護法」第二條第四項[6]之以概括之立法方式規定，並將非公務單位於從事公行政之公權力職務範圍內之行爲，視爲公務機關，以將長期以來公立學校或公立醫院等需靠解釋方知所屬之機關加以明白定義。甚

[4] 參本章第三節第一項。
[5] 事實上這方面是我國大多學者或實務工作者最常質疑之處，參法務部，前揭書。另外，在修正草案中也有相似之規定。
[6] 其規定：非公務單位指不屬第一項至第三項之自然人私法人公司或其他私法上之人合團體；非公務單位於從事公行政之公權力職務範圍內，屬本法所稱之公務單位。

至如「個人資料保護指令」、「個人資料保護公約」一般，只以收集處理個人資料之行爲爲區分方式，而不考慮永遠會一直新增的行業別分類方式[7]，以符合未來之可能變遷，避免經常需解釋或修正法律造成法之不安定性。

3. 不論直間接途徑均應保護：

「電腦處理個人資料保護法」所規定第三條之「足資識別該個人之資料」解釋上有僅指向直接途徑所得之個人資料方受保護，但事實上，在歐洲的經驗裡爲了避免規避或是爲了更完整保護，均無直間接途徑之區分而一體適用保護。在此方面，「電腦處理個人資料保護法」應對之明文化，使解釋上不致有誤會產生。

（二） 架構上之問題：

1. 將基本原則明白表示：

諸如「個人資料保護公約」、「個人資料保護指令」等均將個人資料保護之基本原則加以明白條列可避免疑義，並收有所遵行之效果，不致如現行「電腦處理個人資料保護法」般散落於各條文之中，且許多原則需透過解釋，則易令一般民眾或不具大規模之相關業者難以遵從。事實上爲使一般民眾易於瞭解相關法令，歐洲理事會甚至有「個人資料保護指導方針」，透過一種類似宣導方式之簡單文字爲之。

2. 不必要將許多例外之規定過於嚴苛，並減少不確定法律概念：

「電腦處理個人資料保護法」中過多個人資料保護原則之例外規定，且多有不確定之法律概念。「個人資料保護公約」、「個人資料保護指令」雖也都多多

[7] 另外若考慮行業別的話，也有可能會碰到難以歸類之例子。例如現在流行的網路人力銀行業可能屬於人力服務業（受就業服務法規範）、資訊處理業（透過資訊流通）、網際網路業（以網路爲之），甚至是廣告業（與一般報紙徵人廣告同，不過換至網路平台）等等，則究竟應以何者爲準則難以評斷。

少少有相關之例外，卻也未若我國「電腦處理個人資料保護法」一般之「完整」，大多在最重要之情形下爲之，以同時在促進資訊自由流通與個人資料保護下求取平衡。

（三） 內涵上之問題：

1. 敏感性資料之特種保護原則：

不論是「個人資料保護公約」、「個人資料保護指令」甚或其他許多關於個人資料保護之相關立法例中，均有將特別具敏感性之個人資料種類加以特別保護之基本原則存在，獨我國「電腦處理個人資料保護法」缺少之。不分寬鬆一體適用之結果，不但對於敏感性資料如個人之醫療資料或個人警察資料等等無法特別加以保護之外，對於其他較非敏感性之資料由於可能導致進退失據，而使實際執行保護時過於嚴苛，甚至規範過多之行政相關程序，反易造成資訊流通之障礙，或是如我國現狀一般實際通過行政程序者寥寥可數。

2. 損害賠償：

「電腦處理個人資料保護法」第廿七條第三項已然規定「前二項損害賠償總額，以每人每一事件新臺幣二萬元以上十萬元以下計算」，所以個人資料平均價碼爲此。雖然能證明其所受之損害額高於該金額者，不在此限（第廿七條第三項），不過第四項卻規定「基於同一原因事實應對當事人負損害賠償責任者，其合計最高總額以新臺幣二千萬元爲限」，對於牽連可能甚廣的個人資保護案件來說，不一定能符合實際之需要[8]。即便在新草案中提高其價值，卻也不一定能確實填補損害之價值。反觀「個人資料保護公約」或「個人資料保護指令」均未對此提出上限，其實只需按實際損害金額由法官依個案認定即可，又或擔心

[8] 觀諸該法條之結構，應爲模仿德國「聯邦個人資料保護法」第四十三條第三項之「第一項之違反秩序處五萬德國馬克以下之罰鍰；第二項則處五十萬德國馬克之罰鍰」，但該條款卻是另外由行政機關處以罰鍰之規定，而非對被害人之損害賠償，豈可混爲一談。

賠償金額法官可能認定過低，則設相關下限亦可。

## 二、 關於個人醫療資料

關於我國個人醫療資料方面，最受爭議之所在爲：究竟「病歷」是否爲個人資料？其所有權究竟屬於醫師或是該病人（資料當事人）？若所有權屬於醫師，則該病患是否有知悉所有病歷甚至取得影印或備份之權利？而之所以會有上述爭議，是因爲「電腦處理個人資料保護法」並未明確規範「病歷」是否爲個人資料，更未如「個人資料保護公約」或「個人資料保護指令」直接指定其爲特種之敏感性個人資料。

之所以會有「病歷」是否屬於個人醫療資料之一環的主要爭議點爲，醫療院所或醫師經常會擔心該病歷若落至病人手中，將來可能會成爲醫療糾紛中的「呈堂證供」，或是其獨到之醫療手法外流，而失去「獨門武功」。故認爲該「病歷」應爲醫師之診斷書，爲一種醫學上之「裁判」，理應所有權屬醫療人員所有；但相反的，病人部分卻主張「病歷」乃由其身所出，縱使爲醫師之「裁判書」，也應該使「訴訟當事人」的病患去得到訴訟之結果，並有備份之權利。

按歐洲理事會「醫療個人資料保護建議」的第一部份之解釋，「醫療資料」爲有關個人健康之所有資料，則當然包含所謂「病歷」之資料。又「個人資料保護公約」或「個人資料保護指令」也均將醫療資料列爲特種個人資料，則其當然爲個人資料之一種殊無疑問。

至於其所有權方面，由第三章（圖 3-1）之標準醫療資料流通模式圖看來，個人醫療資料必定經過資料當事人（病患）與醫療院所或醫師兩個階段，則其所有權誰屬必定均有其理由與爭議。但不論是所有權誰屬，該資料當事人有充分基本之閱覽權與複製權是無疑問的。誠如上述，即便認爲該病歷是醫師之「裁

判書」，也應該使「訴訟當事人」的病患去得到訴訟之結果，並有備份之權利！甚至，在歐洲人權法院 *M.G v. The United Kingdom* 案中，判決也指出相關政府單位應有積極之義務，提供完整而無遺漏之當事人所要求之個人資料，而並非由該單位決定提供資料之多寡，則明顯可知至少當事人之接近查詢權（right to access）是一定存在的。

吾人建議「電腦處理個人資料保護法」應儘速明文規定個人之醫療資料包含，病歷，並將其列入特種（敏感性）個人資料中，以加強保護。

## 三、 關於個人警察資料

我國關於個人警察資料之管理雖有「警察職權行使法」第二章爲相關之規範，但究其內容均爲關於個人警察資料之收集或銷毀，偏重於使警察人員能有職權去收集個人之警察資料。但對於個人警察資料所應有之個人資料保護基本原則卻並未完整規範，例如在公開化、知曉個人警察資料之權利、修正與接近之權利等，均無規範，明顯非專爲個人警察資料之保護法律，而是所謂個人資料保護例外之大全。

相對的在個人資料保護面向上，關於個人警察資料只有「警察機關資訊安全實施規定」、「內政部警政署電子計算機作業保密安全實施規定」、「內政部警政署受理犯罪資料查詢作業規定」等等內部機關之行政命令，並未有專門法律之出現，相對於歐洲理事會「關於警察部門之個人資料保護之建議」與歐洲聯盟「針對加強對抗嚴重犯罪之意見」的重視程度與保護程度言，誠有不足，則吾人認爲應儘速制定關於保護個人警察資料之專法。

## 四、 關於個人線上服務資料

網際網路時代來臨，新興事物與態樣頻繁發生，對於我國「電腦處理個人資料保護法」帶來許多衝擊，該法舊有之規範體系與內容顯已不足敷用，論者也對此多所批評。

當前最重要的是，無論是在原有的「電腦處理個人資料保護法」中另增新條文甚至專章，對於網際網路之個人資料保護問題加以處理，或是乾脆如歐洲區域組織一般另外專門對此問題立法之方式(如:「個人資料保護指導方針」、「電子通訊個人資料保護指令」)，總之該問題已經具有相當程度之迫切性，儘速通過立法之態式已經是最基本之要求。

在應特別注意之網路線上個人資料特有之保護原則上，對照歐洲理事會或歐洲聯盟之相關經驗，至少要有如下之保護：

1. 網際網路上保護之客體範圍：

網際網路有其不同於現實生活中的客體保護範圍諸如電子郵件地址(email address)、網際網路通訊協定位址 (IP address)、網域名稱 (domain name)、不變資源定位址 (Uniform Resource Locators; URL)、使用者名稱（Username）、通行碼 (Password)[9]甚至網路個人線上資料之位置資料（location data）、電子通訊資料（traffic data）、通訊（communication）等等都相當與一般現實生活中的姓名、出生年月日、身分證統一編號、特徵、指紋、婚姻、家庭、教育、職業等等觀念不同。在網路特有之資料中有直接途徑可辨識特定個人者，也有需要間接途徑方得辨識個人者，依前述歐洲之體例均應有所保護。

2. 個人資料保護之安全原則：

[9] 關於各該名詞之間接或直接性，參：法務部，前揭書，頁 134-135，林宜隆教授發言。

在網際網路上由於與現實生活中之個人資料保護方法不盡相同，諸如書面登記等均有基本概念上之不同，並且由於網路具備高技術性，其安全方面之保護原則更應強化保障[10]。例如「個人資料保護指導方針」即開宗明義稱網路是不安全的，往往有許多危險存在，但其實有許多方法可以對之加以預防等等，其也提供諸如加密（encryption）、匿名化、安裝相關電子追蹤系統等等方法，並加強宣導線上所處理之資料網路使用者需對之負責，籲請勿寄發有惡意之信函。又「電子通訊個人資料保護指令」也規定電子通訊服務之提供業者應提供適當之技術及組織化之方法，以保障其所提供服務之網路隱私安全；在用戶有可能發生安全上之危險時，必須盡告知義務，包括告知各種可能之救援方法及所需之花費等，顯示其應特別強化在安全部分之保護原則。

3. 與國際之接軌：

未來由於歐盟在個人資料保護規範上之堅持，所以欲與之貿易或爲其他方面之交流的各國均需對該問題加以重視，尤其網際網路之全球化性質濃厚更是如此。論者也有特別提到，在世界貿易組織（World Trade Organization, WTO）架構下在個人資料隱私下有可能成爲整合相關議題之論壇之所在，可能出現並推動所謂類似「資訊隱私一般保護協定（General agreement on Information Privacy）」之協商倡導[11]，則未來在推動網際網路個人資料保護之立法時，必須特別注意國際接軌之問題。

4. 其他基本原則之需要：

[10] 針對私人企業如 ISP 業者等，應強烈建議使用關於企業之建構安全管理方案，並分別從內外部與整體之環境加以觀察，詳細企業建構安全管理方案之流程與內容，可參考：丁惠民，＜電子化時代的管理新議題：網路安全與隱私權保護＞，《電子化企業-經理人報告》，台北：ARC 遠擎管理顧問公司，第 9 期，2000 年 5 月，頁 22-25。

[11] See Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 2000, pp. 1359-1362.轉引註自：劉靜怡，＜資訊隱私權保護的國際化爭議--從個人資料保護體制的規範協調到國際貿易規範的適用＞，《月旦法學》，台北：元照出版，第 86 期，2002 年 7 月，頁 202，註 31。

除上述網路線上個人資料應特別注意之方向外，在一般基本之原則上諸如資料品質原則等均應有所基礎之保護。

### 五、 小結

如上述我國現行相關個人資料保護其實最應改進者不出保護範圍之完整性之強化與新興科技與發展議題之因應二者但是在此些部分擴大落實保障個人資料權利，雖然有利於增加網際網路使用者、消費者等資料當事人之保護，然而，保護範圍擴大與否，亦應顧及是否將會限制電子商務產業或其他各方面之發展。倘若網際網路上蒐集、利用個人資料行爲亦納入規範之內，而沒有所謂商業使用、促進競爭發展之空間存在的話，對於電子商務業者勢必將造成不小之衝擊，另外在其他方面之相關業者諸如銀行保險醫療通訊徵信傳播等也會面臨許多不適應，所以關於保護客體範圍當然不可以無限制擴大至妨礙資訊之自由流通。而這在歐洲的相關法制中也是最重要的精神，故筆者認爲，循序漸進與個人資料隱私保護和資訊自由流通的平衡，是推行上述建議規範的重要方針與基本精神。

## 第三節 執行層面之建議

### 一、 關於「電腦處理個人資料保護法」

1. 設立獨立之主管機關：

在歐洲個人資料保護中設立獨立之機關或單位常是相當普遍且重要的一環，不但可體現政府重視個人資料保護之企圖，更可以使整個個人資料保護之實際執行上更有效率。觀諸我國現制相關之業務乃由法務部所轄且極少之人力

加以管理，則推動起來當然困難重重。論者另外也有指出[12]可在法務部中設立一個局處來對之加以專門管理，並且認爲此舉並不會違背所謂該專責管理機構的公開獨立原則。吾人以爲退萬步言，縱使認爲我國國情與實際執行上推動一專職之主管機關會有所困難，也應仿效歐盟成立一專門之權益保護工作小組[13]，獨立行使諮詢或其他功能（例如強化對於個人資料保護之宣導）之職權。

2. 輕度管理原則：

我國「電腦處理個人資料保護法」第十八至廿條中規定非公務機關需向目的事業主管機關申請登記核准，發給執照，並依第廿一、廿二條公告，不但會使非公務機關怯步，更在實際解釋時，成爲由於難以使爲數眾多之公立醫院與公立學校均完成登記，故將其解釋爲公務機關的理由之一（其實應當從委託公權力行使之法理加以解釋），顯見若要所有業者一一完成登記並公告事實上有一定困難。並且，我國事業目的主管機關也因爲處理個人資料保護之人力有限，難以完成，故在我國行政程序上對於個人資料保護之輕度管理原則乃有所必要。

其實在「個人資料保護指令」相關登記之程序中亦有此輕度管理原則之體現。「個人資料保護指令」第十八條第二項規定於該資料保管人任命一專責之人員負責相關個人資料保護事項等情形，且對於資料當事人之權利與自由不致有負面影響時，即得簡化或免除登記；而同條第四項則規定，會員國得訂定合於「個人資料保護指令」第八條第二款 d 目規定之處理作業免除其登記義務或簡化其登記。而在非自動化處理之方面，歐盟「個人資料保護指令」也在第十八條第五項中規定會員國得明文規定特定或全部有關個人資料之非自動化處理之作業適用於簡化登記。

觀諸「個人資料保護指令」精神乃是爲了平衡個人資料隱私保護與資訊自

[12] 參：法務部，前揭書，頁 53，資策會戴豪君組長發言。
[13] 參：「個人資料保護指令」第廿九條、三十條。

由流通之衡平的體現，吾人以爲，該資訊自由化之體現足供我國借鏡。

## 二、 關於個人醫療資料

在關於個人醫療資料之實際執行面上就我國現行之健保 IC 卡政策言既然已經投入大筆預算開始執行則對於個人資料之相關保護當然更需要注意，以收亡羊補牢之效。筆者認爲在執行上應注意重要者例如：

1. 強化相關效率之控管，以確實達到公益大於私益之目的。

2. 避免 IC 卡之再擴充造成對於個人資料隱私之侵害。

3. 更強化 IC 卡之相關安全措施。

## 三、 關於個人警察資料

相較於全民健保 IC 卡之已經實施並投入大量國家經費已經難有回頭之可能來說，在全民指紋建檔之議題上相反的就個人資料保護觀點來說算是幸運許多。事實上個人警察資料如指紋檔案等結合個人其他基本資料後，對於各資料當事人之侵害可能性直指人權核心已若前述，並且在我國警察單位並未確實重視個人資料保護，導致時有警方人員侵害個人資料或是便宜行事等社會事件發生[14]。當這些警界之亂象並未導正之前，吾人實對於倘通過全民指紋建檔政策

[14] 諸如：記者陳舜協，＜員警與徵信業者合作調閱私人資料均被起訴＞，《中央社》，2003/07/28：「一興徵信社」負責人李政緯與台北縣警局海山分局員警陳皓榮(現已離職)兩人涉嫌合謀，由陳皓榮多次塗改、僞填單據，向民間電信業者調閱特定人的個人資料及通聯紀錄，供徵信社使用。台北地檢署今天將全案偵查終結，依僞造公文書、洩密等罪將李政緯、陳皓榮兩人提起公訴。

起訴書指稱，李政緯、陳皓榮兩人自九十年三月起，基於合謀犯意，李政緯委請陳皓榮利用職務之便，調閱特定人的行動電話通聯紀錄及個人資料，陳皓榮即利用與刑事局偵四隊偵三組隊員共同偵辦案件的機會，影印、塗改刑事局電話紀錄查詢單，向多家民間電信業者調閱三十九支行動電話的個人基本資料及行動電話紀錄。

後之個人資料隱私感到憂心。

對實際執行面向上之觀察，筆者建議：

1. 切勿貿然實施全民指紋建檔政策[15]。

2. 對於警方對個人資料隱私保護需強化其宣導，以避免政府公務人員侵害人民隱私甚至較非公務機關有更大與更經常之侵害可能性。並需導正其勿因便宜行事而任意侵害個人隱私之概念。

## 四、 關於個人線上服務資料

在網際網路之個人線上資料保護上，除了上述規範上應特別注意者外在執行上筆者以爲：

1. 強化業者自律之機制，諸如隱私權標章之實施等。

2. 強化對於使用網路者（資料當事人）個人資料保護之宣導。

---

除此之外，陳皓榮還在九十年四月到六月間，多次塗改同仁偵辦案件時向民間電信業者調閱資料的電話紀錄查詢單，調閱八支行動電話個人基本資料及行動電話紀錄。陳皓榮在獲得上述資料後即將之交給李政緯使用。

全案經刑事局偵四隊偵三組隊員發覺有異查知送辦。台北地檢署今天將全案偵查終結，將李政緯、陳皓榮兩人依僞造公文書、洩露國防以外機密等罪提起公訴。

其他另有包括：記者何祥裕、黃宣翰，＜轉賣民眾電腦資料 保警聲押＞，《聯合報》，2002/04/19；記者葉英豪、呂開瑞，＜洩漏失車資料牟利 一年上百件＞，《聯合報》，2002/04/19；記者宋伯東，＜國華等徵信社 查扣數百捲竊錄錄音帶＞，《聯合報》，2002/04/19，等等不勝枚舉。

[15] 對此，大法官亦有相似之解釋，認爲需有一定之配套防護措施後，方得爲之。參照司法院大法官解釋釋字第六零三號「...指紋乃重要之個人資訊，個人對其指紋資訊之自主控制，受資訊隱私權之保障。而國民身分證發給與否，則直接影響人民基本權利之行使。戶籍法第八條第二項規定：依前項請領國民身分證，應捺指紋並錄存。但未滿十四歲請領者，不予捺指紋，俟年滿十四歲時，應補捺指紋並錄存。第三項規定：請領國民身分證，不依前項規定捺指紋者，不予發給。對於未依規定捺指紋者，拒絕發給國民身分證，形同強制按捺並錄存指紋，以作爲核發國民身分證之要件，其目的爲何，戶籍法未設明文規定，於憲法保障人民資訊隱私權之意旨已有未合。縱用以達到國民身分證之防僞、防止冒領、冒用、辨識路倒病人、迷途失智者、無名屍體等目的而言，亦屬損益失衡、手段過當，不符比例原則之要求。戶籍法第八條第二項、第三項強制人民按捺指紋並予錄存否則不予發給國民身分證之規定，與憲法第二十二條、第二十三條規定之意旨不符，應自本解釋公布之日起不再適用。」

3. 鼓勵使用線上隱私之保護機制，如 PET 等。

4. 落實輕度管理原則。

## 五、 小結

在執行層面上，其實最基礎的不論在任何方面之個人資料保護喚起民眾對其之認知與覺醒是最重要的。吾人以爲，歐洲理事會之「個人資料保護指導方針」足供我國深切學習，相對則是對於政府公務機關或其他非公務機關之業者的宣導。個人資料保護之規範固然重要，但是倘若無確實之執行則又會淪爲重度立法輕度執法之譏。

另方面，政府對於各種可能侵害個人資料權利之政策亦需小心檢討，以避免違背人權之憾，造成人民權益之重大侵害。

# 第四節 結語

縱觀對我國個人資料之相關作爲雖已有算是世界上先進之規範存在，但是其後之落實與即時之修正卻有不足。雖然可以體諒在立法當時鑑於我國國情可能反應激烈，故採取較爲保守之作爲，但個人資料保護之趨勢演變至此，已經不容耽擱！

誠然，實施個人資料保護可能引起政府部門或是業者之反彈，因爲該保護之措施可會直接使其原本之權利或是商業之利益受到節制，但是依照歐洲之經驗，個人資料保護乃是與資訊流通有相輔相成之效果。一旦公務或非公務機關能確實保護個人之資料，則一定使民眾或消費者更具有與之互動或消費之信

心，則在政府方面，可生效率行政之效果，並強化人民對政府之信任；在非公務機關方面，則消費者與業者間更加信任之結果，吾人以爲絕對不輸目前消費者保護觀念逐漸落實後之效果，由於業者的正確觀念，必定使我國在相關商業利益上有長足之進步，並有與國際接軌與競爭之能力。

# 第六章　結論

**歐洲人權新頁之開展—個人資料保護**

本文對於整個歐洲個人資料保護問題於論述後發現，其實在整個歐洲的個人資料保護理論中最核心者，即透過傳統國家與人民間對於人權保障之需求，在由隱私權所延伸的個人資料自決權中一再強調自主與國家規範保護的觀念。而另一個歐洲個人資料保護核心，也是在人權之架構下所出現－－由自由基礎所生之資訊自由流通，乃得與同屬一人權架構之個人資料保護相輔相成，足見歐洲方面對於人權系統理論之紮實。

**歐洲模式之個人資料保護**

透過對於歐洲理事會與歐洲聯盟在個人資料保護方面之法規，亦即「個人資料保護公約」與「個人資料保護指令」二者，歐洲已經初步的在個人資料之保護理念方面對於整個國際有著深遠之影響，雖然其他各國－－尤其是美國，可能有著不同型態之觀念，認爲應以較自由之思考方向落實在業者自律中即可，並藉由安全港原則逐步之削弱「個人資料保護公約」與「個人資料保護指令」二者對其之影響，但誠如論者言，歐洲個人資料保護相關嚴格法規範出現，

乃可收對全球資訊隱私保護牽引與提升之效[16]。

透過相關核心法規範，個人資料保護之基礎原則諸如資料品質原則、特種資料處理原則、資料處理之正當性原則、安全確保原則、排除原則以及資料當事人與保管人之權利義務等均可歸納而呈現，足供相關理論之核心與未來發展所需。

並且，在歐洲對於個人資料之保護不僅只限於理論與法規範之築構上，更有決定性影響的是其後續之在法規範上之更新（例如「電子通信個人資料保護指令」、「關於警察部門之個人資料保護建議」等等諸多延伸法規範）、執行上之落實與理論之再研究（例如混合折衷模式之提出與倡議）等等。在歐洲的經驗裡，吾人發現一新興之法理論系統的誕生與發展並影響到全球，而注入對於人權概念的新血。而歐洲相關之法院在對於個人資料保護之案例裁判時，也都能嚴守公益與私益之分際，對於資訊自由流通與個人隱私保護做出一定程度之衡平裁判。

**案例研究之發現**

在個別領域個人資料保護之探討中，本文分別針對了個人醫療資料、個人警察資料與網際網路個人線上資料加以觀察。在個人醫療資料方面主要發現該種個人資料屬最貼近人身之高敏感度個人資料，並且由於基因與生物科技之進步，對該等個人資料之保護應更強化其注意。在個人警察資料則由於涉及可能的刑罰或行政罰之強制處分，故而必須考慮國家社會公益與個人之私益的平衡，方能同時兼具公益與私益之保護。至於網際網路個人線上資料方面，則發現若需對此方面個人資料能有相當程度之保護，則能順應網路快速發展趨勢之前瞻性立法與執行乃是不可或缺的，並且，能簡明扼要而快速的宣導相關觀念

[16] 參：劉靜怡，＜資訊隱私權保護的國際化爭議--從個人資料保護體制的規範協調到國際貿易規範的適用＞，《月旦法學》，台北：元照出版，第 86 期，2002 年 7 月，頁 201。

意識不可缺少的重要一環。

**吾國個人資料保護之現狀—急起直追的新契機**

另方面當筆者以歐洲之經驗審視在我國方興未艾的個人資料保護相關作爲時則發現，雖我國已有「電腦處理個人資料保護法」對之加以規範，但是由於立法之初鑑於避免造成對社會與經濟之過大衝擊，而以相對較保守之態度去立法。這原本是無可厚非的，但是畢竟該個人資料保護之觀念在我國相關人權團體之大力宣導之下，已經逐漸有其能見度，又隨著網際網路之快速發展，個人資料保護也由之邁向一個影響更大之全新領域，則前述消極之說詞即已經難以成立。另方面雖然我國相關立法草案已提出，惟立法腳步卻相對緩慢，難達成人民此方面之期待與需求，故儘速完成立法實爲當下最重要之步驟。

對照歐洲之相關作爲，我國在立法上明顯未有與時並進之現象，又由於該「電腦處理個人資料保護法」本身原本之保守性格，遂使相關之作爲在實際運用上，出現許多窒礙難行或保護不全之處。面對快速的全球資訊化影響，實應加快腳步迅速立法修正，以符人權立國之信念。

**我國實際案例上之檢視結果實待改進**

個人資料保護之觀念不但在民間之宣導有其重要性，更重要的是在政府方面對於該個人資料權利之體認，在我國更形重要。對於諸多政策在實施或考慮時，除了考量國家之整體經濟或行政效率之發展外，更應對於人權之事項多加注意，以避免淪爲過去帝制或專制時期思考方式之延續。本文透過對於全民健保 IC 卡政策與全民指紋建檔等事涉「全民」議題之檢視中，已發現諸多可能侵害人權之缺憾，諸如在全民健保 IC 卡政策中，偏重經濟層面卻忽略個人隱私權保障，況該經濟成效並非必然達成公益私益難達平衡；在全民指紋建檔議題中一昧追求

實體正義之快速達成而忽略了程序正義與人權之保障;在網站隱私權方面也無明確法規範與有效之執行。則在有更進一步之作爲時，政府似更應考慮歐洲人權法院判斷相關案例之準則－－即該行爲之公益是否確實大於私益以爲權利之衡平。

**個人資料保護之未來發展**

資訊自決（資料保護）與資訊自由之間，應非僅具有典型的衝突關係存在，反應該爲兩種相輔相成之權利已若前述，則個人資料保護理論之開展必定能有效助益資訊自由化之發展，並推動相關產業之經濟與法律成長。在比較法制的觀察之下，我國雖在個人資料保護方面相對於歐洲顯的消極，但未必不是一種促進本身自省對於人權保障之契機；值此人權觀念在我國已受重視之時，吾人以爲，個人資料之保護在我國應具有長遠之發展性！

# ＜參考書目＞

## 一、 中文資料部分：

### （一） 官方資料：

1. 行政院資訊發展推動小組「IC 卡規劃與推行小組」編印，《「國民身份健保和一智慧卡」專案徵求建議書文件》，民國 87 年 6 月 10 日。

2. 行政院衛生署中央健保局，《中華民國國民健保卡實施計畫》，民國 88 年 11 月 24 日。

3. 行政院衛生署中央健保局，《健保 IC 卡建置計畫徵求建議書文件》，民國 89 年 8 月 1 日。

4. 法務部法律事務司，《檢討電腦處理個人資料保護法實施狀況公聽會會議實錄彙編》，台北：法務部，2002 年 2 月。

5. 司法院大法官解釋第六零三號解釋文暨解釋理由書，2005 年 10 月。

### （二） 書籍：

1. 大衛・布林 David Brin 著，蕭美惠譯，《透明社會－個人隱私 vs. 資訊自由》（*The transparent Society: Will technology force us to choose between privacy or freedom?*），台北：先覺出版社，1999。

2. 王泰銓，《歐洲共同體法總論》，台北：三民書局，1997。

3. 台灣人權促進會企畫，李茂生主編，《2001 年台灣人權報告》，台北：前衛出版社，2002。

4. 李震山，《人性尊嚴與人權保障》，台北：元照出版，2000。

5. 林信華，《文化政策新論－建構台灣新社會》，臺北：揚智文化，2002。

6. 張甘妹，《犯罪學》，台北：三民書局，十二版，1998。

7. 許文義，《個人資料保護法論》，台北：三民書局，2001。

8. 陳楚杰，《病歷管理》，台北：宏翰出版社，1995。

9. 勞倫斯·雷席格（Lawrence Lessig）著，劉靜怡譯，《網路自由與法律》（*Code: and other Laws of Cyberspace*），台北：商周出版，城邦文化發行，2002。

10. 黃偉峰主編，中央研究院歐美所，《歐洲聯盟的組織與運作》，台北：五南圖書出版，2003。

11. 葉俊榮、許宗力主持，《政府資訊公開制度之研究》，行政院研考會，1996 年 8 月。

12. 潘大連/黃小魏，《電腦辭典》，台北：貓頭鷹出版社，1997。

13. 蕭文生譯，《「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），司法院印行，1991 年 5 月。

## （三） 學位論文：

1. 王濟民，＜智慧卡（Smart Card）之推廣與應用分析＞，台灣大學商學研究所碩士論文，1999 年 6 月。

2. 吳昊，＜由醫療資訊隱私權之觀點論全民健保 IC 卡政策＞，台灣大學法律學研究所碩士論文，2001 年 7 月。

3. 紀佳伶，＜電子化/網路化政府資訊內容隱私權之研究＞，政治大學公共行政學系碩士論文，2000 年 7 月。

4. 陳志忠，＜個人資訊自決權之研究＞，東海大學法律學研究所碩士論文，2000 年 1 月。

5. 楊富強，＜資訊取得之公法研究－以私人與政府之關係爲中心＞，政治大學法律研究所碩士論文，1989 年 6 月。

6. 葉淑芳，＜行政資訊公開之研究－以隱私權之保障爲中心＞，中興大學法律研究所碩士論文，1999 年 7 月。

7. 詹文凱，＜隱私權之研究＞，台灣大學法律學研究所博士論文，1998 年 7 月。

8. 熊愛卿，＜網際網路個人資料保護之研究＞，台灣大學法律研究所博士論文，2000 年 7 月。

9. 劉坤旺，＜從憲法觀點論警察處理個人資料法制＞，中央警察大學行政警察研究所碩士論文，2000 年 6 月。

10. 簡榮宗，＜網路上資訊隱私權保障問題之研究＞，東吳大學法律研究所碩士論文，1999 年 6 月。

## （四） 期刊論文：

1. 丁惠民，＜電子化時代的管理新議題：網路安全與隱私權保護＞，《電子化企業-經理人報告》，台北：ARC 遠擎管理顧問公司，第 9 期，2000 年 5 月。

2. 李震山，＜論個人資料保護－以人體基因資訊爲例＞，《月旦法學雜誌》，台北：元照出版，第 75 期，2001 年 8 月。

3. 莊庭瑞，＜個人資料保護在台灣：誰的事務？＞，《國家政策季刊》，行政院研考會，第二卷第一期，2003 年 3 月。

4. 廖福特，＜人權宣言？人權法典？--「歐洲聯盟基本權利憲章」之分析＞，《歐美研究》，2001 年 12 月。

5. 劉靜怡，＜資訊隱私權保護的國際化爭議--從個人資料保護體制的規範協調到國際貿易規範的適用＞，《月旦法學》，台北：元照出版，第 86 期，2002 年 7 月。

6. 蕭立承，＜網路安全的危機與保障網路隱私權之策略＞，《電子化企業-經理人報告》，台北：ARC 遠擎管理顧問公司，第 9 期，2000 年 5 月。

7. 賴文智，＜網站會員資料與隱私權之保護＞，《網路資訊》，2001 年 2 月號。

## 二、 外文資料部分：

## （一） 官方資料：

1. Council of Europe, First evaluation of the relevance of Recommendation No. R (87) 15 regulating the use of personal data in the police sector.

2. Council of Europe, Second evaluation of the relevance of Recommendation No. R (87) 15 regulating the use of personal data in the police sector.

3. Council of Europe, Report on the third evaluation of Recommendation N° R (87) 15 regulating the use of personal data in the police sector.

4. Council of Europe, Regional Seminar on Data Protection in the Police Sector, Strasbourg 1999.

## （二） 書籍：

1. Bainbridge, David, *EC Data Protection Directive*, London: Butterworths, 1996.

2. Bloustein, Edward J., *Individual & Group Prvicy*, New Brunswick: Transaction publishers, 2003.

3. Brin, David, *The transparent Society: Will technology force us to choose between privacy or freedom?*, New York: Addison-Wesley Longman, Inc., 1998.

4. Castells, Manuel, *The Internet Galax: Reflections on the internet, business, and society*, New York: Oxford University Press Inc., 2001.

5. Cate, Fred H., *Privacy in the information age*, Washington D.C.: Brookings Institution, 1997.

6. Clayton, Richard, and Tomlinson, Huge, *Privacy and Freedom of Expression*, Oxford University Press, 2001.

7. Colvin, Madeleine (ed.), *Developing Key Privacy rights*, Oxford and Portland, Oregon: Hart Publishing, 2002.

8. Dickson, Brice (ed.), *Human Rights and the European Convention- the effects of the convention on the United Kingdom and Ireland*, London: Sweet & Maxwell Ltd, 1997.

9. Flaherty, David H., Protecting privacy in surveillance societies: the Federal Republic of Germany, Sweden, Canada, and the United States, The University of North Carolina Press, 1989.

10. Freedman, Warren, *The right of privacy in the computer age*, Greenwood Press, 1987.

11. Edge, Hammond Suddards, *Privacy and Communications*, London: CPID, 2001.

12. Ruiz, Blanca R., *Privacy in telecommunications*, Kluwer Law International, 1997.

13. Rotenberg, Marc, *The Privacy Law Sourcebook 2000- United States Law, International Law, amd Recent Developments*, Washington D.C.: Electronic Privacy Information Center (EPIC), 2000.

14. Schwartz, Paul M., and Reidenberg, Joel. R., *Data Privacy Law*, Virginia: MICHIE Law Publishers, 1996.

15. Tugendhat QC, Michael, and Christie, Iained. (eds.), *The Law of Privacy and the Media*, London:Oxford University Press, 2002.

16. United Nations, Human Rights- A Compliation of International Instruments (Volume II- Regional Instruments), Geneva: United Nations, 1997.

17. Wallace, Helen and William, *Policy-Making in the European Union, fourth edition*, Oxford University Press, 2000.

18. Weiler, J. H. H., *The Constitution of Europe- 'Do the New Clothes have an Emperor' and Other Essays on European Integration*, Camberidge University Press, 1999.

## （三） 期刊論文：

1. Albert, Jason, *Privacy on the Internet: Protecting and Empowering Users*, COVINGTON & BURLING, Brussels, 2002/10/01.

2. Liao, Fort, Fu-te, *European Human Rights: Often the first in the world*, The 21st century Seminars Cultural Exchange Programme Europe-Taiwan, Agenda of the 8th seminar, Oct. 20, 2001.

3. Fromholz, Julia M., *The European Union Data Privacy Directive*, 15 Berkeley Tech. L.J. 461, 2000.

4. Froomkin, A. Michael, *CYBERSPACE AND PRIVACY: A NEW LEGAL PARADIGM? The Death of Privacy?* , 52 Stan. L. Rev. 1461, May, 2000.

5. Gauthronet, Serge. and Nathan, Frédéric, *On-line services and data protection of privacy*, study project commissioned from ARETE by DG-XV of the commission of the EC, 1998/12.

6. Heydrich, Michael W., *A brave new world: complying with the European Union directive on personal privacy through the power of contract*, 25 Brooklyn J. Int'l L. 407, 1999.

7. Kang, Jerry, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, April, 1998.

8. Lemley, Mark A., *CYBERSPACE AND PRIVACY: A NEW LEGAL PARADIGM? Private Property*, 52 Stan. L. Rev. 1545, May, 2000.

9. Lessig, Lawrence, *The Law of the horse: what cyberlaw might teach*, Harvard Law Review, 113 Harv. L. Rev. 501, December, 1999.

10. Mallet-Poujol, Nathalie, *The individual's position in a globalised information world: rights and obligations*, report of European conference on data protection on Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data: Present and Future, 19-20 November, 2001 proceedings

11. Masons Study, *Handbook on Cost Effective, Compliance with Directive 95/46/EC*, Study for Commission of EC (DG XV), 1998/08.

12. O'Quinn, John C., *BOOK NOTE: None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (By Peter P. Swire & Robert E. Litan), 12 Harv. J. Law & Tec 683, summer, 1999.

13. Reidenberg, Joel R., *Cyberspace and Privacy: A New Legal Paradigm? Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 Stan. L. Rev. 1315, May, 2000.

14. Reidenberg, Joel R., *Resolving Conflicting International Data Privacy Rules in Cyberspace,* 52 STAN. L. REV. 1315, 2000.

15. Reidenberg, Joel R., *Restoring Americans' Privacy in Electronic Commerce*, 14 Berkeley Tech. L.J. 771, Spring, 1999.

## （四） 條約及相關法令：

## A. Council of Europe:

1. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows.

2. Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, adopted at Oviedo on 4 April 1997.

3. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.

4. Council of Europe Convention for the Protection of Human Rights and Fundamental freedoms.

5. Recommendation No. R (2002) 9 on the protection of personal data collected and processed for insurance purposes.

6. Recommendation No. R (81) 1 on regulations for automated medical data banks (23 January 1981).

7. Recommendation No. R (83) 10 on the protection of personal data used for scientific research and statistics (23 September 1983).

8. Recommendation No. R (85) 20 on the protection of personal data used for the purposes of direct marketing (25 October 1985).

9. Recommendation No. R (86) 1 on the protection of personal data for social security purposes (23 January 1986).

10. Recommendation No. R (87) 15 regulating the use of personal data in the police sector (17 September 1987).

11. Recommendation No. R (89) 2 on the protection of personal data used for employment purposes (18 January 1989).

12. Recommendation No. R (90) 19 on the protection of personal data used for payment and other operations (13 September 1990).

13. Recommendation No. R (91) 10 on the communication to third parties of personal data held by public bodies (9 September 1991).

14. Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services (7 February 1995).

15. Recommendation No. R (97) 18 on the protection of personal data collected and processed for statistical purposes (30 September 1997).

16. Recommendation No. R (97) 5 on the protection of medical data (13 February 1997).

17. ecommendation No. R (99) 5 for the protection of privacy on the Internet (23 February 1999).

## B. European Union:

1. Charter of Fundamental Rights of the European Union.

2. Directive 95/46/EC of the European Parliament and of the European 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.

3. Directive 97/66/EC of the European Parliament and of the Council of 15, December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, Directive 97/66/EC, Official Journal L 024, 30/01/1998 P. 0001 – 0008.

4. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Directive 2002/58/EC, Official Journal L 201 , 31/07/2002 P. 0037 – 0047.

5. EU: Regulation (EC) 45/2001 of the European Parliament and of the Council of 18. December 2000 on 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, Official Journal L 008, 12/01/2001 P. 0001 – 0022.

## 三、 網路資料部分：（均以 2005 年 11 月瀏覽爲準）

1. Council of Europe, Data Protection: http://www.coe.int/T/E/Legal%5Faffairs/Legal%5Fco%2Doperation/Data%5Fprotection/

2. Data Protection Conference, Brussels, 30.9./1.10.2000: URL: http://europa.eu.int/comm/internal_market/privacy/lawreport/data-conference_en.htm.

3. Electronic Privacy Information Center: http://www.epic.org/

4. EPIC Data Retention Page: http://www.epic.org/privacy/intl/data_retention.html

5. Eu, Data Protection: http://europa.eu.int/comm/internal_market/privacy/index_en.htm

6. 全民個人資料保護聯盟： URL: http://www.tahr.org.tw/PDPA/index.htm.

7. 全國檔案目錄查詢網： URL: http://near.archives.gov.tw/index.html.

8. 行政院衛生署中央健保局，健保 IC 卡宣導網站， URL: http://www.enhi.com.tw/

9. 行政院衛生署疾病管制局 SARS 資訊網站：http://www.cdc.gov.tw/sars/

10. 歐洲理事會法律事務總署（Directorate General of Legal Affairs － DG Ⅰ）：URL：http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/National_laws

11. 歐洲理事會個人資料保護：URL:

12. http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Backgr

ound/。

13. 歐盟內部市場之資訊： URL: http://europa.eu.int/comm/internal_market/en/index.htm.

14. 歐盟名詞中英文對照表： URL: http://iir.nccu.edu.tw/eurf/歐盟名詞對照表.xls

15. 歐盟個人資料向第三國傳遞之契約範例： URL: http://europa.eu.int/comm/internal_market/en/dataprot/modelcontracts/index.htm

# ＜索引＞