

（建議使用工具列--〉檢視--〉文件引導模式/功能窗格）

**《大數據應用於犯罪偵防與隱私權之法制研究》**

柯雨瑞[[1]](#footnote-1)　蔡政杰[[2]](#footnote-2)

# 【目次】

壹、[前言](#_壹、前言)

貳、[傳統個人資料保護之舊法制無法因應大數據機制之實際需求](#_貳、傳統個人資料保護之舊法制無法因應大數據機制之實際需求)

參、[兩岸大數據應用於犯罪偵防與隱私權保護之法制現況](#_參、兩岸大數據應用於犯罪偵防與隱私權保護之法制現況)

**》**一、[臺灣地區之法制現況](#_一、臺灣地區之法制現況)

》》（一）[憲法](#_（一）憲法)

》》（二）[個人資料保護法](#_（二）個人資料保護法)

》》（三）[刑法](#_（三）刑法)

**》**二、[大陸地區之法制現況](#_二、大陸地區之法制現況)

》》（一）[憲法](#_（一）憲法_1)

》》（二）[網路安全法](#_（二）網路安全法)

》》（三）[刑法](#_（三）刑法_1)

**》**三、[小結](#_三、小結)

肆、[兩岸大數據應用於犯罪偵防與隱私權保護之法制困境](#_肆、兩岸大數據應用於犯罪偵防與隱私權保護之法制困境)

**》**一、[法令不完備，犯罪偵防手段不積極，使臺灣地區社會對於電子商務交易行為普遍存有不信任感](#_一、法令不完備，犯罪偵防手段不積極，使臺灣地區社會對於電子商務交易行為)

**》**二、[兩岸政府之憲法層級，均缺乏對於公民個資隱私權保護之法制](#_二、兩岸政府之憲法層級，均缺乏對於公民個資隱私權保護之法制)

**》**三、[臺灣地區之網路個資相關法制相對於大陸地區之個資相關法制，顯得趨於狹隘](#_三、臺灣地區之網路個資相關法制相對於大陸地區之個資相關法制，顯得趨於狹)

**》**四、[有關於將大數據科技應用於犯罪偵防部分，法律規範之積極性不足，導致犯罪偵防之手段亦無法充分施展運用](#_四、有關於將大數據科技應用於犯罪偵防部分，法律規範之積極性不足，導致犯)

**》**五、[兩岸政府目前尚未共同著手建置以犯罪偵防為目的之大數據資料庫，不利於兩岸犯罪偵防情資之交流，同時，亦不利於兩岸犯罪偵防相關工作之開展](#_五、兩岸政府目前尚未共同著手建置以犯罪偵防為目的之大數據資料庫，不利於)

伍、[兩岸大數據科技應用於犯罪偵防與公民隱私權保護之法制對策---代結論](#_伍、兩岸大數據科技應用於犯罪偵防與公民隱私權保護之法制對策---代結論)

**》**一、[臺灣地區應強化相關法令措施，以「犯罪偵防」與「保護個資」同時並進之積極作為，取代「拒絕建立數位身分」之消極不作為，並提高民眾使用電子商務之信心，始能有效擴大消費通路，提升國家整體經濟；](#_一、臺灣地區應強化相關法令措施，以「犯罪偵防」與「保護個資」同時並進之)

**》**二、[考量大數據時代之變遷迅速，對於大數據科技應用之相關法制規範，應跳脫現行法律原則之思維，採用較為彈性之規範，或於修法之程序上更為便捷，同時，宜考量建置專法之可行性，同時，將大數據科技應用於犯罪偵防部分，將其明文化於法律之規範之中，以順應需求，俾符合犯罪偵防之用](#_二、考量大數據時代之變遷迅速，對於大數據科技應用之相關法制規範，應跳脫)；

**》**三、[在大陸地區個資保護之相關法制部分，本文建議大陸地區宜儘速通過與正式施行「個人信息保護法」；](#_三、在大陸地區個資保護之相關法制部分，本文建議大陸地區宜儘速通過與正式)

**》**四、[兩岸政府之憲法層級，宜明文規範對於公民個資之資訊權與隱私權之保護法制；](#_四、兩岸政府之憲法層級，宜明文規範對於公民個資之資訊權與隱私權之保護法)

**》**五、[兩岸政府宜基於平等、互惠、互信之原則，共同建置以犯罪偵防為目的之大數據資料庫，以利於兩岸犯罪偵防情資之交流，同時，亦有利於兩岸犯罪偵防相關工作之順利開展。](#_五、兩岸政府宜基於平等、互惠、互信之原則，共同建置以犯罪偵防為目的之大)

【[參考文獻](#a參考文獻)】

。。。。。。。。。。。。。。。。。。[回目次](#a目次)〉〉

# 【摘要】

　　本文之核心研究目的，主要係集中於探討臺灣地區與大陸地區政府，對於大數據科技應用於犯罪偵防與公民隱私權保護法制之現況、困境與對策，主要之研究方法，係為文獻探討法與比較研究法，重要之研究發現，如下所述。在困境方面，本文發現以下之重要現象：一、法令不完備，犯罪偵防手段不積極，使臺灣地區社會對於電子商務交易行為普遍存有不信任感；二、兩岸政府之憲法層級，缺乏對於公民個資隱私權保護之法制；三、臺灣地區之網路個資相關法制相對於大陸地區之個資相關法制，顯得趨於狹隘；四、有關於將大數據科技應用於犯罪偵防部分，法律規範之積極性不足，導致犯罪偵防之手段亦無法充分施展運用；五、兩岸政府目前尚未共同著手建置以犯罪偵防為目的之大數據資料庫，不利於兩岸犯罪偵防情資之交流，同時，亦不利於兩岸犯罪偵防相關工作之開展。

　　基於以上之困境脈絡，本文針對於兩岸政府對於大數據科技應用於犯罪偵防與公民隱私權保護之法制對策方面，玆提出以下之建言，俾供兩岸政府與兩岸社會大眾參考之用：

　　一、臺灣地區應強化相關法令措施，以「犯罪偵防」與「保護個資」同時並進之積極作為，取代「拒絕建立數位身分」之消極不作為，並提高民眾使用電子商務之信心，始能有效擴大消費通路，提升國家整體經濟；

　　二、考量大數據時代之變遷迅速，對於大數據科技應用之相關法制規範，應跳脫現行法律原則之思維，採用較為彈性之規範，或於修法之程序上更為便捷，同時，宜考量建置專法之可行性，同時，將大數據科技應用於犯罪偵防部分，將其明文化於法律之規範之中，以順應需求，俾符合犯罪偵防之用；

　　三、在大陸地區個資保護之相關法制部分，本文建議大陸地區宜儘速通過與正式施行「個人信息保護法」；

　　四、兩岸政府之憲法層級，宜明文規範對於公民個資之資訊權與隱私權之保護法制；

　　五、兩岸政府宜基於平等、互惠、互信之原則，共同建置以犯罪偵防為目的之大數據資料庫，以利於兩岸犯罪偵防情資之交流，同時，亦有利於兩岸犯罪偵防相關工作之順利開展。

　　本文之核心研究目的，主要係集中於探討臺灣地區與大陸地區政府，對於大數據科技應用於犯罪偵防與公民隱私權保護法制之現況、困境與對策，主要之研究方法，係為文獻探討法與比較研究法，重要之研究發現，如下所述。在困境方面，本文發現以下之重要現象：一、法令不完備，犯罪偵防手段不積極，使臺灣地區社會對於電子商務交易行為普遍存有不信任感；二、兩岸政府之憲法層級，缺乏對於公民個資隱私權保護之法制；三、臺灣地區之網路個資相關法制相對於大陸地區之個資相關法制，顯得趨於狹隘；四、有關於將大數據科技應用於犯罪偵防部分，法律規範之積極性不足，導致犯罪偵防之手段亦無法充分施展運用；五、兩岸政府目前尚未共同著手建置以犯罪偵防為目的之大數據資料庫，不利於兩岸犯罪偵防情資之交流，同時，亦不利於兩岸犯罪偵防相關工作之開展。

　　基於以上之困境脈絡，本文針對於兩岸政府對於大數據科技應用於犯罪偵防與公民隱私權保護之法制對策方面，玆提出以下之建言，俾供兩岸政府與兩岸社會大眾參考之用：

　　一、臺灣地區應強化相關法令措施，以「犯罪偵防」與「保護個資」同時並進之積極作為，取代「拒絕建立數位身分」之消極不作為，並提高民眾使用電子商務之信心，始能有效擴大消費通路，提升國家整體經濟；

　　二、考量大數據時代之變遷迅速，對於大數據科技應用之相關法制規範，應跳脫現行法律原則之思維，採用較為彈性之規範，或於修法之程序上更為便捷，同時，宜考量建置專法之可行性，同時，將大數據科技應用於犯罪偵防部分，將其明文化於法律之規範之中，以順應需求，俾符合犯罪偵防之用；

　　三、在大陸地區個資保護之相關法制部分，本文建議大陸地區宜儘速通過與正式施行「個人信息保護法」；

　　四、兩岸政府之憲法層級，宜明文規範對於公民個資之資訊權與隱私權之保護法制；

　　五、兩岸政府宜基於平等、互惠、互信之原則，共同建置以犯罪偵防為目的之大數據資料庫，以利於兩岸犯罪偵防情資之交流，同時，亦有利於兩岸犯罪偵防相關工作之順利開展。

【關鍵詞】大數據、電子商務、犯罪偵防、隱私權

【Key Words】big data, electronic commerce, criminal detection and prevention, right of privacy

。。。。。。。。。。。。。。。。。。[回目次](#a目次)〉〉

# 壹、前言

　　本文係從兩岸政府現行法制及相關文獻分析之途徑，採比較研究方法，探討臺灣地區與大陸地區政府，對於大數據科技應用於犯罪偵防與公民隱私權保護法制之現況、困境與對策，從臺灣地區憲法之隱私保護、個人資料保護規範及刑事法規之有關規定，與大陸地區相對之法規（如：電信和互聯網用戶個人信息保護規定、[刑法](https://www.6laws.net/6law/law-gb/中華人民共和國刑法.htm)、[網路安全法](https://www.6laws.net/6law/law-gb/中華人民共和國網路安全法.htm)等），進行比較研究，秉持兩岸互助合作之精神，就兩岸政府對於大數據科技應用於犯罪偵防與公民隱私權保護之法制現況、困境與對策，詳予論述。

　　本文之研究主題，係聚焦於大數據科技應用於犯罪偵防與公民隱私權保護之法制，此一研究領域，亦會觸及電子商務所衍生之相關犯罪問題之防治(從大數據科技角度切入)，與隱私權之保障，及個人資料保護之議題，尤其是個人資料之使用，其在大數據之運用上，如稍有不慎，就容易發生個資被竊取、盜用、被冒用身分及被詐欺取財等隱私權保護之犯罪問題。

隨著使用網路人口之不斷增長，「電子商務(e-commerce)」之發展，亦是方興未艾；廣義之「電子商務(e-commerce)」，在名詞之定義上，乃指透過網路之使用平台，而以電子之方式，從事所有之商務活動，此等之商務活動，包括：商品交易、廣告、服務、資訊提供、金融匯兌、市場情報、電信、育樂節目與販售活動[[3]](#footnote-3)。「電子商務」在全球之市場中，有非常多之成功案例，分別散見於零售業、智慧居家業、智慧辦公室、智慧城市、車聯網…等等[[4]](#footnote-4)。

　　在國際條約上，相當地引人注目者，乃為在「跨太平洋夥伴協定(Trans-Pacific Partnership，簡稱為TPP)之中，亦訂有一個電子商務之法制專章，係為第14章，專門對於電子商務，進行完整之法規(制)之建制。承上所述，在TPP之中，涉及「電子商務」專章(第14章)之重要法律規範，如下所述[[5]](#footnote-5)：1.在TPP第14章第3條之中，TPP全面性地禁止締約國對於電子傳輸課徵關稅，包括以電子傳輸之內容物；2.於TPP第14章第4條之中，適用「不歧視原則」；3.提升與創新「電子簽章」與「電子認證」之多樣化方式(TPP第14章第6條)；4.促進網路自由與開放(TPP第14章第10條)；5.增進數據之跨境流通性(TPP第14章第11條)；6.禁止「在地化」(本地化)(localization)條款(TPP第14章第13條)；7.執行消費者保護措施(含隱私權之各項保護作為)( TPP第14章第7條、第8條、第14條)；8.促進網路安全方面之合作(TPP第14章第16條)；9.各締約國不得要求取得或移轉「程式原始碼」，作為進入市場之條件；但締約國得基於保護健康、安全或其他合法之監管目標，而取得「程式原始碼」之權利(TPP第14章第17條) [[6]](#footnote-6)。

在一些主要國家，個人資料均是以立法形式（法律保留）進行保護，如美國在1974年頒佈「隱私權法」(The Privacy Act)，訂立「行政機關不應該保有秘密之個人資訊記錄」及「個人有權知道自己被行政機關記錄之個人資訊及其使用情況」等基本原則[[7]](#footnote-7)；德國在1976年通過，「聯邦個人資料保護法」(Bundesdatenschutzgesetz, BDSG)，並在1977年生效，規範包括與資料保護相關之各項原理原則，例如限制蒐集原則、內容完整正確原則、目的明確原則、限制利用原則、安全保護措施原則、公開原則及個人參與原則及責任原則等[[8]](#footnote-8)。英國在1984年制定「資料保護法」，後於1998年通過修正「資料保護法」(The Data Protection Act 1998)，於2000年生效，規範內容可適用於某些特定結構化人工紀錄及電腦化個人資料等規範[[9]](#footnote-9)。

　　兩岸對於大數據應用於犯罪偵防與公民隱私權保護上，均已有相關法制規範，相較之下，大陸地區之現行相關法制，有多處地方之法制機制，值得臺灣地區加以學習之。兩岸法制規範，亦各有優勢，亦各有不足之處，以下將就大數據應用於犯罪預防及犯罪偵查之兩大面向，及應用於公民隱私權之保護法制區塊之現況、困境、回應對策，進行表列分析，並提出因應對策，詳如下表之所述。

。。。。。。。。。。。。。。。。。。[回目次](#a目次)〉〉

# 貳、傳統個人資料保護之舊法制無法因應大數據機制之實際需求

　　在大數據是否需要新立法？及何種之概念，應該為大數據法規範之核心之議題上，國際上，有一篇非常重要之文獻，此篇之論文，名為「未來規範大數據機制之10個問題：比較及實證法律研究」(Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study)，係由兩位德國學者Bart van der Sloot及Sascha van Schendel(2016)，共同發表於2016年「知識產權、資料技術與電子商務法學報」第7期之上(Journal of Intellectual Property, Information Technology and E-Commerce Law ---JIPITEC)。德國學者Bart van der Sloot及Sascha van Schendel(2016)認為，在大數據是否需要新立法部分，在大多數國家，現行之法律機制，是適用於大數據。此外，多數國家之資料保護機關(Data Protection Authorities，簡稱為DPA)亦同意必須持續保障當前之隱私與資料保護原則。然而，大多數DPA亦意識到大數據與資料保護原則之間(between Big Data and data protection principles)，存有根本性之緊張關係(the fundamental tension)。儘管有如此之一個事實，但似乎尚未有新之立法(little new legislation seems to be developed)，專門針對大數據所引發之新危險，被大多數DPA開發與制定出來[[10]](#footnote-10)。

　　一些國家之DPA，有論及未來之「一般資料保護規則」(Some DPAs refer to the upcoming General Data Protection Regulation)，並希望「一般資料保護規則」之內容，包含可協助解決大數據所導致之危險之新規則。一些國家之DPA，所提出之解決方案，乃為數種法規，進行共同規範，與制定專法，兩者並行(A number of DPAs refer to co- and self-regulation)。不過，Bart van der Sloot及Sascha van Schendel(2016)亦指出，有些國家之DPA，如愛沙尼亞、法國、日本、英國等，似乎，正在考慮新式資料處理技術之立法規定。為何需制定新法律規範？係由於對隱私保護之擔憂，亦是由於現行法律之機制，其阻礙大數據技術創新之思維。

　　在回答有關制定大數據流程之新法律規則之問題時，政府需要考慮3個問題。依據Bart van der Sloot及Sascha van Schendel(2016)之觀察，首先，幾乎所有之國家和政府部門，均體認目前之法律監管框架(for the current regulatory framework)，特別是大數據時代下之重要原則，存在著新式及基本之風險(new and fundamental risks)。第二，目前之法律監管框架，似乎是太過於限制、扼殺新技術，及技術創新之使用、運用，特別是在私部門之區塊。第三，在許多之領域，均不確定如何根據大數據之運作流程(in the light of Big Data processes)，應用、解釋現行之行政規則及法律(are unsure how the current rules and laws should be applied to and interpreted)。

　　再者，何種之概念，應該是大數據法律監管之核心？此亦為本文之核心議題。依據Bart van der Sloot及Sascha van Schendel(2016)之觀點，當前之法規，通常以個人及其利益，作為依據，此適用於個人人權和資料保護，渠等之權利及資料保護，其關注之核心，係對個人資料進行處理，即可識別，或個別化某一自然人之個人資料。由於越來越多之資料，並非在個人層面上，進行收集、處理，而係使用聚合保護，此導致產生一般化之模式(general patterns)，或群組之情況(or group profiles)。問題乃在於，傳統上，係聚焦於個人資料之關注，但在大數據技術之運行之下，是否仍然可以維持之，頗有疑義。此與元數據[[11]](#footnote-11)之使用，產生相關聯性(This ties up to the use of metadata)，通常，吾人不清楚元數據在何種之程度上(it is often unclear to what extent metadata)？可以被認定係為個人資料(can qualify as personal data)，此涉及個人資料之定義問題。

　　再者，應該被指出之部分，在大數據之時代，資料靜態之性質(屬性)，越來越少(the nature of the data is less and less static)。但在大數據實踐中，依據Bart van der Sloot及Sascha van Schendel(2016)之觀察，資料通過循環過程：資料被鏈接(data are linked)、聚合(aggregated)、匿名化(and anonymized)。接下來，大數據會對已被處理過之資料，再「去」匿名化(again de-anonymized)。之後，被用於製成個人(for the making of personal)，或甚至匯整成為敏感之剖繪資料(or even sensitive profiles)。然後，再次被假名化(and then again pseudonymised)，被用於統計分析，及群組之剖繪等。目前之法律制度，似乎過於簡單地規範「資料」，在大數據時代之下，傳統上，對「個人資料」之保護機制，似乎，難以維持。國家機關將必須確定將「個人資料」作為一個保護之客體概念，在此一大數據時代下，是否仍然足以作為資料管理之基礎否[[12]](#footnote-12)？

。。。。。。。。。。。。。。。。。。[回目次](#a目次)〉〉

# 參、兩岸大數據應用於犯罪偵防與隱私權保護之法制現況

　　有鑑於大數據之應用，並不限於犯罪預防，或是犯罪偵查。故本文所稱犯罪偵防，係指犯罪預防，再加上犯罪偵查。就許春金教授之觀點，第3級之犯罪預防，實可包括犯罪偵查中之「強制處分權」(如逮捕)。故，犯罪預防可以說一個大概念，內含犯罪偵查之部分強制處分權之作為[[13]](#footnote-13)。不過，一般之社會大眾，仍將犯罪預防與犯罪偵查，視為不同之概念，兩者無法互容。

　　本文仍係以犯罪預防理論為基礎，同時兼顧犯罪預防與偵查作為之刑事司法之手段[[14]](#footnote-14)，因一般社會大眾多不知刑事司法(犯罪偵查)亦可屬犯罪預防之一環，然考量本文所探討大數據應用對於個人隱私權之影響，在主軸方面，同時兼顧犯罪預防與偵查作為，因此採用犯罪「偵防」之用詞，或許，能較犯罪「預防」更為貼切本文欲探討之主題；因此本文所稱之犯罪偵防，具同時包含犯罪「偵」查與預「防」之概念與理論。

　　另有臺灣地區學者將犯罪預防之模式略分為「刑事司法」、「情境」、「發展性」、「社區」及「風險管理」等五類[[15]](#footnote-15)，其中刑事司法犯罪預防，係基於古典犯罪學派之理論，就法律層面之策略，認為國家法律對於犯罪還是具有一定之防制效果及威嚇力。本文相當肯定此一理論途徑之解釋力，認為在電子商務運用普及之大數據時代中，法律對於個人資料之隱私保障更顯得重要，惟有透過完善之立法，治安機關始得以遵循苟實犯罪偵防，保護個人權益，使大數據運用對社會治安可能造成之危害降至最低。本節將從探討臺灣地區與大陸地區目前對於大數據應用而產生隱私權問題與犯罪偵防之法律規範現況，著手探討。

　　因大數據應用於處理犯罪偵防之領域，可謂是相當得多與普遍，首先，就犯罪預防之觀點，應可透過法令之完備（第一級預防）、風險之管理（第二級預防）及刑事司法作為（第三級預防），以大幅提升大數據應用於處理犯罪預防之能量與功效；以下，將三級犯罪預防（含定義）機制及其與大數據應用於處理犯罪防治之領域之關聯性，列表說明如下。

## 表1大數據應用於犯罪預防領域之一覽表（內含犯罪預防之定義）

|  |  |  |
| --- | --- | --- |
|  | 三級犯罪預防實際內涵[[16]](#footnote-16) | 大數據應用於犯罪預防之說明或示例 |
| 第一級預防 | 第一級預防，傳統之觀點，係指根本之預防措施，如在學校實施犯罪預防內化教育，或在社會上進行犯罪預防宣導工作。以期改善或降低整體可能營造犯罪之環境，減少犯罪行為之發生。 | 在大數據應用於第一級犯罪預防之區塊上，可行之機制如下所述：建立完善之大數據應用之法令機制，如修改[個人資料保護法](https://www.6laws.net/6law/law/個人資料保護法.htm)、修改[刑法](https://www.6laws.net/6law/law/刑法.htm)電腦犯罪罪章、制定網路安全法等，完備健全之法制，再透過犯罪預防之宣導，使社會大眾瞭解大數據應用於犯罪預防概念及法令規範，強化大數據應用於第一級犯罪預防之成效，並減少犯罪行為發生。 |
| 第二級預防 | 第二級預防，傳統之觀點，係指運用風險管理(risk management)之概念，針對「高風險」(high risk)之犯罪因子、可能性之犯罪及偏差性之行為，進行控制或消除。 | 在大數據應用於第二級犯罪預防之區塊上，可行之機制如下所述：評估各種犯罪行為可能產生之風險比例數值(risk rate)，針對高風險值之犯罪行為（如：網路詐欺取財、毒品犯罪、竊盜犯罪、酒駕行為、、、），規劃如何透由大數據機制，進行整體之控制，諸如：透由大數據之機制，找出「高風險」(high risk)之潛在犯罪人(potential offender)、潛在被害人(potential victim)、犯罪類型、犯罪場所(犯罪熱點)、犯罪情境、犯罪原因、強化網路警察之功能性，或加重違法後之行政及刑事罰則，以達到犯罪預防之效果。 |
| 第三級預防 | 第三級預防，傳統之觀點，係指對於已經犯罪之對象，由刑事司法機關進行逮捕後，施行矯正措施及更生保護之教化，避免再次犯罪。 | 在大數據應用於第三級犯罪預防之區塊上，可行之機制如下所述：對於已經發生之犯罪行為，由司法警察機關與檢察機關，積極偵查，利用刑事訴訟法之強制處分權，配合大數據之機制，找出犯罪嫌疑人，進行逮捕犯罪嫌疑人，避免犯罪危害之擴大；在被告之服刑期間，透過司法矯正機關之功能，經由大數據之機制，找出有效之矯正措施，安排各種輔導手段予以教化，或使其學習技能，使犯罪者具有謀生能力且能適應社會，減少其再犯罪之機率。進而利用大數據之機制，進行犯罪再犯之評估。 |

【資料來源】作者自繪。

。。。。。。。。。。。。。。。。。。[回目次](#a目次)〉〉

## 一、臺灣地區之法制現況

## （一）[憲法](https://www.6laws.net/6law/law/憲法.htm)

　　臺灣地區[憲法](https://www.6laws.net/6law/law/憲法.htm)對於人民個人資料之隱私權保護部分，並無相關明文規範；但依據2004年12月15日司法院釋字[第585號](https://www.6laws.net/6law/law/大法官解釋92-n年.htm#r585)解釋之理由書所述，隱私權雖非[憲法](https://www.6laws.net/6law/law/憲法.htm)明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活秘密空間免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法[第22條](https://www.6laws.net/6law/law/憲法.htm#a22)所保障。惟其所稱之保障，仍偏屬自由權利之保障，與大數據衍生之個人資料隱私權較無關聯性。

　　至2005年9月28日司法院釋字[第603號](https://www.6laws.net/6law/law/大法官解釋92-n年.htm#r603)解釋，即對於個人之資訊隱私權有進一步之闡釋，其解釋文所述，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。惟[憲法](https://www.6laws.net/6law/law/憲法.htm)對資訊隱私權之保障並非絕對，國家得於符合憲法[第23條](https://www.6laws.net/6law/law/憲法.htm#a23)規定意旨之範圍內，以法律明確規定對之予以適當之限制。

　　因此，臺灣地區之[憲法](https://www.6laws.net/6law/law/憲法.htm)條文雖未明文規定個人隱私權之保護，但就大法官解釋[憲法](https://www.6laws.net/6law/law/憲法.htm)之方向而言，已確立隱私權確實為[憲法](https://www.6laws.net/6law/law/憲法.htm)所保障之基本權利，且進一步奠立資訊隱私權保障之基本原則。

。。。。。。。。。。。。。。。。。。[回目次](#a目次)〉〉

## （二）[個人資料保護法](https://www.6laws.net/6law/law/個人資料保護法.htm)

臺灣地區於1995年制定「[電腦處理個人資料保護法](https://www.6laws.net/6law/law/電腦處理個人資料保護法.htm)」，因應時代變遷[[17]](#footnote-17)，其法令保護範圍明顯不足，遂於2010年將名稱修正為「[個人資料保護法](https://www.6laws.net/6law/law/個人資料保護法.htm)」並作全文修正，於個人資料保護法[第2條](https://www.6laws.net/6law/law/個人資料保護法.htm#a2)第1款之中，明文規定訂定個人資料及個人資料檔案之定義，以及蒐集、處理、利用個人資料之相關規範；至現今大數據時代來臨，為兼顧人格權保障與個人資料合理蒐集、處理及利用，並回應現今民意及社會需求[[18]](#footnote-18)，[個人資料保護法](https://www.6laws.net/6law/law/個人資料保護法.htm)又於2016年3月15日修正施行。

　　個人資料保護法[第1條](https://www.6laws.net/6law/law/個人資料保護法.htm#a1)開宗明義，即闡明並立法目的在於避免人格權受侵害及促進個人資料保護之合理利用；亦就是要確保個人資料之隱私，亦要合理之利用個人資料[[19]](#footnote-19)。在罰則部分，亦規範違反蒐集、處理或利用規定及限制國際傳輸之命令或處分之刑罰，以及妨害個人資料檔案正確之刑罰等，雖沒有針對電子商務及大數據可能衍生侵害個人資料或隱私之情形專章規範，但在各章節之條文中，都可找到適用之規定。

。。。。。。。。。。。。。。。。。。[回目次](#a目次)〉〉

## （三）[刑法](https://www.6laws.net/6law/law/刑法.htm)

　　臺灣地區之[刑法](https://www.6laws.net/6law/law/刑法.htm)並沒有針對大數據運用所衍生之隱私或個人資料犯罪問題訂有專章規範，其有關隱私權之保障之條文亦散落在各章節，如[第306條](https://www.6laws.net/6law/law/刑法.htm#a306)侵入住宅罪，就屬保障居家隱私，以及[第307條](https://www.6laws.net/6law/law/刑法.htm#a307)違法搜索罪，亦在保障個人身體隱私；而與本文研究範疇較具關聯性者，則屬[第315條](https://www.6laws.net/6law/law/刑法.htm#a315)至315條之3之妨害秘密專章，以及[第358條](https://www.6laws.net/6law/law/刑法.htm#a358)至第360條之[妨害電腦使用罪章](https://www.6laws.net/6law/law/刑法.htm#a358)，然而，其規範之內容，亦尚不足完全符合大數據應用下之需求。

。。。。。。。。。。。。。。。。。。[回目次](#a目次)〉〉

## 二、大陸地區之法制現況

　　大陸地區之電子商務發展相當快速，相對的與電子商務相關之個人信息保護及公民網絡空間之合法權益事項，亦有相當多之研究，大陸地區國務院互聯網信息辦公室早於2003年即委託社會科學院法學所針對個人信息保護法進行研究[[20]](#footnote-20)，在2016年第十二屆人大常委會上，因為涉及個人信息之違法事項泛濫，亦增加相關之法律事項予以規範[[21]](#footnote-21)，更於2016年人大常委會通過表決「[網路安全法](https://www.6laws.net/6law/law-gb/中華人民共和國網路安全法.htm)」，至此，「[網路安全法](https://www.6laws.net/6law/law-gb/中華人民共和國網路安全法.htm)」、「[國家安全法](https://www.6laws.net/6law/law-gb/中華人民共和國國家安全法.htm)」、「[反恐怖主義法](https://www.6laws.net/6law/law-gb/中華人民共和國反恐怖主義法.htm)」、「[刑法](https://www.6laws.net/6law/law-gb/中華人民共和國刑法.htm)」、「[保密法](https://www.6laws.net/6law/law-gb/中華人民共和國保守國家秘密法.htm)」、「[治安管理處罰法](https://www.6laws.net/6law/law-gb/中華人民共和國治安管理處罰法.htm)」、「[關於加強網絡信息保護的決定](https://www.6laws.net/6law/law-gb/全國人民代表大會常務委員會關於加強網路資訊保護的決定.htm)」、「[關於維護互聯網安全的決定](https://www.6laws.net/6law/law-gb/全國人民代表大會常務委員會關於維護互聯網安全的決定.htm)」、「[計算機信息系統安全保護條例](https://www.6laws.net/6law/law-gb/中華人民共和國電腦資訊系統安全保護條例.htm)」及「[互聯網信息服務管理辦法](https://www.6laws.net/6law/law-gb/互聯網資訊服務管理辦法.htm)」等法律法規，業已成為大陸地區網絡安全管理之整體法律體系[[22]](#footnote-22)。為與臺灣地區之法令規定作適切之比較，本文僅就[憲法](https://www.6laws.net/6law/law-gb/中華人民共和國憲法.htm)之精神及[網路安全法](https://www.6laws.net/6law/law-gb/中華人民共和國網路安全法.htm)、[刑法](https://www.6laws.net/6law/law-gb/中華人民共和國刑法.htm)等規範進行探討：

## （一）憲法

　　大陸地區[憲法](https://www.6laws.net/6law/law-gb/中華人民共和國憲法.htm)與臺灣地區[憲法](https://www.6laws.net/6law/law/憲法.htm)一般，均無對於公民之資訊隱私權保護有為明文之規定，但是在諸多條文規範及立法精神之中，仍可觀察出大陸地區[憲法](https://www.6laws.net/6law/law-gb/中華人民共和國憲法.htm)對於個人信息保護之精神，如[第38條](https://www.6laws.net/6law/law-gb/中華人民共和國憲法.htm#b38)規定，公民人格尊嚴不受侵犯，禁止用任何方法對公民進行侮辱、誹謗及誣告陷害；[第39條](https://www.6laws.net/6law/law-gb/中華人民共和國憲法.htm#b39)規定，公民住宅不受侵犯，禁止非法搜索或非法侵入公民住宅；[第40條](https://www.6laws.net/6law/law-gb/中華人民共和國憲法.htm#b40)規定，公民之通信自由和通信秘密受法律之保護，除因特定需要，由公安機關或檢察機關依法定程序進行檢查以外，任何組織及個人不得侵犯。

。。。。。。。。。。。。。。。。。。[回目次](#a目次)〉〉

## （二）[網路安全法](https://www.6laws.net/6law/law-gb/中華人民共和國網路安全法.htm)

[網路安全法](https://www.6laws.net/6law/law-gb/中華人民共和國網路安全法.htm)是在2016年11月由大陸地區人大常委會通過，在2017年6月1日正式實施，可謂是相當新之法律，內容規範除禁止網路業者蒐集並銷售用戶個人資料，同時亦在打擊網路詐騙犯罪，網路業者將不得蒐集與服務無關之用戶資訊，用戶亦有權要求業者刪除資訊[[23]](#footnote-23)。

　　整體而言，[網路安全法](https://www.6laws.net/6law/law-gb/中華人民共和國網路安全法.htm)之立法定位，是屬於網路安全基礎之保障；在立法架構上，則是將犯罪偵防、網路控制及違法懲處規定三者合一，有替代刑事法規之效果，而在制度設計上，則以網路運作及信息安全為軸心，設計相關控制節點。從犯罪偵防之角度而言，大陸地區之[網路安全法](https://www.6laws.net/6law/law-gb/中華人民共和國網路安全法.htm)，在目前大數據運用下所需求之最適切之法律規範，然後，因為法律實施不久，其執行成效仍有待觀察。

## （三）刑法

　　大陸地區[刑法](https://www.6laws.net/6law/law/刑法.htm)對於個人信息相關犯罪有直接規範之條文，應屬刑法修正案（七）第[253條之1](https://www.6laws.net/6law/law-gb/中華人民共和國刑法修正案(七).htm#a7)規定之對公民個人信息之保護；[第285條](https://www.6laws.net/6law/law-gb/中華人民共和國刑法.htm#a285)第2款規定之對計算機信息之保護等條文。

[刑法](https://www.6laws.net/6law/law-gb/中華人民共和國刑法.htm)雖是犯罪偵防之基本法，然而隨著網絡世代之掘起，法令規範有明顯不足之情形，究竟應該修正[刑法](https://www.6laws.net/6law/law/刑法.htm)以因應時代需求？或是訂定專法較符合全面性規劃？在實務界及學界各有不同之觀點。就大陸地區目前之作法而言，[網路安全法](https://www.6laws.net/6law/law-gb/中華人民共和國網路安全法.htm)之實行，似較偏向以訂定專法來處理網絡犯罪偵防之需求。

。。。。。。。。。。。。。。。。。。[回目次](#a目次)〉〉

## 三、小結

　　2012年被稱為全球「Big Data元年」，至今短短5年時間，不論在警政、教育、交通、財稅、交通等方面之科技運用，均與大數據密不可分；而兩岸人民對於大數據科技在生活之運用上，大陸地區人民遠較臺灣地區人民使用來的普及。大陸地區人民在生活上，使用實名化之手機，就可以完成購物支付、銀行開戶、叫車、購買交通票券、叫外賣…等，人民之生活圈幾已與大數據科技運用緊密結合。然而臺灣地區在此方面之作為就顯得趨為保守，除法令規範較為不足外，政府投入之資訊基礎建設亦顯然不夠，再者，臺灣地區詐騙案件層出不窮，罰責輕，再犯率高[[24]](#footnote-24)，亦造成部分臺灣地區人民（不論是顧客或是店家）對於電子商務之交易模式亦多持保留態度。

　　亦因為大陸地區人民在生活中已相當廣泛接觸大數據科技之應用，因此，亦可觀察到大陸地區政府在各層級相關之法令規範相當多，力求完善，尤其今年更是以專法處理之方式，實施[網路安全法](https://www.6laws.net/6law/law-gb/中華人民共和國網路安全法.htm)，即使如此，在實務上能否達到高效率之犯罪偵防效果，仍待觀察；而臺灣地區在相關之法令規範上，確實亦有追趕不上大數據時代潮流腳步之跡象，應有相當大之改善空間。

。。。。。。。。。。。。。。。。。。[回目次](#a目次4)〉〉

# 肆、兩岸大數據應用於犯罪偵防與隱私權保護之法制困境

　　有關於兩岸大數據科技應用於犯罪偵防與公民隱私權保護之法制困境，茲以下列研究發現之現象，探討說明如下所言：

## 一、法令不完備，犯罪偵防手段不積極，使臺灣地區社會對於電子商務交易行為普遍存有不信任感

　　臺灣地區社會對於電子商務普遍存有不信任感，仍是因為擔心使用電子商務進行交易，而被盜用身分，或是被詐欺取財，產生裹足不前之情形，然而這是一種因噎廢食之心態，亦會對於臺灣地區在電子商務發展上產生負面之影響。此種現象，亦可歸究於法令之不完備及犯罪偵防手段不夠積極，如有完善之法令可讓人民放心，又有積極之偵防行為作為後盾，應可增加人民之信心。

## 二、兩岸政府之憲法層級，均缺乏對於公民個資隱私權保護之法制

　　以臺灣地區為例，在憲法[第22條](https://www.6laws.net/6law/law/憲法.htm#a22)之中，所衍生出來之[憲法](https://www.6laws.net/6law/law/憲法.htm)基本權，共計有2種，第1種為人格權(釋字[664號](https://www.6laws.net/6law/law/大法官解釋92-n年.htm#r664))；第2種，則為「受國民教育以外之教育權」(釋字[626號](https://www.6laws.net/6law/law/大法官解釋92-n年.htm#r626))。而在上述之人格權(釋字[第664號](https://www.6laws.net/6law/law/大法官解釋92-n年.htm#r664))之中，從人格權衍生出來以下之憲法上「未列舉權」：婚姻家庭權(釋字[242號](https://www.6laws.net/6law/law/大法官解釋61-78年.htm#r242))、收養權(釋字[712號](https://www.6laws.net/6law/law/大法官解釋92-n年.htm#r712))、姓名權(釋字[399號](https://www.6laws.net/6law/law/大法官解釋79-86年.htm#r399))、獲知出生血統權(釋字[587號](https://www.6laws.net/6law/law/大法官解釋92-n年.htm#r587))、性行為自主權(釋字[554號](https://www.6laws.net/6law/law/大法官解釋87-91年.htm#r554))、依意志作為或不作為之一般行為(動)自由權(釋字[689號](https://www.6laws.net/6law/law/大法官解釋92-n年.htm#r689))、免於身心受傷害之身體權(身體不受傷害權)(釋字[689號](https://www.6laws.net/6law/law/大法官解釋92-n年.htm#r689))、契約自由權(釋字[第577號](https://www.6laws.net/6law/law/大法官解釋92-n年.htm#r577))、隱私權(釋字[第585號](https://www.6laws.net/6law/law/大法官解釋92-n年.htm#r585))、資訊自主控制權(釋字[第585號](https://www.6laws.net/6law/law/大法官解釋92-n年.htm#r585))、名譽權(釋字[656號](https://www.6laws.net/6law/law/大法官解釋92-n年.htm#r656))等等。綜上，在憲法學之解釋上憲法[第22條](https://www.6laws.net/6law/law/憲法.htm#a22)之本質，被稱為「未列舉權利」；其中之隱私權(釋字[第585號](https://www.6laws.net/6law/law/大法官解釋92-n年.htm#r585))及資訊自主控制權(資訊自主權)(釋字[603號](https://www.6laws.net/6law/law/大法官解釋92-n年.htm#r603))，均為「人格權」概念下之次級概念；亦即，「人格權」之實質內含，包括多樣化，其中之一項，即為「隱私權」[[25]](#footnote-25)。

　　雖然，透由司法院大法官會議之決議文之模式，賦予隱私權(資訊自主權)具有[憲法](https://www.6laws.net/6law/law/憲法.htm)上之崇高地位；然而，司法院大法官會議所作出之決議文，僅為十餘位大法官之意志，其能否「充分地」、「完全地」代表全國2300萬國民之意志，仍存有相當大之爭議性。臺灣地區之司法院大法官會議所作出之決議文，常受到非常多之批評，釋字[第748號](https://www.6laws.net/6law/law/大法官解釋92-n年.htm#r748)決議文(同性戀者之婚姻家庭權)即是適例。是以，建請仿照外國之立憲例，諸如仿照愛沙尼亞與瑞典之立憲例，直接在[憲法](https://www.6laws.net/6law/law/憲法.htm)之本文之中，加以明文規範為佳。亦即，臺灣地區[憲法](https://www.6laws.net/6law/law/憲法.htm)宜明文地保障「資訊自由權」(freedom of information)。

　　臺灣地區之[憲法](https://www.6laws.net/6law/law/憲法.htm)本文之立憲規範，在資訊權之保障方面，含外國人亦應可平等地享有「資訊權」之規範方面，係屬於缺位之狀態，並未明文化。依據司法院釋字[第603號](https://www.6laws.net/6law/law/大法官解釋92-n年.htm#r603)解釋，[憲法](https://www.6laws.net/6law/law/憲法.htm)肯認「資訊隱私權」；再者，司法院釋字[第585號](https://www.6laws.net/6law/law/大法官解釋92-n年.htm#r585)解釋，亦承認「資訊自主權」受到[憲法](https://www.6laws.net/6law/law/憲法.htm)之保障。然而，本文認為，最佳之立憲方法，仍是於[憲法](https://www.6laws.net/6law/law/憲法.htm)之本文之中，明定「資訊(自主)權」之保障為佳。在外國之憲法立法例部分，芬蘭憲法第12條將「表現」(達)、傳播與取得資訊之權利，明文規範於「表現權」之範圍內。亦即，表現權包括「資訊權」。

在瑞典部分，依據瑞典憲法第2章「基本人權與自由」（Fundamental Rights and Freedoms）中之第1條之規定，「資訊權」(freedom of information)包括：「取得權」(the freedom to obtain)與「接受(收)權」(the freedom to receive information)。另外，於瑞典憲法第2章「基本人權與自由」之第3條之中，則規範對於人民之各項資訊之登錄，不可侵犯人民之「人格完整性」( their personal integrity)。據上所述，瑞典憲法於第2章「基本人權與自由」之第3條之中，係明文承認人民享有「人格完整性」( their personal integrity)，且受到保障，不可侵犯之。再者，在瑞典憲法第2章「基本人權與自由」之第13條之中，則明定對於「資訊權」之限制之各項情況，諸如：基於維護國家安全與公共秩序之需。此外，瑞典憲法第2章「基本人權與自由」第20條第2項，亦規範外國人，亦享有資訊權。

　　除此之外，依照愛沙尼亞憲法第44條第3項之規定，舉凡為愛沙尼亞之公民(An Estonian citizen)，有權依據法律上之程序(pursuant to procedure provided by law)，向愛沙尼亞之國家機關、地方政府(held in state agencies and local governments)、及國家機關、地方政府公務檔案夾之中(and in state and local government archives)，所持有涉及其個人資料之公文檔案資訊，加以「取得」(has the right to access information about himself or herself)。此項資訊取得權，得基於法律之規定，因保護(障)他人之權利及自由(pursuant to law to protect the rights and freedoms of others)、保密孩童之出生資料(or the confidentiality of a child's filiation)、打擊犯罪之所需(and in the interests of combating a criminal offence)、逮補犯罪嫌疑人(apprehending a criminal offender)，或確認犯罪事實之需要(or ascertaining the truth in a criminal procedure)，加以限制之(This right may be restricted)。依照上開愛沙尼亞憲法第44條第3項之規定，為打擊犯罪之所需(and in the interests of combating a criminal offence)、逮補犯罪嫌疑人(apprehending a criminal offender)，或確認犯罪事實之需要(or ascertaining the truth in a criminal procedure)，可以限制公民之資訊自主權。

　　復次，依據，愛沙尼亞憲法第44條第4項之規定，舉凡在愛沙尼亞之外國公民與無國籍人士，除非法律另有規定之外，享有本條第2項與第3項之權利，其權利之行使，等同於愛沙尼亞之本國公民。

　　綜上，在愛沙尼亞憲法第44條之中，賦予愛沙尼亞之公民、外國人與無國籍人士，以「平等」之方式，享有資訊自主權(資訊控制權)，此等之權利，係明文規範於憲法第44條之條文之中。本文贊同此種之立憲模式，有利於憲法學之發展。

兩岸政府之憲法層級，均缺乏明文對於公民個資隱私權直接保護之法制，雖然在憲法條文中，對於人民之人格權、通信權、住宅安全等方面之隱私及相關人身安全之保障，均有明文規範，但是因應時代之快速變遷，是否需要以憲法之高度，直接保障個人資訊隱私等議題，確實值得再深入探討。

。。。。。。。。。。。。。。。。。。[回目次](#a目次4)〉〉

## 三、臺灣地區之網路個資相關法制相對於大陸地區之個資相關法制，顯得趨於狹隘

　　臺灣地區對於網路個資保護較為相關之法律，應屬「[個人資料保護法](https://www.6laws.net/6law/law/個人資料保護法.htm)」及「[電子簽章法](https://www.6laws.net/6law/law/電子簽章法.htm)」，然而其重點仍在於「個人資料」之保護，而非網路犯罪行為之偵防；相相較於上述大陸地區對於個人信息安全各層法令之規範，以及2017年實施之「[網路安全法](https://www.6laws.net/6law/law-gb/中華人民共和國網路安全法.htm)」，臺灣地區之法令，顯得趨於狹隘且不夠完備。

## 四、有關於將大數據科技應用於犯罪偵防部分，法律規範之積極性不足，導致犯罪偵防之手段亦無法充分施展運用

　　臺灣地區司法警察機關在偵防犯罪之過程中，有可能會運用以下之大數據資料庫，諸如：內政部警政署e化勤務指管系統-GIS案件應用分析系統、內政部警政署之警政知識系統、各縣市警察局之「犯罪資料庫管理系統」、戶政資訊系統、役政資訊系統、移民資訊系統、入出國生物辨識系統、犯罪地理分析系統、各重要地點之路口監視攝影機系統、涉及移民署勤業力之航前旅客資訊系統(APIS)、CCTV環境監控設備、RQI連線恐怖分子資料庫、航前旅客審查系統、陸客異常滯台統計查詢系統(監控全台機場港口、防止偷渡、恐怖份子等不法情事)…等等，以上如此眾多大數據之資料庫，均有可能被司法警察機關充作犯罪偵防之用途；首先面臨之問題，乃在於上述之大數據資料，是否均被個人資料保護法[第2條](https://www.6laws.net/6law/law/個人資料保護法.htm#a2)第1款「個人資料」之名詞定義所涵蓋，不無疑義。之所以會產生如此之爭議，乃在於[個人資料保護法](https://www.6laws.net/6law/law/個人資料保護法.htm)之立法過程之中，較欠缺大數據資料庫及電子商務之概念，是以，在[個人資料保護法](https://www.6laws.net/6law/law/個人資料保護法.htm)之中，有關於「個人資料」之定義，本文認為，似有待補充。

　　截至2017年為止，大陸地區有關於個資保護之相關法令，散見於以下之法令：大陸地區「民法通則意見」(第140條)、大陸地區「精神損害賠償司法解釋」(第1條)、大陸地區「侵權責任法」([第2條](https://www.6laws.net/6law/law-gb/中華人民共和國侵權責任法.htm#a2))、大陸地區「[民法](https://www.6laws.net/6law/law-gb/中華人民共和國民法通則.htm)」、大陸地區「消費者權益保護法」([第29條](https://www.6laws.net/6law/law-gb/中華人民共和國消費者權益保護法.htm#b29))、大陸地區「全國人民代表大會常務委員會關於加強網路信息保護的決定」、大陸地區「執業醫師法」([第22條](https://www.6laws.net/6law/law-gb/中華人民共和國執業醫師法.htm#a22))、大陸地區「傳染病防治法」([第12條](https://www.6laws.net/6law/law-gb/中華人民共和國傳染病防治法.htm#a12))、大陸地區「律師法」([第38條](https://www.6laws.net/6law/law-gb/中華人民共和國律師法.htm#b38))、大陸地區「保險法」([第32條](https://www.6laws.net/6law/law-gb/中華人民共和國保險法.htm#d32))、大陸地區「居民身分證法」[(第13條](https://www.6laws.net/6law/law-gb/中華人民共和國居民身份證法.htm#a13))、大陸地區「規範互聯網信息服務市場秩序若干規定」(簡稱為2011規定)、大陸地區「信息安全技術公共及商用服務資訊系統個人信息保護指南」(簡稱為2013指南)、大陸地區「電信和互聯網使用者個人信息保護規定」(簡稱為2013規定)、大陸地區「[網路安全法](https://www.6laws.net/6law/law-gb/中華人民共和國網路安全法.htm)」、「關於辦理侵犯公民個人信息刑事案件適用法律若干問題的解釋」(於2017年，由最高人民法院、最高人民檢察院聯合發布，簡稱「兩高司法解釋」)等等[[26]](#footnote-26)。承上所述，大陸地區有關於個人資料之保護，散見於各種法規之中，尚未出現類似於臺灣地區之「[個人資料保護法](https://www.6laws.net/6law/law/個人資料保護法.htm)」之專法。

　　復次，有關於將大數據科技應用於犯罪偵防部分，兩岸法律規範之積極性，均尚嫌不足，通常相關法令均僅訂有消極之處罰規定，而未訂有主動偵查及預防性之規定。然而，主動偵查之規定，多規範於[刑法](https://www.6laws.net/6law/law-gb/中華人民共和國刑法.htm)或[刑事訴訟法](https://www.6laws.net/6law/law-gb/中華人民共和國刑事訴訟法.htm)，一般行政法規雖亦有行政刑罰之規定，但仍較少訂有偵查權之規定；而預防性之規定，則可參考大陸地區「[網路安全法](https://www.6laws.net/6law/law-gb/中華人民共和國網路安全法.htm)」[第63條](https://www.6laws.net/6law/law-gb/中華人民共和國網路安全法.htm#a63)規定，其違反同法[第27條](https://www.6laws.net/6law/law-gb/中華人民共和國網路安全法.htm#a27)規定有竊取網路數據等違法行為而受刑事處罰人員，終身不得從事網絡安全管理等相關工作，此即屬於預防性條文。有更多更明確之犯罪偵防之條文規定，始能實質達到法律執行之成效。

。。。。。。。。。。。。。。。。。。[回目次](#a目次4)〉〉

## 五、兩岸政府目前尚未共同著手建置以犯罪偵防為目的之大數據資料庫，不利於兩岸犯罪偵防情資之交流，同時，亦不利於兩岸犯罪偵防相關工作之開展

　　本文在此，擬舉出一個有關於跨國之間，建置以犯罪偵防為目的之大數據資料庫之實際案例，亦即，有關美、加兩國之間，共同打擊人口販運犯罪之案件，如下所述。於2001年，美國及加拿大共同偵破11歲美國少女被迫賣淫案[[27]](#footnote-27)。在2001年2月間，有一位位處於美國俄勒岡州波特蘭地區之11歲少女，遭到歹徒之綁架(an 11-year-old child was abducted from Portland, Oregon)，之後，被運送經過美、加兩國之國界，再被販運至加拿大英屬哥倫比亞之溫哥華，並且這一位11歲美國少女，被歹徒脅迫從事性交易(the child was forced into the sex-trade)。

　　透由美、加兩國所共同建構，且相互連線之「阻斷及辨識性交易買春者」(the Deter and Identify Sex Consumers，DISC)之電子資料庫系統，事實上，它是一個大數據資料庫。美加兩國立即進行相互之溝通，並交換情報(worked quickly to communicate information)。上述之「阻斷及辨識性交易買春者」大數據資料庫系統之功能，它連接美、加兩國若干個警察執法機關(links several Canadian and U.S.police forces)。之後，美、加兩國並啟動打擊人口販運犯罪之實際聯合偵處行動(initiated a joint investigation)，偵查之結果，致使罪犯受到美、加兩國之追訴。最後，此一案件之人口販運罪犯，被受到判刑，並被拘禁於美國監獄之中(incarcerated in the United States)。

　　本文茲再以「東協警察組織」(ASEANAPOL)為例，目前，ASEANAPOL正積極地建構一套「東協警察組織電子資料庫系統」(Electronic ASEANAPOL Database System，簡稱為e-ADS)。ASEANAPOL 所屬之e-ADS之構想，乃在於將恐佈份子、毒品販運、通緝罪犯之個資，置於統一之資料庫之中，以供東協國家使用[[28]](#footnote-28)。

　　在此，本文亦積極地建請我方政府，宜爭取能與東協國家共享上述ASEANAPOL所屬之e-ADS系統；復次，東協亦成立「東協警察組織電子資料庫技術委員會」(ADSTC)，ADSTC之功能與任務，乃在於與國際刑警組織共同研商，會商能令上述之e-ADS，與國際刑警組織I-24/7兩個大數據資料庫進行連線之網路介接事宜[[29]](#footnote-29)。

　　反觀兩岸地區之政府，目前，並未共同著手建置以犯罪偵防為目的之大數據資料庫，不利於兩岸犯罪偵防情資之交流，此為非常可惜之處。同時，亦不利於兩岸犯罪偵防相關工作之開展，就兩岸共同打擊犯罪之立場而言，此一部分，兩岸地區之政府，應可再予著墨，朝互助合作之方向再努力。

。。。。。。。。。。。。。。。。。。[回目次](#a目次4)〉〉

# 伍、兩岸大數據科技應用於犯罪偵防與公民隱私權保護之法制對策---代結論

　　有關於兩岸大數據科技應用於犯罪偵防與公民隱私權保護之法制對策部分，本文提出以下之建言，俾供兩岸政府與兩岸社會大眾參考之用。

## 一、臺灣地區應強化相關法令措施，以「犯罪偵防」與「保護個資」同時並進之積極作為，取代「拒絕建立數位身分」之消極不作為，並提高民眾使用電子商務之信心，始能有效擴大消費通路，提升國家整體經濟

　　由於電子商務之本質，乃交易雙方均以電腦(Computer)、手機、電子紙、平板、電腦等新興之手持式電子產品(Handhold Device)，透過有線、無線或行動之網路方式，進行商業交易活動或相關之服務[[30]](#footnote-30)；是以，業者電子商務之各式營業資料與客戶(消費者)資料，均具有大數據之屬性與特質；當執法機關從事犯罪偵防工作時，即有可能運作上述之大數據資料，作為犯罪偵防之素材與基石，以鎖定一位或多位犯罪者之電子商務活動，進而將其繩之以法。

　　是以，將大數據運用於犯罪偵防，恐是一條必走之路；目前，臺灣地區在規範電子商務之機制方面，訂有「電子商務個人資料管理制度建置計畫」與「[個人資料保護法](https://www.6laws.net/6law/law/個人資料保護法.htm)」；但是，就犯罪偵防之工作，須運用電子商務所儲存之大數據資料，以勾劃出犯罪活動之層面而論，臺灣地區「[個人資料保護法](https://www.6laws.net/6law/law/個人資料保護法.htm)」之法規範內容，在[第2條](https://www.6laws.net/6law/law/個人資料保護法.htm#a2)、[第5條](https://www.6laws.net/6law/law/個人資料保護法.htm#a5)、[第8條](https://www.6laws.net/6law/law/個人資料保護法.htm#a8)、[第9條](https://www.6laws.net/6law/law/個人資料保護法.htm#a9)、[第15條](https://www.6laws.net/6law/law/個人資料保護法.htm#a15)之部分，或可供作犯罪偵防之用，但依舊仍有隔靴搔癢與不夠精緻化之感[[31]](#footnote-31)；主要之原因，在於司法警察機關乃是相當「特殊」之公務機關，而非一般文職公務機關，在適用上，乃有不明確之處，本文認為，臺灣地區似可強化上述之[個人資料保護法](https://www.6laws.net/6law/law/個人資料保護法.htm)或另訂專法，另外，似亦可參卓TPP第14章[第7條](https://www.6laws.net/6law/law/個人資料保護法.htm#a7)、[第8條](https://www.6laws.net/6law/law/個人資料保護法.htm#a8)、[第14條](https://www.6laws.net/6law/law/個人資料保護法.htm#a14)之立法精神，另外，並設計專供司法警察犯罪偵防所需之個人資料之運用與處理之法規範，以補強現行之缺漏處。

　　除上述之選項之外，另外，亦可思考在通訊傳播匯流五個法律草案之中，加入司法警察機關運用大數據之個資，進行犯罪偵防之機制，而上述之通訊傳播匯流五法草案，乃指：「電子通訊傳播法」草案、「電信基礎設施與資源管理法」草案、「電信事業法」草案、「有線多頻道平臺服務管理條例」草案及「無線廣播電視事業與頻道服務提供事業管理條例」草案等五種法律之草案。

。。。。。。。。。。。。。。。。。。[回目次](#a目次4)〉〉

## 二、考量大數據時代之變遷迅速，對於大數據科技應用之相關法制規範，應跳脫現行法律原則之思維，採用較為彈性之規範，或於修法之程序上更為便捷，同時，宜考量建置專法之可行性，同時，將大數據科技應用於犯罪偵防部分，將其明文化於法律之規範之中，以順應需求，俾符合犯罪偵防之用

　　以臺灣地區之[個人資料保護法](https://www.6laws.net/6law/law/個人資料保護法.htm)為例，除前文所述，有關於「個人資料」之定義，似有待補充。此外，涉及「公務機關與公務機關」之間，以及「公務機關與非公務機關」之間，「[個人資料保護法](https://www.6laws.net/6law/law/個人資料保護法.htm)」就其所建置或保有之大數據資料庫，如何進行分享與傳遞，以利司法警察機關進行犯罪偵防之用，「[個人資料保護法](https://www.6laws.net/6law/law/個人資料保護法.htm)」條文之規範，似不夠明確化與精細化。再者，個人資料保護法[第15條](https://www.6laws.net/6law/law/個人資料保護法.htm#a15)之「處理」之機制，可否包括公務機關相互間之「傳遞」，亦是有非常大之模糊空間。比較可行之解釋模式，係將「傳遞」列為「利用」之範疇，同時，並將「接收」列為「蒐集」之領域之中[[32]](#footnote-32)。

本文認為，在中文之語義上，「傳遞」與「分享」是否等同於「利用」；「接收」是否等同於「蒐集」，恐有極大之爭議性，比較理想之立法方式，係在界定「利用」與「蒐集」之法律用語之時，宜再精緻化，亦即宜將「傳遞」與「接收」之用語加以界定之。此亦呼應本文之主張，就司法警察機關在犯罪偵防之區塊上，及其衍生之隱私權之保護，現行之「[個人資料保護法](https://www.6laws.net/6law/law/個人資料保護法.htm)」之法規範，過於簡略與不足，有進行修法之必要；或者，另訂專法，亦是理想之選項，本文贊同直接修改「[個人資料保護法](https://www.6laws.net/6law/law/個人資料保護法.htm)」以為因應之。

。。。。。。。。。。。。。。。。。。[回目次](#a目次4)〉〉

## 三、在大陸地區個資保護之相關法制部分，本文建議大陸地區宜儘速通過與正式施行「個人信息保護法」

　　在個人資料保護之立法進度方面，大陸地區目前有2種不同之版本，第1種版本係為大陸地區社會科學研究院法律研究所草擬之大陸地區「個人信息保護法」專家建議稿；第2種之版本，則為學者齊愛民教授於2005年所提出之大陸地區「個人信息保護法示範法草案學者建議稿」(簡為齊愛民建議稿) [[33]](#footnote-33)。綜上所述，本文認為，雖然，大陸地區業已施行「[網路安全法](https://www.6laws.net/6law/law-gb/中華人民共和國網路安全法.htm)」，但「[網路安全法](https://www.6laws.net/6law/law-gb/中華人民共和國網路安全法.htm)」、「關於辦理侵犯公民個人信息刑事案件適用法律若干問題的解釋」不能「完全」取代「個人信息保護法」[[34]](#footnote-34)，大陸地區有關於個人信息(內含隱私權)之保護，宜儘速通過「個人信息保護法」草案為佳，以加大對於民眾個資保護之力道與能量。

。。。。。。。。。。。。。。。。。。[回目次](#a目次4)〉〉

## 四、兩岸政府之憲法層級，宜明文規範對於公民個資之資訊權與隱私權之保護法制

　　兩岸政府之憲法層次，假如針對於各自之憲法「本文」之法規範而言，截至2017年為止，尚未對於「資訊權」之此一項權利，在憲法「本文」之中，用非常明確之憲法用語，加以明確保障之，此為非常可惜之處。玆以臺灣地區之憲法為例，在[第22條](https://www.6laws.net/6law/law/憲法.htm#a22)之中，對於上文所提及「未列舉權利」之內涵，缺乏明文規範，須再閱覽釋字[第585號](https://www.6laws.net/6law/law/大法官解釋92-n年.htm#r585)解釋文，始得窺其內涵。如此之立憲模式，是否適切？頗有爭議性。比較良善之立憲模式，本文建議，兩岸地區之政府，宜各自仿照瑞典與愛沙尼亞之立憲例，於憲法之本文條文之中，明訂對於資訊自決權之保障，及其但書例外之規範。

。。。。。。。。。。。。。。。。。。[回目次](#a目次4)〉〉

## 五、兩岸政府宜基於平等、互惠、互信之原則，共同建置以犯罪偵防為目的之大數據資料庫，以利於兩岸犯罪偵防情資之交流，同時，亦有利於兩岸犯罪偵防相關工作之順利開展

　　兩岸地區之政府，為了共同打擊犯罪與進行司法互助，業已相互簽定與實施「[海峽兩岸共同打擊犯罪及司法互助協議](https://www.6laws.net/6law/law2/海峽兩岸共同打擊犯罪及司法互助協議.htm)」。根據本協議之規定，在立法宗旨方面，主要是為保障海峽兩岸人民權益，維護兩岸交流秩序，財團法人海峽交流基金會與海峽兩岸關係協會就兩岸共同打擊犯罪及司法互助與聯繫事宜，經平等協商，達成本協議。相關內涵如下所述：共分為5章，[第1章](https://www.6laws.net/6law/law2/海峽兩岸共同打擊犯罪及司法互助協議.htm#a1)：總則。[第2章](https://www.6laws.net/6law/law2/海峽兩岸共同打擊犯罪及司法互助協議.htm#a4)：共同打擊犯罪。[第3章](https://www.6laws.net/6law/law2/海峽兩岸共同打擊犯罪及司法互助協議.htm#a7)：司法互助。[第4章](https://www.6laws.net/6law/law2/海峽兩岸共同打擊犯罪及司法互助協議.htm#a13)：請求程序。第5章：[附則](https://www.6laws.net/6law/law2/海峽兩岸共同打擊犯罪及司法互助協議.htm#a21)。在條文方面，共計有24條。很可惜之處，其缺乏共同建置犯罪偵防大數據資料庫之相關條文。

　　兩岸地區之政府，為了達到共同建置以犯罪偵防為目的之大數據資料庫之目標，在此同時，亦宜適切地修改「海峽兩岸共同打擊犯罪及司法互助協議」之相關條文，加入以下之內容，俾利於兩岸地區之政府，共同建置犯罪偵防大數據之資料庫：

　　1.明訂兩岸之建置原則，乃基於平等(對等)、互惠、互信、尊嚴；

　　2.兩岸共同建置犯罪偵防大數據資料庫之目的、用途、方法；

　　3.犯罪偵防大數據資料庫之建置、運用、傳送、接收與處理方法；

　　4.個資隱私權之保障；

　　5.個資遭受侵害之救濟機制；

　　6.與國際及區域性組織之犯罪偵防大數據資料庫(諸如：e-ADS與I-24/7)進行連接，及個資之運用之相關機制。

　　透由上述之機制，本文認為，對於兩岸犯罪偵防相關工作之推展，會有實質性之助益。

。。。。。。。。。。。。。。。。。。[回目次](#a目次4)〉〉

# 【參考文獻】

。[一、中文資料](#_一、中文資料)。[二、英文資料](#_二、英文資料)

# 一、中文資料

◎Marc Goodman(2016)，林俊宏譯，未來的犯罪，新北：木馬文化。

◎William Brittain-Catlin著、李芳齡譯(2007)，境外共和國：揭開境外金融的秘密，天下雜誌出版。

◎十二屆人大常委會：個人信息怎麼保護( 2016)，華律網，2016年10月31日， <http://www.66law.cn/laws/159822.aspx>。

◎土城分局(2015)，刑事局偵破3仟萬城堡別墅機房兩岸電信詐欺集團案，新北市政府警察局新莊分局，上網瀏覽時間：2015/10/01, <http://www.xinzhuang.police.ntpc.gov.tw/cp-492-11757-18.html>。

◎中華人民共和國公安部(2015)，公安部與美國警方聯合摧毀全球最大中文淫穢色情網站聯盟，瀏覽日期：2015/10/30，網址：<http://app.mps.gov.cn:8888/gips/contentSearch?id=2871356>

。

◎內政部警政署(2010)，警察偵查犯罪手冊，台北：內政部警政署。

◎王勁力(2010)，論我國高科技犯罪與偵查－數位證據鑑識相關法制問題研究，科技法律評析，第3期，高雄：國立高雄第一科技大學。

◎王勁力(2013)，電腦網路犯罪偵查之數位證據探究，檢察新論，第13期，台北：台灣高等法院檢察署。

◎王乾榮(2004)，犯罪偵查，臺灣警察專科學校，第369-372頁。

◎王翔正(2011)，網路即時通訊詐欺犯罪偵查，刑事雙月刊45期，42-45頁。

◎王寬弘(2011)，大陸地區人民進入台灣相關入出境法令問題淺探，2011年人口移動與執法學術研討會，桃園：中央警察大學。

◎王寬弘(2012)，大陸地區人民進入台灣相關入出境法令問題淺探，國土安全與國境管理學報，第17期，桃園：中央警察大學，頁155-185。

◎立法院(2015)，防治網路霸淩公聽會：立委王育敏召開公聽會，研商網路霸淩防治，瀏覽日期：2015/11/12，<http://www.ly.gov.tw/03_leg/0301_main/public/publicView.action?id=6512&lgno=00004&stage=8>。

◎刑事警察局偵查第9大隊(2015)，國內首宗兩岸合作偵破最大網站賭博第3方支付中心，上網瀏覽時間：2015/10/01, <http://www.cib.gov.tw/news/Detail/29436>。

◎朱昌俊(2016)，網路安全法不能取代個人信息保護法，2016年11月09日，<http://webcache.googleusercontent.com/search?q=cache:gNer_oileoQJ:http://ep.ycwb.com/epaper/ycwb/html/2016-11/09/content_186075.htm%2B%E7%B6%B2%E7%B5%A1%E5%AE%89%E5%85%A8%E6%B3%95++%E5%80%8B%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E8%AD%B7%E6%B3%95&hl=zh-TW&gbv=2&ct=clnk>。

◎何芸欣(2005)網路詐欺之研究，國立臺北大學碩士論文。

◎余德正（2000）不法使用網際網路之刑事責任。東海大學法律學系研究所碩士論文。

◎呂惠娟(2017)，物聯網與電子商務的發展趨勢，紡織月刊，第249期，頁28-32。

◎李進建( 2015)，論大數據於犯罪偵查之挑戰與因應，全國律師，頁60-70。

◎汪毓瑋(2015)，國土安全理論與實踐之發展，國土安全與國境管理學報，第23 期，頁1-47。

◎周漢華( 2006)，個人信息保護法（專家建議稿）及立法研究報告，北京：法律。

◎孟維德( 2015)，跨國犯罪，台北：五南，頁397-434。

◎孟維德(2005)，海峽兩岸跨境犯罪之實證研究－以人口走私活動為例，刑事政策與犯罪研究論文集（13），頁137-184。

◎孟維德、黃翠紋(2012)，警察與犯罪預防，台北：五南。

◎林山田、林東茂（1997）。犯罪學。臺北：三民。

◎林文龍（2003）線上遊戲犯罪偵查模式之研究。佛光人文社會學院資訊學研究所碩士論文。

◎林宜隆（2009）。網路犯罪：理論與實務，網際網路與犯罪問題，修訂第三版，桃園：中央警察大學。

◎林宜隆、邱士娟(2003)，我國網路犯罪案例現況分析，中央警察大學『資訊、科技與社會』學報。

◎林宜隆、張志汖（2008）。台灣地區網路犯罪現況分析-以刑事警察局破獲之案例為例，知識社群與系統發展學術研討會，臺北：文化大學。

◎林宜隆、黃讚松（2002），建構網路犯罪預防整體概念，中央警察大學『資訊、科技與社會』學報。

◎林宜隆、葉家銘(2008)，論述ISMS資訊安全管理系統發展網路犯罪預防策略的新方法，發表於教育部TANet 2008 研討會，台北：教育部，瀏覽日期：2015/11/1，網址：<http://www.powercam.cc/show.php?id=678&ch=23&fid=119>。

◎邱俊霖(2015)，近年科技犯罪趨勢與犯制對策，刑事雙月刊，第65期，台北：內政部警政署刑事警察局。

◎邱琳雅( 2008)，德國聯邦個人資料保護法（BDSG），金融聯合徵信雙月刊，第8期，頁60-64。

◎宣律師( 2016)，圖解式法典：憲法及相關法規，台北：高點，頁50-56。

◎施能新(2005)，電子郵件犯罪偵查機制之研究，中央警察大學資訊管理研究所碩士論文，16-30頁。

◎柯雨瑞、蔡政杰( 2016)，從犯罪預防觀點探討兩岸跨境網路犯罪之治理，收錄於全球化下之國境執法，台北：五南，頁33-62。

◎洪文玲( 2005)，行政調查制度之研究，內政部警政署警察法學，第4期。

◎范國勇，江志慶(2015)，ATM 轉帳詐欺犯罪之實證研究，刑事政策與犯罪研究論文集（8），頁185-208。

◎個人資料保護法之總說明及部分條文修正說明，<https://www.moj.gov.tw/lp.asp?CtNode=28007&CtUnit=805&BaseDSD=7&mp=001>。

◎徐振雄(2010)，網路犯罪與刑法妨害電腦使用罪章中的法律語詞及相關議題探討，國會月刊，第38卷第1期，台北：立法院。

◎徐源隆（2003）網路拍賣詐欺犯罪之偵查對策，第七屆資訊管理學術計警政資訊實務研討會。

◎高信雄(2012)，跨境網路犯罪研究:基於犯罪偵防策略模型，中央警察大學資訊管理研究所碩士論文。

◎張樹德，翁照琪（2010），兩岸毒品犯罪型態與防治作為之實證研究，2010非傳統安全－反洗錢、不正常人口移動、毒品、擴散學術研討會，桃園：中央警察大學。

◎教育研究院雙語詞彙、學術名詞暨辭書資訊網(2015)，上網瀏覽時間：2015/10/01, <http://terms.naer.edu.tw/>。

◎曹明、程永進、張哲、曹銳生、鄭新傑(2015)，台灣全科醫學模式之我見，上網瀏覽時間：2015/10/05，<http://gp.cmt.com.cn/detail/30561.html>。

◎梁添盛( 2011)，論警察權限之強制手段與任意手段，中央警察大學學報，48 期，頁223〜260。

◎移民署(2015)，公務統計數據，上網瀏覽時間：2015/10/01, <http://www.immigration.gov.tw/ct.asp?xItem=1291286&ctNode=29699&mp=1>.

◎莊忠進（1996）。電腦犯罪偵查與立法之研究，臺北：警專。

◎許春金（2007）。犯罪學，修訂第五版。臺北：三民。

◎許春金，陳玉書(2013)。犯罪預防與犯罪分析，二版，台北：三民。

◎許春金，陳玉書，蔡田木(2015)，中華民國103年犯罪狀況及其分析-2014犯罪趨勢關鍵報告，法務部司法官學院104年委託研究計畫，瀏覽日期：2015/11/1，網址：<http://www.moj.gov.tw/ct.asp?xItem=392644&ctNode=35595&mp=302>

◎許春金、陳玉書( 2013)，犯罪預防與犯罪分析，台北：三民，頁7-11。

◎許慈健(2005)，網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究，93-134頁。

◎許福生(2016)，犯罪學與犯罪預防，台北：元照。

◎郭桓甫( 2015)，兩岸人格權之比較研究－以個人資料保護為中心，嘉義：國立中正大學財經法律學研所碩士學位論文，頁1-141。

◎陳立昇(2015)，疾病篩檢基本概念，上網瀏覽時間：2015/10/05，<http://www.hpa.gov.tw/BHPNet/Portal/File/ThemeDocFile/2007082059425/050427%E7%96%BE%E7%97%85%E7%AF%A9%E6%AA%A2%E5%9F%BA%E6%9C%AC%E6%A6%82%E5%BF%B5_2.pdf>

◎陳孟君(2016)，WTO擬參考主要FTA架構制定電子商務新規則－以TPP電子商務為例，經濟前瞻，第168期，頁97-100。

◎陳明傳(2007)，跨國(境)犯罪與跨國犯罪學之初探，收於第一屆國土安全學術研討會論文集，桃園縣：中央警察大學。

◎陳明傳(2015)，各國入出國管理系統之比較研究，發表於中央警察大學移民研究中心2015年人口移動與執法學術研討會，桃園縣：中央警察大學。

◎陳彥驊(2015)，濫用社群網站，人蛇集團效率高，台灣醒報網站，上網瀏覽時間：2015/10/01, <https://tw.news.yahoo.com/%E7%A4%BE%E7%BE%A4%E7%B6%B2%E7%AB%99%E4%BE%BF%E4%BD%BF-%E4%BA%BA%E8%9B%87%E9%9B%86%E5%9C%98%E6%95%88%E7%8E%87%E6%8F%90%E5%8D%87-091523250.html>。

◎陳惟凡、陳振楠、伍台國( 2016)，電子商務平臺之安全風險評估模式：植基於ISO27001資訊安全管理系統與個人資料保護法，電腦稽核，第34期，頁28-42。

◎陳嘉玫(2011)， 網路安全的社交工程，科學發展461期。

◎黃明凱（2002），網路犯罪輔助偵查專家系統雛型之建構，中央警察大學資訊管理研究所碩士論文。

◎黃秋龍(2008)，中國大陸網路犯罪及其衝擊，展望與探索，第6卷第12期，台北：法務部調查局。

◎黃登銘(2013)，網路犯罪模式分析與偵查機制之研究－以網路詐欺為例，國立宜蘭大學多媒體網路通訊數位學習碩士在職專班碩士論文。

◎楊永年、楊士隆、邱柏嘉、李宗憲(2009)，網路犯罪防治體系之政府職能與角色分析，行政院研究發展考核委員會委託國立臺灣大學研究報告。

◎楊秀莉(2015)，中國內地與澳門網絡犯罪的刑法比較及完善建議，一國兩制研究第1期，瀏覽日期：2015/10/27網址：<http://www.ipm.edu.mo/cntfiles/upload/docs/research/common/1country_2systems/2012_1/p176.pdf>。

◎葉雲宏（2008），網路詐欺犯罪被害影響因素之研究，中央警察大學犯罪防治研究所碩士論文。

◎詹鎮榮( 2015)，公務機關間個人資料之傳遞－以臺灣桃園地方法院行政訴訟102年度簡字第2號判決出發，法學叢刊，第60卷第一期，頁1-25。

◎資策會科技法律研究所(2015)，加拿大保護加拿大國民遠離網路犯罪法生效，保障國民免受網路霸淩，瀏覽日期：2015/11/12，<https://stli.iii.org.tw/ContentPage.aspx?i=6845>。

◎廖有祿、李相臣（2003）。電腦犯罪-理論與實務，初版一刷。臺北：五南。

◎廖福村(2007)，犯罪預防，台北：警專。

◎維基百科(2015)，網路犯罪公約，上網瀏覽時間：2015/10/01, <https://zh.wikipedia.org/wiki/%E7%B6%B2%E8%B7%AF%E7%8A%AF%E7%BD%AA%E5%85%AC%E7%B4%84>。

◎網絡安全法的立法定位、立法框架和制度設計( 2016)，大陸地區網信網，2016年11月10日，<http://www.npc.gov.cn/npc/lfzt/rlyw/2016-11/21/content_2002310.htm>。

◎臺灣地區法規資料庫(2015)，上網瀏覽時間：2015/10/01, <http://law.moj.gov.tw/Index.aspx>。

◎劉佐國，李世德( 2015)，個人資料保護法釋義與實務—第二版—如何面臨個資保護的新時代，台北：碁峰。

◎劉邦乾(2012)，海路毒品販運組織及犯罪手法之研究，台北：國立臺北大學犯罪學研究所碩士論文。

◎蔡美智（1998）。電腦駭客入侵的法律問題，資訊與電腦雜誌。

◎蔡德輝(2009)，犯罪學，台北：五南。

◎鄧煌發(1997)，犯罪預防，桃園：中央警察大學。

◎鄧煌發、李修安(2012)，犯罪預防，台北：一品。

◎鄭厚堃(1993)，犯罪偵查學，中央警察大學出版社，第1-32頁。

◎震宇(1997)，論網路商業化所面臨的管轄權問題（上），資訊法務透析第9期，第18-34頁

◎蕭季慧編(1993)，犯罪偵查與蒐集證據，中央警官學校出版社，第30-38頁。

◎賴錦宏( 2017)，網路安全法，大陸明天上路，聯合報，2017年5月31日，版A8。

◎謝立功(2004)，由大陸觀光客脫團事件論我國國境管理機制，展望與探索第2卷第9期，台北：法務部調查局，頁14-20。

◎謝孟珊(2016)，美國電子商務政策與重要法制簡介，科技法律透析，第28卷第4期，頁50-69。

◎顏旺盛、陳松春(2011)， 迎接21世紀跨境犯罪之挑戰， 刑事雙月刊39期，第 57-60頁。

◎蘇柏毓( 2016)，104年之個人資料保護法修正簡評，科技法律透析，第28卷第4期，頁13-17。

。。。。。。。。。。。。。。。。。。[回參考文獻](#a參考文獻)〉〉

# 二、英文資料

◎Bart van der Sloot & Sascha van Schendel(2016).Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study.Journal of Intellectual Property, Information Technology and E-Commerce Law(JIPITEC), Vol.7.

◎Britz, Marjie T.(2009).Computer Forensics and Cyber Crime : An Introduction, Second Edition.USA: Prentice Hall.

◎Clough, D.(2010).Principles of Cybercrime.UK: Cambridge University.

◎Council of Europe(2015), “Convention on Cybercrime”, Retrieved on 2015/10/02, <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=11&DF=6/21/2007&CL=ENG>.

◎Data Protection Act 1998( 1998), legislation.gov.uk, 1988/7,<http://www.legislation.gov.uk/ukpga/1998/29/contents>.

◎Evans, K.(2011).Crime Prevention: A Critical Introduction.USA: SAGE Publications Ltd.

◎Fennelly, L.& Crowe, T.(2013).Crime Prevention Through Environmental Design, Third Edition.USA: Butterworth-Heinemann.

◎Lab, P.(2013).Crime Prevention: Approaches, Practices, and Evaluations.8th Edition.USA: Routledge.

◎Mackey, D & Levan, K(2011).Crime Prevention.USA: Jones & Bartlett Learning.

◎Public Safety Canada( 2011), Bi-National Assessment on Trafficking in Persons , Public Safety Canada,<https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-ssssmnt-trffckng-prsns/index-en.aspx>.

◎Reyes, A.(2007).Cyber Crime Investigations: Bridging the Gaps Between, Security Professionals, Law Enforcement, and Prosecutors.USA: Syngress.

◎Schneider, S.(2014).Crime Prevention: Theory and Practice, Second Edition.USA: CRC Press.

◎The United States Department of Justice(1974), “Privacy Act of 1974,”<https://ww-w.justice.gov/opcl/privacy-act-1974>.

◎Todd, G.& Bowker, A.(2014).Investigating Internet Crimes : An Introduction to Solving Crimes in Cyberspace.USA: Steven Elliot.

◎Twelfth United Nations Congress on Crime Prevention and Criminal Justice(2015), “Working paper prepared by the Secretariat on recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime, A/CONF.213/9”, Retrieved on 2015/10/02, <http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/V1050320e.pdf>.

。。。。。。。。。。。。。。。。。。。。。。。。。[回首頁](#top)〉〉

1. ### 柯雨瑞（Jui-Rey, Ko）：中央警察大學國境警察學系暨研究所，專任教授。通訊地址：33304桃園市龜山區大崗里樹人路56號。Email：ko@mail.cpu.edu.tw。

   [↑](#footnote-ref-1)
2. ### 蔡政杰（Chen-Chien, Tsai）：移民署視察、中央警察大學國境警察學系兼任講師。通訊地址：臺北市中正區廣州街15號6樓。Email：cpu-cctsai@mail.cpu.edu.tw。

   [↑](#footnote-ref-2)
3. ### 謝孟珊，〈美國電子商務政策與重要法制簡介〉，《科技法律透析》，第28卷第4期，2016年4月，頁50-69。

   [↑](#footnote-ref-3)
4. ### 呂惠娟，〈物聯網與電子商務的發展趨勢〉，《紡織月刊》，第249期，2017年3月，頁28-32。

   [↑](#footnote-ref-4)
5. ### 陳孟君，〈WTO擬參考主要FTA架構制定電子商務新規則－以TPP電子商務為例〉，《經濟前瞻》，第168期，2016年11月，頁97-100。

   [↑](#footnote-ref-5)
6. ### 陳孟君，〈WTO擬參考主要FTA架構制定電子商務新規則－以TPP電子商務為例〉，《經濟前瞻》，第168期，2016年11月，頁97-100。

   [↑](#footnote-ref-6)
7. ### “Privacy Act of 1974,” The United States Department of Justice,1974/12,〈<https://ww-w.justice.gov/opcl/privacy-act-1974>〉.

   [↑](#footnote-ref-7)
8. ### 邱琳雅，〈德國聯邦個人資料保護法（BDSG）〉，《金融聯合徵信雙月刊》，第八期， 2008年10月，頁60-64。

   [↑](#footnote-ref-8)
9. ### “Data Protection Act 1998,” legislation.gov.uk, 1988/7,〈<http://www.legislation.gov.uk/ukpga/1998/29/contents>〉.

   [↑](#footnote-ref-9)
10. ### Bart van der Sloot & Sascha van Schendel. 〈Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study〉. 《Journal of Intellectual Property, Information Technology and E-Commerce Law (JIPITEC)》, Vol. 7. 2016.

    [↑](#footnote-ref-10)
11. ### Metadata，在國內，常被翻譯為：元數據、元資料、詮釋資料、中介資料、中繼資料、超資料、後設資料」、資料定義、資料包。

    [↑](#footnote-ref-11)
12. ### Bart van der Sloot & Sascha van Schendel. 〈Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study〉. 《Journal of Intellectual Property, Information Technology and E-Commerce Law (JIPITEC)》, Vol. 7. 2016.

    [↑](#footnote-ref-12)
13. ### 許春金、陳玉書，《犯罪預防與犯罪分析》（台北：三民，2013），頁7-11。

    [↑](#footnote-ref-13)
14. ### 如第三級之犯罪預防理論，主要則是刑事司法體系內之逮捕、審判、監禁、處遇措施及教化輔導等作為。詳參：許春金、陳玉書，《犯罪預防與犯罪分析》（台北：三民，2013），頁8。

    [↑](#footnote-ref-14)
15. ### 許福生，《犯罪學與犯罪預防》（台北：元照，2016），頁225。

    [↑](#footnote-ref-15)
16. ### 許春金、陳玉書，《犯罪預防與犯罪分析》（台北：三民，2013）。

    ### 許福生，《犯罪學與犯罪預防》（台北：元照，2016）。

    ### 孟維德、黃翠紋(2012)，《警察與犯罪預防》，(台北：五南)。

    [↑](#footnote-ref-16)
17. ### 亞太經濟合作組織(APEC)於2004年訂定APEC隱私權保護原則，作為各會員國有關個人資料保護的最高指導原則，臺灣地區亦參照其9大原則規定修訂個人資料保護法，包括：1.預防損害原則；2.告知原則；3.限制蒐集原則；4.利用個人資料原則；5.當事人自主原則；6.個人資料完整原則；7.安全維護原則；8.當事人查詢及更正原則；9.責任原則。

    [↑](#footnote-ref-17)
18. ### 參考個人資料保護法之總說明及部分條文修正說明，〈<https://www.moj.gov.tw/lp.asp?CtNode=28007&CtUnit=805&BaseDSD=7&mp=001>〉。

    [↑](#footnote-ref-18)
19. ### 劉佐國，李世德，《個人資料保護法釋義與實務—第二版—如何面臨個資保護的新時代》，（台北：碁峰，2015）。

    [↑](#footnote-ref-19)
20. ### 周漢華，《個人信息保護法（專家建議稿）及立法研究報告》，（北京：法律，2006）。

    [↑](#footnote-ref-20)
21. ### 〈十二屆人大常委會：個人信息怎麼保護〉，《華律網》，2016年10月31日，〈<http://www.66law.cn/laws/159822.aspx>〉。

    [↑](#footnote-ref-21)
22. ### 〈網絡安全法的立法定位、立法框架和制度設計〉，《大陸地區網信網》，2016年11月10日，〈<http://www.npc.gov.cn/npc/lfzt/rlyw/2016-11/21/content_2002310.htm>〉。

    [↑](#footnote-ref-22)
23. ### 賴錦宏，〈網路安全法，大陸明天上路〉，《聯合報》，2017年5月31日，版A8。

    [↑](#footnote-ref-23)
24. ### 參考：柯雨瑞、蔡政杰，〈從犯罪預防觀點探討兩岸跨境網路犯罪之治理〉，《全球化下之國境執法》，（台北：五南，2016），頁33-62。

    [↑](#footnote-ref-24)
25. ### 宣律師，《圖解式法典：憲法及相關法規》(台北：高點，2016)，頁50-56。

    [↑](#footnote-ref-25)
26. ### 郭桓甫，《兩岸人格權之比較研究－以個人資料保護為中心》，（嘉義：國立中正大學財經法律學研所碩士學位論文，2015年），頁1-141。

    [↑](#footnote-ref-26)
27. ### Public Safety Canada, 《Bi-National Assessment on Trafficking in Persons 》, 2011, 《Public Safety Canada》,[https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-ssssmnt-trffckng-prsns/index-en.asp](https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-ssssmnt-trffckng-prsns/index-en.aspx)x.

    [↑](#footnote-ref-27)
28. ### 孟維德，《跨國犯罪》(台北：五南，2015年)，頁397-434。

    [↑](#footnote-ref-28)
29. ### 孟維德，《跨國犯罪》(台北：五南，2015年)，頁397-434。

    [↑](#footnote-ref-29)
30. ### 陳惟凡、陳振楠、伍台國，〈電子商務平臺之安全風險評估模式：植基於ISO27001資訊安全管理系統與個人資料保護法〉，《電腦稽核》，第34期，2016年8月，頁28-42。

    [↑](#footnote-ref-30)
31. ### 涉及「個人資料保護法」之法規範內容，尚有待精進之部分，尚可參閱以下之相關論文大作：

    ### 李進建，〈論大數據於犯罪偵查之挑戰與因應〉，《全國律師》，2015年12月，頁60-70。

    ### 邱琳雅，〈德國聯邦個人資料保護法（BDSG）〉，《金融聯合徵信雙月刊》，第8期， 2008年10月，頁60-64。

    ### 洪文玲，〈行政調查制度之研究〉，《內政部警政署警察法學》，第4期，2005。

    ### 梁添盛，〈論警察權限之強制手段與任意手段〉，《中央警察大學學報》，48 期，2011，頁223〜260。

    ### 詹鎮榮，〈公務機關間個人資料之傳遞－以臺灣桃園地方法院行政訴訟102年度簡字第2號判決出發〉，《法學叢刊》，第60卷第一期，2015年1月，頁1-25。

    ### 蘇柏毓，〈104年之個人資料保護法修正簡評〉，《科技法律透析》，第28卷第4期，2016年4月，頁13-17。

    ### 郭桓甫，《兩岸人格權之比較研究－以個人資料保護為中心》，（嘉義：國立中正大學財經法律學研究所碩士學位論文，2015年），頁1-141。

    [↑](#footnote-ref-31)
32. ### 詹鎮榮，〈公務機關間個人資料之傳遞－以臺灣桃園地方法院行政訴訟102年度簡字第2號判決出發〉，《法學叢刊》，第60卷第一期，2015年1月，頁1-25。

    [↑](#footnote-ref-32)
33. ### 郭桓甫，《兩岸人格權之比較研究－以個人資料保護為中心》，（嘉義：國立中正大學財經法律學研所碩士學位論文，2015年），頁1-141。

    [↑](#footnote-ref-33)
34. ### 朱昌俊(2016)，〈網路安全法不能取代個人信息保護法〉，2016年11月09日，〈<http://webcache.googleusercontent.com/search?q=cache:gNer_oileoQJ:http://ep.ycwb.com/epaper/ycwb/html/2016-11/09/content_186075.htm%2B%E7%B6%B2%E7%B5%A1%E5%AE%89%E5%85%A8%E6%B3%95++%E5%80%8B%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E8%AD%B7%E6%B3%95&hl=zh-TW&gbv=2&ct=clnk>〉。

    [↑](#footnote-ref-34)