第一章　緒論

第一節　研究動機

在繁忙的一天中，都有大量的資產或資料，透過電腦網路來傳輸、處理並儲存。美國的金融產業，每天透過電腦網路，處理總值達數兆美元的商業交易。新的工業產品設計資訊、藥品、保險內容、科技研究新知、社會政策、政府立法及國防安全的資訊，這些原來存放在檔案櫃中，或是辦公桌上的書面資料，現在通通可讓人透過電腦網路來取得。高速計算能力的發展，提昇了處理日常商務、娛樂或新媒體的執行效率。有些人甚至預測我們即將可透過網路來投票；各行政機關也都架設網站並提供公開的電子信箱，建立和人民溝通的管道。在本世紀末，高度開發社會中的每個人，可能會擁有數以百計的網路電腦。這些電腦應用在家庭、電話、電視、辦公室或汽車中。這些電腦會互相溝通，減少資源浪費，並提高日常生活的方便性。智慧型房屋和車子，可藉由使用狀況，行程表和當時狀況作適度調整。無論身處何處，都可立刻呼叫這些電腦，查詢並更改它的設定。這種能力可節省資源浪費，並提高生活品質。工業界、學術界和政府也會受到新科技的衝擊。

但這個新的遠景，有它的黑暗面存在。多半已成為傳統犯罪形式的工具，例如竊盜、詐欺、毀損、勒索、間諜等的利用工具。此外，也產生新的，會破壞電腦或是網路的犯罪形式，例如電腦病毒。現在還沒有有效的方法來阻止這些犯罪；使用網路資源的人，會忽略掉網路安全的需求，管理階層的人員，則對於這所帶來的風險認識不清，不願意投入

資金。實際上，對於網路安全認知的訓練不足，錯誤的程式，及不恰當的軟體工程解決方案，都會造成安裝好的網路安全防護機制，出現漏洞。我們對於傳統的檔案系統的防護措施的研發，都累積了數十年乃至於數個世紀的經驗。雖然防護的方法有缺點，但是會面臨到的風險或破壞，確是可以預知的。

自從網路活動普及以來，網路社會應該受到何種程度與型態的規範，一直是廣受討論之問題。到底網路世界的規範應如何建構，方屬完整，當網路世界隨著科技的日新月亦逐漸擴張其規模時，網路世界裡是否有所謂的「網路法律」（The law of Cyberspace）可言，抑或所謂網路裡的法律或規範，仍屬一片渾沌，充其量只是一個模糊不清的觀念，從網路過去發展至今的經驗顯示，網路活動者在網路世界裡經營其網路生活時，往往將自己在現實生活裡所累積的法律經驗帶入其中。事實上，當我們在經營網路生活的同時，也同時生活在現實生活世界裡，從這個觀點來思考網路世界與現實世界的規範交錯問題，當然很難想像現實世界裡的法律制度會與經營網路生活的我們毫不相關。所以當網路活動形成爭議時，我們往往還是得訴諸現實世界的法律制度，作為解決網路爭議的依據。所以這是立法機關必須立法管理和控制的新領域，因為未來或現在多半的犯罪行為，都會在這個領域發生。偵辦人員應該了解新的犯罪手法，使用不同的偵辦方法，以及有哪些法律規定可以防制犯罪。偵辦人員應熟悉電腦犯罪的偵辦。他們的偵辦範圍，不應僅限於如何維護社會資源和利益，也應維護人民的自由和隱私權。隨著全球網路的興起，過去只出現在科幻小說中的劇情，已經蔓延到每個人的日常生活；從在網路上散佈誹謗的文字，到侵入銀行主機盜取信用卡資料，甚至政治貪污、經濟迫害、隱私權侵害、恐怖主義等通通都可以透過電腦網路

進行。對傳統的罪犯而言，網路是一項強大的犯罪工具，此類犯罪所之牽涉實際技術面日新月異，更是現行法律所必須面對的挑戰，此為本文研究動機之來源。

第二節　研究目的

綜覽人類之歷史，尖端技術或科技，必然會成為想要推翻這些技術、或是利用它達成私人目的之人，攻擊或利用的目標。以往亡命之徒會攜槍騎馬進入城鎮，搶劫當地的銀行，但自從電話出現以後，就可以使用電話計畫或執行犯罪（例如敲詐或者綁匪約定交付贖款地點的聯絡工具）。電話竊聽的裝置，可以成為偵防犯罪的工具，但也可成為罪犯監控被害人的電話工具。到了電腦時代，無論好人或壞人都會利用新的技術。許多電腦罪犯都是電腦專家。他們監控網路交通，並伺機竊取信用卡號碼，並利用違法資金轉帳、付費的方式，來竊取他人所得。

新的技術研發，造成新型的犯罪活動；對抗新型犯罪，必須要使用不同的防衛措施，並修訂現行法律以規範此類新型犯罪。技術、犯罪方式及法律之修訂，就有如跳蛙遊戲：技術的進步，可用來建設更好的工具，可以用來犯更嚴重的罪，亦可發展出更有效的犯罪防治方法，同時也必須有新的法律來規範此類新興的活動。

本文主要在就目前網際網路上發生之脫序行為檢視其性特及內涵，若其已侵害刑法保護之法益時，現行法律之規定能否加以規範，以達刑法之預防功能。

第三節　研究範圍與方法

網際網路挾其迅速便捷及無遠弗屆之特性，除了使我們的生活變得更便捷以外，不可諱言的，也產生了新的問題與困擾，網路犯罪即其中之一端。電腦犯罪自從一九八〇年代即時有所聞，而自從網際網路普及後，藉由網路犯罪之技巧、數量、層次以及手法都相繼翻新。相對於國外網路犯罪問題的出現，我國亦因政府大力推動資訊建設，使得網路日益普及，從而亦產生不少的網路犯罪問題，尤其近來色情網站、軍火教父、網路炸彈客、駭客入侵等翻新的犯罪手法相繼出現之後，更引發了社會大眾及政府相關單位對網路犯罪與管理問題的重視。就目前網路的發展與利用而言，網際網路之特性與單純之電腦利用行為迥異，似應將此種行為加以定義為利用網際網路之特性為犯罪手段或犯罪工具之網路濫用行為。惟電腦之運用與網際網路之間已緊密結合在一起，電腦犯罪顯然是屬較高層次之概念。本文擬就刑法及特別刑法之相關規定，對於目前網路上之所產生之犯罪類型加以探討，並瞭解現行法律之規範是否必須因應網際網路之特性所產生之新興犯罪而做立法或修法調整，並參考外國之立法例及實務運作之見解，試就相關之問題提出解決之道。

本文主要可區分為第一章之緒論，第二章電腦犯罪與網路犯罪之概念，第三章一般類型網路犯罪，第四章專業類型網路犯罪，第五章其他類型網路犯罪，第六章網際網路連線服務提供者就網路違法內容之法律責任，第七章結論與建議。

其中第二章先敘述電腦犯罪與網路犯罪之概念，包括電腦犯罪之定義，各國立法概況，與傳統犯罪之不同，網路犯罪之意義，起源，發展

及其特質。第三章一般類型網路犯罪及其刑事責任，包括網路色情，發表不當言論，網路詐欺，煽惑他人犯罪，網路賭博，網路上販賣大補帖。第四章專業類型網路犯罪及其刑事責任，電腦系統進入的概念，未經授權侵入電腦系統，電磁紀錄之不法使用及消除，竄改他人資料之行為，利用網路散佈電腦病毒，包括電腦病毒之意義及成因，散佈電腦病毒之刑事責任。第五章其他類型網路犯罪及其刑事責任，述及非法重製電腦程式或檔案，網址名稱及商標之侵害，網上冒名刷卡，大量商業性電子郵件使用問題，網路不實廣告，有關 MP3 著作權之刑事責任。第六章網際網路連線服務提供者就網路違法內容之法律責任，述及網路違法內容與網際網路連線服務提供者之關連與問題，網際網路連線服務提供者之定義，ISP 對網路違法內容的法律責任，發現違法內容時之權利與義務。第七章為本文之結論與建議，乃將各種不法使用網際網路行為人之刑事責任作整合，並提出刑事立法與執行之建議，針對網路犯罪給予事前的防制與事後之懲罰。

第二章　網路犯罪之概念

由於網際網路之使用必須透過電腦，因此電腦之使用與網際網路之間已緊密結合在一起，網路犯罪亦可包括在電腦犯罪之中，但電腦犯罪顯然是屬於較高層次之概念，在討論網路犯罪之前需先就電腦犯罪之意義作界定，方能瞭解電腦犯罪與網路犯罪間各別之範圍及相互關係。

第一節　電腦犯罪定義

一般而言，造成電腦系統容易受到威脅致釀成極大損害之因素不外：資料被錯誤的輸入、不誠實的受雇人、對公司有成見之受雇人、無法控制之行為或事件、恐怖份子或反對者之破壞行為及自然災害如火災、水災等。由這些因素觀之，電腦犯罪之主要目標是電腦資料及程式，而不是電腦硬體本身。所謂的電腦犯罪實乃藉電腦以遂其犯罪目的（crime by computer）之人的犯罪行為[1]，不一而足。所使用之名稱雖

[1] 參閱羅明通、林志峰、李蒨蔚、洪榮彬、陳麗玲合著，電腦法（下），民國 83 年，頁 370。有關電腦犯罪之定義、所使用名詞及其範疇，學者間容有不同意見，所使用之名稱亦至為分歧，有謂電腦濫用（computer abuse），有謂與電腦相關之犯罪（computer-related crime）、藉電腦協助之犯罪（computer-assisted crime）、電腦詐欺（computer fraud）、電子詐欺（electronic fraud）、自動處理資料犯罪（automatic data processing crime）、電腦入侵（hacking），或者電腦玩家（hacker）及電子資料處理犯罪（electronic data processing crime）等。

不盡相同，惟其所指之內容只有廣狹之分並無實質之差異。首先，探討電腦在該類犯罪行為中所擔任的角色為何，將有助於其定義之界定：

一、電腦為犯罪之目標（objects）

將電腦硬體本身週邊設備或其儲存之資料作為犯罪者攻擊的對象是最普遍的方式。其行為之類別有電腦有電腦本體設備之破壞、儲存資料、程式或得以影響電腦功能之支援、輔助設施的破壞。

二、電腦作為犯罪之主體（subjects）

以電腦作為犯罪地或環境（如侵害隱私權），製造獨特形式之資產如電子貨幣（electrical money）的詐欺以遂其犯罪之目的。

三、電腦作為犯罪之工具（instruments）

某些類型的電腦犯罪內容十分複雜而須輔以電腦為手段或工具以完成犯罪，此時電腦可以扮演主動的角色，例如以自動掃描電話密碼的方式去使用未經許可的電話系統；或擔負被動的角色，偽造一項繼續性侵佔行為的一般分類帳（general ledger）。

四、電腦為掩飾犯罪的象徵（symbols）

電腦可能被用來作為詐欺或恐嚇的掩飾。即以電腦為護身符，利用其偵查及追蹤不易之特點來掩飾行為人之犯行。例如電腦未有錯誤而詐稱電腦有錯誤，以達其詐取或掩飾之目的。

但目前多將之稱為「電腦犯罪」，惟依傳統犯罪理論犯罪主體原限於自然人，然在電腦犯罪之情形，電腦並非自然人，其雖有運算、邏輯等功能，但若無自然人之操作則無法發揮功能，故犯罪之主體係自然人，而非電腦，稱電腦犯罪即有可議之處。且使用電腦犯罪之人，其目標通常是儲存於電腦內之資料（data）或程式（program），故稱電腦犯罪亦有不當。惟此名詞為一般所通用，且由字義即可了解此犯罪之特性，通

俗易懂，一般人亦可望文生義，故本文襲用之。

電腦犯罪之定義，依學者對電腦犯罪用語之不同，可區分為廣義、狹義及折衷三種不同見解，分述如下。

第一項　廣義的電腦犯罪

依美國聯邦調查局對腦犯罪之廣義見解，認為與電腦有關之犯罪（computer-related crime），及凡以電腦為犯罪工具或犯罪目的之所有犯罪皆屬之，其犯罪型態有電腦濫用（computer abuse）、與電腦相關之犯罪（computer-related crime）、藉電腦協助之犯罪（computer-assisted crime）、電腦犯罪及電腦詐欺（computer fraud）等[2]。持廣義見解者，認為電腦犯罪乃指「與電腦有關之犯罪」，乃泛指所有與電腦科技或電腦系統有關的犯罪，或泛指所有與電子資料處理有關之犯罪，申言之，即凡以電腦為犯罪工具，或以電腦為犯罪目的之所有犯罪行為，均屬電腦犯罪，由此定義下之電腦犯罪，不論主觀上或客觀上均牽涉到電腦，因此，許多屬於傳統之犯罪類型者（如竊盜、詐欺），將會因為電腦之介入，即被視為「電腦犯罪」，其範圍似嫌過大[3]，易導

---

[2] 參閱房阿生、吳振村著，電腦犯罪及防治方法之研究，司法週刊社印行，民國 78 年 9 月，頁 4，10。

[3] 例如位於新竹科學工業園區之宏碁電腦公司，於民國 73 年 3 月 18 日失竊十六位元電腦之積體電路（integrated circuit，簡稱 IC）七十餘萬片一案，此為單純之竊盜案，若依廣義說之見解，因所失竊之物與電腦有關，即應被視為電腦犯罪，其不當之

致無法正確估計電腦犯罪數字。

第二項　狹義的電腦犯罪

狹義見解者認為，所謂電腦犯罪乃指與電子資料處理有關之故意而違法之財產破壞行為，換言之，凡以故意竄改、毀損、無權取得或無權利用電腦資料、程式或電腦設備之違法破壞財產法益之「財產罪」，始屬電腦犯罪。亦即除犯罪之主觀構成要件外，客觀行為尚須為利用電腦或相關知識之行為，且犯罪客體需為侵害財產法益之犯罪，始能稱之。此說將電腦犯罪僅界定為財產犯罪，則又使電腦犯罪之定義，顯得過於狹隘，因為電腦犯罪之領域中，除有破壞財產法益之財產罪外，尚有如破壞電腦祕密的電腦間諜罪（computer espionage），此並非破壞財產法益，故僅將電腦犯罪界定為財產罪，亦屬不當。

第三項　折衷式的電腦犯罪

依廣義說採「與電腦有關之犯罪」（computer-related crime）之定義過於浮濫，而狹義說又無法遏止並無任何財產損失而出於故意而濫用電腦之行為人，兩者均不能符合目前科技迅速發展的社會需求。故有學者對此二說加以修正，認為：犯罪行為與電腦之操作或處理作業過程有相當程度之關聯，或係因科技之發展而產生之新型犯罪，如侵害軟體

處顯而易見。見聯合報 73 年 3 月 20 日第三版報導。

或程式等行為，方構成電腦犯罪，較能符合電腦犯罪之定義，且不致於有漏網之魚。

此說之定義又有以下不同之見解：

一、所謂電腦犯罪係指行為人濫用電腦或破壞電腦而違犯具有電腦特質之犯罪行為。

二、所謂電腦犯罪乃指以電腦為工具，而使自己獲益或使他人遭受損失之犯罪行為。而所謂以電腦為工具，係指以電腦本身為犯罪對象，或利用電腦作為犯罪工具而言。

三、所謂電腦犯罪係指以下列之目的故意接近電腦系統或電腦網路者：（一）以詐欺或奪取之目的而執行程式，（二）以陷他人於錯誤或詐欺之目的而獲取金錢、財產或服務，或（三）任何人惡意接近、改變、增減、損壞電腦系統、電腦網路或資料者均為電腦犯罪。

另外，在國際組織方面之見解，如國際經濟合作開發組織（Organization for Economic Cooperation and Development OECD），於一九八三年五月組織一特別委員會（ad hoc），延聘專家學者討論電腦犯罪有關問題，而將電腦犯罪或電腦有關之犯罪定義為：「關於自動化資料處理與（或）資料傳輸中任何非法、不道德或越權之行為」（any illegal, unethical, or unauthorized behavior involving automatic data-processing and/or transmission of data ），以作為 OECD 對各會員國之立法建議[4]。

---

[4] 參閱楊富強著，電腦犯罪之立法與電腦安全，法學叢刊，第 134 期，民國 78 年 4 月，頁 126。

第四項　小結

因為就電腦犯罪之特質以觀，對於電腦系統之破壞行為，在電腦依存性越高的社會中，可能不只造成財產法益的破壞，而是在鉅額財產損失之外，尚造成非財產法益之損害，例如危害政府機關的運作、侵害個人隱私等；因此電腦犯罪應包括財產犯罪與非財產犯罪，故折衷說之見解除兼顧財產與其他法益之保障外，同時在適用上較富彈性，較之廣義說與狹義說見解已無前述廣義說範圍過大之弊，復不限於財產之犯罪始有其適用，亦無狹義說之偏，實較可採。惟因科技發展之迅速，資訊流通已隨著網路之國際連線更趨快速與便捷，為因應現今資訊之發展狀況，應將電腦犯定義稍作修正為「電腦犯罪指行為人濫用電腦、利用混淆或破壞電腦及網路之行為，致使電腦及網路無法發揮正常功能者[5]」較為妥當與適切。

第二節　網路犯罪

近來由於網路上的脫序行為不斷發生，逐漸引起社會大眾對於網路問題的重視，因此，在報章雜誌及新聞媒體上即出現所謂網路犯罪一詞，而網路上之所以產生種種問題，乃肇因於政府大力推動網際網路的普及，所以網際網路已成為現代人生活中資訊流通的重要工具及來源，在討論網路犯罪之前，必須先瞭解網際網路之起源、意義及特質，才能認

[5] 參閱羅明通、林志峰、李蒨蔚、洪榮彬、陳麗玲合著前揭書，頁 373。

識藉由網際網路作為媒介及工具而為犯罪行為之網路犯罪，以下本文先就網際網路之起源、意義及特質予以說明。

第一項　網際網路之意義

目前各行各業各領域都正熱烈地談論一個熱門的話題，那就是網際網路(Internet)，到底什麼是網際網路(Internet)呢？首先，讓我們先瞭解與 Internet 關係密切的一個名詞--「電腦網路」。將兩部以上的電腦串接在一起，就形成所謂的「電腦網路」；電腦網路的連線範圍可大可小，如只限在某一個辦公室或辦公大樓內部的網路，我們稱之為「區域網路」(LAN，Local Area Network)；另外有的電腦網路連線範圍相當大，可以橫跨不同的城鎮、國家，甚至不同洲，我們稱之為「廣域網路」(WAN，Wide Area Network)。Internet 就是由全球數萬個這種大大小小的電腦網路所組成的網路，其上連接有超過成千上萬部的電腦，包括無數政府機關、企業、學術機構與個人用戶。原本儲存在個別電腦中的各類資料，經過 Internet 傳送，可以讓使用者跨越空間的距離，交換有用的資訊。

在電腦資訊的世界中，所謂區域網路（Local Area Network）由前述可知係指企業或學校內部由個人電腦所連結組成的資料傳輸系統，藉由區域網路之連結，企業或學校可透過內部之個人電腦互相傳輸資料，

但區域網路與區域網路之間，即各企業之間或各學校之間如欲透過網路相互連結，則往往因為各區域網路之間使用之硬體、軟體可能都不相同而導致無法連結，為解決此問題，遂經由制定 TCP/IP（Transmission Control protocol/Internet Protocol）通訊協定，採取相同之標準，以便將全世界的各區域網路透過電話線或光纖互相連結成一個大型網路，即一般所稱之「網際網路」（INTERNET）。

雖然每個使用者都可以透過不同的管道進入網路世界中，但一般而言，進入網路世界的管道通常有兩種方式，第一種是使用者藉由自己之個人電腦及連線設備[6]，經由撥接帳號與網路連線服務者提供者（Internet Service Provider，簡稱 ISP）連結之後，而與網際網路連結；第二種方式則是透過學校、企業或網路咖啡廳[7]之網路主機（network host）與網際網路相連結。進入網際網路後，便可經由各種方式取得各式各樣所需之資訊，目前最常使用的方式大致上有全球資訊網（World Wide Web，簡稱 WWW）、電子佈告欄（Bulletin Board Service，簡稱 BBS）、電子郵件（E-Mail）、新聞群組（Newsgroup）以及聊天室（Chat Room）等方式，透過上述之方式所傳輸之資訊內容多為文字、圖畫、音樂甚至動畫及影像，因此隨著網路科技的日益發展，藉由網路傳送資訊

---

[6] 所謂連線設備包括軟體及硬體部份，以目前多數個人使用者之使用方式而言，硬體部份是數據機（MODEN 俗稱魔電），軟體部份則是電腦中的撥接軟體、瀏覽軟體與一個電話號碼。其連接方式是利用撥接軟體透過數據機、電話號碼撥號與 ISP 連結。

[7] 所謂網路咖啡廳，係指咖啡廳內提供已連結網際網路之電腦供客人上網，顧客除了可在店內享受咖啡等餐點服務之外，並可利用網際網路找尋所需之資訊或與外界溝通。

之模式，已產生了一個新興的傳播媒體，一個不同於傳統的傳播媒體，成為一個在現實世界中並無特定地理位置，但卻超越空間距離之限制而為全世界每個使用者都能達到的電子空間（Cyberspace）。

第二項　網際網路之起源及發展

如果蒸汽機的發明，是人類自農業時代進入工業時代之關鍵，那麼電腦之發明，毋寧是將人類自工商業社會帶往科技文明的先鋒；如果飛機之發明，使兩地之間縮短了距離，那麼網際網路技術的開展則使世界變成無距離。

網路是由一九六〇年代後期的分封交換網路揭開序幕，當時美國國防部發展的一項 ARPANET（Advanced Research Projects Agency Network）的軍事計畫即是目前 Internet 的前身。該計畫乃在於使所有在美國各地之電腦，能讓美國科學家及研究人員分享資料，共享軟硬體設備，並使政府在核子戰爭爆發時，網路之某部份遭到破壞之情況下，所有其他電腦仍能維持連線之正常運作。到了一九八〇年代，ARPANET 正式分裂成兩個網路；其一僅供國防部使用，另一則是供與政府單位簽約的研究單位使用，後者透過美國國家基金會（NSF）輔助其電腦技術，並積極研究發展，將其原本採用的 NCP 協定改由 TCP/IP（Transmission Control protocol/Internet Protocol）所取代，成為其通訊協定的標準，自此 NSFNET 亦開始提供業界使用，並收取費用，直到一九九〇年 NSFNET 正式取代 ARPANET 成為 Internet 的骨幹，從而 Internet 即蓬勃發展至今。

網際網路在早期由美國 ARPANET 發展之後，並非立即成為世界各國通用之網際網路，而是隨著電腦科技發展逐漸演進，直至一九九三年二月美國總統柯林頓組成資訊建設特別委員會（Information Infrastructure Task Force，簡稱 IITF）提出國家資訊基礎建設（National Information Infrastructure，簡稱 NII）之構想後，便在全世界形成一股 NII 的熱潮，我國隨之在一九九四年七月成立國家資訊建設委員會並提出國家資訊基礎建設之政策，著手推動網路普及，且在網際網路相關電腦硬體及軟體之功能大幅提昇與普及化的配合之下，使得網際網路成為已經成為新興之傳播媒體。Internet 近年來的蓬勃發展若以「爆炸」性的發展形容並不為過，一九九三年一月時全球連接上 Internet 的主機數為一百三十一萬台，三年後，即一九九六年一月仍僅有九百四十七萬台，至一九九七年一月已增加至一千六百萬台。此一數據反映出 Internet 的確有著不可忽視的發展潛能。不過電腦本身在目前並非如電視機一般的普及於每個家庭，網際網路的使用，事實上在目前更是不容易達成全面性的使用，但在可預見之未來，在電腦硬體設備、價格及軟體之使用設計日趨人性化等各方面客觀條件改善之情況下，或許電腦及網際網路未來將成為家庭必備的家電用品之一。甚至有專家預估，在西元二千年，Internet 的用戶將達到十億人次，它將會成為家庭的資訊公共設施（Information Utility）就像水、電一樣。

網路其迅速便捷及無遠弗屆之特性，除了帶來人們意想不到的便捷生活以外，不可諱言的，也帶來一些新的問題與困擾，網路犯罪即其中之一端。電腦犯罪自從一九八〇年代即時有所聞，而自從網路普及，網路犯罪之技巧、數量、層次以及手法都相繼翻新。相對於國外網路犯罪問題的出現，我國亦因網路的逐漸普及，產生不少的網路犯罪問題，尤

其近來色情網站、軍火教父、網路炸彈客、駭客入侵等翻新的犯罪手法相繼出現之後，更引發了大眾及政府相關單位對網路犯罪與管理問題的重視，甚至有成立「科技警察」或「網路警察」以抗網路犯罪之呼籲，網路犯罪儼然已成為目前最熱門的話題之一。

第三項　網路犯罪之意義

近來在報章媒體上時常可見「網路犯罪」（Cybercrime）一詞，然而究竟網路犯罪所指為何，國內尚無學者對此加以定義，縱有討論網路犯罪之論述亦多將其認為仍屬電腦犯罪之一環，電腦犯罪中的電腦網路類型即為網路犯罪。然亦有論者認為就目前網路的發展與利用而言，網際網路之特性與單純之電腦利用行為迥異，應將此種行為加以定義為利用網際網路之特性為犯罪手段或犯罪工具之網路濫用行為[8]。惟本文以為雖然目前電腦之運用與網際網路之間已緊密結合在一起，但電腦犯罪顯然是屬較高層次之概念，應有將網路犯罪自電腦犯罪中獨立出來之必要。所謂的「網路犯罪」應為以網路為犯罪場所的電腦犯罪行為，歸屬於電腦犯罪中電腦網路類的犯罪型態，本文擬將其定義為「利用網際網路提供的服務型態而從事刑事不法的犯罪行為。」如利用網際網路為場所，傳遞、散布不實或不妥言論、圖片甚或進行恐嚇，或成立站台進行簽賭等交易行為。

---

[8] 馮震宇、劉志豪著，我國網路犯罪類型及案例探討，月旦法雜誌，第 41 期，民國 87 年 10 月，頁 84。

網路上的違法行為接連發生，使得網路又黑又黃--黃的，從招徠會員販賣色情圖片到成立網友國外買春團；黑的，從黑槍軍火販售到教人製做炸彈。而黃黑以外，還有網路老鼠會及網路不實廣告等詐欺行為。這林林總總的網路犯罪態樣，不但使檢調單位傷透腦筋，也使家長憂心忡忡--擔心孩子上網看了不該看的受到不良影響，也擔心孩子誤觸法網仍不自知。

當上述種種脫序行為藉由網路呈現出來，再經由媒體廣泛報導後，網路成了犯罪淵藪、違法樂園的印象也在一般大眾的心中渲染開來。民眾不僅要求追緝網路犯罪，而主張另立新法管制網路內容者更大有人在。究竟網路上的犯罪目前有無法律可管？我國目前有無必要再立新法來管制網路內容、維持網路秩序？本文將針對目前網路上呈現的犯罪態樣，在現行法律架構與體制下逐一解析其法律責任、偵查瓶頸與防治之道；同時介紹國際對網路內容管制的看法，並進一步探討如何透過法律管制層面以外的管理機制，達成資訊自由與網路秩序雙贏的局面。

第四項　網路犯罪之特質

第一款　隱匿性

網際網路之活動，固然是即時的、互動的，但另一方面卻也是不可知的、匿名的，因為任何人都能以代號、暱稱等暢行於網際網路之中，

而透過網路之連結，其能幾乎不受限制的隨時隨地上載或下載各種合法或非法資訊，而由於這種匿名性，使得資訊之流通更加暢行無阻。因此網際網路犯罪的特質之一，就是具有隱匿性，亦即行為人雖非電腦資料的有權使用者，或未經同意而使用他人電腦進行犯罪行為，或行為人隱匿其真實身分，而仍不易被察覺。此特性乃源於網際網路開放、分散且互通的架構特性，是故其資訊的流通性往往不受有形國家主權或疆域的限制，也因而產生所謂「網路無國界」的特性，使得網路犯罪的偵查與防治顯得相對的困難，因為網路犯罪已經不受時間及空間距離之限制，與傳統犯罪相較已不可同日而語。經由網路相互通聯之結果，聰明的犯罪者只要使用匿名、代號或冒用他人之名義使用其帳號，或是利用境外提供匿名轉信的網站傳送資訊，檢調機關便難以偵查或追蹤其具體的犯罪事證。因為雖能追查出是從哪一台電腦作出違法之行為，但並不表示電腦之所有人就一定是行為人。例如學校之電算中心、網路咖啡廳…等公眾得任意使用的電腦設備即為此「隱匿性」犯罪之最佳場所。

第二款　技術性

電腦係高科技的產品，欲藉其從事不法行為，必須具備一些基本的電腦知識，而利用網際網路則必須具備較單純電腦使用更深入的知識，若是利用網路逃避電腦安全系統的稽核防護，更需要有高度的電腦知識方得為之，因此利用網路犯罪之手法實在具有高度之技術性；亦有學者

將之稱為「專業性」[9]。

第三款　擴延性

早期電腦犯罪主要之犯罪行為多為程式操縱、電腦間諜與電腦破壞等，此類行為通常須具有電腦之專業知識始能違犯，且其犯罪結果所造成之損害雖鉅，但並無擴延性。然而隨著電腦及網際網路之普遍應用，越來越多的人可以接觸電腦並且運用電腦。相對的，因為網際網路普遍化的結果，利用網路所觸犯之犯罪行為亦隨之普遍化，再加上網路不受地理空間之限制且具即時性之特質，往往導致一個網路犯罪行為迅速擴延至各地區，影響層面及地區均非傳統犯罪所能相比擬。例如近來之色情網站之問題，利用網路誹謗，以及軍火教父案等，均顯示出網路犯罪行為之擴延性。

第四款　偵查困難

根據 FBI 美國國家電腦犯罪特勤組（National Computer Crime Squad；NCCS）的估計，平均有百分之八十五至九十五的電腦網路入侵案件未被發現[10]。另一項調查統計更顯示，只有百分之一的電腦犯罪曾被

---

[9] 參閱林山田著，電腦犯罪之研究，政大法學論叢，第三十期，民國七十三年十二月，頁 52。

[10] 參閱沈文智著，INTERNET 網路安全手冊，民國 86 年，頁 2。

偵查過。網路犯罪之發現不易、偵查困難之原因在於犯罪者多以匿名且結果發生時，可能已無從追蹤；再者檢調人員之電腦或網路專業知識不足，無法即時採取有效方法展開追蹤調查，甚至須仰賴專業人員方得進行之。

第五款　犯罪客體多樣化

網路犯罪的另一個特色，就是犯罪態樣繁多；有針對電腦軟體之入侵或損壞者，如入侵電腦竄改資料，散播電腦病毒等類型；有利用網際網路所提供之服務特性而犯者，如色情網站、利用電子郵件恐嚇或發表不當言論等。由於網路犯罪之態樣繁多，故其犯罪客體亦因此而多樣化，且不限於財產犯罪，此係一般犯罪所未有之特點之一。

第五項　網路犯罪之類型

網路犯罪主要係指透過網際網路提供的服務型態而從事非法的犯罪行為，如全球資訊網(WWW)、遠端登入(TELNET)、檔案傳輸(FTP)、電子郵件(E-MAIL)、電子佈告欄(BBS)、新聞討論群組(NEWS)或線上即時交談(如 IRC 或 ICQ)均可能為犯罪者所利用。網路犯罪基本上可區分成三部分，第一部分為「一般類型的網路犯罪」種類如下：網路色情、網路恐嚇、網路誹謗、網路約會強暴、網路婚外情、網路銷贓、網路黑店、網路金光黨、網路賭博及網路妨害名譽與偽造文書等；第二部分為「專業類型之網路犯罪」，其種類如下：著作權及隱私權的權利侵犯；第三部

份則為「其他類型的網路犯罪」亦即新興的犯罪類型，其種類如下：網路蟑螂、電腦駭客、癱瘓服務攻擊、非法重製電腦檔案及程式、利用網路散佈電腦病毒、網上冒名刷卡、網址名稱及商標權之侵害、大量商業性電子郵件之使用等。

第三節　網路犯罪與傳統犯罪之不同

造成網路犯罪日益嚴重的原因，主要因為現在是資訊時代，重要的資產都是逐漸以資訊表現出來，而資訊在處理、傳遞及儲存時，很容易遭到竄改、偽造、竊取、毀滅等不法行為的威脅，造成莫大的侵害與損失，但此新興的犯罪型態與傳統犯罪顯有不同，分述如下：

一、犯罪方法

在十幾年前，搶銀行是一件相當辛苦的工作，為了躲避銀行的監視器及偵查機關的查緝工作，除了手槍、安全帽、口罩、裝錢的袋子及交通工具外，仍需有接應的把風者，如今時代變了，修改電腦存款記錄或控制電腦，透過網際網路，在任何地方只須透過電話線及電腦，即可能突破系統漏洞及修改銀行電腦存款資料檔案，而達到犯罪的目的。這樣的犯罪手法目前雖未出現於國內，然美國的花旗銀行因遭駭客入侵並盜領四十萬美金存款，致前六大客戶撤資的事實，不得不讓國內的檢警調相關執法單位加快提昇偵查能力，以期遏阻此種修改電磁記錄，破壞電腦處理正確性的犯罪型態在國內持續發展擴大。除了傳統類型之犯罪如網路色情、網路賭博及網路詐欺等係利用網際網路為媒介或犯罪工具

外，尚有許多新興之犯罪類型出現，例如網路駭客入侵篡改、破壞電腦資料、電腦病毒之散布等為網路犯罪所獨有，犯罪手法多面而複雜，容後詳述。

二、犯罪時地

網路犯罪時間無晝夜之分，可以在一天二十四小時中的任何一個時間地點進行，且此類智力性的犯罪不易被發覺，又由於其具有電子作業之特性，犯案時間亦可短至以毫秒（millisecond）計，實與傳統的犯罪行為以時日為計算單位者不可同日而語。至於網路犯罪地點，幾乎無地理空間上之限制犯罪者只要利用電腦終端機（computer terminal）的鍵盤（keyboard）或電話（telephone）透過網際網路的連接就可以翻越圍牆、超越市界、省界甚至國界與該電腦連線或話機（online）之電腦系統進行犯罪，令人防不慎防。

三、犯罪手段

網路犯罪之手段除對電腦系統之軟體（software）進行破壞之外，另破壞通訊網路（communication networks）、資料（data）等亦均為犯罪手段。申言之，透過電腦處理、儲存之一切有形、無形資產，且可透過網際網路連結者，以及廣大看不見的被害人，均無一能倖免，皆有被網路犯罪侵害之可能。其犯罪之手段均係透過網際網路以和平方式即非暴力之手段為之，與傳統之暴力犯罪使用強暴、脅迫等手段有所不同。

第四節　網路犯罪之行為人

第一項　特徵

網路犯罪者，不若傳統的刑事犯，來自較低的社會階層，也不是其墮落的結果，亦非暴力型犯罪人，相反的，大部分的網路犯罪者皆處於受信任之地位，多具備現代高科技專業知識，而其亦不因性別而有差異。依目前各國的經濟情況而言，皆花費鉅額經費及投入眾多的專家從事傳統犯罪之研究，卻甚少致力於此類犯罪的研究，其結果誠如著名電腦犯罪學者 August Bequai 所認為將導致錯誤的引導，因為許多電腦相關的犯罪日漸細分且每天危害我們的社會；而此類與電腦相關之網路犯罪案件或未被發覺或偵查，縱然發現了，專家或警察等負責調查工作之人員沒有足夠的能力去了解更高明之犯罪，上述種種原因皆導致網路犯罪的研究日益困難。依據美國「司法統計局」（Bureau of Justice Statistics）就數百件電腦犯罪者案例歸納出下列典型電腦犯罪者之特徵[11]：

---

[11] 參閱電腦犯罪理論與實務問題研究，司法院研究年報第十八輯第十八篇，87 年 6

一、年齡：其年齡大約從十五歲至四十五歲之間。行為人之年齡普遍都很年輕，而且有很多人經常變換職業。此乃由於電腦有關之職業，係在短短數年間發展而成之新興行業，而從各行各業中吸收不少人才，故在與電腦有關之職業之從業人員中，就有為數不少之轉業者。

二、性別：許多此類犯罪者為男性，但女性犯罪者在此領域內已有逐漸增加之趨勢。

三、專業經驗：犯罪者之範圍從具有高度科技經驗至很少專業知識甚至無任何經驗者均有之。根據研究結果顯示[12]，此類型之犯罪有百分之三十七的行為人，擁有電腦特別知識。在百分之二十一的案件中，必須具有電腦之專業知識，始能違犯。約有百分之一的行為人對於企業之內部組織及其電腦之安全措施，有相當之了解。

四、犯罪者之背景：行為人通常不具有任何前科記錄，而屬於初犯或「機會犯」。

五、犯罪者之目標：包括個人、政府及商業機構。

六、個人特質：聰明、動機強且極願接受電腦的挑戰，通常為一令人滿意之受雇者及工作認真者，多為最後一位被懷疑者，許多設計電腦病毒之人，即為此類型之行為人。

七、角色：大多數的案例顯示此類犯罪者均單獨行動，但二個以上共犯之情形日益增加。

八、犯罪行為：至少在表面上，網路犯罪是一個社會形態（常軌）下的脫軌行為。

月，頁 22-23。

[12] 參閱林山田著，電腦犯罪之研究，政大法學論叢，30 期，73 年 12 月，頁 54。

九、安全系統：通常很鬆散或根本不具安全系統，許多企業之網路並未設置防火牆。

十、評價：與此犯罪者面談，許多人對於本身之行為皆認只是遊戲或惡作劇，而非犯罪。

第二項 動機

一般而言，網路犯罪者特性較為狡滑、欺瞞。其犯罪動機歸納而言之，有以下數種[13]：

一、獲得經濟利益（economic gain）：為增加個人的財產而竊取金錢、財產或盜用服務。

二、薄弱的安全措施（poor security）：企業本身的電腦系統安全措施薄弱，因此安全系統的鬆散就構成犯罪者侵害的目標。

三、玩遊戲（game playing）：許多資料處理的專家們均將電腦當作是一種玩具。

四、對機構的怨恨（hatred of the organization）：犯罪者可能為了掩飾錯失行為而對機構產生憎恨心理。

五、勞工關係（labor-relation）：勞資關係的不良引起受雇人直接侵害雇用者之角色。

六、經濟問題（economic problems）：犯罪者可能正陷於嚴重的經

[13] 參閱電腦犯罪理論與實務問題研究，司法院研究年報第十八輯第十八篇，87 年 6 月，頁 23-25。

濟困境。

七、自滿（ego）：對於電腦的挑戰及逃避偵查的挑戰。依據美國史丹福研究所之研究結果認為行為人之動機大多是出於好勝心與冒險心，開始之時，只是要嘗試其電腦知識有無辦法超越電腦系統之安全防護措施。

八、情感失調（emotional maladjustment）：心理疾病或不穩定都可能是犯罪因素。

九、意識形態（ideology）：政治極端份子及恐怖份子可能以電腦網路系統作為控制階層（ruling class）之工具，而加以攻擊。

十、政治因素：除為名、為財外，部分駭客組織也會提出激進的政治訴求。過去自稱「地下兵團」的駭客團體便以違反人權為由，宣稱將入侵摧毀中共和伊拉克電腦系統；「電子擾亂劇場」的駭客團體則以攻擊程式，試圖癱瘓墨西哥總統和五角大廈的網站，以聲援墨西哥反抗軍。另外像印度、巴基斯坦間的核爆爭議，南斯拉夫科索沃戰爭期間，也都發生過地下駭客組織入侵網站行為，試圖表達不同的政治立場。此外，對於外國機構電腦系統之攻擊可以破壞一國之政治、經濟穩定，而先前因為「兩國論」所演變之網路上的口水戰，兩岸駭客互相較勁。一九九九年八月八日首度開戰的是監察院、屏東縣政府、台大圖書館、營建署、NII 等單位網站的首頁被大陸駭客入侵。網頁被「世界只有一個中國、也只需要一個中國」為主題的相關聲明取代。台灣駭客不甘示弱亦開始「反攻」以類似手法入侵了大陸證券監督管理委員會、陝西科技網、中華人民共和國鐵道部等網站，修改首頁內容為支持兩國論相關言論。雙方你來我往文中甚至出現「解放」與「光復」等敏感字眼。

第三項　態樣

第一款　飛客(PHREAK)

所謂「飛客」(PHREAK) 是指利用電腦網路來盜用他人電話號碼，以進行搗蛋或犯罪的人。如凱文.米尼克利用以破解一般電話的手法侵入行動電話系統，以便能於任何地方用某一不特定的行動電話，並做為連上電腦網路的工具，藉此隱藏自己的真實位置。電話公司的交換機是具有特殊作業系統的電腦，它會提供撥接埠(DIAL-UP PORTS)做為遠端診斷及維護之用途，通常電話飛客及電腦犯罪組織成員會利用這些撥接埠，做為竄改交換機系統管道，藉此他們便能夠打免費電話或提供開放的聊天專線。

第二款　鬼客(CRACKER)、怪客、快客

「鬼客」(CRACKER)又稱怪客、快客是指蓄意破解他人的密碼或攔截傳輸中的網路資料，以從事惡作劇行為的人。鬼客最喜歡探索網路密碼的弱點，其方式約有二種，一種為遠端嘗試使用者名稱及密碼，此乃因早期如 TELNET 等服務並未管制單一使用者登入失敗的次數限制，使鬼客可利用遠端主機的背景程式(因所運用的系統資源大，且怕被真正的系統管理者中斷制止)以某種演算程序長時間地嘗試不同的使用者名稱，取得使用者名稱後，再以相同方式嘗試不同的使用者密碼，因所有的運算

均交由電腦處理，等待數小時或數天後，鬼客即可取得部份正確的進入方式。另一種方式為取得密碼檔(使用者名稱為明文)後，再利用網路上公開的 CRACK 程式，以暴力（BRUTE-FORCE）式和字典（DICTIONARY）式的攻擊侵害取得可能的密碼，此乃因 UNIX 密碼檔案的預設值是任何人均可讀取，且係以八位元組的雜湊函數運算，使得它更容易遭受"暴力字典強姦法"的攻擊(以英文+數字+亂碼方式可防止密碼被攻擊盜用)。

第三款　駭客(HACKER)、黑客、害客

「駭客」（HACKER）又稱黑客、害客，指的是外賊，機構外的行為人，蓄意以非法之方式，未經電腦主機所有人或系統管理者的同意而逕行進出電腦系統，並使用高超技術進行不法侵害的電腦玩家。因偵查所需的技術性較高，偵查也較困難。

第四款　惡客(ABUSER)

「惡客」(ABUSER)指的是內賊，是指因失業或埋怨而故意利用先前的權力破壞或刪改電腦電磁記錄的內部同仁。公私機關因經濟不景氣、員額裁減或其他原因實施裁員減薪時，電腦工作人員因失業或埋怨而故意破壞、刪除或更改電腦軟硬體設備、檔案或密碼。

第五款　小結

在技術上及實務上而言，目前國內並未發現飛客，可能與現今技術較成熟，且相關運用與知識國內研究者較少有關，又鬼客研發的 CRACK 程式，在網路上垂手可得，使得國內大學生對電腦駭客的入侵攻擊方式感興趣，他們也希望透過網路突破種種的系統安全保護措施，進而享受進入別人電腦主機「到此一遊」的樂趣，有的甚至會在入侵主機的網頁上留下「裸女」圖，以炫耀他的戰績，這樣的行事作風，也樹立起駭客的獨特性格。也許是許多國內外的電腦犯罪報導「神化」了部分的網路駭客(HACKER)，產生了成功駭客(即不被發現的入侵者)為虛擬網路世界之主(SUPERVISOR)-位高權重(ROOT)的假象，導致許多國內的大學生及系統管理者開始學習駭客技倆，探索網路系統的安全與漏洞，以成功侵入其他主機，破解密碼並不被發視為至高無上的榮耀。

第三章　一般類型之網路犯罪及其刑事責任

第一節　網路色情

現實世界所存在的社會問題都有可能是網路上之問題，尤其是色情問題更是猖獗，在網路發展的各式各樣的行業中，色情網站是最迅速發展的一個行業。目前我國網路上最受歡迎、最熱門的網站竟然是所謂的「成人網站」也就是一般人所稱的色情網站。根據一九九七年四月底交通大學思源基金會聚寶盆網路搜尋器所公佈的調查顯示，前一百大熱門網站中，排名前三十名內竟然有高達七成是所謂「成人網站」，且根據網路業者之概略估計，至八十六年九月底前至少有一百個以上之中文成人網站，色情網站之氾濫程度可以想見。由於色情行業可以說是網路上利潤最高的一個行業，所以在網路上出現的色情網站可以說是如雨後春筍般的冒出來。最近國內警方就破獲一宗高中生經營的的色情網站，成立才半年之久，獲利即已高達上百萬元。[14]

由於網路四通八達且無國界限制，想取得養眼的色情圖片簡直是易如反掌。如果網友抱著「獨樂樂不如眾樂樂」的心情，在網路上將色情圖片信手拈來再隨手貼上；更進一步者，乾脆招收會員、透過網路販賣

[14] 由雲林地檢署指揮省刑大偵二隊所查獲的色情網站，而該網站的負責人年僅十七歲，每月平均有十多萬的收益，其利用未成年之青少年作為經銷的下手，成為非常嚴密的行銷網，參閱民國 87 年 5 月 21 日，聯合報，第五版。

色情圖文大賺一筆，諸如此類的行為究竟會不會觸犯法律？既有體制的規範為何？

第一項　色情之認定

要處理網路上之色情問題，就必須將色情的定義加以明確化，但是何謂色情，是一種不確定之的法律概念，且會隨著社會風氣的改變而有不同的內涵，是否能以一般法律用語加以明確地定義，在目前而言仍有困難。我國現行刑法所欲禁止的色情，依刑法第二百三十五條的用語是「猥褻」。但這兩字性質上係屬於不確定之法律概念，實務上並無一個明確且統一的判斷標準，往往因為法官主觀認定之不同而有不同的結果，「運氣好」的被告，可能遇上觀念開放的法官而獲判無罪；「運氣差」的被告，遇上觀念保守的法官，卻因此而多了一項前科，這實在不是一個法治國家所應該有的現象。

根據司法院大法官會議在民國八十五年七月五日釋字第四百零七號解釋揭示「猥褻的出版品，乃指一切在客觀上，足以刺激或滿足性慾，並引起普通一般人羞恥或厭惡感而侵害性的道德感情，有礙於社會風化之出版品而言。」本號解釋並指出「猥褻出版品與藝術性、醫學性、教育性等出版品之區別，應就出版品整體之特性及其目的而為觀察，並依當時之社會一般觀念定之。」而且「有關風化之觀念，常隨社會發展、風俗變異而有所不同」。此種「猥褻」之界定，與一般人對於色情之認知有所不同。一般人可能認為裸體的圖片，就是色情圖片。但就法律層面而言，單純的裸露身體並不當然就構成法律所要限制及處罰之猥褻圖

片。同時猥褻之界定常隨社會發展及風俗變異而有不同的標準，不能一概而論。就目前實務上的判決與解釋觀察，仍無明確之定義及標準。例如台北及板橋地方法院有兩個判決均引用釋字第四百零七號解釋，卻作出不同的判決。在一家書店販賣閣樓雜誌被控妨害風化的案子中，承審法官認為猥褻之概念應與時俱進，扣案雜誌固然有女性裸露三點的照片，但表情自然，並無淫褻之意，故判決被告無罪；惟案件上訴至高等法院時又被宣判有罪[15]。但在另一件電腦遊戲軟體涉嫌妨害風化案件中，承審法官卻認為，卡通造型的裸女動畫露出兩點，雖然只出現三十秒，但是該內容在客觀上足以刺激並引起一般人性慾，而侵害性的道德感情故被告犯行即堪認定，構成妨害風化罪[16]。可見各個法官對於猥褻仍無法有一致的定義。

第二項　憲法保障人民言論自由之考量

美國通訊標準法（Communications Decency Act，簡稱 CDA）於一九九六年二月一日通過。主要是防止青少年經由網路接觸有害的資訊，其內容對於藉由通訊設備傳送淫穢或猥褻資訊與十八歲以下之青少年，

[15] 參閱臺灣高等法院八十六年度上易字第六三六一號刑事判決及臺灣板橋地方法院八十六年度易字第三三三八號刑事判決。

[16] 參閱臺灣台北地方法院八十六年度易字二七三九號刑事判決。

或是明知利用其設備為傳送色情資訊的行為而允許者，最高可處兩年以下有期徒刑或罰金或二者併罰。

該法第二百二十三條第(d)對於「明顯違法」（patently offensive）的意義，是指「任何人明知利用交互的電腦服務以展示任何明顯違反共通社會標準的評論、要求、建議、圖片等，或展示任何的性器官或排泄器官與此類器官的活動，而讓十八歲以下之青少年接觸到。有以下之行為時，不論是否係使用者主動要求或傳送者，以及明知並允許利用其設備觸犯此行為者」而言。本法通過後立即引起軒然大波，美國公民自由聯盟（American Civil Liberties Union，簡稱 ACLU)、美國圖書館聯盟（American Library Association，簡稱 ALA）與電子隱私資訊中心（Electronic Private Information Center，簡稱 EPIC）等團體，紛紛向法院提起違憲訴訟。該等團體均指出通訊標準法當中有關猥褻（indecency）條款範圍過於廣泛，係不當的擴張了言論管制範圍，而且違反了美國憲法增修條文第一條對表意自由保障之規定。

一九九七年六月二十六日，美國聯邦最高法院對於通訊標準法做成判決，以七比二之多數，形成通訊標準法違憲之判決。美國聯邦最高法院表示「傳輸猥褻資訊」（indecency transmission）和「明顯違反」（patently offensive）條款的用語過於模糊，認定的範圍可能會過廣，剝奪了美國憲法第一修正法保障民眾言論自由（the freedom of speech）的基本權利。再者，通訊標準法除了欠缺明確性之外，雖然其基於保護青少年免於接觸有害之資訊，而具有利益，但資訊標準法卻也因此限制了成年人基於憲法所賦予寄發以及接收資訊之權利。故美國聯邦最高法院認為，若有其他的方法可以達到通訊標準法所欲追求的目標，則通訊標準法對成年人資訊所加諸之負擔即係不可容忍，而由於現行可以就現

有軟體或其他相關科技設備與相關制度來管制色情資訊，因此通訊標準法所採取的手段即非唯一合適之手段。

雖然通訊標準法被宣告為違憲，但並不表示在網路上傳輸任何形式之的內容都是合法的。只是在保護青少年之同時，也必須注意其他基本的人民權利，而所採取的手段是否適當，是否以逾越了必要程度，仍必須善加考量。因此我國若要以法律限制人民的自由時，除了考慮憲法對於人民之基本權利之保障，與憲法第二十三條要件之限制，需符合上述情況所制定之法規，才不會與憲法保障人民基本權利之精神相牴觸。

CDA 對於言論成現形式幾乎是採取一網打盡的方法加以管制，使得出現在網站上的所有訊息都可能成為有害未成年人身心的色情言論。但是就色情網站的營運成效而言，圖片和影像才是真正能夠吸引喜好色情網友的要素。對於喜好網路色情的成年網友們，這種處以拘禁和高額罰款的刑罰規定是否有礙於成年網友的言論表達自由呢？成年網友的權益保障是否符合比例原則呢？保障兒童不受網路有害資訊之傷害是社會大眾的共同期望，雖然司法人員希望兒童能遠離網路色情言論的傷害，但是我們不得不承認保障成人言論自由權利之重要性。而言論自由基礎理論相關學說中，最廣為被討論的四種學說是：

（一）言論自由市場說（Marketplace of Ideas）：由英國 John Milton 所提出之學說，其目的為說服英國國會廢止對出版物事前限制之制度。美國聯邦最高法院大法官 Oliver W. Holmes 在一九一九年以「市場機能」的觀點說明追求真理乃為自由之最終目的及手段，此即所謂的「言論思想之自由市場理論」[17]。

[17] 參閱林子儀著，言論自由與新聞自由，86 年，頁 16-24。

（二）健全民主程序說：此說認為言論之價值在於幫助人民參與民主政治的決定，因此不是所有言論都值得保障。

（三）表現自我說（Self-fulfillment）：大法官 William O. Douglas 是倡導表現自我說之言論自由理論的先趨，在期早期的最高法院判決中，即已明確地表明他的主張是憲法保障言論自由之目的即在保障個人之獨立自主。

（四）安全閥說（Safe-Valve）：自由發表言論的權利，可以作為不滿民怨之發洩管道，其功能類似巨大機械運轉之安全閥作用，有助於社會體制之安定運作[18]。

在四種理論中，Reed 法官採與 ACLU V. Reno（I）一案中與最高法院持相同審理態度，從「自由市場理論」出發，認為 COPA 一案中「不雅言論（Indecent speech）」與健全民主程序並無相關，同時此類「低價直（Law Value）的言論」亦與自我實現完成自我的宗旨目標無涉。儘管這類低俗不雅的言論並無太大的社會實用價值，這一類言論仍然受到美國憲法第一增修條文的保障。

言論自由為現代民主社會的重要人權指標，我國憲法第十一條「人民有言論、講學、著作及出版之自由」之明文規定保障了人民的言論自由及出版自由。人類文明即將邁入二十一世紀，人類訊息的交流傳遞卻因為網路資訊科技的發明與發展，而有不同的面貌。網際網路的出現對傳統媒體造成的影響，及其引領媒體演化之事實，使得民眾及一般廣電媒體在訊息的發表、取得、發行等層面，出現了迥異於往的方式。但言

[18] 參閱余依婷、鄭慧文、法治斌合著，從 ACLU V. Reno（II）看美國如何管制色情言論，資訊法務透析，88 年 10 月，頁 36-37。

論自由的精神不變，涉及言論自由本質、表達、管理、規範等議題，卻有了不同的面貌。此時正是重新思考言論自由在二十一世紀之新價值觀的最佳時機，而不應區分網路新興媒體與傳統廣電媒體。

第三項　網路色情之類型

根據目前所發生的「網路色情」的犯罪態樣加以分析，可以將其分為下列數種類型：

第一款　張貼色情或猥褻性質之圖片或文字

行為人自行設立網站張貼具有色情或猥褻性質之圖片或文字，此類行為通常係藉由公開之網址，得由不特定之人以網路連結之方式進入網站，開啟網頁觀賞。基本上，網路的無邊春色可以用於刑法第二百三十五條來規範，因為這個條文規定「散布或販賣猥褻之文字、圖畫或其他物品，或公然陳列，或以他法供人觀覽者，處一年以下有期徒刑、拘役或科或併科三千元以下罰金。」而在網頁上張貼或招收會員販賣色情圖片，便屬於刑法第二三五條所規範的「散布」或「販賣」猥褻圖文的行為。此外，司法院院字第二一七九號解釋對「公然」的定義為「不特定或多數人所得聞見」，由於網際網路可供「不特定或多數人」上網閱覽，依此推論，貼色情圖片的網友即可能該當了刑法第二百三十五條所禁止

的「公然陳列」或「以他法供人觀賞」猥褻圖文。

依新修正之刑法第二百三十五條第一項規定，就其犯罪構成要件檢視之，其張貼圖文之行為縱使未符「散布」或「公然陳列」[19]之要件，亦屬「以他法供人閱覽」之客觀構成要件。

實際上已有許多觸犯刑法第二百三十五條的案例發生，像張姓夫婦設立「說說成人網站」，利用該網站傳送男女交媾等猥褻畫面，並以月費兩百元的價碼招收想觀賞圖片的會員；台北地院判處這對夫妻各八個月與五個月的徒刑，得易科罰金。另外，「禁忌樂園」網站則是由黃姓男子以每月一百五十元的會費招收會員，然後將他由國際色情網站下載的色情圖片以電子郵件傳送給會員；結果板橋地院對之判處四個月徒刑。

另外，兒童及少年性交易防治條例中亦有相關規定，該法第二十七條禁止「拍攝、製造未滿十八歲之人為姦淫或猥褻行為之圖畫、錄影帶、影片、光碟、電子訊號或其他物品」，同法第二十八條進一步規定散布、販賣、公然陳列或以他法供人觀賞上述猥褻物品者，處三年以下有期徒刑，得併科新台幣五百萬元以下罰金。換言之，如果在網路上張貼、放映的猥褻圖畫、影片、光碟等內容的主角是未滿十八歲的未成年人，便觸犯了兒童及少年性交易防治條例第二十七條、第二十八條之規定。

[19] 所謂散布係指對於不特定之多數人散發傳布而言；而公然陳列則是指置於不特定多數人可以目睹之狀態。

第二款　傳送具有色情或猥褻性質之圖片或文字

網際網路對年輕人口的影響，除了在日常生活中花大量的時間坐在電腦桌前靜態的使用電腦網路外，更甚而發展出動態的實際參與網路內容的演出。例如在美國佛羅里達州的坦帕市（Tampa, Florida），有六名十八到二十二歲不等的大學女學生，共住在一棟裝設有四十架攝影機的房子裏，提供她們二十四小時全天候生活作息的立即轉播，並以「窺淫宿舍（Voyeur Dorm）」網站作為號召。有興趣的網友只要每個月付三十四美元的費用，便保證能收到清涼養眼的畫面，而這些網站的盈收，將分紅給這些女學生，作為她們生活費和學費的支付來源。帕坦市的城市區域委員會對此種行為做出裁定，認為該網站的經營者違反該市不得在住宅區經營成人娛樂事業的規定。六名帕坦市市議員則投票一致通過支持該委員會的裁定，並要求關閉此網站。

國內日前也已發生過相類似的案例，也是傳送妙齡女子生活寫真的影像於網路上，以招攬會員觀賞。姑且不論就道德層面，或公共秩序善良風俗面其適當性與否，若單純從法律規定觀之，若僅為單純的傳送生活畫面，就目前我國刑法之規定，尚不至於涉及任何法律問題。惟若網站內容已涉及猥褻的程度，根據刑法第二百三十五條之規定，「散布、播送或販賣猥褻之文字、圖畫、聲音、影像或其他物品，或以他法供他人觀覽、聽聞者…….」，則該行為已該當刑法第三百三十五條之構成要件，應負刑事責任。

行為人利用網際網路傳送具有色情或猥褻性質之圖片或文字至他人網站或電腦主機。利用網際網路「傳送」圖文至他人網站或電腦主機，

屬散布行為應無疑義，至於行為人所傳送之圖文檔案在未經編碼之過程前雖僅為「電磁記錄」，與傳統上本罪所欲規範之對象不同，然透過電腦及相關機器設備的處理可將此等電磁記錄轉換成圖片或文字顯現在電腦螢幕上，而可為人之知覺所認識，故此行為亦可以第二百三十五條第一項之罪處斷。而上述之情形，若該色情猥褻之圖片中之「主角」係為未滿十八歲之兒童或青少年，則應適用兒童及青少年性交易防治條例第二十八條之規定，可處三年以下有期徒刑，得併科新台幣五百萬元以下罰金。至於在網路上張貼（post）或傳送具有「色情」或「猥褻」性質之圖片或文字是否能有效的以法律規範，或是否適合以法律規範之，有無違反言論自由之限制等問題，目前雖仍有爭論，然在我國刑法相關規定未修正前，尚無法改變目前之現況。

第三款　網路上媒介色情交易

目前有些色情網站提供留言版給網友上網留言[20]，以尋找性伴侶或尋求一夜情。甚至有些網站更以招收會員之方式，為其加入之會員媒介色情交易，或者組團至國外買春等行為出現。如果該網站有營利之行為，且這些留言訊息涉及性交易，則可能構成刑法第二百三十一條第一項「意圖使男女與他人為性交或猥褻之行為，而引誘、容留或媒介以營利者」。且須注意的是，刑法第二百三十一條第二項有常業犯之規定，若行為人係以此為職業，恃媒介色情交易為生者，則須依此常業犯之規定加重其

[20] 參閱蔡美智著，談網路犯罪，資訊法務透析，民國 88 年 1 月，頁 39。

處罰。

第四項　小結

言論自由為現代民住社會的重要人權指標。我國憲法第十一條規定：「人民有言論、講學、著作及出版之自由。」明文保障了人民言論自由及出版自由。人類文明即將邁入二十一世紀，人類訊息的交流傳遞卻因為網路資訊科技的發明與發展，而有了不同的面貌。網際網路的出現對傳統媒體造成的影響，及其引領媒體在訊息的發表、取得、發行等層面，出現了迥異於往的方式，正是最好的例證。惟言論自由的精神不變，但是涉及言論自由本質、表達、管理、規範等議題，卻有了不同的面貌。憲法所保障之言論自由種類亦包括「低價值的言論」，但是「色情言論」則不屬憲法保障之範籌。言論是否涉及色情的判斷標準，與其發表散播的媒體無關，亦即網路新興媒體的色情言論認定標準等同於傳統媒體。

第二節　發表不當言論

第一項　網路恐嚇

一九九六年，一封發自中山大學的電子郵件（E-mail）恐嚇要暗殺美國總統柯林頓，一九九七年四月十八日，又再次有人利用電子郵件恐嚇高雄的中信飯店，要求交付九百萬元，否則將炸毀飯店。此種利用網

路電子郵件來達到其恐嚇危害安全或恐嚇取財之目的，是否能以現行刑法加以規範？

第一款　刑法刑法第三百零五條恐嚇罪之適用

行為人以加害生命、身體、自由、名譽、財產之事，恐嚇他人，致生危害於安全者，構成刑法第三百零五條之恐嚇罪。本罪之「恐嚇行為」係指以加害生命、身體、自由、名譽、財產等事通知他人，使其發生畏懼。加害之內容則以加害生命、身體、自由、名譽、財產等事項為限，若為此等內容以外之事項，即不能成立本罪。且必須行為人係以不法之惡害通知他人，方足當之，若以正當合法之事通知他人，雖他人心生畏懼，也不能成立本罪。又行為人只要客觀上將其加害生命、身體、自由、名譽、財產等事項，通知他人即為已足，至於行為人主觀上是否真有實現加害之意圖，則與本罪之成立無關。惟行為人所通知之惡害必須為行為人所能左右控制，且在客觀上，一般人均認為足以對人構成危害者，始為本罪之恐嚇。至於恐嚇之方法係語言、文字或舉動等，亦均非所問。但恐嚇行為必須直接或確定之間接對行為客體為之，若係不確定之間接為之者，亦非本罪之恐嚇。所謂「確定之間接」係指行為人雖不直接恐嚇被害人，但將其恐嚇事實告知特定人，明示其通知被害人，而不確定之間接則是指行為人僅對不特定人揚言恐嚇事實，並無明示任何人將其恐嚇事實轉知被害人[21]。而行為人之恐嚇行為，一旦完成，而能使被害

[21] 參閱林山田著，刑法各罪論（上），民國 88 年，增訂二版，頁 167-168。

人心生畏懼，即可成立本罪，而不待行為人所恐嚇之事項，成為事實，方構成本罪。

第二款　刑法第三百四十六條恐嚇取財罪之適用

行為人意圖為自己或第三人不法之所有，以恐嚇使人將本人或第三人之物交付，構成刑法第三百四十六條第一項之恐嚇取財罪。本罪之行為乃恐嚇而取財，就刑法理論而言，學者認為本罪之恐嚇行為係指以強暴或脅迫或其他不法手段，使人心生畏懼而受其強制，但尚未達不能抗拒之程度而言[22]。換言之，即被恐嚇者雖受行為人以強暴或脅迫或其他不正方法之恐嚇，但其作為或不作為尚有相當程度之意思自由，否則如被恐嚇者之意思自由已完全喪失，毫無選擇之餘地而不得不交付財物，則已超出恐嚇罪之不法內涵，而應科以強盜罪。但實務上對於恐嚇取財之「恐嚇行為」認為係指以將來之惡害通知被害人，使其心生畏怖為已足，若進而對被害人施用強暴脅迫，自非僅為恐嚇，而應構成其他相當之罪名。又認為行為人若對被害人施用強暴脅迫，縱未至不能抗拒之程度，亦不能論以恐嚇罪[23]。並認為若以目前危害相加，則為脅迫，施以暴力，則為強暴，均與恐嚇之意義不符。此種見解會使得強盜罪與恐嚇罪之間形成一個條款間隙，按恐嚇罪之本質乃在於被恐嚇者由於行為人之行為而心生畏懼，至對其本人或第三人之財產，做合乎行為人之不法

[22] 參閱林山田著，刑法各罪論（上），民國 88 年，增訂二版，頁 381-383。

[23] 最高法院四十五年臺上字第一五八三號判例參見。

獲利意圖之處分。因此，只要能使被恐嚇者心生畏懼，而且客觀上足以使行為人達到不法獲利意圖之行為，即可認定為該當本罪之恐嚇行為。職是之故，以未來之惡害通知他人，使其心生畏懼，固為本罪之恐嚇行為，但以現時之危害，甚而施以強暴或脅迫，只要是此等強制行為，並未強至使被害人不能抗拒之程度，則仍屬於恐嚇行為之範圍，而可依據本罪處斷。否則依實務之見解，行為人出於不法獲利之意圖，而以強暴或脅迫等不法手段，雖尚未至不能抗拒之程度，但被害人心生畏懼而交付財物，則既不能論以本罪，又不能論以普通強盜罪，造成處罰上之漏洞。

恐嚇行為係以言語、文字或舉動，均非所問。故以電子郵件作為恐嚇通知之工具，與傳統之恐嚇行為並無二致，仍可構成本罪。至於恐嚇內容不限於生命、身體、自由、名譽或財產，而且也不以違法者為必要，即使以法律所許可之方法，作為恐嚇取財或得利之手段，亦可成立本罪。但網路駭客若以侵入電腦系統使被害人之電腦當機之方式迫使被害人交付財物之行為，則依學者之見解，因係以現時之危害，向被恐嚇者施以脅迫，但只要是此等強制行為，並未強至使被害人不能抗拒之程度，則仍屬於恐嚇行為之範圍，而可依據本罪處斷。但若依實務之見解，則因網路駭客係以脅迫之方式為之，故與恐嚇取財罪之構成要件不該當，且被恐嚇者尚未至不能抗拒之程度，亦無法該當刑法強盜罪之構成要件，此處即造成強盜罪與恐嚇罪之間形成一個條款間隙。因此，應將實務上對於恐嚇行為之解釋，加以修改為「以惡害通知他人，或以強暴脅迫或其他不正當之方法，使他人心生畏懼，但尚未至不能抗拒之程度」，如此便可彌補前述強盜罪與恐嚇罪之間所形成之條款間隙，而且更能符合恐嚇罪之本質，同時對於日新月異的網路犯罪，亦能發揮對抗犯罪之功能。

第三款　小結

美國總統生命之事由恐嚇之，若因此而致生危害於其安全，即應該當刑法第三百零五條之恐嚇危害安全罪；而後者之行為人係意圖為自己或第三人不法之所有，利用電子郵件傳遞恐嚇之訊息，要求中信飯店將其財物交付之。然最後未取得財物，但仍然該當刑法第三百四十六條有關恐嚇取財之規定，至其財物取得與否僅為既未遂之判斷依據而已。至於網路駭客以侵入電腦系統使被害人之電腦當機之方式迫使被害人交付財物之行為，則必須對恐嚇行為之內涵依恐嚇取財罪之本質，重新加以檢討，始能加以規範。

第二項　妨害名譽或信用罪

名譽及信用乃是個人在社會活動中一種重要之生活利益，名譽係指個人人格在社會生活上所受之評價，而信用則指個人之經濟行為或經濟能力在經濟活動中所受之評價，這兩者與個人之社會評價與其經濟地位及經濟活動能力等，均有極為密切之關係，故刑法乃特設專章，加以保護。使個人之名譽及信用，不受他人無端之破壞。

第一款　公然侮辱罪之適用

按公然侮辱他人之行為，構成刑法第三百零九條之公然侮辱罪。行為人之公然侮辱行為須對特定人為之，方能成立本罪，如對不特定人或不能推知之人公然辱罵，自不能構成本罪。故本罪之行為客體只限於侮辱行為所對之特定人或依侮辱行為可得推知之人。所謂公然侮辱係指行為人在不特定人、多數人或特定之多數人共見共聞下或得以共見共聞下，侮弄辱罵特定人或可得推知之人，如在公共場所，以粗鄙語言，向特定人辱罵，即可構成本罪。惟並不以實際上果有共見共聞之情況為必要，僅須在事實上有與不特定人或多數人得以共見共聞之狀況即可。而所謂之多數人乃指人數眾多，非經相當時間之分辨，難以計數者而言，包括特定之多數人在內。又公然嘲弄或謾罵他人不問以言語、文字或舉動，均可構成本罪。侮辱時被害人是否在場聞見，或公然侮辱後，被害人之名譽是否實際受到損害，均不影響本罪之成立。但單純的對他人不禮貌之行為或言詞，或是疏忽而不尊重他人，則與本罪之行為不相當，惟有時此等行為與本罪之侮辱行為，其界限模糊而不易區分，此應就案情整體地判斷，其判斷標準包括行為人之年齡、教育程度、職業、與被害人之關係、行為地之方言或用詞習慣等。

在不少網站上，可以看到電視或電影女明星的頭被接到裸女身體的照片。這種移花接木的行為，依具體情形而定，有可能構成刑法上的公然侮辱罪。例如將形象良好清新之玉女明星的頭接到色情雜誌所刊登之裸女照片或猥褻色情圖片上，因為在網路上不特定人均得任意進入閱覽該網頁內容，已屬公然之狀態，而該等裸女照片或猥褻色情圖片之合成圖片無異為對該女明星人格之貶抑與扭曲，同時亦對其名譽造成損害，故應構成刑法第三百零九條之公然侮辱罪。

目前網路上許多網站均提供所謂「聊天室」之服務[24]，讓網友透過聊天室以文字敘述之方式做相互之溝通，此種聊天室具有互動性、即時性與隱匿性，且非一對一的聊天，而係不特定之多數人相互聊天。此時若有人在聊天室中以文字侮辱他人，是否有刑法第三百零九條公然侮辱罪之適用？按網際網路中之聊天室，只要連結上該網頁之後，任何人均得任意進入該聊天室而不受限制，因之，在網路上之聊天室聊天時，應可認為係處於事實上有與不特定人或多數人得以共見共聞之公然情狀。雖然在網路聊天室中使用者大多用綽號或暱稱，但仍係屬特定人或可得推知之人，故若有行為人以文字嘲弄或辱罵他人時，即可構成刑法第三百零九條之公然侮辱罪。

第二款　加重誹謗罪之適用

民國八十七年五月，一位淡江大學學生在該校 BBS 站上批評該校校長「充其量不過是隻哈巴狗」，而遭到該校記大過處分[25]。八十六年十一月間，政大一名學生因在校園網路上發布不實言論，辱罵教授，遭該教授提出告訴後，為台灣高等法院依加重誹謗罪判處拘役五十五天，成為

[24] 此種聊天室之種類繁多，有限定主題之聊天室，亦有無主題之聊天室，此為時下網路族最熱門之交友方式，由於具有互動性、即時性與隱匿性，因此亦容易產生許多違法之弊病。

[25] 參閱中時電子報，http://www.cj\hinatime.apers/xfocus/87052515.htm。

國內首宗利用網際網路誹謗他人而被判刑確定的案例[26]。此外在台灣大學的 BBS 站上亦曾發生二名教授遭不明人士冒名發表誹謗同校其他三位教授之文章，事後透過電信局之協助終於查獲冒用者之帳號及真實姓名，並予起訴。

若行為人意圖散布於眾，而指摘或傳述足以毀損他人之名譽之事者，構成刑法第三百一十條第一項之普通誹謗罪。行為人以散布文字或圖畫之方法而犯普通誹謗罪者，則構成同條第二項之加重誹謗罪。而侮辱罪與誹謗罪不同，兩者宜妥加區分：行為人不摘示事實而公然侮弄辱罵特定人或可推知之人，構成侮辱罪；若行為人指摘傳述足以損害他人名譽之具體之事件內容，則構成誹謗罪。所謂「指摘傳述足以損害他人名譽之事」即指出摘發或宣傳轉述足以損害他人名譽之具體之事件內容。行為人必須針對特定人或可能推知之人，實施本罪之行為，方構成本罪；否則，如非對於特定人或不能推知之人，指摘傳述足以損害名譽之具體內容，自不成立本罪。又指摘與傳述並不以公然為限，故雖非公然而僅私相指摘，亦可能構成本罪。而刑法上所謂「散布」係指擴散傳布於眾，包括一次擴散傳布於不特定人、多數人或特定之多數人以及一次散布於一人，但反覆多次為之，使其擴散於眾[27]。

惟若行為人之指摘或傳述係以文字或圖畫之方法為之者，即構成加重誹謗罪，因為若以文字或圖畫而加指摘或傳述，則足以損害他人名譽之事，因寫成文字或繪成圖畫，流傳顯較單純以口頭方式為廣，故將此等行為方法作為加重構成要件之依據。

---

[26] 參閱聯合報 87 年 3 月 27 日第 7 版。

[27] 參閱林山田著，刑法各罪論（下），民國 88 年，增訂二版，頁 703。

在今日網際網路蓬勃發展之情形下，網際網路儼然以成為另一種新興之傳播媒體，網路上之留言版、討論區、聊天室或 E-mail 等均為網路上發表個人意見之管道，因為在網際網路上，不特定人均得任意進入閱覽網頁內容，所以在網路上之留言版、討論區、聊天室或 E-mail 中指摘或傳述足以損害他人名譽之事，解釋上應可認為係刑法上所稱之「散布」。尤其 E-mail 更是威力強大，可以在短時間內發送大量之電子郵件，不受時間及空間距離之限制，其影響力及破壞力已非傳統「黑函」所能比擬。

第三款　小結

因此，這種利用 E-mail、BBS 站或其他網路之媒介散布或傳述不法言論如誹謗、公然侮辱或妨害信用等之行為，依其情形可分別成立刑法妨害名譽或信用罪章之各罪，與一般妨害名譽案件之不同，僅在於其所利用之傳播工具之不同而已，適用上並無問題。問題在於其所利用之工具，即網際網路，所造成之損害結果及層面，遠遠超過傳統之犯罪工具，目前刑法所規定之刑責是否有視其損害之結果予以加重之必要，即值吾人深思。

第三節　網路詐欺

網路上「老鼠會」已經存在於網路世界相當時日，網路金錢連鎖信就在國內 BBS 站中以短期致富之名義流傳。在八十六年底，更有一自稱

為「台灣駭客教父」之男子，虛設網路服務公司佯稱免費贈送帳號及電子郵件信箱，騙取網友之帳號及電子郵件信箱販售圖利[28]。又美國曾發生「雷爾運動」的網路詐欺案例[29]，某組織透過網路刊登複製人的廣告，向不孕夫婦以及同性戀者推銷「無性生殖」與「細胞儲存」的技術，費用是美金二十萬元；但根據生物科技開發中心的說法，目前生物技術尚無法複製人體，而且各國法令亦禁止人體複製，因此，這只是另一種詐欺的形式。由於政府大力推動網際網路的普及與利用，因此網路詐欺之行為未來將不易杜絕。此外尚有所謂「網路黑店」及「網路金光黨」的詐欺類型在網路上出現，網路黑店係指利用網路購物發展網路黑店並於收款後關站，因網際網路服務業者對客戶真實身份未詳加確認，一般人均可免費成立短暫網站，提供部份商品廣告於網路上，伺多數客戶繳款後即閉站歇業。而網路金光黨則指以類似老鼠會方式發連鎖發財信，並以多層次傳銷方式經營，如連鎖發財信、郵遞名單事業及網路投資遊戲等等。

由於此種詐欺行為所詐欺之對象仍為自然人，而其僅係以利用網路服務為其犯罪方法之一部，與傳統上刑法所規範之詐欺行為並無不同，只是利用現代科技產物作為犯罪工具而已，是故以刑法之詐欺罪加以規範應無疑義。

---

[28] 被補之嫌犯在 BBS 站上佯稱其能破解他人之網路帳號，藉此吸引貪小便宜的網友購買帳號盜用，再將前來購買者之帳號轉賣他人，據警方調查被害人已超過十五萬人。參閱民國 86 年 12 月 27 日，聯合報，第六版。

[29] 參閱張雅文著，網路犯罪之法律責任與防治建議，請參見 http://suc.m.org.tw/neuaw/paper/crime.htm

惟若行為人係以利用不正之方法將虛偽不實之資料輸入電腦而影響其處理資料之結果，此種行為是否亦可視為刑法上之「詐欺」，則容有討論之餘地。傳統之詐欺行為，除行為人在主觀上須具有為自己或第三人不法所有之意圖外，在客觀上更須有以「詐術」使人將本人或第三人之物交付或得財產上不法之利益或使第三人得之之行為。而所謂詐術係指「以欺罔之手段，使人陷於錯誤」，且行為人之實施詐術，必須引致被騙者之錯誤，方有成立刑法詐欺罪之可能[30]。但電腦是依其程式設計者所設計之程式執行並作出反應，並不會因為行為人之詐術而陷於錯誤，故利用不正之方法將虛偽不實之資料輸入電腦而影響其處理資料之結果的行為，無法該當刑法原有的第三百三十九條詐欺罪之構成要件。惟亦有論者認為電腦為所有者手腳之延伸，對電腦詐欺即係對於所有者詐欺，仍可成立刑法上之詐欺罪。然而基於刑法罪刑法定主義之原則，實不宜將詐術之範圍加以過度之擴張。為解決此一爭議，修正後之刑法第三百三十九條之三對此已予以規範，明定：「意圖為自己或第三人不法之所有，以不正方法將虛偽資料或不正指令輸入電腦或其相關設備，製作財產權之得喪、變更記錄，而取得他人財產者，處七年以下有期徒刑。」

第四節　煽惑他人犯罪

[30] 參閱林山田著，刑法各罪論（上），民國 88 年，增訂二版，頁 327。陳煥生著，刑法分則實用，自版，民國 79 年 10 月修訂版，頁 495-497。最高法院五十三年臺上字第一八一一號判例參見。

網路的發展也提供了一個煽惑他人犯罪的另一個管道。例如民國八十六年六月，有人在國立清華大學的網路討論區的「跳蚤市場」上公然販賣 FM2；同年九月一名楊姓青年即在網路上設立「軍火教父」之網站將國外的軍售網站翻譯成中文在加註台灣買主的購買方式，提供有關販賣槍枝的圖片及文字之資訊，並且在搜尋引擎奇摩網站上登錄該「軍火教父」之網址，提供不特定多數人上網查詢「軍火教父」刊載之資訊，該網站僅係提供一個販售槍枝的媒介管道，尚未有販售槍枝之行為。台北地方法院認為楊姓青年的行為觸犯了刑法第一百五十三條第一款的「以他法公然煽惑他人犯罪」，判處有期徒刑五個月，緩刑三年[31]。此案在台灣的網路界引起軒然大波，一時之間火光四射，法務部為此別成立專案小組，全面清查網路犯罪行為[32]。

另一個案例則是網路上教製炸彈，民國八十六年九月，某私立大學資訊系陳姓學生，在學校網站建立「無政府份子文件」個人網頁。他並將國外相關討論群組中介紹各種炸藥製造方法、過程與威力的文章、轉載張貼於個人網頁上，供不特定之人觀看、討論。由於各類炸彈或爆裂物非經中央主管機關許可，任何人不得製造，若有未經許可為製造之者，應依槍砲彈藥刀械管制條例第十一條之規定科以刑責。台北地方法院認為陳姓學生將介紹炸彈等爆裂物之製作方法的文章轉載張貼在其個人網頁上，顯係刺激慫恿他人犯製造炸彈等爆裂物之犯罪，而該網頁並未設定密碼，不特定人進入電腦網際網路後，均得任意再進入陳姓學生之個人網頁閱覽上開文章，陳姓學生之煽惑行為以置於不特定人得以共見共

---

[31] 參閱蔡美智著，談網路犯罪，資訊法務透析，民國 88 年 1 月，頁 39。

[32] 參閱民國 86 年 9 月 9 日，中國時報，第六版。

聞之公然狀態，係觸犯了刑法第一百五十三條第一款之以文字公然煽惑他人犯罪，且為連續犯，結果判刑十個月，緩刑三年，並交付保護管束[33]。

按行為人以文字、圖畫、演說或他法，公然煽惑他人犯罪違背法令或抗拒合法之命令者，構成刑法第一百五十三條之煽惑他人犯罪或違法抗命罪。所謂煽惑乃指煽動誘惑之意，一般大眾本無犯罪之意思，或雖有犯罪之意思，但仍未著手實行之時，將因行為人之煽動或誘惑行為，而使其生犯罪之意思或更堅定其本有之犯罪意思。純就行為本質而言，煽惑時與教唆有相同之處。

行為人必須公然煽惑，方能構成本罪，否則，如非公然煽惑者，自無本罪之適用，只能就其煽惑內容科以教唆犯。稱「公然煽惑」係指在不特定人、多數人、特定之多數人共見共聞或可得共見共聞之情狀下從事煽動誘惑工作而言。本罪既須公然煽惑，始能成罪，故可知煽惑對象必須為不特定人、多數人或特定之多數人等一般民眾。

至於煽惑之方法，行為人必須以文字、圖畫、演說或他法實施煽惑，方構成本罪。行為人用以煽惑之文字、圖畫或演說不以自己創作者為限，即使利用他人之文章、圖畫或他人之演說辭而實施煽惑，亦可構成本罪。再者，行為人只要煽惑他人犯罪，即為已足，而不以煽惑他人犯特定之罪為必要。至於行為人煽惑他人所犯之罪究為刑法抑或特別刑法之罪？則在所不問。

由前述法院之判決可知，實務上將網際網路認為係屬公然之情狀，而為不特定人所得共見共聞。因為任何人只要能連結上網際網路，均可自由瀏覽網頁之內容而不受時間與空間之限制。惟台灣台北地方法院八

[33] 參閱蔡美智著，談網路犯罪，資訊法務透析，民國 88 年 1 月，頁 40。

十七年度易字第四二九號刑事判決所指出「..未設定密碼，不特定人進入電腦網際網路後，均得任意再進入陳姓學生之個人網頁閱覽上開文章，陳姓學生之煽惑行為以置於不特定人得以共見共聞之公然狀態..」之見解，似認為若該個人網頁如有設定密碼，即非屬不特定人得以共見共聞之公然狀態，此種見解容有疑義。蓋若該個人網頁雖設有密碼，但卻對外招收許多會員，會員可憑密碼進入網頁閱覽，此種行為與特定之多數人得共見共聞之情況無異，但依前述之實務見解，似非刑法上所稱之公然。此種解釋會造成有心者以設定密碼之方式，規避法律之規定，故本文認為應就實際上之情況認定是否為公然之情狀，而非以是否有設定密碼為判斷之標準。

第五節　網路賭博

目前，賭博行為仍是我國法律所禁止之行為，刑法對之設有處罰之規定。然而近年來社會上所發生之職棒賭博案、有線電視頻道賭博案，更說明了這種肇因於人類貪婪特性之行為，即使在法律禁止之下，人們也會想盡一切辦法，規避法令之限制。而網路的發展毋寧是為賭博行為提供了一個極佳的環境，使得賭徒們有了一個絕佳的管道從事賭博行為，網路賭博行為是否可以現行刑法之賭博罪加以規範，似乎因此產生了不小之衝擊，殊值吾人加以注意。

按行為人在公共場所或公眾得出入之場所賭博財物者，構成刑法第二百六十六條第一項之普通賭博罪。依刑法第二百六十六條之規定，普通賭博罪之構成要件中對於「場所」有其要件之限制，即須在公共場所或公眾得出入之場所賭博財物，且須非為供人暫時娛樂之物方構成本

罪。故行為人於此等場所以外之地方賭博者，如住宅或公眾不得出入之店舖內賭博，縱令賭博之人及賭具為戶外所易見，或其賭聲為戶外所易聞，亦均不構成本罪，而為社會秩序維護法第八十四條規定之「於非公共場所或非公眾得出入之職業賭博場所，賭博財物者」所加處罰之行政不法行為。

稱「公共場所」係指多數人公共使用或聚集之場所，如道路、公園、廣場、軍營與公署，惟如公署已劃出一部，為職員眷屬居住，若另闢有出入門戶，不與該公署同一門禁者，自不能謂為公共場所，故在此眷屬寢室內賭博財物者，即不構成本罪。又稱「公眾得出入之場所」則指不特定人隨時得以出入之場所，如餐廳、飯店、酒樓、百貨公司、山野僻靜處、公共防空壕洞或防空室、旅館等。惟如旅館之某一特定房間，若由某人承租住入，即視同私人住宅，而非公眾得出入之場所，故如在旅館租一房間而由特定人聚賭，自亦不構成本罪。又僅邀約特定人在家賭博，尚不能謂係當然為公眾得出入之場所。因此，被邀參與賭博之人自亦不構成本罪。「網站」是否可認為係傳統刑法觀念中之「場所」，即有疑義。因為傳統刑法上所稱之場所係指占有實際空間體積之實體，且可透過人 知覺直接感受其存在之空間 而網際網路之世界乃是電腦網路所虛擬出來之世界，雖然它具有互動性與即時性，但仍非現實生活中我們可以直接以人之知覺感覺其存在者，仍必須透過電腦之處理始能感覺其存在。因此，若採肯定見解似與刑法之罪刑法定主義之要求有所扞格，已超過文義解釋上之範圍，且在自宅賭博並不構成本罪，若其在自宅透過網路參與賭博反構成本罪，顯與一般之國民感情相悖；且若認為該當刑法上之賭博罪，則行為人之電腦及網路設備是否為刑法第二百六十六條第二項所稱之「賭博器具」，得否予以沒收，亦生疑義。依刑法第二百

六十六條第二項之規定，當場賭博之器具與在賭櫃或兌換籌碼處之財物，不問屬於犯人與否，均沒收之。所謂「當場賭博之器具」係指在賭博現場直接用以賭賽輸贏之器具，如各類之紙牌、麻將牌、象棋、骰子、輪盤等。傳統之賭博器具在網路賭博中均由電腦虛擬而成，而透過電腦螢幕顯現出來，自無從沒收。但電腦及網路設備解釋上雖亦可認為係賭博之器具，但得否認為「當場」賭博之器具，則容有疑義。而所謂「在賭櫃或兌換籌碼處之財物」係指賭博當場陳置於賭櫃上或存放於兌換籌碼處之現鈔、有價證券或其他財物。若行為人係以信用卡在網路賭博時支付所下注之賭資，則該等賭資得否認為係賭博當場陳置於賭櫃上之其他財物而依刑法第二百六十六條第二項之規定加以沒收，亦有疑問。凡此種種問題，在嚴守罪刑法定主義之前提下，均已造成刑法上之處罰漏洞，實非條文解釋所能解決，應從立法規範著手，始能解決問題。

關於網路賭博行為，美國國會於一九九七年三月提出之「網路賭博禁止法」草案（Internet Gambling Prohibition Act）賦予法院得以發出禁制令禁止電信公司與互動式電腦服務提供者（Interactive Computer Service Providers）接收或傳送有關網路賭博之電腦資訊。而同年八月所提出之「州際線路法」修正草案（The Interstate Wire Act）中亦對網路賭博行為加以規範，其規定不論電話、傳真或網路，凡透過線路下賭注或接受賭注均屬違法之行為[34]。由於我國現行刑法對於此種新興之賭博方式並無特別之規定，是否該當刑法上賭博罪之構成要件非無疑問，因此，美國之立法例值得作為我國規範網路賭博行為之參考。有關單位應儘速研擬相關規定因應，以免網際網路成為規避刑法賭博罪

[34] 參閱馮震宇、劉志豪前揭著，頁 87。

之管道。

第六節　網路上販賣大補帖

網路上販賣大補帖或泡麵[35]的情形十分盛行，主要是因為有利可圖，一片空白之光碟片成本約為新台幣三十五元，在經過燒錄設備將電腦程式軟體或電腦遊戲拷貝至光碟上後，可以成本之十倍至三十倍之價格出售，由於許多原版的電腦作業系統程式價格十分昂貴，動輒上萬，一般之上班族與學生均負擔不起，而這些人又是主要的電腦使用人口，所以大補帖之魅力可想而知。在暴利之驅使之下，行為人四處寄送廣告電子郵件或在 BBS 站上刊登訊息以販賣大補帖。此外尚有所謂網路銷贓，乃指假借網路的二手貨園地販賣免稅商品（如寫真集或遊樂場招待券）、大補帖或贓物等物品，使二手貨販賣園地變成銷贓園地。

電腦程式依著作權法第五條第十款之規定，為著作權法所稱之著作。故販賣大補帖之行為已觸犯著作權法第九十一條第二項之規定，意圖銷售或出租而擅自以重製之方法侵害他人之著作財產權，可處六個月以上五年以下有期徒刑，得併科新台幣三十萬元以下罰金。且若行為人係以此為職業，即賴以維生者，則依著作權法第九十四條有常業犯之加重規定，可處一年以上五年以下有期徒刑，得併科新台幣四十五萬元以下罰金。而利用網路銷贓之行為，依刑法第三百四十九條第二項之規定，

[35] 一般社會大眾對於非法拷貝之軟體，例如電腦程式軟體、電腦遊戲、影音光碟等均俗稱為大補帖或泡麵。

搬運、寄藏、故買贓物或為牙保者，處五年以下有期徒刑、拘役或科或並科一千元以下罰金。如行為人以之為常業者，依刑法第三百五十條之規定，處六月以上五年以下有期徒刑，得並科三千元以下罰金。

第七節　網路交友之陷阱

第一項　類型

因為網際網之迅速發展與普及，加上網路具有即時性及互動性，因此網路即成為提供現代人交友的另一個途徑，而且網路不受地理空間之限制，即使位於地球的另一端，也可透過網際網路互相傳遞即時的訊息，因此網路交友之便利性，已非傳統之筆友所能比擬。但是由於網路具有隱匿性，任何人可以輕易地在網路上取得虛擬的網路身分，此一特性變成為有心人士從事不法行為之工具，近年來因網路交友而產生之問題不斷增加，產生所謂的「網路約會強暴」及「網路婚外情」。

所謂「網路約會強暴」指透過聊天或交友網站的相互對談，彼此留下聯絡方式，以集體郊遊或兩兩相約等方式約會見面，俟時機成熟始進行強暴等不法勾當。而「網路婚外情」則是指利用網路的交友訊息認識朋友或性伴侶，有些網站公開徵求性伴侶，或提供同性戀、已（未）婚或男（女）性別等選項供不特定之第三人選擇，如換妻(換夫)俱樂部在網路上公然招收會員，這樣的方式易衍生網路婚外情；對未成年的學生而

言，類似這種網路交友、約會的情形，每天都在發生，也許有人幸運，認識了未來的另一半，也許有人不幸，遭受無端的騷擾，甚至危害到生命安全。

第二項 刑事責任

前述之網路約會強暴如為行為人單獨為之，依刑法第二百二十一條之規定，對於男女以強暴、脅迫、恐嚇、催眠術或其他違反其意願之方法而為性交者，處三年以上十年以下有期徒刑。如行為人為二人以上或使用藥劑者，依刑法第二百二十二條之規定，可處無期徒刑或七年以上有期徒刑。而網路婚外情如行為人為有配偶之人而與他人發生性行為時，依刑法第二百三十九條之規定，有配偶而與人通姦者，處一年以下有期徒刑。其相姦者亦同。

第四章　專業類型之網路犯罪及其刑事責任

由於電腦科技之進步，網路世界正逐漸形成，在新的虛擬網路世界中，非法入侵的消息時有所聞，自早期的 Morris 案到近期的五角大廈遭入侵案，網路入侵案之手法，可謂越來越有防不勝防之勢，在美國甚至已經出現反駭客入侵的保險[36]。過去駭客最中意的入侵對象不外是美國五角大廈、中情局、NASA 等機密等級較高的軍方電腦系統。近年來由於電子商務發展迅速，駭客紛紛轉戰著名的大型網站，雅虎不斷受到侵擾攻擊，就是最明顯的例子。有的駭客一戰成名，如九四年俄羅斯駭客侵入花旗銀行，偷走了一千萬美元；但也有失手而鋃鐺入獄，如專門入侵企業網站的著名駭客凱文．米特尼克。在現今的網路環境中，駭客（Hacker）橫行，病毒入侵又屢見不鮮，此項藉由網路之入侵手段而竄改或破壞資料之行為所能造成之危害程度，並非吾人所能預料，而現行法律對此種行為能否加以規範，即有討論之必要。

第一節　電腦系統進入之概念

[36] 參閱蔡美智著，電腦駭客的罪與罰-談網路入侵的法律問題，資訊法務透析，民國 87 年 7 月，頁 17。

電腦系統都設計有安全系統，必須利用通行密碼與其他可供識別身分之方法才能進入電腦系統之內部，此與傳統上人類以門鎖、籬笆、圍牆、守衛來防範居住安寧與隱私權不受侵犯相類似，進入電腦系統之行為與進入住家的情形是否相同？首先必須先對電腦系統進入之概念加以了解。在美國許多州之電腦犯罪法中有十三州對於進入（access）概念採取以下之定義「接近、指示、溝通、儲存資料、取出資料或其他方式使用電腦、電腦系統或電腦網路」[37]。由此可知，電腦系統之進入在概念上與進入住家是有所不同的。access 這個字的原始字義是「接近」，但在美國許多州之立法中已擴大其範圍，尚包括儲存資料、取出資料等使用電腦、電腦系統或電腦網路之行為。

第一項　電腦安全系統之性質

在早期電腦安全的概念較不普及的時候，許多系統都沒有安全措施，但隨著被入侵的事件屢屢發生，現在幾乎所有的系統都有安全措施，例如透過使用密碼來限定資料之存取，使網路之安全性獲得保障，但此種保障並不是絕對的。

在電腦犯罪之具體個案中，行為人之犯意往往難以加以認定，很難判斷行為人進入電腦系統係出於犯罪之故意，但是要進入電腦系統必須經過安全系統之檢測，而電腦之安全系統被設計成當其發現使用者無權

[37] 參閱蔡蕙芳著，電腦犯罪與刑事立法的課題，台大碩士論文，民國 83 年 6 月，頁 68。

使用時，會通知無權使用這項訊息以警告行為人，並阻止行為人進入，行為人如仍執意進入，這項通知會被當成證明行為人明知無權使用電腦仍執意實施犯罪行為之間接證據。而且進入電腦系統不會留下指紋、圖畫、文字等證據，但是安全系統可作記錄。所以美國紐約州及德州之電腦犯罪法將安全系統列入電腦犯罪之成立要件[38]。

第二項　電腦系統進入之性質

進入電腦與之後的犯罪行為間之關係就像侵入住宅竊盜，破解安全系統進入電腦系統內部之行為，與傳統竊賊開鎖行為相似，但是此種行為雖可類比為侵入住宅罪，但實際上並非侵入住宅罪，所以，進入電腦系統在現行法律下是不可罰之行為。在網路入侵的犯罪中，進入電腦系統為犯罪必經之過程，就像縱火罪中行為人必須準備火苗點火是相同的，這種行為是毋須法律規定的，所以，進入電腦系統是網路侵入犯罪之行為之一部，因此，在取得他人資訊或修改資訊或從事電腦詐欺的目的下，從事電腦系統入侵行為則此行為即是犯罪行為的一部，可依據各該行為所該當之構成要件加以處罰，在此論點之下，行為人出於犯罪故意進入電腦系統時，行為便已著手[39]。若電腦系統之進入為電腦犯罪或網路入侵犯罪之必經過程，那麼進入電腦系統之行為是否為刑法上所稱之「不罰之前行為」？所謂不罰之前行為（Straflose Vortat）係指已

[38] 參閱蔡蕙芳前揭文，頁 69。

[39] 參閱蔡蕙芳前揭文，頁 70。

合併在後行為加以處罰之前行為，亦稱為與罰之前行為（Mitbestrafter Vortat）。因為對於在後之主要行為之處罰，已足以涵蓋在前之次要行為，故使前為不罰。雖有前後二行為，在表面上好像是裁判確定前犯數罪，而屬於行為複數之實質競合，可是在事實上，前行為只是後行為之前階行為，故與法律競合同屬一種不純正之競合，只是假性之實質競合（Scheinbare Realkonkurrenz），而可準用法律競合之補充關係處理之[40]。前行為對主行為之關係，大多存在於預備行為，未遂與既遂構成要件之間，危險行為與實害行為之間。基此，惟有將進入電腦系統行為加以犯罪化，則此種行為方有可能與之後的犯罪行為構成不罰之前行為關係。

第二節　未經授權侵入電腦系統

第一項　入侵者

與網際網路關係最密切的電腦濫用行為乃入侵者或稱駭客（hacker），早期這種行為人被稱為 phone freak，freak 在俚語中的用法是用來形容狂熱者或行家，但是負面的意思則係指瘋子般的狂熱者。

[40] 參閱林山田著，刑法通論，民國 83 年 8 月增訂四版，頁 511。

這些人在剛開始侵入電話系統之目的只是要逃避長途電話費用的支付，當電話網路開始子電子接線系統自動化之方式運作時，這種侵入行為便隨之擴張至電腦，由電腦去做接線的工作。而 hacker 通常是指運動場上沒有經驗與技術不佳的人，to hack 這個行為是有不斷地重複不規律或笨拙動作的意思，所以便有人用 hacking 來指「任意地嘗試電話號碼以試圖進入電話系統」的行為。

由於個人電腦日益普及化之原因，使得電腦使用者之年齡層逐年下降，許多心智尚未成熟的小孩及青少年大量介入，形成一種電腦小玩家之次文化，逐漸出現所謂之電腦海盜行為（Computer Piracy），此類玩家以破解他人電腦系統之通行密碼為樂，侵入對方禁區後留下「到此一遊」的標誌或者將對方網頁之內容做更改以嘲笑對方之安全措施，然後拍拍屁股離開，其樂無窮，但卻帶給對方無窮的恐慌。對於這些行為人而言，破解一個複雜的系統與征服埃佛勒斯峰是一樣的。

第一款　利用網路無權侵入他人電腦系統

所謂「無權侵入他人電腦系統」，乃指行為人本無權使用他人電腦系統而卻侵入他人電腦系統以利用其服務之行為[41]。而所謂網路駭客的廣義定義為「行為人未經授權逕行進出電腦系統」，狹義定義為「機構外的行為人(指外賊)蓄意以非法之方式，未經電腦主機所有人或系統管理者的同意而逕行進出電腦系統，並使用高超技術進行不法侵害的電腦玩

[41] 參閱馮震宇、劉志豪前揭著，頁 88。

家」，基本上行為人利用電腦進入網際網路即處於使用狀態，而其只要經過登入（Log in）的程序，即可進入他人之電腦系統，在此階段之前的行為尚非取得他人電腦之服務，必須在行為人透過指令或程式的輸入，並且使用到中央處理單元（CPU：Control Process Unit）及消耗 CPU 的處理時間（CPU Time ）之後才有所謂利用其時間或服務之行為。

再者，利用他人電腦時間或服務之行為，雖然刑法修正草案第三百二十二條之一第二項規定，未經合法授權，擅自使用他人之電腦或其他相關設備者，依前項之規定處斷，其目的即在於欲對電腦之「使用竊盜」類型予以處罰，但民國八十六年刑法修正時並未對此加以修正，以致對於此類型為仍無法加以處罰。然若非僅是單純之入侵並使用電腦，而是對他人之資料擅自儲存取用時，依新修正之刑法第三百二十三條規定：「電能、熱能及其他能量或電磁記錄，關於本章之罪，以動產論」觀之，似可該當竊盜罪[42]。但竊取電磁記錄之行為在解釋上會面臨極大的難題，所謂「竊取電磁記錄」，就文義上之解釋應包括兩種含義，一是電磁記錄之實體，例如磁碟片。另一個則是指電磁記錄所涵的抽象的意識內容。雖然依修正後之刑法第二百二十條第三項的定義，電磁記錄是指以電子、磁性或其他無法以人之知覺直接認識之方式所製成之記錄，而供電腦處理之用者。依此立法之定義，刑法第三百二十三條所謂所謂電磁記錄指的也應該是以電磁方式記錄一定意識內容的實體物。但若此處電磁記錄所指的是電磁記錄的實體物，本屬動產，那麼本來就可以適用竊盜罪中竊取他人動產的文字規定，根本不須增訂此規定。所以本條修正文字中所稱之電磁記錄，立法者所要規範的對象，應該是電磁記錄所內

[42] 參閱馮震宇、劉志豪前揭著，頁 88。

涵之抽象的意識內容[43]。但是如此一來，解釋上也是有根本的困難，申言之，所謂竊取他人電磁記錄之行為，是否該當刑法上竊盜罪的竊取概念？容有疑義。蓋竊盜罪構成要件中的竊取，刑法上的解釋是行為人破壞原持有人的持有支配關係而建立新的持有支配關係[44]。然而此處所謂竊取電磁記錄的情形，事實上指的是以重製之方式獲得該電磁記錄。一方面固然行為人是得到他人的電磁記錄的內容，建立其對於電磁記錄內容的持有支配關係，但是另一方面，電磁記錄之持有人並未因此而喪失他對於電磁記錄內容的持有支配關係。此種電磁記錄事實上之特性，使得所謂竊取電磁記錄根本沒有辦法該當於刑法上竊盜罪的竊取要件，自然不能構成刑法上的竊盜罪。

第二項　刑法侵入住宅罪之適用

對於未經允許而侵入他人電腦系統之行為看似與無故侵入他人住宅之行為相類似，行為人無故侵入他人住宅、建築物或附連圍繞之土地或船艦者，構成我國刑法第三百零六條第一項之侵入住宅罪，亦稱妨害居住自由罪。本罪所保護之法益乃是個人之住屋權（Hausrecht）。所謂住屋權[45]係指個人居住之場所有不受其他無權進入者或無權滯留者之干擾與破壞之權利，故住屋權之重心在於個人對其住屋權所及之範圍有決

[43] 參閱黃榮堅著，刑罰的極限，民國 87 年，頁 318-319。

[44] 參閱林山田著，刑法各罪論（上），民國 88 年，增訂二版，頁 208-209。

[45] 參閱林山田著，刑法各罪論（上），民國 88 年，增訂二版，頁 168-169。

定何人可以進入或停留之自由，個人在其居住處所有不被干擾或其居住安寧有不被破壞之自由。而未經授權侵入他人電腦系統之行為，是否該當刑法上侵入住宅罪之構成要件？按本條構成要件中所規定之行為地以他人之住宅、建築物或附連圍繞之土地或船艦為限，電腦系統是否等同於此等行為地，即有加以討論之必要。

住宅係指供人住宿之房屋，故電腦系統非此處之住宅。建築物乃指圍有牆壁，上有屋頂，可供居住或其他用途之土地上定著物而言，基此，電腦系統亦不屬建築物，更非船艦。而附連圍繞之土地則指附連或圍繞他人住宅或建築物之土地，且其上設有牆垣、籬笆或壕溝、鐵絲網等安全防衛措施者。故刑法第三百零六條所規範之行為地僅為「住宅」、「建築物」、「附連圍繞之土地」或「船艦」，並未包括「電腦系統」，因此在罪刑法定主義之原則之下，目前對於單純侵入電腦系統之行為並不該當侵入住宅罪，而無法以現行之刑法加以處罰。

第三節　電磁記錄之不法使用與消除

第一項　電磁記錄之性質

在網路犯罪中，電磁記錄為犯罪侵害的客體之一，且與網路犯罪之關係密切，蓋其不僅因為違犯方式與傳統刑法上體會之違犯方式迥異，傳統刑法之規定往往無法對於此等行為加以規範，近年來其刑事立法已漸為各國所重視，然究其原因，乃在於對所謂「電磁記錄」之意義及其在刑法上之評價為何，故於探討相關問題前，實有必要對此加以釐清。

第一款　電磁記錄之意義及範圍

電磁記錄之意義，依日本昭和六十二年修正之刑法第七條之二規定：「本法所稱電磁記錄者，謂依電子方式、磁氣方式或其他無法以人之知覺加以認識之方式所製作之記錄，而供電子計算機處理資料之用者。」本條所稱「電磁記錄」非指保存資料之媒體本身，而係指在媒體上特定資料記載之狀態而言，因此，其亦包括程式在內[46]。但是在日本學界仍有部份學者及實務界之判決卻使用與法律條文不同的名詞，以「電磁記錄物」稱之，持此見解之學者認為，所謂「記錄」，乃係指「所記述之事實，須能流傳於後者」，所以記錄本身必須是指能資料記載於特定的記錄媒體上，由此觀點來看，法律條文雖規定「電磁記錄」，實際上應係指「電磁記錄物」[47]。持反對見解者則認為所謂之電磁記錄物會使人誤解其意義係指記載記錄的記錄媒體整體而言，且與文書一樣，都是指物理上固定附著於特定物之記錄，所以電磁記錄一詞較電磁記錄物為妥當[48]。而我國最高法院八十一年度第十一次刑事庭會議決議中亦曾使用「電磁記錄物」之名詞，惟電磁記錄與電磁記錄物乃係不同之概念，因為電磁記

---

[46] 參閱楊富強前揭著，頁 138。

[47] 參閱邱垂發著，不正利用自動設備之研究，輔大碩士論文，民國 83 年 6 月，頁 18。

[48] 參閱邱垂發著前揭文，頁 17。

錄係現代社會資訊化、電腦化所產生的，與傳統上人類之觀念所認知之記錄概念，例如以文字、符號、圖畫等方式，在想像上所得之可能結果未必相同，雖然在想像上可將電磁記錄認定為記錄，但是何種範圍內才是刑法所規範的電磁記錄則會因個人之學識差異與認知不同，產生迥異之認定結果。為解決此一問題，日本現行刑法第七條之二特別明文對於電磁記錄之意義與範圍加以界定。依其規定，所謂電磁記錄必須符合二個要件，首先必須是依電子方式磁氣方式或其他無法以人之知覺加以認識之方式所製作之記錄，所以必須諸如磁氣帶、磁碟片、光碟等依人之無法辨識其存在或狀態者，始符合電磁記錄之定義，所以縱使記錄本身之功用雖在使用於資訊處理上，但若該記錄仍可藉由人之知覺加以確認其存在或狀態者，仍非所謂之電磁記錄，例如打孔卡（Punch card)、條碼（bar code）等；再者必須是藉由電子計算機作為資訊處理之用之記錄，換言之，必須藉由電子計算機之運作，用以處理資訊之演算、檢索等之記錄，才是電磁記錄，例如電腦程式，惟錄影帶錄音帶雖亦符合第一要件，但是因為此等記錄，並非以電子計算機做為資訊之處理，故仍非此處所稱之電磁記錄。

依八十六年十一月二十六日修正之我國刑法第二百二十條之規定，修正最主要的文字是「在紙上或物品上之文字、符號、圖畫、照相，依習慣或特約，足以為表示其用意之證明者，關於本章及本章以外各罪，以文書論。」其次，「錄音、錄影或電磁記錄，藉機器或電腦之處理所顯示之聲音、影像或符號，足以為表示其用意之證明者，亦同」。同時在同條第三項增訂「稱電磁記錄，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記錄，而供電腦處理之用者。」由於社會進步，科技發達，錄音、錄影、電腦之使用，極為普遍，原條文之規定已不足

以適應事實之需要，故予修訂。至於第三項增訂電磁記錄定義為立法解釋，乃係參酌日本刑法第七條之二之立法例，可避免適用時發生爭議。

第二款　電磁記錄之文書性

刑法上所稱之文書，其概念上可分為狹義、廣義及最廣義三者[49]；狹義文書係指以文字或得以文字代替之符號，記載於物體之上之意思表示，且得作為證明一定法律關係或交易上重要事實關係者而言。廣義文書則尚包括圖畫，至於最廣義文書除前二者外，凡在紙上或物品上之文字、符號，依習慣或特約而具有思想之內容者謂之。我國刑法條文中言及文書者甚多，應分別視其規定而認定文書之意義究採何者，由我國修正後之刑法第二百二十條之規定觀之，應採最廣義之文書概念。而學者通說認為所謂之文書須具備有體性、文字性、持續性、意思性及名義性等要件。

文書之意義與要件已如前述，而電磁記錄是否符合刑法上所要求之文書概念，實有加以討論之必要；

第一目　肯定說

日本學界通說採肯定說[50]，認為電磁記錄乃藉由電腦特有之記號（電腦語言），記載表意人的意識內容，而在法律上具有重要性者，且若透過

---

[49] 參閱邱垂發著前揭文，頁 20。

[50] 參閱邱垂發著前揭文，頁 21。

印表機列印出來的話，實與文書之再生性具有一體不可分之關連性。換言之，電磁記錄本身雖然無法目視或閱讀，但可藉由列印，將作為電磁記錄內容之人的思想、觀念之表示，轉換成可目視或閱讀之文書形式出現。再者，由於資訊社會的發展，傳統上以文書方式記載之記錄，以廣泛地被電腦機械記載方式即電磁記錄所取代，若仍固守舊有之觀念，勢必造成偽造或變造電磁記錄之行為排除於刑法規範之外的不合理現象，同時亦會危害社會之交易安全及公共信用。

第二目　否定說

持否定見解之學者認為，電磁記錄無法包含於傳統文書之概念中。日本實務上亦有持否定見解者[51]認為關於刑法上文書之概念，乃係指使用文字或得以文字代替之符號，在某程度永續狀態下記載於物體上之意思或觀念表示，且該表示之內容得證明法律上或社會上生活重要事項者。故依一般所承認之文書概念，將電磁記錄視為文書之觀念是有問題的。所謂之電磁記錄並非表現於有體物上，只不過是帶有「正負」的磁氣而已，若將這種磁氣視為得以文字代替之符號，則未免過度擴張文書之概念。學者並認為肯定說所言「電磁記錄藉由印表機之列印，實與文書之再生性具有一體不可分之關連性」之概念，實際上乃是為了維持傳統之文書概念，而將文書之前階段或文書之材料亦視為文書，基此立論所設定之文書適用範圍，顯然是有疑問的。

[51] 參閱邱垂發著前揭文，頁 22。

第三目　小結

我國刑法第二百二十條之規定，按照我國學說及實務之說法，本條乃係「準文書」之規定，換言之，這樣的東西本來並不是文書，只不過立法者透過本條之規定，將其視為刑法上之文書。而電磁記錄是否為刑法上所稱之文書？事實上我們可以開機開啟檔案，讓儲存在磁碟上的資料以我們可以理解的文字符號在螢光幕上顯現出來，所以磁碟上儲存的資料好像是符合了上述文書的定義。在從電腦處理磁碟資料的功能以及保護電腦資料安全的必要性來看，似乎也應該把儲存在磁碟上的資料歸納到文書的範圍裡去。但是如果仔細的分析實際的情況，亦即電磁記錄的存取過程，我們是在電腦的螢光幕上才能理解磁碟上儲存的資料內容。至於磁碟本身的上面，並沒有我們可以理解的東西，因為磁碟上的電磁記錄的本身並不是任何方式的文字符號的直接縮影，而是透過轉化的過程，藉由電磁脈衝以及人的肉眼看不到的磁化點記錄在塗有氧化鐵的底板上。我們之所以無法理解這樣的記錄，主要並不是因為它細小的肉眼無法看見，而是因為上面所存在的根本就不是任何文字符號。如此，雖然顯現在電腦螢光幕上的是文字符號，但是附著在磁碟上的並不是文字符號，根據學說及實務對於文書概念的定義，電磁記錄都不是刑法上所稱的文書，也不是所謂的準文書[52]。為解決此一問題，八十六年十一

[52] 參閱黃榮堅著，電腦犯罪的刑法問題，台大法學論叢，25 卷 4 期，民國 85 年 5 月，頁 202。

月二十六日修正之我國刑法第二百二十條之規定，除將電磁記錄列為準文書之外，並將電磁記錄之定義增訂立法解釋，修正之目的，顯然是為了彌補原來的文書定義無法包括具有文書功能的非文書，以避免利益保護上的漏洞，並杜日後適用上之疑義。

增修條文上的文字，大致上已有立法例可尋，然必須特別注意的是，雖然電磁記錄可能是文書，但並不是所有的電磁記錄都是文書。因為關於文書，除了它存在的形式要件以外，還有更重要的二個要素，第一是該電磁記錄必須足以為表示其用意之證明，第二則是必須與權利或義務有關或法律交往所形成之法律關係具有重要性之事實為思想內容。換言之，電磁記錄之內容必須要使人可以理解，製作人藉著這一些東西是要傳達什麼意思，而意思的內容必須與社會的交易安全與信用有關。這裡所謂的意思傳達的技術是某一些符號依習慣或特約可以指涉某一些固定的對象，也就是約定成俗的表達技術。因此，如果不是透過約定成俗的表達技術，即使是電磁記錄也不是刑法上所稱之電磁記錄。例如電磁記錄如果是一張一般的圖片，那麼因為圖片無法傳達什麼經過約定的固定的意思，所以它不是文書。同理可推，電磁記錄的內容如果是電腦程式，那麼它也不是文書。因為電腦程式根本不是給人和人之間來傳達意思用的。

第三款　電磁記錄之有價證券性

有價證券乃屬有關權利義務的文書之一，係財產權之化身，在經濟交易上與貨幣有相同之作用，故刑法將偽造文書及偽造有價證券，予以

分別規定。有價證券之意義，學說不一，其種類、名稱亦因性質不同而異。一般以有價證券，為有一定價值之權利證書。凡欲實行券面所表示之權利時，必須佔有該證券。即權利行使與證券佔有，兩者不可分離[53]。換言之，有價證券必須具備財產性、占有性，至於是否須具有流通性為必要則有爭議[54]。

在電磁記錄中與有價證券之關係最密切的莫過於「電話卡」與信用卡，故本文即以此二者為例加以討論。按公共電話卡（以下簡稱電話卡）係由電信事業機構發行，乃卡式電話機預付使用費的一種卡片，於卡片中，儲存著可利用之金額（或度數）之電磁記錄（或光線折射密碼），卡片插入電話機中，其可使用之金額即可經由電話機中之計算器（或讀卡機）顯示出來，使利用者得以明確知悉其尚有可使用之金額若干。信用卡則是消費者向發卡機構訂定契約，由發卡機構發給消費者卡片，消費者得憑發卡機構發行的卡片，向特約商店，以簽字記帳之方式，購物、取得服務或享受其他利益，無須以現金付款，由發卡機構向特約商店付款，嗣日後於一定期間向發卡機構繳款結帳之一種記帳消費方式。而信用卡上均有磁條以記錄卡片之卡號、授權碼、有效期限、信用額度等資料，此等資料均係以電磁記錄之方式記載於磁條上，可藉由特約商店之刷卡機讀取資料。目前我國社會已逐漸進入以信用卡為塑膠貨幣（PLASTIC MONEY）之時代，而其發展無遠弗屆。故對於信用卡的法律性

---

[53] 參閱陳煥生著，刑法分則實用，民國 79 年 10 月修訂版，頁 191。

[54] 採肯定說者有褚劍鴻，採否定說者有甘添貴、蔡墩銘、林山田；實務見解原採肯定說後改採否定說。

質是否為有價證券即有加以探討之必要[55]。

第一目　電話卡

關於電話卡是否為有價證券，在日本的學說及實務上之見解分歧不一，頗多爭議[56]。持肯定見解者認為電話卡應屬刑法上有價證券之概念，但所持之立論及範圍仍有不同，一說認為電話卡之磁氣部份即是有價證券，換言之，即電磁記錄本身就是有價證券，因為刑法上有價證券的本質在於「權利的化身性」，故證券上能表示財產上之權利者，即具有「權利的化身性」特色，此外，權利的行使與證券之占有亦必須合一者，亦為有價證券之特色。因此，電話卡乃係藉由卡片上之磁氣資訊，而將權利有體化，再者該權利之行使與電話卡之占有具有不可分之關係，所以

---

[55] 據統計國內信用卡包括威士（VISA）卡、萬事達（MASTER）卡、美國運通（AMERICAN EXPRESS）卡、大來（DINERS CLUB）、吉世美（JCB）卡及聯合信用卡，國內卡之發卡量及簽帳金額亦逐年快速成長，七十六年間信用卡之發卡數約三十三萬六千張、流通卡數約二十二萬四千張、簽帳金額亦僅約新台幣六十三億七千八百萬元，至八十三年間信用卡之發卡數已達四百三十四萬八千餘張、流通卡數約二百七十一萬五千張、簽帳金額約新台幣一千三百一十五億伍千三百萬元，迄八十六年二月止，國內信用卡之發卡數已超過九百六十四萬張，流通卡數約五百八十萬張，簽帳金額約新台幣二千七百二十四億零九百萬元，而八十六年一月份之單月簽帳金額即高達三百一十億八千萬元，平均以每年百分之三十之速度成長。

[56] 參閱邱垂發著前揭文，頁 27-29。

應認為電話卡是有價證券；另一說則認為電話卡有可理解之形狀、外觀，而且基於表示於卡片上的利用度數，可以藉由電話機顯示出剩餘度數，所以電話卡乃表示財產上之證券，具有有價證券性，且應將包含磁氣部份之全體視為有價證券。至於日本實務上亦有認為「做為刑法所規定偽造變造有價證券客體的有價證券，係指能於證券上表示財產上的權利，而且該權利之行使必須占有該證券。電話卡不但得利用卡式公共電話機顯示財產上的權利，且權利的行使必須占有該電話卡，所以電話卡該當於刑法上所稱之有價證券，是毫無疑問的」。

持否定見解者認為刑法偽造有價證券罪是偽造文書罪之特別規定，基於此點，有價證券必須為文書，但依昭和 62 年刑法修正條文之規定，將電磁記錄與文書做區別而將其規定為準文書，所以電話卡的磁氣部份既然並非文書，自不得謂電話卡為有價證券。日本實務上亦有採此見解者。

按有價證券係表示財產權利之書證，為文書之一種，且其權利之行使與該證券之占有必須合一，至於是否需具有流通性，我國學說通說及實務最近見解則採否定看法。因此，電話卡之行使與占有電話卡具有不可分離之關係在認定上固無疑問，但電話卡是否具有文書性，則是問題之關鍵。電話卡雖由外觀上無法以肉眼辨識卡片上磁氣部份所記載之表示內容（可使用之度數或金額），但當卡片插入電話機後，經由電話中之讀卡機（計算器）的作用，即可顯示卡上磁氣部份之表示內容，因此，電話卡上之磁氣部份乃是電磁記錄，依刑法第二百二十條第三項之規定具有文書性。否定見解以有價證券必須為文書為前提，而電磁記錄為準文書而非文書之論點否定其為有價證券，此種看法頗值商榷。因為對於主張「有價證券不一定屬於文書」之概念者，否定說此種推論未必正確。

再者，電磁記錄係具有文書功能的非文書而經由法律規定之擬制，將其視為刑法上的文書，故其文書性應不容置疑，由此看來定說之見解應不足採。至於肯定說之見解，一般有價證券應從證券之外觀及其全體特徵之觀察，並判斷證券之作成是否由真正作成權限者所為，以決定真實權利是否已被轉化（即權利之化身性），所以不能僅從證券之特定部份來肯定權利之化身性。此外，電話卡之磁氣部份只不過是啟動卡式公共電話機或是顯示剩餘金額之磁氣資訊的媒介物，若將此磁氣部份認為是權利之化身，則與有價證券的本質在於將無形之權利予以化身為有體物的目的有違。換言之，對於電磁記錄此種資訊電腦化之新應用媒體，我們在思考其文書性及有價證券性時，應就其應用方式加以全體觀察，不能囿限於電磁記錄使用上之某一階段來肯定或否定其文書性及有價證券性。故我們在判斷電話卡之權利表示性時，應綜合卡面表示部份及磁氣記錄部份所磁印之剩餘金額加以考慮。

第二目　信用卡

信用卡之持有人得使用信用卡向特約商店簽帳消費，而特約商店有接受持卡人簽帳消費之義務，而信用卡之行使與信用卡之占有具有不可分離之關係，由此觀之，信用卡乍看之下似為有價證券。惟信用卡並非表示特定財產權，而僅表示持卡人為加入發卡機構之信用卡契約之會員，有使用信用卡消費之資格而已。換言之，信用卡係信用卡聯合處理中心制作，經由發卡機構發給其持卡人之資格證明書，持卡人提示信用卡僅證明其為發卡機構之會員而已，並非行使信用卡上所表彰之權利。

從而，信用卡並非有價證券，僅屬刑法第二百十二條所定有關能力服務或其他相類之證書者[57]。信用卡雖非有價證券，惟持卡人如不提示信用卡，即不能對特約商店簽帳消費。反之，雖非合法之持有人，但是如其提示信用卡而未經特約商店查覺者，仍得消費簽帳。故信用卡具有與現金相同之經濟上功能。從而信用卡實具有財產上之價值，而為財物之一種，得為竊盜、強盜、詐欺、侵占等財產上犯罪之客體。

第三目　小結

電磁記錄之應用於現代資訊社會中，非常廣泛，因此對於其意義與範圍必須有一明確之標準，修正後之我國刑法第二百二十條已對此加以規定。尤其是藉由電磁記錄之定義，我們便可以了解其規範之範圍為何，亦即必須以電子、磁性或其他無法以人之知覺直接認識之方式所製成之記錄，而供電腦處理之用者，基此，電話卡及信用卡上之磁氣部份均為刑法上所稱之電磁記錄。關於電磁記錄之文書性及有價證券性，雖然於日本引起頗大之爭議，且關於文書性之問題亦於日本刑法中加以增訂，但日本學界及實務上迭有不同之意見。我國刑法已於第二百二十條增訂電磁記錄為準文書及其定義之規定，雖然電磁記錄可能是文書，但並不是所有的電磁記錄都是文書。因為關於文書，除了它存在的形式要件以外，該電磁記錄還必須足以為表示其用意之證明。換言之，電磁記錄之

[57] 參見最高法院七十年台上字第三七四三號判決，認為信用卡屬資格證券之一種，最高法院刑事裁判選輯第二卷第四期第八頁。

內容必須要使人可以理解，製作人藉著這一些東西是要傳達什麼意思，如此方能具備文書性。

但是值得深思的是，是否具有文書性之電磁記錄即具有有價證券性？按具有文書性之電磁記錄種類繁多，然以最常見之電話卡、信用卡、影印卡、提款卡而言，電話卡具有價證券性已如前述，至於影印卡與電話卡之功用，雖然提供勞務上或有差異，但使用本質上並無不同，故亦可肯定其有價證券性。而信用卡並非表示特定財產權，而僅表示持卡人為加入發卡機構之信用卡契約之會員，有使用信用卡消費之資格，故僅屬一種資格證券，不具有價證券性。惟提款卡之使用，須持卡人先於金融機構或郵局內開立帳戶，並於帳戶中存入一定之金額之存款，後藉由提款卡之申請及利用，以使用其帳戶內之存款。由此觀之，持卡人在金融機構或郵局內之金錢債權與該提款卡之占有及利用，具有相當密切不可分之關係，似乎具有有價證券性。但是有價證券若喪失或毀失則證券上所表彰之財產權便隨之消滅，惟在提款卡之情形，若提款卡因故喪失（例如遭竊）占有或毀失（例如毀損），持卡人除得依相關途徑救濟外（例如掛失、申請補發），其於金融機構或郵局內之金錢債權仍得提出其他證據加以行使（例如存簿及印章），並不當然消滅。所以提款卡雖具文書性並不具有價證券性。

第二項　篡改他人資料之行為

行為人入侵電腦系統並竄改他人之電磁記錄之問題，攸關網路安全之維護。例如民國八十三年底至八十四年七月間，EPSON 公司連續被一名離職工程師，熟知該公司所有電腦網路結構、超級使用者帳號與密碼，

利用網路連線侵入該公司之元件資料庫[58]，擅自將其底稿設計製造之元件資料予以更改，致使該公司在不知情的情況下，根據此底稿而設計製造出錯誤之晶片無法使用[59]。

此處所稱之「竄改」與刑法上所稱之「變造」相當，故竄改他人電磁記錄之行為是否該當刑法上變造私文書罪，其關鍵在於「電磁記錄」是否為刑法上所稱之文書？在刑法修正前，最高法院曾作出決議，認為「非不可視為刑法所保護之文書」[60]，而修正後之刑法第二百二十一條第二項已明文規定「錄音、錄影或電磁記錄，藉機器或電腦之處理所顯示之聲音影像或符號，足以為表示其用意之證明者」，為刑法上之準文書，若是更改、刪除電腦中之資料僅是變更原電磁記錄中內容之一部分，則可能構成變造文書罪。如果因電磁記錄更改始有其內容，則可能該當偽造文書罪；又若其行為是毀棄損害或致令不堪使用者，則可能成立刑法第三百五十二條第一項之毀損文書罪。至於竄改之行為是否該當「足以生損害於公眾或他人者」之構成要件，仍須視個案而定。以往實務上認為只要有「損害之虞」為已足，並不以實際發生損害為必要[61]，因此，若更改他人電腦中之資料，只要被害人若不知情而加以處理即會產生損害，則可認為有損害之虞，而已該當「足以生損害於公眾或他人者」之構成要件。

---

[58] 所謂元件資料庫是指用來設計晶片之積體電路佈局的基礎程式。

[59] 參閱蔡美智著，談網路犯罪，資訊法務透析，民國 88 年 1 月，頁 36。

[60] 參照最高法院 81 年 9 月 8 日八十一年度第一次刑事庭決議。

[61] 參照最高法院 22 上字第 874 號判例、最高法院 26 上字第 1432 號判例、最高法院 47 台上字第 358 號判例。

又對於個人資料加以竄改時，依電腦處理個人資料保護法第三十四條之規定，意圖為自己或第三人不法之利益或損害他人之利益，對於個人資料檔案加以非法輸出、干擾、變更、刪除或以其他非法方法妨害個人資料檔案之正確，致生損害於他人者，可處三年以下有期徒刑、拘役或科新台幣五萬元以下罰金。因此變更、刪除他人電腦中之資料，若為個人資料，且因該等行為而致生損害於他人時，行為人即有刑責。

惟若其更改、刪除之電磁記錄係受著作財產權保障之著作或是有著作人格權之著作時，依著作權法第九十二條之規定，擅自以公開口述、公開播送、公開上映、公開演出、公開展示、改作、編輯或出租之方法侵害他人之著作財產權者，可處六月以上五年以下有期徒刑，得併科新台幣三十萬元以下罰金。又著作權法第十七條規定，著作人享有禁止他人以歪曲、割裂、竄改或其他方法改變其著作內容、形式或名目致損害其名譽之權利。違反者，依著作權法第九十三條第一款之規定，可處二年以下有期徒刑，得併科新台幣十萬元以下罰金。但著作權法第九十二條所稱之「改作」必須是另為創作，若不是另有創作，則基於罪刑法定主義之要求，應無著作權法第九十二條之適用。

第一款　刑法偽造、變造文書罪之適用

所謂「偽造」係指無製作權者製作虛偽文書而言，即假借他人名義，而製作在外形上足以使人認為係出自作成名義人之具有不真實性之文書。行為人必須為無製作權人而假借或捏造他人名義而製作文書，方能構成本罪之偽造行為，故行為人若係有製作權而以自己名義而製作，自

無偽造可言，縱所製作之文書內容與其真意不符，且涉及他人之權利，亦非本罪之偽造。又如行為人對於文書本有製作權，縱令其不應製作而製作，因係以自己名義而製作，故無偽造之可言。反之，行為人對於文書本無製作權，縱係以自己名義而製作，則有可能成立本罪之偽造。又行為人若串令他人冒用自己名義作成文書，縱使所載不實，仍屬虛妄行為，亦非本罪之偽造。由於我國刑法對行為結果之限制規定，故虛偽文書必須足以生損害於公眾或他人，方能構成本罪。因此，行為人之行為雖可該當本罪之偽造行為，但其行為結果若不足以生損害於公眾或他人者，亦不構成刑法上之偽造文書[62]。

所謂「變造」乃指無權修改文書內容者，擅自更改填寫真實文書之內容而言，故變造之行為客體必須為真實文書。行為人必須為無權修改文書所載內容之人，故有更改權之人或無更改權之人事先已得有更改權人之同意或授權者，在其權限範圍內修改文書內容之行為，自非刑法上變造行為。又共同制作之文書，其部份制作人未經全體之同意，而擅自更改文書之內容，亦足以構成變造。原則上，文書之原制作人可能具有更改權，但文書作成後，原制作權人亦可能喪失此等更改權，故雖為自己制作之文書，但對該文書業已喪失更改權者，若擅自更改文書內容，自亦可構成變造。行為人必須就本為真實之文書而為竄改，方能構成刑法上之變造行為，故若就本為虛偽之文書而加以修改，則非變造，而可能成立偽造。至於行為人所竄改之真實文書，係他人名義或係自己名義？則非所問。真實文書經變造後，其「證明資格」與「文書品質」，並不因之完全消失，否則，真實文書之證明資格或文書品質，若竟因變造行為

[62] 參閱林山田著，刑法各罪論（下），民國 88 年，增訂二版，頁 588-592。

而完全消失者，則非變造，而為偽造[63]。

偽造或變造文書之結果必須足以生損害於公眾或他人者，始構成偽造、變造文書罪，否則，如行為之結果並不足以生損害於公眾或他人者，自不負本罪之刑責。偽造或變造文書之結果有發生損害公眾或他人之虞時，即可認定為足以生損害於公眾或他人，而構成本罪，而不以公眾或他人果已遭受損害為必要。簡言之，及偽造或變造行為實際上以否發生損害？並不影響本罪之成立。至於偽造或變造行為之結果，是否足以生損害於公眾或他人？則應就案件之具體情狀而為判斷。行為人之偽造或變造行為完成後，若其行為結果有足以生損害於公眾或他人之危險者，即可成立本罪，而不可以行為人尚未將其偽造或變造之虛偽文書提示於人，或尚未達於行使之階段，即認定為不足以生損害於公眾或他人。又行為人所偽造或變造之虛偽文書，即使假定為真實文書，其在法律上亦為無效者，則對於此等偽造或變造行為是否有足生損害於公眾或他人之虞，亦應就實際之行為情狀而為判斷，不可僅以該虛偽文書即使為真實文書亦為無效之事實，即判定偽造或變造之結果不足以生損害於公眾或他人[64]**。**

偽造或變造行為之結果所生之損害究為民事上之損害？抑或其他損害？均不影響本罪之成立。所謂之損害亦不以經濟價值者為限，其他非經濟價值之損害，亦可該當本罪之損害。又偽造或變造之行為所生之

---

[63] 參閱林山田著，刑法各罪論（下），民國 88 年，增訂二版，頁 594-595。

[64] 參閱林山田著，刑法各罪論（下），民國 88 年，增訂二版，頁 596-598。

損害，並不以真正名義人為限，凡因偽造或變造行為而足以蒙受損害者，即為本罪之被害人。此外，偽造或變造行為完成後，有足以生損害於公眾或他人之虞者，即足以成立犯罪，雖真正名義人事後表示追認，亦不影響業已成立之罪名[65]。

第二款　刑法毀損罪之適用

毀棄損壞罪乃行為人故意毀棄或損壞他人之物之財產罪，係侵害財產法益之一種特別形態，行為人只要出於故意，而毀棄損壞他人之物即為已足，不以取得他人之物，或獲取利益為必要，故與其他財產罪顯然不同。本罪之刑法條款乃保護財物不為他人之故意行為所侵害，其所保護之內容即是「物之保全利益」。

第一目　刑法毀損文書罪之適用

行為人毀器、損壞他人文書，或致令不堪用，足以生損害於公眾或他人者，構成刑法第三百五十二條之毀損文書罪。本罪之行為客體是他人之文書，係指屬於他人所有之文書，易言之，即指處分權屬於他人之文書，至於文書係由何人制作？則非所問，即使由行為人制作之文書，但該文書已為他人所有，亦為他人文書，而可成為本罪之行為客體。

---

[65] 參閱林山田著，刑法各罪論（下），民國 88 年，增訂二版，頁 598-599。

在紙上或物品上之文字、符號、圖書、依習慣或特約，足以為表示其用意之證明者，依刑法第二百二十條之規定，關於本章及本章以外各罪，以文書論。而錄音、錄影或電磁記錄，界機器或電腦之處理所顯示之聲音、影像或符號，足以為表示其用意之證明者，依同條之規定亦同。

本罪之行為有三，即毀棄、損壞及致令不堪用。行為人只要實施三種行為中之任何一種，即足以構成本罪。所謂毀棄係指毀滅拋棄而根本毀滅文書之存在，如將他人之文書全部燒毀。所謂損壞則指損害破壞文書，使文書之外形為之改變，並減低文書之效用等，此與毀棄而使整個文書滅失，在程度上顯然有別。所謂致令不堪用，係指損壞以外之足使文書喪失其效用之行為，如塗改文書之內容而使文書失效。

行為人之行為必須足損害於公眾或他人，方能構成本罪，故若行為並不足以產生損害公眾或他人之行為結果，自不負本罪之刑責。行為人之行為只要足生損害於公眾或他人即為已足。換言之，即行為有損害之虞，即足以該當此一構成要件，並不已行為實際業已發生損害為必要。至於判斷行為人之行為，是否有此行為結果，並不以公眾或他人之財產法益，有無遭受損害之虞為限，即使在其他之公私權利義務關係上，於客觀上具有遭受行為損害之危險者，亦可成立本罪。

第二目　刑法毀損器物罪之適用

行為人毀棄、損壞文書、建築物、礦坑或船艦以外之他人之物或致令不堪用，足以生損害於公眾或他人，構成刑法第三

百五十四條之一般毀損罪。

本罪之客體為文書、建築物、礦坑或船艦以外之他人之物，其範圍相當廣闊，包括動產與不動產、有體物或無體物、動物、植物或礦物、氣體、液體或固體，且不以具有經濟價值之物為限，即使係毫無經濟價值者，如一張古老破舊之照片，或一封亡友之書信等，也與一部價值數百萬之汽車，同樣受到本條款之保護，故凡他人對之認為有保全利益之物，即可成為本罪之行為客體。

所謂他人之物係指非自己所有，而屬於他人所有之物，包括他人單獨所有，或自己與他人共有，或他人與他人共有，但不包括無主物。又他人包括自然人與法人。此外，雖為他人之物，然卻屬刑法毀棄損壞罪章中以外之其他罪名之行為客體，則應適用各該罪之條款加以處斷，此自非本罪之行為客體[66]。

本罪之行為有三，即毀棄、損壞及致令不堪用。行為人只要實施三種行為中之一種，即可構成本罪。所謂毀棄係指毀滅或拋棄而根本毀滅物之存在，如將他人之物燒毀，或將他人之物拋沉大海中，或將他人之動物殺死是。毀棄有時可能係一種嚴重程度之損害，使物對於特定目的之可用性完全滅失，如洗掉錄有特定聲音之錄音帶。所謂損壞乃指損害或破壞，使物之外形發生重大之變化，並減低物之可用性。至於多數之物組合而成之組合物，則只要減低其組合目的之「使用能力」即可認定為損壞。原則上可認為行為人之作為或不作為而對物發生作用，因而使物之性質、外形及特定目的之可用性，較其原來之狀態，顯有不良之改

[66] 參閱林山田著，刑法各罪論（上），民國 88 年，增訂二版，頁 420。

變者，即為本罪之損壞[67]。

所謂致令不堪用係指損壞以外之足使他人之物喪失其特定目的之效用，如將手錶分解成無數之細小零件、或以油彩塗污名畫或肖像，或插入外物或取出零件使機器無法運轉、或以不易清刷之油漆在建築物之牆上塗寫標語、或以強力膠貼標語於他人建築物上，所有人須花費相當時間或金錢，方能清刷者。此外將他人汽車、摩托車之輪胎放氣，雖然輪胎本身並未受損，但汽車或摩托車作為交通工具之可用性將為之喪失，所有人雖可另行打氣而恢復此等可用性，但須花費相當之時間與金錢，故可認為係本罪之致令不堪用。

行為人單純把他人之物移離物之原有位置，而對之並不加以毀損，他人之物之性質、外形及其功能並無任何不良之改變，自不該當本罪之行為，如將他人之戒指藏匿所有人住宅中不易發現之處，或把集郵者之貴重郵票挾入書頁中，而放置於集郵者之書架上等，此等行為僅為民法上損害賠償之問題，而不成立本罪。惟若行為人之藏匿行為，將必然地造成該物之損害，或滅失之結果，如將生銹或受潮即失效之物藏匿於潮濕之處，或將戒指藏於垃圾桶之中，則仍可構成本罪。

行為人之行為必須足生損害於他人，方能構成本罪。行為人之行為只要足生損害於公眾或他人即為已足，不以行為實際已生損害為必要。換言之，行為人只要實施毀損行為，公眾或他人將有遭受損害之虞者，即可成立本罪，而不可以行為尚未發生實害，即認為係本罪之未遂之行為，因本罪不設未遂犯之處罰規定，故為刑法所不處罰之行為。實務上則認為若行為人之毀損行為並未發生實害之結果，因本條之罪並無處罰

[67] 參閱林山田著，刑法各罪論（上），民國 88 年，增訂二版，頁 421。

未遂犯之之規定，自不應加以處罰[68]。此種見解乃基於本罪之構成要件以使所毀損之物，喪失全部或一部之效用之立論所推演出來之結果，但卻忽略條文之規定尚有「足生損害於公眾或他人」之構成要件，而非規定「致生損害於公眾或他人」，故實務之見解不無可議之處。

第四款　刑法妨害公務罪之適用

由於社會不斷地發展，政府的事務亦不斷地增加，而在現代電腦科技不斷發展之下，企業界已經大量電腦化以應付日益龐大的工作量及資料處理，政府其實也與企業界一樣面臨日益龐大的工作問題，為增加行政效率，節省處理時間以及便利民眾，只有電腦化才能解決此一問題。由電腦負責通訊工作和資料的存收與處理，許多行政機構利用電腦製作檔案，例如電話費、電費、水費通知單等都是利用電腦處理與列印出來。在我國政府推動業務電腦化已有多年，而為應付現代多元之社會，人民與政府間的頻繁互動，政府對於攸關人民權利義務關係的各種資料如戶籍、學籍、護照、牌照、權狀、憑證、檢驗文件、決定書等的資訊系統都是政府規劃發展的項目，目前各項為民服務電腦化系統正在積極推動中，另一方面戶政機關與監理單

[68] 參見最高法院四十七年臺非字第三十四號判例，本判例認為被告潛至他人豬舍，投以殺鼠毒藥，企圖毒殺豬隻，惟其企圖毒殺之豬既經獸醫救治，得免於死，則其效用當無全部或一部喪失情事，且本條之罪，又無處罰未遂犯之規定，自應為無罪之諭知。

位亦透過電腦連線之方式使得作業程序簡化，而民眾亦不須往返奔波。同時，隨著網際網路之發展與普及，預期至九〇年代，政府的服務工作將有突破性的改變，目前先進國家發展中之「一處交件，全程服務」的嶄新服務方式，將會逐漸為行政機關所採用。

如果以網路侵入之方式造成行政機關之電腦當機，甚至使處理中之資料全部滅失，來干擾或妨害公務之進行，是否有刑法妨害公務罪之適用？即有加以討論之必要。

第一目　妨害公務執行職務罪

行為人對於公務員依法執行職務時，施強暴脅迫者，構成刑法第一百三十五條第一項之妨害公務員執行職務罪。故本罪之行為為施強暴脅迫而妨害公務員執行職務[69]，行為人必須對公務員實施強暴脅迫，始構成本罪，否則，若對公務員並無強暴脅迫之情事，縱對公務員之職務行為有所妨害，亦不負本罪之刑責。而意圖使公務員執行一定職務或妨害其依法執行一定職務或使公務員辭職，而施強暴脅迫者，則構成刑法第一百三十五條第二項之強制公務員執行職務或辭職罪。

所謂「強暴」乃只逞強施暴，使他人無以抗拒。行為人可能以有形體力或其他行為，造成被害人一種心理上或生理上被強制之狀態，而足

[69] 此處的執行公務乃指公務員行使高權的統治行為而言。

以妨礙被害人之意思決定自由與依其意思決定而行動之自由[70]。學說上區分強暴為直接強暴與間接強暴等兩種型態，前者係指以身體的強制力直接強制行為客體，達成行為目的[71]；後者則是行為人間接地對行為客體以外之第三人，或行為客體之所有物，施以強暴，而得強制行為客體，依照行為人之指示做成意思決定作為、不作為或忍受。

所謂「脅迫」乃以言詞或舉動，顯示加害他人之意思，或以加害他人之意思通知他人，使其產生畏懼，而得加以威脅或逼迫[72]。脅迫與前述之間接強暴有所區別，脅迫用以威脅行為客體之惡害乃是不久將來之未來惡害，但是間接強暴則為現時存在之惡害。換言之，脅迫可能發生之惡害只是未來的一種可能，但是間接強暴之惡害則為現在業已發生。

而以網路侵入之方式，竄改行政機關電腦系統內之資料，進而導致行政機關之電腦當機，無法正常運作，進而妨害行政機關行使其高權之統治行為時[73]，亦是對於公務員之執行職務加以妨害，由前述可知，此等行為並不該當刑法上妨害公務罪中有關強暴、脅迫之構成要件，如此便產生處罰上之漏洞。因為這種非強暴脅迫之行為方式，雖然表面上是和平的手段，但是在今日行政機關全面電腦化之情形下，其所造成之危害遠甚於傳統妨害公務罪所規範之個別暴力行為，所帶來的影響是全面

---

[70] 參閱林山田著，刑法各罪論（上），民國 88 年，增訂二版，頁 141。

[71] 此有兩種可能性，一種是剝奪行為客體之意思活動，另一種則是排除行為客體之意思形成。

[72] 參閱林山田著，刑法各罪論（上），民國 88 年，增訂二版，頁 142。

[73] 例如行為人由網路侵入稅捐稽徵機關電腦系統進行破壞，使得電腦當機停擺，無法利用電腦處理對於人民課稅的的統治行為時。

性的，實值吾人加以注意。

第二目　毀損公務上掌管之文書物品罪

按行為人毀棄損壞或隱匿公務員職務上掌管或委託第三人掌管之文書、圖畫、物品或致令不堪用者，構成刑法第一百三十八條之毀損公務上掌管之文書物品罪。本罪之行為客體為公務員職務上掌管或委託第三人掌管之文書、圖畫或物品，可能成為本罪行為客體之文書、圖畫或物品雖不必為公文書或公物，亦不問其所有權屬誰？但必須為公務員職務上掌管或委託第三人掌管者，故如非公務員職務上所掌管或委託第三人掌管之文書、圖畫或物品，即不能成為本罪之行為客體，若對之加以毀棄、損壞或隱匿，自不構成本罪，而應依刑法第三百五十二條毀損文書罪或刑法第三百五十四條一般毀損罪處斷。

稱「公務員職務上掌管」係指公務員基於職務關係而掌管，「委託第三人掌管」則指公務員基於職務關係而委託第三人代為掌管之而言，故公文書或物品已發交私人持有者，即非委託第三人掌管，或如因私人關係而委託保者，自亦不能成為本罪之行為客體。又所謂「第三人」當係包括自然人與法人。

本罪之行為有四，即：毀棄、損壞、隱匿、致令不堪用。何謂「毀棄」，「損壞」或「致令不堪用」解釋上均與毀損文書罪之解釋相同，在此不再贅述。稱「隱匿」係指隱匿行為客體，而使人不能或難於發現其所在。而且行為人只要有四種行為中

之一種，而不待任何結果之發生，即足以構成本罪。此與刑法第三百五十二條毀損文書罪及刑法第三百五十四條一般毀損罪尚須具足生損害於公眾或他人之行為結果方能成罪之情形不同。此外，本罪為毀損罪之特別條款，故行為一旦該當本罪即無另構成毀損罪之餘地。

依新修正之刑法第二百二十條之規定：「在紙上或物品上之文字、符號、圖書、依習慣或特約，足以為表示其用意之證明者，關於本章及本章以外各罪，以文書論。」且「錄音、錄影或電磁記錄，藉機器或電腦之處理所顯示之聲音、影像或符號，足以為表示其用意之證明者，亦同。」而所謂「電磁記錄」依刑法第二百二十條第三項之規定係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記錄，而供電腦處理之用者而言。因行政機關全面電腦化之原因，許多資料之處理與儲存均依賴電腦，故如行為人所竄改之資料符合「錄音、錄影或電磁記錄，藉機器或電腦之處理所顯示之聲音、影像或符號，足以為表示其用意之證明者」之要件者，即為刑法上之準文書，又此等準文書係公務員平時處理公務時，藉由電腦操作所製作，解釋上應為公務員職務上所掌管，故行為人之行為可依刑法第一百三十八條處斷。惟若行為人所竄改之資料僅為電腦程式而並無足以表示其用意之證明者，即非刑法第二百二十條所謂之準文書，即無刑法第一百三十八條之適用餘地。於此即出現處罰之漏洞，應立法加以補救。

第五款　刑法公共危險罪之適用

妨害資料處理程序之方法有兩種，一種是資料變更，另一種則是以破壞、損壞資料處理設備或者資料媒體的方法，即物理力的方式，如以物理力對於電腦硬體設備之侵害。若對於大眾運輸系統、交通管制系統之電腦控制程式加以變更影響其正常運作，此等行為是否構成刑法公共危險罪章之罪名，亦值得我們加以注意。

第一目　刑法第一百八十四條之適用

台北捷運木柵線在馬特拉公司與台北市政府的談判破裂後，於八十五年六月三日旋即發生捷運系統行控中心的當機事件，該中心所使用的VAX 電腦竟然有四小時又三十四分鐘無法正常運作，迫使捷運局以半人工代替電腦操控以運轉電聯車。無人操作的捷運電聯車是靠著電腦的操控而運作，而前述之不明當機事件令人不禁懷疑是否有人透過電腦網路在搗蛋，此一事件讓社會付出極大的成本，但當機的事件背後卻可能隱含網路犯罪。為了工作需要，馬特拉曾從巴黎總公司建立一條數據傳輸線路與行控中心電腦連線，因此有人懷疑當機事件可能與網路連結有關。另外亦有人懷疑行控中心電腦是否「中毒」，而導致當機的發生。若行為人由網路侵入捷運局之行控中心的電腦系統，竄改其資料導致電腦當機，其行為是否成立刑法第一百八十四條之「妨害舟車及航空機行駛安全罪」，按行為人損壞軌道、燈塔、標識或以他法致生火車、電車或其他供水、陸、空公眾運輸之舟、車、航空機往來之危險者，構成刑法第

一百八十四條第一項之罪。本罪之行為客體為軌道、燈塔或標識。所謂「軌道」乃指供火車或電車行駛之用而固著於一定路線之軌轍包括鐵軌、枕木、水泥軌枕、道釘等。稱「燈塔」則係指建造於沿海岬角島嶼之塔狀建築物，以供船舶航行擬定方向之用。至於「標識」則係指為引導水、陸、空交通工具行駛或航行之用而設之標記或符號，如鐵路之號誌、道路之交通路標或海上浮標等。

本罪之行為為損壞或以他法使供水、陸、空交通工具發生往來之危險。行為人以直接方法損害行為客體，使其喪失引導交通往來之效用，固為該當本罪之行為，即使以損壞以外之其他方法，而能使軌道、燈塔、標識等喪失其引導交通往來之效用者，亦可該當本罪。因此，前述捷運局行控中心電腦當機之情形，行為人之行為並非以他法使軌道、燈塔、標識等喪失其引導交通往來之效用，所以與本罪之構成要件不該當，不成立本條之罪[74]。惟行為人若係以竄改資料之方式，使得由電腦控制之軌道、燈塔、標識等喪失其引導交通往來之效用者，則仍有構成本條之罪的可能。

此外，本罪之行為必須對於供水、陸、空公眾運輸之交通工具構成往來危險者，亦即使交通工具一旦行駛或航行即足生傾覆、相撞、出軌、失事、沈沒之虞者，方能構成本罪。

第二目　刑法第一百八十五條之適用

[74] 有認為構成刑法第一百八十四條之罪者，參閱蔡蕙芳前揭著，頁 117。

按行為人損壞或壅塞陸路、水路、橋樑或其他公眾往來之設備或以他法致生往來之危險者，構成刑法第一百八十五條第一項之損壞或壅塞陸路罪。本罪之行為客體為陸路、水路、橋樑或其他公眾往來之設備。稱「陸路」係指路上供公眾或車輛往來之道路，鐵路雖為陸路之一種，但因其鋪有軌道，已為刑法第一百八十四條之保護客體，而無再列為本罪行為客體之必要，故本罪所稱之陸路即不包括鐵路。稱「水路」係指供舟筏、船舶航行之水道，橋樑則指架構於河川上以供公眾或車輛往來之設備。至於「其他公眾往來之設備」則為概括之規定，凡足以供公眾往來者，不問其種類，均屬此範圍，例如港灣之設施、陸路之石級、登山之攀索等均是。而捷運局行控中心之電腦係控制捷運電聯車之設備，解釋上應可認為係「其他公眾往來之設備」。

本罪之行為有三，即損壞、壅塞或他法，行為人只要有三種行為之任何一種，即足以成罪。稱「損壞」係指以直接之方法破壞陸路、水路、橋樑或其他供公眾往來之設備，使其喪失交通效用。稱「壅塞」則指以有形之障礙物以遮斷或阻塞陸路水路或橋樑上之交通。又所謂「他法」則指損壞、壅塞等破壞方法以外之一切足以使陸路、水路、橋樑或其他公眾往來設備喪失交通效用之其他方法而言。由網路入侵捷運局行控中心之電腦系統竄改資料，進而導致電腦當機之行為，即係以他法使其他公眾往來設備喪失交通效用之行為。

本罪之行為須致生交通往來之危險，方能成罪。換言之，即行為人之行為結果只要客觀上可以認定足有發生交通危險之虞者，即可構成本罪，不以發生實害為必要[75]。否則，如行為雖已使陸路、水路、橋樑或

[75] 參閱林山田著，刑法各罪論（下），民國 88 年，增訂二版，頁 486。陳煥生著，刑

其他公眾往來設備遭受損壞或壅塞，但並無足以發生交通危險之虞者，自不負本罪之刑責。因此，由網路入侵捷運局行控中心之電腦系統竄改資料，進而導致電腦當機之行為，若有足生交通往來之危險者，即構成本罪。

第三目　刑法第一百八十八條之適用

行為人藉網際網路侵入中華電信公司之電腦系統中，竄改資料導致電腦當機無法正常運作，使得電信交換系統停擺影響電話之通訊，此種行為是否有刑法第一百八十八條之適用，按行為人妨害鐵路、郵務、電報、電話或供公眾之用水、電氣、煤氣事業者，構成刑法第一百八十八條之妨害公用事業罪。本罪之行為客體為鐵路、郵務、電報、電話或供公眾之用水、電氣、煤氣等事業。此等事業以提供民生之日常需要之公用事業為限，至其為公營，抑或民營？則在所不問。

本罪之行為針對鐵路、郵務、電報、電話或供公眾之用水、電氣、煤氣事務之妨害行為，舉凡一切作為或不作為，而足以妨害鐵路、郵務、電報、電話或供公眾之用水、電氣、煤氣等公用事業者，均可能該當為本罪之行為。故行為人透過網際網路侵入中華電信公司竄改資料導致電信交換系統當機之行為，應可認定為妨害電話之公用事業之行為，而成立本罪。

法分則，民國 79 年 10 月修訂版，頁 158。最高法院七十九年台上字二二五〇號判決參見。

第四目　小結

現在電腦與網際網路備普遍使用於各行各業，自動化已成為不可擋的社會發展趨勢，自動化交通設備與自動化交通控制設備越來越普及，許多公用設施也自動化，例如捷運、醫院等。進入自動化公用設備的電腦系統消去資料或以其他方法妨害電腦的運作，會造成他人生命、身體的危險，有關電腦運作妨害的行為除了使電腦本身不能正常運作外，更重要的是這種行為所引起的附帶其他結果，換言之，即許多自動化之公用設施亦隨之停擺，此種結果所帶來之危險將造成重大的損害，而許多行為亦非傳統之公共危險罪可加以處罰，造成處罰上之漏洞，對於法益之保護顯有不足，因此，有立法補救之必要。

第六款　刑法準詐欺罪之適用

在十幾年前，搶銀行是一件相當辛苦的犯罪，為了躲避銀行的監視器及偵查機關的查緝工作，除了手槍、安全帽、口罩、裝錢的袋子及交通工具外，仍需有接應的把風者，如今時代變了，網路駭客只須修改電腦存款記錄或控制電腦，透過網際網路，在任何地方只須透過電話線及電腦，即可能突破系統漏洞及修改銀行電腦存款資料檔案，而達到犯罪的目的。這樣的犯罪手法目前雖未出現於國內，然美國的花旗銀行卻已發生遭駭客入侵並盜領四十萬美金存款之情形，此種修改電磁記錄，破

壞電腦處理正確性的犯罪型態依我國刑法第三百三十九條之三規定，意圖為自己或第三人不法之所有，以不正當方法將虛偽資料或不正指令輸入電腦或其相關設備，製作財產權之得喪、變更紀錄，而取得他人財產者，處七年以下有期徒刑。

第四節　利用網路散布電腦病毒

第一項　電腦病毒之意義及成因

病毒思想幾乎與電腦同時誕生，八〇年代電腦病毒這個概念正式誕生，源於一九八六年有人因自己設計的軟體時常遭非法拷貝而設計，但也有專家指出，它實際上是美國一些電腦神童所想出來的，最初只是寫惡作劇的程式整朋友，後來把玩笑擴大，將病毒藏在磁片當中，跟不知情的使用者交換磁片，這種惡作劇的方法很快便引起仿效，於是各種各樣的病毒不斷出現。

所謂的電腦病毒（computer viruses），一般係指有意破壞電腦系統運作者，刻意設計之一種特定的電腦程式，經輸入後隱藏寄生在開機時之程式、應用程式及作業系統程式中，或是依附在可供執行之電腦程式上，它也可能藏在其他週邊設備或資料庫內，或以偽裝方式潛伏於磁碟片、硬式磁碟機或電腦記憶體內，於間隔一段時間後，它會不斷地自動複製程式本身，蔓延並衍生許多拷貝，或自動增加無益之程式，連續擴散直到佔滿整個記憶體或磁碟機的空間為止，將其他資訊吞噬、覆蓋使電腦作業緩慢或甚至無法操作。如它被發現，有時還會改變檔案潛逃，

轉移至其他地方寄生，甚至透過電腦網路連線，侵入別的電腦或磁碟片，再以蠶食鯨吞的方法，使電腦當機。此外，電腦病毒另一種襲擊方式，係以設置一項定時炸彈方式，即由病毒設計者將程式輸入後，設定一項讓病毒發作之重要指令、密碼、文字、符號、複製之次數或時間，予以一觸即發的破壞。例如以電腦內之時鐘作啟動器，再設定一個特定之時間如年、月、日（system date），屆時即自動引發而破壞電腦之資料，達到損害之目的。美國加州刑法典有對電腦病毒為定義：「電腦污染物是指被設計在電腦、電腦系統或電腦網路中，違反資料所有權人意思或未受其允許情形下，去改變、損害、毀滅、記錄或傳送資訊的電腦程式。包括，但不僅限於以下所述，通常被稱為電腦蟲或電腦病毒的那些具有自動複製或自我繁殖能力，被設定去污損電腦程式或資料，耗損電腦材料，改變、損害、毀滅、記錄或傳送資料或者以其他方法霸佔電腦、電腦系統或電腦網路的正規的運作[76]。」由此定義觀之[77]，這樣的規定處罰

---

[76] 原文為：「Computer contaminant means any set of computer instruction that are designed to modify, damage, destroy, record, or transmit information within a computer , computer systems, or computer network without the intent or permission of the owner of the information. They include, but not limited to, a group of computer instructions commonly called viruses or worms, which are self-replication or self-propagating and are designed to contaminate other computer program or computer data, consume computer resources, modify, destroy, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network」

[77] 參閱蔡蕙芳前揭著，頁 119-120。

範圍的範圍很廣，例如有些並不會造成資料毀損的惡作劇性電腦病毒，如果突然介入電腦運作，將有可能被認為是霸佔電腦、電腦系統或電腦網路的正規的運作之電腦犯罪行為。

一提到電腦病毒，在資訊界就必定會聯想到美國 Morris 一案，Morris 當時為康乃爾大學電腦科學研究所博士班一年級的學生，他為了要凸顯當時電腦網路安全在防護上的缺失，因此撰寫了一個所謂的蠕蟲（Worm）或病毒（Virus）的程式，透過麻省理工學院（Massachusetts Institute of Technology）的電腦系統將此程式放到網際網路上，造成美國境內的許多電腦系統都因網路的相互連結而被傳染，最後因此當機。據估計每台電腦因此所受損失分別在二百美元到五萬三千美元之間，全球之電腦系統都因此而遭受空前的損失。目前電腦病毒種類繁多，良莠不齊（可分為良性及惡性兩類），通常皆以個人電腦為攻擊目標，大致有 C-Brain、Scores、NVIRS、Alameda、資料犯罪一二三（Data Crime 1,2,3）或稱哥倫布日、磁碟殺手（Disk Killer）、黑色星期五（SUMSDOS）、耶路撒冷（Jerusalem）、巴勒斯坦解放組織（PLO）、世界和平日、耶誕卡程式、和平標誌及國產的兩隻老虎、快樂星期六及 CIH 等等不一而足，為化解這些病毒，已有許多解毒程式，例如九轉還魂丹、Kill Bug、病毒疫苗抗體程式（vaccine software）、IBM 亦有消除病毒程式之病毒掃描程式（virus scanning program）等等，但電腦病毒所產生之速度遠超過解毒程式之設計速度，每天都有新的病毒被設計出來，所以關鍵點仍是「預防勝於治療」，例如避免使用來路不明之盜版軟體、勿隨意拷貝他人程式、不要隨意互借磁片、透過網路連線時注意避免傳播帶有病毒程式等等。

第二項　散布電腦病毒之刑事責任

由於各機關、公司行號大量使用電腦，故其電腦系統內之程式及資訊均成為業務上不可或缺之工具，其價值之高、重要性之大，實不言而喻。而設計電腦病毒之人，其破壞或影響他人程式及資訊之行為，是否違反我國法律之規定即有討論之必要。

一、毀損器物罪

一般而言，所謂電腦當機，係指暫時地使電腦系統無法正常運作，只要經過程式或軟體的修改即可恢復正常運作，並未致電腦硬體本身達到不堪使用之地步，故與刑法第三百五十四條之毀損一般物品罪中有關「毀棄」、「損壞」、「致令不堪用」等構成要件並不相符，所以不成立本罪。而刑法上所謂之物，兼括動產、不動產、財產等，可滿足人類生活需要或慾望性質之物。在學理上，刑法學者對於刑法上之物的認定有下列不同之見解：

（一）有體物說：認為刑法上之物應指有形體之物而言，必須具有一定體積，占有一定之空間，吾人可得認識其存在之物，與物理學上之物概念一致。

（二）物理管理可能性說：認為物應指通常置於物理可能管理狀態之物。

（三）持有可能性說：主張物以可能持有者為有體物。至於電氣、熱能及其他能量或電磁記錄因其持有可能，亦屬物。

（四）效用說：指物乃得為財產權目的具有經濟價值之有體物。

我國刑法以有體物說為原則，且以有體物中之動產為限，而以不動產及電氣、熱能及其他能量或電磁記錄為例外，因電磁記錄本身並非物，故修正後之刑法第三百二十三條特別規定，電磁記錄關於竊盜罪以動產論。準此，電磁記錄因並非具有一定形體之有體物，且毀損罪中又無特別規定，散布電腦病毒以侵害程式及資訊等電磁記錄之行為實難論以毀損器物罪。

二、毀損文書罪

至於因受電腦病毒干擾而使電腦檔案及程式等電磁記錄無法正常運作或甚至受損壞而無法使用時，依新修正之刑法第二百二十條第二項之規定，電磁記錄足以為表示其用意之證明者，為刑法上之準文書。因此若因電腦病毒之散布行為致刑法第二百二十條第二項所稱之電磁記錄被侵害，且已達「毀棄」、「損壞」或「致令不堪用」之程度，足以生損壞於公眾或他人時，即該當刑法第三百五十二條第一項之毀損文書罪。惟若侵害之程度尚未達「毀棄」、「損壞」或「致令不堪用」之程度，而僅係干擾他人電磁記錄之處理時，則依新增修之刑法第三百五十二條第二項之規定，干擾他人電磁記錄之處理，足以生損害於公眾或他人者[78]，

[78] 行政院修正草案的主要理由是「干擾他人電磁記錄之處理，足以影響電腦之正常運作例如以電腦病毒方式，即利用程式透過電腦連線系統進行複製，佔據記憶容量，干

亦科以相同之刑責。但若所毀損之電磁記錄並非刑法上之準文書時，即不能因為課侵害之客體為電磁記錄而認為可該當刑法第三百五十二條第一項毀損文書罪之構成要件，而應依同條第二項之規定處罰。

擾電腦之正常運作功能，如其情形足以生損害於公眾或他人時，宜以刑罰加以規範。」

第五章　其他類型之網路犯罪及其刑事責任

網際網路之發展帶給人類最大的利益莫過於人們可以透過網路的連結特性，迅速且大量地交換、傳遞訊息，然而「水能載舟，亦能覆舟」，資訊之取得太過方便往往也造成有心人士開始濫用資訊，進而侵害他人之權利。

第一節　非法重製電腦程式或檔案

關於此類網路犯罪類型，國內所發生最著名的案例就是凱訊光碟月刊於一九九四、一九九五年間，將台灣學術網路上，tw.bbs 諸討論區上張貼之文件收錄至光碟內，隨其雜誌月刊銷售之行為。行為人利用網路下載（download）電子佈告欄上網友發表之言論，並製成光碟片隨刊販售，其所涉及之問題在於 BBS 站上所發表之言論是否為著作權法所要保護之客體；下載網路上之文章而製成光碟片是否構成著作權法上所稱之「重製」，此種行為能否主張為「合理使用」而免責？

由於我國著作權法對於著作權人的權利規範極為廣泛，但是對於限定著作權人權利之限制規定卻極為嚴格，明顯的偏向於保護著作權人，而不利於著作利用人，因此若根據我國著作權法之相關規定，目前在網路上涉及他人著作的各種利用行為，若不符合著作權法第四十四條至六十三條之除外規定（我國稱之為著作財產權之限制，國外則稱為合理使用），幾乎都會違反著作權法之規定。因此，在 BBS 站上發表之具原創性

之言論應屬於著作，而得受著作權之保護。他人未經同意而重製即會侵害著作權，是故，光碟月刊社下載 BBS 站上之著作並製成光碟出售，依該案之起訴書所言，及最高法院之判決以觀，法院明顯係依據著作權法規定認定其行為係重製之行為，且不屬著作權法第五十一條之合理使用範圍，故予以論罪科刑。可見我國嚴苛的著作權法規定對於國內業者利用網路將會有極大之影響，因此，應審慎思考找尋著作權保護與網路發展間之平衡點。

第一項　刑法竊盜罪之適用

竊盜罪乃行為人出於「取得意圖」，而竊取「他人動產」之財產罪，係最常見之犯罪行為。按行為人意圖為自己或第三人不法所有，而竊取他人動產者，構成刑法第三百二十條第一項之普通竊盜罪。

第一款　保護法益

竊盜罪為財產犯罪，其所破壞之法益乃財產法益。而竊盜罪所破壞之財產法益，計有「動產之所有權」與「持有權」，故竊盜罪之被害人，也就包括物之所有人與持有人。茲就兩者分述如下：

一、動產所有權

所有權乃基於物權而形成之一種法律方式之「物的支配關係」，所

有人在積極方面可以自由使用、收益、處分其所有物，在消極方面則得排除他人之干涉、侵奪與妨害，所有物被侵奪或受妨害時，可請求返還、除去妨害、所有物有受妨害之虞時，則可請求防止妨害。動產被他人以不法所有之意圖而竊取，所有人事實上喪失所有物，而未能行使其所有權，故本罪所保護之法益為動產所有權。

二、動產持有權

社會日常生活中，動產並非恆久在所有人之持有中，而是往往由於法律上或事實上之需要，而由所有人以外之第三人持有，此等持有人雖對該物無所有權，但在事實上卻擁有支配權與監督權。持有物一旦被竊，則持有人之持有法益也將因而受害。所謂「持有權」乃是對於動產之事實支配與監督權，它與民法上之占有權在外形上由於均係對物在事實上之支配與管領，故很類似，但在法律實質上卻是不同的。

第二款　竊盜罪之行為客體

本罪之行為客體為他人之動產。所謂動產係指土地及其定著物等不動產以外之物。所謂物依據德、日民法之規定，係指「有體物」，故德日刑法學者，也均以此規定，而認為可作為本罪之行為客體者，唯限於具有體積，佔有空間之有體物[79]。我國民法對於物之意義並無明文規定，

[79] 參閱林山田著，刑法各罪論（上），民國 88 年，增訂二版，頁 204。

故刑法上似不必拘泥於有體物之限制。惟可能成為竊盜罪之無體物，在實例上並不多見，如電氣、熱氣等。但電氣發明後，大陸法系諸國刑法未免將其解釋為物，適用竊盜之構成要件，則無異是類推解釋之運用，有違罪刑法定主義，故特定條文規定以財物論，或特定竊電條款，我國也採瑞、日立法例，不但在刑法上規定「電氣關於本章之罪，以動產論」（刑法第三百二十三條），而且又於電業法第一百零六條規定竊電條款。近年來由於電腦與網際網路之普及化，對於電磁記錄是否得為竊盜罪之客體迭有爭議，故八十六年十月八日修正公佈之刑法第三百二十三條規定：「電能、熱能及其他能量或電磁記錄，關於本章之罪，以動產論。」故依現行刑法之規定，電磁記錄關於竊盜罪得視為動產，所以可成為竊盜罪之行為客體。

第三款　竊取行為

所謂「竊取」係指行為人違背他人之意思，或者至少未得他人之同意，而以和平之手段，取走其持有物，破壞他人與其持有物之「支配持有關係」[80]。換言之，即以非暴力之手段，打破他人對其持有物之「支配持有關係」，使其無法行使對持有物之支配權與監督權，並建立一個新的持有支配關係，而使自己或第三人成為該物之持有人，取得該物之支配管領力。

[80] 參閱林山田著，刑法各罪論（上），民國 88 年，增訂二版，頁 206。

首先就竊取手段而言，有認為竊取行為只要以非暴力或和平之手段，違反持有人之意思，或未得持有人之同意，而取走其持有物，即足當之，並不以係乘人不知不覺，且以祕密或隱密之方法為必要[81]。但國內學者通說[82]均以乘人不知或不覺，且以祕密或隱密行之為必要，實務上亦認為如此[83]。

至於竊取行為過程方面，包括兩個行為過程，即首先破壞他人對物原有之持有支配關係，其次再建立一個新的持有支配關係。故只有原來持有支配關係之破壞，而尚無新持有支配關係之建立，則非完整之竊取行為。此等情況下，根本即不構成竊盜罪[84]，或只成立竊盜未遂。破壞他人對其持有物之持有支配關係，乃竊取之第一步行為。物只要在他人持有中，而處於他人之支配與監督之下，則此持有支配關係，即可加以破壞，而構成竊取行為。因此，破壞他人對其持有物之持有支配關係，乃為判斷是否為竊取行為之關鍵。

第四款　小結

在網路上透過網際網路之連結，進入他人之電腦系統內並對他人之資料擅自儲存取用時，依新修正之刑法第三百二十三條規定：「電能、熱

---

[81] 參閱林山田著，刑法各罪論（上），民國 88 年，增訂二版，頁 207。

[82] 持此看法之學者有韓忠謨、蔡墩銘、趙琛、陳煥生等。

[83] 最高法院二十二年上字一三三四號判例參見。

[84] 例如打開鳥籠，而讓他人飼養之金絲雀飛走之行為。

能及其他能量或電磁記錄，關於本章之罪，以動產論」觀之，似可該當竊盜罪[85]。但竊取電磁記錄之行為在解釋上會面臨極大的難題，所謂「竊取電磁記錄」，就文義上之解釋應包括兩種含義，一是電磁記錄之實體，例如磁碟片。另一個則是指電磁記錄所涵的抽象的意識內容。雖然依修正後之刑法第二百二十條第三項的定義，電磁記錄是指以電子、磁性或其他無法以人之知覺直接認識之方式所製成之記錄，而供電腦處理之用者。依此立法之定義，刑法第三百二十三條所謂電磁記錄指的也應該是以電磁方式記錄一定意識內容的實體物。但若此處電磁記錄所指的是電磁記錄的實體物，本屬動產，那麼本來就可以適用竊盜罪中竊取他人動產的文字規定，根本不須增訂此規定。所以本條修正文字中所稱之電磁記錄，立法者所要規範的對象，應該是電磁記錄所內涵之抽象的意識內容[86]。但是如此一來，解釋上也是有根本的困難，申言之，所謂竊取他人電磁記錄之行為，是否該當刑法上竊盜罪的竊取概念？容有疑義。蓋竊盜罪構成要件中的竊取，刑法上的解釋是行為人破壞原持有人的持有支配關係而建立新的持有支配關係[87]。然而此處所謂竊取電磁記錄的情形，事實上指的是以重製之方式獲得該電磁記錄。一方面固然行為人是得到他人的電磁記錄的內容，建立其對於電磁記錄內容的持有支配關係，但是另一方面，電磁記錄之持有人並未因此而喪失他對於電磁記錄內容的持有支配關係。此種電磁記錄事實上之特性，使得所謂竊取電磁記錄根本沒有辦法該當於刑法上竊盜罪的竊取要件，自然不能構成刑法

[85] 參閱馮震宇、劉志豪前揭著，頁 88。

[86] 參閱黃榮堅著，刑罰的極限，民國 87 年 12 月，頁 318-319。

[87] 參閱林山田著，刑法各罪論（上），民國 88 年，增訂二版，頁 208-209。

上的竊盜罪。

此問題之發生在於立法者忽略了一般財產權及智慧財產權在事實關係上的差異，新修正條文中所說的電能、熱能或其他能量，雖然和智慧財產權一樣屬於無體的性質。不過，電能、熱能或其他能量至少不是一種純粹抽象的思考內容。電能、熱能或其他能量至少都還有具體的消長現象存在。例如一千瓦的電能，如果被竊用了三百瓦，所剩下的就是七百瓦。因此要適用竊盜罪的構成要件，並無問題。但是一個思想的內容，所謂被竊取走了，事實上也就是別人也窺知了原智慧財產權人的思想內容而已，那麼就很難符合竊盜罪中支配關係移轉的概念。這是對於兩種事實關係不同的財產利益的不法取得，試圖用相同的一個條文做規範，以致於發生文字上無法勝任的結果。

關於此問題之解決，關鍵在於刑法上竊取行為之定義，除非我們能夠對於竊盜罪中所謂的「竊取」修改其涵義，否則所謂竊取電磁記錄，還是不能構成竊盜罪。有學者認為[88]如果我們可以修正竊取行為之涵義，將重點擺在行為人建立新的持有支配關係上，而不必以把破壞原來的持有支配關係為要件。如此一來，未經授權或同意複製他人電磁記錄之行為就可以該當竊取之定義了。但這樣解釋的結果，是否會過度擴張竊盜罪原來所涵蓋之範圍？就竊盜罪原來所要規範的對於有體動產的竊取而言，由於其有體，所以在物理性質上，只要有建立新的持有支配關係，必然在另一方面會破壞原來的持有支配關係。因此，事實上不至於因為要件的縮減而造成擴大規範範圍的情形。惟本文以為為了更精確的定義竊取行為，我們不妨把竊盜罪的竊取定義成「剝奪專屬支配關係

[88] 參閱黃榮堅著，刑罰的極限，民國 87 年，頁 321。

[89]」。這樣的概念下，一方面既可以網羅立法者所要規範的竊取電磁記錄的行為，另一方面也還可以保持竊盜罪原來所要規範的範圍不致發生變動。

第二項　刑法妨害祕密罪之適用

關於個人祕密的保護，這一次的刑法增修，也有幾個條文的變動。在刑法第三百十五條，新條文之規定是「無故開拆或隱匿他人之封緘信函、文書或圖畫者，處拘役或三千元以下罰金。無故以開拆以外之方法，窺視其內容者，亦同。」新條文除了提高罰金額度之外，行為的客體包括了圖畫。同時，行為的模式標括了其他方式的窺視。

所謂無故以開拆以外之方法窺視其內容，立法者的意思，除了用以規範以前學說曾討論之不須開拆信封即可透視信函內容之行為之外，最主要的應該是針對透過電腦而窺視電磁記錄之內容的情形。不過在這裡，會有一些問題發生。首先，如上所述，並不是所有的電磁記錄都是文書。例如電腦程式，就不是文書。因此，電腦業者所最擔心的對於電腦程式的「竊取」、竄改或毀損行為之前的入侵行為，還是無法用本條加以規範。其次，本條第一項列為行為客體的是封緘信函、文書或圖畫，依新舊條文文字對照以及立法用意來看，可以該當本條構成要件所稱的文書或圖畫，也是以封緘為限。有問題的是，電磁記錄如果是文書，而

[89]亦有學者主張可將竊取行為定義成「未經持有人同意而建立新的持有支配關係」，國內學者採此看法者為黃榮堅。

且無故以開拆以外之方法窺視其內容者，固然也可能構成犯罪。但是此處的電磁記錄也必須符合「封緘」的要件。然而，在文字的理解上，封緘應該是針對日常生活中實體的信函而言的，對於電磁記錄並沒有所謂的封緘。事實上，對於電磁記錄，所有人有時候會另為加密的處理，其作用與信函或文書之封緘相同，但條文的用字就是「封緘」而非「經過其他保密程序」，所以在罪刑法定主義之前提下，我們必須仔細思考。所以，如果要對窺視電磁記錄內容者論以妨害祕密罪，在文字解釋上可能產生疑慮。畢竟視窗軟體中所出現代表電子郵件的「信函」之圖形並不等同於日常生活上的信函。當然，在立法者之主觀意願以及立法之客觀需求的因素下，就「封緘」作擴張解釋在現實上是勢所難免的。但為免過度擴張其範圍，解釋上必須加以限制。關於此一問題，德國刑法對於電磁記錄之保護，是和書信的保護分開規定的（德國刑法第二百零二條以及第二百零二條 a)。對於電磁記錄，是以資訊的加密處理為要件。並且，對於電磁記錄的祕密保護，並不是透過「文書」的用詞和概念，而是直接稱之為資訊，所以也不會有「文書」的意義範圍上的困擾[90]。因此，可參考德國刑法條文之規定，被窺視的行為客體如果是屬於電磁記錄，必須是特別經過加密處理的而且具有文書性質的電磁記錄。

關於網路犯罪而與妨害祕密有關的，另外有刑法第三百十八條之一，「無故洩露因利用電腦或其他相關設備知悉或持有他人之祕密者，處二年以下有期徒刑、拘役或五千元以下罰金。」，以及刑法第三百十八條之二，「利用電腦或其他相關設備犯第三百十六條至第三百十八條之罪者，加重其刑至二分之

[90] 參閱黃榮堅著，刑罰的極限，民國 87 年，頁 351。

一。」的規定。

關於電腦處理個人資料之保護，我國電腦處理個人資料保護法第三十三條以下有相關的刑罰規定。在這種情況下，另外又在刑法當中就相同的問題作規定，立法上顯得凌亂。不過基本上，由於兩個法規所要保護的法益是一樣的，所以，如果行為人一行為同時該當於刑法第三百十八條之一以及電腦處理個人資料保護法第三十三條以下有相關的刑罰規定，那麼應該認為屬於法條競合。大致上，由於電腦處理個人資料保護法第三十三條以下有相關的刑罰規定，在構成要件上是針對特別意圖或特別的行為方式所作的規定，所以應先適用。

在整個有關妨害祕密罪的立法體系上應該思考的問題是，關於個人資料的保護，除了刑法原有的第三百十五條以下的規定外，是否限於電腦所處理的個人資料，法律才加以保護？我們應該先思考一下，透過電腦處理個人資料保護法或刑法相關條文的增修，法律所要保護的法益為何？由法律的規定，我們不難看出法律所要保護的是「個人祕密」。不過既然如此，那麼立法的技術標準應該很清楚：如果個人祕密應該加以保護的，就是應該加以保護，而和是否用電腦來處理沒有關係。如果個人祕密沒有保護必要的，就是沒有保護的必要，也和是否用電腦來處理沒有關係。依我國目前的立法標準來看，保護的標準似乎並不是建立在個人資料保護的必要性上，而是建立在電腦的關係上。因此，產生一種現象，電腦的使用一方面使某些人資訊的所有人變成特權階級，另一方面卻又使某一些資訊的窺視者承擔起電腦的原罪。以致於模糊了焦點，使人

產生疑惑，到底這些立法目的是否果真是為了個人祕密的保護？這一個問題，亦出現在刑法第三百十八條之二的規定上，為什麼利用電腦或其相關設備犯刑法第三百十六條至第三百十八條之罪者，就要加重其刑至二分之一？如果所考慮的是損害範圍的大小，那麼以電腦的使用作為區分的標準，標準不免過於僵化且不當。果真如此，那麼對於其他之犯罪類型是否增訂使用電腦犯之者加重其刑之規定，其不當顯而易見。

第三項　刑法背信罪之適用

行為人為他人處理事務，意圖為自己或第三人不法之利益，或損害本人之利益，而違背其任務之行為，致生損害於本人之財產或其他利益，構成刑法第三百四十二條第一項之背信罪。而本罪之行為主體必須為為他人處理事務之人，至於所謂「事務」之範圍向來即有廣狹兩種不同之見解，採狹義見解者[91]認為本條所稱之「事務」，應以財產上之事務為限，故為他人處理非財產上之事務者，即不可能成為本罪之行為主體。採廣義見解者[92]則認為本條所稱之事務，不以財產上之事務為限。按本罪為破壞財產法益之財產犯罪，故行為人為他人所處理之事務，自以限於財產上之事務為宜，況且本條對於行為主體之規定，僅言「為他人處理事

[91] 採此見解之學者有趙琛、林山田。

[92] 採此見解之學者有蔡墩銘。

務」，與大陸法系各國刑法之背信條款相較[93]，顯然鬆弛而不夠明確。因此，若採廣義見解來解釋本條所稱之事務，則會使本罪之適用範圍擴張至幾近濫用之程度，此顯有為背信罪之罪質。

由於本條「為他人處理事務」之概括規定，太過籠統而不明確，故解釋上所謂之事務，除前述在種類上之限制外，在事務之性質上也宜作相當之限制，即指為他人處理外部關係的財產上法律事務。再者本罪係處罰行為人濫用權限與信託義務之違背。因此，本罪所謂之事務，在性質上應限於具有相當責任性之事務，若他人對於行為人並無相當之授權，兩者之間並不存有所謂之信託關係，行為人所從事者只是機械性之工作，無須也無權做成任何決定者，則非本罪之事務。

而該當本罪之構成要件之背信行為，應包括事務處分權限之濫用與信託義務之違背行為，此兩類行為不問係以積極之作為，抑或以消極之不作為，均可該當本罪之背信行為。且行為人之違背任務之行為必須造成將事務委由其處理之他人，在財產或其他利益上之損害，方能構成本罪。條文上所謂「致生損害於本人之財產」係指將事務委由行為人處理者本人之財產價值之減少，包括積極之損害與消極之損害，前者如現有財產之減少，後者如妨害現有財產之增加，或喪失日後可得之利益。當然這裡的損害也是專指處理外部關係的利益損失，換言之，是違背本人意思而損及本人利益的一種利益輸送[94]。因此，公司職員未經授權經由

---

[93] 如德國刑法之背信條款，則限於依據法律規定、官署命令或法律行為，而有權處分他人財產者；或依據法律規定、官署命令、法律行為或因事實之信託關係，而管理他人財產者。

[94] 參閱黃榮堅著，刑罰的極限，民國 87 年，頁 210。

網路之連結，進入公司之電腦系統的行為，或者公司職員於上班時間，利用公司的網路專線上網，處理自己之事務等，均非受公司委託處理公司與第三人之間的法律關係事物，亦即並非外部財產關係上之事務，所以並不會構成背信罪。

第四項　電腦資訊與隱私權

第一款　隱私權之理論

隱私一語，在我國傳統觀念上本帶有負面的、貶抑的價值，所謂「君子坦蕩蕩」、「君子慎獨」在在均顯示所謂隱私在我文化中實無形成之可能，是以探討隱私權理論之起源，自須外求。自從一八九〇年，美國律師 Samuel D. Warren 及 Louis Brandeis 兩人聯名發表「隱私權」（The Right of Privacy）一文以來，隱私權之觀念即漸漸在法領域取得一席之地，不僅在英美法系國家得以確立其基本權利之地位，在大陸法系國家亦被認定屬於一般人格權之重要內容之一[95]。

然而，原始隱私權之概念係起源於「家是個人之城堡」（An Englishman's house is his castle）之傳統觀念，亦即「獨處不受他人干涉之權利」（the right to be let alone）之類消極面之意義，然而在高度現代化之社會中，科技極為發達，，所謂偷窺、非法侵入住宅

[95] 參閱洪榮彬著，資訊時代之資訊處理與資料保護 —以德國聯邦個人資料保護法為中心，私立輔仁大學法律研究所碩士論文，民國 82 年 6 月，頁 1。

竊取資料、拍照、攝影甚至竊聽等等侵害隱私權之模式，有的已有改變，有些雖未改變，然其手段則大為翻新，抑有進者，隨著資訊化社會之來臨，已如前所述，電腦挾著排山倒海之威力，深入影響到社會每一層面之生活，尤其在資訊與資料之蒐集、儲存與交流之完整、便利，使得不僅國家機關、公司行號，甚至個人行為，均可能對人民之隱私權造成嚴重之威脅，在美國自從羅斯福總統實行新政（New Deal）開始，因為採行社會救濟福利政策之需要，各政府部門上自聯邦調查局、國稅局、下至各金融機關、教育機構及各州福利機構，對全國人民之私人資料之蒐集可謂巨細靡遺，因此人民之隱私權保護岌岌可危，如再加上隨意將個人提供某種特定目的使用之資料用於他處等資訊濫用之因素，情況之嚴重性不言可諭。由於上開原因,「資料保護」遂成為現代隱私權之最重要內容，此即「資訊隱私權」（Information Privacy）[96]。其與傳統隱私權最大之不同在於，除了前述不受干擾之消極意義外，現代隱私權之內涵已包括「掌握個人有關資料之權利」（The right to exercise control over information about oneself）[97]，而其較完整之詮釋則係德國聯邦憲法法院於西元一九八三年十二月十五日於「人口普查法案」一案判決中所揭示之「個人資料自決權」（Recht aufinformation elle Selbstbestimmung）之概念，其從一般人格權中引導出個人對於其個人資料之交付與使用原則上有自由決定權，並且認為法律保留、隱私權保

[96] 參閱廖緯民著，論資訊時代的隱私權保護--以「資訊隱私權」為中心，資訊法務透析，民國 85 年 11 月號，頁 22。

[97] 參閱陳宏達著，個人資料保護之研究，私立輔仁大學法律研究所碩士論文，民國 81 年 7 月，頁 33。

護及蒐集所得之資料之使用應受到「嚴格與具體之目的限制」[98]，此判決為個人資料之保護與資訊濫用之禁止建立了不可搖撼的里程碑。

第二款　資料之保護、保全與公開

資料保護，依據歐洲理事會（Council of Europe）於一九八一年一月二十八日所制定之「有關個人資料自動化處理之個人保護公約」(The Convention for Protection of Individuals with Regard to Automatic Processing of Personal Data）將其定義為：「對於個人在面臨關於其個人資料之自動化處理時，所給予之法律上保護」[99]。

資料保全與資料保護係分屬不同概念，在個人資料自動化處理之過程中，資料保全較之資料保護更早被使用，其最初之目的在於防止資料傳播過程中所產生之錯誤，因此所謂資料保全，應係指確保所蒐集之資料真實地存在，避免滅失或錯誤，而資料保護之目的則在於「避免人格權受損害，並促進資料之合理使用」[100]。

資訊公開係國家民主化過程中，由新聞媒體首先發難，針對其新聞報導之需要，乃特別強調人民有「知的權利」已為其報導新聞建立理論基礎，而其衍生之結果，不僅新聞媒體，即各別之個人本於國民主權，

---

[98] 參見洪榮彬前揭著，頁 506-507；陳宏達前揭著，頁 66。

[99] 參閱洪榮彬著，個人資料保護概論（上），高雄律師會訊，民國 85 年 1 月創刊號，頁 16。

[100] 參閱電腦處理個人資料保護法第一條條文。

均得強調其知的權利以要求政府機關提供其必要之資訊，以供其監督政府施政及個人生活、事業之判別。是以資料保護與資訊公開係屬不同範疇之理論，前者係著重在個人隱私權之保護，後者則強調人民對政府知的權利，惟目的不同，其規範對象亦有差異，然而此二種均為現代資訊社會化中極為重要之基本人權，因此如二者有所衝突時，究以保護何者為優先，即成為兩難課題，惟有妥慎思索每個個案中公共利益與個人權利之平衡點何在，方能求其圓滿解決，非可一概而論。

第三款　電腦處理個人資料保護法之適用

第一目　公務機關之資料處理

依電腦處理個人資料保護法之規定，公務機關對於個人資料之蒐集或電腦處理，非有特定之目的，並符合電腦處理個人資料保護法之要件，不得為之。而依照電腦處理個人資料保護法第七條之規定，其要件有三，即於（一）法令規定職掌必要範圍內者、（二）經當事人書面同意者、（三）對當事人權益無侵害之虞者。關於前二要件固無疑義，然第三款所謂「對當事人權益無侵害之虞」則難以明確界定，何況公務機關如既非於法定職掌必要範圍內，又未經當事人同意，其蒐集或電腦處理個人資料之動機何在恐多費猜疑，因此不應使公務機關得擅權

對個人資料予以蒐集或電腦處理。

此外，電腦處理個人資料保護法就公務機關對個人資料之利用也設有限制，應於法令職掌必要範圍內為之，並與蒐集之特定目的相符。惟在例外之情形下，得為特定目的外之利用，即（一）法令明文規定者、（二）有正當理由而僅供內部使用者、（三）為維護國家安全者、（四）為增進公共利益者、（五）為免除當事人之生命、身體、自由或財產上之急迫危險者、（六）為防止他人權益之重大危害而有必要者、（七）為學術研究而有必要且無害於當事人之重大利益者、（八）有利於當事人之權益者、（九）當事人書面同意者。

第二目　非公務機關之資料處理

所謂「非公務機關」依電腦處理個人資料保護法第三條第七款之規定，係指（一）徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人、（二）醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業、（三）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。

依電腦處理個人資料保護法第十八條之規定，非公務機關對個人資料之蒐集或電腦處理，須有特定目的，並符合下列情形之一，始可為之：（一）經當事人書面同意者、（二）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者、（三）已公開之資料且無害於當事人之重大利益者、（四）為學術研究而有必要且無害於當事人之重大利益者、（五）依本法第三

條第七款第二目[101]有關之法規及其他法律有特別規定者。

非公務機關為個人資料之蒐集、電腦處理或國際傳遞及利用，依電腦處理個人資料保護法第十九條之規定，必須經目的事業主管機關依本法登記並發給執照。另外徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人，依規定亦須經目的事業主管機關許可並經登記及發給執照。

非公務機關對於個人資料之利用，依電腦處理個人資料保護法第二十三條之規定，應於蒐集之特定目的必要範圍內為之。但於例外之情形下，可不受特定目的之限制，而得為特定目的外之利用，即（一）為增進公共利益者、（二）為免除當事人之生命、身體、自由或財產上之急迫危險者、（三）為防止他人權益之重大危害而有必要者、（四）經當事人書面同意者。

非公務機關在為國際傳遞及利用個人資料時，在特定之情形下，依電腦處理個人資料保護法第二十四條之規定，目的事業主管機關得限制之，即（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。

[101] 電腦處理個人資料保護法第三條第七款係對於非公務機關之定義，第二目是指醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業。

第三目　違反電腦處理個人資料保護法之處罰

意圖營利，違反電腦處理個人資料保護法第七條、第八條、第十八條、第十九條、第二十三條之規定或依第二十四條所發布之限制命令，致生損害於他人者，依電腦處理個人資料保護法第三十三條之規定可處兩年以下有期徒刑、或拘役、或科或併科新台幣四萬元以下罰金。

意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法輸出、干擾、變更、刪除或以其他非法方法妨害個人資料檔案之正確，致生損害於他人者，依電腦處理個人資料保護法第三十四條之規定可處三年以下有期徒刑、或拘役或科新台幣五萬元以下罰金。

第二節 大量商業性電子郵件之使用問題

未經請求而傳送大量電子郵件一般通稱為 spam，其中未經請求的商業性電子廣告信件（Unsolicited Commercial Email，簡稱 UCE），因其數量龐大，不當轉嫁營運成本，尤其造成 ISP 與使用者困擾而屢屢引發抱怨抗議；而根據 Forrester Research 一九九九年七月的調查，五十家網路公司中，三分之二以上認為經過使用者同意而發送的個人化電子郵件廣告扮演著「重要」或「非常重要」的角色。古諺云：「水能載舟，亦能覆舟」；同樣的大量電子廣告信因其運用之不同，可能造成網路環境的負擔，亦可能成為繁榮電子商務的助力，其中蘊含的問題實不容忽視。

第一項　國內處理大量電子郵件廣告相關法律規範與瓶頸

對於大量電子郵件廣告造成的問題，檢視國內相關法律，可由刑法第三百五十二條第二項及電腦處理個人資料保護法來思考問題之解決方向，但各有「適用範圍有限」及「證明困難」等瓶頸存在，以下分別敘述。

第一款　刑法第三百五十二條第二項之適用

依據民國八十六年公布施行的刑法修正條文第三百五十二條第二項規定，凡干擾他人電磁紀錄之處理，足以生損害於公眾或他人者，處三年以下有期徒刑、拘役或一萬元以下罰金。有認為干擾他人電磁記錄之處罰規定在刑法第三百五十二條毀損文書罪中，其處罰比刑法第三百五十四條普通毀損罪重，而與毀損文書罪相同，因認為此處之電磁記錄需符合刑法上文書之條件[102]，惟刑法第三百五十二條第二項既稱干擾他人「電磁記錄」而未稱文書，解釋上因認為此處所稱之電磁記錄應惟較廣義的電磁記錄，而非較狹義的電磁記錄僅指準文書。判斷可否援引該條文據以處罰電子廣告信的寄件人，第一，在客觀要件上，檢視該大量電子郵件廣告是否已干擾他人電磁紀錄，如嚴重至 ISP[103]系統當機或使

---

[102] 刑法上所稱之文書，因其須為有體的意思表示，故具有持續性；因其確立法律關係的重要手段且具有確認作用，故具有證明性；又其須足以揭示出具者與內容的對象關係故亦具有保障性。

[103] 即指網際網路連線服務提供者（Internet Service Provider）乃提供通路讓使用

用者電子信箱爆掉，應屬符合；然若單純只是郵件較多不堪其擾，並未達成對他人電磁紀錄之干擾，則尚無法引用該條文。第二，在主觀要件上，須審查發信者有否干擾他人電磁紀錄之故意，存在干擾之故意方有本條之適用，若無故意亦無法引用該條文；例如，須證明廣告主有當掉 ISP 系統、灌爆使用者信箱的故意才能引用該條文。

因此，並非所有濫發大量電子郵件廣告之行為皆可援用刑法第三百五十二條第二項加以處罰，其限制在於客觀上須造成系統當機等等干擾電磁記錄之情況，如僅只於設備消耗等困擾尚無法適用該條文；而且主觀上尚須證明行為人有干擾電磁記錄之意圖，關於此點仍存爭議，有認為發送電子商業廣告信之目的是為了廣告，大量電子郵件廣告發動者並不知道使用者與 ISP 的設備與狀況，無法判斷其收到廣告信後使用者或運作者是否受到干擾，因此無法證明發信者有干擾他人電磁記錄之意圖[104]；亦有認為發信者就大量電子郵件對網路環境及 ISP 可能產生之影響均已知悉，應有不確定故意存在[105]。本文以為若全然採取前說之見解，則對於濫發電子郵件之行為幾乎無法適用刑法第三百五十二條第二項之規定加以處罰，但是若將發送大量電子郵件廣告者一概認為存在不確定故意，則失之過嚴，每個運用大量電子郵件發廣告的人不見得都真的了解電子郵件傳送之過程及其網路環境相關影響，故應依據個案判斷，包

者與網際網路連線之機構。

[104] 參閱張雅文著，大量商業性電子郵件廣告之法律問題與管理機制，資訊法務透析，民國 88 年 9 月，頁 15-16。

[105] 參閱張雅文著，大量商業性電子郵件廣告之法律問題與管理機制，資訊法務透析，民國 88 年 9 月，頁 15-16。

括考量行為人從事之行業與生活對網路可能之了解程度，以及考量網路環境環境中一般民眾對網路及電子郵件等了解程度為何。目前實務上尚未出現以刑法第三百五十二條第二項處理大量電子郵件廣告之案例。

第二款　電腦處理個人資料保護法之適用

其實大量電子郵件廣告的問題，最根本源頭在於 e-mail address 取得與利用之管理，我國電腦處理個人資料保護法能否解決此問題？根據電腦處理個人資料保護法第六條規定，個人資料之蒐集或利用，應尊重當事人之權益，依誠實信用方式為之，不得逾越特定目的之必要範圍。而根據電腦處理個人資料保護法第七條、第十八條之規定，公務機關、醫院、學校、電信業、金融業、證券業、保險業、大眾傳播業、徵信業以及以蒐集或電腦處理個人資料為主要業務之團體或個人，對個人資料之蒐集與電腦處理，應有特定目的，並符合法令職掌內、經當事人同意，或原有契約關係存在、已公開之資料、為學術研究而無害於當事人等要件；另外，根據電腦處理個人資料保護法第八條、第二十三條規定，個人資料利用時，除非符合該法例外之情形，否則基本上必須於蒐集之特定之目的必要範圍內，方可利用其蒐集來的個人資料。

仔細分析，我國電腦處理個人資料保護法目前並無法從源頭解決大量電子郵件廣告，其一，e-mail address 單獨存在是否構成電腦處理個人資料保護法所稱「足資識別個人身分」之保護客體仍有爭議；國內某 ISP 公司就其使用者利用「小郵差派報軟體」蒐集電子郵件地址，並利用之代客送件一案，承辦檢察官即以該行為並未構成對姓名、生日等等「足

資識別個人身分」之個人資料蒐集，而為不起訴處分。其二，規範主體限於八大行業與「以蒐集或電腦處理個人資料為主要業務者」，並無法規範八大行業以外蒐集、利用個人資料者，例如，透過 e-mail 搜括軟體在 BBS 站等討論區抓取上網者 e-mail address 者，多非屬「以此為主要業務者」之個人、團體或電子商家，而無法以電腦處理個人資料保護法規範之。

第三款　偽造、變更發信源頭與路徑相關法律規範

有些大量發送未經請求之商業性電子廣告信者，為規避過濾軟體的過濾阻擋，而不斷變更、偽造發信源頭與路徑，一是發信人的身份與 e-mail address，二是 ISP address。在假造身份與 e-mail address 方面，如在身分設定（identity）的姓名（name）、電子郵址（e-mail address）、所屬組織（organization）等等欄位，擅自填入他人公司名稱商號姓名以及電子郵址與所屬組織等資訊，並以之散發大量電子廣告信，則侵害民法第十九條之姓名權，該條除保障自然人之姓名之外，已註冊之商號亦屬之[106]；若廣告進一步涉及販賣或輸出入相同商品或進行類似使用造成與他人商品混淆時，可能構成公平交易法第二十條第一項第一款之違反[107]。然而，多數的假造情況，行為人並非使用他人商號或姓名，而是隨

[106] 最高法院二〇年上字第二四〇一號判例參照。

[107] 公平交易法第二十條第一項第一款規定：「以相關事業或消費者所普遍認知之他人姓名、商號或公司名稱 ……，為相同或類似之使用，致與他人商品混淆，或販賣、運

意取一個代號來用，這樣就沒有侵害的問題。至於變更 IP 方面，由於 IP 是一連串的數字，非公司名稱、非姓名、亦不構成文書，甚者有些廠商使用浮動、非固定的 IP，此等情況法律無法規範，過濾軟體也無法運作。

第二項 外國法制趨勢

美國自一九九五年起，有關大量電子郵件廣告之寄信與拒絕收信的權利抗衡，以及言論自由、隱私權與侵權相關爭議不斷，除了透過訴訟途徑解決外，聯邦與華盛頓州、維吉尼亞州、德州、達華州等等亦嘗試透過立法解決問題；歐洲處理該問題雖不若美國廣泛而深入，但歐盟亦於一九九八年十一月正式提出處理 spam 之原則，以下就美國之立法概況與歐盟相關指令說明之。

第一款　美國聯邦國會相關立法草案

美國國會先後曾提出數部草案以解決 spam 的問題，一為「電話消費者保護法修正案」草案（Telephone Consumer Protection Act of 1991），該法原本規定業者不可以透過電話或傳真從事行銷活動，修正案提議擴

送、輸出或輸入使用該項表徵之商品者。」

大適用範圍，將網際網路傳送電子郵件亦納入規範 –除了寄件人與收信人本來就有商務往來或私人關係外，一律禁止以電子郵件發送廣告信件。二是「網路公民保護法」草案（the Netizen's Protection Act of 1997），修訂美國的電信法（the Communication Act of 1934），禁止商家未經同意即傳送給消費者電子廣告信，除非本來就有商務或私人關係存在，並要求寄信人必須在信中載明身份與相關資訊。另外，「電子信箱保護法」草案（the Electronic Mailbox Protection Act of 1997），規定發信者必須提供正確信頭資訊（來源、主題等），並強制其提供消費者拒收信件的選擇[108]。

另外，「未經請求電子商業廣告信篩選法案」（the Unsolicited Commercial Electronic Mail Choice Act）草案，規定 ISP 經使用者要求必須為其過濾電子廣告信，就 FTC 與使用者對未經請求電子郵件之申訴必須予以回應；此外，發信者必須經消費者請求後方得發出商業性電子廣告信，並應於信的主題部分載明為「廣告」，以利過濾軟體運作，讓消費者選擇是否將之刪除。

一九九八年五月十二日，參議院通過 Anti-Slamming Amendments Act，草案整合了上述法案精神，修訂 Communication Act of 1934，規定電子郵件信頭來源，主題資訊必須正確，必須提供真實的聯絡管道，收件人要求時必須將之自郵遞名單中移除；同時賦予 FTC 與州政府皆有執行該法之權力。但截至目前，美國政府對該問題解決之態度：留待業界

[108] 參閱張雅雯著，大量商業性電子郵件廣告之法律問題與管理機制，資訊法務透析，八十八年九月，頁 20。

自律，政府暫不介入規範[109]。

第二款　歐洲聯盟

歐盟執委會於一九九八年十一月十八日在布魯塞爾，發佈一份「歐盟指令因應電子商務市場在法制面應有規範之提案」（Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market）【98/0325（COD）】。在有關商業通訊往來廣告部分，該報告強調以「透明性」（Transparency）建立消費者的信心，並確保交易公平性；同時指出解決大量電子郵件廣告問題之必要性，為避免消費者受到侵擾，凡透過電子郵件進行商業性通訊者，應使對方能清楚辨識該電子郵件為商業廣告，以利消費者即時反應，因而建議必須提供消費者未打開電子郵件前即知為商業信件之相關資訊。

歐盟執委會認為，像在討論區中進行廣告或是大量電子郵件廣告等等具侵擾性的商業通訊模式，以引發許多訴訟案；但歐盟多數會員國對於此等行為，並無清楚的法律規範要求其應指明涉及商業性活動或指明由誰贊助；因此，在該份有關電子法制的歐盟指令提案中，特別於第七條規範未經請求之商業通訊（unsolicited commercial），規範對象包括透過電子郵件以及討論群傳送未經請求之商業訊息，要求其「必須特別註明，讓收件人未開信前即可得知此為商業通訊」。同時指出原歐盟指令有

[109] 參閱張雅雯著，大量商業性電子郵件廣告之法律問題與管理機制，資訊法務透析，八十八年九月，頁 20。

關個人資料處理以及通訊中隱私權保護之規定【Article 10(2)of Directive 97/7/EC,Article12（2）of Directive 97/66/EC】，並無法涵蓋未經請求商業電子郵件問題，因此有必要提案增定新指令，未來期能進一步透過會員國於消費者保護法或公平交易法加以規範。但歐洲反對未經請求商業電子郵件聯盟（EuroCAUCE）批評此提案，僅讓收件人不必打開信件即可刪除，處理的問題有限，並無法有效解決收信人在傳輸、下載、儲存上耗費不必要時間與費用之問題[110]。

第三款　我國處理機制之分析與建議

我國大量電子郵件廣告之處理機制可由技術管理、自律管理與政府管理三個方向分析。

一、技術管理面

國內 ISP 在電子郵件的過濾技術上，像 Hinet 的自動偵測程式、SEEDNet 過濾特定網域之信件、大眾的「垃圾終結者」，皆是透過科技輔助來處理未經請求之電子郵件廣告的問題。美國 AOL 採用的工具”PreferredMail”，預先把寄未經請求之電子郵件廣告的網域名稱輸入，將來由此網域發出的電子信件就會自動被過濾掉，AOL 的用戶便不會受到這些廣告信件的騷擾。但是，如果某用戶想要收到特定之廣告信，可以找出發出該特定廣告信的網域，並將針對該網域部分的過濾設定解

[110] 參閱張雅雯著，大量商業性電子郵件廣告之法律問題與管理機制，資訊法務透析，八十八年九月，頁 24-25。

除掉，便可以收到自己想要的廣告信了，而其他的廣告信仍然照常被過濾掉。而由 E-Scrub Techonlogy 發展出的”DeadBolt”，功能與”PreferredMail”類似，設定寄發電子廣告信函的黑名單，再將由黑名單所列的網域寄來的信通通過濾掉。

將之分類，過濾電子廣告信的技術大致有下列幾種：一是確認發信源頭的 ISP、Domain Name 或回郵地址，將從預設的 IP、DNS、e-mail address 發出的信件一律過濾掉；但是此一方式將同一來源的信件，不論是不是廣告信全數刪除、無一倖免，所以不夠精確，而且當發信者設定第三者之 IP 為發信源頭，並不斷變換，這招過濾方法便行不通。其次，亦有 ISP 設定一定時間內發信量過大者，即以自動偵測程式加以過濾；這種不問內容、以量過濾的方式，很容易誤砍無辜信件，例如他人訂閱之電子新聞、雜誌等，而發信者反制過濾時只要分批發信、每次發信量不超過攔截標準，便可躲過攔截。國內第一大網路服務公司 Hinet 於一九九七年三月為過濾電子廣告信，採用的電子化自動偵測程式誤刪了六萬用戶訂閱的 PC HOME 新聞，成為喧騰一時的新聞事件，刪與不刪似乎都有困擾。另外，以內容中的關鍵字過濾的方式，例如美國一過濾軟體分析兩百萬封廣告信後，發現廣告信標題多含「免費提供」、「！」或「？」，因此設定凡電子郵件中含有此類字眼與符號者，一律過濾；這個方法同樣會產生誤刪使用者想要之郵件卻漏掉廣告信之缺失。

上述過濾技術可分為由 ISP 端過濾與由使用者端過濾兩種，從實用面觀察，ISP 端可直接過濾省去儲存與處理廣告信件的成本，但會有 ISP 越俎代庖替使用者決定是否看過廣告信之爭議；而等到由使用者端才過濾，缺點則是 ISP 仍須花費處理與儲存廣告信件之成本。

從法律觀點來看，由使用者端過濾較為精確，使用者自行設定 IP、

DNS、關鍵字等較無紛爭；因為一但這樣的選擇權交由 ISP 執行，發信者可能會質疑 ISP 並無權利從中攔截寄給收信者之廣告信（除非收信人授權），而收信者則可能質疑 ISP 無權利為其決定其是否收受廣告信以及收哪些廣告信，侵害其接受資訊之自由；甚至，有些 ISP 為了增加過濾軟體刪除廣告信之精確性，避免誤刪信件，偶爾還抽樣檢閱是否為廣告信，這更侵犯了使用者隱私權，而產生侵害使用者言論自由權或隱私權之疑義。

為避免上述 ISP 誤刪信件、侵犯言論自由與隱私權等爭議，建議在處理流程中加入給予使用者選擇的機制，例如：於契約中說明 ISP 處理電子廣告信件之政策，讓使用者決定是否選用該家 ISP；或 ISP 雖提供過濾電子郵件廣告之服務，但事先提供使用者是否交由 ISP 過濾的選擇權。

目前技術上陸陸續續有業者開發讓消費者選擇電子廣告信的產品，例如，加州的 Power Agent，讓網友自由填選有興趣收到廣告信的項目，再向商店收取費用，幫他們寄發電子廣告信函。而由 NetCreation 所提出的 Opt-In E-Mail，則讓網友由 3000 個主題中挑選出有興趣收到廣告的主題，將來便只會收到跟選定主題相關的電子廣告信。

第三節　網址名稱及商標權之侵害

網址名稱（Domain Name）之於網路世界，猶如人類社會之地址一般，所謂網址名稱即是網際網路上一個類似地址的識別碼（identifier），而網址名稱對於網路世界的重要性又不僅止於「地址」

的功用，它在網路世界中又近似於自然人之姓名或法人之名稱，網路使用者可以透過網址名稱而推斷該網站係由何人所提供或所提供之服務或資訊類型為何。此種類似姓名或法人組織名稱之特性也造成了網址名稱之相同或近似是否違反商號名稱專用權或商標專用權之爭議。故網路出現所謂「網路蟑螂」，因網域名稱(DOMAIN NAME)係採先申請先使用(不可重覆)且單一公司僅能申請固定數目網址(IP ADDRESS)，目前發現有人以多個公司名稱同時申請多個網域名稱及網址，以備將來可販賣牟利。如有非麥當勞公司搶先申請 WWW.MCDONALD.COM 網域名稱，造成該公司如欲設網頁需另謀他法或向原申請人購買的現象。

因此，網路上即發生有關網址名稱爭議之案例，例如雅虎（YAHOO）案，多係商標專用權人通常不論商品或服務類別而主張應根據其商標專用權而取得網址名稱，或是對於他人已先行登記之相同或類似網址名稱主張侵害其商標專用權。然而從商標法學之觀點看來，由於網址名稱只是網際網路上的一個電子地址，其功能僅在提供一個得使網路使用者接觸資訊之機會，並非表彰其商品或服務，故網址名稱似非可受商標法保護之「商標」。

至於網址名稱之使用是否會構成商標名稱專用權之侵害？根據商標法之一般原則，必須他人使用與商標相同或類似文字，而造成消費者對於商品來源或服務的提供者的誤認，方構成侵害。然就網址名稱之功能而言，似乎不一定會造成消費者之混淆誤認；若無造成混淆誤認之虞，自無侵害商標專利之疑慮。

第四節　網上冒名刷卡

一名自稱來自香港的網路駭客，最近在一個成人網站論壇中張貼布告，詳細公布一張信用卡的持卡人姓名、卡號及有效期限等資料，鼓勵大家「試用」這張「免費」信用卡訂閱成人網站商品，還教導網友在購物時最好不要填寫自己的電子郵件地址，以免身分曝光，這名駭客並自稱是原持卡人在網路上購物時，被他無意間破解安全模式獲得的，這名駭客還強調他自己曾盜用過這張信用卡，而且未被識破[111]。

目前網路活動雖然熱絡，然而網路環境之保密功夫尚在萌芽的階段，不少人在網路上登錄這個，訂購那個，整個晚上忙的不亦樂乎，遇到畫面不時出現提醒你注意網路上傳輸資料可能被截取的警語對話框，還覺得掃興透了，進而選擇「以後不要再出現此警語對話框」的人，大有人在（為數不少）。平常遇到有人調查戶口就緊張兮兮的人，一旦到了網路上卻往往失去了警覺心，成為掏心挖肺有問必答的的透明人，許多在網路上傳輸的個人資料往往是以明碼進行，一旁伺機而動的網路駭客於是有機可乘，截取資料做不法用途，上述案例即是明證。

關於駭客於網路上干擾或變更個人資料傳輸路徑以截取資料供不法使用之行為，依電腦處理個人資料保護法第三十四條規定，意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法輸出、干擾、變更，刪除或以其他非法方法妨害個人資料檔案之正確，

---

[111] 參閱李智祥著，「網上冒名刷卡，駭客觸法多」，法律與你，民國 86 年 10 月，頁 144。

致生損害於他人者，處三年以下有期徒刑、拘役或科新台幣五萬元以下罰金。而截取他人信用卡之資料是否該當刑法上之竊盜罪，有認為此信用卡之資料在網路上轉成電磁記錄，依新修正刑法第三百二十三條之規定，電磁記錄關於竊盜罪以動產論，進而認為在網路上截取信用卡資料之行為該當刑法之竊盜罪[112]。惟竊盜罪構成要件中的「竊取」，刑法上的解釋是行為人破壞原持有人的持有支配關係而建立新的持有支配關係。然而此處所謂截取電磁記錄的情形，事實上指的是以重製之方式獲得該電磁記錄。一方面固然行為人是得到他人的電磁記錄的內容，建立其對於電磁記錄內容的持有支配關係，但是另一方面，電磁記錄之持有人並未因此而喪失他對於電磁記錄內容的持有支配關係。此種電磁記錄事實上之特性，使得所謂竊取電磁記錄根本沒有辦法該當於刑法上竊盜罪的竊取要件，自然不能構成刑法上的竊盜罪。

又駭客自己盜用他人信用資料進行交易獲得財物或財產上之不法利益之行為，實務上認為因駭客本身並非授信之合法對象，其以詐術行使此項信用資料而獲得財物或財產上不法利益，已該當刑法第三百三十九條之詐欺罪[113]。惟有疑問者，乃被害人為者？特約商店就駭客冒用信用卡消費之款項，仍得向發卡機構請求支付，是特約商店之全體財產並無減少，則特約商店是否為詐欺罪之被害人，即有疑義。按各種財產犯罪，可區分為「對個別財產之犯罪」與「對全體財產之犯罪」二種。前者係指只要被害人之財物本身有損失時，行為人即構成犯罪，即使其全

---

[112] 參閱李智祥前揭著，頁 145。

[113] 參閱林邦樑著，信用卡法律問題之研究，台灣台北地方法院士林分院檢察署八十三年度研究發展報告，民國 83 年 7 月，頁 48-51。

體財產可能未受損害，亦不影響其犯罪之成立；而後者則不論個別財產有無損失，如全體財產未減少，即未發生損害，申言之，即不構成犯罪。依目前學界之通說，刑法第三百三十九條第一項之詐欺取財罪係屬於對個別財產之犯罪，而同條第二項之詐欺得利罪，則屬於對全體財產之犯罪。是駭客不法利用截取之信用卡資料向約商店詐得財物，縱使特約商店得請求發卡機構撥付款項，其全體財產不致受有損害，惟特約商店既誤認冒用者為合法之持卡人而交付財物，其喪失對該貨物之持有，本身即屬一種損害，故特約商店亦屬被害人。但亦有學者持反對看法[114]，認為冒名刷卡之情形，由於特約商店只要履行一定的義務，即使是信用卡被冒名刷卡之情形，發卡銀行還是必須給付消費價款。因此對於特約商店而言，根本不在乎使用人是否為無權使用信用卡，更何況網路購物不同於一般持卡消費，不須持卡人之親筆簽名，特約商店更無從認定使用者是否為無權使用。故行為人並非使用詐術使人陷於錯誤，所以不構成傳統的詐欺罪。另外，從發卡銀行受到損害的角度來看，由於信用卡的使用並非持卡人為發卡銀行處理事務，所以也不構成背信罪。然得否以刑法第三百三十九條之三加以規範？首先，本條所規定的所謂的取得財產或是財產利益，都必須透過製作財產權之得喪、變更記錄而取得他人之財產或財產利益。然而使用信用卡購物，其取得購買物品是因為買賣關係而取得的，並不是因為製作財產權之得喪、變更記錄而取得的。其次，刑法第三百三十九條之三是所謂類似詐欺罪的規定，除了行為對象涉及機器外，基本上還是具備詐欺罪之性質，但是網路冒名刷卡之行為卻完全不具備詐欺的基本性質，所以立法者若有意對此等行為造成發卡

[114] 參閱黃榮堅著，刑罰的極限，月旦出版公司，民國 87 年 12 月，一版，頁 329-330。

銀行之損害加以規範，技術上應另外單獨加以規範。

再者，該名駭客上網鼓勵網友一起來不法使用所截取之信用卡資料之行為，由於網路係供不特定多數人閱覽即交換資訊的地方，這位駭客又係用文字、圖畫等傳播力較強的工具公然煽惑他人犯罪，因此亦該當刑法第一百五十三條之煽惑他人犯罪之罪。

第五節　癱瘓服務攻擊

第一項　發生

八十九年二月七日下午起一連三天，駭客連續攻擊大型網站從平均每天使用者高達八百七十萬四千人的雅虎開始，當機時間長達五小時，幾乎同一時間，首日在那史達克交易所掛牌上市的網路零售商 buy.com，也從下午二時起連續當機六小時。雅虎估計數小時的當機至少損失五十萬美元。

網路駭客族「食髓知味」，八十九年二月八日週二下午五時三十分起陸續再向網路最大零售商亞馬遜 網路最大拍賣商電子海灣 eBay 及有線電視新聞網 CNN 的網站「下手」，當機時間從三點五小時至五小時不等，由於手法與前一天類似，已引起美國聯邦調查局的注意，認為這是一項有組織有預謀的犯罪。隨即在八十九年二月九日週三再傳出新的「受害者」，分別是網路證券商 E*Trade 及科技新聞網路出版商 ZDNet，晚上七時起這兩個每天平均上網人數分別達十八萬三千人及七十三萬四千人的大型網站，當機三個多小時。

這七個遭駭客攻擊的網站除了 CNN 和 ZDNet 沒有網路商務交易活動，其他的網站都有大量的網路交易，雖然在當機過程中網路駭客並沒有竊取這些公司的內部機密資料，也沒有盜用客戶的信用卡資料，但已對市場倚賴日深的網路商務交易投下令人擔心的變數，如果不及早防堵將造成更大的財務損失。且由於駭客藉由不知情的第三者群起癱瘓包括網路最大搜尋引擎雅虎等網站，手法高明，即使司法單位聯手調查，恐怕也很難查出這些駭客的真正身分，網站安全如果不能及早強化，將是未來發展網路經濟的致命殺手。

第二項 攻擊方式

究竟網路駭客是如何癱瘓這些高知名度的網站？根據專家表示，基本上網路駭客先利用一部電腦在網路上找一些沒有「防火牆」，也就是對駭客沒有特別防範措施的電腦，駭客在找到這些無辜的「第三者」後，取得進入這些電腦的管道，再利用這些電腦作為攻擊特定網站的工具。而美國聯邦調查局在查獲能用來在網路上發動諸如此類攻擊的工具後，向各網站發佈警告。這些工具程式很容易在網路上找到和下載，使得駭客更能得心應手。目前仍很難抓到躲藏在假冒網址背後發動攻擊的駭客。

由於駭客進行的癱瘓服務攻擊必須使用第三者的電腦作

為攻擊起點，然後在電腦內植入程式，讓駭客可以從遠端下指令，對目標網站發出大量的資訊，導致受害網站不勝負荷而當機。據調查發現，作案電腦不只在美國境內。調查人員發現駭客利用德國境內一台電腦攻擊美國知名網站，充分印證網路無國界的特性。

美國聯邦調查局發現加州大學聖塔巴巴拉分校的一台電腦，是這次駭客攻擊著名網站時的中繼站。加州大學的一名發言人表示，捲入本案的這台桌上型電腦，隸屬該校的一間實驗室，當有線電視新聞網的網站受到攻擊之前，這台電腦一度遭過駭客闖入。不過，根據美國聯調局的調查，它只是被駭客選中的一個「分身」而已。當駭客發動大規模攻擊行動之初，都會先入侵一些不相干的電腦，並把這些不相干的電腦做為它們的中繼站，故佈疑陣來掩飾真正的攻擊行動。而網路駭客們最喜歡選擇的對象，便是大學裡的電腦系統。

駭客破壞網站的方式粗分為兩種，首先是發動所有之前被設定的電腦同時間向特定的網站發送訊息，並尋求確認，由於網站在同一時間收到太多的電腦指令，負荷過多因而當機，電腦無法運作；另一種方法則是，駭客利用挑選好的電腦群向特定的網站傳送一些電腦無法理解的資訊，由於亂碼過多導致電腦當機。電腦專家認為，從近日來網站接連癱瘓案例來看，駭客的攻擊行動至少計畫了數個月之久，絕非「一時興起」所為，駭客人數也可能不只一個人。在每項攻擊行動中，駭客使用一種技術劫持網際網路上的數十台、甚至數百台電腦，然後指示這些被劫持的電腦使用一些毫無意義的資訊對目標網站進行

轟炸。因為網站的伺服器企圖容納所有這些假資訊，不消多久，伺服器的記憶容量和其他資源就耗費精光。結果遇上真的顧客時，它的反應不是緩如牛步就是完全停止。儘管這種攻擊行動會癱瘓伺服器提供網頁給顧客的能力，卻不致破壞系統的完整性，也無法取得儲存在伺服器中的資料，所以不致危及一些諸如信用卡號碼等敏感的顧客資料。據雅虎公司表示，該公司在網際網路上遭到「五十幾台電腦」的資訊轟炸。

由於電腦的安全系統並未遭實際入侵，因此，僅為「癱瘓服務攻擊」，純係因駭客傳送龐大資訊導致其他人一時之間實際上根本無法利用該網站。但倘若用戶設法進入網站，仍能正常使用網路提供的服務。

第三項　中文網站的隱憂

網路駭客橫行，繼續對美國主要網站發動攻擊，以美國最大的網站都無法倖免駭客的侵襲，相形之下，台灣的中文網站更為脆弱，必須加強軟硬體防護措施。雖然駭客族並未進入這些網站竊取公司及客戶的資訊，但已令網路業者及消費者坐立難安，對電腦網路及電子商業的發展構成直接威脅。最近的駭客攻擊行動證明了網路是相當脆弱的，美國的主要網路公司投資了大量金錢與人力，保護網站的安全，但仍無法阻止駭客族的攻擊。台灣網際網路在追求快速發展的同時，往往不願投資在防護措施上，現在事實證明了這些駭客族可輕易對全球任何一個角落的網站進行攻擊，台灣的網站可能更不堪一擊。

根據專家指出，加強網站的安全防護是一項非常昂貴及無趣的工作，有時甚至感到是無謂的浪費，卻又不得不作，最近的事件將可喚起網路公司的危機意識，迫使所有網路公司加強「防火牆」等工作。因為駭客行動是一視同仁，不但是民間的商用網站，政府及私人的網站也可能成為他們攻擊的目標，換而言之，任何網站都應有安全警覺，建立最完善的防護體系。

目前駭客族的動機仍不明朗，這些駭客可能只是想證明他們是「無敵的」，即使如此，他們的行動已造成有形及無形的傷害，如此一來，所有網站今後必須要作更多的安全投資，而消費者對網路安全的信心可能也有待重新建立。

第四項　癱瘓服務攻擊行為之刑事責任

依據刑法新修正之第三百五十二條第二項規定，凡干擾他人電磁紀錄之處理，足以生損害於公眾或他人者，可處三年以下有期徒刑、拘役或一萬元以下罰金。判斷可否援引該條文據以處罰發動癱瘓服務攻擊之網路駭客之關鍵，第一，在客觀要件上，必須有干擾他人電磁記錄處理之行為；第二，在主觀要件上，行為人必須有干擾他人電磁記錄處理之故意存在。有認為干擾他人電磁記錄之處罰規定在刑法第三百五十二條，其處罰與毀損文書罪相同，因認為此處之電磁記錄需符合刑法上文書之條件[115]，惟刑法第三百五十二條第二項既稱干擾他人「電磁記錄」

[115] 參閱註 102。

而未稱文書，解釋上因認為此處所稱之電磁記錄應惟較廣義的電磁記錄，而非較狹義的電磁記錄僅指準文書。而癱瘓服務攻擊有二種攻擊方式，一種是網路駭客設定電腦同時間向特定的網站發送訊息，並尋求確認，由於網站在同一時間收到太多的電腦指令，負荷過多因而當機，電腦無法運作；另一種方法則是，駭客利用挑選好的電腦群向特定的網站傳送一些電腦無法理解的資訊，由於亂碼過多導致電腦當機，此等行為已屬故意干擾他人電磁紀錄，應該當刑法第三百五十二條之構成要件。

第六節　網路不實廣告之規範與相關法律責任

網路商家若在網路上刊登不實廣告以詐術使人陷於錯誤，用以牟取不法的利益，可能該當刑法第三百三十九條「意圖為自己或第三不法所有，以詐術使人將本人或第三人之物交付」的詐欺罪；可處五年以下有期徒刑、拘役或科或併科一千元以下罰金。前述『複製人』或網路老鼠會廣告的刊登人，涉嫌以欺騙手段讓網友誤信其廣告所言為真而交付金錢，諸如付廣告主二十萬美金換取『無性生殖』，或是將錢附在幸運信內寄回給廣告主或其指定之人等，都是刑法第三三九條詐欺罪所規範的行為。

除了刑法外，國內各行各業的商家上網路作生意刊登廣告，均需遵守消費者保護法第二十二條企業經營者應確保廣告內容之真實之規定，不得任意刊登不實廣告。而公平交易法第二十一條也規定企業不得在商品或其廣告為不實或引人錯誤之表示。

除了消費者保護法與公平交易法之外，針對各種有關人體健康的事業，可供規範網路不實廣告的法律還有醫療法、藥事法、食品衛生管理法與化妝品衛生管理條例，違反的廠商會被處以罰緩或停業、吊照等行政處分。食品衛生管理法第二十條便規定食品商有真實廣告的義務，不得藉大眾傳播工具播載虛偽、誇張、捏造事實或易生誤解的廣告；如果某飲料廣告商藉由網際網路這個大眾傳播工具刊登廣告，聲稱該飲料之健康屬性深具某種「特異功效」，如果與事實不符而有誇張或捏造的情形，依同法第三十三條，負責人將被處以三千元以上三萬元以下罰鍰，情節重大或一年內再犯者，甚至會被吊銷營業或設廠許可證照。坊間有許多美容豐胸瘦身乳膏或藥品，莫不誇大強調其迅速功效，假設上網廣告有虛偽誇大的事實，根據化妝品衛生管理條例第二十四條，禁止廠商於傳播工具登載虛偽誇大之廣告；像同法第三十條對此可處分五萬元以下罰鍰，情節重大或一年內再犯者將被吊銷營業或設廠許可證照。

針對網路醫療與藥物廣告管理亦有詳盡規定。醫療法為防範不實廣告於第六十一條規定，醫療機構刊登醫療廣告不得假借他人名義宣傳或以「祖傳祕方」等方式廣告宣傳；假設某醫療診所上網刊登以「祖傳祕方」治病的廣告訛詐消費者，便違反了第六十一條，而根據同法第七十七條的規定，這個診所可能被處以一個月以上或一年以下停業處分，嚴重者還會被撤銷開業執照或醫師證書。而藥商上網廣告則須注意藥事法第六十八條規定，藥物廣告不得假借他人名義、藉採訪報導或以其他不正當方式宣傳，違反者會被處以三萬元以上十五萬元以下罰鍰。

第七節　MP3 之著作權問題

在過去, 要將一片 CD 上之音樂儲存於磁片上必須使用數百片磁片, 如果要將一首歌曲從網路上下載，需要數小時，不會有人去從事這種沒有效率的儲存傳輸工作, 直到 MP3 音樂檔案格式發展後, 一切改觀。MP3 音樂檔案格式目前已成為網路音樂的標準，其原本只能在電腦上播放, 自從一九九八年下半年, 美國 Diamond 公司製造出 Rio MP3 隨身聽(美金約 200 元以下，台灣市場目前約新臺幣 6500 元)後，在唱片界造成不小的震撼, 主要在於著作權如何保護之問題。根據一九九九年五月四日 PC Home 電子報的報導，一九九八年底在美國引起廣泛爭議的 Diamond Rio PMP300 隨身聽（以下簡稱 Rio), 將透過代理商正式引進台灣, 且與各大網際網路服務提供者（以下簡稱 ISP）及網際網路內容提供者（以下簡稱 ICP）合作推廣 MP3。這則消息透露出廠商看好 MP3 音樂的市場前景。但美國五大唱片公司之一的 EMI 公司的統計指出，MP3 格式的風行不但使得美國唱片業者因此每年約損失 50 億美元的盈收, 更使得購買唱片的主要消費群，也就是 15 至 24 歲的消費者減少購買。這些數字已經足以顯示 MP3 的確成為網際網路上傳輸音樂的主要格式, 以下本文將先就 MP3 的技術面做一簡單介紹，再進一步分析其相關著作權法上的問題。

第一項　MP3 格式

MP3 全名為 MPEG Layer3(Moving Picture Experts Group 1, Audio Layer 3)，是聲音壓縮標準的一種。MPEG 聲音壓縮技術目前共分三層,

它們是 MPEG Layer1、 MPEG Layer2 及 MPEG Layer3。層次愈高，壓縮技術複雜度就愈高。MPEG Layer1 的壓縮效率為一比四，MPEG Layer2 的壓縮效率為一比六至一比八之間，MPEG Layer3 的壓縮效率則可達一比十至一比十二之間。換言之，使用 MP3 技術可以將一般音樂檔案壓縮成十至十二分之一的數位錄音檔案。例如一般 CD 中一首原檔案 40　50MB 大小的歌曲經過壓縮後只有 3.3　5MB 的大小，以現有之技術，一張 640MB 的 MP3 光碟可以放得下近 200 首歌，台幣 200 元至 400 元的 MP3 大補帖就可以容納 12 張專輯。[116]。

MP3 的 CD 製作方式首先利用電腦取得 CD 音樂檔，再用電腦 MP3 壓縮軟體，將音樂壓縮成 MP3 格式的聲音，隨後用光碟燒錄機將檔案燒錄在光碟上，使用者祇要利用 MP3 解壓縮軟體就可以播放音樂。此外，利用 MP3 技術經過壓縮後的音樂之播放音質聽起來與 CD 的音質相去不遠。MP3 使用「失真性壓縮演算法」過濾掉人類無法聽到的聲音以獲取更多儲存空間，因此，以 MP3 技術壓縮後的音樂，實際上應該會比 CD 差，所以讓人聽起來像是沒有經過壓縮一樣，不過那種失真度是人類聽覺所無法察覺，於是它就被很多人利用來將音樂做成 MP3 的音樂檔。由於 MP3 是使用數位格式，反復重播也不會受壓縮及解壓縮程序影響到品質，其音質媲美 CD，亦不會因震動而跳針，極適合運動或通勤者使用。另外，播放 MP3 音樂只需要上網路下載免費播放程式即可，例如目前網路上使用最普遍的 Winamp，只須一台個人電腦，不需要其他特殊硬體設備。在

[116] MP3 之著作權法問題，常天榮著，資策會科技法律中心，參閱網址 http://stlc.iii.org.tw/stlc_c.htm；MP3 所帶來的著作權問題，章忠信著，參閱網址 http://sparc.nhltc.edu.tw/~honda/audio/mp3/mp3.htm。

這種種誘因之下，MP3 使用者自然愈來愈多，一時之間在網路上日益普及流行。

第二項 MP3 隨身聽案例

MP3 不但已經造成美國唱片業者流失大量主消費群，還造成唱片公司每年損失 50 億美金的收入。因此當生產音效卡起家的美國 Diamond 公司開始生產販售播放 MP3 隨身聽時，美國唱片工業協會(Recording Industry Association of America Inc.；以下簡稱 RIAA)就與之展開一場訴訟[117]。

本案發生於一九九八年十月，因本案被告 Diamond 有鑑於 MP3 技術能將音樂壓縮成原長度十二分之一的數位錄音檔案而絲毫不影響在網路上播放的音質，又能方便網路族下載後快速儲存在個人電腦的硬碟中，播放 MP3 格式音樂檔案的隨身聽勢必成為市場上的熱門商品，於是計畫生產可以播放 MP3 音樂檔案的隨身聽，並決定於去一九九八年十一月二十三日起販售。此舉遭到 RIAA 的嚴重反彈，在同年十月九日就向加州中區地方法院提出申請，主張 Diamond 的行為違反美國現行著作權法第十章第十七條，其生產之 Rio 屬於一九九二年美國家用錄音法(Audio Home Recording Act of 1992，即美國現行著作權法第十章)所定義的數位錄

[117] MP3 之著作權法問題，常天榮著，資策會科技法律中心，參閱網址 http://stlc.iii.org.tw/stlc_c.htm；MP3 所帶來的著作權問題，章忠信著，參閱網址 http://sparc.nhltc.edu.tw/~honda/audio/mp3/mp3.htm。

音設備(digital audio recording device)之一種，因而要求法院暫時禁止 Diamond 銷售該隨身聽的行為[118]。該法案為了彌補著作權人因為消費者自行使用數位錄音設備錄製音樂著作，造成音樂著作相關權利人於產品銷售上所可能產生之損失，規定生產數位錄音設備之廠商均應於所生產之的設備中使用系列重製管理系統〔Serial Copy Management System，簡稱 SCMS〕或其他具有相同功能的系統，以避免數位錄音媒介遭大量重覆地重製。此外，生產、進口或銷售數位錄音設備及數位錄音媒介之廠商更必須向美國著作權局繳交使用報酬，以便於分配予相關著作權人。

Diamond 生產的隨身聽名為 Rio，記憶體容量為 32MB，雖然不大，但可以外接記憶卡以增加記憶容量，正因為記憶卡外接可以移動的特性，使用者就能夠將電腦中的 MP3 音樂錄到該記憶卡上，也可以將錄好音樂的外接記憶卡轉借給其他 Rio 使用者。就 Rio 本身的功能而言，它只能播放，除非連接電腦，否則不能錄音。另外，Rio 沒有輸出功能，所以也無法將錄進去的音樂傳輸到其他設備上。

被告 Diamond 針對 RIAA 的主張，提出具體反駁，認為 Rio 的功能只是單純地將已經被壓縮的音樂檔案重新播放(playback)，但並不具備美國家用錄音法中所規定的「獨立的錄音功能」(independently capable of making recordings)，因此 Rio 不算一種錄音設備，不應該屬於美國家用錄音法定義下的數位錄音設備。但加州法院法官並不同意 Diamond

---

[118] MP3 之著作權法問題，常天榮著，資策會科技法律中心，參閱網址 http://stlc.iii.org.tw/stlc_c.htm；MP3 所帶來的著作權問題，章忠信著，參閱網址 http://sparc.nhltc.edu.tw/~honda/audio/mp3/mp3.htm。

這項說法，法官的理由有二項：第一項，法官認為從美國家用錄音法法條的文字上來看，該法只要求所謂的數位錄音設備具有錄音之功能，並沒有規定此一功能必須可以獨立運作；第二項，如果採取 Diamond 對於法條的解釋見解，將會違反該法保護著作權人的立法目的。

暫時禁止令的申請如果想要獲准，原告必須能夠說服法官，如果法官不核發時，原告自己將受到之傷害是「不可回復」的。雖然法官認為 Rio 應受該美國家用錄音法的規範，但針對於 Diamond 販售 Rio 的行為可能造成原告不可回復之傷害這個部分，法官的看法是，雖然損害的確有可能造成，但根據美國家用錄音法之規定，任何生產數位錄音設備的廠商都必須在其所生產的設備中使用複製管理系統(serial copy management system)或其他具有相同功能的系統，以避免數位錄音檔案遭到非法盜錄。此外，為了彌補著作權人因為消費者自行使用數位錄音設備錄製音樂以後，在音樂產品銷售上所可能產生的損失，生產數位錄音設備的廠商還必須根據規定向美國著作權局提存一定的權利金，以便將其分配給相關著作權人。因此法官認為 RIAA 可能受到的損害可以因為適用該法中關於權利金(royalty)分配的規定獲得補救，所以並不是不可回復的損害(irreparable injury)，因此駁回 RIAA 的請求[119]。加州洛杉磯聯邦地方法認定 Rio 並非「家用錄音法案(Audio Home Recording Act)」所稱之數位錄音設備，不必裝置 SCMS，亦無須繳交使用報酬。原告 RIAA 不服，向聯邦第九巡迴法院提出上訴。1999 年 6 月 15 日，法院以全票

[119] MP3 之著作權法問題，常天榮著，資策會科技法律中心，參閱網址 http://stlc.iii.org.tw/stlc_c.htm；MP3 所帶來的著作權問題，章忠信著，參閱網址 http://sparc.nhltc.edu.tw/~honda/audio/mp3/mp3.htm。

通過，駁回上訴(Recording Industry Association of America, et al. v. Diamond Multimedia Systems, U.S. 9th Circuit Court of Appeals 9856727 , June 15, 1999)。此一判決對於錄音工業誠為一大打擊，使得藉由網路下載錄音著作之侵害無從遏止。

聯邦第九巡迴法院法官於判決中指出，從「家用錄音法案」所定義之「數位錄音設備」字面觀察，電腦或其硬碟之主要目的並不是在供製作數位錄音設備，因此不能認為是「數位錄音設備」(Under the plain meaning of the act's definition of digital audio recording devices, computers (and their hard drives) are not digital audio recording devices because their 'primary purpose' is not to make digital audio copied recordings)從而不必裝置 SCMS，亦無須繳交使用報酬。法院更進一步說明，Rio 僅在使一般消費者電腦硬碟上之檔案得被攜帶外出，完全符合「家用錄音法案」促進個人利用之立法目的。

第三項　MP3 與我國著作權法間的關係

目前在網路上隨處可見提供免費 MP3 音樂下載的網站，MP3 具有之小容量和音質佳的特性，除了是使用者個人自製音樂精選集的絕佳工具，也吸引不少校園裡的熱心同學將 CD 內的音樂壓縮成 MP3 格式上載到網路，提供其他同學下載聆聽，為莘莘學子們省下不少的零用錢。但此種行為究竟有無違反我國著作權法之規定，以下本文試依我國著作權法上的規定分析其法律責任。

第一款　音樂著作權

依我國著作權法第五條之規定，本法所稱之「著作」共有十種，而與音樂有關的有「音樂著作」以及「錄音著作」。音樂著作包括曲譜、歌詞及其他之音樂著作；錄音著作則包括任何藉機械或設備表現系列聲音而能附著於任何媒介物上之著作。所以一首歌曲可能存在數種著作權，包括詞、曲的音樂著作、將詞曲錄製成音樂的錄音著作，如果該音樂著作是一首演唱曲，若該演唱人的演唱具有原創性時，則會另外成立表演著作。

第二款　以 MP3 標準壓縮他人音樂或錄音著作之刑事責任

如將他人的音樂或錄音等著作之音樂檔案以 MP3 標準壓縮，此種轉換的動作，實際上即是一種「重製」的行為。依我國著作權法第三條第五項之規定，所謂重製是指以印刷、複印、錄音、錄影、攝影、筆錄或其他方法有形之重複製作。而壓縮他人音樂著作，就其行為本身是包括複製以及壓縮兩個程序，因此該當我國著作權法中「以其他方法有形之重複製作」的要求，屬於我國著作權法規定所稱之重製行為。而依著作權法第二十二條之規定，著作人除本法另有規定外，專有重製其著作之權利。未經著作人之同意擅自重製其著作，即為侵害著作權之行為，依著作權法第九十一條之規定，擅自以重製之方法侵害他人之著作財產權者，處六月以上三年以下有期徒刑，得併科新台幣二十萬元以下罰金。

第三款　將他人 MP3 音樂下載到自己家用電腦中

並非所有的著作使用權都屬於著作人。著作權法為了促進文化發展，平衡著作人以及使用人的權利，還是預留一塊供人合理使用各項著作的空間。此項空間即規定在著作權法第四十四至第六十五條，只要符合其中任何一條的規定，就可以在不經過著作人授權之情形下使用其著作。對於一般個人而言，依著作權法第五十一條之規定，供個人或家庭為非營利之目的，在合理範圍內，得利用圖書館及非供公眾使用之機器重製已公開發表之著作。例如為了節省自己存放空間的目的，使用自己家裡的電腦，將多片自己擁有的 CD 製作成 MP3 格式，此種方式即屬合法。但是使用必須在「合理範圍」內，如果使用者集合多張朋友的 CD 製作「精選集」，應該就不屬於合理使用的範圍。至於由網路下載檔案的行為是否合法，基本上，下載實際上亦為複製檔案加上傳輸檔案兩個程序，故亦屬於著作權法所謂「重製」之行為，因此，為供個人使用而由網路下載一份檔案的這種重製行為，即可主張著作權法第五十一條的合理使用。

第四款　將他人 MP3 音樂上載或轉寄

檔案的上載和轉寄均與下載相同，亦屬於一種重製的行為。但除了重製之行為以外，實際上也涉及了傳輸的行為。雖然我國著作權法中，並無任何規定對於傳輸的行為做直接的規範，不過著作權法第二十四條第一項「著作人專有公開播送其

著作之權利」的規定，論者有認為可以擴張解釋來包括網路傳輸的行為。依著作權法第三條第一項第七款的規定，所謂的公開播送是指基於公眾接收訊息為目的，以有線電、無線電或其他器材，藉聲音或影像向公眾傳達著作內容。依照這樣的定義，似乎可以包含網路，因為網路傳輸即屬以其他器材的方式進行，同時網路傳輸的目的也在向公眾傳達著作內容，而傳輸的內容可以是聲音或影像。惟亦有持反對見解者，因為公開播送權的制訂原本是針對無線電廣播與有線電視的播送，並無意規範網路上的傳輸問題。

我國現行著作權法的規定對於網路傳輸既無明確規範，適用公開播送權又有立法背景不同的考量，如果採取擴張解釋適用公開播送之規定於這些相當於網路傳輸的行為時，那麼，未經著作人同意而於網路上公開播送其著作者，依照本法第九十二條之規定，將被處以三年以下有期徒刑，得併科新臺幣十五萬元以下罰金。以此為常業者，根據第九十四條之規定，則會處以一年以上七年以下有期徒刑，得併科新臺幣四十五萬元以下罰金。此與罪刑法定主義之原則有違，因此，本文認為不應就此部份做擴張解釋。

第五款　小結

不論 MP3 帶給著作人的是危機還是契機，單就 MP3 這個技術而言，突顯出網路科技的發展日新月異，不斷地會帶給傳統著作權法各式各樣的衝擊，唯有積極瞭解國際發展趨勢，修改本法律中無法配合科技發展

的部分，如此，才能夠在這個數位時代裡繼續保障著作人以及使用人雙方的利益。

第六章　網際網路連線服務提供者就網路違法內容之法律責任

網際網路的發展在新興傳輸媒介中異軍突起，它快速蔓延、跨越國界且深入家庭，不但改變了空間概念，更顛覆了人們的習慣模式；然而，法律體制面對這個新領域時，卻略顯遲鈍、反應不及。由於現行法律針對傳統上壁壘分明的電信、廣播、電視等不同領域的法律規範，立法背景與立論基礎大相逕庭；但隨著數位科技的進步，電話、電視、廣播與電腦所提供之聲音、影像、圖片、資料等訊息皆可藉由網路傳送呈現消費者眼前，使得各傳訊領域的界限漸趨模糊，而網路之國際特性，更將法律適當的規範範圍由單一國家提升至全球，這一切迫使各國檢討現行法令適用於網路之可行性。

網際網路連線服務提供者（Internet Service Provider，以下簡稱 ISP）就網路上種種違法或不當內容應負的法律責任與義務為何即是顯著之例。究竟應將 ISP 視為提供通路的傳統電信業者，抑或將其與提供內容的傳播媒體業者等同看待，這根本性的問題將影響 ISP 有否過濾網路內容的能力與地位、須否與提供違法內容的使用者同負連帶責任、知悉違法或認為不妥當的內容時得否逕自移除等議題，實值吾人深入探討。

第一節　網路違法內容與網際網路連線服務提供者之關連與問題

當網路上出現誹謗、恐嚇、著作權侵害、詐欺、不實廣告等違法內容時，受害人可能一時之間無法確認行為人是誰，提供網路連線服務的 ISP 因目標顯著、財力雄厚，很容易首當其衝成為訴求對象或一併列為被告。舉例而言，Religious Technology Center，and Bridge Publications，Inc.，v. Netcom Online Communication Services，Inc.，Dennis Erlich，and Tom Klemesurd 一案，原告便要求負責連線的 ISP- Netcom Online Communication Services 中斷其他被告連線，遭 Netcom 拒絕後，旋即將之同列為侵害著作權的被告。

當 ISP 因為網路上之違法內容而被列為共同被告時，因目前 ISP 的身分定位模糊不清，導致適用法律時產生下列疑義：首先，究竟 ISP 是否會因此被認定為相關犯罪之共同正犯或幫助犯？其次，ISP 會面臨的訴求是，當網路上發現疑似違法內容時關係人要求 ISP 須即時移除該筆資料或停止放置該內容的客戶連線服務，ISP 有無義務在一定期間內回應？

最後，聲稱受害的第三人要求 ISP 提供使用者資料，根據電腦處理個人資料保護法之規定，ISP 的義務與責任為何？

第二節　網際網路連線服務提供者之定義與概況

網際網路連線服務提供者的本質究竟較傾向傳統電信業者或傳播媒體業者乃根本性問題，故宜先說明網際網路連線服務提供業者之定義，並就其服務態樣與範圍加以定位。

第一項　網際網路連線服務提供者之定義

網際網路連線服務提供者（Internet Service Provider）乃提供通路讓使用者與網際網路連線之機構。一般 ISP 提供的網路連線服務有撥接式與固接式兩種，撥接式透過數據機（modem）以電話連上網路，固接式則是透過數據專線（ISDN）、ATM 等固接式電信網路加以連線。除了上述的連線服務外，另一種 ISP 常見的服務是虛擬主機（Virtual Host 、 Web Host），讓小型用戶的網站掛在 ISP 的伺服器（Server）下，即 ISP 向用戶收取費用並提供伺服器之一部份記憶體空間（space memory）放置用戶之網站[120]。

常與網際網路連線服務者（ISP）混淆之概念為線上服務提供者（Online Services Provider，簡稱 OSP），OSP 提供上線後各項網際網路加值服務，如資料庫（databases）查詢、論壇（forums）服務或各項檢索工具（如 E-mail、WWW browser、FTP 等）以便用戶取得網上資源。舉例而言，WESTLAW 提供法律資料庫之查詢、LEXIS-NEXIS 提供法律

[120] 參閱張雅雯著，網際網路連線服務提供者就網路違法內容之法律責任（上），資訊法務透析，民國 87 年 3 月，頁 30。

與新聞資訊之查詢、Dow Jones Interactives 提供財經與新聞搜尋皆為提供資料庫服務之 OSP，而美國 EasyLink（AT&T）則是提供 E-mail、EDI 等檢索工具的 OSP[121]。

雖然 ISP 與 OSP 定義有所不同，但許多大型 OSP 在提供線上服務外亦兼做 ISP，提供網際網路連線服務。像 American Online、CompuServe Information Service 這兩大 OSP 除了提供各種線上資料庫服務外，也都同時提供各種線上資料庫服務；另外，Genie 既提供 BBS、 roundtables 等論壇服務又提供連線服務亦是一例[122]。

第二項　國內 ISP 之服務狀況

目前國內使用者連上網路有三種途徑，除了少部分利用 cable modem 經有線電視的光纖纜線上網外，主要便是藉由台灣學術網路（Taiwan Academic Network ；TANET）與民間 ISP 業者所提供的商用網路連線服務連上網際網路。其中，商用網路的用戶約有八十萬，中華電信公司的 HiNet 擁有近二分之一的客戶，財團法人資訊工業策進會的 SEEDNET 次之，其他正式統計主要提供網路連線服務的 ISP 約有五十家左右[123]。

---

[121] 同註 110。

[122] 同註 105。

[123] 經濟部商業司商業自動化計劃納入統計之 ISP 為 45 家，參見 http://www.ec.org.tw/service/；資策會推廣服務處 NII 應用群所統計之台灣地區

國內的網際網路連線服務提供者目前除了提供上述 ISP 的基本業務—連線服務[124]與虛擬主機服務[125]外，大部分漸將業務擴展至連線以外的網際網路加值服務，例如 HiNet 的網路商品街（HiGo）與 HiNet104 電子查號系統，SEEDNET 的網路影音服務（Audio/Vedio Center）以及提供會員路透即時資訊，商標檢索、電子出版資料庫、股神通即時股票分析系統、聊天室、備忘錄、留言版等服務的線上資訊網；此外，市面上其他 ISP 所提供之服務尚包括 Internet 與 Internet 整體網路系統規劃架設、HomePage 設計製作、Domain Name 申請、E-mail、線上購物、視訊會議系統、網路廣告托播等等各式各樣與網路相關之服務[126]。

第三項　連線服務提供者與內容提供者之區隔

如同美國主要的網路服務公司身兼 ISP 與 OSP—同時提供連線服務與其他線上服務，台灣 ISP 也一樣不只單純地提供連線服務而已，還包

Internet 連線服務公司則有 59 家，參見 http://www.psd.iii.org.tw/inews/service.htm。

[124] 即一般網路服務公司廣告所稱之國際網路架設諮詢與安裝，國際網路撥接服務，或號稱聯接 128k、256k 專線、T1 等撥接、固接之連線業務。

[125] 一般網路服務公司廣告所稱之 Virtual Host、WWW 虛擬主機架設、虛擬主機出租服務、WWW 店面及硬碟空間承租、HomePage 放置服務皆為此類。

[126] 參閱張雅雯著，網際網路連線服務提供者就網路違法內容之法律責任（上），資訊法務透析，民國 87 年 3 月，頁 31。

含了各種網路加值服務。綜觀國內 ISP 所提供的種種服務，從公司整體電腦網路架設、安裝、諮詢顧問、虛擬主機建置、網頁（HomePage）的設計製作等，乃至 ISP 自己設置網站提供線上購物、線上廣告以及前述各式各樣的線上資訊提供與查詢，從上游到下游，從與網路連線相關的各種硬體設置到與網路內容相關的各式資訊資源的提供，網路服務提供者的身分因其服務態樣與範圍的不同而有差異，很難單純地為其下一個簡單的定位，而定位的差異將更近一步影響其對網路出現違法內容時的法律責任。

傳統法律領域內，通路服務提供者（Conduit Provider）與內容提供者（Content Provider）之法律責任與義務有相當差距。舉例而言，單純提供電話連線服務的電信業者，只提供電信通路，對客戶利用其電話所為之通訊內容無權干涉，而客戶之通話內容若涉及違法情事，傳統電信業者亦不必為此負擔法律責任[127]；相反的，提供內容的傳播媒體業者，除了必須就其本身所提供的內容負起應負的責任外，因其對刊登或播放之內容有事先編輯審閱之能力與機會，有時尚須為第三者所提供之內容負起連帶法律責任，廣告媒體事業之連帶法律責任即為實例[128]。

探究網際網路服務提供者對網路違法內容之法律責任，必先探討其定性是通路服務提供者或內容提供者，若是單純提供網際網路連線服務

---

[127] 電信法第八條第一項規定：「電信之內容及其發生之效果或影響，均由使用電信人負其責任。」

[128] 出版法第三十二、三十七、三十九、四十條，廣播電視法第二十一、四十三條，與有線電視法第三十五、五十七、六十條，對平面媒體、廣播、無線及有線電視業者提供之內容要求不得有違善良風俗或法令，違者處以行政處分或罰鍰之規定。

的業者（ISP），性質較傾向類似電話業者的 Access Provider ；反之，若是單純提供網路資料庫服務的業者（OSP），性質則傾向類似媒體服務事業的 Content Provider；比較麻煩的部分在於國內多數網際網路服務提供者既提供連線又提供與內容相關的線上服務，此時業者就網路違法內容之法律責任為何，應視該業者當時所扮演之角色，究竟是連線服務提供者、網站站主抑或本身根本是提供該違法內容之人而定。

第三節　ISP 對網路違法內容的法律責任

第一項　詐欺內容與不實廣告

隨著網路購物的流行，網路廣告量遽增；但廣告品質卻因缺乏管理機制而良莠不齊，其中不乏詐欺性廣告或不實廣告。例如前述之「雷爾運動」的「複製人」，該組織透過網路刊登複製人的廣告，向不孕夫婦及同性戀者推銷「無性生殖」與「細胞儲存」的技術，費用是美金二十萬元；然而根據生物開發科技中心的說法，目前生物技術尚無法複製人體，而且各國法令亦禁止人體複製，果真如此，在網路上廣告複製人體並收取費用，不僅不實在還可能構成刑法上之詐欺罪。

第一款　網際網路服務提供者相關法律責任

ISP 就這些網路不實廣告或詐欺性內容的法律責任為何，由於國內 ISP 業務態樣繁多，應視個案中 ISP 本身就是廣告刊登者，或是 ISP 是網路商場主人提供一般大眾廣告版面，抑或 ISP 僅只提供網際網路連線服務，ISP 扮演的角色不同、定性不同，其法律責任即有差別。

第一目　本身即是網路不實廣告或詐欺性內容的刊登者之 ISP

若 ISP 本身就是這些網路不實廣告或詐欺內容的刊登者，負擔起行為人應有的刑事責任較無疑義。像雷爾運動或網路老鼠會等為了騙取金錢而刊登不實廣告之行為，該當於刑法第三百三十九條之詐欺罪「意圖為自己或第三人不法所有，以詐術使人將本人或第三人之物交付者，處五年以下有期徒刑、拘役或科或併科一千元以下罰金。」除了刑法外，國內各行各業的商家上網路做生意刊登廣告，均需遵守消費者保護法第二十二條企業經營者應確保廣告內容之真實之規定，不得任意刊登不實廣告。而公平交易法第二十一條也規定企業不得在商品或其廣告為不實或引人錯誤之表示。此外，針對各種有關人體健康的事業，可供規範網路不實廣告的法律還有醫療法、藥事法、食品衛生管理法與化妝品衛生管理條例，違反的廠商會被處以罰鍰或停業、吊照等行政處分。

第二目　兼任網站經營者提供廣告版面的 ISP

原本單純提供連線的 ISP，若兼做 OSP 提供客戶各種網路資訊之擷取或兼營網路商場，進而提供網路廣告版面收取費用時，其性質已非原本純粹的通路服務者（Access Provider），反而較類似於傳統報業、廣播業與電視業放置或插播廣告的行為，只不過傳輸媒介改變成電腦與網路，提供廣告版面之媒體業者性質並無改變，應有消費者保護法第二十三條：「刊登或報導廣告之媒體經營者，明知或可得而知廣告內容與事實不符者，就消費者因信賴該廣告所受之損害與企業經營者負連帶賠償責任，前項損害賠償責任，不得預先限制或拋棄。」與公平交易法第二十一條第四項：「廣告媒體業明知或可得而知其所傳播或刊載之廣告有引人錯誤之虞，仍予傳播或刊載，亦應與廣告主負連帶損害賠償責任。」等廣告媒體業連帶責任之適用。

針對這個問題，行政院消費者保護委員會於八十六年曾作出解釋[129]，認為依消費者保護法施行細則第二十三條之規定，消費者保護法第二十二條、第二十三條所稱之廣告，包含了利用電子視訊、電子語音、電腦或其他方法，可使不特定多數人知悉其內容之傳播者均屬之，故網路上廣告亦屬消費者保護法規範範圍，於網路上經營廣告業務者，即屬消費者保護法第二十三條之「媒體經營者」。據此解釋，除連線服務外兼營網站廣告經營之 ISP 亦應一併適用廣告媒體經營者之連帶責任。

[129] 參見台八十六消保法字第〇〇六四八號函。

第三目　僅提供網際網路連線的 ISP

產生爭議的部份在於當 ISP 僅提供連線服務並未兼營網站廣告時之法律責任。誠如上述，單純提供連線服務的 ISP 類似傳統電信業者是 Conduit Provider，依電信法第八條第一項之規定，電信之內容及其發生之效果或影響，均由使用電信人負其責任，照此推論，ISP 的客戶在網路上刊登的廣告由用戶自負其責，ISP 並無責任。

然而，根據上述行政院消費者保護委員會函之說明，除了廣告網站經營者外，將一般的網際網路提供者亦納入規範，依此而言，連只提供連線的 ISP 亦必須為其用戶所刊登之廣告負起消費者保護法與公平交易法所課予之廣告媒體業者連帶責任。這將對 ISP 產業及網路發展造成莫大衝擊。根據消費者保護法第二十三條之規定，此一連帶損害賠償責任不得預先限制或拋棄，所以 ISP 無法於簽訂網際網路服務契約時事先限制或排除掉該責任。由於目前國內每家 ISP 的設備、技術與人力均不相同，如何判定各業者對使用其連線客戶所刊登的不實廣告「明知」或「可得而知」，一時之間恐怕難以找出標準答案；如此一來，加諸 ISP 的責任過重而且處於不明確的狀態，因為每一種情況都能被解釋成「可得而知」，如果業者想避免法律上之責任，就必須找專人天天坐在螢幕前監看、查證用戶的廣告實不實在，有無欺騙情況，在實際執行上十分困難。更何況現在 ISP 市場競爭厲害，目前大部分是賠本經營，照此解釋，業者負擔更重，經營更困難；倘使業者將因此產生的風險成本轉嫁到消費者身上，普遍提高連線費用，將減低大眾使用網路的意願，其結果恐與現階段發展網際網路的理想漸行漸遠。

詳審消費者保護法對「媒體經營者」或公平交易法對「廣告媒體業」所以規定需負連帶責任的理由，主要著眼於報紙、雜誌、電視等傳統媒體對其廣告的掌控性，這些傳統媒體實際上可以過濾、管理經由該媒體所刊載播送的廣告，顧客與其連帶責任才能督促媒體本身進行廣告管理的義務。反觀網路這個新興媒體，廣告的方式與傳統媒體截然不同，廠商的廣告甚少經由 ISP 加以排版、編輯，而是商家付費後在自己的網站廣告，ISP 並未經手。由於廣告內容數量龐大，商家製作或變更網路廣告的時間又不一定，ISP 要監控實際上很困難。既然 ISP 並無傳統媒體的能力與地位去「控制網路廣告」，縱強課以管理義務，迫其負擔連帶責任，亦難以達成如傳統媒體般的廣告管理成效，徒然加重 ISP 無謂的負擔、造成網路發展之阻礙。以目前的科技與環境而言，將 ISP 納入廣告媒體業者連帶責任範圍實不恰當。

第四目　小結

對網路上不實廣告的處理，現存的規範有刑法、消費者保護法、公平交易法、醫療法、藥事法、食品衛生管理法與化妝品衛生管理條例等等，或重或輕均對違反商家加以處分；網路廣告行為不過轉換新的宣傳媒體管道，只是工具改變而本質並無不同，斷無只因「出現於網路」就排除上述法律適用的道理，許多民眾因為網路是新興媒介就認為既有的法律規範無法適用，而誤將網路視為無政府狀態的違法天堂，政府應加強法治教育的宣傳。另外，美國聯邦交易委員會（Federal Trade Commission）前陣子便與美國國家消費者聯盟（National Consumer

League）共同發表聲明，提醒消費者如何辨識網路不實廣告提供消費者一些網路廣告陷阱閃躲祕訣，亦值得參考。

主要問題在於單純提供連線 ISP 被課與「廣告媒體業者連帶賠償責任」所產生的衝擊。現階段課予 ISP 過重責任恐有礙網路整體環境的正常發展，美國也有類似的困境，美國的國會議員 Raggio 於一九九七年在一項有關網路廣告的立法草案中，便提案規定 ISP 業者對客戶所登的廣告不須負法律責任，除非 ISP 明知或參與該廣告之準備才須負責[130]。我國若欲解套，一方面可仿效美國以立法明文限制 ISP 的法律責任，或者透過司法解釋將單純提供連線的 ISP 排除於消費者保護法「媒體經營者」或公平交易法「廣告媒體業」的範圍外；因為消費者保護法或公平交易法本身並未對「媒體經營者」或「廣告媒體業」加以定義，將 ISP 納入規範乃透過行政令函依施行細則所為之解釋，顯已逾越母法之授權，並無司法拘束力。

第二項　侵害他人著作權之內容

網路常常見侵害他人著作權之態樣為使用者或網路商家在自己的網頁上，BBS 及其他討論區非法重製、散布或轉貼他人有著作權之作品，如前述美國 Religious Technology Center 離職員工 Dennis Erich 將 RTC

[130] 參閱張雅雯著，網際網路連線服務提供者就網路違法內容之法律責任（上），資訊法務透析，民國 87 年 3 月，頁 35-36。

受著作權保護之著作物張貼於新聞討論區一案即為是例[131]。由於在網路上非法侵害他人著作權之情事因成本低廉、品質卓越而情況普遍，對著作權人而言，逐一找出不同之侵害者（網路侵害者）提出告訴實質上有困難且不敷成本，因而傾向要求 ISP 作守門員甚至擔負責任。對於 ISP 就其客戶（使用者）在網路上侵害他人著作權之行為應擔負如何的法律責任目前尚無定論，以下針對不同主張與國際上計有判例及立法趨勢歸納作介紹。

第一款　ISP 對使用者著作權侵害行為應負擔法律責任之不同主張

第一目　直接侵害責任（Direct Infringment）

著作權法的直接侵害責任概念類似於侵權行為法的無過失責任（Strict Liability）[132]，並不以認知（Knowledge）或過失之存在為責任成立之要件；原告只需證明其對該著作物擁有著作權以及對方侵害了該著作物中具原創性之部份即可，對方

---

[131] 參閱張雅雯著，網際網路連線服務提供者就網路違法內容之法律責任（中），資訊法務透析，民國 87 年 5 月，頁 17。

[132] 例如，因身分或地位而必須負擔侵權行為法的無過失責任者，如危險動物的飼養者因其飼養之動物或商品製造人因其製造之商品造成他人之損害時，其責任的成立不以其對侵害之造成有認知或有過失為成立要件，其理在於為了因為自己利益將風險引入社會之人必須承擔該風險，故課與較嚴格之法律責任。

縱無認知或過失亦可成立著作權直接侵害責任。

採直接侵害責任的典型案例是 Playboy Enterprises , Inc. v. Frena，被告 Frena（BBS 站）的使用者將原告 Playboy 雜誌的照片透過網路在該站非法重製（包括上傳與下載），Playboy 控告 Frena 允許客戶利用其網路非法重製 Playboy 受著作權保護之照片侵害其著作權，Frena 抗辯其對客戶非法侵害他人著作權之行為毫不知情，但法院認為知情與否並不影響著作權侵害責任之成立，BBS 站主縱不知情亦須為其使用者之著作權侵害行為負擔法律責任[133]。

若以此論斷網路服務提供者之責任，則當其網頁或伺服器內出現侵害他人著作權之資訊時，縱對使用者的侵害行為並無認知，亦成立直接侵害責任。美國 NII 智慧財產權報告的白皮書（White Paper）即認為[134]，網路服務提供者既然提供用戶網路服務獲取利益，便應該負擔因此產生的風險，亦即在用戶侵害他人著作權時負擔直接侵害責任是其經營業務本應負擔的成本；並以書商、錄音帶、報紙、電腦軟體等零售商亦必須負擔無過失責任為由，認為網路服務提供者應等同前述各提供流通管道之零售商，並無差別待遇之理由，故亦須負擔無過失責任適用直接侵害責任之標準。此外，網路服務提供者較著作權

[133] 參閱張雅雯著，網際網路連線服務提供者就網路違法內容之法律責任（中），資訊法務透析，民國 87 年 5 月，頁 18。

[134] 參閱張雅雯著，網際網路連線服務提供者就網路違法內容之法律責任（中），資訊法務透析，民國 87 年 5 月，頁 18。

所有人更容易透過契約或技術等機制防止用戶侵害他人著作權，且其負擔損害賠償責任後可以透過提高網路服務費或透過保險將增加成本轉嫁分擔等等，都是支持該論點的理由。

第二目　代理侵害責任（Vicarious Infringment）

代理侵害責任與直接侵害責任相同之處是都不以「認知」為責任成立要件，但不同之處是代理侵害責任的成立須符合下列兩個要件：一是被告有權力及能力控制侵權行為人的行為，二是被告直接因該侵權行為而得到財產上利益。至於 ISP 是否適用代理侵害責任，在前述 RTC v. Netcom 一案，法官以上述兩個要件檢核 Netcom，發現 Netcom 並未因使用者之侵權行為而獲致財產上利益，不符合第二個要件而排除 Netcom 適用代理侵害責任[135]。

第三目　輔助侵害責任（Contributory Infringment）

相較於直接侵害責任與代理侵害責任，輔助侵害責任的最大不同處在於要求被告對侵權行為有所認知；其次，要求被告對著作權侵害行為有鼓勵、參與或實質幫助。認為網路服務提

[135] 參閱張雅雯著，網際網路連線服務提供者就網路違法內容之法律責任（中），資訊法務透析，民國 87 年 5 月，頁 18-19。

供者可以適用輔助侵害責任的主要案例為前述 Netcom 一案，法院認為若適用直接侵害責任將使每個網路服務提供者承擔不合理的法律責任，但若 ISP 對使用者之著作權侵害行為有充分認知與實際參與，則可適用輔助侵害責任。

由於輔助侵害責任成立要件較嚴格，要求須有實際認知，對網路服務提供者較為有利，美國的 OSP 多數主張以此為其成立著作權侵害責任之標準；在美國 NII 對智慧財產權報告 Green Paper 發佈後，Computer Serve, American On-Line, Lexis, Prodigy 等主要 OSP 便針對該報告傾向認同直接侵害責任之觀點聯名反對，要求以「實際認知」（actual knowledge）為判斷其責任之標準[136]。

第四目　免責（Exempt from liability as common carriers）

單純提供電話線服務的電信業者，因只提供電信通路，對客戶利用其電話所為之通訊內容無權干涉，故客戶之通話內容若涉及違法情事，傳統電信業者亦不必為此負擔法律責任，此亦電信法第八條第一項規定：「電信內容及其發生之效果或影響，均由使用電信人負其責任。」同樣的，單純提供連線的 ISP 亦應可主張其與電話公司都是提供通路連線服務的業者，實際上對使用者利用網路連線交換的訊息內容並無權利用

[136] 參閱張雅雯著，網際網路連線服務提供者就網路違法內容之法律責任（中），資訊法務透析，民國 87 年 5 月，頁 19。

過濾、編輯、審查或監控，故不應要求對其通路上傳送之內容負責。

第二款　各國立法例

第一目　美國

前述 NII 的 White Paper 雖然對網路服務提供者著作權侵害責任的認定標準傾向於直接侵害責任，但由於爭議性過大，報告中並未提出明確統一的標準，而是建議將該議題留給政府、網路服務提供者與著作權所有人共同研商解決方案。經過兩年多的討論與各方勢力的遊說，目前美國國會中就網路服務提供者之著作權侵害責任有了新的發展：

1On-Line Copyright Liability Infringment Act

本草案前身即為 On-Line Copyright Liability Limintation Act，於一九九八年二月更名 On-Line Copyright Liability Infringment Act，但內容並無重大變動。主要目的乃保護 ISP 與 OSP，避免其因使用者之著作權侵害行為而負擔過重責任，該法案規定：(1) 網路服務提供者並不會只因傳輸或機器自動重製、暫存了使用者侵害他人著作權之資訊，便需負擔著作權直接侵害責任、輔助侵害責任或代理侵害責任，但前提是該網路服務提供者並未主動發動該傳輸、挑選編輯該筆資訊、機器自動重製暫存之時間並未超過執行該筆傳輸所需之時間。(2) 如果該網路服務者並未知悉或察覺該筆侵權資訊之存在、並未因該著作權侵害行為而直接獲有財產上利益，網路服務提供者便不須負擔輔助侵害責任或代理侵害責任。

2Digital Copyright Clairification and Technology Education Act

本法案強調單純提供連線、傳輸服務的 ISP（Access Provider），**不會有直接、代理或輔助任何形式的著作權侵害責任，並闡明對網路上傳輸之內容沒有編輯、修改權能的網路服務提供者不應負擔責任，除非** ISP **收到著作權侵害的通知且有合理機會限制該著作權侵害行為。**

第二目　德國

德國關於 ISP **對網路內容之法律責任，可由其電信使用法**（Gesetz ueber die Nutzung von elediensten）**之規定見其端倪，首先明定電信服務提供人就其本身所提供之資料內容，應依法律一般規定負其責任；而就他人提供之資料內容只在其明知或技術上可期待其足以阻止該資料內容上載之範圍內，負其責任；至於將第三人提供之資料內容轉介他人連結使用者，包括因使用人之要求而自動及暫時持有該資料等情況，均不須負責任**[137]。

第三款　小結

雖然對網路服務提供者就網路上出現侵害他人著作權內容時應負責任為何眾說紛紜，但歸納美國與德國最近的立法例，可發現以下之趨

---

[137] **參閱廖緯民著，聯邦資訊與電信服務架構性條件件構規制法，資訊法務透析，民國** 86 **年** 11 **月。**

勢：單純提供連線的 ISP 不須負責；其他情況則綜合了代理侵害責任與輔助侵害責任之概念：除非該著作權侵害內容是 ISP 自己提供或曾參與修改、編輯、幫助、明知、獲致財產上利益等等，否則 ISP 不必負責。

由於美國多數大型的網路服務提供者，均同時提供連線服務與線上服務，性質上即非單純的通路提供者（Access Provider），故較少業者會堅稱其應比照單純連線業者般同享免責權；因此 On-Line Copyright Liability Infringment Act 綜合了代理及輔助侵害責任標準，明確限定網路服務提供者只在條文列舉之情況方負責任之規定，應能切合美國業者之需求。

至於台灣，由於許多的業者早期經營時純粹只提供消費者連線服務，其業務類型傾向單純提供通路服務，故多數認為其應有電信法第八條之適用而得主張電信事業對電信內容的免責規定；因此，類似 Digital Copyright Clairification and Technology Education Act 開宗明義闡述單純提供連線傳輸之 ISP 免責之規定較為合宜。而資策會科技法律中心就我國著作權法修正條文，建議新增第八十七條之一「提供電子通訊網路服務或設備之人，對於第三人藉由其網路服務或設備而為之著作權侵害行為，不負著作權侵害責任。」即為釐清單純提供連線 ISP 之責任。

針對「單純提供連線服務的 ISP 不負著作權侵害責任」的規定，可能有人會誤認 ISP 將因此完全不受著作權法規範致使網路著作權侵害情形更形惡化，事實不然；蓋因 ISP 本身若兼營資訊內容提供服務且自己於網路上重製了該筆侵害他人著作權之資訊供使用者使用，ISP 本身即為著作權侵害之行為人，得適用著作權法第九十一條加以處罰，而於 ISP 明知第三人提供資訊侵害他人著作權卻又參與修改、編輯等情形則有著作權法第八十八條之共同侵權行為可資處理。至於單純提供連線之

ISP，若僅因其提供連線傳輸而被課與幫助犯責任實不合理，應有前述免責規定之適用。

較具爭議性之問題在於 ISP 受告知期網路上有疑似侵害他人著作權之資訊時，有無權利將該筆資訊移除？明知而未刪除該資訊是否成立幫助犯？此乃現行法中易生衝突，令 ISP 難以抉擇之關鍵問題，本文將在本章第四節中加以討論。

第三項　賭博網站

從六合彩、撲克牌到職籃、職棒的下注，從台灣到全球，種類繁多，媲美拉斯維加斯的賭博網站日益興盛，這些以賭博為內容的網站乃將賭場虛擬化，讓網友直接在電腦中鍵入下注金額，透過網路呈現賭博遊戲與結果，以 Casinos of the South Pacific 為例，上網者可以下注玩撲克牌或水果盤；有些網站要求先存放五百元美金在「客戶基金」帳戶內以便客戶賭輸時直接扣款，有些網站接受信用卡付款，贏錢則以匯帳方式取款。

網路賭博內容得否於網路上自由傳輸，各國看法亦頗分歧，在台灣有觸犯刑法賭博罪之嫌，但在允許賭博的國家則有其生存空間，於是出現了虛擬賭場跨國設站的情形，並以此在廣告中極力標榜網址所在地賭博合法，所以全世界的網路賭客在此虛擬網站賭博絕不違法，還因此引發了跨州、跨國網路賭博的管轄權爭議。當網際網路連線服務提供者

碰上賭博網站，在現行法規範下會不會成為賭博罪的幫助犯或構成圖利提供賭場罪？網路傳輸的賭場是國內賭場或國際賭場對其法律責任有無差別？以下就 Access Provider 或兼為 Content Provider 分別討論之。

第一款　兼營網路賭場的 ISP

第一目　刑法第二百六十八條之分析

若網際網路連線服務提供者本身同時設站提供網路賭博的服務以利使用者簽賭六合彩或職棒等，是否會構成我國刑法第二百六十八條「意圖營利供給賭博場所或聚眾賭博者，處三年以下有期徒刑，得並科三千元以下罰金。」之規定，關鍵應為「網路賭場」是否為該條所稱之「賭博場所」。

由於傳統破獲的賭博場所皆為賭客穿梭其中，使用實際賭具進行賭博的實際地點，而網路這個虛擬空間並無實際所在，其是否包含於刑法「賭博場所」之概念尚存討論空間；本文認為刑法第二百六十八條所欲規範者乃提供設備、規劃處所使大眾得因此進行賭博並藉以牟利之行為，而設置賭博網站之 ISP，藉由網路設備提供大眾於該網站中進行賭博以獲利，除設備與賭博場所「科技化」、「虛擬化」改成透過網路、網站進行外，其提供設備、園地以利大眾共同進行賭博之行為與傳統之實

際賭場並無二致，但刑法第二百六十八條所稱之「場所」係指占有實際空間體積之實體，且可透過人 知覺直接感受其存在之空間。因此，若採認為網際網路可為刑法第二百六十八條所稱之「場所」似與刑法之罪刑法定主義之要求有所扞格，已超過文義解釋上之範圍。

倘若將來政府改採設立離島賭博專區等管理政策，將一般賭博場所合法化，那麼，或可考慮以核發執照的方式妥善管理賭博網站、賭客年齡等，屆時台灣的 ISP 方可設立合法的賭博網站、提供合法的賭博服務；但在目前政府尚未有任何政策轉變的情況下，實不宜獨厚網路賭博，應修正刑法賭博罪之規定，就網路賭博加以規範；因此，若 ISP 現在兼營賭博網站無法以刑法第二百六十八條圖利提供賭場罪加以規範。

第二目　跨國規避責任之分析

有些賭博網站因其實際所在地禁止賭博，為規避法律責任而申請外國網址、租用外國 ISP 的虛擬主機、透過國外銀行交易賭博資金、轉播國外賭博內容等等，企圖藉由迂迴國外之手段來規避國內管轄權，事實上，這些「跨國」手段並不會影響賭博網站之法律責任。

以台灣而言，依刑法第四條之規定，犯罪行為地在國內者，我國仍然有管轄權；所以，縱使賭博網站網址於美國申請、資金轉換於中南美洲銀行、以國外賽馬或運動為賭博內容，提供賭博服務之網站與賭客（網路使用者）下注賭博實際操作電腦之地仍在台灣，所以我國仍有管轄權。實例上如前一陣子國內警方破獲名為「龍虎榜」網路賭場，該賭場透過網路轉播位在菲律賓的有線電視賭博頻道，利用網路科技在虛擬的空間

裡聚集了上億的賭資，雖然以菲律賓賭博頻道為內容，實際進行賭博地仍在我國，仍為我國刑法所禁止。而美國聯邦政府於一九九八年三月控告十幾個美國足球、曲棍球、職籃等賭博網站，這些網站雖然於中南美洲銀行進行資金交易或設站，然實際操作地點仍在美國境內，聯邦政府認為該類跨國網站並不足規避聯邦禁止透過通訊賭博之規定。是以，國內提供網路賭博服務的 ISP，縱透過上述各類迂迴國外的手段，因實際操作進行之犯罪行為地仍在台灣，依然無法規避刑法第二百六十八條意圖營利供給賭博場所罪之適用。

第三目　單純提供連線服務之 ISP

一、是否成立幫助犯之分析：

上述 ISP 除提供連線服務外，因另提供賭博內容服務，而有刑法圖利供給賭博罪之適用；但在 ISP 僅單純提供連線服務的情況，若其客戶開設網路賭場或上網賭博，ISP 是否成立相關賭博罪之幫助犯不無疑問。

首先，ISP 之客戶利用其連線服務與虛擬主機之服務設立賭博網站，該客戶本身並不該當刑法第二百六十八條之意圖營利供給賭博場所罪，已如前述；其次一般客戶使用 ISP 之連線服務進出該網路賭場賭博，同前述推論，網路因屬虛擬空間，非刑法所稱之場所，一般客戶亦不該當刑法第二百六十六條之普通賭博罪。惟若刑法賭博罪修正後，將網路賭博納入規範後，則提供連線服務與虛擬主機服務之 ISP 是否成立相關賭博罪之幫助犯，應視其是否存在幫助之故意。設若 ISP 本即知道其客戶使用其連線或租用虛擬主機乃為架設賭博網站，ISP 即成立第二百六

十八條意圖營利供給賭博場所罪之幫助犯；否則，在 ISP 並不清楚其客戶有人設立賭博網站進行賭博而無幫助故意存在時，單純以相關賭博罪之主犯乃使用 ISP 之連線或虛擬主機服務即課與 ISP 幫助犯之法律責任，不但有違幫助犯之成立要件，且不恰當。有認為單純為 access provider 的 ISP 可主張適用電信法第八條之規定而得免責[138]，本文以為基本上此等 ISP 並無幫助的故意，故並不成立刑法第三十條之幫助犯，因此無須主張電信法第八條之規定。至於提供連線服務之 ISP 最初不知客戶涉及賭博知情事，但於知悉後卻仍繼續為其提供連線或虛擬主機服務者，應認為有幫助故意而成立刑法第二百六十六條或第二百六十八條之幫助犯。

二、立法之必要性：

由於賭博站盛行，美國國會於一九九七年三月提出「網路賭博禁止法」草案（Internet Gambling Prohibition Act of 1997）[139]，與 ISP 責任相關部份，同時明確規定除了為新聞報導或在傳輸與收受州（國）均合法之情況外，任何人明知而利用通訊器材幫助賭博下注資訊之傳輸或接受者，將處以一年以下有期徒刑或科（併科）五千元以下罰金。美國之所以有制定新法之需求，乃因各州對於賭博是否違法之法律規定不一致，而在禁止賭博之州網路賭博同樣違法一事並無爭議；反觀我國，刑法既有賭博罪之明文規定，效力及於全國，單純提供連線服務之 ISP 是否成

[138] 參閱張雅雯著，網際網路連線服務提供者就網路違法內容之法律責任（中），資訊法務透析，民國 87 年 5 月，頁 24。

[139] 參閱張雅雯著，網際網路連線服務提供者就網路違法內容之法律責任（中），資訊法務透析，民國 87 年 5 月，頁 24。

立幫助犯，提供賭博服務之 ISP 是否成立圖利提供賭博場所罪，這些問題以原本的刑法機制即可解決，並無另立新法之必要。

第四項　猥褻內容

色情資訊與猥褻圖文因網路跨越國界，取得快速方便而隱密的特性，成為搜尋引擎中熱門的尋找對象，sex、adult 等字更在各國尋引擎關鍵字的排行榜中高居不下，如何處理網路色情資訊、保護未成年人免受有害資訊的影響，成為近幾年來國際間網路政策的熱門話題，提供網路色情資訊服務是否應受法律規範、是否以法律明文課與 ISP 義務以助問題解決等均是重點爭議，以下分別探討國內外對 ISP 提供或傳輸色情資訊之法律責任與相關義務。

第一款　提供色情資訊之 ISP 法律責任

ISP 在連線服務外另提供色情資訊內容供使用者擷取瀏覽時是否違反各國見解不同，除了涉及以兒童為主角的色情資訊全球咸認不妥外，一般色情圖文得否在網路傳遞國際間差異頗大：例如美國最高法院認為全面封殺網路色情是違憲的、侵害人民言論自由，但大陸、新加坡則全面管制網路色情資訊。而國內對網路色情內容目前以刑法第二百三十五條「散布或販賣猥褻之文字圖畫」處理，實際案例如張姓夫婦在八十七年一月間設立「說說成人網站」，利用該網站傳送男女交構等猥褻畫面，並以月費兩百元的價碼招收想觀賞圖片的會員；另有「禁忌樂園」網站

藉電子郵件將由國際色情網站下載的色情圖片傳送給會員等，均於八十六年依該條文判處徒刑。因此，若國內 ISP 提供色情資訊內容服務，在現行法下應有刑法第二百三十五條之適用。

第二款　單純提供連線 ISP 之責任與義務

單純提供網路連線服務的 ISP，當客戶使用其連線於網路散布或販賣猥褻資訊時，ISP 是否會因其扮演了提供連線傳輸資訊或提供虛擬主機服務供客戶放置該筆資訊而有刑法第二百三十五條幫助犯之適用，應視 ISP 是否知悉客戶散佈或販賣色情資訊之行為，有無幫助之故意而定。

在 ISP 知悉客戶使用其連線或租用虛擬主機以散佈或販賣色情資訊，或雖不知情但受告知後卻仍繼續提供該客戶連線或虛擬主機之服務者，應認為有幫助故意而成立刑法第二百三十五條之幫助犯；除此之外，應認為 ISP 對使用者散佈或販賣色情資訊之行為不知情，並無提供設備幫助犯罪之故意而無法律責任。

由於 ISP 的客戶成千上萬，大型的 ISP 如美國的 AOL 全球客戶高達一千萬、台灣的 Hinet 使用者四十萬、SEEDNET 用戶二十萬，ISP 很難知道每位客戶是否在其網頁中放置色情資訊，更何況由於網路之特性使然，每個提供網頁內容的使用者在每分每秒內都可能重新修改網頁內容加入猥褻資訊；因此，純就技術而言 ISP 或許能夠知悉其客戶的網頁內容為何，但實際執行面上，ISP 不太可能監看知悉用戶的網頁內容為何，以美國聯邦通訊委員會（FCC —Federal Communications Commission）為例，他們預估這樣的監督看網頁有害資訊制度將耗費 800 名人力。所

以，不宜僅因 ISP 提供連線或租用虛擬主機服務，便驟然推論 ISP 因技術尚可知使用者於網路放置猥褻資訊且又提供連線幫助而認定其為幫助犯，應考慮 ISP 實際上不可能得知所有客戶之網頁內容或傳輸內容，並無幫助故意而不會成立幫助犯。

由於網路跨越國界的特性，縱以刑法之處罰禁止國內人民散佈或販賣色情資訊，仍無法杜絕民眾由國際網路快速、方便地獲取各式各樣的猥褻資訊，為避免網路色情資訊氾濫影響兒童身心，國際間不約而同對應而來的機制差異頗大。首先，新加坡 ISP 必須配合政府提供的黑名單網站（black list）不得提供使用者連線到這些網站，否則 ISP 違法將被廣播局吊銷執照，而大陸則規定國際聯網遨遊祇能透過官方的 ISP（郵電局）之服務，祇能進入政府認可的網站（white list）。至於美國傾向將瀏覽何種網站的選擇權交給使用者，透過分級與過濾技術處理該議題，國會中”Family – Friendly Internet Access Act of 1997”草案則進一步要求 ISP 免費提供過濾軟體[140]。

上述新加坡、大陸透過 ISP 限制民眾瀏覽國際色情資訊之管道，由政府公然介入管制恐有侵害人民言論自由、大開民主倒車之虞，類似之做法在台灣並不可行。因此，透過分級、過濾等技術甫以業者自律是目前可資參考之政策，至於透過法律強制要求 ISP 提供免費軟體等暫不適宜，因為網路不論在技術面或環境面均尚在發展，不恰當馬上透過法律鎖定技術或課與 ISP 責任，短期內透過業者自律、市場機制來實施網路分級或過濾制度，政府從旁獎勵過濾軟體發明、加強社會與家庭教育宣

[140] 參閱張雅雯著，網際網路連線服務提供者就網路違法內容之法律責任（中），資訊法務透析，民國 87 年 5 月，頁 26。

導，讓網路環境在使用者與業者互動下，自行發展出適合社會價值體系之機制，而法律面目前宜保持彈性，等環境面、技術面都穩定了，屆時再進一步評析考量有無配合整體機制之必要[141]。

第五項　侮辱、誹謗他人之內容

由於網路匿名特性的掩護，利用網路公然侮辱或誹謗他人之情事時有所聞，例如八十七年三月初，一則指稱某 A 公司衛生棉內藏重卵致吃掉使用者子宮的不實消息，便於短短兩個禮拜內在網路上廣為流傳[142]；同樣

---

[141] 參閱張雅雯著，網際網路連線服務提供者就網路違法內容之法律責任（中），資訊法務透析，民國 87 年 5 月，頁 26-27。

[142] 八十七年三月在網路上流傳轉寄之電子郵件，其內容指稱「某保險公司的一位未婚女性客戶因身體不適而就醫，結果醫生赫然發現女病人的子宮被蟲吃掉一半，……發現女病人使用之 XX 牌衛生棉居然隱藏蟲卵，醫生不敢貿然下結論，於是跑到便利商店買了五包同牌衛生棉再檢查，結果五包中竟有二包有蟲卵。那位女性受害者向該公司抗議欲提出告訴，未然該公司卻想以一千萬元息事寧人。」之後該則誹謗消息的標題從「女性消費者須知」到「恐怖的訊息」，從模糊的產品影射到明確指摘　A 公司的 B 衛生棉有問題，從 BBS 站美容版蔓延到各討論區，再透過電子郵件的轉寄傳播至每位女性網友幾乎人手一封，再加上好事網友加油添醋，「子宮切除手術」、「千萬遮羞費」、「請大家轉告老婆姊妹」、「改用別的牌子，一同抵制不肖廠商」等說法紛紛出爐，終致引起軒然大波，嬌生公司出面發表聲明，刑事警察局資訊事著手調查，整個事件到四月初新聞報導警方查出原發信者，A 公司打算提起告訴而暫告一段落。

地由於網路的匿名性使然，被侮辱誹謗者無從確認發言人身分，因而向網際網路服務提供者申訴求償。就趨勢而論，近兩年來美國發生的數個網路誹謗案，網路業者均被列為共同被告，例如一九九八年一月美國財富（Fortune）雜誌於報導中指稱洛杉磯第一銀行 Thomas Kemph 收受賄賂，Kemph 便將 AOL、Prodigy、Earthlink 等網路服務提供者並列為被告；然而，究竟網際網路服務提供者對網路誹謗是否須負法律責任見解頗為紛歧，以下就英美判例與立法趨勢分析之。

第一款　美國相關案例與 47 U.S.C.§230

第一目　適用侵權行為法的影響與衝突

美國法院分析網際網路服務提供者是否須對網路誹謗負責，首先思考其定位為何，是類似於傳統侵權行為法中誹謗言論所刊載之出版者（publisher），抑或是流通該刊物的散布者（distributor）；若類似刊物出版者，因其對刊物內容有增刪編輯、發行與否之控制權，故亦須就刊物內容之誹謗言論負責；反之，若其地位類似書店或書報攤等流通刊物的散布者，除非其就該誹謗言論之存在有實際認知，否則無須就該誹謗言論負責，而區別的關鍵點便在究竟該網際網路服務提供者對於網路內容有無編輯控制權。

例如在 Stratton Oakmont, Inc. v. Prodigy Servs. Co.,一案，法官認為 Prodigy（網際網路服務提供者）對其 BBS 站上的言論，以過濾軟體濾掉其認為猥褻或冒犯性的訊息，對其網上內容實行了編輯控制權，故其地位類似於傳統的出版者而非散布者，因而課與 Prodigy 等同原始出版

者的無過失責任，判決其須就網路誹謗言論負法律責任。

Oakmont 判決以編輯控制權之有無，清楚地辯明了網路業者在傳統侵權行為法上的地位，但卻引發了抑制業者自律的反效果；原本網路服務業者對於網路論壇上如三字經等明顯的冒犯性言論會自動加以刪除，但在 Oakmont 的標準下，業者「過濾刪除的動作」將被認定為「有編輯控制權」再進一步與「必須就誹謗言論負責」劃上等號，影響所及，大大降低了業者這類初步的、自律性過濾意願，正如一位休士頓的網路服務提供者 Ed Cavazos 就該案對 ISP 的影響表示：「當你知道自律會導致必須負法律責任的結果時，就沒有人願意甘冒風險進行自律。」[143]

第二目　47 U.S.C.§230 的免責規定

美國國會於一九九六年電信法（Telecommunication Act of 1996）中有關 ISP 免責規定紓解了 Oakmont 判決造成網路服務提供者不願自律的負面影響。47 U.S.C.§230 首先澄清網路服務提供者的定位，規定「任何互動式電腦服務的提供者或使用者不應被視為其他內容提供者所提供資訊之出版者或發表者」，將之排除於上述侵權行為法出版者之範圍外；同時規定「任何互動式電腦服務的提供者或使用者，若基於善意而自動過濾或提供他人科技方法以限制其認為猥褻、淫亂、齷齪、極度暴力、性騷擾或其他令人不悅的言論（不論這些言論是否受憲法保障），並不會因

[143] 參閱張雅雯著，網際網路連線服務提供者就網路違法內容之法律責任（下），資訊法務透析，民國 87 年 6 月，頁 18。

此而須負擔法律責任。」47 U.S.C.§230 之立法，排除了各州侵權行為法之適用，使得網路服務提供者不會因曾有任何過濾或編輯等行為，而導致須就使用者之網路誹謗言論負擔法律責任。

第三目　Zeran v. American Online Inc

Zeran v. American Online Inc 案法官爰引 47 U.S.C.§230 確認了網路服務提供者就第三人於網路所提供之誹謗言論免責。該案的事實發生於一九九五年四月二十五日，有人在 AOL 的 BBS 站上張貼廣告販賣 T 恤，廣告詞並寫明這些 T 恤上所印的標語，亦即一些有關四月十六日奧克拉荷馬市聯邦大樓爆炸案之粗俗下流標語，最後署名 Ken（即原告 Kenneth Zeran）並留下原告在西雅圖住家的電話作為購買 T 恤的聯絡方式；由於是死傷慘眾舉國矚目的爆炸案，以此為標題的粗鄙標語引發群眾憤怒，隨後 Zeran 平均兩分鐘便接到辱罵他的電話，甚至有奧克拉荷馬市的居民打電話威脅要殺死他；然而，這則販賣 T 恤的廣告並不是 Zeran 貼的，而是來自一位無法確認身分的人。Zeran 於一九九六年四月二十三日對 AOL 提起訴訟，主張 AOL 應負侵權行為法第三人誹謗之責任，AOL 以 47 U.S.C.§230 主張免責。一審判決 AOL 勝訴，Zeran 不服提起上訴，第四巡迴法院判定 AOL 得依據 47 U.S.C.§230 主張免責，Zeran 不得依據州法主張 AOL 有編輯權故須負責。

本案另一個爭點在於：Zeran 認為 47 U.S.C.§230 僅明文規定網路服務提供者非出版者（publisher），故其排除的只是出版者的無過失責任，網路服務提供者仍有散佈者（distributor）責任的適用，換言之，在其知

道或有理由知道時亦應負責；Zeran 認為其已通知 AOL 該誹謗不實資訊之存在，然其後仍繼續有冒名販賣低俗標語 T 恤、鑰匙圈等系列產品的廣告出現在 AOL 的 BBS 站上，故主張 AOL 既受有通知、知道誹謗行為存在，便應負起侵權行為法誹謗言論所載刊物散佈者之責任。法官以 47 U.S.C.§230 立法理由駁斥之，認為國會之所以立該法乃為保障言論自由、確保網路這個提供多元意見發表機會的論壇，由於網路服務業者的用戶多則上百萬，若非賦予業者完全的免責權，業者為避免面對潛藏的訴訟糾紛，可能會嚴格限制用戶於網路發表言論的數目與言論類型而造成寒蟬效應；而且「收到通知的網路業者便須就其後言論負責」（notice-based liability）的理論將使所謂的「受害者」以逸待勞（發個通知等著提起訴訟求償），而網路業者卻疲於檢查監視訊息，如此同樣會造成業者為避免麻煩乾脆嚴格限制上網訊息的效應；肯認國會確保網路多元意見的論壇管道、確保言論自由之立法意旨，法官認為 47 U.S.C.§230 提供網路業者完全的免責保護，不須負擔出版者責任，亦無散布者責任，更不會因為受有通知而應負法律責任[144]。

第二款　英國一九九六年誹謗法案（The Defamation Act of 1996）

網際網路服務提供者對網路誹謗得否主張免責，依據英國一九九六年誹謗法第一條的規定須審核兩個要件：首先是非著作人、編輯人或發行人；其次則是以採取合理之注意且不知或無理由要求其知悉其行為有

[144] 參閱張雅雯著，網際網路連線服務提供者就網路違法內容之法律責任（下），資訊法務透析，民國 87 年 6 月，頁 19-20。

助於誹謗言論之發布。

由於該法對編輯之定義為對內容有編輯或相同責任或可決定發布與否之人，因此網際網路服務提供者若對網路內容有編輯權者，即為該條所稱編輯而無法就使用者於網路發布之誹謗言論主張免責，就這點英國誹謗罪之立法立場與上述美國 47 U.S.C.§230 及 Zeran 案不同，較類似上述美國 Stratton Oakmont 判決之觀點；至於其他未提供網路內容服務且對網路內容沒有編輯控制權的 ISP，例如單純提供連線的 ISP，即屬英國誹謗法第一條第三項所規定之「操作、提供任何設備系統或服務，使該誹謗言論得以電子形態被讀取、重製、散布或提供者」以及「藉由該傳播系統得以向公眾提供或傳輸誹謗言論，而該系統之操作者或提供者對於傳輸者並無控制權」，而被明文排除於著作人、編輯或發行人之外，只要該 ISP 能進一步證明已採取合理之注意，而且不知或無理由要求其知悉所提供之網際網路服務有助於誹謗言論之發布便可主張免責[145]。

此外，英國誹謗法並規定網際網路服務提供者就網際網路言論應提供申訴管道、經確認為誹謗應為更正及道歉之處理，同時規定 ISP 於訴訟前將誹謗言論刪除者得以免責。

第三款　我國法律

論及我國 ISP 對網路誹謗言論之法律責任，較無疑問的是若 ISP 本

[145] 參閱張雅雯著，網際網路連線服務提供者就網路違法內容之法律責任（下），資訊法務透析，民國 87 年 6 月，頁 20。

身即為發表該誹謗言論的人即構成誹謗罪；基本上，透過電子郵件或網路 BBS 站、新聞討論區誹謗他人與透過傳統途徑誹謗，其違法性並無二致，例如政大外交系學生於八十六年透過 BBS 站校園版指控教授利用學生一案業經台北地院判決誹謗罪[146]。

引起法律爭議的部分在於 ISP 要不要就使用者的誹謗言論負責任？依照電信法第八條第一項「電信之內容及其發生之效果或影響，均由使用電信人負其責任。」令 ISP，抑或是根據民法第一百八十五條，當 ISP 用戶利用 ISP 提供之網路服務於網路誹謗他人，而 ISP 有有故意或過失（例如 ISP 知情或受有通知未處理之情形）致使被誹謗者因遭受財產上或非財產上損害，而要求 ISP 負擔共同侵權行為責任。

上述兩種主張均於法有據，如何取捨方能求得具體個案之公平正義又能符合言論自由與網路健全發展應為考量關鍵。首先，就單純提供連線服務的 ISP 而言，其為通路服務者的特性與一般電話業者並無二致，令其適用電信法第八條主張免責應較少爭議。然而對於提供其他線上服務的業者，尤其對 BBS 討論區等實行其編輯權能的業者，若欲依電信法主張完全免責則對受害人不公恐難令人信服，但前述 Zeran 案法官認為賦予 ISP 散布者責任或 noticebased 責任會引發寒蟬效應的政策考量亦不無道理，如何在兩者間選擇最適合我國的解決方案，不論答案是前者或

[146] 八十六年十一月政大邱姓學生於網路發表「趙姓教授假借分數評鑑的權柄，驅使整班學生為趙教授個人的學術事業勞動 …」，雖其未曾聽聞學長提及趙性教授要求學生上課作摘要、報告並繳交磁片以利用學生，但台北地方法院承審法官認為，邱姓學生未加查證是否屬實即於網路上傳述足以誹謗教授名譽之事，該當刑法誹謗罪而處以拘役五十五日，得易科罰金。參見聯合報 87 年 3 月 24 日第 7 版。

後者均應透過立法及早確立網路業者的風險分擔與成本分析。

第六項　軍火販售、教做炸彈、販售違禁藥品與其他違法內容

對於網路上炸彈、槍械、麻醉藥品等違禁物的製作介紹與販售內容，姑不論各個判決有否檢視提供內容者有無煽惑他人犯罪之意圖與其判決之正確性，實務上面對這類個案均以煽惑他人犯罪處理；例如八十六年九月間引起爭議的「軍火教父」，該網站將國外的軍售網站翻譯成中文，在加註台灣買主的購買方式於網路上販賣槍枝，檢警以煽惑他人犯罪加以偵辦[147]；同年九月下旬出現的「無政府份子文件集」，則是在網路上介紹並連結治國外交人製造炸彈之網站[148]，由於教做炸彈之步驟鉅細靡遺，致生法界認定是否構成煽惑他人犯罪之疑義，法院亦以煽惑他人犯罪處有期徒刑十個月[149]。其他違法內容如網路恐嚇，像寄自國內大學恐嚇要暗殺美國柯林頓總統的電子郵件、要脅欲炸燬高雄中信飯店索價九百萬元的電子恐嚇信等，以及網路偽、變造文書等等，這類型的犯罪，除非 ISP 本身是行為人，否則截至目前為止尚未有 ISP 因此而成為共犯或幫助犯之案例；ISP 在面對這類型違法內容所遭遇之困擾並非法律責任，而是面對檢警調單位要求協助偵查時進退兩難之處境，關於這點將於下一段發現違法內容時 ISP 之權利與義務中討論。

---

[147] 參閱自由時報，86 年 9 月 13 日，11 版。

[148] 參閱中國時報，86 年 9 月 23 日，6 版。

[149] 台灣台北地方法院刑事判決八十七年度易字第四二九號。

第四節　發現違法內容時 ISP 之權利與義務

當 ISP 客戶在網路上傳輸或張貼違法內容，ISP 能否停止該用戶之網路服務、刪除資料或透露該用戶的姓名住址電話？ISP 主動為之與經受侵害第三人要求或檢警調單位要求而為之有無差異？以下由電信法之授權、契約權義與電腦處理個人資料保護法來討論 ISP 知悉違法內容後之權利義務。

第一項　停止用戶網路服務與刪除資訊

ISP 知悉用戶違法時得否主動或經第三人要求而停止用戶之網路服務，根據電信法第二十二條 ISP 對販售違禁品、賭博、詐欺等違法內容，有權利主張其妨礙治安而停止並拒絕對該用戶繼續提供網路連線、e-mail 等服務[150]；另外，對提供色情資訊營利的用戶，ISP 得援引電信法第八條停止提供虛擬主機租用、連線等網路服務給以妨害公共秩序及善良風俗內容為營業的用戶[151]。

然而，有些被第三人指稱為誹謗或侵害著作權之內容，究竟是事實

[150] 電信法第二十二條：「電信事業非依法律不得拒絕電信之接受與傳遞。但對電信之內容顯有危害國家安全或妨礙治安者，得拒絕或停止其傳遞。」

[151] 電信法第八條第二項：「以提供妨害公共秩序及善良風俗之電信內容為營業者，電信事業得停止其使用。」

還是誹謗、是合理使用或著作權侵害尚無定論，並非電信法第二十二條「顯有危害國家安全或妨害治安」之情形，且誹謗出現最多之狀況為個人透過 e-mail 或於論壇上發表之意見，無法適用電信法第八條以提供妨害公共秩序及善良風俗內容為營業之規範，這種情況下若 ISP 片面停止對用戶提供網路服務，可能有違反契約之虞。

此外，ISP 得否刪除用戶疑似違法之網路言論，例如 ISP 認為構成猥褻或煽惑他人犯罪之言論，或第三人申訴遭侮辱、誹謗與侵害著作權之內容，由於認定是否違法、是否侵害他人權利並非 ISP 的執掌範圍，電信法並未賦予業者刪除疑似違法內容之權限，ISP 貿然刪除恐會有侵害用戶言論自由與違反網路服務契約義務。

ISP 若欲避免同時面對第三人申訴求償與用戶控訴其債務不履行或箝制言論自由的兩難處境，目前可先透過網路服務契約與用戶約定；當第三人告知 ISP 用戶傳輸或張貼之網路內容侵害其權益時，ISP 有權將係爭內容先行移除，於一定期限內等候雙方提出證據或說明；若用戶持續傳輸或張貼系爭網路內容，ISP 得暫時停用該戶之網路服務。但就長期考量，政府若能權衡 ISP 與消費者權益擬定類似的立法規定，當能更有效的維持網路秩序。

至於 ISP 有無義務於知悉違法情形後立即停止用戶連線服務並移除該資訊，以著作權侵害為例，論者以為網路服務提供者若受有通知，始負有檢查管理之義務、應立即展開調查或暫時移除該資訊，否則成立幫助犯並應負共同侵權責任；但本文不贊同此種論點，首先，法律並未課與 ISP 檢查監督之義務、未強制其應停止連線服務或刪除資料，上述電信法第二十二條僅賦予 ISP「得」停止提供電信服務之權利，並未課與 ISP「應」停止服務之義務，至於移除資料與其他檢查監督之義務亦無任

何法律規範；其次，論者依民、刑法主張 ISP 未履行管理義務而應負擔共同侵權行為，成立幫助犯，本文認為 ISP 亦可依電信法第八條第一項電信內容由使用者自負責任來主張免責，這是法律再面臨新科技時所產生規範效果不明確的狀態，應進一步由政策考量什麼是最適合網路社會、最有利網路環境正面發展的法律規範，且由於網路資料量龐大，ISP 實質上不可能監督控管，加上如 Zeran 案認為以通知為基礎課與 ISP 法律責任恐會引發寒蟬效應之考量，本文認為不宜斷然課與 ISP 幫助犯與侵權行為連帶法律責任。

第二項　提供申訴人用戶個人資料與協助犯罪偵查

當自稱權利受害之第三人要求 ISP 透露用戶（侵權者）個人資料，包括姓名、住址、e-mail address 等等，ISP 並不能任意透露，因為 ISP 屬於電信業者是電腦處理個人資料保護法規範的對象，而為了保障個人的資訊隱私權，電腦處理個人資料保護法規定除非符合該法例外之情形，否則個人資料蒐集者基本上必須於蒐集之特定目的必要範圍內方可利用其蒐集來的個人資料。因此，ISP 原則上必須在其蒐集之特定必要範圍內（例如為處理與提供網路服務相關事宜）才能利用（透露）所蒐集的客戶個人資料；除此之外，ISP 只有在符合電腦處理個人資料保護法第二十三條的情況才可以將客戶個人資料透露給第三人；像是為了增進公共利益，免除當事人生命、身體、自由或財產之急迫危險、防止他人權益重大危害而有必要或是經過當事人書面同意後或符合防止「他人權益重大危害」條款方可給予申訴人客戶之個人資料；然而，客戶之網

路言論是否構成他人「重大」危害個人主觀認定不同，將來若生糾紛仍須依法院認定而定。

至於檢警調偵查人員要求 ISP 協助調查提供客戶個人資料、通訊紀錄甚或助其監看使用者上網活動時，ISP 依法應如何處理？首先，提供客戶個人資料之要求雖然是由檢警調人員配合辦案所提需求，仍有上述電腦處理個人資料保護法第二十三條之適用，故若為增進公共利益防止他人權益重大危害而有必要之情況下，ISP 即可提供偵查人員客戶之個人資料；其次，對於客戶通訊紀錄之提供，因電信法第七條課與電信事業對電信之有無及內容守密之義務，ISP 及其服務人員只有在司法、監察或治安機關依法定程序調查蒐證時才可提供客戶上網紀錄。最後，關於協助檢警調單位針對犯罪嫌疑人進行網路監聽之要求，目前可依民國八十八年七月十四日總統公布施行之「通訊保障及監察法」對於網路監聽提供合法依據與程序。

第五節　小結

以上就網路違法內容 ISP 的法律責任進行初步分析與討論，大致的趨勢是提供違法內容的 ISP 須就該違法內容負擔法律責任、單純提供連線服務的 ISP 可比照傳統電信通路服務者主張免責；較麻煩的部分是除了通路服務外上提供其他網路服務的 ISP，其責任為何、標準何在法律見解差異頗大，除了會依著作權侵害、誹謗等主題不同而有差別外，各國看法亦有相歧之處。而法律責任的不明確，使 ISP 在經營業務時面對潛在的法律糾紛經營較為困難，在美國更因此出現 ISP 必須購買保險以

分擔因網路侵權內容產生的賠償費與訴訟費等風險。然而，除了保險外，更應該由法律面、自律面與管理面建立妥善機制來為不明確法律責任所產生之問題解套。

目前國際就網際網路服務業者對網路違法內容之法律責任，立法趨勢傾向賦予業者除名之外免責之規定，例如德國多元媒體法第一條第五項第三款規定電信服務提供人就他人提供之資料內容，只在其明知或技術上可期待其足以阻止該資料內容上載之範圍內負其責任[152]。而美國的 47U.S.C§230 排除網路服務提供者因過濾或編輯行為導致須就使用者網路言論負責之可能性；國會 On-Line Copyright Liability Infringment Act 以及 Digital Copyright Clairification and Technology Education Act 則闡明除非 ISP 明知或受有通知而不刪除，否則不虛偽使用者侵害他人著作權的網路內容負責。

此外，ISP 仍面臨另一問題；經通知違法的網路內容可能最後結果並未違法，然 ISP 為符合法律免責之要求於接獲通知後將該內容在技術上可行、經濟上合理的範圍內即時刪除，法律若無對應的規定，ISP 依舊無法免除用戶違反契約之控訴，為解決這個問題，Digital Copyright Clairification and Technology Education Act 提供了數個平衡機制：（一）被通知有侵害著作權內容後 ISP 刪除或阻絕內容傳輸之處理只需維持十日或直到收到法院命令為止。（二）ISP 若因受有通知而為刪除或阻絕該內容傳輸等處理而被訴，不論該內容是否真的構成侵害，ISP 均不須負擔任何法律責任。（三）要求申訴人必須於通知中提供真實住址電話或

[152] 參閱張雅雯著，網際網路連線服務提供者就網路違法內容之法律責任（下），資訊法務透析，民國 87 年 6 月，頁 25。

e-mail address、指明侵害內容所在、提供擁有著作權或對方非法使用之合理證明等，並課與於通知中為虛偽陳述之申訴人一千美元以上之損害賠償。

我國政府目前既無明確立法賦予 ISP 監控網路內容的權限與責任，然一些法律中尚留存著 ISP 須與用戶負連帶法律責任的可能性，業者很難經營，實應及早明確立法；本文認為，目前網路事業還在萌芽成長的階段，加以網路國際化與資料量龐大的特性，政府不宜課與業者過重責任與義務，上述德國、美國 ISP 除明知外免責與 ISP 受通知後依法定程序處理即可主張免責等規定實值我國參考。

除了等待立法解決問題外，現階段網際網路服務提供者以契約規範自律管理亦對問題的解決有所幫助。透過契約來解決法律真空與衝突、由當事人雙方之合意明定彼此權利義務，例如於契約之用戶自律條款明定不得於網路上從事侵害他人權益之行為態樣、使用者違反而導致第三人損害時的責任歸屬與 ISP 之求償權，用戶違反自律條款時之處理模式與規章，例如 ISP 有權自網上刪除該筆資料並停止該用戶之連線服務等等，如此即可事先預防法律糾紛的產生，將可能涉訟的法律成本降到最低，不但有助於 ISP 在競爭激烈的市場中順利發展，並可讓用戶藉由契約規範了解自己的權利義務，進而事先避免違法行為之發生。

但是透過契約的自治機制雖為現階段問題解決提供了出路，然就長遠而言，充分討論形成共識以立法確立 ISP 法律責任才是根本之道；但法律的介入應是維持網路秩序的最後防線，因此在立法分派處理網路違法內容之責任義務時，應同時考量資訊自由與網路秩序之平衡，以及該標準對網路社會後續發展所造成之衝擊，才能真正解決問題而非衍生問題，也才有助於網路環境的正面發展。

第六章　網際網路連線服務提供者就網路違法內容之法律責任

第七章　結論與建議

第一節　結論

在繁忙的一天中，都有大量的資產或資料，透過電腦網路來傳輸、處理並儲存。在本世紀末，高度開發社會中的每個人，可能會擁有數以百計的網路電腦。這些電腦會互相溝通，減少資源浪費，並提高日常生活的方便性。但這個新的遠景，有它的黑暗面存在。從網路過去發展至今的經驗顯示，網路活動者在網路世界裡經營其網路生活時，往往將自己在現實生活裡所累積的法律經驗帶入其中。事實上，當我們在經營網路生活的同時，也同時生活在現實生活世界裡，所以當網路活動形成爭議時，我們往往還是得訴諸現實世界的法律制度，作為解決網路爭議的依據。網際網路相關法律問題眾多，而網路安全與秩序維護亦甚為重要，這又牽涉到網路犯罪(包括不法入侵、破壞篡改、金融犯罪、施放病毒)、色情、誹謗，甚至擴及前陣子網路上販賣武器等等不一而足的問題，相關法律規範亟需深思。所以這是立法機關必須立法管理和控制的新領域，因為未來或現在多半的犯罪行為，都會在這個領域發生。此外，偵辦人員應該了解新的犯罪手法，使用不同的偵辦方法，以及有哪些法律規定可以防制犯罪。對傳統的罪犯而言，網路是一項強大的犯罪工具，此類犯罪所之牽涉實際技術面日新月異，更是現行法律所必須面對的挑戰。

本文除結論與建議外，各章之主要內容可略述於下：

【第二章】中討論網路犯罪之定義，實際上並非先有一個明確的定義，然後再演繹出種種可能的犯罪類型，而是先有了因電腦網路的使用，因有心人士利用網路從事不法行為，而其使用行為侵害刑法所保護之法益，進而產生了各種不同的犯罪型態，然後才由這些具體犯罪類型中歸納出一個抽象的概念。雖然目到前為止，國內學者間尚未對網路犯罪予以明確之定義，亦未歸納出確切的犯罪類型，不過若欲解決網路犯罪之認定問題，似可參考定義經濟犯罪之模式，經由對網路犯罪基本模式的確立，以行政命令的方式確立網路犯罪的含義，以解決網路犯罪定義內涵之問題。

【第三章】中所討論之犯罪均為傳統之犯罪類型，網路僅為犯罪之工具或媒介，此類犯罪並非因網際網路之出現而產生，僅係舊有之犯罪類型透過網路實施犯罪而已，例如網路色情、網路賭博、網路恐嚇等均可用原有之刑法規定加以規範。惟因網際網路之特質造成此類犯罪之構成要件解釋上發生疑義，由於我國現行刑法對於網路是否該當賭博罪構成要件中所稱之場所，適用上發生疑義，亦無特別之規定，是否該當刑法上賭博罪之構成要件非無疑問，因此，美國之立法例值得作為我國規範網路賭博行為之參考。

【第四章】中討論對於未經允許而侵入他人電腦系統之行為看似與無故侵入他人住宅之行為相類似，但並不該當刑法上侵入住宅罪之構成要件，因此在罪刑法定主義之原則之下，而無法以現行之刑法加以處罰。駭客入侵電腦系統並竄改他人之電磁記錄之問題，此處所稱之「竄改」與刑法上所稱之「變造」相當，且依修正後之刑法第二百二十一條第二項已明文規定「電磁記錄」為刑法上之準文書，若是更改、刪除電腦中

之資料僅是變更原電磁記錄中內容之一部分，則可能構成變造文書罪或毀損文書罪。如果以網路侵入之方式造成行政機關之電腦當機，甚至使處理中之資料全部滅失，來干擾或妨害公務之進行並不該當刑法上妨害公務罪，應立法加以補救。若對於大眾運輸系統、交通管制系統之電腦控制程式加以變更影響其正常運作，此等行為構成刑法第一百八十四條之「妨害舟車及航空機行駛安全罪」，另外，由網路入侵捷運局行控中心之電腦系統竄改資料，進而導致電腦當機之行為，即係以他法使其他公眾往來設備喪失交通效用之行為，若有足生交通往來之危險者，即構成刑法第一百八十五條第一項之損壞或壅塞陸路罪。

【第五章】中討論進入他人之電腦系統內並對他人之資料擅自儲存取用時，雖有新修正之刑法第三百二十三條規定，但因電磁記錄事實上之特性，使得所謂竊取電磁記錄不能構成刑法上的竊盜罪。因此，不妨把竊取定義成「剝奪專屬支配關係」。一方面既可以將立法者所要規範的竊取電磁記錄的行為納入，另一方面也不致於擴張竊盜罪原來所要規範的範圍。在整個有關妨害祕密罪的立法體系上，關於個人資料的保護，其立法的技術標準應該是個人祕密應該加以保護的，就是應該加以保護，而和是否用電腦來處理沒有關係。但依我國目前的立法標準來看，保護的標準似乎是建立在電腦的關係上。對於大量電子郵件廣告造成的問題，檢視國內相關法律，可由刑法第三百五十二條第二項及電腦處理個人資料保護法來解決。由於網址名稱只是網際網路上的一個電子地址，並非表彰其商品或服務，故網址名稱並非可受商標法保護之「商標」。又駭客自己盜用他人信用資料進行交易獲得財物或財產上之不法利益

之行為，應該當刑法第三百三十九條第一項之詐欺取財。受電腦病毒干擾而使電腦檔案及程式等電磁記錄無法正常運作或甚至受損壞而無法使用時，是否已達「毀棄」、「損壞」或「致令不堪用」之程度，而該當刑法第三百五十二條第一項之毀損文書罪或僅係干擾他人電磁記錄之處理時，應依新增修之刑法第三百五十二條第二項之規定處罰。對於發動癱瘓服務攻擊之網路駭客，則屬該當刑法新修正之第三百五十二條第二項規定凡干擾他人電磁紀錄之處理，足以生損害於公眾或他人者之構成要件，而得加以處罰。

【第六章】就網路違法內容 ISP 的法律責任進行初步分析與討論，大致的趨勢是提供違法內容的 ISP 須就該違法內容負擔法律責任、單純提供連線服務的 ISP 可比照傳統電信通路服務者主張免責；較麻煩的部分是除了通路服務外上提供其他網路服務的 ISP，其責任為何、標準何在法律見解差異頗大，除了會依著作權侵害、誹謗等主題不同而有差別外，各國看法亦有相歧之處。目前國際就網際網路服務業者對網路違法內容之法律責任，立法趨勢傾向賦予業者除明知外免責之規定，我國目前既無明確立法賦予 ISP 監控網路內容的權限與責任，然一些法律中尚留存著 ISP 須與用戶負連帶法律責任的可能性，業者很難經營，實應及早明確立法

第二節　建議

任何犯罪固然無法全部防患於未然，惟事前如有妥善之預

防措施，則必能減低犯罪之發生率。同樣地，網路犯罪雖然可能有刑責，但事後追訴實不如事前預防，尤其網路犯罪大多發生於安全防護系統較弱，或欠缺稽核程序之電腦系統，故事前之預防，必能防制相當大部分之電腦犯罪。因此，一方面須修訂現行刑法，使其能夠有效地掌握網路犯罪；另一方面則必須強化刑事司法機關追訴與審判網路犯罪之能力，而能確實依據刑法與相關法律之規定，繩網路犯罪於法。本論文認為抗制網路犯罪之具體措施如下：

壹、網路安全之維護

一般而言，網路安全管理是全面性、整體性的，即便是設置了最嚴密的防火牆、設定了最嚴密的存取控制，也必須有電腦的使用者、操作者、或管理者予以配合。因此在網路安全維護方面，應特別強調滿足資訊安全的基本原則也就是：機密性（confidentiality）、完整性（integrity）、近便性（availability）。在上開基本原則之外，尚須補充其他安全控制，例如用身份識別及認證（authentication）、檔案的存取控制（access control）、稽核（auditing）及無可否認性（non-repudiation）等，將可提供網路更多更安全的保護。

一、 建立網路倫理規範

利用網路之服務及其他權利侵害型之犯罪，本質上與一般傳統犯罪

並無太大不同，僅其行為係利用網路或與網路相關而已，故此類之犯罪防制之道與一般犯罪理論相同，換言之，倫理及法治觀念之教育係最根本之課題。我們必須建立尊重他人的權利之觀念，使網際網路的使用者培養尊重他人權利（包括智慧財產權）之觀念。因此加強倫理及法治的觀念與教育，建立共同遵守的行為準則或「網路倫理規範」即為防制網路犯罪之第一步。網路世界有其特殊之規則或規範，在各種不同的網路社群裡，早已發展出為其成員所遵循，甚至為多數網路使用者所認同的「網路習慣法」（customary rules）與「網路禮儀」（netiquette）。因此，我們可以在這些舊有的基礎上，建立一套網際網路使用者應有之正確觀念及使用網際網路之規範。

二、加強電腦網路系統之安全措施

網際網路所涉及之安全問題，除因網路病毒導致之安全風險外，一般常見者，即為網路駭客入侵系統所造成之風險。為有效防止不明駭客之入侵，一般網路伺服器應設置安全裝置，例如利用認證（Authentication）或使用者帳戶（user's account）、防火牆（fire wall）、資料加密（data encryption）等措施來保護網路之安全。

（一）使用認證程序

認證就是提出某些特定的資訊，用以確認使用者的程序，亦稱使用者帳戶，通常係由一個使用者名稱和密碼組合而成，一個區域網路使

用者可利用此一帳戶開啟電腦並進入區域網路伺服器[153]。而在網路上，當用戶欲通過某一網路關卡或需向通訊之一方證明自己的身份時，必須出示可供對方認證的資訊，故藉由認證程序可以避免他人未經授權侵入電腦系統。例如當我們撥接連結網路時，需輸入識別碼（user-name）及密碼（password）以登入。因此，使用者帳戶一般為最基本的防護措施。除此之外，尚可採用其他的認證方法例如「生物認證法」、「電子信物法」等方法[154]，作為輔助之工具。

（二）防火牆之設置

所謂防火牆，可分為一般防火牆和病毒防火牆，前者又稱安全閘道器（secure gateway）係一種系統或綜合數種系統將二個或二個以上網路予以區隔之安全裝置，可以有效控制所有封包來源、應用管道及目標，目的在隔絕外來的非法入侵。因此，防火牆的使用可使連接網際網路之各區域網路大幅降低遭非法入侵的次數及頻率。後者則為保護電腦系統不受電腦病毒傳染之安全裝置，在網路上傳輸檔案時可以偵測檔案中是

---

[153] 區域網路（a Local Area Network；LAN），係指一群電腦彼此互相連線或是連線到中央電腦，且所有的電腦實體均離的不遠，例如，大部分公司內使用的網路。另所謂廣域網路（a Wide Area Network；WAN），係指一群電腦彼此互相連線或是連線到中央電腦，但至少有一部或多部電腦和其他一部或多部電腦實體距離很遠。而網際網路即為來自不同且為數眾多之區域網路及廣域網路之連結。

[154] 所謂「生物認證法」例如以指紋、聲紋或視網膜作為辨識之方法，「電子信物法」則是利用電子身份證明如磁片或 IC 卡作為身份確認之用。

否有電腦病毒程式，目的在排除電腦病毒程式的傳輸。目前網路世界中幾乎每個月都有許多新的病毒產生，隨著科技之進步，相信病毒會越來越厲害，企業應不斷地更新防毒程式，並建立病毒防火牆（Viruswall）以排除或減緩電腦病毒傳染之速度。

（三）利用加密、解密之技術

網際網路是開放式的，其流通的資訊很可能被任何人隨意攔截、讀取，為防範資料為他人所擷取，透過資料加密之後的傳輸則是有效的辦法[155]。其主要功能在於保護封包資訊在網路傳送過程中不被攔截。同時，經過加解密技術之運用，亦可達到網路封包資訊來源確認及資訊隱密之目的。

貳、建立網際網路連線服務提供者之管理制度

[155] 所謂資料加密，係指網路資訊封包在傳送過程中以各種加密演算方式將可閱讀資料轉變成一種非經解密鑰匙解密而無法閱讀之形式。加密演算之目的係將資料隱匿不供任何人觀看，以確保資料的隱密性。解密鑰匙則可將加密資料轉換回可閱讀之形式。通常，經由增加加密鑰匙位元數，即可增加解密鑰匙的長度，亦會因此而增加破解密碼之難度。

一、停止用戶網路服務

ISP 知悉用戶違法時依電信法第二十二條之規定，對於販售違禁品、賭博、詐欺、煽惑他人犯罪等違法內容，應主張其妨礙治安而停止並拒絕對該用戶繼續提供網路連線、e-mail 等服務[156]；另外，對於提供色情資訊營利的客戶，ISP 應依電信法第八條之規定，停止提供虛擬主機租用連線等網路服務給以妨害公共秩序及善良風俗內容為營業的客戶[157]。

二、提供用戶個人資料與協助犯罪偵查

檢警調偵查人員要求 ISP 協助調查提供客戶個人資料、通訊記錄甚或監看使用者上網活動時，依照電腦處理個人資料保護法第二十三條之規定[158]， ISP 即應提供檢調人員客戶之個人資料；其次，對於客戶通

---

[156] 電信法第二十二條規定：「電信事業非依法律不得拒絕電信之接受與傳遞。但對電信之內容顯有危害國家安全或妨礙治安者，得拒絕或停止其傳遞。」

[157] 電信法第八條第二項規定：「以提供妨害公共秩序及善良風俗之電信內容為營業者，電信事業得停止其使用。」

[158] 電腦處理個人資料保護法第二十三條：「非公務機關對個人資料之利用，應於蒐集之特定目的必要範圍內為之。但有左列情形之一者，得為特定目的外之利用：

一、為增進公共利益者。

二、為免除當事人之生命、身體、自由或財產上之急迫危險者。

訊紀錄之提供[159]，在司法、監察或治安機關依法定程序調查蒐證時，ISP即應提供客戶上網記錄。關於協助檢警調單位針對犯罪嫌疑人進行網路監聽之要求[160]，如符合通訊保障及監察法第五條之規定，即應協助網路監聽以偵查犯罪。

參、修正現行刑法中之相關條款

於網路犯罪所涉及之層面極為廣泛，並非僅單純的牽涉到實體刑法之部分，在民法、行政法、營業秘密法、智慧財產權相關法律以及刑事程序法等領域中也存在著許多亟待解決之課題。但針對業已發生之網路犯罪，必須使用刑法之制裁手段，科處行為人相當之刑罰，始能有效地嚇阻網路犯罪，達到一般預防之功能。在我國規範網際網路之法律制訂前，為因應網際網路時代來臨所產生之網路犯罪處罰問題，應針對網路犯罪行為之特性，修正現行刑法中之相關條文，其中以刑法第二

三、為防止他人權益之重大危害而有必要者。

四、當事人書面同意者。」

[159]電信法第七條：「電信事業或其服務人員對於電信之有無及其內容，應嚴守秘密；退職人員亦同。前項規定依法律程序查詢者不適用之。」

[160] 通訊保障及監察法第三條第一項第一款將通訊定義為：「利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信。」，由此定義觀之，網路亦為其所規範之通訊之一。

百六八條及第一百三十五條之修正較可迅速達到規範之目的，以規範網路犯罪行為，今試擬條文如下：

一、刑法第二百六十八條賭博罪

「意圖營利，供給賭博場所或聚眾賭博者，處三年以下有期徒刑，得併科三千元以下罰金。

利用電腦或其他相關設備提供他人賭博財物或聚眾賭博者亦同。」

說明：依刑法第二百六十六條之規定，普通賭博罪之構成要件中對於「場所」有其要件之限制，即須在公共場所或公眾得出入之場所賭博財物。因為傳統刑法上所稱之場所係指占有實際空間體積之實體，且可透過人 知覺直接感受其存在之空間。而網際網路之世界乃是電腦網路所虛擬出來之世界，雖然它具有互動性與即時性，但仍非現實生活中我們可以直接以人之知覺感覺其存在者，仍必須透過電腦之處理始能感覺其存在。「網站」是否可認為係傳統刑法觀念中之「場所」，若採肯定見解即與刑法之罪刑法定主義之要求有所扞格，已超過文義解釋上之範圍，因此對於網路賭博應另行規定，利用電腦或其他相關設備提供他人賭博財物或聚眾賭博之行為類型，始能解決問題。

二、刑法第一百三十五條妨害公務罪

「對於公務員依法執行職務時，施強暴脅迫者，處三年以下有期徒

刑、拘役或三百元以下罰金。

意圖使公務員執行一定之職務或妨害其依法執行一定之職務或使公務員辭職，而施強暴脅迫者，亦同。

利用電腦或其他相關設備妨害公務員依法執行一定之職務者，依第一項之規定處斷。

犯第一項及第二項之罪，因而致公務員於死者，處無期徒刑或七年以上有期徒刑。致重傷者，處三年以上十年以下有期徒刑。」

說明：以網路侵入之方式，竄改行政機關電腦系統內之資料，進而導致行政機關之電腦當機，無法正常運作，亦是對於公務員之執行職務加以妨害，惟此等行為並不該當刑法上妨害公務罪中有關強暴、脅迫之構成要件，如此便產生處罰上之漏洞。這種非強暴脅迫之行為方式，雖然表面上是和平的手段，但是在今日行政機關全面電腦化之情形下，其所造成之損害將遠甚於傳統妨害公務罪所規範之個別暴力行為，且產生的影響是全面性的，故應於刑法第一百三十五條第三項增定有關此類犯罪行為之處罰。

肆、強化網路犯罪偵查功能

為求有效地追訴與審判網路犯罪，刑事偵查人員必須具備足夠之電腦、網際網路專業知識以及電腦應用在某些作業上之專業知識，始能從事有效之犯罪偵查工作。目前網路犯罪偵查的瓶頸主要有下列四項：一是欠缺資訊技術人員之支援，導致

追查與蒐證的遲延而喪失先機。二是缺乏專業鑑定機構，三是ISP用戶管理以及網址登記制度不完善，此為造成追查中斷之瓶頸。最後一項犯罪偵查的障礙在於利用國外網路服務的犯罪行為，因此針對上述瓶頸本論文提出解決方法如下：

一、刑事偵查人員電腦專業知識之訓練

首先，應積極培訓檢調資訊人才，例如法務部新成立的網路犯罪防治中心，以及刑事警察局的資訊室等，相關編制下須培訓資訊犯罪偵查專才，對日後網路犯罪偵查大有幫助。而網際網路之使用屬於高科技之產物，且其具有隱匿性之特質，因此往往不法使用網際網路者，亦具有難以發現、追蹤及複雜之特性。當發生網路犯罪時，由於其特性使然，必須由有專業知識之犯罪偵查人員加以偵查防治，始能達到遏阻網路犯罪、懲罰網路犯罪者之目的。目前我國雖已朝此方向進行，在刑事警察局設置有電腦犯罪偵防小組，高等法院檢署也成立電腦犯罪防治中心，但電腦科技之法展迅速，仍須持續加強諮詢人才的訓練，方能效從事網路犯罪偵查工作。

二、網路犯罪專業鑑定委員會之設立

由於電腦科技與電腦系統之專業知識在網路犯罪追訴與審判中之重要性，故應於電腦同業公會中，成立網路犯罪之專業鑑定委員會，接受檢察署或法院之委託，從事網路犯罪有關

之專業鑑定，提出客觀而公正之鑑定之結果，以作為追訴與審判之參考依據。

三、健全用戶登錄、管理及網址登記制度

為避免發生檢警人員在偵查網路犯罪時，循線追蹤行為人使用的 ISP 或網址，最後查出來卻是假名字，徒然浪費辦案時間之情形。其解決之道在於建立健全的用戶登錄與管理制度以及健全的網址登記制度，這兩者可透過政府獎勵與輔導 ISP 業者經由自律建立共同的規範與制度，或透過交通部第二類電信服務業發照辦法中相關的管理機制來規範。

四、加強國際間合作

由於網路的一大特質是「跨越國界」，為解決行為人使用國外 ISP 的網路連線服務、利用國外網站或登記國外網址時，因缺乏國際合作，國外之網站不願配合執法人員之調查工作，所造成執法人員在調查上之困難。我們應尋求跨國合作管道，可以藉由與其他國家簽訂司法互助協定，共同合作打擊網路犯罪，達到對抗跨國性網路犯罪之目的。

參考資料

壹、參考書目

一、 David Icove,Karl Seger & William Vonstorcb 原著，陳永旺編譯，電腦犯罪，美商歐萊禮股份有限公司台灣分公司，民國 88 年 7 月再版。

二、 Thomas J.Smedinghoff 著，網路犯罪，張台先、陳玥菁編譯，儒林圖書股份有限公司，民國 86 年 2 月初版一刷。

三、 甘添貴著，刑法總論講義，國立中興大學圖書部，民國 77 年 9 月初版。

四、 沈文智著，INTERNET 網路安全手冊，碁峰資訊，民國 86 年。

五、 房阿生、吳振村著，電腦犯罪及防治方法之研究，司法週刊社印行，民國 78 年 9 月。

六、 林子儀著，言論自由與新聞自由，月旦出版社股份有限公司，86 年 6 月一版三刷。

七、 林山田著，犯罪問題與刑事司法，77 年。

八、 林山田著，刑法各罪論（下），自版，民國 88 年，增訂二版。

九、 林山田著，刑法各罪論（上），自版，民國 88 年，增訂二版。

十、 林山田著，刑法特論（下），三民書局股份有限公司，民國 79 年 9 月，再修訂三版。

十一、 林山田著，刑法特論（上），三民書局股份有限公司，民國 78 年 9 月，再修訂三版。

十二、 林山田著，刑法通論，自版，民國 83 年 8 月增訂四版再刷。

十三、 陳志龍著，人性尊嚴與刑法體系入門，作者自版，民國 81 初版。

十四、 陳志龍著，法益與刑事立法，作者自版，民國 81 二版。

十五、 陳家駿著，電腦智慧財產權法，蔚理初版社有限公司，民國 79 年 7 月初版。

十六、 陳煥生著，刑法分則實用，自版，民國 79 年 10 月修訂版。

十七、 黃榮堅著，刑罰的極限，月旦出版公司，民國 87 年 12 月，一版。

十八、 葉茂林著，資訊法律（二），書泉出版社，民國 86 年 6 月初版。

十九、 褚劍鴻著，刑法分則釋論下冊，臺灣商務印書館，民國 78 年五月五版。

二十、 褚劍鴻著，刑法分則釋論上冊，臺灣商務印書館，民國 78 年五月五版。

二十一、 蔡敦銘著，刑法各論，三民書局，民國 81 年 9 月修訂初版。

二十二、 羅明通、林志峰、李蒨蔚、洪榮彬、陳麗玲合著，電腦法（下），群彥圖書股份有限公司，民國 83 年 11 月初版。

貳、期刊論文

一、 C.R.Swanson and Leonard Territs 原著，徐昀譯，電腦犯罪之範圍、型態、原因及調查，刑事科學第十八期，民國 73 年 9 月。

二、 余依婷、鄭慧文、法治斌合著，從 ACLU V. Reno（II）看美國如何管制色情言論，資訊法務透析，88 年 10 月。

三、 李柏宏、廖有祿著，電腦犯罪之問題與對策，警學叢刊 26 卷 6 期，85 年 5 月。

四、 李智祥著，「網上冒名刷卡，駭客觸法多」，法律與你，民國 86 年 10 月。

五、 李雅萍整理，電腦犯罪之偵查與追訴，智慧財產權管理季刊第十四期，民國 86 年 7 月。

六、 林山田著，電腦犯罪之研究，政大法學論叢，30 期，73 年 12 月。

七、 林邦樑著，信用卡法律問題之研究，台灣台北地方法院士林分院檢察署八十三年度研究發展報告，民國 83 年 7 月。

八、 林慧蓉撰，論網際網路資訊安全與隱私之保護 ─以營業祕密之保護為中心，私立東海大學法律研究所碩士論文，民國 87 年 12 月。

九、 邱垂發撰，不正利用自動設備之研究，私立輔仁大學法律研究所碩士論文，民國 83 年 6 月。

十、 信用卡法律關係之研究，司法研究年報地十八輯第十七篇，民國 87 年 6 月。

十一、 洪榮彬著，個人資料保護概論（上），高雄律師會訊，民國 85 年 1 月創刊號。

十二、 洪榮彬撰，資訊時代之資訊處理與資料保護─以德國聯邦個人資料保護法為中心，私立輔仁大學法律研究所碩士論文，民國 82 年 6 月。

十三、 張雅文著，大量商業性電子郵件廣告之法律問題與管理機制，資訊法務透析，民國 88 年 9 月。

十四、 張雅雯著，網際網路連線服務提供者就網路違法內容之法律責任（下），資訊法務透析，民國 87 年 6 月。

十五、 張雅雯著，網際網路連線服務提供者就網路違法內容之法律責任（上），資訊法務透析，民國 87 年 3 月。

十六、 陳宏達著，個人資料保護之研究，私立輔仁大學法律研究所碩士論文，民國 81 年 7 月。

十七、 陳美伶著，考察美國電腦犯罪之防制研究（下），法學叢刊，第 127 期，民國 76 年 8 月。

十八、 陳美伶著，考察美國電腦犯罪之防制研究（上），法學叢刊，第

126 期，民國 76 年 4 月。

十九、 陳家駿著，談資訊網路與電腦犯罪（下），電工資訊，民國 86 年 8 月。

二十、 陳家駿著，談資訊網路與電腦犯罪（上），電工資訊，民國 86 年 7 月。

二十一、 陳煥生著，刑法上之電腦犯罪，刑事法雜誌，第四十二卷第三期，87 年 6 月。

二十二、 陳榮良著，電腦犯罪問題之探討，刑事科學第十二期，民國 70 年 9 月。

二十三、 馮震宇、劉志豪著，我國網路犯罪類型及案例探討，月旦法雜誌，第 41 期，民國 87 年 10 月。

二十四、 黃榮堅著，電腦犯罪的刑法問題，台大法學論叢，25 卷 4 期，民國 85 年 5 月。

二十五、 楊富強著，電腦犯罪之立法與電腦安全，法學叢刊，第 134 期，民國 78 年 4 月。

二十六、 電腦犯罪理論與實務問題研究，司法院研究年報第十八輯第十八篇，司法院印行，87 年 6 月。

二十七、 廖緯民著，論資訊時代的隱私權保護--以「資訊隱私權」為中心，資訊法務透析，民國 85 年 11 月。

二十八、 廖緯民著，聯邦資訊與電信服務架構性條件件構規制法，資訊法務透析，民國 86 年 11 月。

二十九、 蔡美智著，電腦駭客的罪與罰-談網路入侵的法律問題，資訊法務透析，民國 87 年 7 月。

三十、 蔡美智著，談網路犯罪，資訊法務透析，民國 88 年 1 月。

三十一、 蔡蕙芳撰，電腦犯罪與刑事立法的課題，國立台灣大學法律研究所碩士論文，民國 83 年 6 月。

三十二、 閔張雅雯著，網際網路連線服務提供者就網路違法內容之法律責任（中），資訊法務透析，民國 87 年 5 月。

三十三、 錢世傑著，網際網路色情資訊防範措施之相關問題探討，全國律師，民國 87 年 11 月。

三十四、 蘇宏文著，淺談電腦病毒與電腦犯罪，向電腦病毒說「不」，法律與你，84 年 2 月。

三十五、 蘇宏文著，網路犯罪罪難逃（下），法律與你，86 年 12 月。

參、WWW 網站

一、 http://suc.m.org.tw/neuaw/paper/crime.htm

二、 http://www.ec.org.tw/service/

三、 http://www.psd.iii.org.tw/inews/service.htm

四、 http://www.psd.iii.org.tw/inews/usrall.html.

五、 http://www.stlc.iii.org.tw/

六、 http://www.crime.org.tw

七、 http://www.pu.edu.tw/gec/news58.htm

八、 http://www.edu.tw/tanet/tanet-rules/crime.html

九、 http://stlc.iii.org.tw/seminar/870527

十、 http://stlc.iii.org.tw/seminar/870527/sld024.htm

十一、 http://notes.ncu.edu.tw/cld/

十二、 http://sparc.nhltc.edu.tw/~s889057/NetCrime.html

十三、 http://www.star100.com.tw/discuss/teclaw/69.htm

十四、 http://www.ba.ntust.edu.tw/eb/team2/messages/24.htm

十五、 http://www.hmes.kh.edu.tw/~jang/internet-learn1/nti.dj.net.tw/security/THREAT/SECU_CASES.html

十六、 http://www.chinatimes.com.tw/news/papers/online/national/n8921003.htm

十七、 http://www.csit.edu.tw/csitshow/InfoTech/tanetr2.htm

十八、 http://www.dgt.gov.tw/notes/890215-1.htm

十九、 http://tpc.moj.gov.tw/html/1/1_4_2d.htm

二十、 http://www.ic.tcg.gov.tw/htm/plan/plan-3/new/new8.htm

二十一、 http://news.yam.com.tw/computer/200002/11/10829000.html

二十二、 http://search.yam.org.tw/b5/yam/ccnet/virsec/hacker

二十三、 http://tech.is.net.tw/cybercash/9908/index4.html

二十四、 http://www.3wave.com.tw/document/O205/

二十五、 http://www.cc.nctu.edu.tw/~ltc/8705091.html

二十六、 http://www.chinatimes.com.tw/report/cn_tw_strait/webwar.htm

二十七、 http://www.smartnet.com.tw/news/economic/finance_other/finance_other20000211_12952.html

二十八、 http://ip-148-027.shu.edu.tw/news/990810/99081004.html

二十九、 http://www.tam.gov.tw/news/1999/99070501.htm

三十、 http://www.cdn.com.tw/daily/1998/12/01/text/871201d9.htm

三十一、 http://www.im.cpu.edu.tw/~illin/crime/4-2-1.htm

三十二、 http://bach.im.cpu.edu.tw/~illin/crime/4-2-1.htm

三十三、 http://nlg3.csie.ntu.edu.tw/systems/summary/sjhuang58linkfile.html

三十四、 http://stlc.iii.org.tw/stlc_c.htm

三十五、 http://isc01.moea.gov.tw/~ecobook/season/sag5_2/sag2-a6.htm

目　次

謝　誌

隨著這本論文的定稿，也代表我將告別東海大學八年的學習生活。同時，對我而言，也是我人生生涯上另一個重要的里程碑。從小就不愛唸書的我從沒想過自己有一天會唸研究所，直到自己僥倖通過研究所、司法官及律師的考試，一路走來雖不能說是順利，但實在是慶幸自己的幸運，雖然中間曾休學服兵役，但終於在司法官受訓階段完成本論文。

促成這本論文的完成，要感謝的人當然很多。不過，最應感謝之人莫過於恩師張麗卿老師，無論是從大學時期甚或於研究所的授課內容中，張老師深入淺出且旁徵博引的上課方式，不但給予我刑法概念上的啟蒙，更於討論問題時給予我多元的思考模式及空間。而論文撰寫期間，從論文題目的選定到內容架構的安排，張老師對於本論文的架構及論述用語上，皆逐一斧正，悉心指導，給予我相當重要的助益，此份恩情，令我難以忘懷。另外，論文口試時承蒙林東茂老師及柯耀程老師的撥冗指正，對本論文之內容及架構提供了重要而寶貴的意見，於此亦一併致上我的謝意。

除此之外，論文寫作期間，司訓所同學廖健男、蔡立文對於論文內

容意見的提供，本文於此亦一併致謝。

最後，從求學階段開始父母親所給予我一切精神上、物質上無止盡的支持，讓我無任何負擔地學習；女友惠玲八年來的陪伴照顧，替我分憂解愁，使我能通過研究所及國家考試，都是本論文完成的背後原動力。在此，獻上我內心最誠摯的感謝。

余德正　謹誌