電腦犯罪問題—美國刑事立法之參考

私立玄奘人文社會學院講師
蔡懷卿

摘　要

本篇文章之內容主要係在概述美國各州及聯邦政府，針對電腦犯罪問題之特質，例如電腦犯罪行爲客體－資訊之無體性，電腦犯罪之迅捷和隱密性對於金融秩序所帶來之巨大破壞潛能，對於公共安全所產生之重大威脅等考量，修正傳統普通法（特別是「竊盜相關犯罪」之規定）所作的一些立法努力。文中將關於州立法之討論範圍分爲：金融詐騙犯罪類、資訊竊盜犯罪類、連線使用犯罪類等三大類；其次討論聯邦相關立法。此外，有鑒於網際網路之蓬勃發展，文中簡介美國國會關於網路色情立法管制之嘗試，以及相關之違憲司法審查判例Reno v. ACLU, 117 S.Ct. 2329 (1997)，以供參考。文末對於我國最近電腦犯罪之相關刑法修訂，作一逐條檢視，並盡可能從前面所討論之美國刑事立法觀點來思考和檢討。

壹、前　言

電腦爲近半世紀才有之文明科技產物，而其逐漸在個人間普遍使用，所謂個人電腦（PC）亦不過是最近四分之一世紀的事情。社會進入資訊時代之後，犯罪之手法易隨之推陳出新，針對電腦資訊科技所引起之新事物現象或改變行爲模式，法律作爲社會控制之手段有加以調整因應之需要。美國於電腦科技之應用發展上，居於先進之地位，故它也是首先面對這些由電腦衍生之新犯罪現象，必須作出法律調整和適應的國家之一。本文嘗試就美國各州及聯邦政府關於電腦衍生犯罪之刑事立法政策，作一淺略之探討，並就我國最近關於電腦犯罪之刑法修正條文加以檢討，期收比較之功。

分析一電腦系統之架構，可以發現通常它有五個部門（或流程）易於遭受非法入侵：資料輸入(data input)、程式(programming)、中央資料處理(central data processing)、資料輸出(data output)、以及電子通訊(electronic communication)。上述每一個部門皆有可能遭受以下幾種形式之侵略：輸入不實之資料、篡改現有之資料、竊取系統上儲存之資料、或盜用系統之收費服務時間，猶有甚者，將整個系統摧毀破壞。由這些侵襲的部門和侵襲的手段之不同組合，關於電腦犯罪之討論，可以演成一煩瑣複雜之技術侵犯可能性清單。然則，如此分類容易模糊討論焦點，吾人毋寧將注意力集中於電腦被人非法使用侵害法益之方式，而非資訊技術本身。

電腦使用方式有四個特質，因此易受濫用：第一、愈來愈大量之高價值資訊被存放於電腦，電腦儲存使得迅速大量複製或銷毀資料成爲可能，因而增高犯罪風險。第二、透過電腦系統之交易，非經由人爲過程形成決策判斷，而是由機器依預設之程式自動作判斷並執行，容易遭不法之徒操控和影響結果。第三、電腦軟硬設備本身，以及投資於維護系統之人力物力構成一高價資產，容易成爲竊盜之犯罪客體；而其與傳統竊盜罪客體不同之一點在於，它可以盜用之方式被竊取有價之運算時間，而無須將有形硬體或其上儲存之資料移走。第四、大量之資訊透過電話線、衛星無線電波或其他通訊方式以高速度傳輸。因此容易於資料傳送之中途，遭受第三人以遙控方式攔截篡改，相對地增高風險。

針對前述犯罪風險，吾人已發展出許多技術設計對抗之，例如：於傳送時將資料轉換成密件之形式(encryption)，收到後須再經解碼之程序(decryption)才能閱讀，如此一來，在中途資料訊號若被攔截，也將只是一堆無法解讀的機器亂碼；或者，於進入系統時須先通過多層密碼(password)關卡才能進入系統等防範措施。然而，於多人使用同一系統時，洩漏密碼之或然率將增高，但這是無可避免的結果，就像任何再嚴密的（非電腦）傳統資料系統，也無法完全防止竊盜入侵一樣。

上述電腦系統對抗犯罪之脆弱性，更由於犯罪發覺和起訴舉證之不易，而加深了問題的困難和嚴重性。非如傳統犯罪會在現場留下指紋腳印，或其他蛛絲馬跡，電腦犯罪常以遠端遙控方式連上系統，靜悄悄地變更資料或操作指令，欲察覺犯罪和異常本就不易；發現犯罪後，也沒有任何目擊證人可提供證詞，只能依賴資訊專業上之證據和解說，來進行起訴和審判，而這些專業知識，對於檢察官和法官來說，有時並不一定是很熟悉或能迅速掌握的。

以下嘗依德州大學尼瑪教授（Raymond T. Nimmer）之分類〔註一〕，先將美國各州對於電腦犯罪之處理模式，分爲下列幾種電腦非法使用類型來進行討論：(一)金融詐騙犯罪類/電腦詐欺，(二)資訊竊盜犯罪類，(三)連線使用犯罪類〔註

二〕。隨後，並檢視美國聯邦政府關於電腦犯罪之相關法律規範。這些範圍之討論屬於較狹義之電腦犯罪，更廣義之電腦犯罪應包括所有需以電腦科技知識犯罪、起訴、審判，受刑罰法規規範之行爲，而可更進一步納入隱私權侵犯、智慧財產權侵犯等議題（這些法益在我國亦皆以刑罰法規保護）。但因這些不法行爲在美國多係屬民事範疇，故在此從略。

另外，由於近年來網路使用之蓬勃發展，網路色情與言論自由之爭議成爲另一項新的關注焦點。美國國會於1996年通過所謂通訊約束法(Communications Decency Act)，對於電信通訊內容之妥當性加以規範。其涵蓋範圍甚廣，影響所及，凡在網際網路上傳送猥褻(obscene)或不雅(indecent)之文字圖畫者，理論上皆可能觸及刑責。因此，美國民權自由聯盟(American Civil Liberties Union, ACLU)入稟美國聯邦最高法院，主張此部份法律違憲。美國聯邦最高法院於1997年6月作出Reno v. ACLU, 117 S.Ct. 2329 (1997) 之判決，將此一有爭議性之立法宣告違憲。本文亦就此一案之爭議以及判決作一簡單介紹，以供參考。

貳、美國各州關於電腦犯罪之立法概況

㈠ 金融詐騙犯罪類 (Financial Fraud) —侵害有體財產法益〔註三〕

傳統普通法所面對之問題

自從各公司行號和金融機構開始大量使用電腦作爲會計記帳工具之後，傳統上居於財務信任地位職員之監守自盜犯罪模式，就進入了一個新的電腦紀元。然而，電腦的引進，並未創造出新形式之犯罪。傳統的竊盜、詐欺、不實表示、僞造文書、以及其他詐僞犯罪類型依舊存在。電腦與傳統之簿記系統一樣，也都會受到篡改資料、使用僞造文件請領付款等之不法侵略。然而，電腦爲古老的犯罪製造了一種新的犯罪手法，而這些新的手法，大幅提高了竊取巨額金錢之可能性，以及長期隱瞞事實之犯罪能力。

涉及電腦之金融詐騙犯罪，一般均可依各州傳統的竊盜罪及相關之制定法起訴。目前美國各州均已將其固有之判例法原則加以制定法化(codified)。各州在普通法(common law)基礎上發展出之近代刑法，多半以單一「竊盜相關犯罪」(theft-related offenses)來規範這類傳統之竊盜犯罪類型。但仍有一些州於其刑法典內，保留普通法之傳統分類方式，區分竊盜(larceny)、背信(embezzlement)、詐欺(fraud)、僞造文書(forgery)等各種相關犯罪。此等制定法重視特定犯罪之行爲態

樣，並在適用上彼此互相排斥；如此一來遂使現代之電子交易犯罪，在適用傳統刑法概念時，發生分類上上之困難。

比如說，當吾人欲區分竊盜與背信，而系爭錢財款項係由電子記錄所表示時，就會發生分類問題。傳統上，此兩種犯罪形態的區別，係以受雇人被告於犯罪前是否合法占有(lawful possession)該款項爲準，如未擁有合法占有權即爲竊盜，反之則爲背信；而受雇人於受託保管財物時，如已經有據爲自己所有之非法意圖，其占有自始即爲非法，故亦爲竊盜；但如非法意圖係萌生於受託之後，則原始占有爲合法，後來據爲己有之行爲爲背信〔註四〕。電子世界內的合法占有權如何界定是一個問題；一般說來，它應當取決於財產移轉時誰擁有該款項的支付權。然而，在大多數的情形下，這個竊盜與背信的分類問題，已因現代制定法將這兩者與其他普通法財產犯罪形態合併爲單一之犯罪類型，而不復存在。

此外，如何區分詐欺與僞造文書也經常成爲一個問題。電子世界內的支票交易，可能係依照被告所提供之不實資訊，經由電腦簽發和列印支票（並且可能還經由線上傳送資料來支付〔註五〕）。理論上，電腦所列印的支票本身並非經「變造」之僞造文件，反而是被告提供不實資訊導致該支票被列印之詐騙行爲構成了詐欺罪。於電腦系統直接進行交易之場合，這項詐欺推論確有其存在之必要性。

背信性質如何界定更是一項爭議，此一爭議即使在已將各種普通法財產犯罪合併爲單一犯罪類型之各州也還存在。某些犯罪規定有「欺騙」(deception)之構成要件，因此被告可辯稱，只有「人」纔能被欺騙，「機器」無法被欺騙〔註六〕。這個問題係以「有效同意」(effective consent)的概念來解決，現代法律以此區分經同意之有效占有移轉，與因詐欺、脅迫而所爲之無效移轉。依照有效同意的概念，發票人僅同意基於合法之資訊來支付支票款項，不論被告直接從人或間接從機器取得款項並無區別。

針對電腦詐財之特別立法：電腦詐欺罪 (Computer Fraud)

有鑒於電腦犯罪之特質，許多州紛紛修改其制定法，加入特別針對電腦詐欺之條文。這些立法大體上均界定「電腦詐欺」爲：未得授權接近電腦，故意實施一詐騙計畫，以達財務金融上之目的。下列各州爲防堵電腦詐欺之立法例：

德拉瓦州（Delaware）〔註七〕

「任何人明知....無權接近....任何電腦，而以虛僞、詐欺、不實表示或承諾之手法....達到下列目的：(1)策劃或實行詐騙他人之計畫；或

(2)取得金錢、財產、或服務，

成立電腦詐欺罪。」

亞利桑那州（Arizona）〔註八〕

「任何人無權接近、竄改或損毀任何電腦、電腦系統或電腦網路，或其任何之一部份，意圖設立或執行任何計劃或詭計，用詐欺或不實之手法，詐騙、控制他人財產或服務，成立一級電腦詐欺罪。」

「任何人意圖無權接近、竄改或損毀任何電腦、電腦系統或電腦網路，或其中所存之任何電腦軟體、程式、或資料，成立二級電腦詐欺罪。」

維吉尼雅州（Virginia）〔註九〕

「任何人無權使用一電腦或電腦網路以遂行下列意圖：

1. 詐欺取得財產或服務；
2. 背信或竊盜；或
3. 侵占他人財產，

應構成電腦詐欺之犯罪。」

電腦詐欺或爲重罪(felony), 例如亞利桑那州、佛羅里達州〔註十〕，或依竊取財產價值決定刑罰度，例如：明尼蘇達州、康乃迪克州、維吉尼雅州、密西根州、猶他州、新墨西哥州〔註十一〕。

此等電腦詐欺立法具有兩項作用：首先，它爲一些電腦相關名詞界定其法律定義，俾免適用上之爭議與紛擾。其次，此類立法創設一有別於傳統竊盜罪之新型態之犯罪要件，檢方只須證明被告以特定故意(specific intent，類似於我刑法之意圖要件)接近(access)他人之電腦或電腦系統，無須證明行爲客體財產與其所有人分離之事實（此即英美法竊盜罪larceny之carrying away要件，或所謂asportation requirement）。因電腦犯罪常無文件紀錄可追蹤，在許多情形之下，「接近」也許是唯一能證明之事。這雖減輕起訴時之舉證負擔，但也使許多此類電腦詐欺案件，於錢財尚未到手就被捕時，其「故意」或「特定故意」之證明頗具爭議性。

多數州將此罪訂爲企圖犯(attempt crime)〔註十二〕型態，其刑事責任不待犯罪目的達成方纔成立；並且，無須等到將不實意思表示於他人方成立，只以有不法詐財之意思「接近」他人電腦之行爲爲必要。其所反映出之政策觀點是將電腦單獨視爲一受保護資產，此無形保護法益係獨立於電腦所有人因非法入侵所招致之實際財物損失。

此類關於電腦詐欺之立法，有一類型係規定有「無權」接近之要件者，有四個州：亞利桑那州、德拉瓦州、喬治亞州、北達科打州明文規定「欠缺授權(without authorization)」爲犯罪構成要件〔註十三〕。理論上，這有可能使受雇人（經授權接近使用公務電腦）之利用職務非法行爲被排除於外。依此一論點，此種電腦詐欺罪將重點置於遠端接近之罪犯，而監守自盜之受雇人則是以其他刑法條文

(例如embezzlement背信, conversion侵占)追訴之。相反的，另一類型未規定「無權」要件之州，受雇人之犯罪行爲可受電腦詐欺罪涵蓋，但如何區分無心之作業疏失與故意之詐欺將成問題〔註十四〕。

㈡ 資訊竊盜犯罪類 (Information Theft)—侵害無體財產法益

如前所述，電腦詐欺基本上是傳統犯罪以新犯罪手法包裝，舊酒裝新瓶，本質上它仍然是一竊盜相關犯罪。然而資訊時代之社會生活亦產生一些新的行爲態樣，無法以舊的犯罪概念規範之，所謂資訊竊盜即是一例。「資訊竊盜」指接近電腦俾複製或取得數據資料、公式、電腦程式等資訊內容之行爲，其所涉及者不僅止於無權使用電腦，更擴及至其他層面。由於資訊之價值逐漸增高，且經由電腦甚容易取得此種資訊，遂使吾人無法不對此問題不加重視。

傳統之竊盜相關犯罪，所保護者爲可感覺之有體財產(tangible property)，如錢財、動產等。但接近電腦之罪犯所取走的數據資料（和其隱密性所具之價值）乃係「無體物」(intangible)，是以欲證明資訊或理念非獨立創作發展而係得自盜取他人，也就格外困難。在有形財產之竊盜，被害人所被剝奪的是看得到之物。反之，在資訊竊盜，被告雖取得利益但並不奪走被害人所擁有之財產；除非被告將所有電腦上的資料破壞殆盡，被害人被剝奪的只是附於資訊之排他性(exclusivity)與祕密性(secrecy)〔註十五〕。也就是說，在侵害發生之前，資訊所有人對此一祕密資訊擁有絕對控制權，可以自己使用(use)獲利，或授權(license)他人使用以取得對價。侵害發生之後，原所有人雖仍擁有資訊之占有及使用權，但不復爲絕對排他，而是與犯罪被告共有(shared)，因此同一資訊之價值已大幅降低。由於原所有人仍占有該資訊，傳統竊盜罪之非法取走(asportation)要件，於資訊被竊取之情形即無法滿足，因爲單以閱讀、複製、或記憶資訊內容之方式，即可帶走其價值。

然而，一般之觀念仍認爲這種現代犯罪形態是一種竊盜，應該以竊盜罪處置。爲了克服這種矛盾，結果吾人必須擴張解釋「非法取走」之觀念，使其意義包括原物主免於被剝奪占有之情形。早期一些法院亦挖空心思，延伸解釋實定法上之竊盜罪構成要件，例如：加州法院解釋，將電腦資料之列印報竊盜罪表(printout)帶走，即該當於取走(carrying away) 他人之財產〔註十六〕。德州法院解釋，電腦程式該當於法條上之書面(writing)要件〔註十七〕。

另一困難處在於傳統竊盜罪之「故意」要件(intent to steal)：僅只複製他人之程式或數據資料，似乎不足以達到永久剝奪別人財產之故意(intent to deprive permanently other's property〔註十八〕)，因爲原有物主雖被剝奪了一些無形價值，其程式或資料仍舊留在電腦裏。

這些困難點顯示，用傳統竊盜罪來規範當代新事物已稍嫌過時。由於傳統竊盜罪刻意強調行爲客體之有形性，不經意中排除掉了一個現代重要法益之保護範圍－無體財產之安全。在許多州，這些困難已經由立法修改原有條文得到一部份解決，但仍然無法修補所有法律漏洞。創設一個新犯罪類型，而沿用傳統竊盜罪之處罰，是一種較佳之解決方式。

有鑒於既有竊盜罪對資訊竊盜規範之不足，美國各州最常見之解決方式是修訂竊盜相關犯罪法律，擴大竊盜罪之定義及於資訊竊盜。比如科羅拉多州擴大「財產(property)」定義涵蓋「資訊，包括經電子處理所產生之資料，以及電腦軟體.....無論是以機器可解讀或人可解讀之形式表示」〔註十九〕。俄亥我州增修「財產」定義爲「包括但不限於經電子處理、產生、或儲存之資料，傳送中之資料，以機器或人可辨識形式表示之電腦程式，以及任何與電腦有關文件之原本或複製本」〔註二十〕。其他如懷俄明州、羅德島州、蒙他納州、明尼蘇達州等亦有類似之立法修正〔註二一〕，但此種定義雖能規範電腦相關之資訊竊盜，卻無法涵蓋與電腦資料不相關之營業祕密竊盜（討論於後），故仍須以更廣泛之財產定義方能規範之。而且，若僅就財產一詞重新定義，其他竊盜相關犯罪之規定維持不變，前述「非法取走」、「故意」等要件不明確之問題仍然存在。有些州，例如華盛頓州，就將「故意非法剝奪他人財產(an intent to deprive other's property)」規定爲要件，而更進一步重新定義剝奪(deprive)爲：「除一般意義外，[剝奪亦指]未經授權使用或複製紀錄、資訊、資料、營業祕密、或電腦程式，若上述等係爲私有性質(proprietary)」〔註二二〕。因此，如所涉及者係私人性質資料，故意複製或使用該資料將包括於竊盜定義之內。

至於一資訊何時方受保護，這些竊盜相關制定法並未提供清楚之界限，因此有可能導致被告所接近者爲一眾所周知之資訊，當事人並未盡力維護資訊隱密性，而被告仍被起訴之情形。如被告未經授權接近他人電腦，即使儲存於電腦上之資訊早已公開，亦可據此以竊盜罪將被告入罪；這種情形並不合理，因此，俄亥我州定義「財產」包含「電子資料」，且將「故意剝奪他人財產」之定義延伸至：「以不支付適當對價之故意使用....他人財產.....，並且無其他合理或正當理由不支付適當對價。」〔註二三〕

營業祕密竊盜 (Trade Secret Theft)

營業祕密竊盜不一定限於與電腦有關之資訊竊盜。營業祕密之概念可溯源普通法判例，制定法只不過是將之成文化。美國侵權行爲法彙編（第一版）將之定義爲：「使其占有人擁有商業上優勢和利益，具相對新奇性和祕密性之材料」〔註二四〕。此一民法定義不限於有形物，刑法定義亦同。加州刑法定義「營業祕密」

如下：「任何科技資訊、設計、製程、程序、公式、電腦程式、或儲存於電腦之資訊.....其具有祕密性和未公開性，且使其利用者比無該營業祕密之競爭對手擁有優勢。」〔註二五〕一些營業祕密竊盜罪之要件規定，必須有營業祕密附著之有形物被非法取走，此要件雖保護合理之舉證責任，但卻增加法院適用和解釋法律之困難〔註二六〕。

營業祕密所欲保護之法益爲此一資訊祕密性所帶來之商業競爭優勢，如其被以不正當方式竊取，此利益將會喪失。因此，如一資訊業已經公開，其也就不復再有所謂祕密或排他之利益存在。故營業祕密將刑罰只限於具相對祕密性和具體商業價值之資訊者，排除已公開之資訊，即使該資訊是僅以訂閱(subscription)方式有限度提供亦不例外。營業祕密之新穎性和祕密性要件，在民事和刑事案件上之要求標準不同，有時可能會引起明確性之困擾。加州刑法將一資訊推定爲祕密，如果其所有人採取合理措施防止資訊流入非經選擇之人手上〔註二七〕。此種以推定方式所產生之刑事責任，獎勵所有人維護其資訊祕密性所採取之努力。

許多州之刑事立法將刑罰度與所竊取財產之價值相連，此點雖符合傳統竊盜罪之刑罰原則，但有財產價值評估困難之問題。由於資訊係紀錄於有形媒介物之上，故如該媒介物亦被竊取時，財產價值必須就有形和無形物兩者價值一併評估，但可想像得到的，主要價值應是在於無形部份(但有形物占有之移轉提供了舉證之方便)〔註二八〕。對於竊取財產之價值，一般立法上有三種評估模式。第一種評價取決於所謂市場價值，但營業祕密所涉之財產係無形，又因其爲一祕密，故無確實交易和市場價格，只能假設一市場價值。第二種評價取決於重置成本。第三種評價取決於對原物主之損失，此可以明尼蘇達州之立法爲例〔註二九〕：「電子脈波...資料或資訊...電腦軟體或程式之價值，應考慮其所有者因喪失該項物件所致之合理經濟損失。此經濟損失數目之決定包括但不限於所有人之排他使用權和處分權。」

雖然資訊竊盜所涉及之法益價值甚高，但亦非全然均須以刑事制裁保護，契約法或侵權行爲法之民事制裁亦可提供保護。因此，立法政策上所須考慮的問題是，在民事制裁之上必須加上多少公法保護才算適當。雖然各州對此之立法反應不一，但可確定的一點是，有些高價值資訊以目前之民事救濟方式保護仍嫌不足，而有些低價值資訊則無須以刑法過度保護，認識此一點對未來之刑事政策制定是相當重要的。

㈢ 連線使用犯罪類 (Access and Use Crime)—侵害社會安全法益

前述兩種電腦犯罪類型，透過電腦進行之金融犯罪及資訊竊盜犯罪，與傳統概念之竊盜犯尚有些許相通之處。但是除了這些竊盜類似行爲，還有一些與電腦

相關且具侵害性之行爲（不在上述範疇之內）在某些州也受到刑法之規範。這些行爲包括：未經授權接近電腦、使用電腦、及修改電腦資料，惟其均不涉及錢財或經濟利益之竊取。

無權接近 (Unauthorized Access)

對於這些不法行爲之防止，雖較不易沿用傳統之犯罪保護範疇，但在電腦系統發展之過程當中，期待法律維護系統完整性(integrity)之要求逐漸受到肯認和重視。即使不具侵害之故意，單純之擅入電腦系統行爲往往也是具有破壞性的。這種闖入系統之行爲可能干擾，甚或毀壞他人之財產，此一財產雖係以無形之電子脈波形式存在，但卻代表他人心血之努力成果，並可能影響及許多人之權益。至於刑事政策上之考量則當然是：在什麼程度範圍內，對於故意或非故意之破壞系統行爲，是否課以刑事責任和制裁。

美國至少有十州對不法侵入電腦系統行爲課以刑事制裁〔註三十〕：亞利桑那州、德拉瓦州、喬治亞州、密西根州、新墨西哥州、南卡羅萊納州、北答柯達州、羅德島州、田納西州、以及猷他州。這些制定法通常將接近(access)定義爲：「對於電腦或電腦系統接近、下指令、與之通訊、儲存資料於、從之攫取資料、或其他使用其資源之方式。」〔註三一〕不論行爲人之無權使用是否爲故意，亦不論其是否對系統或所含資料確實造成任何損害，刑事責任均成立。亞利桑那州將之定位爲電腦詐欺，其他州立法制裁此種行爲者，多以「電腦濫用(computer abuse)」稱之，但內容大致相同。

此種刑事制裁可視爲前述電腦詐欺罪或資訊竊盜罪之較低層級犯罪(lesser included offense)。制裁電腦濫用罪之州，通常亦有電腦詐欺罪之立法；後者要件之一爲以不法之意圖接近電腦，前者則無須此種特別故意。此種對於電腦濫用罪之制裁，亦反映出立法者認爲無權接近，無論是否伴隨其他犯罪事實，此行爲本身即已是一嚴重之反社會行爲。因爲電腦所處理之資料價值與日俱增，無權侵入系統所可能招致之破壞後果也就日益嚴重。

拋開其他法益之保護考慮，此種制裁之重心係置於隱私權保護。立法者認爲有必要以刑事制裁來維護一電腦系統之完整性，即使侵入者並無破壞之惡意。也許會有人認爲此種刑罰是過度之立法反應，但它應該可視爲保護一種與公共危險罪所保護者類似之法益。各州對此所規定之法定刑不同，顯示出各該州立法者對此種嚴重後果之關切程度。比如北卡羅納州規定爲輕罪(misdemeanor)〔註三二〕，而喬治亞州則定爲最高可至十五年有期徒刑之重罪(felony)〔註三三〕。

無權使用 (Unauthorized Use)

上述這些立法制裁「無權接近」電腦行爲之州，當然同時亦制裁「無權使用」

行爲。有些州將這種行爲態樣另外分開處理，例如：佛羅里達州、密蘇里州、科羅拉多州、蒙他納州等〔註三四〕。依利諾州、懷俄明州則是將無權「使用」定義包含無權「接近」〔註三五〕。當然，無權使用電腦服務與傳統之竊盜罪有異，不在其規範之範圍。因爲，很明顯地，使用電腦處理資料之服務(service)並非有體財產一此於其他以不法方式取得任何服務之情形亦然。因此各州須針對竊盜罪作出調整，使其涵蓋無權使用電腦服務之情形。通常這包括兩種不同之行爲態樣，此可以懷俄明州之立法爲例：

「任何人明知並未經授權(i)接近一電腦....(ii)阻擾有權人使用他人所有、與他人依約操作之電腦系統之服務時，觸犯一對電腦使用者所犯之罪」〔註三六〕。

由於無權接近和使用電腦往往占據其他合法有權人使用共享時段(time share)之電腦時間，剝奪其使用電腦處理資料之機會，這種立法模式反映出立法者重視使用者對隨時能接近電腦系統這種方便之倚賴與保護期待，認其爲一種應受刑事保護之重要法益。

非法修改資料 (Criminal Modification of Data)

電腦系統儲存了龐大之業務或研究發展資料，其價值匪淺。雖然在大多數情形，系統侵入者係懷有一獲取經濟利益之不法意圖（或特定故意），但即使不具此種意圖，亦不能排除其因故意或過失改變系統資料，甚或摧毀整個系統資料，所帶來災難之可能性。此種行爲將使電腦系統因輸入不正確之資料產生不易察覺之錯誤運算結果，使企業誤判其動向，或使整個電腦系統作業停擺，使依賴系統資料進行之業務活動停頓，威脅到企業之生存。

雖然這種破壞行爲對公眾是一種嚴重威脅，但它不能適用傳統損毀罪(vandalism)，因爲它所涉及的客體是無體物。因此，許多州針對無權修改和摧毀電腦資料或電腦程式之行爲直接立法規範。多數將其與無權接近或無權使用之犯罪一併規範處理，其罪刑亦相當，從輕罪至十五年有期徒刑之重罪不等〔註三七〕。如無權竄改和摧毀電腦資料係爲一詐取錢財或利益之不法計劃時，則將改用前述之電腦詐欺罪或資訊竊盜罪（或一般竊盜罪），科以更高之刑罰度。

多數州在這種立法對於所破壞系統資料之性質並不做區分，例如：學生竄改學業成績（不威脅公共安全），和電腦駭客(hacker)竄改醫院病歷資料（威脅公共安全），均作同樣之規範和處置。而且，一般來說它們對於只有接近電腦行爲（情節較輕），和兼有竄改資料之行爲（情節較嚴重），處罰並無不同。此或許爲立法政策須加檢討之處。

參、美國聯邦政府之電腦犯罪相關立法〔註三八〕

聯邦刑法在財產犯罪上一般係居於次要地位，僅於聯邦政府利益受到侵犯時才介入。但因爲電腦犯罪經常涉及利用州際通訊設備，以遠端終端機遙控跨州犯罪。且大多數美國銀行和金融機構均屬於聯邦儲備銀行(Federal Reserve) 監督之體系，故前述電腦詐欺之金融犯罪亦免不了聯邦政府之介入。

㈠ 盜用聯邦公產

聯邦法典第18篇第641條禁止竊盜、背信、或侵占聯邦財產〔註三九〕。此法只適用於行爲客體爲屬於聯邦政府有價值之物(thing of value)。判例顯示，它並不排除無形客體，例如電腦資訊〔註四十〕；它亦包括電腦使用時間之服務〔註四一〕。

㈡ 妨礙州際通訊

聯邦法典第18篇第1341條禁止郵件詐欺，並適用於任何利用郵件以行詐騙之計劃〔註四二〕。聯邦法典第18篇第1343條禁止任何利用有線、無線、或電視通訊以行跨州詐騙之計劃〔註四三〕。兩者皆適用於涉及州際通訊〔註四四〕之電腦犯罪，但只限於特定通訊形式之詐騙以及有計劃之詐騙，並且州際通訊必須是犯罪計劃中重要之一環〔註四五〕，僅因州際交易涉及跨州電纜之通訊是不足的。另一相關法令是聯邦法典第50篇第1343條(Omnibus Crime Act)〔註四六〕，有關通訊資料傳輸之無權攔截與監聽，但本法只限於有線線路上聲音之攔截，不及於其他種類之通訊。

㈢ 贓物之州際運送

跨越州界運送贓物(interstate transportation of stolen goods)違反聯邦法典第18 篇第2314條〔註四七〕，但這只限於有形物(tangible)。理論上，這可適用於將竊盜之電腦程式列印報表資料或磁片攜帶過州界，但不適用於以連線下載之方式竊取資訊的情形。

㈣ 電子資金交易犯罪

由於現代金融機構之運作倚賴電子交易之程度日益加深，此類型之犯罪也將有增無減。這方面之重要聯邦法律規範爲聯邦法典第十五篇第1693條－電子資金交易法(Electronic Funds Transfer Act, EFTA)〔註四八〕。EFTA定義「電子資金交易(Electronic Funds Transfer, EFT)」爲：「任何資金之交易.....經由一電子終端設備、電話設備、或電腦所發起.....授權金融機構對其帳户登錄借記或貸記」

〔註四九〕。EFTA 並含有濫用電子資金交易系統之刑事制裁；第1693條第(n)項定義「借記設備(debit instrument)」爲「(任何)經由其吾人可發起一電子資金交易之.....卡片、條碼、或其他設計，但支票除外」〔註五十〕，同條項第(3)款對於以詐騙方式利用借記設備取得服務、金錢、貨物、或任何有價值之物課以刑事責任。

㈤ 侵害聯邦電腦罪

美國國會首次特別針對電腦法罪之立法爲聯邦法典第十八篇第1030條－1984年聯邦電腦犯罪法(Federal Computer Crime Act)〔註五一〕，其嗣後並經數次修正。本法針對濫用電腦危及國家安全之情事加以規範，第1030條第(a)項第(1)款刑事制裁無權或越權接近電腦以取得特定國家安全範疇之資訊〔註五二〕，如行爲人係故意或有理由可知該資訊之取得係用以傷害美國或幫助他國，違者可科以十年有期徒刑。其次，本法針對與聯邦政府運作有關之電腦，禁止其無權接近或越權使用，竄改、毀滅、或洩漏資料。本法同時並提供處罰無權接近電腦侵犯個人財務隱私之法源。依第1030條第(a)項第(2)款，未經授權接近電腦以取得「財務隱私權法(the Right to Financial Privacy Act)所定義之金融機構內金融紀錄.....或公平信用調查報告法(the Fair Credit Reporting Act)所定義之消費者信用調查報告資訊」將構成一年以下有期徒刑之刑事責任。但本特別法只規範政府所有電腦、與政府有契約電腦、或金融機構電腦(之消費者金融資訊)，其他不在此限但屬於跨州商務交易(interstate commerce)範圍者之電腦犯罪，則須適用其他一般法律。

肆、網路色情相關規範之爭議

關於猥褻出版品對成年人該不該管制？或只對未成年人管制？應管制到什麼程度？政府是否應把公權力放在打擊其他更嚴重之犯罪上？這些問題無論在美國或其他國家，都是被討論話題。有別於大多數之其他犯罪行爲，軟性之色情或猥褻出版品不涉及暴力衝突，並與文學、藝術創作有重疊之灰色地帶，故其管制之必要性爲美國法學界所檢討〔註五三〕。

近年由於電腦和網路的興起，數位革命推翻了往昔只能以「原子」(油墨、紙張等有形物質)爲交易單位之出版形式，代之以電子傳送「位元(bit)」之出版形式〔註五四〕，其所能傳遞資訊之數量、種類、速度、以及檢索之方便等，顛覆了吾人擴散思想文化之傳統模式。出版也從以往必須有資財力的出版公司或文化事

業才能辦得到的事，變成任何人在網路上架設一網站首頁或BBS即可爲之「個人出版」，而且跨越國界無遠弗界。

由於這種個人出版者爲數眾多，任何一國家欲對之加以二十四小時監控管理，幾乎是不可能作到。在這種情形下，隱藏在人性內心被抑制之原始慾望，就在網路上的色情言論或猥褻出版品中蓬勃地反映出來。由於這些出版內容部份威脅到兒童或青少年的身心健康和安全，故各國均嘗試管制網路色情。然而，任何這種嘗試努力，無可避免地將會和言論自由的保護利益發生對立衝突。

美國國會於1996年制定電信通訊法(Telecommunications Act)〔註五五〕，全法共七章，其原本主要是針對區域性電話服務市場、多頻道影視市場、以及無限廣播市場之管制，並非專門關於網際網路(Internet)之特別立法；然而在參議院小組委員會將法案送全院審查後，臨時被添加入引發本案爭議之附帶修正案，並獲表決通過。其第五章(又名通訊約束法Communications Decency Act, 簡稱CDA)被加入「低俗不雅內容傳送」條款("indecent transmission" provision)〔註五六〕以及「顯然令人厭惡之展示」條款("patently offensive display" provision)〔註五七〕。依這些條文之文義，可賦予行政機關極大權限，檢查並約束網路上之文字和圖畫，引發國會是否踰越立法權限，限制憲法第一修正條款所保障人民言論自由之爭議。

第223條第(a)項禁止明知而傳送猥褻(obscene)或低俗不雅(indecent)之訊息給予任何18歲以下之收受訊息者。相關條文如下〔註五八〕：

(a) 任何人－

(1) 於州際或國際通訊 －

. . . . . .

B) 經由通訊裝置明知地 －

i) 製作、創造、或鼓勵創作，並

ii) 發起傳送通訊，

任何評論、請求、意見、建議、形象、或其他通訊，其內容爲猥褻或低俗不雅者，明知收受訊息者爲18歲以下之人；無論製作該訊息者是否爲原始發動通訊者；

(2) 明知而允許任何在其控制下之電信通訊設備被用於第1)段文所禁止之活動，並有將該設備供使用於此種活動之故意，

將被依第18篇之罰則處分，或處兩年以係有期徒刑，或兩者併科之。

第223條第(d)項禁止在可能爲18歲以下之人收到訊息之狀況下，明知而傳送或展示顯然令人厭惡(patently offensive)之訊息。相關條文如下〔註五九〕：

(d) 任何人—

(1) 於州際或國際通訊中明知地 —

A) 向18歲以下之特定人或特定多數人，使用互動式電腦服務傳送(to send)，或

B) 在可能爲18歲以下之人收到訊息之狀況下，使用互動式電腦服務展示(to display)，任何評論、請求、意見、建議、形象、或其他通訊，其內容描述性、排泄活動或器官，依當代社區標準衡量，顯然地令人厭惡；無論使用該服務者是否爲原始發動通訊者；

(2) 明知而允許任何在其控制下之電信通訊設備被用於第(1)段文所禁止之活動，並有將該設備供使用於此種活動之故意，

將被依第18篇之罰則處分，或處兩年以係有期徒刑，或兩者併科之。

由於上述條文涵蓋甚爲廣泛，國會爲緩和其對言論自由之衝擊效應，另於第223條第(e)項第(5)款提供積極抗辯事由(affirmative defenses)給予任何以善意、合理、有效、適當之行爲，限制未成年人接近管制通訊之人。相關條文如下〔註六十〕：

(5) 對於依本條(a)(1)(B)或(d)項起訴，或因使用(a)(1)(B)設備活動被依(a)(2)起訴者，得爲抗辯，如該人—

A) 已經以在整體情況下爲善意、合理、有效、適當之行爲，限制或防止未成年人接近本條所管制之通訊，其可以任何適當之對未成年人通訊管制手段爲之，包括任何現有科技可行之方法；或

B) 已經規定使用者必須提供信用卡、貸記帳號、成人接近密碼、或成人身份號碼等查證方式，限制接近通訊之措施。

由於認爲相關「低俗不雅(indecent)」條文規定失之明確(too vague)，不足以提供符合罪刑法定主義之刑事責任基礎，並有掐制言論自由之寒蟬效應(chilling effect)，美國民權自由聯盟(ACLU)遂於本法一經總統公布生效後，立即在1996年2月8日提出憲法訴訟。賓夕法尼亞州東區聯邦地院認爲系爭CDA法令侵犯言論自由，將之宣告違憲。聯邦政府以司法部長Reno女士爲代表提起上訴，美國聯邦最高法院也隨即於隔年迅速作出回應，於1997年6 月26日作出Reno v. ACLU, 117 S.Ct. 2329 (1997) 一案之判決，確定CDA違憲。

本案之重要關鍵在於：國會以管制「低俗不雅」言論標準取代過去之「猥褻」標準，是否能通過憲法檢驗。聯邦最高法院於Miller v. California, 413 U.S.15 (1973)已認定猥褻言論不在憲法保障範圍，並於該案中建立起一套辨識「猥褻」之三個標準：一、引發淫慾(appeal to the prurient interest；而此一引發淫慾之

判定標準係依照所謂「當代社區標準」contemporary community standard)；二、顯然令人厭惡(patently offensive)；三、欠缺重大文學、藝術、政治、科學價值(lack of serious literary, artistic, political, or scientific value)。聯邦最高法院肆後於FCC v. Pacifica Foundation, 438 U.S.726 (1978)，維持了一件聯邦通訊委員會(FCC)限制「低俗不雅」廣播之行政命令，認爲其不違憲。該案係FCC 處罰無線電台於下午時間在收音機中連續播送一段名爲「骯髒字眼(Filthy Words)」之廣播，文字涉及排泄器官、性器官或活動等「低俗不雅、顯然令人厭惡」之內容，其雖無引發淫慾之虞，但可能對孩童身心造成不良之影響，故遭停播處分。聯邦最高法院雖於Pacifica此一個案中肯認政府於某些情況下得限制「低俗不雅」言論，以保護政府在其他方面之迫切利益，但從未將「低俗不雅」言論與「猥褻」言論明白劃上等號，給予完全相同對待。這一問題遂於Reno v. ACLU又重新浮上檯面。

本案中聯邦政府除Pacifica一案之外，尚提出數個判例支持其有利觀點，但均未被聯邦最高法院採納。限於篇幅，在此不擬詳加討論每一爭點，惟筆者觀之聯邦最高法院解釋理由，可認系爭CDA法令有下列缺失，是遭宣告違憲之原因：

㈠ 規範不夠明確：舉例來說，任何人在網路通訊或電子郵件上討論避孕方法、同性戀、甚至監獄強暴事件之後果等嚴肅話題，亦難保不被刑事起訴之威脅；因爲理論上這些討論之通訊內容皆該當於第223條之構成要件，而且可能被傳達到未成年人之手上。

㈡ Miller之「猥褻」定義僅限於性活動，而CDA之「低俗不雅」定義則擴及：(1)排泄活動；(2)與性和排泄有關之器官。此對於言論自由限制之涵蓋層面較廣，故須接受更嚴格之審查。

㈢ CDA可以更少限制手段(least restrictive alternative)達成同樣效果（若用大陸法系之用語，即「違反比例原則」）；聯邦最高法院認爲不可只爲保護小孩，遂將成人之言論自由降至小孩之水準。

㈣ 由於網路之觀眾遍及全國（甚至全球），故如CDA之被告遭起訴，一定是在全國較保守之地區被起訴，並將依照對其最不利之「社區標準」來判斷其內容是否引起淫慾（參見前述Miller案三個標準之第一項），此亦爲對言論自由不利之因素，故更須接受嚴格審查。

我國關於網路色情的管制情形

我國目前關於網路色情的主要規範爲刑法二百三十五條：「(第一項)散布或販賣猥褻之文字、圖畫或其他物品，或公然陳列，或以他法供人觀賞者，處一年以下有期徒刑、拘役或科或併科三千元以下罰金」。而關於「猥褻」之認定，業

經司法院大法官釋字四百零七號解釋在案（其「猥褻」之定義與前述美國Miller案大體上相去不遠〔註六一〕；惟適用我國之「社區標準」或「社會一般觀念」，所得之尺度必然與美國迥異）。我國憲法第十一條雖亦同美憲修正第一條保障人民言論自由，但無類似美憲之「國會不得立法限制....」等直接限制立法文字，所以對立法自由形成之限制空間較小，從而行政權限可能之範圍亦較大。

關於網路色情的管制，我國目前在運作上尚無大礙，未有要求單獨特別立法之呼聲。然而，這是否係以保護未成年人爲名，犧牲對於成年人言論自由不必要限制之代價來達成，值得我們隨時檢討。如現有科技的水準已有辦法對於網路使用者之年齡加以篩選時，吾人應盡量降低對成年人自主權之干涉，避免國家家長主義(paternalism)之心態。

在未來資訊優先的時代，國家之競爭力取決於資訊傳遞之效率；雖然猥褻言論（相對於政治言論）屬於所謂低價值言論(low value speech)，但是對於任何言論之過度管制，皆將侵及個人之人格形成，獨立判斷力之養成，並造成抑制其他合法言論之寒蟬效應(chilling effect)，故任何對於言論之管制不可不戒愼。同時，網際網路是一跨越國界之事物現象，有時可能涉及國際私法之管轄權問題，故吾人亦不能完全漠視他國相關法律之存在，應隨時注意其發展，並於必要時作出相對之立法反應。

伍、我國最近電腦犯罪立法之檢討

我國於八十六年十月八日修正公布刑法第二百二十條、第三百十五條、第三百二十三條及第三百五十二條條文；並增訂第三百十八條之一、第三百十八條之二、第三百三十九條之一至第三百三十九條之三條文，針對電腦犯罪修訂新法。以下茲逐條檢討之。

第二百二十條

在紙上或物品上之文字、符號、圖畫、照像，依習慣或特約，足以爲表示其用意之證明者，關於本章及本章以外各罪，以文書論。

錄音、錄影或電磁紀錄，藉機器或電腦之處理所顯示之聲音、影像或符號，足以爲表示其用意之證明者，亦同。

稱電磁紀錄，指以電子、磁性或其他無法以人之知覺直接認識之方式所製成之紀錄，而供電腦處理之用者。

〔檢討〕：本次修法增加關於「電磁紀錄」方面之規定，用以涵蓋電腦資訊。此次我國係將日本有關電磁紀錄的規定，連同用語一起移植至我刑法，但日本係將電磁紀錄的定義放在刑法總則（如同刑法第十條關於公務員、文書等用語之定義），而我國則是放在刑法分則。這一個表面上安排之小差別，卻產生概念結合之解釋問題，甚至導致全面性重刑化〔註六二〕。

美國各州在刑法典以專章針對電腦犯罪加以定義和規範，例如：computer（電腦），computer network（電腦網路），computer system（電腦系統），computer program（電腦程式），computer software（電腦軟體），services（服務），computer services（電腦服務），data（資料），private personal data（隱私個人資料），property （財產權），financial institution（金融機構），financial instrument（金融支付工具）等與電腦犯罪有關之名詞，多半均分別定義，並集中於專章特別規範和處理。

我國未採如此作法，而係將相關規範散見在刑法分則條文中，有時不免有無法互相配合(coordination)之虞。例如本條欲以有體之文書(documents)概念加以修改，將之延伸至無體之資訊(information)，可能就會有問題產生。文書之性質爲用來表達意思，所以本條第一項和第二項均加上「足以爲表示其用意之證明者」之要件，此於電腦資料(data)可以適用，但於電腦程式(computer programs)即有問題，因其只是執行運算之一連串數學和邏輯指令，並不含有任何表意〔註六三〕。依本條規定，電腦程式之重要法益，在本次修法可能會不經意地被排除在刑法保護之外。

此外，本條第三項之「電磁紀錄」一辭，對於即將到來之大量資訊將以「光學儲存媒體」（雷射光碟）形式儲存的時代而言，似乎又已稍嫌不足。雖然本條文同時設有「或其他無法以人之知覺直接認識之方式所製成之紀錄」之要件以資補充，但此爲一種「混合構成要件」，以概括規定授權裁判官補充立法之方式，能免則宜免。同時，以電磁(electro-magnetic)一辭來涵蓋與其性質不盡相同之光學(optical)事物〔註六四〕，亦容易產生誤解。

上述這些問題，如以特別法之方式分開處理〔註六五〕，或許較容易得到注意和迅速解決。

三百十五條

無故開拆或隱匿他人之封緘信函、文書或圖畫者，處拘役三千元以下罰金。無故以開拆以外之方法，窺視其內容者，亦同。

〔檢討〕：本次修正雖增列「無故以開拆以外之方法，窺視其內容者，亦同」之字句，以規範「電子郵件 (e-mail)」，然而，本條既以「封緘信函」爲構成要

件，e-mail在何情況下視爲封緘信函或明信片，本條並未詳加規定。是否以密碼(password)限制接近電腦(restricted access)即等同於封緘？此點尚有待觀察。如前所述，此類問題之產生皆肇因於本次刑法修正時，立法者強欲將傳統「有體」文書、信函之概念擴展至「無體」之資訊，而兩者之性質不同，將之勉強湊合，只有問題叢生，徒增困擾〔註六六〕。

我國刑法關於電腦之妨害祕密罪，於美國各州多係以 "access crime"之「無權接近罪」治之（詳見前述連線使用犯罪類之討論），其制定係基於保護公共安全與便利之法益概念，構成要件較爲簡單，一般均僅以未得授權接近他人電腦系統爲已足。

第三百十八條

公務員或曾任公務員之人，無故洩漏因職務知悉或持有他人之工商秘密者，處二年以下有期徒刑、拘役或二千元以下罰金。

第三百十八條之一

無故洩漏因利用電腦或其他相關設備知悉或持有他人之秘密者，處二年以下有期徒刑、拘役或五千元以下罰金。

第三百十八條之二

利用電腦或其相關設備犯第三百十六條至第三百十八條之罪者，加重其刑至二分之一。

〔檢討〕：原第三百十八條公務員妨害祕密罪增加「因利用電腦或其他相關設備」知悉他人秘密（第三百十八條之一）以規範電腦新事物，並加重刑罰以茲嚇阻（第三百十八條之二）。但此或許與「電腦處理個人資料保護法」之刑罰法規重疊，依特別法優於普通法而被競合和吸收〔註六七〕。

美國之聯邦法律對於無權或越權接近聯邦政府電腦，以取得國防、外交、原子能等國家安全資訊者，處以十年以上重刑。本次增修之第三百十八條之二，就條文之文字以觀，此種對於公務員利用電腦設備妨害業務祕密之「加重二分之一處罰」，似乎只能侷限於第三百十六條至第三百十八條之洩漏「一般祕密」者，反而不及於後果較爲嚴重之第一百零九條至第一百十二條之洩漏「國防祕密」者。此亦爲將電腦犯罪相關規定於刑法分則中作凌散修改(piecemeal reforms)所生缺點之另一事例。

第三百二十三條

電能、熱能及其他能量或電磁紀錄，關於本章之罪，以動產論。〔檢討〕：原條文爲「電氣」改爲「電能、熱能及其他能量或電磁紀錄」，以茲涵蓋電腦與隨附之新事物現象。本次修法除了將電磁紀錄或資訊「準文書化」（第二百二十

條第二項）之外，亦將之「準動產化」。本條無視電磁紀錄或資訊之無體性，強欲將之與有體動產歸爲同類處理，將作爲表徵物之電磁記錄，與作爲被表徵物之動產劃上等號，易滋生問題〔註六八〕。此外，如前所述〔註六九〕，未將新興之「光學」儲存媒體與「電磁紀錄」儲存媒體一同考慮，亦算是一種缺失（雖則目前條文上仍可以「其他能量」一辭涵蓋之）。

第三百三十九條

意圖爲自己或第三人不法之所有，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。

以前項方法得財產上不法之利益或使第三人得之者，亦同。

前二項之未遂犯罰之。

第三百三十九條之一

意圖爲自己或第三人不法之所有，以不正方法由收費設備取得他人之物者，處一年以下有期徒刑、拘役或三千元以下罰金。

以前項方法得財產上不法之利益或使第三人得之者，亦同。

第三百三十九條之二

意圖爲自己或第三人不法之所有，以不正方法由自動付款設備取得他人之物者，處三年以下有期徒刑、拘役或一萬元以下罰金。

以前項方法得財產上不法之利益或使第三人得之者，亦同。

第三百三十九條之三

意圖爲自己或第三人不法之所有，以不正方法將虛僞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。

以前項方法得財產上不法之利益或使第三人得之者，亦同。

〔檢討〕：原三百三十九條詐欺罪增設之一、之二、之三等三條文，三百三十九條之一與三百三十九條之二這兩條的規定，顯然是爲解決前述詐欺「人」與詐欺「機器」的爭議〔註七十〕，針對金融卡犯罪等而設的。然而它與電腦犯罪又不必然一定有關，因爲除了以供電腦處理之磁卡從機器詐騙錢財和服務之不正方法外，還有許多其他不具電腦特質之不正方法，亦可以取得錢財和免費服務（比如說爬牆進動物園，如動物園非用人工收票而係以自動投幣機入場），但這些顯然並非新法所欲規範者。「不正方法」一辭似嫌範圍過廣泛(overbreadth)。

三百三十九條及之一、之二等之第一項皆先規範取得他人(有形)之「物」的行爲，第二項再規範取得他人(無形)之「財產上不法利益」的行爲。然而三百三十九條之三卻於第一項、第二項皆用「財產」和「財產上不法利益」。因我國民

刑法均未就「財產」一辭特別加以定義，民法僅就「物」、「動產」加以定義，故筆者猜測，此處之「財產」用語是否近似於英美法之"property" 概念？依布萊克法律辭典(Black's Law Dictionary)，「財產(property)」一辭指屬於某人之權利的集合(an aggregate or a bundle of rights)，「財產上利益(proprietary interest)」乃隨附於該財產權利之利益，而「物(thing)」則爲該財產權利之客體(the object of a right)，例如：擁有某公司股票之財產權利，即可享有分配股利之財產上利益，而股票爲表徵該財產權之客體物(evidence of right)。如依此解釋，三百三十九條之三第二項即成第一項之贅文，因其所指者並不超出第一項之範圍。

三百三十九條之三關於「製作或變更紀錄」之要件可能有一問題：如本文先前所討論者，資訊竊盜(information theft)無須如本條規定製作或變更財產權紀錄，僅以「複製」甚或「窺視」之手段，即可取得他人之無體財產或經濟利益（亦無須滿足「非法取走」之asportation要件）。本條之規定似並未將此種information theft之特質完全加以考量。

第三百五十二條

毀棄、損壞他人文書或致令不堪用，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。干擾他人電磁紀錄之處理，足以生損害於公眾或他人者，亦同。

〔檢討〕：原毀損器物罪關於以磁力之作用或使用破壞程式之方式，而使磁帶或磁碟所儲存之紀錄消失之行爲，在刑法評價尚可否該當餘毀損罪之毀損，向有爭議〔註七一〕。持否定意見者認爲磁帶之磁化或儲存在磁帶上之資料，並非第三百五十二條之「文書」或第三百五十四條之「物」。本次修正特增設「干擾他人電磁紀錄之處理」部份條文，以規範電腦駭客施放電腦病毒(computer virus)之不法情形。

宜注意者，我國並未如美國某些州將access crime定爲舉動犯，處罰單純之「無權接近」電腦行爲，而係須要證明有「足以生損害於公眾或他人」之危險才處罰。對於純惡作劇之業餘電腦駭客，嚇阻作用可能稍嫌不足〔註七二〕。

陸、結　語

電腦的發明對於現代人的生活方式和行爲態樣，已經產生無以倫比之廣大深遠影響；近幾年來網路的普及化，以及電腦儲存媒體之低價化、大量化，勢又將

對於我們的社會文化生活展開另一波新的衝擊。生活和行事方式的改變，意味著犯罪形態也將推陳出新，法律亦須隨時作出因應調整，以跟隨時代的脈動前進。本次刑法修正，反映出立法者能順應時代潮流之趨勢，隨之作出彈性調整；惟新法仍存有許多爭議之處，有待學界之繼續討論和實務判決之釐清，並於下次修法時納入考量。

註　釋

註一：Nimmer, The Law of Computer Technology, (Boston; Warren, Gorham& Lamont, 1985). 以下簡稱Nimmer.

註二：關於電腦犯罪之分類，國內學者上有許多其他不同之分類法，茲舉數例供作比較參考：

一、林山田教授：

(1)電腦操縱－輸入操縱、程式操縱、輸出操縱；(2)電腦間諜；(3)電腦破壞；(4)電腦竊用

二、林永謀大法官

(1)對電腦之犯罪－「加害於電腦之行爲」及「洩漏、竊用、藉電腦獲得資訊之行爲」

(2)惡意使用電腦之犯罪

三、劉江彬教授

(1)電腦破壞(computer sabotage)；(2)竊用電腦(theft of service)；(3)濫用電腦；(4)安全系統之破壞

註三：標題之前半部爲Nimmer氏之分類方式，後半部爲筆者對此種分類性質之補充註解。

註四：Perkins & Boyce, Criminal Law, pp.354-357 (Foundation Press, 1982); Lafave & Scott, Criminal Law, pp.644-654 (West, 1972).

註五：例如以發行 "Quicken"個人理財軟體著稱之Intuitive公司，就提供了一種"Checkfree"之電子支票代付服務。

註六：我國實務界對於原刑法三百三十九條詐欺罪 "以詐術使「人」將本人或第三人之物交付"之規定，亦有使「自動付款設備」（或其內建之「電腦」）陷於錯誤，非使「人」陷於錯誤，與詐欺罪構成要件不該當之疑義。司法

研究年報第十八輯第十九篇：「電腦運用所衍生法律問題之研究」，133頁，司法院印行（民國86年）。

註七："Whoever knowingly....without proper authorization, access..... any computer.....for purpose of : (1) devising or executing any scheme to defraud [another], or (2) obtaining money, property or services.....by means of false or fraudulent pretenses, representation or promises shall be guilty of computer fraud." Del. Code Ann. Tit. 7 Sec.858a (1982). 參見註1，Nimmer, p.9-11.

註八：Ariz. Rev. Stat. Ann. Sec. 13-2301(E). "A person commits computer fraud in the first degree by accessing, altering, damaging or destroying without authorization any computer, computer system, computer network, or any part of such computer, system, or network, with the intent to devise or execute any scheme or artifice to defraud or deceive, or control property or services by means of false or fraudulent pretenses, representations or promises.

A person commits computer fraud in the second degree by intentionally and without authorization accessing, altering, damaging or destroying any computer, computer system or computer network or any computer software, program or data contained in such computer, computer system or computer network." 參見：司法研究年報第十八輯第十八篇：「電腦犯罪理論與實務問題研究」，183頁，司法院印行（民國86年）。

註九：Virginia Computer Crimes Act. "Any person who uses a computer or computer network without authority and with the intent to: 1. Obtain property or services by false pretenses; 2. Embezzle or commit larceny ; or 3. Convert the property of another shall be guilty of the crime of computer fraud". 同上註，218頁。

註十：Ariz. Rev. Stat. Ann. Sec. 13-2301(E). "Computer fraud in the first degree is a class 3 felony. Computer fraud in the second degree is a class 6 felony." 同上註，183-184頁。

Fla. Stat. Ann. Sec. 815.03. "..... Except as otherwise provided in this subsection, an offense against intellectual property is a felony of the third degree, punishable as ..... If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to

obtain any property, then the offender is guilty of a felony of the second degree, punishable as ..... " 同上註，189頁。

註十一：Minn. Stat. Sec. 609.87 thru 609.89; Conn. Gen. Stat. Ann. Sec. 52 thru 53a; Va. Code Sec. 18.2-152.1 thru 18.2- 152-14; Mich. Stat. Ann. Sec. 752.797; Utah Code Ann. Sec. 76-6-703; NM Stat. Ann. Sec. 30-16A-3.

註十二：英美法之 "attempt crime"依字面直譯爲「企圖犯」，然其實質意義較接近大陸法系之「未遂犯」，其實指只要具有犯特定罪之企圖而付諸實施，無待目的結果之實現即可獨立成立另一刑事責任之謂。

註十三：Ariz.Rev.Stat.Ann.Sec.13-2301(E), 13-2316; Del.Code Ann. Tit.7, Sec.857, 858 ; Ga. Code Ann. Sec.26-9951(a)－26-9953; ND Cent. Code Sec. 12-106, 12-108.

註十四：同註 1 Nimmer, 9-12.

註十五：同註 1 Nimmer, 9-13.

註十六：Ward v. Superior Court, 3 CLRS 206 (1972).

註十七：Hancock v. State, 402 SW 2d 906 (1966).

註十八：英美刑法Larceny之 "intent to deprive permanently other's property"，相當於我刑法二百三十條「意圖爲自己或第三人不法之所有」之意思要素，此種intent爲specific intent，乃係特別主觀違法要素，非一般之故意。

註十九：Colo.Rev. Stat. Sec.18-5.6-101(8): property includes "information, including electronically produced data, and computer software.....in either machine readable or human readable form."

註二十：Ohio Rev. Code Ann. Sec. 2901.01(J)(1): "Property includes but is not limited electronically processed, produced or stored data, data while in transit, computer programs in either machine or human readable form, and any original or copy of a document associated with computers."

註二一：Wyo.Stat.Sec.6-3-502; RI Gen.Laws Sec.11-52-1; Mont.Code Ann.Sec.45-2-101(54); Minn.Stat.Sec.609.87.

註二二：Wash. Rev.Code Ann. Sec. 9A.56.010(e)(5): "In addition to its common meaning ["deprive" means] to make unauthorized use or an unauthorized copy of records, information, data, trade secrets, or com-

puter programs, provided that the aforementioned are of a private proprietary nature."

註二三：Ohio Rev. Code Ann. Sec.2913.01(C)(3): "use....property....with the purpose not to give proper consideration in return....and without reasonable justification or excuse for not giving proper consideration."

註二四：Restatement (First) of Torts Sec.757: "material of relative novelty and secrecy that conveys a commercial benefit or advantage to its possessor."

註二五：Cal. Penal Code Sec.499(c): "[A trade secret is] any scientific or technical information, design, process, procedure, formula, computer program or information stored in a computer....which is secret and is not generally available to the public and [which] gives one who uses it an advantage over competitors who do not know or use the trade secret."

註二六：見前揭註16和註17，加州法院和德州法院關於有體物(tangible)之解釋。

註二七：同上註。

註二八：例如竊取之營業祕密紀錄於筆記本，筆記本之價值爲有形，祕密資訊之價值爲無形，兩者皆爲犯罪行爲客體。同理，如將電腦之列印資料竊走，理論上，列印報表之紙張價值雖微乎其微，亦是行爲客體(但顯然主要價值係在無形部份)。當然，大多數之電腦犯罪係以連線、資料複製之方式完成，所以無有形客體可資證明。

註二九：Minn.Stat.Sec.45-2-101(69)(a)(iii)："The value of electronic impulses... data or information....computer software or program....shall be considered to be the amount of the economic loss that the owner of the item might reasonably suffer by virtue of the loss of the item. The determination of the amount of such economic loss includes but not limited to consideration of the value of the owner's right to exclusive use or disposition." 見註1，Nimmer, p.9-20.

註三十：5A Ariz.Rev.Stat.Ann.Sec.13-2316; Del.Code Ann.tit.11, Sec.858; Ga. Code Ann. Sec.26-9952(a); NM Stat.Ann.Sec.30-16A-3, 30-16A-4; NC Gen.Stat.Sec.14-454; ND Cent.Code Sec. 12.1-06.1-08; RI Gen Laws Sec.11- 52-1-11-52-4; Tenn.Code Ann.Sec.39-3-1404; Utah Code Ann. Sec.76-6-703. 見註1，Nimmer, p.9-21.

註三一："to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resource of, a computer or computer system." 見註1，Nimmer, p.9-21.

註三二：NC Gen.Stat. Sec.14-454.

註三三：Ga. Code Ann. Sec.26-9952(a).

註三四：Fla.Stat.Ann.Sec.915-06; Mo.Ann.Stat.Sec.569.095; Colo.Rev.Stat.Sec. 18-5.5-102; Mont.Code Ann.Sec.45-6-311.

註三五：Ill.Ann.Stat.Sec.16-9; Wyo.Stat.Sec.6-3-504.

註三六：同上註Wyo.Stat.部份。

註三七：參見註32與33。

註三八：Nimmer, pp.9-24 to 9-29.

註三九：18 USC Sec. 641.

註四十：U.S. v. Girard, 601 F2d 69 (2nd. Cir.), cert.denied, 444 U.S. 871 (1979); U.S. v. Truong Dinh Hung, 629 F2d 908 (4th Cir., 1980).

註四一：U.S. v. Sampson, 6 CLRS 879 (ND Cal., 1978)

註四二：18 USC Sec. 1341.

註四三：18 USC Sec. 1343.

註四四：U.S. v.Seidlitz, 589 F2d 152 (4th Cir., 1978),由遠端終端機透過連線盜取電腦軟體者，適用聯邦法典第1343條，因爲被竊資訊之電子脈波跨越了州界。

註四五：U.S. v. Computer Services Corp., 511 F.Supp. 1125 (ED Va., 1981), 一超收電腦服務帳款之詐騙事件涉及跨州之連線電腦，但法院認爲跨州電纜只被用來提供電腦服務，而該項服務本身並無其他證據指其爲惡劣或欺騙性質之服務，或有任何不實之事實陳述被透過州際通訊系統傳遞，故透過州際電纜傳遞之服務資料並非詐騙計劃重要相關之因素，不適用聯邦法典第1343條。反之，U.S. v. Giovengo, 637 F2d 941 (3rd Cir., 1980), 則認爲以電腦遙控州際通訊進行與機票買賣有關之詐騙，可適用聯邦法典第1343條。

註四六：50 USC Sec.1809 (1982).

註四七：18 USC Sec.2314.

註四八：15 USC Sec.1693.

註四九：15 USC Sec.1693(a)(6): "(any) transfer of funds.....which is initiated through an electronic terminal, telephone instrument, or computer.....

(to) authorize a financial institution to debit or credit an account."

註五十：15 USC Sec.1693(n): "(any) card, code, or other device, other than a check .....by the use of which a person may initiate an electronic fund transfer."

註五一：18 USC Sec.1030.

註五二：這些國家安全範疇爲：經美國政府之法律或行政命令規定，爲國防或外交上原因，須加保護以防止無權洩露之資訊，或任何經1954年原子能法所限制之資料。

註五三：Ronald Dworkin, "Do We Have a Right to Pornography? ", A Matter of Principle, p.335, Cambridge, Harvard University Press (1985) [refer to "the 1979 Williams Report"]

註五四：參見：Nicholas Negroponte, Being Digital，pp.1-20, N.Y., Vintage Books (1995)（中譯本：尼葛洛龐帝著，齊若蘭譯，數位革命，天下文化，1995年）。

註五五：47 USC Sec.151, et seq.

註五六：47 USC Sec.223(a).

註五七：47 USC Sec.223(d).

註五八：47 USC Sec.223(a): Whoever-

(1) in interstate or foreign communications-

B) by means of a telecommunications device knowingly-

i) makes, creates, or solicits, and

ii) initiates the transmission of,

any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication;

(2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity,

shall be fined under Title 18, or imprisoned not more than two years, or both.

註五九：47 USC Sec.223(d):

(d) Whoever-

(1) in interstate or foreign communications knowingly-

A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or

B) uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; or

(2) knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity,

shall be fined under Title 18, or imprisoned not more than two years, or both.

註六十：47 USC Sec.223(e)(5):

(2) It is a defense to a prosecution under subsection (a)(1)(B) or (d) of this section, or under subsection (a)(2) of this section with respect to the use of a facility for an activity under subsection (a)(1)(B) of this section that a person-

(A) has taken, in good faith, reasonable, effective, and appropriate actions, or under the circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology; or

(B) has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number.

註六一：釋字第四〇七號：「.....惟猥褻出版品，乃指一切在客觀上，足以刺激或滿足性慾，並引起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。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爲觀察，並依當時之社會一般觀念而定之。又有關風化之觀念，常隨社會發展、風俗變異而有所不同，主管機關所爲釋示，自不能一成不變，.....」。

註六二：李茂生，"資本、資訊與電腦犯罪"，權力、主體與刑事法－法邊緣的論述，208-209頁，台大法學叢書編輯委員會編輯 (1998年)。以下簡稱「李文」。

註六三：黃榮堅，"刑法增修後的電腦犯罪問題"，罪與刑－林山田教授六十歲生日祝賀論文集，310-311頁，(台北，五南出版，1998)。以下簡稱「黃文」。

註六四：磁碟機是利用鐵和某些物質可以磁化的特性，將磁場紀錄於這些物質（通常爲氧化鐵）表面，磁碟的表面（無論軟碟或硬碟）就好似一由許多點排成的陣列，每個點代表一個位元，可以磁化成相當於0或1的極性。電腦資料就以0與1的電子訊號形式表示，經由讀寫頭(Read/Write Head)的電磁感應轉換手續，儲存於磁碟表面的這些磁場陣列上；或於讀取時，將磁碟上的磁場紀錄，反方向的轉換成相對應電流之數位訊號，供電腦運算。（參見：1998十月號PC home雜誌，176頁）

雷射則是高度定向與單一波長的光束，把光束集中在某一個小點上，若此定點有一類似鏡面之光滑平面，光束就會原封不動的反射回去；若此點有個大小適中的凹洞，由凹洞底部反射的光線，會與凹洞周圍反射的光線有不一樣的相位，兩種不同相位的光線會互相干涉，產生和原先截然不同的反射光束。電腦光碟表面含有許多凹洞和空白，與唱片的凹槽類似，電腦光碟機在讀取資料時，以雷射光掃描旋轉中的碟片，偵測反射回來的光束性質，獲知光碟平面與凹洞的變化，而產生相對應的電子訊號。目前的電腦光碟技術有CD-ROM, CD-R, CD-RW, DVD等幾種。CD-ROM是目前最普遍的光學裝置，爲一般新電腦皆有之標準配備，它只含現成資料，不能寫入並儲存新資料；CD-R表面由一層有機染料層構成，可以燒錄資料一次；CD-RW表面由一層相變合金層構成，可以燒錄資料多次；另外現正開始逐漸流行的DVD，則是一種超高儲存容量的光學媒體。（同上，190頁； 另見Bill Gates, The Road Ahead, Rev.Ed., p.31, (N.Y., Penguin Books, 1996).）

由以上所述磁碟和光碟之原理，可見兩種儲存媒體之性質和作用並不盡相同，概以「電磁紀錄」稱之，恐有不妥。

註六五：劉江彬教授就傾向單獨立法，因爲電腦犯罪有其特性，有些行爲與單純的刑事犯罪有別。參見：劉江彬，資訊法論－電腦與法律問題之探討，200頁，台大法學叢書編輯委員會編輯 (1988年，二版)

註六六：參見：黃文312-314頁，及李文209-219頁。兩位教授對於將電磁記錄準文書化(與準動產化)所滋生的體系混淆，皆有精闢之分析。黃文331頁提及德國刑法202條將「資訊」與「文書」分開處理，其202條(1)項規定妨害祕密行爲之對象是他人經特殊加密處理之資訊，而202條(2)項則將資訊定義爲電子、磁性或其他無法以感官直接辨識所儲存或傳送者。這似乎是一較佳之立法處理方式。

註六七：宜注意者，刑法第二十八章之妨害祕密罪，與電腦處理個人資料保護法第五章之刑罰，皆係告訴乃論。

註六八：參見前揭李文。

註六九：見註六三。

註七十：見註六。

註七一：司法研究年報第十八輯第十八篇：「電腦犯罪理論與實務問題研究」，73頁，司法院印行（民國86年）·

註七二：當然，施放病毒行爲不一定須要以連線access之方式爲之，亦可以散佈帶有病毒之磁碟片等其他方式爲之，故本條之毀損罪與連線犯罪不一定有交集。