臺灣嘉義地方法院檢察署

104 年度自行研究報告

# 網路犯罪之新趨勢與規範狀態之初探～從物聯網之發展談起

撰稿人員：檢察官陳靜慧

審查人員：檢察長羅榮乾

中華民國 104 年 12 月

# 摘要

在今日人類日常生活中扮演重要角色的電腦，大約係於西元1950年誕生，自此人們得以大量儲存資料、簡化運算；電腦的使用從早期的軍事用途、科學運算，發展至小單位之公司、個人之間，作為日常文書處理、美術繪編、商業管理等輔助工具，隨之於二十世紀末興起的網際網路更以極快速、極廣泛的姿態席捲人類世界，由職司犯罪偵查的角度切入，所謂「電腦犯罪」、「網路犯罪」往往具有散布快速、證據難以取得、證據易銷毀、身分隱密、跨國管轄等特性，而近代興起的「物聯網（Internet of Things)」，或有稱之為「萬物聯網（Internet of Everything)」，更是人類智慧在網路科技的一大進展，物聯網世界中的「資訊裝置型態(Devices with Information）與控制裝置型態(Devices have control over things)」走向多元化，伴隨而生的「資訊安全（Information Security）危害行為」與「奪取所有權及控制權行為（Ownership and Right of Control)」實已挑戰目前的法律規範體系。歐洲理事會各會員國所簽署的「網路犯罪公約」可謂係提供各國制訂關於電腦網路犯罪規範之參考基準，本研究擬就現行關於電腦網路相關犯罪之處罰規範出發，佐以網路犯罪公約之內容，再針對蓬勃發展的物聯網類型及其犯罪類型予以析述，希冀在不久的將來，面對物聯網世界應運而生的諸多法律挑戰，犯罪偵查之方向得以明確與穩健。

# 目次

# 第一章、 研究緣起

網際網路在現代生活中扮演著不可或缺的角色，網路科技之發展不斷推陳出新、日新月異，傳統之犯罪類型亦隨之趨於複雜化，以販毒案件為例，新興之通訊軟體(如：SKYPE、LINE、SLACK、微信等）早已取代電話通信或簡訊之聯絡方式，單純施以電信通訊監察絕無法竟其功[1]；而所謂網路犯罪，性質上為電腦犯罪[2]之一種，顧名思義，即是透過電腦網際網路之設備遂行犯罪行為；網路犯罪的類型隨著科技發展隨之複雜化、多樣化，由偵查犯罪角度言之，網際網路儼然已成為重要的犯罪管道，大量的犯罪資料隱身於浩瀚的網路世界中，就管轄權之界定而言，犯罪行為甚至可能跨越數個司法管轄區域之外，在面對網路形式的銀行詐欺、信用卡詐欺、盜取個人資料、網路（兒童）色情（影音檔）及其他方面相同或相似類型的電子化犯罪時，全球檢察官無不希望已具足相關知識、經驗，或已將自身能力提升到一定水準，得以應付這類新興犯罪型態的挑戰[3]；司法機關究應如何在這「數位溝通(digital communication)」成為常態趨勢的時代扮演

[1] 由販毒案件之實務判決觀察，透過通訊軟體 LINE 爲毒品交易聯繫工具已成常態，參見臺灣臺北地方法院 104 年度訴字第 72 號刑事判決、臺灣臺北地方法院 104 年度訴字第 178 號刑事判決、臺灣臺北地方法院 104 年度重訴字第 20 號刑事判決、臺灣士林地方法院 104 年度訴字第 256 號刑事判決、臺灣嘉義地方法院 104 年度訴字第 359 號刑事判決、臺灣嘉義地方法院 104 年度訴字第 392 號刑事判決、臺灣高雄地方法院 104 年度訴字第 237 號刑事判決等。

[2] 關於電腦犯罪之定義，持最廣義見解者認爲凡屬與電腦有關之犯罪均稱爲「電腦犯罪」，後述之歐洲理事會網路犯罪公約（The Council of Europe Convention on Cybercrime）可謂即係採取最廣義之見解。

[3] 參見　黃玉婷，<認識國際檢察官協會之全球檢察官電子犯罪防制網絡>，檢察新論第 13 期，2013 年 1 月，第 2 頁。

預防犯罪、打擊犯罪的角色？適時掌握網路科技的脈動、針對可能衍生的犯罪行為進行防杜與規制，實為今日法律人刻不容緩的課題！

關於電腦網路犯罪的偵查問題，涉及司法管轄權之界定[4]、證據之取得[5]等與一般傳統犯罪相較之下具特殊性之疑義，學說及實務上針對該等特殊性問題亦多討論；本研究旨在針對網際網路應用之新趨勢—物聯網—所可能衍生的法律問題及其規範方式進行探討。

析言之，隨著科技發展，網路實體系統(Cyber-Physical System, CPS, 即所謂「物聯網」，又可稱為 Internet of Things, 簡稱為 IoT)的趨勢同樣無可避免，而所謂「物聯網」係指實體物件的聯絡網絡可透過網際網路等技術交流溝通；目前已發展的物聯網型態包括：可穿戴裝置、智慧能源系統、無人機、醫聯網與聯網汽車等，隨著越來越多的產品與網路產生連結，利用安全性堪慮的無線網路來竊取資料或遠端操控裝置的網路犯罪風險亦隨之提高。換言之，物聯網並非提供人們分享資料、相互通訊之平台，而係使各種設備之間可以取得資料、彼此通訊，在此一願景下，人類仍可繼續使用

[4] 電腦網路犯罪之司法管轄，亦是爭議問題焦點之一。因電腦網路犯罪行爲地未必爲結果發生地，且因時間與空間上之隔閡，故其應以資訊發出端或接收端作爲司法管轄的劃分仍有爭議。另外，犯罪行爲人之電腦資訊設備之主機端若設立於國外，則我國於犯罪偵查時，就會產生極大的阻礙與困難。例如：犯罪行爲人將網路伺服器架設於國外，我國偵查之執行即有實質上之困難。參見王勁力，<電腦網路犯罪偵查之數位證據探究>，檢察新論第 13 期，2013 年 1 月，第 17 頁。

[5] 電腦網路犯罪之證據，多以電磁紀錄等數位資料之狀態存在，但電磁紀錄等數位資料極其容易遭到增修刪改、甚至滅失，對精通資訊科技的犯罪者於實施犯罪之後，即可輕易將相關數位資料與證據刪去修改等，必對電腦網路犯罪之偵查帶來嚴重之影響。參見王勁力，前揭文，第 17 頁。

現有的網際網路科技進行溝通交流，然此一網際網路科技的應用同樣發生在「物」上，或可稱之為 M2M（machine-to-machine ）通訊，當設備之間彼此連線時，首先會產生大量的資料，亦即該設備與周遭環境透過網際網路產生互動，依此所演變的科技革命將為人類生活帶來無窮的舒適與便利；然而，物聯網所帶來的好處可能伴隨諸多隱憂，大部分關於物聯網的潛在問題均涉及物聯網內各種智慧性設備所蒐集的資訊，該等資訊之安全性保障如何？個體隱私權的保護措施為何[6]？是否可能遭盜用於不法用途？若個人資料遭盜用於犯罪行為之實行，法律責任之歸屬應如何評價？

本研究擬由現行法律制度下關於電腦網路犯罪之規制狀態出發，並進一步針對「物聯網」之發展模式予以類型化，再針對可能的規制方式進行闡述，期以在層不出窮的網路犯罪事件中，提供初步的思考與建議。

[6] 許多人相信物聯網會是「大舉開放」的時代，每一筆交易、每一個動作、每一個人、每一件事物，都完全透明。有了這樣的透明，每一件設備之間互相連線時，你才能夠信任；你必須信任這些東西的運作，信任它們會爲你著想。也有些特別注重隱私的人，認爲物聯網業者不應當收集這些資料，即使是匿名的也不行。隱私倡議人士也希望一切透明，但它們想要智慧設備製造廠商能完全透明，告知所收集的資料爲何、用途爲何。消費者如果想拒絕這些資料外流，應當可以選擇關閉資料傳輸。關閉資料傳入物聯網也有個問題，這會讓智慧設備立刻變回智障設備。物聯網就是靠資料的流通，才獲得智慧；如果資料不動，你就只有一堆彼此獨立的感應器。參見<物聯網如何改變世界（The Internet of Things）>，Michael Miller 著/胡爲君譯，第 267 頁。

# 第二章、網路犯罪之定義與型態

## 第一節、網路犯罪之定義

關於網路犯罪的定義，在學說上有從不同角度切入而為相異之論述，或有謂行為人所違反故意或過失的犯罪行為中，具有網際網絡特性者，即屬電腦犯罪之延伸，換言之，此一型態乃電腦系統與通訊網路相結合之犯罪，惟在性質上較偏重於網際網路之應用[7]；另有論者認為，所謂「網路犯罪」係指利用網際網路之特性為犯罪手段或犯罪工具，性質上為網路濫用行為，其所稱「網際網路之特性」包括：大量傳播、即時性、匿名性等特性[8]；若以使用電腦資訊網路的觀點，論者亦曾將關於網路犯罪之型態區分為「阻害電腦網路機能系列之犯罪」及「非法使用電腦網路系列之犯罪」兩大類，所謂「阻害電腦網路機能系列之犯罪」係指由於故意、過失或事故等因素，損害電腦網路主機、端末裝置等電腦網路本身及其附帶設備，以及對輔助記憶體如光碟、硬碟或軟式磁碟所錄之資料或程式加以損害以阻害電腦網路機能之犯罪行為，其中關於網路硬體部分，係指以物理力對網路硬體設備之破壞，另就關於網路軟體機能方面之侵害，又可依犯罪行

[7] 網際網路之特性，包括分散性、開放性、互通性、隱密性、立即性等，參見林宜隆，＜網際網路與犯罪問題之研究＞，中央警察大學，2003 年 3 月，第 71 頁。

[8] 馮震宇，我國網路犯罪類型及案例探討，收錄於＜網路法基本問題研究（一）＞，學林，1997 年 7 月，第 337 頁。

為人違反之方式區分為「輸入操縱(input manipulation)」、「程式操縱(program manipulation)」與「輸出操縱(output manipulation)」等三種態樣，而所稱「非法使用電腦網路系列之犯罪」，則係指以企圖獲利或妨害業務為目的，故意窺視、塗損等惡作劇行為，進而無權或逾越權限使用電腦網路，或對網路系統輸入不實資料或程式，或消極地不輸入應輸入之資料等，其類型可大別為「周邊犯罪（peripheral crime)」、網路詐欺（internet fraud）與網路之非法使用等[9]。

## 第二節、我國現行法律規範狀態及實務運作

### 壹、刑法妨害電腦使用罪

關於電腦犯罪的法律規制狀態，我國刑法第 323 條原規定為：「電氣關於本章之罪，以動產論」；其後，於民國 86 年 10 月 8 日修正公布為：「電能、熱能及其他能量或電磁紀錄，關於本章之罪，以動產論」亦即將「電磁紀錄」增列為準動產[10]；嗣後，再於民國 92 年 6 月 25 日修正公布為：

[9] 林宜隆，＜網路使用的犯罪問題與防範對策之探討＞，收錄於《第三屆資訊管理學術暨警政資訊實務研討會論文集》，1998 年 5 月，第 21 頁至第 22 頁。

[10] 然而，該次修法同時增訂刑法第 339 條之 1「不正利用收費設備詐欺罪」、第 339 條之 2「不正利用自動付款設備詐欺罪」及第 339 條之 3「不正利用電腦詐欺罪」等三罪，讓原先第 343 條的準用各罪規定出現「失誤」，僅能準用於第 339 條之 3、第 340 條、第 341 條及第 342 條之罪，故於民國 88 年刑法修正時修正第 343 條爲:「第 323 條及第 324 條之規定,於前 7 條之罪準用之。」換言之，電磁紀錄視爲動產之規定，在普通詐欺罪、不正利用收費設備詐欺罪、不正利用自動付款設備詐欺罪、不正使用電腦詐欺罪、常業詐欺罪、準詐欺罪及背信罪皆得準用之。參見參見 廖宗聖、鄭心翰，<從網路犯罪公約談我國妨害電腦使用罪章的修訂>，科技法學評論，第 7 卷第 2 期，2010 年，第 69 頁。

「電氣、熱能及其他能量，關於本章之罪，以動產論」，本次修法時立法理由載明為:「本條係86年10月8 日修正時，為規範部分電腦犯罪，增列電磁紀錄以動產論之規定，使電磁紀錄亦成為竊盜罪之行為客體。惟學界及實務界向認為：刑法上所稱之竊盜，須符合破壞他人持有、建立自己持有之要件，而電磁紀錄具有可複製性，此與電能、熱能或其他能量經使用後即消耗殆盡之特性不同；且行為人於建立自己持有時，未必會同時破壞他人對該電磁紀錄之持有。因此將電磁紀錄竊盜納入竊盜罪章規範，與刑法傳統之竊盜罪構成要件有所扞格。為因應電磁紀錄之可複製性，並期使電腦及網路犯罪規範體系更為完整，爰將本條有關電磁紀錄部分修正刪除，將竊取電磁紀錄之行為改納入新增之妨害電腦使用罪章中規範。」民國92年新增刑法第36章妨害電腦使用罪章，其中刑法第359 條即明定：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處5 年以下有期徒刑、拘役或科或併科20萬元以下罰金」。該條之立法意旨載明為：「電腦已成為今日日常生活之重要工具，民眾對電腦之依賴性與日俱增，若電腦中之重要資訊遭到取得、刪除或變更，將導致電腦使用人之重大損害，鑒於世界先進國家立法例對於此種行為亦有處罰之規定，爰增訂本條 。」

學者有認為，「資訊」與「資料」為常使用之電腦術語，並被視為同義詞而交互運用，其實「資訊」（information ）

一詞在西方源於拉丁語"informatio"，指傳達思想之過程與內容；「資料」則係呈現資訊之材料，除有體物本身外，還包括有體物上之文字、圖畫或符號，凡是呈現資訊之素材，可被稱為資料。「電磁紀錄」本身僅係資料，用以呈現資訊，電磁紀錄之取得即係資訊之取得。舊刑法第 323 條電磁紀錄竊盜罪之侵害客體係電磁紀錄，所保護之法益其實係電磁紀錄上有財產價值之資訊，此乃因資訊具備無體性，並不適合作為行為客體。與此相關者，「營業秘密法」[11]所保護之營業秘密，其實即為「資訊」，此由營業秘密法第 2 條有關「營業秘密」之定義，即為：「方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊。」即可窺知[12]；如電磁紀錄上承載著受著作權或營業秘密法所保護之資訊，則未獲同意無權複製他人電磁紀錄之行為，即會侵害電磁紀錄所呈現出無體資訊之「資訊之專屬性或排他性使用」（the exclusive of information），此種財產上利益侵害即為舊刑法第 323 條電磁紀錄竊盜罪所要規範者[13]。惟大多數電磁紀錄之取得皆以檔案複製或線上資料傳送、下載之方式進行

[11] 我國於民國 85 年制訂營業秘密法，其立法目的在於保障營業秘密，維護產業倫理與競爭秩序，調和社會公共利益。（參見該法第 1 條規定）

[12] 營業秘密法第 2 條規定：「本法所稱營業秘密，係指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，而符合左列要件者：一、非一般涉及該類資訊之人所知者。

二、因其秘密性而具有實際或潛在之經濟價值者。三、所有人已採取合理之保密措施者。」

[13]參見　蔡蕙芳，電磁紀錄無權取得行爲之刑法規範，中正法學集刊第 13 期，第 109 頁至第 119 頁

，此種電磁紀錄複製行為並不符合傳統竊盜罪之「竊取」定義，因此有前述 92 年間刑法之修正。

析言之，立法者之所以在 86 年修正刑法第 323 條而增列「電磁紀錄」視為以動產論後，繼續於 92 年提出第 359 條（列為新增第 36 章妨害電腦使用罪章中條文之一），無非係因立法者認為並非所有應受刑法保護之資料皆具有財產價值，立法者對於電磁紀錄之保護，採取了不僅只是在保護財產之觀點，更著重於如電磁紀錄係未經同意而被無權取得時，由此導致刑法之保護法益可能遭致侵害之危險。而就法益保護之觀點而言，刑法第 359 條之保護法益，除「資訊與資料之私密性、完整性、可使用性」外，同時還包含「實害」，因如僅意在保護「資訊與資料之私密性、完整性、可使用性」，則凡未經授權而取得他人持有中之未公開電磁紀錄，即已侵害資料隱私權，構成要件上毋須以「致生損害」為必要，立法者在該條文中添加「致生損害於公眾或他人」之構成要件，顯有意藉此限制本條之適用範圍[14]，以符刑法謙抑之要求，防止過度之處罰[15]。觀諸舊電磁紀錄竊盜罪係財產犯罪，刑法第 359 條無故取得電磁紀錄罪則係關於資料安全之刑法規範，92 年刑法修正公布後，舊電磁紀錄竊盜罪與舊電磁紀錄侵占罪均無法再被適用，只能依刑法第 359 條無故取得電磁紀錄罪代替，學者有認為，如此立法政策是否妥適，非無

[14]參見　蔡蕙芳，前揭文，第 156 頁至第 158 頁

[15]參見　李茂生，刑法新修妨害電腦使用罪章芻議【上】，臺灣本土法學雜誌第 54 期，第 243 頁

疑義。刑法第 359 條無故取得電磁紀錄罪既以「致生損害」為要件，即係要求有事實上損害始克該當，應屬結果犯之規定，相對於「足以生損害」或「有受損害之虞」等危險犯之規定，係只要求有發生損害之危險為已足之情形，並不相同。在此意義下，僅只單純「得知」電磁紀錄之資訊內容，尚非屬本條所謂之「取得」，還須持有電磁紀錄之備份，並造成損害，方構成刑法第 359 條之「取得」行為；學說上有認為，該條所謂之「無故取得電磁紀錄」，係以無權侵入系統為前提，由此而接觸、刺探到未獲授權存取之電磁紀錄，並將電磁紀錄予以複製而言[16]；至於依行為人身分原有接觸或控制電磁紀錄之權限，只是違反公司資訊安全規範將該等資訊帶回家工作時，因行為人並無洩漏之動機或目的，即不宜機械性使用刑法第 359 條保護屬於民事訴訟範圍之營業秘密爭執，以免逸脫電腦或網路犯罪之立法原意[17]。

就資訊本身而言，營業秘密法所保護之「秘密」性質上亦屬「資訊」之一種，無論係 92 年刑法修正前之電磁紀錄竊盜罪，抑或修法後之刑法第 359 條無故取得電磁紀錄罪，此等規範之主要立法目的，均非意在為營業秘密提供保護，以處罰不正取得營業秘密之行為。由於現行營業秘密法未具有規定刑事處罰之條文，因此營業秘密之刑事保護，僅賴於

[16]參見　蔡蕙芳，前揭文，第 163-165 頁；林山田，刑法各罪論【上冊】，第 555 頁

[17]參見　張紹斌，刑法電腦專章及案例研究，軍法專刊第 54 卷第 4 期，第 89、90 頁

依據具體情況之不同，援引適當之刑法條文為之。而從前述刑法之修法過程與構成要件解析，亦顯示刑法之修正與變化，將會影響營業秘密之刑法保護範圍，此種無意識之連動關係，從刑事立法政策而言並非妥適，如欲建立完善之營業祕密保護法制，根本之道應採取類似著作權法之立法模式，以營業秘密法為基礎，針對營業秘密之性質，制定各種不同行為態樣之刑事處罰規定，方屬妥適[18]。

刑事立法保護法益之核心內涵之一在於犯罪類型之建構，而犯罪類型之建構，又以規範與處罰之行為態樣最屬重要。以營業秘密為例， 關於不法侵害營業秘密之行為，主要包括「取得」、「洩漏」與「使用」等三種。如再配合行為階段之發生順序與營業秘密取得之原因合法與否，則得組合為「合法取得營業秘密 後之不法洩漏」、「合法取得營業秘密後之不法使用」、「不法取得營業秘密」、「不法取得營業秘密後之不法洩漏」、「不法取得營業秘密後之不法使用」等各種行為態樣。在我國現行保護營業秘密之刑事立法現狀下，除「合法取得營業秘密後之不法洩漏」、「不法取得營業秘密」有明文處罰外，其餘各種行為態樣是否或有無適當之規範與處罰依據， 實仍有待立法補充[19]。據此，為處理前述營業祕密保護之刑事法制困境，我國曾先後提出各種相應法案，包括刑法部分條文修正草案（新增妨害農工商

[18]參見　蔡蕙芳，同前，第 181 至第 182 頁；陳彥嘉，同前，第 44 頁。

[19]安見　陳彥嘉，同前，第 66 頁。

罪之刑法第 255 條之 1 、第 255 條之 2 、修正妨害秘密罪章之刑法第 317 條及增訂第 317 條之 1 ）、公平交易法部分條文修正草案、科技保護法立法草案、敏感科學技術保護法立法草案及營業秘密法部分條文修正草案（增訂第 15 條之 1 、第 15 條之 2 ），終因各種因素而遲未能完成立法[20]。而作為我國民、刑事法規之主要法律被繼受國，並為營業秘密法立法時所參酌法制之一之德國，該國有關營業秘密保護之法律建制，係採取民、刑事立法同兼之方式，其中刑事立法係以「不正競爭防止法」（ 原名「不正競爭禁止法」，Gesetz gegen den unlaute ren Wettbewerb，簡稱 UWG ）內之規範為核心，並輔以刑法中之部分相關條文，共同築起有關營業秘密刑事立法保護之主要架構[21]。立法意旨係將營業秘密法定位為民法之特別法，該法所稱之「營業秘密」，並未等同於刑法保護之「工商秘密」，而刑法妨害電腦使用罪章原非以保護營業秘密為其規範意旨，致我國就營業秘密保護之刑事立法規範出現漏洞，刑法第 359 條無故取得電磁紀錄罪中所謂之「無故取得他人電腦之電磁紀錄」，係以無權侵入系統為前提，由此而接觸、刺探未獲授權存取之電磁紀錄，並將電磁紀錄予以複製而言。是以，論者有認為，基於憲法為保障人權意旨所肯認之罪刑法定原則，如行為人係合法取得他人營業秘密之電磁紀錄，其後加以不法使用或不

[20]參見　陳彥嘉，同前，第 113 至第 276 頁，關於各種有關刑事立法保護規範之比較與整理。
[21]參見　陳彥嘉，同前，第 278 頁。

法洩漏時，依其情節可能該當刑法第 317 （洩漏業務上知悉之工商秘密罪）、318 （洩漏公務上知悉之工商秘密罪）、318-1(洩漏電腦或相關設備秘密罪)、318-2(加重規定）、335(普通侵占罪）、336(公務公益及業務侵占罪）、342 條（背信罪）等條文之構成要件或民事侵權行為責任。

簡言之，刑法第 359 條之無故刪除他人電腦之電磁紀錄罪之成立， 須以無故刪除他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人為要件，且揆諸該條文立法理由可知，該條文所保障者乃「電腦使用人」，而非「電腦中檔案所有人」；又所謂「刪除」乃指使電磁紀錄完全消失或使部分消失致不能再現電磁紀錄之意義而言。再者，刑法所稱電磁紀錄者，謂以電子、 磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄，刑法第 10 條第 6 項定有明文；依此，刑法第 359 條之無故取得他人電磁紀錄罪主要是係為了因應電磁紀錄具有「可複製性」之特性而訂定，則在行為人取得電磁紀錄（即複製電磁紀錄）前後，因未必會同時破壞他人對該電磁紀錄之持有，則對被害人的整體財產總額並無影響，此與一般財產犯罪之態樣不同；而行為人取得電磁紀錄後，若只是單純的持有，也不會減少被害人的整體財產總額，而真正會使被害人整體財產總額產生影響者，應係行為人的後續的其他利用行為。是以，若認為所謂之「損害」係被害人整體財產之減少，亦即指減少被害人現有之利益，或喪失將來可得之利益，則真正致使此一「損害」者，當係

行為人其他後續利用行為，而非「取得電磁紀錄」之行為，則亦不符合無故取得電磁紀錄「致生」損害之要件（因為行為人取得電磁紀錄後，不一定會有後續利用行為，故取得電磁紀錄與後續利用行為間，並無因果關係，則取得電磁紀錄與「損害」間亦無因果關係；至於後續利用行為，亦可能另構成犯罪）。故若認「損害」係指被害人整體財產總額之減少，則刑法第 359 條之無故取得電磁紀錄罪將少有構成的可能（亦即僅有取得電磁紀錄時同時破壞了被害人對於該電磁紀錄之持有時才會構成），此殊非立法之原意。另依上開立法源由，亦可知立法者係希望以「無故取得」來取代「竊取」之概念，是以無故取得電磁紀錄罪所侵害財產利益之內容，乃是特定財產之所有權或持有權，故性質上屬於「侵害個別財產利益之犯罪」，學理上即認為此種犯罪被害人的整體財產是否減少並非重點。與此相較，刑法第 342 條背信罪，則屬於「侵害整體財產利益之犯罪」，故須以被害人整體財產價值產生減損為要件。刑法第 359 條之無故取得他人電磁紀錄罪既與刑法第 342 條之背信罪，在性質上完全不同，兩者之所謂「致生損害」自然亦不得為相同之解釋。論其實際，刑法 359 條乃是將之無故「取得」、「刪除」、「變更」電磁紀錄 3 種犯罪態樣併列，且此 3 種犯罪態樣均以「致生損害於公眾或他人」為要件，此 3 種犯罪態樣之「致生損害於公眾或他人」要件，自應為相同之解釋。而就無故「刪除」電磁紀錄而言，行為人一有「刪除」之行為，即已造成被害

人被害人整體財產價值之減少，亦即造成「損害」，則「致生損害於公眾或他人」的要件，豈不是贅文？承上所述，法院實務判決有認為「致生損害於公眾或他人」乃係立法者為了達到立法謙抑之要求所設的要件，亦即行為人不僅有「刪除」電磁紀錄之行為，而且尚須該電磁紀錄對於公眾或他人有相當之財產價值或祕密性，在法律評價上可以認為行為人的刪除行為係「造成損害」時，才構成犯罪，以避免刑罰範圍過於擴張[22]；此外，立法者既已認識到電磁紀錄之可複製性[23]，並肯認「無故取得」電磁紀錄之行為具有可罰性，將之與「刪除」、「變更」併列，自然係將之為相同評價，則在無故「取得」電磁紀錄之態樣，自然不能因為他人對該電磁紀錄之持有並無影響即認為「損害」並未發生，而也應認為該電磁紀錄對於公眾或他人有相當之財產價值或祕密性時，在法律評價上即可以認為行為人的「取得行為」係「造

[22] 參見最高法院 104 年度訴字第 2335 號刑事判決：「…刑法第 359 條所規定「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人」罪，屬於結果犯，必須該行為已致生損害於公眾或他人之結果，始構成本罪。否則，縱有無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄行為，倘未致生損害於公眾或他人之結果，因該罪無處罰未遂犯之明文，自不成立該罪。換言之，刑法第 359 條之罪，以「致生損害」於公眾或他人為構成要件，屬於結果犯，此與僅以「足以生損害」於公眾或他人為構成要件之罪，例如刑法第 210 條之偽造私文書罪，以有足生損害於公眾或他人之危險，即行成立，迥然不同。…」

[23] 參見最高法院 104 年度台上字第 5295 號刑事判決：「…依刑法第 323 條修正理由說明，因電磁紀錄具有可複製性，與其他電能、熱能經使用後即消耗殆盡之特性不同，行為人於建立自己持有時，未必會同時破壞他人對該電磁紀錄之持有，對被害人整體財產總額並無影響，與竊盜罪構成要件有所扞格，改納入刑法妨害電腦使用罪章。依此，如果以侵害財產法益之觀點解釋刑法第 359 條不法取得電磁紀錄罪，將無故限縮其適用範圍，且違反該章保護電腦使用者免受侵害之本質不符…」

成損害」[24]；此為法院實務判決向來對於刑法第 359 條取得、刪除、變更電磁紀錄罪之見解。

然而，隨著對於資訊安全的重視日益提高，近期法院實務見解則認為妨害電腦使用罪之保護法益係在於維持電子化財產秩序，故並不以實際上對公眾或他人造成經濟上之損害為限。只要電腦中重要資訊發生得喪變更，已足導致電腦使用人發生嚴重損害，即足該當[25]，且就該條所稱「刪除」而言，最高法院 104 年度台上字第 3392 號判決甚至明確指出：「刑法第 359 條之破壞電磁紀錄罪，係指行為人無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人。所稱『刪除』，固係指反於電磁紀錄製成之方法，將電磁紀錄完全或部分消除之謂，惟是否必使之永久消除而無法回復，始得謂為『刪除』，在學理上非無爭議；然就該『刪除』係刑事法上之『構成要件』觀之，自應基於當代共通之學理，或本乎相關之法規，而為合乎立法本旨之闡釋。查 92 年 6 月 25 日修正公布新增刑法妨害電腦使用罪章所定之罪，其保護法益兼及個人及社會安全法益，並非僅

[24] 參見臺灣臺北地方法院 94 年度訴字第 1561 號刑事判決。

[25] 臺灣高等法院 104 年度上訴字第 1094 號刑事判決：「按「無故取得、刪除或變更他人電腦或其他相關設備之電 磁紀錄，致生損害於公眾或他人者」，構成刑法第 359 條之罪。而電腦已成爲今日日常生活之重要工具，民眾對電腦之依賴性與日俱增，若電腦中之重要資訊遭到取得、刪除或變更，將導致電腦使用人之重大損害（參照該條之立法理由），足認本條犯罪之成立雖以對公眾或他人產生具體之損害爲必要，然本項法益既係在於維持電子化財產秩序，故並不以實際上對公眾或他人造成經濟上之損害爲限。只要電腦中重要資訊發生得喪變更，已足導致電腦使用人發生嚴重損害，即足該當。被告 000 未經告訴人同意，擅自將告訴人網站上之文章等電磁紀錄刪除，造成告訴人須另花費時間、人力 始能將其網頁重建，並造成告訴人上開網頁文章之電磁紀錄之喪失，足認被告 000 上開行爲業已造成告訴人之損害甚明。」

止於個人法益（參行政院會同司法院送立法院審議之原修正草案修正說明）；而刑法第 359 條規定之立法意旨，無非認「電腦已成為今日日常生活之重要工具，民眾對電腦之依賴性與日俱增，若電腦中之重要資訊遭到取得、刪除或變更，將導致電腦使用人之重大損害，鑒於世界先進國家立法例對於此種行為亦有處罰之規定，爰增訂本條。」（參立法理由），顯見本罪之立法係鑒於電腦之使用，已逐漸取代傳統之生活方式，而所有電腦資料皆係經由電磁紀錄之方式呈現，電磁紀錄有足以表徵一定事項之作用（諸如身分或財產紀錄），則對電磁紀錄之侵害，亦可能同時造成身分或財產上之侵害關係，嚴重影響網路電腦使用之社會信賴及民眾之日常生活。參諸對電腦及網路之侵害行為採刑事處罰已是世界立法之趨勢，乃增訂該罪，對行為人科以刑事罰。故而本罪規範應係重在維持網路電腦使用之社會安全秩序，並避免對公眾或他人產生具體之損害。不論行為人所使用之破壞方式為何，祇要無故刪除他人電腦或其相關設備之電磁紀錄，即該當於刪除之構成要件。復因電磁紀錄本身具有可複製性，又不具有損耗性，縱被複製亦不致因此而消失，而依現行之科技設備，若要回復被刪除之電磁紀錄，亦非難事，故解釋上，應認電磁紀錄遭受無故刪除時，即已產生網路電腦使用之社會安全秩序遭受破壞之危險，至於該電磁紀錄事後得否回復，均無礙於『刪除』之成立。倘其刪除行為，又已致生損害於公眾或他人，本罪即已該當。否則，行為人於刪除電磁紀錄

時，祇須先保留備份之電磁紀錄，俟東窗事發後再行提出，或事發後要求將電腦或其相關設備送由專門機構依現行之科技設備予以回復，即不構成刪除電磁紀錄之罪，則本罪之規範目的豈不落空。是本罪所稱『刪除』，顯不以使電磁紀錄永久消除而無法回復為必要。」

實務上亦具相當重要性之刑法妨害電腦使用罪章條文，當屬刑法第358條之無故侵入電腦或相關設備罪。刑法第358條規定：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」由此規範內容可知，關於無故侵入電腦或相關設備之行為態樣分為兩個層次，其一為透過無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞等方式（第一層次之行為），其二為入侵他人電腦或其相關設備（第二層次之行為）[26]，當行為人以「無故輸入他人帳號密碼」、「破解使用電腦之保護措施」或「利用電腦系統之漏洞」[27]入侵他人電腦或其相關設備，即屬違反無故入侵電腦或相關設備罪。

---

[26] 依立法理由之說明，無故侵入他人電腦之行爲以刑罰相繩已是世界立法之趨勢，且電腦系統遭惡意入侵後，系統管理者必須耗費大量時間與人力進行檢查、修復，才能確保電腦系統的安全性，因此，此種行爲之危害性已經達到科以刑事責任之程度，爲保護電腦系統之安全性，特增訂無故入侵電腦或相關設備罪。參見 廖宗聖、鄭心翰，前揭文，第72頁。

[27] 論者有認爲，基本上僅有「無故輸入他人帳號密碼」之構成要件可被實務界加以使用，其他兩個行爲態樣之規定並無太大之用處，只要「無故輸入他人帳號密碼」之構成要件該當即可解決電腦犯罪一半以上的問題。參見　張紹斌，<刑法電腦專章及案例研究>，軍法專刊，第54卷第4期，第88頁。

另外，鑑於電腦及網路已成為人類生活之重要工具，分散式阻斷攻擊（DDOS）或封包洪流（Ping Flood）等行為已成為駭客最常用之癱瘓網路攻擊手法，故於 92 年修法新增訂刑法第 360 條關於干擾電腦或相關設備罪：「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金」依該條立法理由之說明，本條之規範目的旨在以刑法保護電腦及網路設備之正常運作，且其處罰之對象乃對電腦及網路設備產生重大影響之故意干擾行為，為避免某些對電腦系統僅產生極輕度影響之測試或運用行為亦被繩以本罪，故加上「致生損害於公眾或他人」之要件，以免刑罰範圍過於擴張[28]。再者，有鑑於電腦病毒、木馬程式、電腦蠕蟲程式等惡意之電腦程式，對電腦系統安全性危害甚鉅，往往造成重大之財產損失，致生損害於公眾或他人[29]，故亦於 92 年修法增訂刑法第 362 條關於製作專供犯本章之罪之電腦程式罪[30]。

由前揭說明可知，我國刑法關於妨害電腦使用罪之行為態樣包括有：無故侵入電腦或相關設備（刑法第 358 條）、無故取得、刪除變更電磁紀錄（刑法第 359 條）、干擾電腦

[28] 刑法第 360 條規定之增訂理由參照。

[29] 1999 年 4 月 26 日發作之 CIH 病毒造成全球約有六千萬台電腦當機，鉅額損失難以估計，即爲著名案例。參見刑法第 362 條增訂理由。

[30] 刑法第 362 條規定：「製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」

或相關設備（刑法第 360 條）、製作專供犯電腦犯罪之電腦程式罪（刑法第 362 條），其中除刑法第 358 條外，其餘犯罪類型均明訂須以「致生損害於公眾或他人」為要件，在立法方式上採取實害犯而非危險犯之模式。

**貳、個人資料保護法**

就立法沿革而言，為保護人民之資訊自決權益，使個人人格權得到完善之防護，不需時時處於恐懼其個人資料遭竊之狀態，在我國法制上有針對個人人格完整性制訂專法規定，此即「個人資料保護法」前身「電腦處理個人資料保護法」，針對過度侵害人格權之行為施以刑事制裁，而「電腦處理個人資料保護法」之立法目的雖在於保障人格權、促進個人資料之合理利用，然其保護客體僅限於經電腦處理之個人資料，若未經電腦處理之個人資料，即不屬該法所保障之範疇；基此立法疏漏，而有「個人資料保護法」之修法[31]。

個人資料保護法第 1 條即開宗明義規定：「為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。」，針對本條於（舊法之電腦處理個人資料保護法）84 年 7 月 12 日制定時，即於其立法理由內宣示：「電腦科技進步迅速， 使電腦能大量、快速處理各類資料，且運用日趨普及，因而對國民經濟之提

[31] 「電腦處理個人資料保護法」係於民國 101 年 9 月 21 日修法，更名爲「個人資料保護法」。

昇有重大貢獻。惟個人資料因濫用電腦而侵害當事人權益之情形日漸嚴重，亦引起民主先進國家之關切。故經濟合作暨發展組織（OECD）於 1980 年 9 月通過管理保護個人隱私及跨國界流通個人資料之指導綱領，歐洲理事會亦於 1981 年完成保護個人資料自動化處理公約，並提出 8 項原則以供遵守。迄今已有瑞典、美國、紐西蘭、德國、法國、丹麥、挪威、奧地利、盧森堡、冰島、加拿大、英國、芬蘭、愛爾蘭、澳洲、日本、荷蘭等 17 國制定相關法律以保護個人資料」。因此，就上揭法條及其立法理由相互參照之下，本法就個人資料保護之目的，乃是避免因濫用當事人之資訊而侵害其權益，故凡是針對個人資料之蒐集、處理及利用，必須在合理使用之範圍內始得為之，以避免造成個人人格權受到侵害；反面言之，若資訊之內容不足以造成個人人格權之侵害，甚至根本無法辨識、特定究係何人之資訊，自不在本法保護之範圍內。蓋以資訊之本身，若根本無法確定究係何一對象，自不會有個人人格權被侵害之問題[32]。

按維護人性尊嚴與尊重人格自由發展，乃自由民主憲政秩序之核心價值，隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第 22 條所保障，其中就個人自主控制個人資料之資訊隱私權而言，乃保障人

[32] 參見台灣高等法院 104 年度上訴字第 1393 號刑事判決。

民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權（司法院大法官釋字第 585 號解釋理由、第 603 號解釋文參照）。是前揭釋字第 585 號解釋揭諸隱私權為受憲法第 22 條所保障之非列舉基本權之一，釋字第 603 號解釋文除指出隱私權為受憲法第 22 條所保障之非列舉基本權之一，且更進一步將隱私權擴展至人民得自主決定其個人資料之「資訊自主權」。而所謂隱私權，乃係基於人格尊嚴、個人之主體性及人格發展所必要，屬民法第 195 條規定所明定之人格權之一種，旨在保障個人在其私領域的自主，即個人得自主決定其私生活的形成，不受他人侵擾，及對個人資料自主控制，是隱私權侵害類型可分為：（1 ）私生活的侵入、（2 ）私事的公開、（3 ）資訊自主的侵害。隱私權之概念，逐漸演進至當前具有積極性之資訊隱私權，即「免於資料不當公開之自由」或「對自己之資料之蒐集、輸入、累積、流通、使用，有完全決定及控制之權利」[33]。

其次，就個人資料保護法之重要規範內涵論之，個人資料保護法第 6 第 1 項規定：「有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：一、法律明文規定。二、公務機關執行法定職務或非公務機關履行法定義務所必要，且

[33] 參見許文義著，個人資料保護法論，第 53 頁至第 54 頁。

有適當安全維護措施。三、當事人自行公開或其他已合法公開之個人資料。四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序所為蒐集、處理或利用之個人資料。」另關於非公務機關對於個人資料蒐集或處理之規範，依個人資料保護法第19條第1項規定：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、法律明文規定。二、與當事人有契約或類似契約之關係。三、當事人自行公開或其他已合法公開之個人資料。四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。五、經當事人書面同意。六、與公共利益有關。七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。」另依個人資料保護法第20條第1項規定：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為增進公共利益。三、為免除當事人之生命、身體、自由或財產上之危險。四、為防止他人權益之重大危害。五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。六、經當事人書面同意。」

個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯；非公務機關對個人資料之利用，除第 6 條第 1 項所規定資料外，應於蒐集之特定目的必要範圍內為之，個人資料保護法第 5 條、第 20 條第 1 項本文分別定有明文。而個人資料保護法第 5 條、第 20 條所稱之特定目的「必要」範圍，其內涵實即指比例性原則。依憲法第 23 條「憲法所列舉之自由權利，除為防止妨害他人自由、避免緊急危難、維持社會秩序或增進公共利益所必要者外，不得以法律限制之」之規定，此原則之衍生權，包括：合適性原則、必要性原則及狹義比例原則（即過量禁止原則）…合適性原則，乃指被告行使之手段須可達其目的；必要性原則，指在所有可能達成目的之方法中，被告應選擇對告訴人最小侵害之手段，即最小侵害原則；禁止過量原則，係指被告所欲完成之目的及使用手段，不能與因此造成之損害或負擔不成比例。又按非公務機關對個人資料之利用，除第 6 條第 1 項所規定資料外，應於蒐集之特定目的必要範圍內為之，但為防止他人權益之重大危害，得為特定目的外之利用，個人資料保護法第 20 條第 1 項但書第 4 款固有明文；惟揆諸舉重明輕之法理，縱係符合此款規定之「特定目的外之利用」，亦應受前開第 5 條揭諸之「誠實信用原則」、「正當合理關聯原則」（即須與「所要防止重大危害之權益保護」有正當合理關聯），以及第 20 條第 1 項本文規定之

「必要」範圍之內涵即比例原則之規範，始符法體系解釋之意旨[34]。法院實務判決亦指出，個人資料保護法第 2 條第 1 款規定，所稱個人資料係指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。又個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯，個人資料保護法第 5 條定有明文。再依同法第 20 條第 1 項前段之規定，因故取得他人個人資料者，原則上僅得於蒐集之特定目的必要範圍內，就該個人資料加以利用[35]。

針對違反個人資料保護法之主要刑責，規定於該法第 41 條：「違反第 6 條第 1 項、第 15 條、第 16 條、第 19 條、第 20 條第 1 項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金。

---

[34] 參見臺灣臺北地方法院 104 年度易字第 106 號刑事判決。

[35] 參見臺灣臺北地方法院 104 年度易字第 325 號刑事判決：「…觀諸上開個人基本資料查詢結果、戶役政連結作業系統資料，乃法院為特定當事人之身分、審理 案件所需，被告自其與告訴人之訴訟案件閱卷取得上開資料，自僅得於蒐集之特定目的必要範圍內，就該個人資料加以利用，而不得逾越特定目的之必要範圍，詎被告竟仍逾蒐集目的必要範圍，率爾將上開載有告訴人個人資料之文書張貼於該大廈之公布欄使不特定多數人得以見聞，且告訴人之個人資料實與社區公共利益無關，不得無故公然揭露之，此依被告之學經歷，自無不知之理，是被告此舉自屬濫用個人資料，且顯足生損害於告訴人之隱私權。是被告就上開個人基本資料查詢結果、戶役政連結作業系統資料之利用行為，已逾蒐集該個人資料特定目的之必要範圍，而足生損害於告訴人，其違反個人資料保護法第 20 條第 1 項之規定，而犯同法第 41 條第 1 項之罪，至為明確。」

意圖營利犯前項之罪者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。」其處罰要件須以「足生損害於他人」為前提[36]，且若行為人係基於營利意圖而違反個人資料保護法相關規定者，即須加重處罰，此即我國目前關於個人資料保護之法律規制狀態。

## 第三節、網路犯罪公約（Cyber-crime Convention）概述

國際間關於網路犯罪之法律規制，即屬 2001 年 11 月由歐洲理事會[37]的 26 個歐盟成員國以及美國、加拿大、日本和南非等 30 個國家的政府官員在布達佩斯所共同簽署的國際公約--《**網路犯罪公約**》（Cyber-crime Convention）；事實上，經濟合作暨發展組織（Organization for Economic Co-operation and Development ,OECD）自 1983 年起即著手進行關於網路犯罪之立法研究，對各國網路犯罪之立法進行分析比較，同時評估提出國際統一立法之可能性，於 1986 年發表了「電腦有關犯罪：法律政策分析」之報告[38]，其主

[36] 相較於電腦處理個人資料保護法刑事責任規範皆以「致生損害於他人」之實害犯形式加以制訂，現行個人資料保護法的刑事責任要件則皆盡改爲「具體危險犯」的規範類型，即無庸實際上損害的發生，僅需「足生損害於他人」，即得以本條相繩，而依法院向來之實務見解「所謂足生損害，固不以實已發生損害爲必要，然亦必須有足以生損害之虞者，始足當之」…由此可知個人資料保護法對於法益保護之程度顯然更爲提高。參見葉奇鑫、李明臻，<打擊網路犯罪新紀元：個人資料保護法施行下檢察實務的衝擊與挑戰>，檢察新論第 13 期，2013 年 1 月，第 70 頁。

[37] 歐洲理事會與「歐盟理事會（European Council）」不同，歐洲理事會係於 1949 年 5 月 5 日由十個歐洲國家在法國 Strasbourg 設立，成員國多爲歐洲國家，其主要成立宗旨在於宣揚人權、民主與法制等基本價值。

[38] Miriam F. Miquelon-Weismann, *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process？*,23 J. MARSHALL J. COMPUTER & INFO. L. 329,332（2005）

要內容在於針對各國共通之網路犯罪類型(如：詐欺、偽造、修改電腦程式或資料、未經授權進入電腦、侵害著作權、竊取營業秘密等)均應施以刑事制裁;其後,歐洲理事會於 1989 年發表 No. R.(89)9 電腦犯罪相關建議[39]，繼於 1996 年設立研究網路犯罪之專家委員會、於 1997 年 4 月設立「網路空間犯罪專家委員會（Committee of Experts on Crime in Cyber-space, PC-CY），負責研擬網路犯罪公約，並於 2000 年 12 月 31 日完成初稿，稱為「歐洲理事會網路犯罪公約草案」經歐洲理事會通過後，「網路犯罪公約」成為全世界第一部針對網路犯罪行為所制訂的國際公約。而「網路犯罪公約」制定的目標之一，旨在期望使國際間對於網路犯罪的立法有一致共同的參考標準，同時希望國際間在進行網路犯罪偵查時有一個國際公約可供遵循、支持，而得以有效進行國際合作。

網路犯罪公約除序言外，本文分為四章，共計 48 個條文。序言內容說明《網路犯罪公約》的功能、目標[40]；其次，

[39] Recommendation No. R.(89)9 of the Committee of Ministers to Member States on Computer-related Crime.

[40] 網路犯罪公約的前言旨在闡述該公約之宗旨，包括以下 8 點：(1) 網路犯罪公約之會員國均須慮及歐洲理事會之目標在於達成會國國間之一致和諧;(2)網路犯罪公約之會員國均承認與該公約非歐洲理事會會員國合作之價值;(3)網路犯罪公約會員國均認可追求打擊網路犯罪、保護社會共通犯罪政策之要求，尤指透過適當立法與國際合作之進行;(4)網路犯罪公約會員國均意識到電腦網路數位化、匯流化與全球化之深遠影響;(5)網路犯罪公約會員國均關注電腦網路與電子資訊可能被利用於犯罪之風險,同時關於該等犯罪之證據可能會被儲存或傳輸於電腦網絡當中;(6)網路犯罪公約之會員國認可會員國與私人企業合作共同打擊網路犯罪之必要性，以及保護使用、發展資訊科技之正當利益需求性;(7)網路犯罪公約會員國均相信有效打擊網路犯罪將有賴持續增加、快速及運作良好之國際合作模式;(8)網路犯罪公約會員國均確認該公約旨在制止破壞、濫用電腦系統、網際網路，以及資料之保密性、完整性與可使用性之必要，該制止係藉由將侵入行爲予以犯罪化，同時加強國內外偵查、起訴之權限，期以有效打擊網路犯罪，進而提供快速、可靠的國際合作協議供遵循。參見 Cybercrime Convention, *supra* note 1, pmbl ; *See also* Jay Fisher, *The Draft Convention on Cybercrime: Potential Constitutional Conflicts*, 32 UWLAL. REV. 339, 343-44(2001)

該公約第一章為定義性規範，說明術語之使用內容，亦即對網路犯罪涉及的術語進行名詞定義，包括有電腦系統（computer system）、電腦資料（computer data）、服務提供者(service provider)與電信資料（traffic data）等；該公約第二章為關於國家層面的措施，包括：刑事實體法、刑事程序法和管轄權三個部分，其目為要求各簽約國於各國國內應採取的措施，且在程序法部分則規定有關電子證據調查的特殊程序法制度，值得注意者為，在規範非法擷取（Illegal access）的行為方面，《網路犯罪公約》要求各國應立法明定非法擷取為犯罪行為並應予處罰；第三章為國際合作章節，包括一般原則和特殊規定兩個部分，在一般原則中包含規範引渡及相互合作等相關問題，而特殊規定則係有關電腦證據取得的問題，其規定簽約國應建立一周七天且一天二十四小時皆能聯絡合作機制的網路，各國也要對於相關人員加強訓練，並配給必要的裝備以配合各國合作事項的進行；第四章為「最後條款」，主要規定《網路犯罪公約》的簽署、生效、加入、區域應用、公約的效力、聲明、聯邦條款、保留、保留的法律地位和撤回、修訂、爭端處理、締約方大會、公約的退出和通告等事項。

網路犯罪公約在第二章國內必須採取的措施當中，又細分為第一節「刑事實體法」、第二節「刑事程序法」與第三節「管轄」；根據第二章第一節之規定，網路犯罪之類型可

區分如下[41]：1、侵害電腦資料和系統保密性、完整性與可利用性之犯罪（第 2 條至第 6 條）：第 2 條為「非法進入罪（Illegal Access）」，第三條為非法截取罪（Illegal Interception)[42]、第 4 條為「資料干擾(Data Interference）罪」[43]、第 5 條為「系統干擾（System Interference）罪」[44]、第 6 條為「設備濫用（Misuse of devices）罪」[45]。2、電腦相關犯罪（第 7 條及第 8 條）：第 7 條為「電腦相關偽造罪（Computer-related Forgery）」[46]、第 8 條為「電腦相關詐欺（Computer-related fraud）罪」[47]。3、內容相關犯罪（第 9 條）：第 9 條為兒童色情犯罪（Offences related to child pornography）[48]。4、侵犯著作權及相關權利之犯

[41] 參見 廖宗聖、鄭心翰，前揭文，第 65 頁。

[42]此類行為包括非法截取電腦傳送的「非公開性質」電腦資料，此項規定是用以保障電腦資料的機密性。根據歐洲理事會說明，如果電腦資料在傳送時，沒有意圖將資訊公開時，即使電腦資料是利用公眾網路進行傳送，也屬於「非公開性質」的資料。(參照《網路犯罪公約》第三條)

[43]包含任何故意毀損、刪除、破壞、修改或隱藏電腦資料的行為，此項規定乃是為了確保電腦資料的真確性和電腦程式的可用性。

[44]此一規定與第四條的「資料干擾」不同，關於系統干擾之規範乃是針對妨礙電腦系統合法使用的行為。根據歐洲理事會的說明，任何電腦資料的傳送，只要其傳送方法足以對他人電腦系統構成「重大不良影響」時，將會被視為「嚴重妨礙」電腦系統合法使用。在此原則下，利用電腦系統傳送電腦病毒、蠕蟲[44]、特洛伊木馬程式或濫發垃圾電子郵件，都符合「嚴重妨礙」電腦系統，即構成「系統干擾」的行為。

[45]所稱「設備濫用」包括生產、銷售、發行或以任何方式提供任何從事上述各項網路犯罪的設備。由於進行上述網路犯罪，最簡便的方式即是使用駭客工具，因此間接催生了該等工具的製作與買賣，在立法上即有需要嚴格懲罰這些工具的製作與買賣，由根本面杜絕該等網路犯罪行為。

[46]所稱「偽造電腦資料」包括任何虛偽資料的輸入、更改、刪改、隱藏電腦資料，導致相關資料喪失真確性。目前依照歐洲理事會各成員國法律，偽造文件都是犯罪行為，需要接受刑事制裁，故此規定只是將無實體存在的電腦資料也納入「偽造文書」的文書範圍。

[47]所稱「電腦詐騙」包括任何有詐騙意圖的資料輸入、更改、刪除或隱藏任何電腦資料，或干擾電腦系統的正常運作，為個人謀取不法利益而導致他人財產損失，均屬需以刑事處罰的犯罪行為。

[48]所稱「兒童色情犯罪」包括一切在電腦系統生產、提供、發行或傳送、取得及持有兒童的色情資料，此項規定是泛指任何利用電腦系統進行的上述兒童色情犯罪行為。

罪（第 10 條）：第 10 條即指侵犯著作權及相關權利的行為（Offences related to infringements of copyright and related rights），包括數條保障智慧財產權的國際公約列為侵犯著作權的行為，「網路犯罪公約」規定這些行為必須為故意、大規模進行，並使用電腦系統所達成的。

另就程序部分而言，根據網路犯罪公約第二章第二節規定，打擊網路犯罪之偵查程序區分為[49]：1、偵查權限及人權保障共同條款（第 14 條及第 15 條）、迅速保存已儲存的電腦資料及迅速保存和部分揭露傳輸之資料（第 16 條及第 17 條）；3、電腦資料提供命令（第 18 條）；4、搜索及扣押已儲存之電腦資料（第 19 條）；5、即時傳輸資料的蒐集和內容資料之截取（第 20 條及第 21 條）。

在國際法上，《網路犯罪公約》為世界上第一個打擊網路犯罪的國際公約，對世界多數國家的相應立法產生重要影響，遵循《網路犯罪公約》有助於建立更廣泛的共同打擊網路犯罪的國際司法合作，對打擊跨國網路犯罪具有相當程度之重要作用。

[49] 參見參見 廖宗聖、鄭心翰，前揭文，第 65 頁。

# 第三章、物聯網之發展與規制狀態

## 第一節、物聯網之意義

何謂「物聯網（Internet of Things, IoT）」？現今的網際網路是由機器組合而成的網絡，所有連上網路的機器均以滿足人類使用者的需求為目的，與此不同，物聯網的目的並非在人與人之間建立起聯繫網絡（Internet of People），而係將「物」與「物」彼此連結，（更進一步言之，物聯網所稱之「物」包括無生命之物與有生命之個體，例如利用穿戴設備追蹤人體的健康狀況或位置訊息即屬適例）；物聯網所連線的設備結合成網絡後，將產生大量的資料訊息，透過網際網路應用下的傳輸設備，使其他設備得以進行自動化之行動，易言之，「物聯網」此一概念之理念即在於透過相互連線的智慧化設備、裝置，在人類生活中創造更高度自動化、智慧化的生活品質，而就連上物聯網的設備本身言之，通常稱之為「智慧化設備」，（諸如坊間常見的智慧電冰箱、智慧電視機、智慧洗衣機等，族繁不及備載），論其實際，該等設備本身並無特殊性，然透過與其他設備連線互動，即可能產生具有智慧性的生活品質[50]。

[50] 以汽車爲例，若汽車發生故障，目前的技術可使汽車感應器發現故障狀態，啓動「檢查引擎」之燈號，此爲感應器技術之簡單應用；在未來的物聯網，會有更多感應器，與其他設備以更智慧化的方式相互通訊，以後再也不是只有一個感應器連到「檢查引擎」燈號，新的智慧汽車會具備多組感應器，大部分都內建於各種汽車零件，當一個感應器發現某項零件即將故障，以前只是亮起檢查引擎燈號，現在感應器會告知車上的控制器或「大腦」。控制器會找到故障零件，然後當汽車能連上網際網路（通常是開到你家裡的 Wi-Fi 網路範圍內）時，自動送出訊息給你熟識的汽車保養廠，保養廠內的電腦會檢查關於故障零件的資訊，判斷需要做哪些維修、訂購更換零件（如果沒有庫存），並聯繫你的手機上的行事曆軟體，預約更換零件的時間。再也不用忍受不知所云的警告燈號，不用擔心在路邊拋錨，也不需要自己去預約，所有必須零件都會與其他必須零件通訊，讓你的汽車儘快恢復到正常狀態，儘量不需要讓你操心。參見　Michael Miller 著/胡爲君譯，前揭書，第 9 至 10 頁。

科技發展的腳步永遠走在法律規制的前頭，立法機關往往必須實際面對現實上的法律問題，才能進一步針對可能產生的違法狀態進行規範，輕者處以行政裁罰，涉及法益侵害程度嚴重者則施以刑事刑罰之制裁。以 Google 所研發的自動駕駛汽車為例，內部有各種感應器與技術可以偵測汽車周遭狀態，包括立體攝影機、360 度攝影機、雷達與聲納等設備，該等設備具有各自相異的作用距離與視野角度，在駕駛過程中扮演不同的角色、分擔不同的責任，此種無人駕駛汽車的科技在理論上有諸多優勢，如：可以透過意外迴避系統降低交通事故之發生率、減低因行車事故導致之死傷人數、減少駕駛時間、透過避免擦撞系統之設計而減少交通壅塞情形、可減少交通警察或號誌設備之配置、減少駕駛之雇用成本等，然而，誠如「水可載舟、亦可覆舟」，自動駕駛汽車在法律層面可能衍生的疑義亦不容忽視，舉例言之，自動駕駛汽車若因系統故障發生行車事故，究竟應由車主負責？或應由汽車製造廠商負責？自動駕駛汽車之電腦系統若遭駭客入侵而將車輛駛往他處、或蒐集汽車內部資訊，因此所導致之法律糾紛應由何人負責？雖然自動駕駛汽車正式問世的時間仍屬未知，然而科技的發展與應用日新月異，在科技發展的同時，法律制度的研究與配套措施必須迎頭趕上，這也正是本研究希冀透過對物聯網發展之瞭解，探討網路犯罪之新趨勢與其可能規範方式之探討目的所在。

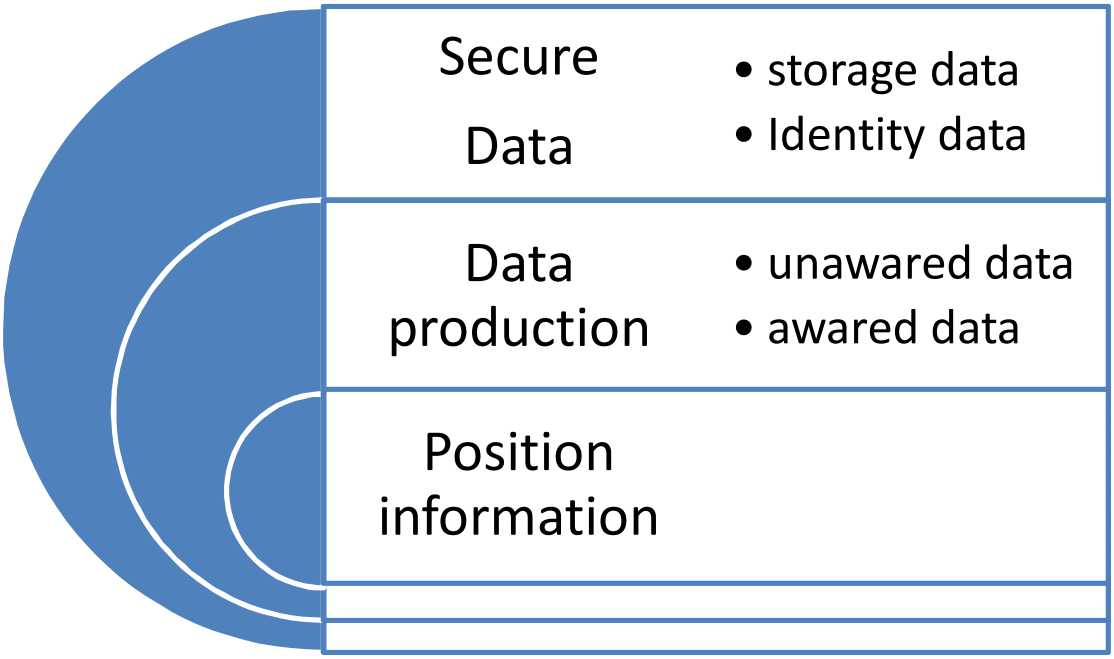
## 第二節、各式物聯網之型態（Types of IoT）

### 一、資訊裝置（Devices with Information）

所謂「資訊裝置（Devices with Information）」係指透過網際網路所連結的設備之間可透過取得、蒐集與傳送資料結合為一體，由各該設備所蒐集的資料本係供該設備所使用，而不同的設備則可蒐集不同類型的資料[51]，就具體運作模式而言，透過各感應器所蒐集的資料傳輸到其他連結的設備或服務設施上，進行資料比對過程，再依據比對結果做出最後的決策，以溫控器裝置為例，使用者可以依據歷史使用量資料，作為判斷究竟應開啟暖氣或冷氣之基準，同時配合電費費率之考量計算，使溫控器裝置於優惠費率時段開啟、於尖峰時刻暫時關閉運作，進而達到節費目的，此即物聯網技術應用在資訊裝置所可發揮的智慧化功能。

在資訊裝置的類型上，則可大別為「資料安全性」、「資料產生」與「定位資訊」三種類型。

[51] 例如：水表內的感應器會蒐集關於住家用水的資料，用了多少、使用時機。住家溫控器裡面的感應器會蒐集暖氣與冷氣（A/C）的使用時間、每天早晚的室內溫度（與室外溫度）等等。汽車內的感應器會蒐集引擎溫度、油量等資訊，裝在高速公路上的感應器，會蒐集交通流量，甚至氣溫等資訊。參見 Michael Miller 著/胡爲君譯，前揭書，第 33 頁。




## （一）隱密性資料（Secure Data）

關於隱密性資料（Secure Data）之類型，依其資料性質之不同，可區分為「儲存性資料（storage data）」與「識別性資料(identity data)」兩類，所謂「儲存性資料(storage data )」係指該資料內容本身儲存於物聯網所連結的設備當中，必須透過識別性機制始可取得、蒐集；而所稱「識別性資料（identity data)」則為前述儲存性資料中所稱之識別性機制，如：密碼、指紋、聲紋、掌紋等；此等隱密性資料可謂係所有物聯網運作的基礎，不法侵入行為的對象可能包括儲存性資料與識別性資料在內，進而透過所取得之資料內容遂行各種犯罪行為，如銀行詐欺、信用卡詐欺等。

## （二）資料產生（Data production）

所謂資料產生（Data production）係指該裝置本身的作用在於產生資料，依其所產生資料之內容或過程是否為使用者所知悉作為區別基準，可大別為「未知資料（unaware data)」與「已知資料（aware data)」兩種態樣，所稱「未知資料（unaware data)」係指使用者對於所產生的資料過程或資料內容並不知悉者而言，如環境資料(environmental data）與虛擬實境（virtual reality）[52]等；而「已知資料（aware data)」則指使用者對於資料產生之過程與內容均屬明知者而言，其應用種類如體溫血壓監控器、鍋爐溫度或室內溫度等，目前發展中的穿戴式科技亦為產生已知資料之物聯網類型，智慧手錶可謂係最為一般人所熟知的穿戴式科技。

## （三）定位資訊（Positioning information ）

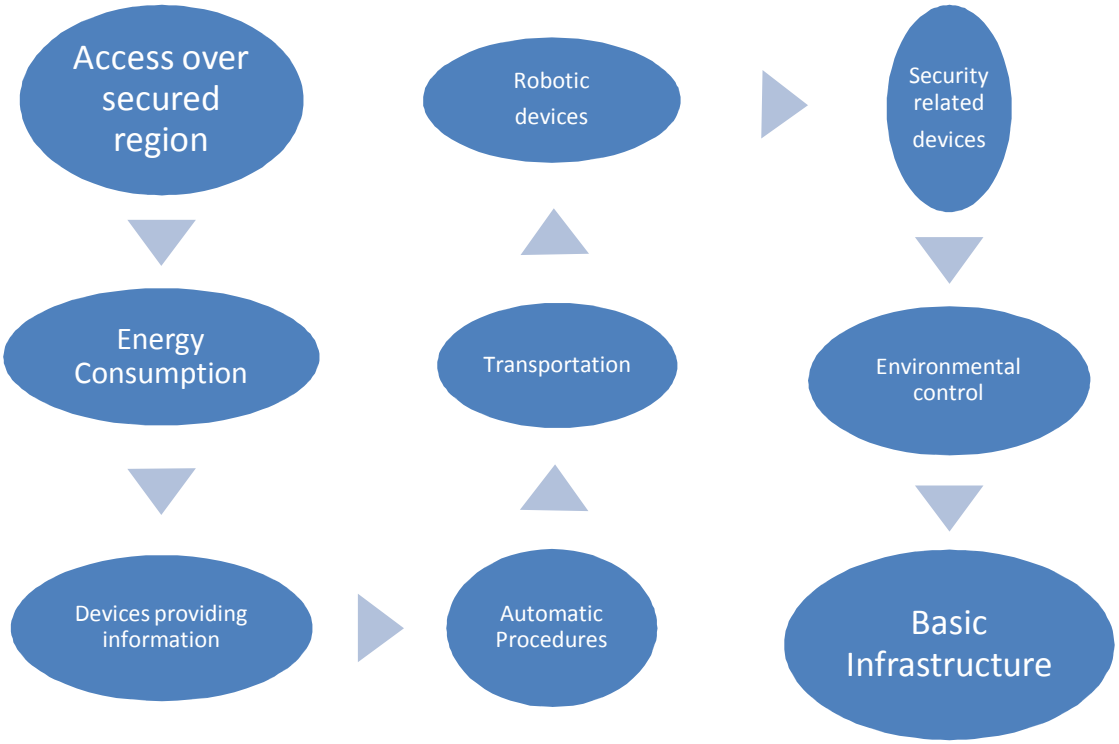
所謂定位資訊（Positioning information )」係指該裝置本身具有存取使用者位置資料之功能，該等裝置係透過衛星資料或基地台訊號取得相對之地理位置訊息，再運用此等資料進行資料傳輸、處理工作；舉例而言，行車導航器即

[52]虛擬實境（Virtual Reality)，簡稱 VR 技術，也稱人工環境，是利用電腦模擬產生一個三度空間的虛擬世界，提供使用者關於視覺、聽覺、觸覺等感官的模擬，讓使用者如同身歷其境一般，可以及時、沒有限制地觀察三度空間內的事物。

為相當普及的定位資訊運用模式，透過行車導航器所配置的GPS 系統蒐集定位資訊，提供使用者規劃行車路徑與方向；而就可蒐集定位資訊之穿戴式科技而言，具備GPS功能的穿戴設備體積通常很小，其設計功能在於讓使用者可以隨身放進外套或襯衫口袋內，當需要瞭解使用者的行蹤時，即可透過電腦或智慧手機，將對應的智慧手機應用程式開啟，以取得此等「定位資訊」。

## 二、控制裝置（Devices have control over things）

所謂「控制裝置(Devices have control over things)」係指透過網際網路所連結的各項設備可產生控制性功能，其類型包括如門禁裝置之具控制出入權之裝置（Access over secured region,）、具控制監測能源權之裝置（Energy Consumption）、具蒐集產製資訊權之裝置（Devices providing information）、控制流程自動化之裝置（Automatic procedures）、可控制實體行動權之裝置(Transportation)、人工智慧裝置(Robotic devices)、安全監控裝置(Security related devices)、環境控制裝置(Environmental control)、基礎設施控制裝置(Basic infrastructure)等。




## (一)安全區域管控裝置(Access over secured region)

所謂「安全區域管控裝置(Access over secured region)」係指該等裝置之使用目的在於管控特定區域之進出安全，如門禁裝置、具控制出入權之裝置等。

## (二)具控制或監測能源之裝置(Energy Consumption)

所謂「具控制或監測能源之裝置(Energy Consumption)」係指該設置本身之使用目的在於控制或監測能源系統，其應用重心在於電源開關之控制，若該電源開關遭不法侵入，可

能衍生財產權之侵害。

### （三）具蒐集產製資訊權之裝置（Devices providing information）

所謂「具蒐集產製資訊權之裝置（Devices providing information）」係指該設置之作用在於蒐集產製資訊權，若不法侵入該等裝置，可能消極地造成該設置本身無法運作，或積極地奪取該設置中所產製之資訊於不法用途。

### （四）控制流程自動化裝置（Automatic procedures）

所謂「控制流程自動化裝置（Automatic procedures）」係指機械化操作之過程係由自動化程式設定並運轉，如自動洗衣機、自動櫃員機或自動販賣機等，均屬適例。

### （五）可控制實體行動權之裝置（Transportation）

所謂「可控制實體行動權之裝置（Transportation）」係指該裝置之作用在於控制實體物品之行動能力，自動駕駛汽車即屬適例，利用各種感應器、電腦與智慧技術，自動駕駛汽車可以感應自身與馬路上其他汽車間之關連性，並根據

已設定好的座標位置導航[53]

## （六）人工智慧裝置（Robotic devices）

所謂「人工智慧（Artificial Intelligence ），簡稱AI」，或稱為「機器智慧」，係指由人工製造出來的系統所表現而出之智慧，依此所產生的「人工智慧裝置（Robotic devices)」則係將人工智慧應用於各式裝置上，如：無人機（Drone)、機器人（Robots）等；以無人機為例，此種無人駕駛之飛機（unmanned aerial vehicle）依其功能不同，在類型上可區分為民用和商用無人機（提供非軍事作業的功能)、戰鬥無人機（可攻擊敵人設施[54])、後勤無人機（執行貨運與其他後勤功能)、偵察無人機（提供資訊)、研發無人機（提供測試與其他功能，協助無人機技術的開發)、標記與誘餌無人機（為地面與空中火力標記目標）等[55]。

---

[53] 一輛完全自動駕駛的汽車需要用到多種科技，如：360 度攝影機，看見車子的四面八方；適應路況定速控制，在車流中保持速度；緊急煞車與方向輔助盤，避免碰撞；GPS，準確判斷位置與導航路線；雷達與光學偵測及測距（LIDAR, Light Detection and Ranging）系統，感應你與其他車輛或物體間之距離；立體攝影機，辨識車輛以外的物體，如行人與自行車。參見 Michael Miller 著/胡爲君譯，前揭書，第 150 頁。

[54] 美國軍方最愛用無人機，至今已經部署了超過 11,000 台無人機，軍方的無人機可以執行各種任務，從空中偵察到比較有爭議的遙控戰鬥。偵察無人機具備 HD 攝影機；戰鬥無人機則攜帶飛彈與炸彈。有些專家相信，無人機最終可以取代大部分載人的軍機，飛行員不用再冒生命危險。Michael Miller 著/胡爲君譯，前揭書，第 167 頁。

[55] 參見 Michael Miller 著/胡爲君譯，前揭書，第 166 頁。

## （七）安全監控裝置（Security related devices）

所謂「安全監控裝置（Security related devices）」係指基於保全之需求，對於特定空間或特定對象安裝監控系統，如典型之門禁監視器、生命徵象監視儀。

## （八）環境控制裝置（Environmental control）

所謂「環境控制裝置（Environmental control）」係指透過網際網路之連線設備，對周遭環境的空氣品質、溫度、濕度等因子予以控制之裝置，在現實生活上常見的空調、冷暖氣機即屬適例；進一步言之，就整體環境而言，透過物聯網之應用對環境因素進行監控，可同時確保整體環境是否遭受侵害，論者有稱之為「環境物聯網」，亦即可透過物聯網來監視各種環境要素[56]；不可諱言，全球性的氣候變遷主要導因於工業發展所造成的環境污染，要如何透過物聯網的應用對抗氣候變化？其主要方式為減少全球能源消耗量、減少碳排量，其具體手段則係將地區性的作法[57]擴展到全球性，

[56] 例如：「二氧化碳感應器」可監視汽車排氣、工廠空氣污染、甚至農地產生的有毒排氣；「水感應器」可監視海洋、河流與湖泊的水質，判斷水域是否適合魚類與植物生存；「輻射感應器」監視核能電廠周圍的輻射指數，必要時發佈外洩警報；「林地中的感應器」監視可燃氣體與濕度，偵測可能造成森林火災的狀況；「電磁感應器」監視各種行動電話基地台、高壓電線、Wi-Fi 路由器與其他電子設備的電磁波。參見 Michael Miller 著/胡爲君譯，前揭書，第 256 頁。

[57] 舉例言之，「智慧溫控器」可以改善住家與公司的冷暖氣效率；「智慧照明系統」可讓住家、公司公共區域、大樓與道路僅在需要時開燈；「智慧家電與電子設備」可以在能源使用量（與費用）較低時才啓動，「智慧電網」可改善電力送到顧客端的路線；「智慧汽車、道路與停車場」可減少汽車駕駛時間，進而減少車輛的能源消耗；「智慧農耕系統」可增加農作物產量，減少水、能源與農藥的用量；「智慧監視系統」如 Air Quality Egg 可協助個人與企業監視空氣與水的品質；利用物聯網對抗氣候變化，是靠許多微小的改變來累積出成果。例如，交通管理問題。如果你住在都會區，你早已經習慣在早晚通勤時間塞車，這是工作的一部份。然而浪費在塞車的每一秒，也都在浪費能源，光是在美國，一年就浪費了 19 億加侖。換算過來，相當於多排放了 1.86 億噸的二氧化碳（CO2）。利用智慧交通管理科技，這些碳排放量可以大幅降低，如果物聯網可以幫助你避開塞車，一路順暢通開往目的地，浪費的能源就可以減少、污染也減少，大家都受益。參見 Michael Miller 著/胡爲君譯，前揭書，第 258 至第 259 頁。

使地球處於適度控制下的妥適模式。

### （九）基礎設施控制裝置（Basic infrastructure）

所謂「基礎設施控制裝置（Basic infrastructure）」係指透過網際網路連結與基礎設施（如：交通號誌、自來水廠、電力廠）相關之設備，其具體應用如：交通號誌控制、自來水流閥、變電器廠、電信設備、下水道系統等。

## 第三節、物聯網遭濫用之方式

看似便捷的物聯網應用世界裡，隱藏著諸多陷阱與憂慮，其遭濫用的方式可依其侵害方式之不同，大別為「資訊安全性（information security）之侵害」與「所有權及控制權（Ownership and Right of control）之侵害」兩大類型，茲分敘如下：

### 一、資訊安全性（information security）

關於「資訊安全性（information security）」遭侵害之類型，依其侵害模式之不同，又可區分為「個資竊取（Identity Theft）」、「資料竊取（Data Theft）」、「利用竊得之資料進行非具奪取實物控制權之詐騙（Cheat with collected information）」與「資訊竄改（misleading

information)」四種態樣，茲分敘如下：

### （一）個資竊取（Identity Theft）

所謂「個資竊取（Identity Theft)」係指行為人以不法侵入方式獲取個人之識別性資料（identity data)，據以知悉儲存性資料（data storage）之內容，進而利用所竊取之個人資料遂行犯罪行為。

### （二）資料竊取（Data Theft）

所謂「資料竊取（Data Theft)」係指行為人以不法侵入方式獲取具有價值之識別性資料（identity data)，據以知悉該等儲存性資料（data storage）之內容，如：金融帳戶資料、病患身體健康數據等。

### （三）利用竊得之資料進行非具奪取實物控制權之詐騙（Cheat with collected information）

所謂「利用竊得之資料進行非具奪取實物控制權之詐騙（Cheat with collected information)」係指透過個資竊取、資料竊取所得之資料，進一步利用於不涉及奪取實物控制權之詐騙行為，傳統常見的幫助詐欺案件，係詐欺集團透過人頭帳戶詐取財物，該詐欺集團實已取得人頭帳戶之控制權[58]；然在物聯網的世界中，犯罪行為人並不需要實際取得

[58] 實務上亦有關於幫助詐欺案件中，詐欺集團並未取得人頭帳戶直接控制權的例外情形，其典型狀況爲詐欺集團取得帳戶使用者之信任，誘使帳戶使用者代爲提領被害人匯入帳戶之款項，論其實際亦屬間接控制該帳戶。

實物控制權，僅需透過利用竊得資料進行不法目的之使用，即可能遂行犯罪目的；如：透過取得控制汽車狀況之識別性資料，進而為相對應之詐取維修費用之行為。

### （四）資訊竄改（misleading information）

所謂「資訊竄改（misleading information）」係指透過個資竊取、資料竊取所得之資料，進而竄改裝置之內容資訊以誤導決策人，使之為錯誤決策，如：透過取得控制病患身體健康數據之識別性資料，侵入該等裝置修改數據，進而使病患、醫師誤信其身體健康惡化而需大量使用藥物或治療。

## 二、所有權及控制權（Ownership and Right of control）之侵害

關於違反所有權及控制權之型態，可依其所侵害法益之內容，區分為「實質或虛擬方式侵入保全區域（Invasion and breakthrough）」、「取得控制能源使用權（Up and Down regulation of Energy）」、「創製錯誤資訊以誤導並取得控制權（Creating misleading information）」、「控制或修改自動化流程（Taking over automatic procedures）」、「制或取得實物（theft and stealing）」、「整位置資料以取得實物控制權（Leading to wrong destination）」、「取得財

物、動產及不動產之控制權(Control over property)」、「入侵金融相關帳戶取得金融所有權(Taking over accounts and money)」、「因控制以上項目而威脅生命權(Life threatening actions)」、「大規模破壞(Mass destruction)」等十種態樣，茲分敘如下：

## （一）實質或虛擬方式侵入保全區域（Invasion and breakthrough）

所謂「實質或虛擬方式侵入保全區域（Invasion and breakthrough)」係指以實質或虛擬方式，利用所獲取具控制出入權之裝置資訊侵入保全區域，進而為財物竊取行為等不法犯行。

## （二）取得控制能源使用權（Up and Down regulation of Energy）

所謂「取得控制能源使用權（Up and Down regulation of Energy)」係指透過取得具控制監測能源權之裝置控制權，遂行特定不法目的；著名的「 Stuxnet 電腦蠕蟲事件」即屬適例[59]。

[59]2010 年 7 月首次被發現的強力電腦蠕蟲，據信是由美國和以色列情報人員合作研發，還得到英國和德國協助。情報和軍事專家指出，以色列曾在內蓋夫沙漠狄莫納基地的核設施內，測試「Stuxnet」電腦蠕蟲。該病毒 2009 年 11 月導致伊朗核設施五分之一的離心機被迫關閉，經此一役，估計伊朗至少要延遲至 2015 年，才可能製造出核彈。報導指出，以色列過去兩年一直在內蓋夫沙漠戒備森嚴的狄莫納設施（Dimona）內，模擬與伊朗安裝在納坦茲核設施離心機幾乎一模一樣的離心機，測試這種具有極大破壞力的電腦蠕蟲，這是以色列和美國聯手對付伊朗核武野心而採取的行動之一。Stuxnet 蠕蟲程式包括兩大部分，其中之一是意圖讓伊朗的離心機在運轉時失控，另一部分則秘密記錄伊朗核電廠的正常作業活動，然後在發動破壞期間重新顯示這些紀錄，讓核電廠營運人員誤以為電廠一切正常。參見 2011 年 1 月 17 日，自由時報國際版報導。

### （三）創製錯誤資訊以誤導並取得控制權（Creating misleading information）

所謂「創製錯誤資訊以誤導並取得控制權（Creating misleading information）」係指透過產生未知資訊(unaware data）的資訊裝置，將該資訊內容竄改後取得物聯網裝置之控制權，進而得以遂行其他犯罪行為。

### （四）控制或修改自動化流程（Taking over automatic procedures）

所謂「控制或修改自動化流程（Taking over automatic procedures）」係指透過物聯網裝置之連結，控制或修改自動化流程之運作。

### （五）控制或取得實物（theft and stealing）

所謂「控制或取得實物（theft and stealing）」係指利用物聯網所連結之設置（如：保全裝置、監控系統）等，進行實物之偷盜行為；舉例言之，行為人可能透過控制賣場或便利超商與物聯網相連接之保全系統，修改資料庫內的結帳設定，使系統誤以為商品已結帳，而掩護偷盜行為。

### （六）調整位置資料以取得實物控制權（Leading to wrong destination）

所謂「調整位置資料以取得實物控制權（Leading to

wrong destination)」係指利用物聯網所連結之設置（如：保全裝置、監控系統）蒐集之定位資訊，透過調整位置資料之方式，進行實物之偷盜行為，因而取得實物之控制權，伊朗與美國之間的無人機事件即屬此等類型[60]。

## （七）取得財物（動產及不動產）之控制權（Control over property）

所謂「取得財物(動產及不動產)之控制權(Control over property)」係指利用物聯網所連結之裝置取得之識別性資料得以用來作為控制實體財物(包括動產及不動產)之手段，進而使該等財產權發生得、喪、變更之狀態。

## （八）入侵金融相關帳戶取得金融所有權（Taking over accounts and money）

所謂「入侵金融相關帳戶取得金融所有權(Taking over accounts and money)」係指行為人透過取得與金融帳戶相關之物聯網認證裝置，而得以入侵被害人之金融相關帳戶，

[60] 2012 年 12 月 4 日，伊朗軍方聲稱，他們在波斯灣海域成功擄獲了一架美國「掃描鷹」無人飛機。這也是去年 12 月以來，伊朗擄獲的第二架美國無人機。不過伊朗沒有說明他們究竟是如何成功擄獲這架無人飛機。伊朗伊斯蘭革命衛隊發表聲明說，這架美國無人機當時正在波斯灣水域巡邏，進行偵查活動並收集情報，無人飛機一進入伊朗領空後就被他們俘獲。2011 年 12 月，伊朗曾利用電子戰技術擄獲一架美軍 RQ-170「哨兵」無人偵察機。據報導，當時伊朗是成功侵入這架無人機的控制系統，更改導航程序，誘使飛機在伊朗境內降落。事後，伊朗公開了這架被俘獲的無人機畫面，還表示要解密並複製這架無人機，讓美國十分尷尬，美國總統歐巴馬公開要求伊朗歸還也被一口回絕。2012 年 4 月，伊朗表示已經恢復了這架無人機的相關數據，並已開始建造複製品。

針對帳戶內之財產權進行非法移轉行為，而取得該金融所有權而言，舉例而言，現今金融機構常以各種認證裝置作為其金融帳戶之識別系統，若行為人不法入侵該認證裝置而控制其識別系統，即可能遂行財產犯罪。

## （九）因控制以上項目而威脅生命權（Life threatening actions）

所謂「因控制以上項目而威脅生命權(Life threatening actions)」係指行為人透過實質或虛擬侵入保全區域、取得控制能源使用權、創製錯誤資訊以誤導而取得控制權、取得財物（動產、不動產）之所有權、侵入金融相關帳戶而取得金融所有權等方式，進而操控可能為威脅生命權之資訊。

## （十）大規模破壞（Mass destruction）

所謂「大規模破壞（Mass destruction)」係指大規模裝置自毀或控制以上項目，進而造成系統性破壞等情形；著名的例子如伊朗駭客於 2013 年入侵美國紐約近郊萊伊鎮（Rye）的波曼大道水壩（Bowman Avenue Dam)，水壩的電腦系統遭到駭客攻擊，其嚴重結果可能在附近地區造成洪水。據信駭客是通過手機信號裝置侵入，美國政府遲至 2015 年 12 月 21 日始對外承認該起事件。

## 三、現行針對物聯網之法律規範與可能之規制方向

犯罪行為人若透過物聯網機制進行危害資訊安全之犯罪行為，或奪取資訊之所有權及控制權，在現行法律體系下之規制狀態為何？茲分敘如下：

### （一）危害資訊安全（Information Security）之行為

關於危害資訊安全之行為應如何施以制裁，就我國現行法制而言，其法律依據包括前述之刑法妨害電腦使用罪章及個人資料保護法[61]之相關規定，而在物聯網的架構下，危害資訊安全之行為包括：「個資竊取（Identity Theft)」、「資料竊取（Data Theft)」、「利用竊得之資料進行非具奪取實物控制權之詐騙（Cheat with collected information)」與「資訊竄改（misleading information)」四種態樣，就其法律效果論之，單純之資料（包括個人資料、金融帳戶資料等）取得行為或竄改行為，若尚未造成客觀上之損害，基於刑法謙抑之思想，國家實體刑罰權尚無介入之必要，此亦為目前實務上針對妨害電腦使用罪及違反個人資料保護法

[61] 論者指出，個人資料保護法第 41 條主要規範之對象爲個人資料保護法已明定行爲合法要件之情形，包括醫療、基因、性生活、健康檢查、犯罪前科五大類個人資料（合稱特種個人資料）蒐集處理利用的原則禁止與例外合法事由、公務機關與非公務機關蒐集處理利用個人資料應具備之合法要件、公務機關與非公務機關欠缺合法要件時例外合法的事由，以及中央目的事業主管機關對非公務機關「國際傳輸行爲」之限制等，個人資料保護法係將此等規範要求提升至刑事責任層次，督促公務機關與非公務機關高度注意其個人資料蒐集、處理、利用行爲，以期導正舊法保護不彰之個資運用環境，並遏止行爲人忽視法律規範，甚至加諸他人難以回復之人格權侵害。參見葉奇鑫、李明臻，前揭文，第 70 至第 71 頁。

行為之一貫立場；茲有疑義者為，危害資訊安全之行為人是否需具備「營利意圖」[62]？觀諸刑法關於妨害電腦使用罪章之規定，均以「無故」作為要件，而所稱「無故」之法律意義則為「無正當理由」，解釋上若行為人係以營利意圖為目的，即可評價為不具備正當理由；惟就個人資料保護法第 41 條第 1 項規定而言，則未區分行為人是否具備營利意圖，論者即指出，基於刑罰之最後手段性，若不問行為人營利意圖之具備與否，一旦有違法蒐集、處理、利用個人資料之現象而「足生損害於他人」時，一律以刑罰相繩，恐產生施罰過當之疑慮[63]。

### （二）奪取資訊之所有權與控制權（Ownership and Right of control）之行為

單純的資訊取得、蒐集或竄改行為若未造成損害（不論是實害或具體損害），尚非屬國家刑罰權發動之對象，已如前述；然而，若行為人之行為涉及奪取資訊之所有權與控制權，在目前的現行規範下，是否仍該採取相同的處罰基準？

由奪取資訊之所有權與控制權之行為態樣觀之，不論係

[62] 101 年個人資料保護法之修法過程中，法務部本研擬將個人資料保護法第 41 條第 1 項刪除，其理由在於非意圖營利違反個資法規定足生損害於他人之行爲，原則上以民事損害賠償、行政罰等救濟即爲已足，且須課予刑事責任者，於相關刑事法規已有規範足資適用，個人資料保護法部分條文修正草案總說明，https://www.moj.gov.tw/ct.asp?xItem=279906&ctNode=28007&mp=001（造訪日期：2015 年 12 月 22 日）

[63]參見　葉奇鑫、李明臻，前揭文，第 72 頁。

「實質或虛擬方式侵入保全區域（Invasion and breakthrough）」、「取得控制能源使用權（Up and Down regulation of Energy）」、「創製錯誤資訊以誤導並取得控制權（Creating misleading information）」、「控制或修改自動化流程（Taking over automatic procedures）」、「制或取得實物（theft and stealing）」、「整位置資料以取得實物控制權（Leading to wrong destination）」、「取得財物、動產及不動產之控制權（Control over property）」、「入侵金融相關帳戶取得金融所有權（Taking over accounts and money）」、「因控制以上項目而威脅生命權（Life threatening actions）」、「大規模破壞（Mass destruction）」，其可能造成的危險性均遠遠高於前述之危害資訊安全行為，透過物聯網機制而控制、取得實物、財物所有權、金融所有權、能源使用權、保全系統等，行為人或許尚未引爆實際上之損害，然國家刑罰權若遲至客觀上損害發生始介入，是否已造成極難彌平之損害？

華爾街日報於 104 年 12 月 21 日披露，伊朗駭客曾侵入紐約市附近一座水壩的電腦系統，這起事件如今已引發白宮以及企業對美國基礎設施面臨安全隱憂的廣泛關切。被入侵的水壩是位於萊伊鎮（Rye）的波曼大道水壩（Bowman Avenue Dam），萊伊鎮在紐約市東北方約 20 哩處。水壩的電腦系統是在 2013 年遭到駭客攻擊，可能在附近地區造成洪水。報導指，駭客是通過手機信

號裝置侵入的。波曼大道水壩高 20 呎，為 Blind 河的一座混凝土結構大壩，距長島灣約五哩。萊伊市長賽蘭諾說，駭客入侵水壩的電腦系統後，聯邦調查局（FBI）來向萊伊鎮的技術管理人員詳細詢問。水壩遭到駭客入侵很難發現，聯邦調查人員最初以為，攻擊美國水壩的駭客，通常會以規模更大的水壩為目標，如俄勒岡州的一座水壩。美國和伊朗的網路駭客交鋒不斷，在美國間諜使用 Stuxnet 公司的電腦蟲軟體，進入並損壞了伊朗的核設施後，伊朗駭客是以攻擊美國銀行的網站予以還擊。許多企業的電腦控制系統老化，易於遭到攻擊。美國有 5 萬 7000 多個企業的控制系統與網路相連，國內安全部發言人證實，波曼大道水壩遭駭後，國安部設立了 24 小時不間斷的網路資訊共享系統，如果重要基礎設施的安全脆弱或是出現威脅，他們將隨時提供協助[64]。此一水壩事件即屬前述關於因取得基礎設施控制裝置（Basic Infrastructure）控制權而可能造成「大規模破壞（Mass destruction）」之情形，本文以為，關於奪取資訊之所有權與控制權之行為，基於其行為模式之侵入性程度較高，在立法上不宜以具體危險犯或實害犯之規範方式為之，否則恐造成難以回復之損害，惟是否應區分不同類型、不同程度之奪取資訊之所有權與控制權行為加以規範，則屬

[64]http://udn.com/news/story/6809/1394336-%E4%BC%8A%E6%9C%97%E9%A7%AD%E5%AE%A2-%E6%9B%BE%E5%85%A5%E4%BE%B5%E7%BE%8E%E5%9C%8B%E6%B0%B4%E5%A3%A9%E7%B3%BB%E7%B5%B1。（造訪日期：2015 年 12 月 25 日）

立法上應與物聯網發展模式同步研擬之技術層次問題。

# 第四章、結論—心得及建議

物聯網所衍生的現實問題影響層面極度廣泛，或許大部分的人對於「物聯網」一詞尚屬陌生，但事實上物聯網的應用早已無所不在。學者指出，資訊科技發展提升人們生活品質的同時，也帶來一些新的困擾，因為這一個科技成果也往往被利用來作為為非作歹的工具，新的資訊科技雖然也會帶來損害，但是新的資訊科技更帶來絕大的利益。直接可以看到的時間效益、空間效益不說，更深一層的意義例如人類活動範圍的擴張，同時也代表了人類人格權的擴張[65]，實屬的論；以今日世界而言，物聯網的發展更將網路資訊科技帶往更高、更遠的境界，未來的世界網路應用只有更為蓬勃發展的可能，身處在瞬息萬變的時代，誠如學者所述，在犯罪的預防與偵查上，這會永遠是一場技術的戰爭，而且甚至是一場沒有結局的戰爭，但是在價值判斷上，似乎也沒有理由放棄這樣的戰爭，而因電腦及網路的使用所製造出來的利益衝突情境是形形色色，我們必須在種種新的經驗中去尋找互動關係的尺度[66]；本文所介紹的物聯網世界，即將或已經改變你我日常生活的食、衣、住、行、育樂模式，現行刑法關於

[65] 參見 黃榮堅著，<電腦犯罪的刑法問題>，刑罰的極限（學術論文集），元照出版，1999 年 4 月，第 208 頁。
[66] 參見　黃榮堅，前揭文，第 208 頁、第 210 頁。

妨害電腦使用罪及個人資料保護法所規制的行為態樣，恐已無法全面性規範物聯網所產生之衝擊，如何在各式各樣的物聯網應用型態可能衍生的法律風險進行規制，尋求科技發展與社會生活秩序維持之平衡點，乃當代法律人的重要課題。