第三常設委員會

第 3/III/2009 號意見書

事由：《打擊電腦犯罪法》法案。

一、引言

澳門特別行政區政府於二零零九年二月十二日向立法會提交《打擊電腦犯罪》法案，立法會主席於當日根據議事規則的規定接納了該法案。

上述法案於二零零九年二月二十三日在立法會全體會議上引介以及進行一般性討論和表決，並在十九票贊同票的情況下，獲得多數通過。立法會主席於同日透過第 208/III/2009 號批示將該法案派發給本委員會進行細則性審議及製作意見書。由於法案涉及複雜的技術內容，委員會曾向立法會主席申請延長細則性審議的期限，申請獲接納。

委員會在政府代表的協助下，對該法案展開了分析，為此，分別在二零零九年三月二十日、二十七日，四月一日，五月二十一日、二十五日及六月十七日舉行了會議。其間，為了從技術層面上完善本法案，立法會顧問團與政府的顧問團舉行了多次的工作會議。

基於法案的內容以及其範圍包括了一些屬程序性質的規定，本委員會根據八月二十一日第 42/95/M 號法令第三十條第三款的規定，於二零零九年四月六日致函澳門律師公會進行諮詢，邀請其就本法案提出意見。截至簽署本意見書之日為止，本委員會沒有收到該公會的任何意見。

二零零九年五月二十七日，政府提交了新的法案文本，其中若干內容反映了委員會的意見以及立法會顧問團對法案的法律技術分析。本意見書所引述的條文就是出於法案最終文本。

二、引介

法案理由陳述指出：*"隨着資訊科技的日趨進步，電腦及互聯網的使用越來越普遍，.....但與此同時，越來越多不法份子利用便利的資訊科技作為犯罪的新平台，這無疑為世界各地在預防及打擊電腦犯罪方面帶來了新挑戰。.....電腦犯罪的類型多樣化，且具有廣泛性、智慧性、隱匿性、迅速性及偵查難等特點，傳統的打擊犯罪方法面對在互聯網上所實施的虛擬行為時顯得束手無策。不法份子除了透過資訊科技來實施傳統類型的犯罪外，例如詐騙、盜竊、毀損等犯罪，亦會利用資訊科技實施新型犯罪，例如傳播電腦病毒、不當截取電腦數據資料、干擾電腦系統等犯罪，從而對資訊領域的運作安全造成威脅。針對各種濫用資訊科技的不法行為，採取立法措施除了可防止犯罪行為的發生外，亦可促進虛擬世界內的安全文化，保護個人資料及隱私，從而加強人們對資訊世界的信心。"*

理由陳述還指出："*在澳門特別行政區的法律體系中，.....有關打擊電腦犯罪的法律措施並不足夠。因此，有需要完善有關規定，以訂定某些侵犯電腦或網絡行為的新罪狀，並對某些本身屬犯罪而透過互聯網實施的行為加重處罰.....*"

本法案是經參考歐洲委員會於二零零一年十一月二十三日在布達佩斯簽訂的《打擊網絡犯罪公約》以及內地、香港、台灣、新加坡、葡萄牙、德國及美國等多個地區及國家關於預防及打擊電腦犯罪的法例後而編製的。

在法案的引介中，提案人強調法案的主要內容包括：

1. 在立法形式上，採用編製一項特別法而不是將這些新的犯罪類型加入《刑法典》內；

2. 在刑事實體內容方面，訂定：

（1）新的犯罪行為類型，包括不當獲取或使用電腦數據資料、不當進入電腦系統、不當截取電腦數據資料、損害電腦數據資料、干擾電腦系統、用作實施犯罪的電腦裝置或電腦數據資料及電腦偽造等犯罪。

（2）法人的刑事責任，此規定與國際法文書要求對實施電腦犯罪的法人追究刑事責任的規定相接軌。

（3）在某些情況下，刑罰的加重，是為了加強電腦系統或

電腦數據資料的保密性及完整性。

3. 在刑事訴訟規定方面，賦予具職權的當局在打擊電腦犯罪方面更有效的調查工具，包括：

（1）明確規定電腦系統、電腦數據資料儲存載體、電腦數據資料或電腦程式可作為證據。

（2）訂定多項必需及迫切的措施：如當局有理由相信有關電腦數據資料有助刑事調查工作，則可採取例如迅速保存資料、查閱路由數據資料（但不包括內容數據資料）、阻止他人查閱特定及不法的電腦數據資料等措施。

理由陳述亦指出："*本法案並無就涉及言論自由的任何事宜訂定新的罪狀或作出更多的限制，*（因此），*本澳市民依法享有言論自由，這項基本權利是受到《基本法》保障的，所發表的言論，不論是否透過互聯網進行，僅當違反法律的明文規定，方會受到處罰。*"

三、概括性審議

1. 在現代社會裏，無論是在經濟發展抑或人們的日常生活中，資訊及通訊科技都扮演著一個很重要的角色。從經濟層面來說，"各國依賴融入全球經濟來維護本身經濟興盛的現象越趨明顯。隨著網絡空間成為主要的貿易渠道，為電子商務設置一個安全的法定平台

亦變得更加重要”[1]；從個人生活層面來說，電腦，尤其是互聯網，使人與人之間的聯絡變得更加方便，而且將取得一些從其他途徑難以獲取的內容變得容易，甚至是表達意見的一個開放平台。因此，“互聯網作為通訊的空間及渠道，已使公開發表意見普遍化且促進了意見的交流。今天，廣泛傳播個人思想已不是難事，互聯網容許市民大眾從純粹被動的消費者角色變為更具積極性通訊製作者的角色”[2]。由於資訊及通訊科技本身的特點，資訊及通訊科技今天已成為很多人個人發展的要素之一，對於他們來說，*距離已不再是一個問題，全球一體化也從而得到體現*[3]。

正如本委員會過去已指出的，“隨著新科技的普及使用，與使用有關的風險也隨之提高。在很多廣為人知的個案中，互聯網使用者因保安系統存在問題成為新型犯罪手法的受害人：從侵犯隱私權，到濫用個人資料，到進行財產性質的欺詐或其他類型的犯罪。在令人讚嘆的‘新科技世界’裏存在著極險峻的一面，從而阻止或妨礙了新通訊技術潛力的充分發揮。因此，有必要提高互聯網使用的內在安全性”[4]。

2. 雖然各類資訊科技均可被濫用及作不法用途（即不按法律使用），但不能因此就斷言應以刑法來解決該等問題。因為法律秩序

---

[1] Peter Grabosky, 'The Gobal Cyber-Crime Problem: The Socio-Economic Impact', in *Cyber-Crime – The Challenge in Asia,* Roderic Broadharst & Perter Grabosky (ed.), Hong Kong University Press (2005), p. 50.

[2] 冼沛文，- 澳門立法會關於法律及公民權利的第二輪系列研討會基本權利 – 鞏固及未來發展，*互聯網與基本權利 - 審查的民間化：互聯網內容監管與言論自由*。

[3] 第三常設委員會關於《電子文件及電子簽名》法案的第 2/II/2005 號意見書，可到 http://www.al.gov.mo/lei/leis/2005/05-2005/parecer_cn.pdf 查閱。

[4] 同上。

要求首先識別應受刑法保護的法益，然後看所涉及的行為會否對該等具刑法意義的法益構成危險。刑法應是保護法益的最後手段，只在所有其他保護方法都顯示無效的情況下，才予以運用（刑法的補充性原則）。[5]

當立法會進行打擊電腦犯罪的立法工作時，本委員會便就上述的要素作出分析，認為有關行為本身及其結果均應受到譴責，法案建議的內容符合刑法的補充性原則，由此，可肯定資訊科技領域中的不法行為具備應以刑法規範的必需要件：

a) 從受影響的法益層面來說，該等行為可對傳統上應受到刑法保護的法益構成危險，此方面的法益包括名譽、人身自由、性自由、性自決、受保護的私人生活、財產或法律關係上的穩定。另一方面，基於資訊科技對人、社會及經濟的重要性，容許將資訊本身的安全設定為應受刑法保護的獨立法益，目的是確保公共電信網絡的安全，以及加強人們使用這些網絡的信心[6]。

b) 就資訊工具對具刑法意義的法益可能構成危險而言，人們普遍認同這些工具本身的特點，如迅速性、周密性、可靠性、技術性及適應性，已賦予其潛在的狡詐及隱匿的性質，因而使之成為危害受刑法保護的基本法益的適合工具[7]。

---

[5] 見劉守芬、葉慧娟：《網絡越軌行爲犯罪化正當性探討》，載張平主編《網絡法律評論》（第六卷），法律出版社 2005 年。

[6] 見 Lorenzo Picotti, 'Biens juridiques pretégés et techniques de formulation des incriminations en droit pénal de línformatique', in *La Cybercriminalité,* Revue Internationale de Droit Pénal, Vol. 77 (2006), pp. 525-568.

[7] 見 Ricardo Mata y Martin, 'Criminalidad Informática: una introducción al Cibercrimen', in *Temas de*

c) 在刑法的補充性原則方面，國際上的趨勢是運用刑法來保護有可能受到資訊及通訊科技領域中的不法行為影響的法益。雖然在資訊安全方面已存在一些機制，包括通訊網絡本身的結構、訂定互聯網服務中介人的民事責任，以及由使用者本身為自我保護而採用的一些系統等，但這些機制不夠嚴厲，對於防止資訊工具被濫用而言，單靠這些機制本身是起不了必需的阻嚇作用。

基於以上理由，委員會得出結論，為維護法律制度中的基本法益，有必要將影響或利用資訊及通訊科技的行為刑事化。這也對於在澳門法律體制中引入一般被稱為電腦犯罪的規定提供了合理解釋。

3. 電腦犯罪可被理解為：*所有利用電腦系統來達到犯罪目的的行為或此犯罪行為的對象就是電腦系統*[8]。

根據上述的定義，可通過確定兩大類的犯罪來界定現著手進行立法的事宜的範圍，有關的犯罪均涉及電腦系統[9]：第一類，以電腦系統*為犯罪工具*，第二類，電腦系統是犯罪對象。

3.1. 被納入電腦犯罪定義中的第一類刑事不法行為，是由法律秩序所側重的利用資訊工具實施犯罪的不法行為所組成，因為法律秩序認為利用資訊科技作案會對欲保護的法益構成更大的危險。在此

Direito da Informática e da Internet, Coimbra Editora (2004), pp.197-236.

[8] 見 Garcia Marques & Lourenço Martins, *Direito da Informática*, Almedina (2000), p. 494.

[9] 根據法案第二條（一）項所載的定義，“電腦系統”是：任何獨立的裝置或一組互相連接或相關的裝置，當中一個或以上的裝置按照程式執行自動處理電腦數據資料的工作；

情況下，有關犯罪的實施是受到規限的，即有關行為必須透過在有關罪狀中特定的工具而作出[10]。由於利用資訊科技實施犯罪會產生特別的危險，澳門的法律秩序於《刑法典》中，將詐騙（第二百一十一條）和資訊詐騙（第二百一十三條）作出區分。後一種犯罪的犯案工具就是利用電腦系統。

在電腦犯罪的定義中，只應包括以上所指的情況。在《刑法典》[11]及刑事單行法律[12]中所規定的大多數罪狀，對於科技而言，均以中性的方式訂定，即犯罪行為得以任何方式作出，包括利用電腦系統的方式。就這些沒有針對科技而制定的法律，利用電腦系統作為犯罪工具在刑事上是沒有意義的，且可與利用任何其他工具實施犯罪相提並論[13]。

例如侮辱罪（《刑法典》第一百七十五條），是指某人將侵犯他人名譽或別人對他人觀感的事實歸責於他人，即使以懷疑方式作出該歸責，又或向他人致以侵犯其名譽或別人對其觀感的言詞，至於

[10] 例如，分別於法案第十條及第十一條中規定的電腦偽造罪及電腦詐騙罪。

[11] 例如，恐嚇（第一百四十七條）、脅迫（第一百四十八條及第一百四十九條）、販賣人口（第一百五十三條-A）、淫媒（第一百六十三條及第一百七十條）、誹謗（第一百七十四條）、侮辱（第一百七十五條）、侵犯對已死之人之思念（第一百七十九條）、侵犯行使公共當局權力之法人（第一百八十一條）、侵入私人生活（第一百八十六條）、違反保密（第一百八十九條）、勒索（第二百一十五條）、煽動戰爭（第二百二十九條）、煽動滅絕種族（第二百三十一條）、種族歧視（第二百三十三條二款 b 項）、使用虛假證明（第二百五十條）、侵犯宗教感情（第二百八十二條）、公然教唆犯罪（第二百八十六條）、公然讚揚犯罪（第二百八十七條）、以實施犯罪恐嚇（第二百九十四條）、煽動以暴力變更已確立之制度（第二百九十八條）、煽動集體違令（第三百條）、脅迫本地區之機構（第三百零三條）、侮辱官方象徵（第三百零九條）、縱放被拘禁之人（第三百一十三條 b 項）或違反司法保密（第三百三十五條）等罪。

[12] 例如，清洗黑錢（第 2/2006 號法律第三條）、煽動叛亂及竊取國家機密（第 2/2009 號法律第四及第五條）、層壓式傳銷（七月十五日第 6/96/M 號法律第二十八條-A）、資助及煽動恐怖主義（第 3/2006 號法律第七及第八條）等罪。

[13] José de Oliveira Ascensão, 'Criminalidade informática', in *Direito da Sociedade da Informação,* Vol. II, Coimbra Editora (2001), p. 203.

是透過哪類工具作出該歸責，則不重要。然而，法律體制亦容許考慮所利用的犯罪工具作為衡量已造成的損害，如《刑法典》第一百七十七條所規定的，如侵犯是藉著便利其散布的方法作出，則刑罰加重。

由於上述作為犯罪的手段在刑事上是沒意義的，因此，該等犯罪不會納入電腦犯罪的範圍內。即使是利用資訊工具實施犯罪，但受保護的法益仍維持不變，因此，無需為實質回應該新模式的犯罪設定新的罪狀。[14]

3.2. 除了將電腦系統作為犯罪工具的情況外，還有其他情況，即將電腦系統本身作為犯罪活動的對象或目標。此類情況就是可被納入電腦犯罪的第二類犯罪。

作為承認電腦系統在當代生活中的重要性及該系統所面對的風險的一種回應[15]，可將資訊科技的安全、保密性及完整性定為應受刑法保護的獨立法益[16]。為使社會能充分應用資訊及通訊科技的各種便利，必須在虛擬世界內存在一種安全文化來保護個人資料及隱私，從而加強人們對資訊世界的信心[17]。將科技應用於個人生活、社會及

---

[14] 見 Emeline Piva Pinheiro, *Crimes virtuais: Uma análise da criminalidade informática e da resposta estatal*, p. 25, disponível em http://www.pucrs.br/direito/graduacao/tc/tccII/trabalhos2006_1/emeline.pdf.

[15] Quanto aos tipos de riscos detectados na internet, *vd. Symantec Global Internet Security Threat Report–Trends for 2008,* Vol. XIV (2009), 查閱：http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf 。

[16] 見 Lorenzo Picotti, 'Biens juridiques pretégés et techniques de formulation des incriminations en droit pénal de linformatique', *cit.*, pp. 560-563。

[17] 理由陳述。

經濟上已成為普遍的現象，而所有電腦系統均載有一套關於其使用者的寶貴資料，正因如此有人想透過不正當獲取及操縱該等資料來圖利。因此，電腦系統的使用必須是安全的，系統中所載的資料的完整性必須得到保障，且有關內容及其使用者的保密性亦須受到尊重。眾所周知，沒獲許可的第三人利用一些特定軟件亦可進入有關電腦系統或其部分內，尤其是當電腦連接到互聯網時。此一事實可產生具不同程度危險性的後果，可以是單純知悉有關電腦系統中所載的資料、編製可作商業用途的涉及有關電腦使用者行為的簡介、侵犯電子通訊、或違反保護電腦系統的安全措施，甚至可以是散播病毒性的程式，尤指電腦病毒，目的是改變或毀壞電腦數據資料、影響電腦程式的運作或干擾電腦系統或電腦程式的正常運作[18]。

由於科技的最新發展，需要對於受法律保護的新法益進行獨立規範，同時，人們已經意識到一些特定行為能對該等法益產生影響，而現有的法律規定不能夠為該等法益提供必需及適當的保護，這就意味著有必要在犯罪定義範圍內，對以電腦系統為犯罪活動對象的行為訂立新的罪名。

4. 將涉及電腦的不法行為定為犯罪是國際性趨勢，眾多國家和地區已就電腦犯罪訂定了特殊的刑事規範[19]。由於電腦犯罪不受國界或政治因素所限，不同的法律秩序在打擊這類犯罪時採用相對統一的刑事規範，顯得尤為重要。

---

[18] 見 Esther Morón Lerma, *Internet y Derecho Penal: 《Hacking》y otras Conductas Ilícitas en la Red*, 2ª ed., Editorial Aranzadi (2002), pp. 29-45。

[19] 見 Pauline C. Reich (ed.), *Cybercrime & Security, Oceana Publications* (2009).
皮勇：《網絡安全法原論》，中國人民公安大學出版社，2008 年，第 445-484 頁。

現正審議的法案，與很多地區和國家包括中國內地、香港、台灣、新加坡、葡萄牙、德國及美國所採取的立法手段的方向是相同的，且如理由陳述所言，是經參考歐洲委員會《打擊網絡犯罪公約》後編製的。

《打擊網絡犯罪公約》於二零零一年十一月二十三日在布達佩斯簽訂，並自二零零四年七月一日起於國際法律秩序中生效。雖然是歐洲委員會內簽訂的一份國際法文書，但不屬該區域性國際組織成員的國家亦可加入。現時，已有四十六個國家[20]簽署了這份布達佩斯公約，而經批准程序後公約已於其中二十六個國家[21]生效。

法案的制定以在電腦犯罪方面最重要的國際法文書為依據，這點十分重要。雖然澳門特區因沒有加入該公約而不受其約束，但仍自願追隨公約所倡議的其中一個基本目標，即從實體刑法層面作出立法上的配合，這對打擊此類新型犯罪起著關鍵的作用，將有利於在有關事宜上的國際合作，尤其在刑事司法互助方面。

當澳門將侵犯資訊的安全、完整性及保密性的行為訂為犯罪，並採取與其他法律秩序相類似的規定時，就具備更有效的法律工具，以偵查大多涉及多個國家的電腦犯罪。事實上，“當某些與電腦

[20] 當中有四個不是歐洲委員會的成員國：南非、加拿大、日本及美國。
[21] 公約於下列歐洲委員會成員國的法律秩序中生效：亞爾巴尼亞、德國、亞美尼亞、波赫、保加利亞、克羅地亞、塞浦路斯、丹麥、斯洛伐克、斯洛文尼亞、愛沙尼亞、芬蘭、法國、荷蘭、匈牙利、冰島、義大利、拉脫維亞、立陶宛、前南斯拉夫馬其頓共和國、摩爾多瓦、挪威、羅馬尼亞、塞爾維亞及烏克蘭。此外，公約亦於美國（非歐洲委員會的成員國）生效。

有關的行為被某個國家的法律訂為犯罪，而其他國家的法律卻沒有這樣的規定時，可能會導致無法合作偵查犯罪，無法將罪犯繩之於法。也就是說，當某犯罪者透過三個、四個或五個國家傳達其通訊，之後有關後果才發生在受害人身上時，只要其中一個國家的法律未能配合，便足以為罪犯提供擋箭牌，讓其規避其他國家執法者的追蹤”[22]。在一般的法律秩序中，針對與電腦有關的不法行為在刑事上存在一定程度的統一規範，這與《打擊網絡犯罪公約》的目標相符，且能消除妨礙在打擊這類犯罪方面的國際司法合作機制全面運作的其中一個重大障礙。這個合作，以各地之間對應受刑法保護的價值存在共識為前提，而這個共識體現於雙重處罰原則，即*引致提出刑事司法互助請求的違法行為，按照請求方及被請求方的法律，均應可科處刑事處分*[23]。實體刑法在電腦犯罪方面的統一規範，正反映了這個共識的存在。

5. 為確保法律秩序不受與電腦有關的犯罪所侵害，有必要訂定基本的法律框架，包括相關的實體刑法、有關搜索及扣押的程序法以及證據法。[24] 實體刑法無疑是重要的，但單靠實體刑法可能不足以有效打擊電腦犯罪。由於電腦犯罪所採用的技術手段特殊，使這些犯罪具有“偵查難等特點，傳統的打擊犯罪方法面對在互聯網上所實施的虛擬行為時顯得束手無策”[25]。 事實上，互聯網信息的散播迅速，犯罪主體難於辨識，實施犯罪的有形證據不多且證據易於銷毀，

[22] Peter Csonka, 'The Council of Europe Convention on Cyber-Crime: A Response to the Challenge of the New Age', in *Cyber-Crime – The Challenge in Asia, cit.* (2005), p. 306.
[23] 第 6/2006 號法律第六條第一款。關於澳門對雙重處罰原則的適用範圍，可參閱第一常設委員會就《刑事司法互助》法案編製的第 2/III/2006 號意見書：http://www.al.gov.mo/lei/leis/2006/06-2006/parecer_cn.pdf.
[24] Peter Grabosky, 'The Global Cyber-Crime Problem: The Socio-Economic Impact', *cit.* (2005), p. 50.
[25] 理由陳述。

此外，眾所周知，電腦犯罪的偵查工作面對極大的困難，主要體現於以下方面[26]：

1）難以找出違法行為人；

2）嶄新科技加大了偵查的難度；

3）出現實施犯罪的新技術；

4）使用資訊密碼的技術普及；

5）難以確定實施不法行為的時間；

6）受害人不合作。

5.1. 法案除了在澳門的法律秩序引入新類型的犯罪外，還訂定旨在利於偵查電腦犯罪和偵查透過電腦系統進行犯罪的刑事訴訟規定，以及建立一個搜集和保存任何犯罪的電子證據的特別制度。

委員會同意有需要就電腦犯罪訂定專門的刑事訴訟規定。這些規定能使刑事偵查的傳統方法與新的科技，尤其是易於隱藏犯罪行為人身份和毀滅數碼載體內的證據的科技相適應。

很明顯在現代社會，在個人權利和安全需要兩者之間持續出現一種張力，當欲打擊的現象超越傳統犯罪的模式時，張力就越大。然而，打擊這類犯罪的困難和犯罪時所利用手段的特點，均不得成為取替澳門特區現行法律制度的結構性原則的理由。因此，法案必須在體現刑事偵查效率方面的安全和公正價值與對個人權利、自由和保障

[26] 馮文莊，由現實到虛擬世界 - 虛擬（網絡）社區生活之若干刑事問題研究，澳門大學法學院（2005）。

的尊重之間取得平衡。委員會認為適宜為打擊這種犯罪現象訂定專門的措施，但絕不能以此為理由，訂定近乎“例外情況”的制度，容許在法治社會的一般框架規定以外來打擊。此處的一般框架規定就是澳門特區為內部保安活動所訂定的綱要法，而打擊犯罪就是此法範圍內所規範的事宜[27]。

5.2. 在細則性討論本法案時，所提出的疑問是關於法案內的刑事訴訟規定和為了使電腦犯罪的偵查更有效率而向有權限當局授予權力的問題。一方面是由於法案內的特別制度與《刑事訴訟法典》一般補充制度之間的關係不確定，另一方面是由於擔心所建議的特別制度可能會過分限制在憲制層面訂定的市民的權利、自由和保障。

5.2.1. 就法案與《刑事訴訟法典》的關係，委員會有機會了解提案人的立法意向。提案人重申法案並非為了取消關於取證方法的一般制度，尤其是關於搜索、扣押和截取或透過電腦系統或遠程信息處理系統進行會話錄音或通訊的權限。因此，司法當局採取這些行動的權限，以及刑訴法規定的保護依法受保護的秘密的制度按照一般規則受到確保[28]。法案訂定的證據迅速保存制度只容許以數碼格式儲存的犯罪證據得以保存。法案規定由刑事警察機關[尤其是司法警察局，第 5/2006 號法律第七條第一款（十）項規定，司法警察局獲授予調查與資訊有關的犯罪的專屬職權]決定採取這些緊急措施，而在接獲有權限司法當局命令之前採取這些措施具有例外性質，即如遇有緊急

[27] 見第 9/2002 號法律和第二常設委員會關於《澳門特別行政區內部保安綱要法》法案的第 4/II/2002 號意見書。

[28] 見 Paulo Dá Mesquita, *Direcção do Inquérito Penal e Garantia Judiciária,* Coimbra Editora (2003).

情況或如有延誤可對重大價值的法益構成嚴重危險的情況，這完全與《刑事訴訟法典》本身規定的搜查、搜索（第一百五十九條第四款）和扣押（第一百六十三條第四款）制度一樣。委員會和提案人就法案和《刑事訴訟法典》的特別關係意見一致，為此，委員會努力尋求方案使法案的條文能清楚明確展示法案的立法意圖。

5.2.2. 關於限制市民的權利、自由和保障，委員會認為法案沒有扭曲澳門特區法律秩序的基本原則，也沒有純因這一法律的訂定而包含可損害《基本法》規定的權利、自由和保障的機制，尤其是在言論自由、私隱和通訊秘密的層面上。在這一方面，法案得以就各種價值取得平衡。

a) 首先，法案沒有意圖限制市民的言論自由。就刑事實體法方面，理由陳述特別對此作出闡述，指出"值得强調的是，本澳市民依法享有言論自由，這項基本權利是受到《基本法》保障的，所發表的言論，不論是否透過互聯網進行，僅當違反法律的明文規定，方會受到處罰，本法案並無就涉及言論自由的任何事宜訂定新的罪狀或作出更多的限制。"而就刑事訴訟法而言，法案訂定的偵查權力，是基於這類犯罪的性質和特徵以及予以打擊的需要。證據保存措施不會使截取透過電腦系統傳送的通訊內容或訊息內容的資料成為正當的行為。

在澳門，《基本法》訂明澳門居民享有言論自由（第二十七條），亦規定除依照法律的規定及適用於澳門的公約，

尤其是《公民權利和政治權利國際公約》，不得限制該自由（第四十條）。該公約亦有相同的規定，在其第十九條中，訂定言論自由的行使得受某些限制，但這些限制只應由法律規定並為尊重他人的權利或名譽及保障國家安全或公共秩序，或公共衛生或道德的條件所必需。因此，言論自由在虛擬世界裏，應有其範圍，且應受到為任何通訊環境或方式設定的一般限制所約束[29]。

b) 其次，法案尊重市民的隱私權，所規定的措施是與迅速保存一般電腦數據資料有關，但被視為較嚴厲的措施亦只涉及路由數據資料[30]而已。這些資料是一種關於網絡上某通訊的路線的描述，由起點至終點，從而容許辨別某部電腦終端機於何時何日曾通過某一 IP 地址（互聯網協議的地址）進入互聯網。路由數據資料是由電腦於通訊鏈中所形成的數據資料，以便將通訊從發出地引領至目的地，是通訊本身的輔助資料，但不會顯示通訊的內容，亦不容許從中得知任何其他可曾有的通訊，更不會顯示可推斷出有關人士私人生活上的個人資料，例如習慣、行為標準、態度等資料[31]。因此，鑒於路由數據資料對調查電腦犯罪非常重要，

---

[29] 見 Mark Turner, 'Liberté d'éxpression, censure et intégrité sur l'Internet, in *Les Droits de l'homme dans de cyberspace,* Unesco/Economica (2005), pp. 31-46。
根據第二條（五）項規定，"路由數據資料"是指，*與透過電腦系統所作通訊有關的所有電腦數據資料，而該電腦數據資料是由構成通訊鏈的要素的電腦系統所產生，並顯示出通訊的來源、目的地、路徑、時間、日期、大小、持續時間或基本服務的類型。*

[31] 見 Pedro Verdelho, 'A Reforma Penal Portuguesa e o Cibercrime', in *Revista do Ministério Público, Ano 27, n.º 108 (2006),* pp. 117-120 及歐洲委員會關於《打擊網絡犯罪公約》的解釋性報告，葡文文本可到以下網址查閱：
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese-ExpRep.pdf。

因為通過這些資料可重建有關通訊的路線，故路由數據資料的取得並沒抵觸《基本法》第三十條及第三十二條，以及其他單行法規關於保障個人隱私權的規定[32]。

c) 最後，法案並沒有侵犯《基本法》第三十二條規定的通訊保密權。這項權利旨在防止通訊內容被不當知悉，不管通訊以何種方式進行，因為，"在資訊迅速發展的現代社會，包括利用任何通訊方式進行的信息交換，已成為一種重要的社會資源"。[33] 然而，這項權利是可受限制的：一方面，第三十二條本身已規定，在有關機關基於公共安全和追查刑事犯罪的需要，而依照法律規定對通訊進行檢查的情況下，可對通訊保密權加以限制；另一方面，《基本法》第四十條承認法律可對澳門法律體系中的權利作出限制，只要法律有所規定，且不與《公民權利和政治權利國際公約》、《經濟、社會與文化權利國際公約》及國際勞工公約根據該第四十條第一款規定適用於澳門的有關規定相抵觸。[34]

法案規定的機制，不容許警察當局進入透過電腦系統或遙距系統傳達的通訊內容，不論是電郵、SMS[35]短信、通過 VOIP[36] 系統進行的談話等。[37]

---

[32] 關於澳門法律制度中保護隱私權的原則，見第三常設委員會關於《*個人資料保護法*》*法案*的第 3/II/2005 號意見書，可到 http://www.al.gov.mo/lei/leis/2005/08-2005/parecer_cn.pdf 查閱.

[33] 《澳門基本法釋要》第 73-74 頁，楊允中著，2003 年澳門特別行政區政府法務局出版。

[34] 就澳門對權利的限制制度，可參閱第二常設委員會關於《澳門特別行政區內部保安綱要法》法案的第 4/II/2002 號意見書。

[35] "Short Message System".

[36] "Voice Over Internet Protocol".

[37] 參閱 Armando Veiga/Benjamim Silva Rodrigues, *Escutas telefónicas – Rumo à Monitorização dos Fluxos Informacionais e Comunicacionais Digitais*, 2.ª ed., Coimbra Editora (2007).

如需進入，應依循《刑事訴訟法典》對電話監聽所訂定的制度：法典第一百七十五條將該法律制度延伸至*以有別於電話之其他技術方法傳達之談話或通訊*。這樣，對數碼通訊內容進行監控的可能性是本法案範圍以外的事，且這種監控只能在內部安全受嚴重威脅的情況下才能作出。只有在面對這種威脅的情況下，為了集體安全或全體居民的安寧，某些人的個人權利才應讓步。[38]

5.2.3. 要強調的是，法案關於迅速保存電腦數據資料的訴訟制度是針對具體的刑事訴訟程序。保存資料就是將一些已存在且被儲存起來的資料加以保存，以免其質量或現狀變更或受損。資料的保存旨在將儲存在某一電腦系統中的數據資料不被觸動及保持安全。

第十六條規定的特別措施適用於經數據資料持有人，例如服務提供者，收集並存檔的電腦數據資料，因此，這些措施並不適用於即時收集的路由數據資料，亦不適用於保存未來的路由數據資料或即時查閱通訊的內容[39]。此外，現建議的措施是針對具體個案的調查且只在有關情節顯示有需要時方可採用。

5.2.4. 基於上述理由，委員會認為法案所載的規定並不違反市

[38] 電腦通訊的管制亦可按第 9/2002 號法律《澳門特別行政區內部保安綱要法》第十八條的規定進行：如有強烈跡象顯示內部保安因犯罪活動而受到擾亂，得按照《刑事訴訟法典》規定實行通訊管制。參閱第二常設委員會關於《澳門特別行政區內部保安綱要法》法案的第 4/II/2002 號意見書。

[39] 見前述解釋性報告。

民享有的權利、自由及保障。然而，委員會亦清楚知道，打擊具特殊性的電腦犯罪（不論是電腦犯罪，抑或是有組織犯罪、跨境犯罪、“白領犯罪”或恐怖主義犯罪）可能會令執法者傾向攬權，行使一些法案或立法意向沒有賦予的特別權力。委員會認為，是次立法並無意設定一個全面監控電腦系統及遠程信息處理系統中可公開獲取的內容，或通過這些系統進行的通訊內容。預防電腦及遠程信息犯罪的措施只應用於警察調查的目的，且僅限於預防某一具體危險或遏止某一特定違法行為必需範圍內，而不得具有一般預防的作用。委員會深信將來執行打擊電腦犯罪法的人員必定以法治主導原則來判斷其行動範圍。

四、細則性審議

除進行了上述的概括性審議之外，委員會還根據《立法會議事規則》第一百一十七條的規定，對法案所規定的具體解決方案是否切合法案所訂的原則進行了細則性審議。

委員會與提案人緊密合作，完成了法案細則性審議。在審議期間，主要討論的問題以及引入的主要修改是：

1－ 標的（*第一條*）

在本法律標的的方面加入相應規定，目的是讓人們即時了解本

法所載的整套規定的具體範圍。因為委員會認為，法案最初文本的第一條的行文只是本法律標題的重複，故未能發揮其作為標的的作用，而在新的行文中則說明了本法律旨在訂定電腦犯罪（刑事實體法），以及設立就實施犯罪而於電子載體中搜集證據的制度(刑事訴訟法)。

2– 定義（*第二條*）

關於定義方面的規定，目的是透過建立統一的概念來規範統一本法律的理解。涉及資訊科技的事項適宜採用定義方式，因為科學本身的概念及資訊技術均具有高技術性特點，定義的規定有助解讀者及應用者理解本法律所採用的術語。因此，本法案載有一條關於定義的規定，而這些定義與布達佩斯《打擊網絡犯罪公約》中所載的定義十分接近。

根據第二條（一）項的規定，“電腦系統”是指：“任何獨立的裝置或一組互相連接或相關的裝置，當中一個或以上的裝置按照程式執行自動處理電腦數據資料的工作”。

法案新文本中，對該定義作出了若干修改，尤其是刪去了關於能執行自動處理電腦數據資料工作的裝置的列舉[40]。首先，由於所列舉的只限於目前已知的科技，因此，隨著新裝置的面世，列舉的裝置便會過時，本法律亦隨之變得脫節。刪去列舉這個部分目的是使本

[40] 法案最初文本關於電腦系統的定義是，“電腦系統：任何獨立的裝置或一組互相連接或相關的裝置，尤其是獨立個人電腦、數碼個人備忘記事本、數碼機上盒、個人視訊錄影機、流動電話，當中一個或以上的裝置按照程式執行自動處理電腦數據資料的工作”

法律在科技層面上儘可能保持中性。另一方面，所列出的裝置亦有可能引起理解上的疑問，因而導致應用本法律時出現不太正確的情況，特別是流動電話這個提述。例如，只容許通過模擬技術進行語音通訊的流動電話，便不包括在本法律的適用範圍內。因為此類流動電話既不在現訂定的罪狀的適用範圍，亦不包括在現建議的訴訟措施中。須知，現今科技的發展容許流動電話具備遠不只語音通訊一項功能，還可具備其他一系列的功能。如具備處理數據的功能，已不只是“流動的電話”，而是“流動的電腦終端機”。具備此功能的流動電話就包括在電腦系統的定義內。最後，刪除有關裝置的列舉亦是基於布達佩斯公約中關於電腦系統的定義並不包含任何科技應用的舉例。

歐洲委員會關於《打擊網絡犯罪公約》的解釋性報告中對電腦系統概念的解釋有助理解本法案對電腦系統的定義。按照該公約，電腦系統是“由用於自動處理數碼數據的硬件和軟件組成的設備，可包括輸入、輸出及儲存的裝置，可獨立運作或與其他類似的裝置在網絡上連接。‘自動’的意思是無需人手直接介入，而‘數據處理’就是，通過執行一個電腦程式來操作載於電腦系統內的數據”。

電腦系統的定義中提及到電腦數據資料，數據資料的定義載於第二條（二）項（此定義並沒有任何修改），內容是：*是事實、資料或概念的任何展示，而該展示是以一種可於電腦系統內處理的形式為之，包括可使電腦系統具執行功能的程式*。此定義是來自公約的，而公約就採用了國際標準化組織（ISO）關於數據的概念。根據該定義可將電腦數據資料理解為，轉化成二進制語言的數據資料，也就是

說，可由電腦處理的語言，包括事實、信息或概念[41]。

在定義方面，法律的新文本刪去了載於最初文本第二條（六）項關於“內容數據資料”的定義。內容數據資料是電腦數據資料中關於通訊內容或訊息內容的資料。由於在整份法案的規定中並沒有對此概念作出提述[42]，因此已予刪除。需要強調的是，第十六條規定的特別措施容許迅速保存所有電腦數據資料[43]，但不容許查閱有關的內容，除非屬《刑事訴訟法典》規定的制度範圍。第十六條第一款（二）項容許查閱某些電腦數據資料的規定亦只涉及路由數據資料而已。因此，若加入關於內容數據資料的定義可能會誤導解讀者及應用者，誤以為特別措施亦可包括查閱通訊內容資料，但此點卻不是本法案的立法原意。

3 – 補充法律（*第三條*）

在分析第三條的過程中，曾考慮是否有需要將之納入本法案的規定內。

第一款規定“《刑法典》的規定，補充適用於本法律所規定的犯罪”。由於《刑法典》第八條已有一般的規定，第一款就顯得有點多餘。《刑法典》規定，“本法典之規定，補充適用於可為特別性質之法例所處罰之事實，但另有規定者除外”。因此，嚴格來說，特

[41] 見 Pedro Verdelho, 'Cibercrime', in *Direito da Sociedade da Informação,* Vol. IV, Coimbra Editora (2003), p. 361.
[42] 除了第二條（四）項附帶提及該概念作爲“基本資料”定義的消極界定。
[43] 第十六條第一款（一）項首部分。

別法無需重複一般法已規定的事項，除非想將之排除[44]。然而，委員會認為說明《刑法典》是補充適用的，畢竟有助於加強了解作為特別法的本法案與一般刑法之間的關係。

至於第二款，目的是確保其他與保護特殊電腦系統有關的犯罪規定維持不變，尤其是第 8/2002 號法律（澳門特別行政區居民身份證制度）第十四條及第 8/2009 號法律（澳門特別行政區旅行證件制度）第十五條規定的旨在處罰攻擊身份證明文件及旅行證件集成電路及相關資料庫安全的犯罪規定。

4 - 不當進入電腦系統（*第四條*）

歐洲委員會關於《打擊網絡犯罪公約》的解釋性報告[45]中指出，不當進入電腦系統基本上是包括涉及對電腦系統安全（即保密性、完整性及可使用性）造成危險及攻擊的違法行為。保護反映了相關組織及人們能在安心無慮的情況下管理、操作及控制自己的電腦系統的需要。預防未經許可進入的最可行辦法顯然是引入及發展有效的安全措施。然而，一個覆較為廣泛的回應辦法亦必須包括刑法關於威脅及所採用措施的規定。

“進入”一詞是指，進入整個或部分電腦系統（硬件、組件、儲存於系統內的數據資料、目錄、路由數據資料及內容數據資料）。“進入”是包括侵入可通過公共電信網絡進入的電腦系統，或侵入同

[44] 見前述作品，José de Oliveira Ascensão, ‘Criminalidade informática’, p. 205。
[45] 前述解釋性報告（第 44-50 點）。

一網絡內某個電腦系統，例如局部區域網路（LAN）或某一組織的內部網路（例如企業的私人網路）內的電腦系統。

"未經許可"的進入方予以處罰，因為沒有許可就會構成不當進入，換句話說，如經有關電腦系統或其部分的所有人或權利人許可的進入（例如對有關電腦系統進行測試、保護或維修）就不是犯罪。此外，如進入一個公開讓公眾自由進入的電腦系統亦不是犯罪，因為該進入是一種權利。

該犯罪的主觀要素僅限於直接故意（意圖），故此因過失而作出的不當進入不可予以處罰。然而，該犯罪必須為基於特定故意而實施，即有關進入必須存有"任何不正當意圖"，因此，只要行為人明知未經許可且存有任何不正當意圖而進入整個或部分電腦系統即屬違法。法案新文本改變了上述的主觀要素，將不當獲取電腦數據資料的意圖刪除了，原因是，此意圖屬另一獨立犯罪的部分，即第五條規定的犯罪。

基於上述主觀要素，進入的犯罪行為與其他經進入有關電腦系統後而實施的犯罪構成競合，尤其是獲取、使用或提供電腦數據資料等犯罪（第五條），或不當截取罪（第六條）、損害電腦數據資料罪（第七條）、干擾電腦系統罪（第八條）、電腦偽造罪（第十條），又或電腦詐騙罪（第十一條）。

如果進入是藉違反保護有關電腦系統的安全措施而作出者，

例如進行關鍵詞解碼或破釋加密內容，則屬加重不當進入罪，因為此行為應受特別的譴責，而相對的加重刑罰就是普通的不當進入罪刑罰的加倍。

普通的不當進入罪是準公罪：非經告訴不得進行刑事程序，而具正當性提出告訴的人就是被侵犯的電腦系統的擁有人。委員會認為適宜讓受害人自行決定是否要行使告訴權，因為在有些情況下如將電腦系統的弱點公開可能對其擁有人所造成的損害比有關犯罪行為本身所造成的損害更大。但加重的不當進入罪，基於公共利益理由可設定為公罪。然而，實際上，如系統擁有人不告訴，司法當局未必知道有加重不當進入罪的發生。

5 - 不當獲取、使用或提供電腦數據資料（*第五條*）

從比較法的層面而言，相對關於電腦犯罪的一般立法經驗，以及布達佩斯《打擊網絡犯罪公約》所規定的一系列犯罪，第五條規定的犯罪是本澳法律的一項革新。然而，此項創新只是最起碼的共識並且不妨礙各國在國內法中將其他行為訂定為犯罪[46]。

將有關行為訂定為犯罪目的是保護每一個人資訊方面的私隱權及自決權。第五條規定的犯罪，其罪狀的客觀要素是，獲取、使用或向他人提供屬於別人的電腦數據資料。立法者希望，即使是從正當途徑，即經許可進入而得到的該等數據資料亦受保密的保障。無論進

[46] 見前述解釋性報告第 34 點。

入是否正當，未經有關數據資料擁有人的許可，行為人不得獲取、使用或向他人提供此等資料。

“獲取”是有別於“進入”，“獲取”是指不論行為人是透過竊取抑或製作副本的方法，將電腦數據資料弄到手。重點是，行為人透過獲取便能控制不屬其擁有的數據資料。“使用”意味行為人利用該等資料，也就是說，從中得益。然而，本法案無意將純粹屬個人使用非本身所擁有的電腦數據資料納入本犯罪的罪狀中。因此，構成第五條第一款訂定的“使用”罪，行為人必須在與第三人接觸時，對該等資料作出利用，不論是否存在經濟利益亦言。基於此，分發的行為包括在內，即將別人的數據資料發送予第三人，或與第三人分享，又或出售予第三人。“向他人提供”則涉及支配，即將別人的數據資料變成無數第三人可查閱的資料的行為，尤其是將有關資料上載到不同的網站（*upload*）。

根據第二款的規定，不當獲取、使用或提供電腦數據資料的罪行如涉及某類受特別保護的數據資料，則屬加重罪。因此，涉及敏感資料[47]或受法律保護的任何類別的秘密（尤指職業、司法、醫務、國家或澳門特區、宗教或商業等秘密）適用的刑罰是普通犯罪刑罰的加倍。然而，本條所規定的普通罪抑或加重罪均屬準公罪。

曾有意將分散於法案最初文本多條規定中涉及使用電腦數據資料的處罰歸納在現正分析的犯罪中。基於此理由，法案最初文本第

[47] 第 8/2005 號法律（個人資料保護法）第七條採用的概念。

六條第二款涉及使用不當截取電腦數據資料的加重情況已被刪除。委員會認為以統一的方式處理所有濫用電腦數據資料的情況較按獲取電腦數據資料的方法來區分有關使用更為恰當，更何況原適用的刑幅之間存在重大差異[48]。

6 - 不當截取電腦數據資料（*第六條*）

將有關行為訂定為犯罪目的是保護源自受《基本法》第三十二條保護的通訊秘密而產生的資料通訊專有權及隱私權。一如禁止對人與人之間的電話談話進行監聽及錄音一樣，本規定亦禁止不當截取於電腦系統內或電腦系統之間進行的數據資料的通訊[49]。

所謂截取，是指利用技術手段取得載於某電腦系統內的資料的行為。“利用‘技術手段’進行截取，是指透過直接的方法，即透過進入及使用電腦系統，或間接的方法，即利用截取信息或非法監聽的電子裝置，對通訊內容進行監聽、監控或監視，以及獲取資料內容。截取亦可包括錄音。這裏的技術手段，既包括在傳輸線路上安裝技術設備和使用收集及收錄無線通訊內容的裝置，也可包括使用密碼（passwords）及訪問代碼。利用技術手段是一項限制性的要件，以

[48]處最高五年徒刑，或科最高六百日罰金（最初文本第六條第二款）及其他情況處最高一年徒刑，或科最高一百二十日罰金（普通犯罪），以及處最高二年徒刑，或科最高二百四十日罰金（加重罪。）

[49]根據前述的解釋性報告第 55 點，“以數據傳送方式進行的通訊可在單一的電腦系統內部進行（例如從中央處理器（CPU）向顯示器或打印機傳輸資料，或可以在屬同一人擁有的兩個電腦系統之間傳輸資料（兩部電腦之間的通訊），又或可以在人和電腦之間，如自然人通過鍵盤傳輸資料”。

避免過度處罰[50]。” 所指的技術手段可涉及應用電磁儀器、聲學設備、機械工具或其他工具。

第六條第二款對犯罪未遂作出規定（第七條、第八條、第十條及第十一條也有如此規定）。在對本法案進行細則性審議時，委員會有鑒於若干犯罪未遂對受保護的法益所構成的危險程度，曾考慮是否需要及適宜對該等犯罪未遂的行為作出處罰。經分析後，並根據布達佩斯公約就界定應受處罰的犯罪未遂所訂定的標準，法案新文本明確規定不當截取、損害電腦數據資料、干擾電腦系統、電腦偽造及電腦詐騙的犯罪未遂是受處罰的。屬加重罪的情況，如果最高刑罰是超過三年徒刑時，則適用《刑法典》第二十二條關於犯罪未遂之可處罰性的一般規則。

7 - 損害電腦數據資料（*第七條*）

訂定第七條的犯罪目的是，給予電腦數據資料與有形財產關於遭受明顯毀損方面所享有的相同保護[51]。在此情況下，受保護的法益是儲存於電子系統內的數據資料的完整性及正常運作或正確使用[52]。關於主觀要素方面，要求的只是一般的故意。

為幫助了解第七條第一款所規定的不同行為，“‘損壞’及‘破壞’雖然屬重疊行為，但主要是指，負面更改數據或程式的完整

[50] 前述解釋性報告第 53 點。
[51] 見《刑法典》第二百零六條（毀損）。
[52] 前述解釋性報告第 60 點。

性或資料內容。‘消除’電腦數據資料，則等同毀滅有形財產，因為消除會刪去有關數據及使之無法辨認。‘刪除’電腦數據資料是指，所有或任何阻止或終止向有權進入電腦或儲存數據資料載體的人提供數據資料的行為。‘更改’意味將已存在的數據資料變更[53]。”

損害罪會因應所造成的財產損失價值（第三款及第四款）訂定為加重罪。“巨額財產損失”及“相當巨額財產損失”的定義於《刑法典》中有所規定，分別載於第一百九十六條(a)項及 (b)項。本條第四款（二）項亦為損害罪訂出另一加重情節，但所依據的並不是所造成的財產損失價值，而是受損害資料的性質（具重要學術、藝術或歷史價值，又或對科技發展或經濟發展具有重大意義的電腦數據資料）。

不論是普通的損害電腦數據資料罪的刑罰，抑或是加重罪的刑罰均與《刑法典》分別於第二百零六條及第二百零七條規定的普通及加重毀損罪的刑罰是一致的。

8 - 干擾電腦系統（*第八條*）

訂定第八條的犯罪目的是，處罰故意阻止正當使用電腦系統的行為。本條受保護的法益是，運作正常的電腦系統其操作者及使用者的利益。“干擾”是指，所有或任何擾亂電腦系統正確運作的行

[53] 同上第 61 點。輸入惡性代碼，如病毒及惡性程式，例如人稱“特洛伊木馬”的程式，屬本犯罪的範圍，而因此行爲導致數據資料變更亦包括在內。

為，包括通過輸入、傳送、損壞、破壞、更改、刪除或消除電腦數據資料等方式作出的干擾[54]。

法案新文本降低了本條犯罪的刑罰（由原來的最高五年徒刑，或科最高六百日罰金變為處最高三年徒刑或科罰金）。此變更目的是，統一本法案所規定的不同普通罪[55]的刑罰，同時亦希望將普通的干擾電腦系統（第一款）與加重的干擾電腦系統（第三款）區分開。法案原文本並無如此區分，普通罪及加重罪的最高刑幅均為五年，只在最低刑幅有所區別。

9 - 用作實施犯罪的電腦裝置或電腦數據資料（*第九條*）

本犯罪的特定及獨立刑事違法行為是，某些蓄意利用電腦裝置或電腦數據資料來實施危害電腦系統或電腦數據資料的秘密性、完整性及可使用性等犯罪的行為。受保護的法益與第四條至第八條所保護的法益相同，只是對有關法益提前作出刑事保護，即對一些提供該等裝置予欲實施電腦犯罪的人的交易行為作出處罰。此制度相當於《刑法典》第二百六十三條關於侵犯通訊之工具的交易而訂定的制度。

第九條第一款要求特定的故意：無論實施本款規定的哪一個

[54] 同上第 65-66 點。
[55] 第六條至第十一條規定的罪在未加重前劃一科處處最高三年徒刑或科罰金。

行為，該行為亦必須涉及主要是為了實施電腦犯罪而設計或調整的電腦裝置或電腦數據資料。此外，單純占有不可處罰之，且“分發”及“向他人提供”的概念應分別理解為，將電腦數據資料發送予他人的行為，以及將裝置連線（online）供他人使用[56]的行為。

10 - 電腦偽造（*第十條*）

電腦偽造罪的設定，目的是給予電子文件與《刑法典》第二百四十四條及二百四十五條給予可觸知的文件，即紙質文件所規定的同類保護。

電腦偽造，是指未經許可製作或改製電腦數據資料，使之具有不同的證明力來影響以這些電腦數據資料所傳達的信息真實性為基礎的法律關係[57]。因此，要求虛假數據資料，是“可作證明之用，因此看起來能產生與被偽造的文件相同的效力。這裏所保護的，是法律交易的安全性及可靠性，尤其是作證明之用的文件，因為當通過虛假證明使人在法律關係中受欺騙時，被侵犯的法益就是有關的法律關係。如是者，電腦【偽造】罪只在偽造的‘文件’可作證明之用的條件下方會成立[58]。”本條規定適用於“被操縱的電腦數據沒有印製成文本但直接應用在其他電腦處理上的情況，例如銀行交易、會計業務，甚至付款。有關行為可使電腦將虛假文件當真正文件處理，就如

[56] 前述解釋性報告第 72 點。
[57] 同上第 81 點。
[58] Helena Moniz, *O Crime de Falsificação de Documentos – Da Falsificação Intelectual e da Falsidade em Documento,* Coimbra Editora (1999), pp. 270-271.

令某人將一份虛假文件當真正文件接受[59]。”

不論是電腦偽造罪（第一款）抑或故意使用偽造文件罪（第二款），法律要求特定的故意：意圖使人在法律關係中受欺騙（第一款），或意圖造成他人有所損失或為自己或第三人獲得不正當利益（第二款）。

兩項罪行均設有加重處罰，以行為人的特殊身份、虛假文件的特別價值（準用《刑法典》第二百四十五條訂定的分類）或涉及合格電子簽名的安全性（根據第 5/2005 號法律的規定）作為加重的情節。

為了統一不同電腦犯罪的處罰，一如對干擾電腦系統的刑罰所作出的調整一樣，法案新文本亦降低了本條規定的刑罰。同時，委員會亦認為電腦偽造的刑罰應與《刑法典》關於偽造文件的刑罰相同。因此，將最初文本中所載的刑罰降低後，普通偽造文件罪，不論文件的性質，科處最高三年徒刑或科罰金。如此調整能在刑事制度層面上取得更大的和諧。

11 - 電腦詐騙（*第十一條*）

第十一條訂定的電腦詐騙罪，屬侵犯財產罪：此罪的設立，目的是保護因受詐騙而有財產損失的人的財產（而並非電腦數據資料

[59] Manuel António Lopes da Rocha, 'A Lei da Criminalidade Informática', in *Legislação – Cadernos de Ciência de Legislação,* no.º 8, Instituto Nacional de Administração (1993), p. 72.

或電腦系統的所有人或使用者）。所規定的罪狀與現廢止的《刑法典》第二百一十三條所訂定的罪狀相類似，但刪去了於本法案第五條中規定的未經許可使用電腦數據資料的部分。本罪的客觀罪狀所包括的行為均涉及具有詐欺的意圖，為自己或第三人牟取不法利益，導致他人財產損失的操縱電腦行為。設定第一款（二）項所指的介入電腦數據資料處理的結果，目的是確保所有主要的操縱手段均包括在內，例如操縱硬件、阻止輸出數據資料到打印機，以及影響數據資料的登記或數據流，又或執行程式的序列[60]等行為。所謂不正確設定電腦程式（第一款（三）項），是指設定與原本的電腦程式目的相反的電腦程式，從而產生新的指令，導致原本的電腦程式產生明顯的相反結果[61]。

電腦詐騙有別於《刑法典》第二百一十一條規定的一般詐騙罪，因為電腦詐騙是一項執行上受到約束的犯罪。一般詐欺罪可通過行為人耍弄任何誤導或欺騙手段來實施，但電腦詐騙，則必須通過第一款列出的任一手段實施[62]。

12 - 刑罰的加重（*第十二條*）

第十二條第一款規定，如犯罪行為涉及澳門特別行政區公共實體的電腦數據資料或電腦系統，則第四條至第十一條設定的電腦犯

---

[60] 見前述解釋性報告第 87 點。

[61] 見 Paulo Pinto de Albuquerque, *Comentário do Código Penal,* Universidade Católica Editora (2008), comentário ao artigo 221.°, p. 609。

[62] 見 Manuel Lopes Maia Gonçalves, *Código Penal Português Anotado e Comentado,* 17ª ed. (2005), anotação ao artigo 221.°, p. 769.

罪的刑罰加重。刑罰的加重是為了加強對當局使用電腦的保護，即加強保護“公共實體的電腦系統或電腦數據資料的保密性及完整性”[63]。

第二款的規定，實際上將互網聯等同於《刑法典》第一百七十七條第二款及第一百九十二條（b）項規定的社會傳播媒介。這兩條條文分別規定，透過社會傳播媒介作出誹謗罪及侮辱罪，以及透過社會傳播媒作出《刑法典》第一百八十四條至第一百八十九條規定的侵犯受保護的私人生活罪的加重刑罰（第一百九十二條），因為透過該媒介，接觸到有關典型行為的人數會增加，因而擴大有關侵犯的有害影響。“社會傳播媒介”的定義包括印刷品、電台及電視台。雖然有種傾向將互聯網亦包括在該定義中[64]，但如此做法有可能引起關於該定義範圍的疑問。因此，為了避免在理解本法案方面出現疑問，法案第十二條第二款將互聯網與其他社會傳播媒介作出等同。然而，此等同僅當互聯網作為有關犯罪的典型行為的廣泛傳播工具時方適用，也就是說，藉互聯網廣泛傳播具侮辱性、詆毀性或侵入性的行為。因此，如果互聯網是作為純粹分發之用（例如透過電郵），則加重刑罰不適用之，但如果是作為提供構成有關罪狀的內容（例如將內容載入網站），則適用。在第一種的情況下，儘管有使用互聯網，但並沒有將之作為廣泛傳播犯罪行為之用。

還需指出，如果誹謗罪及侮辱罪，即使是以間接的方法透過互聯網作出，且被害人是《刑法典》第一百二十九條第二款（h）項

---

[63] 理由陳述。

[64] 見 Luís Brito Correia, *Direito da Comunicação social,* Vol. I, Almedina (2000), pp. 22-24，以及前述 Paulo Pinto de Albuquerquer 的作品, anotação ao artigo 183.º, p. 502。

所指的任一人，《刑法典》第一百七十八條的加重規定亦是適用的：由於《刑法典》第一百七十八條對第一百七十四條、第一百七十五條及第一百七十七條規定的刑罰作出加重，因此，通過互聯網對正在執行職務的公務員、教學人員、公共考核員、證人或律師作出誹謗及侮辱，或因其職務對之作出該等行為者，科處第一百七十七條第二款經第一百七十八條規定的加重刑罰（基於所使用的媒介），即第一百七十七條第二款的最低及最高刑罰均提高二分之一的處罰（基於受害人的特殊身份）。

13 - 刑事訴訟規定 — 一般規定（*第十四條*）

第十四條行文的修改，是爲了明確界定法案所載訴訟制度的範圍。這樣，擬就獲取及保存證據方面建立特別制度所針對的犯罪為：

1） 打擊電腦犯罪法規定的犯罪；

2） 透過電腦系統實施的[65]、載於《刑法典》及其他單行刑事法律的犯罪；

3） 涉及在電子載體搜集證據的任何犯罪[66]。

相對《刑事訴訟法典》而言，第十五條及第十六條是特別規定，如本法沒有特別訂明者，則適用《刑事訴訟法典》的規定。因此，法案維持刑訴法規定的一般適用原則。

[65] 例如於互聯網實施的誹謗罪。對於其他一些可透過電腦系統進行犯罪的例子，可參閱本意見書第 11 項及第 12 項註釋。

[66] 例如，對在恐嚇或貪污罪實施過程中交換的電子郵件的扣押，適用本法的規定。

14 - 扣押（第十五條）

該條最初行文規定，電腦系統、電腦數據資料儲存載體及電腦數據資料或電腦程式，均可採納作為證據。考慮到證據的合法性原則（《刑事訴訟法典》第一百一十二條），即“凡非為法律所禁止之證據，均為可採納者”的原則，既然法律沒有禁止獲取和使用電腦系統、電腦數據資料儲存載體及電腦數據資料或電腦程式作為證據，故無需作出以上的規定。將法案原來的第十五條第一款刪除，完全不影響法庭採納電子載體證據,或使用電腦系統或電腦數據資料作為證據的可能性。事實上，《刑事訴訟法典》第一百五十三條亦規定了電子程序複製物的證據價值。

法案新文本的第十五條第一款規定可直接或透過副本對電腦系統、電腦數據資料儲存載體及電腦數據資料進行扣押，作為獲取證據的方法。因此，《刑事訴訟法典》第一百六十三條、第一百六十八條及第一百六十九條所載的制度亦適用於電子證據[67]。

第十五條第五款明確規定，《刑事訴訟法典》（第一百六十四條及第二百三十五條）適用於扣押電子郵件或任何方式的私人電子通訊，例如短信（SMS），對此不設有任何特別制度。因此，針對這類行動的司法保障仍然有效，即對這類扣押必須有預審法官的介入。刑事

[67] 關於電子資料的扣押，可參閱馮文莊，“刑事訴訟程序中新科技的應用：刑事訴訟中證據數字化之若干思考”，《在二十一世紀所面臨的挑戰》刑事訴訟國際研討會會議錄，法律及司法培訓中心 2007，165-183 頁；Pedro Verdelho, ‘A obtenção de prova no ambiente digital’, in *Revista do Ministério Público*, Ano 25, n.º 99 (2004), pp. 117-136.

警察機關有權限在某刑事訴訟程序中進行扣押，但當涉及廣義上的電子形式的通訊時則除外。

同樣，扣押律師事務所、醫生診所或銀行機構的電子證據或與依法受保護的秘密有關的電子證據時，必須依循刑訴法規定的一般制度（《刑事訴訟法典》第一百六十五條至第一百六十七條），即其內所載的司法保障完全適用。對電子通訊內容的截取亦然——《刑事訴訟法典》第一百七十五條將電話監聽的法律制度延伸至以有別於電話的其他技術方法傳達的談話或通訊（《刑事訴訟法典》第一百七十二條至第一百七十四條）。

15 - 特別措施（*第十六條*）

對於法案第十六條所載制度，之前已於概括性審議的第 5.2 點中作過分析。於細則性審議中需特別說明的是，有關行文上的修改主要是爲了強調，實施該條規定的行為的權限屬司法當局特別是檢察院所有，檢察院在其領導刑事偵查的權力範圍內，可命令採取第十六條第一款規定的特別措施。正是由於這些是特別措施，對於採取的必要性，檢察院負有說明理由的特別義務。而事實上法案新文本亦強調了檢察院應儘可能主持有關工作的需要。

在其他急需取得及保存證據的緊急情況下，刑事警察機關同樣可根據《刑事訴訟法典》的規定介入。在此再一次強調，這種介入具例外性質，不應成為常規的做法。倘刑事警察機關在沒有司法當局

事先許可下採取特別措施，有關措施需於七十二小時內被確認效力，否則無效。第十六條第二款及第三款對在打擊電腦犯罪法範圍內採取的特別措施所規定的制度，與《刑事訴訟法典》第一百六十三條第三款至第五款對扣押所規定的制度相同。在這些條款中，同樣規定了司法當局的一般權限、刑事警察機關緊急介入的可能性以及於七十二小時內由司法當局確認效力的內容。

第十六條第四款訂定，按第一款（五）項針對被視為不法電腦數據資料所作出的移除命令的司法申訴。在這裏，司法當局對相關的電腦數據資料作出預先的判斷，並命令阻止公眾予以查閱，以便制止重要的法益受到侵犯。由於此措施執行時可能對受憲法保障的言論自由造成限制，因此法案規定，就該司法判決進行全面調查的可能性，訂明按第一款(五)項規定所採取的措施可向刑事起訴法官申訴。擁有申訴權的人不僅是被命令進行移除的人（互聯網服務提供者），亦包括因該命令而受到影響的人，即被移取的電腦數據資料的擁有人。十日的申訴期限與《刑事訴訟法典》就扣押所規定的申訴期限相同（第一百六十三條第六款與十月八日第 55/99/M 法令第六條第二款)。雖然本法案只為第一款（五）項所指的情況訂定司法申訴，但此事實並不妨礙就按本法案規定所作出的扣押補充適用《刑事訴訟法典》關於申訴的規定。

五、 結論

委員會經細則性審議及分析後認為：

a) 本法案具備在全體會議作細則性審議及表決的必需要件；

b) 有必要邀請政府委派代表列席為細則性表決法案而召開的全體會議，以提供必需的解釋。

二零零九年六月十七日

委員會

鄭志強

（主席）

許輝年

（秘書）

賀定一

高開賢

張立群

楊道匡

高天賜

梁安琪

李從正