第一常設委員會

第 3/VI/2019 號意見書

事由：細則性審議《網絡安全法》法案（卷宗編號 20/2018/VI）

一、引言

澳門特別行政區政府於二零一八年九月十二日向立法會提交了《網絡安全法》法案，隨後，立法會主席根據《議事規則》的規定，透過第 1265/VI/2018 號批示接納了該法案。

法案在二零一八年十月十八日舉行的立法會全體會議上被引介及作一般性討論，並以二十七票贊成及三票反對，獲得了多數通過。

同日，立法會主席透過第 1344/VI/2018 號批示將法案分發給本委員會進行細則性審議工作，並要求委員會於二零一九年一月十八日前完成分析審議及提交意見書。然而，由於在該段期間內，委員會也在細則性審議其他法

案，故此，委員會曾向立法會主席申請延長細則性審議法案及提交意見書的期限，並獲得批准。

根據第 30/VI/2018 號通知，立法會顧問團 C 工作小組被指派協助委員會進行法案的細則性審議工作。

委員會於二零一八年十一月九日，二零一九年一月七日、九日、十一日和二十五日，二月一日，四月八日，五月七日以及五月二十二日共舉行了九次小組會議，對法案進行分析審議，政府代表列席其中的七次會議。此外，基於從技術層面完善法案的相關規定的考慮，立法會顧問團與政府顧問團分別於二零一九年三月四日和六日共舉行了兩次技術會議。

二零一九年五月二十日，政府向立法會提交了本法案的最後文本，當中部份內容反映了本委員會的意見及立法會顧問團的法律技術分析。因此，除另有說明外，本意見書對法案各條文的引述，是以法案的最後文本為依據，然而，在有需要時亦會提及法案最初文本的條文。

二、引介

根據附隨本法案的理由陳述，“隨着互聯網及通訊技術高速發展和廣泛應用，澳門特別行政區如同其他的國家或

地區一樣，正朝智慧城市的方向發展，「工業 4.0」引領澳門進入人工智能及大數據的網絡時代，資訊化與社會各領域的活動和各階層市民的日常生活密切相關。電腦、資訊網絡及互聯網成為各行各業及廣大市民日常生活的必要工具。

誠然，資訊化及人工智能為人們、企業及機構帶來莫大裨益與方便，但正因為其異常重要，面對全球網絡安全威脅，公私領域的網絡和資訊安全面臨網絡入侵及襲擊的嚴峻挑戰，為確保主要資訊網絡運作暢順及無間斷，以及為保障電腦數據資料的保密性和完整性，有必要制定適當的防護機制。

澳門特別行政區政府曾在《二零一六年財政年度施政報告》保安範疇強調'由於技術的缺陷和防範意識的不足，資訊系統的高危漏洞必然有增無減，公私領域的網絡和資訊安全正面臨嚴峻的挑戰；各種形式的網絡犯罪及網絡安全事故，正以前所未有的規模、嚴重性和複雜程度出現'。

基於此，本法案旨在從法律上構建上述的防護機制，清楚制訂網絡安全方面的義務和責任，透過強化公共和私人機構營運的關鍵基礎設施的網絡安全，維護公共安全、公共秩序及社會穩定等重大公共利益，以及保障澳門居民的利益……。

本法案的直接保護標的是公共部門和營運關鍵業務的私人實體的資訊網絡及資訊系統，如運輸、電訊、銀行和保險、醫療衛生、水電供應等……業務。本法案稱此等公共部門及私人實體為關鍵基礎設施營運者。

本法案選取上述領域及實體的理由是，一旦有關的資訊網絡及系統受到襲擊，將造成極大的衝擊，直接危害公共安全及秩序，以及廣大市民的福祉，無可避免地將對社會帶來嚴重後果。”

特區政府於二零一七年十二月十一日至二零一八年一月二十四日就本立法提案進行了公開諮詢，並於二零一八年九月六日公佈了諮詢總結報告。（詳情載於：https://www.gss.gov.mo/media/Relatorio_C.pdf）。根據該文件，“市民普遍贊成本澳建立網絡安全防護體系，其中有意見認為隨着本澳發展成為‘智慧城市’、普及電子支付，建立網絡安全防護體系有助本澳防範因受到網絡攻擊而影響社會的運作，贊同政府儘快完善相關法律保障市民，尤其是對個人信息容易外洩等問題必須正視。……超過 87% 的意見認為建立網絡安全防護體系屬有必要且具有迫切性，業界與公眾均指出網絡安全是公共安全及個人安全的前提及保障，為確保網絡運作良好、網絡數據保密及完整，澳門特別行政區有必要透過立法，構建良好的防範性管理體系。”

三、一般性分析

資訊科技是社會經濟發展和社會福祉的基本工具。資訊科技在日常的廣泛應用，大大增強了信息傳播、人際溝通或遠距離貿易的潛力。然而，基於資訊科技在當今社會的重要性，人們對科技的依賴意味着為個人和集體所帶來的安全風險將進一步加劇。一般市民往往不會覺察到資訊科技亦應用在如電網、水網或交通運輸網，衞生護理的提供，食物的供應，銀行或金融的活動等用作維持社會生活的基礎設施上，以確保其正常及有效運作。上述只是高度依賴資訊網絡及系統良好運作的一些例子，可見該等行業的資訊網絡及系統必須受到保護，以抵禦因有意或無意的行為致使相關網絡及系統的運作受到影響或效率下降的風險。

(一) 網絡安全的概念

安全概念[1]現時涵蓋資訊或網絡層面的安全，即網絡安全。網絡安全被視為一種具有掌控進入互聯的資訊系統以及存取系統內資訊[2]的能力，而且網絡安全是以保護由人類

[1] "保護的相對條件，能夠消除可識別為對某人或某種事物存在構成的威脅"（Security and Defense Studies Review, 第一卷，第 2 頁，關於國家安全與人類安全：概念問題與政治後果，Marco Cepik 著，華盛頓，二零零一年），引述於立法會第二常設委員會第 4/II/2002 號意見書，關於《澳門特別行政區內部保安綱要法》（第 9/2002 號法律）。

[2] Jennifer L. Bayuk et al., Cyber Security Policy Guidebook, Wiley & Sons，新澤西， 2012 年，

和物質領域以外的社會生活為目的，從而相應地對個人及其財產作出保護。事實上，“網絡世界是現代社會、安全、經濟及業務的正常運作的一個關鍵領域，因為，在當今全球化的世界中，存取大量的資訊是人類的相同期望。基於資訊必須受到保護，以免有未經許可的存取或更改事件的發生，因此，需要為長期存取和交換資訊訂定安全標準[3]。”網絡安全旨在保護資訊網絡及系統，以及包含在或運行於該等載體的數據其固有的價值[4]，而且對於已超越經濟價值的，如隱私權等基本權利的行使提供相若的保護。這種保護首先視乎網絡的構造，也就是說，資訊網絡及系統的構思和設計方式，以及承受風險的脆弱度。而且還需配有一系列適當的立法措施（無論是刑事性質或行政性質）、科技防護工具（包括加密系統、防火牆、認證及防入侵機制等防毒應用程式及避免服務中斷的工具[5]）；此外，亦需視乎公司或政府在確保資訊網絡及系統，以及其內含的電腦數據的良好運作方面的組織文化。再者，亦視乎於

第1頁。

[3] Fernando Freire 和 Paulo Viegas Nunes, «Estratégia da Informação e Segurança no Ciberespaço», in IDN Cadernos, n.º 12， 2013 年，第 10 頁。

[4] 有關網絡安全的內涵方面，國際標準化組織(International Standard Organization)亦有相關的定義。可參看，皮勇：“網絡安全法原論”(Research on Cyber-Security Law)，武漢大學刑事法研究中心學術叢書 2，中國人民公安大學出版社，北京，2008 年 9 月，第 341 頁。

[5] 法案最初文本第二條第一款（一）項所載的列舉，關於各種科技防護手段的性質及運作方式。見 James Graham, Richard Howard e Ryan Olson (eds.), Cyber Security Essentials, CRC Press, Boca Raton， 2011 年，第 1-69 頁。

個人對資訊安全重要性的意識或敏感度[6]。

網絡世界的戰略價值增強了危害社會正常運作或從資訊中獲取不法經濟利益的攻擊。公權力就應對這些網絡攻擊，如未經許可存取或更改資訊網絡及系統的資料，往往將這些未經許可的行為列作刑事化處理，正如澳門特別行政區亦通過了《打擊電腦犯罪法》（第 11/2009 號法律）。然而，本身的刑事犯罪框架設計並不妨礙須設有其他機制以防止網絡攻擊的發生，或當無法防止襲擊發生時，亦能及時發現並作出快速的技術性應對，以消除或減低因攻襲而產生的負面影響[7]。本法案所設立的網絡安全體系正是為了建立適當的體制，以便作出有效應對。該體制是依據網絡安全的法定概念進行構建：根據法案第二條第一款（一）項的規定，“網絡安全”：是指澳門特別行政區為確保關鍵基礎設施營運者所使用的資訊網絡及電腦系統正常運作，以及電腦數據資料的完整性、保密性及可用性而開展的長期性跨領域活動，尤其防止該等網絡、系統及數據資料因未經許可的行為而受到不利影響。”

[6] 例如，在選擇一個安全的關鍵字時。見 Jennifer L. Bayuk et al.，前引，第 7-13 頁。

[7] 參閱 Nathan Alexander Sales, «Regulating Cyber-Security», in *Northwestern University Law Review*, 第 107 冊, 2013, 第 1546-1552 頁.

（二）澳門特別行政區網絡安全體系：特徵及組織框架

澳門特別行政區的網絡安全體系的建立具有三個主要特徵：1) 為社會的正常運作識別出關鍵領域及對其作出必須的保護；2) 就網絡安全範疇制定公共與私人實體的組織性合作法律文件；及 3) 具有明顯的預防和技術特徵。

2.1. 首先須指出，現時建立的系統只是為了保護被認為對社會正常運作至關重要的網絡和資訊系統。因此，「關鍵基礎設施」的概念是非常重要的，即“對社會正常運作具有重要意義，且一旦遭到擾亂、破壞、數據資料洩漏、停止運作或效能大幅降低，可能嚴重危害社會福祉、公共安全、公共秩序或其他尤為重要的公共利益的資產、資訊網絡和電腦系統”〔第二條第一款（三）項〕。一如法案的理由陳述所指：“本法案選取上述領域及實體的理由是，一旦有關的資訊網絡及系統受到襲擊，將造成極大的衝擊，直接危害公共安全及秩序，以及廣大市民的福祉，無可避免地將對社會帶來嚴重後果”。由此產生了日後法律在適用範圍上的一個消極界限：本次提案所產生的保護機制，僅有利於公共或私人實體操作的關鍵基礎設施的網絡和資訊系統，即僅限於這些實體。同樣地，所規定的義務，亦僅限於操作有關關鍵基礎設施的營運者，即僅限於這些營運者。

為社會正常運作而識別的主要領域包括整個公共行政及法案第四條第三款所指的領域。因此，《網絡安全法》並非適用於澳門一般市民及全澳所有的資訊網絡及資訊系統的一般法律，該法律僅適用於被視為關鍵基礎設施及其營運者。正如諮詢總結報告所言，“《網絡安全法》的立法原意旨在遵照‘保障市民安全、尊重個人隱私’ 的原則下，為澳門社會的關鍵基礎設施構建一個良好的防範管理體系，防範及減少網絡攻擊對本澳社會的影響”（第10頁）。

法案第四條規定了關鍵基礎設施的兩種營運者：公共營運者及私人營運者。首先，所有公共實體均被視為關鍵基礎設施的公共營運者，其使用的網絡、系統及資訊數據均受到保護（第四條第二款）。但排除於該分類及法律適用範圍者包括有“不使用資訊網絡或電腦系統，又或根據適用的組織法規或行政長官批示的規定，僅使用由其他公共實體負責網絡安全的資訊網絡或電腦系統的澳門特別行政區公共部門、機關或實體”〔第五條第一款（一）項〕。另一方面，根據第四條第三款的規定，關鍵基礎設施的私人營運者分為三類：

1) 全公共資本公司；
2) 活動僅限於科學及技術領域的行政公益法人；
3) 具資格以經營批給、向行政當局提供服務、准照、執照或相同性質的憑證的方式，在下列特定

領域從事業務的私法實體：

- 供水；
- 銀行、財務及保險業；
- 在醫院提供衛生護理；
- 污水處理和垃圾收集及處理；
- 燃料和受衛生檢疫及植物檢疫的食品的總批發供應；
- 法定屠宰場宰殺動物；
- 電力及天然氣的供應及分配；
- 提供定期海、陸、空運輸的公共服務；
- 港口、碼頭、機場及直升機場的營運；
- 視聽廣播（但不適用於其業務僅限於娛樂節目廣播[8]）；
- 經營娛樂場幸運博彩；
- 經營固定或流動的公共電信網絡；
- 提供互聯網接入服務。

政府向委員會指出，初步確定了 117 個關鍵基礎設施的私人營運者，主要集中的領域包括銀行、金融及保險業務等不同行業(共 64 個實體)。該名單由政府送交委員會知悉，並指出會不定期對名單作出修改，而根據第二十七條(二)項的規定，該名單將於本法案通過後透過補充法規公佈。

[8] 根據第五條第一款(二)項的規定不適用。

2.2. 網絡安全系統的第二個特徵就是，視澳門特別行政區為維護集體利益的實體，作為自然而然的領導角色，並透過多個公共及私人實體的參與實現本提案及現設立的制度的目的。因此，倡議網絡安全體系的組成機構與關鍵基礎設施的公共及私人營運者之間的組織性合作。就是該等機構有義務履行法案所規定的各項義務，尤其有義務提醒專責實體有關管理及應對網絡安全事故。因此，根據本法律的規定制定網絡安全管理制度，分擔管理責任，該等責任分別為公共實體之間的責任（尤其是網絡安全委員會[9]和網絡安全事故預警及應急中心）、有關公共實體在網絡安全範疇上履行新的監管職能的責任及關鍵基礎設施營運者的責任。該等責任的分擔是建基於社會各方的共同協作及努力，並以維護社會不受網絡安全事故而造成的負面影響為目的。

在組織性方面，制度分為多個層面及預計會有不同的參與者：

1) **網絡安全委員會**：屬於頂層機關及具有政治性質，其負責訂定實現網絡安全目標的一般性及策略性的方向（第七條一款）。該機關由行政長官領導。
2) **網絡安全事故預警及應急中心**（預警及應急中心）：是一個專門及技術性機構（即不被納入公

[9] 在最初文本中，“網絡安全委員會”被稱為“網絡安全常設委員會”。

共行政架構的行政機關），主要負責管理及執行有關網絡安全緊急事故應對措施。預警及應急中心的構想是作為危機管理及處理的實體。因此，該中心應集中接收與網絡安全事故有關的資訊；訂定應對網絡安全事故的例外措施，尤其是正在發生或即將發生的嚴重網絡安全事故；協調各不同參與實體的應對，以防止或減少網絡安全事故的影響；實時檢視在關鍵基礎設施營運者的資訊網絡與互聯網之間傳輸的電腦數據資料的流量及特徵；及就網絡安全事故發出預警。預警及應急中心是一個擁有網安方面專業技術的實體，因此其他實體有需要時，可向該中心要求提供專門技術支援及協助。預警及應急中心由司法警察局統籌。

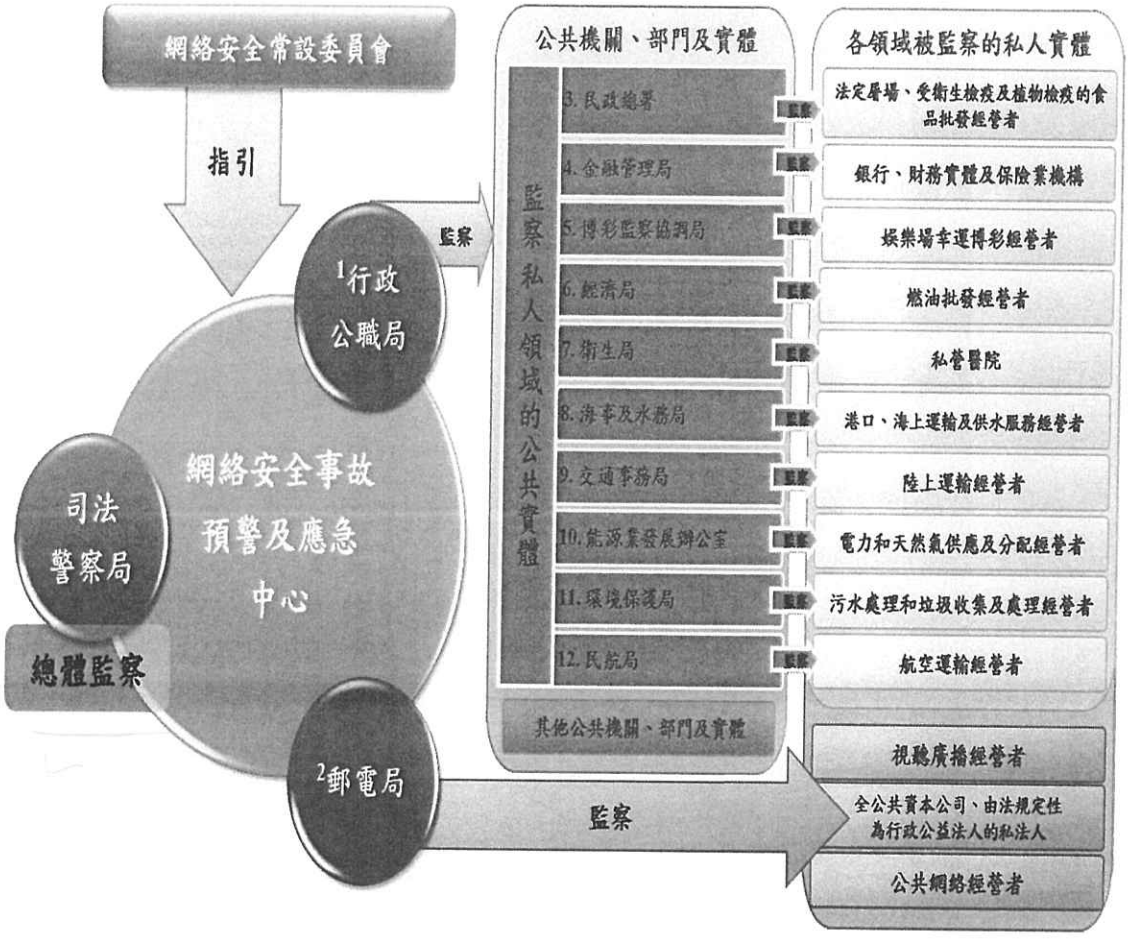
3) **網絡安全監管實體**：是指關鍵基礎設施營運者在其業務領域內遵守網絡安全義務的情況作出長期常規性監測的實體。預料行政公職局將負責監察其他公共營運者的關鍵基礎設施，以及“由 11 個公共部門分工負責監察相應私人領域的關鍵基礎領域營運者”[10]。

4) **關鍵基礎設施營運者**：其義務載於法（案）的第三章，而該等實體是領先對可能存在的網絡安全事故承擔起保護責任的實體，並對事故進行探測及予以化解，在其有需要時亦可要求預警

[10] 諮詢總結報告，第 4.3 點，第 19 頁。

及應急中心及相關的監管實體提供協助。嚴格而言，雖然關鍵基礎設施營運者並沒有納入在澳門特別行政區網絡安全體系的組織架構中(注意：沒有載於第六條的規定)，但該等營運者卻是體系運作的根本要素。

澳門特別行政區網絡安全管理體系架構



來源：澳門特別行政區政府-諮詢總結報告(2018)

委員會努力釐清組成網絡安全體系的不同實體之間的關係。擬加強系統的金字塔結構，以及賦予體系中的網絡安全委員會的頂層職能。因此，在法案的最後文本規定網絡安全委員會有權“監督網絡安全體系內其他實體在本法律範圍內所開展的活動”〔第七條第二項〕，及網絡安全事故預警及應急中心“應監管實體的要求，在其履行職責時給予技術支援”〔第八條第一款（七）項〕。

另外，委員會亦考慮了將尤其涉及規範權限（第三條第二款）及處罰（第二十一條）權限的監督權限賦予十一個不同實體的立法取向。委員會內部提出的憂慮是，大量的監督實體可能會引致法律在適用上有不一致的情況，且在發出技術規範時會出現不協調，以至在適用將來的網絡安全法時會出現不願承擔的態度。倘若存在一個具監督功能的中央實體，其在規範及處罰方面採用統一的標準，則此等情況便可避免。然而，提案人指出基於各類關鍵基礎設施的特殊性，與透過單一的監督實體以集中的方式作出監管相比較，認為由相關領域的專有部門進行監管較為適宜。此外，提案人亦指出賦予網絡安全委員會的政策協調職責，以及賦予網絡安全事故預警及應急中心的技術合作職責，可確保執法上具有統一的標準。

2.3. 第三個須迫切強調的特徵，是關係到按現設立的體系所作出介入的類型。該等介入主要屬技術性質的預防

性介入，且不取決於預防所針對的行為的不法性。

對關鍵基礎設施營運者的電腦網絡、系統及數據進行的保護，是由營運者本身採用的技術解決方案作出。這些營運者有義務設立所需的技術、人力、組織及程序性的條件，以預防、偵測及緩解倘有的網絡安全事故，亦可得到組成體系的公共實體的支援及協調。因此，這個技術回應並不取決於法律體系對造成網絡安全事故的不許可行為的處理方法。至於有關行為是否構成刑事上的不法行為，本法案沒有給予解決，但在本地法律體系中的其他現行法律，尤其是《打擊電腦犯罪法》（第 11/2009 號法律）中則已有解決方法。因此，本法案將使澳門特別行政區在防範網絡攻擊方面的法律結構變得完整，而這個須結合技術預防的防範。而因應現設的網絡安全體系、與刑法及第 11/2009 號法律所載的電腦犯罪清單使有關的一般及特別預防有所加強。根據提案人向委員會所作的解釋，“法案建立一個行政管理體系，旨在透過規範關鍵基礎設施運營商的義務及責任來確保澳門特別行政區的網絡安全。《網絡安全法》是一部旨在‘保護、預防及管理’的法律；至於涉及互聯網、資訊及電腦方面的刑事罪行仍在《打擊電腦犯罪法》規管。《網絡安全法》的內容屬於事前預防措施，針對關鍵基礎設施的網絡安全作出防範性管理……。而現行《打擊電腦犯罪法》是針對電腦及網絡犯罪行為的刑事法律，屬於事後的刑事偵查措施。”

（三） 維護基本權利

委員會考慮了本法案與澳門市民行使及享有某些基本權利之間的關係。由於網絡安全法法案對言論自由和通訊保密等所帶來的影響，曾引起社會上一些行業的質疑。諮詢總結報告中提到存在“擔心政府會藉着《網絡安全法》……使網絡監控合法化，侵害市民的言論自由、通訊保密等權利”[11]。在公開諮詢中指出的憂慮，在立法會分析法案的過程中，不論是一般性還是細則性的審議亦曾被探討。有關憂慮反映在兩個方面：電腦數據檢視的可能性以及司法警察局的權限範圍。

3.1. 電訊自由及保密受《基本法》第三十二條保護，根據有關規定“除因公共安全和追查刑事犯罪的需要，由有關機關依照法律規定對通訊進行檢查外，任何部門或個人不得以任何理由侵犯居民的通訊自由和通訊秘密”。同樣，言論自由及私隱亦受到同一法律保護。根據該等的規定，澳門特別行政區的網絡安全體系，以及在其範圍內採取的措施均有必要尊重《基本法》所載的基本權利的保障。須提醒的是，正如《基本法》第十一條第二段所規定的，“澳門特別行政區的任何法律、法令、行政法規和其他規範性文件均不得同本法相抵觸”。

[11] 諮詢總結報告，第 1 點，第 10 頁。

提案人藉此機會重申法案在這一事宜上的立法取向。首先，對作為整體法律體系，肯定了特別是作為將來的網絡安全法的基本原則的個人私隱的尊重。其次，釐清了“《網絡安全法》的內容屬於……措施，針對關鍵基礎設施的網絡安全作出防範性管理，並非侵害市民言論自由、個人隱私或干預新聞自由等個人基本權利”。提案人亦藉此機會澄清了“就進行監察時會否侵犯市民的隱私權的問題，……網絡安全事故預警及應急中心和監察實體的人員不得直接或透過還原數據包技術，以取得個人資料、行業資訊或通訊內容，否則，監察人員須承擔按第 8/2005 號法律《個人資料保護法》、第 11/2009 號《打擊電腦犯罪法》和《刑法典》規定的刑事和行政違法等責任，以及《澳門公共行政工作人員通則》規定的紀律責任。如果在符合《民法典》規定的情況下，還須承擔相關民事責任”。

對於有關維護市民的基本權利、自由及保障方面的擔憂，在分析有關為預防、偵測及打擊網絡安全事故〔第三條第一款（五）項〕而可檢視關鍵基礎設施營運商網絡與互聯網之間傳輸資訊數據的規定時尤其突出。這一檢視是由司法警察局作出的實時檢視[12]，檢視僅涉及機器語言或二

[12] 檢視關鍵基礎設施營運者的網絡與互聯網之間的電腦數據傳輸，是網絡安全事故預警及應急中心被賦予的權限，這一權限具體是由司法警察局行使的(第八條第三款)。

進制語言，以及限於對關鍵基礎設施營運者的網絡與互聯網之間的傳輸流量及特徵作出分析（第八條第一款（五）項及第二款）。

現時法案僅容許對通訊數據作出檢視，從而排除了對通訊內容的取得的可能性。正如保安司司長在 2018 年 10 年 18 日的全體會議上引介法案時所表示的，“將來相關負責部門在執行法律時，只會及只能依法評估網絡數據流量和網絡攻擊資訊所帶來的各種安全風險，從而發出預警和指引以保障網絡安全，並非、亦不可能實施網絡資訊內容的監察活動，因此不可能構成對公眾言論自由的限制、剝奪甚至損害。實際上，在網絡安全的前提下，居民的通訊自由和個人隱私會進一步受到法律的有效保障。除非得到司法機關的批准，否則相關部門不會亦不可能介入任何網絡內容，也不會、亦不可能對網絡內容或言論進行解碼。”

委員會考慮並接納了提案人就證明將來的網絡安全法並不會對市民的基本權利、自由及保障，尤其是言論自由及通訊保密等權利帶來負面影響所提出的事實及法律解釋。雖然在實務上不會發生，但理論上通訊數據的取得是有助發現使用者的行為規律，從而創建使用者的類型[13]，而

[13] 政府向委員會表示“關於這個問題，特別需要強調的是監察時只是流水式檢測數據流量及數據包特徵，經過檢測的數據流量不會作任何保留，亦不會記錄任何資

有關數據應透過法律對通訊的不可侵犯的保障而受到保護[14]。因此，委員會認為倘若能以毫不含糊的行文明確反映上述的立法取向並規定相關的具體保障，即可消除有關尊重基本權利方面的質疑。基於此，委員會提出應在條文內明確規定禁止對受監控的資訊數據進行收集或解碼，例如禁止取得通訊內容[15]（第八條第二款，最後部分）。這一後加部分代表着一項額外的保障，就是網絡安全法並不是一種控制網絡空間的通訊內容及言論自由的工具。

委員會重申，在藉着保障基本權利而保障福利、治安和公共秩序的同時，對加強網絡安全給予配合是重要的。與提案人在不同場合曾作出的表示相類似，相信在澳門特別行政區的法律體系內，有適合應對因濫用網絡安全法而損害市民權利、自由及保障的行政、民事及刑事機制。在回應委員會的提問時，提案人解釋“市民可透過行政申訴、向檢察院和/或廉政公署投訴，或是提起相關的司法訴訟(例如：確認權利或受法律保護之利益之訴、命令作出依法應作之行政行為之訴、實際履行非合同民事責任之訴)追

料，確保既不涉及個人資料，亦不涉及行業資訊或通訊內容。為此，‘中心’及監察實體人員不可能直接或透過還原數據包技術獲取到個人資料、行業資訊或通訊內容”。

[14] 見 António Manuel Abrantes，《O acesso a dados de tráfego pelos Serviços de Informações à luz do direito fundamental à inviolabilidade das comunicações》，*Revista do Ministério Público*，第156冊，2018，第162頁-第163頁。

[15] 電腦數據的檢視會對實時的數據安全進行檢測，例如數據流量、目的地及特徵等，旨在識別出異常情況或具攻擊性的襲擊信號，而不是對數據內容進行檢視。

究上述各類責任。”

3.2. 根據法案，司法警察局是預警及應急中心的組成機關之一，並對其進行統籌；檢視關鍵基礎設施營運者的資訊網絡與互聯網之間傳輸的電腦數據資料；並對網絡安全主要負責人及其替代人候選人的適當資格發表意見。

委員會就網絡安全體系中賦予司法警察局的職能進行了分析。正如提案人所稱，本法規“專門規範網絡安全行政管理的法律，以守護、防範、管理為主的法律，以行政方式規範關鍵基礎設施應對網絡安全的要求”。在這樣的一項法規中，對於由具有預防犯罪、刑事偵查、協助司法當局職責的刑事警察機關[16]承擔主導地位的這一內容尤其受到委員會的關注。委員會要求提案人解釋司法警察局在網絡安全體系中擔任此種角色是基於何種立法政策，擔任此角色會否無意中改變本體系的行政屬性，令其具有警務特點。

政府解釋稱，這一取態參考了各地網絡安全體系，不少國家和地區賦予警務機關監測網絡安全和相關執法職責，例如中國公安及香港警署。在澳門“司法警察局作為《打擊電腦犯罪法》的主要執法部門，一直了解本澳的網絡安全情況，亦在過去多宗調查和打擊本澳曾發生的網絡

[16] 參閱第 5/2006 號法律《司法警察局》第二條第一款。

安全事件上累積了不少的實務經驗”。此外，司法警察局擁有監測網絡安全所需的技術力量，長期以來致力培養專業精幹的網絡安全和電腦法證人員。在這一方面，司法警察局“多年積極派員到鄰近地區和世界各地出席網絡安全峰會、網絡安全培訓和交流，累積了網絡安全方面不可缺少的交流網、經驗、人才和能力，相信這些均對如何能有效從技術上及早預防和發現本澳總體網絡安全問題相當重要。在及時性響應方面，從各地近年頻頻發生的網絡安全攻擊事故所見，網絡攻擊跨國、複雜、隱蔽且證據易變易失，整個事前、事中和事後的聯動性需要相當緊密，把發現攻擊苗頭到刑事調查介入緊密聯動，才能對網絡安全攻擊事件作出有效的響應和溯源，充分體現《網絡安全法》與《打擊電腦犯罪法》的互補關係。”因此，提案人相信賦予司法警察局的職責，尤其是執行網絡安全事故預警及應急中心的電腦數據資料的檢視，對構建本澳網絡安全體系並對其運作起積極作用。

對於司法警察局透過執行第 11/2009 號法律在資訊安全方面獲得技術力量這一理據，委員會表示理解。另外，由司法警察局集中進行監測可減少涉及的個人和實體，有利於降低侵犯個人資料隱私權的潛在風險。故此，委員會接受了本法案這一立法取向。但是，根據法案最初文本第十條第一款(二)項，要求司法警察局就關鍵基礎設施營運者的網絡安全主要負責人及其替代人的專業經驗發表意見，

委員會認為不合理。然而，即使該必需意見無約束力，但是專業經驗不應受其限制，而且關鍵基礎設施營運者有意聘用的專業人士的技術能力也不應由一個警察機關負責評估。因此，在最後文本中，司法警察局的意見僅針對擬指定為網絡安全主要負責人及其替代人的人士的適當資格及倘有的禁止情況（第十條第六款）。而根據《行政程序法典》第九十一條第二款，此意見必需且無約束力。也就是說，此意見必須徵求（根據第十條第六款），但徵求意見者無須遵從相關結論。倘若關鍵基礎設施私人營運者不向司法警察局徵求該等意見，則根據法案第十五條第一款的規定構成行政違法行為。

(四) 網絡安全義務

提高特區網絡安全標準意味着關鍵基礎設施營運者需採用一系列防範網絡襲擊的措施。而相關實體是因為其個人利益——往往是經濟利益而採取此類措施，以便保證其資訊網絡及電腦系統的正常運作，保護其電腦數據資料的安全。就此問題，《公開諮詢總結報告》提及有意見認為保障網絡安全是關鍵基礎設施營運者本身的責任，而公權力不應干預此類實體——多數是企業——的管理。然而，此類基礎設施涉及社會核心領域，具有重大的社會意義。因而除具有上述個人利益之外，還涉及集體利益，要求關鍵

基礎設施營運者須採取有效機制保護資訊網絡、電腦系統和數據資料的安全。這是因為只要一個營運者的安全堪憂，就會影響其他營運者，繼而波及整個社會。因此，法案引入了一系列網絡安全義務，一旦法律生效，所有關鍵基礎設施營運者，不論是公共的還是私人的，均必須履行。這些義務旨在推廣一種網絡安全文化，並透過制定法律和建立組織統一安全標準、統籌應對網絡安全事故、為預防和打擊此類事件提供更多的技術方案。

根據法案的理由陳述，第三章涉及網絡安全義務，"內容包含本法案的核心規定。關鍵基礎設施營運者以標準化及監察模式有效地推行網絡安全的義務，確保達至這項全新法律制度的下列主要目標：確保關鍵基礎設施營運者所使用的資訊網絡及電腦系統的可操作性、完整性及可用性，以及電腦數據資料的保密性，以防止該等資訊網絡、電腦系統及數據資料遭受未經許可的行為所損害或任何形式的影響。"

法案對關鍵基礎設施私人營運者規定了一系列組織性義務（第十條）；程序性、預防性及應變性義務（第十一條）；自行評估及報告義務（第十二條）；以及合作義務（第十三條）。而公共營運者的義務由第十四條規定。

4.1. 網絡安全義務適用於網絡安全私人營運者的內部組

織方面。根據第十條的規定，此類營運者必須建立專門處理網絡安全的單位，並為其運作配置合適的人力、財政、物力及財產資源。特別是在人力資源方面，所有私人營運者有義務指定具備專業經驗的人士擔任網絡安全主要負責人及其替代人。這些人士應以澳門特別行政區為常居地，以便預警及應急中心隨時聯絡，在有需要時，可針對即將發生或正在發生的網絡襲擊啟動內部保護措施。[17]

除要求網絡安全主要負責人及其替代人具有勝任的專業經驗之外，法案還要求須具備履行職務的適當資格。網絡安全的性質敏感，不僅對關鍵基礎設施所屬的領域具有重要意義，而且對個人資料保護亦然。因此，要求這一領域的負責人應品行端正。第十條第二款規定："在審查適當資格時，應考慮任何基於其嚴重性、多發性或其他應予重視的情節而對確保網絡安全構成重大疑慮的事實。"這是一種對候選人的品德進行的判斷，由私人營運者和司法警察局，分別於甄選擔任此類職務的人士時和發出相關意見時作出。必然影響適當資格的情況有三種：

1) 因第 2/2009 號法律《維護國家安全法》規定的犯罪被判刑；

[17] 根據理由陳述，"設立'網絡安全主要負責人'的職位，旨在於組織內引入較大的個人責任機制。該建議要求有關人員須具備適當資格及專業經驗，並訂定某些強制規定，確保其在澳門特別行政區切實聽候安排，以便與當局合作，尤其是在緊急情況下。"

2) 因電腦犯罪或偽造技術註記罪、損壞或取去技術註記罪、以資訊方法作侵入罪、不當利用秘密罪、違反函件或電訊保密罪或違反職業保密罪被判刑；

3) 因其他任何可處超過五年徒刑的犯罪被判刑。

在這些情況下，法律以不可推翻的方式推定，行為人被判罪行的性質，或此類罪行的抽象刑罰幅度的嚴重性，顯示此人不具有履行如此重大職務所需的良好品德。因此，不得指定因此類犯罪被判刑者擔任網絡安全主要負責人或其替代人（第十條第三款）。透過法案細則性審議，這一禁止制度變得更加清晰，加強了第十條第三款規定罪行的絕對禁止性質，基於此類罪行而被判刑者不得擔任相關職務。但是，鑒於刑罰不具有喪失職業權利的必然效力（《刑法典》第六十條第一款），因此，認為有必要對此法定障礙在時間上進行限定，最後，於法案內建立了一個與六月三日第 27/96/M 號法令第二十四條稍有區別的依法恢復權利的特別制度。因此，第十條第四款改為規定禁止期間的事宜：

1) 如被判處五年或以下徒刑，自暫緩執行刑罰期滿、服刑終止或延長服刑終止之日起計五年；

2) 如被判處超過五年的實際徒刑，自服刑終止或延長服刑終止之日起計十年。

委員會擔憂網絡安全方面的本地專業人士可能比較稀缺。而履行組織性義務，尤其是為網絡安全管理單位配置合適的人力資源，以及指定網絡安全主要負責人及其替代人方面，可能因為勝任此類技術性、高專業性職務的人士不足而遇到困難。政府對此問題表示理解，指出一直透過與內地對口部門交流與合作，加強司法警察局內此領域的人員培訓。政府有意深化培訓策略，但不排除聘用非本地專業人員，以填補公營及私營部門本地人力資源的缺口。

4.2. 程序性、預防性及應變性義務（第十一條）旨在為關鍵基礎設施私人營運者制定網絡安全管理制度及相關的內部操作程序。此制度應規定根據技術規範確定的內部保護措施在實踐中的實施方式，以便對網絡安全事故進行檢視、預警及應對。第十一條還規定了將網絡安全事故通知預警及應急中心及監管實體的義務，但並不妨礙營運者應立即開展應對嚴重事故的行動。預防性義務方面，營運者應對其資訊網絡的運作狀況進行管理，透過測試及軟件升級，確保資訊網絡不被入侵並保持適當的安全標準。

4.3. 據理由陳述所載："第十二條所指的自行評估及報告義務有兩個目的：強制要求關鍵基礎設施營運者定期自行評估，同時，讓公共當局知悉真正及具體的情況，藉此建議調整及改善有關的法律或法規制度，以提升澳門特別行政區網絡安全的水平"。私人營運者可自行評估其資

訊網絡及電腦系統是否安全或存在風險，亦可將相關工作以商業形式委託他人進行。

4.4. 第十三條規定的合作義務"是為確保在網絡襲擊的緊急情況下能作出適當且有效的介入。然而，網絡安全事故預警及應急中心的代表僅在為查核防護機制義務的遵守情況下，方可進入營運者的關鍵基礎設施……。面對網絡襲擊時的介入是根本性的工作，其目的在於防止營運者的網絡及電腦系統因網絡安全威脅擴散而受病毒感染。"[18]

委員會曾就私人營運商的合作範圍，尤其是預警及應急中心及監管實體進入營運者的設施及設備方面提出疑問。有議員關注到該進入對個人私隱及通訊、職業或商業秘密潛在影響的問題，以及考慮到視聽廣播營運者亦包括在網絡安全法的主體適用範圍內（第四條第一款及第三款（一）項的（10）分項，故亦關注新聞自由會否因而受到影響。

政府解釋，只有獲適當認可的機構的代表提出要求，方可進入相關設施及設備，且目的亦只是為了核實履行屬於程序性、預防性及應變性義務的情況。換言之，預警及應變中心及監管實體的代表可要求進入，以監察營運者是否有就網絡安全事故採取保護、檢視、預警及應變等內部

[18] 理由陳述。

措施。根據委員會獲得的解釋，當預警及應變中心為避免或減少嚴重網絡安全事故的影響而按照第八條第一款（二）項的規定執行例外的網安措施時，設定該進入的可能性尤為重要。在此情況下，預警及應變中心的人員應可進入營運者的設施及設備，以確保技術措施有效及正確運用。

提案人向委員會保證，進入有關設施及設備的權力僅為監察第十一條所規定的義務，並不能用於核實營運者履行其他義務或其他方面的活動。監察其他義務的工作，由監管實體透過向營運者以索取資料方式進行，而有關資料有可能需要以文件證明。

4.5. 公共營運者亦須遵守網絡安全義務。儘管法律基於公共營運者的公共性質而強加其一些特殊義務，但第十四條所規定的義務與私人營運者所須遵守的義務是相若的。整體而言，網絡安全義務是平等地適用於公共及私人營運者：第十四條第一款（三）項，以準用方式規定公共營運者須履行第十一條至第十三條賦予私人營運者的義務。這些實體均須“對內及在其負責網絡安全的公共部門、機構或實體範圍內，履行和促使履行”相關網絡安全義務〔第十四條第一款（三）項〕。

4.6. 最後要說明的是，法律規定關鍵基礎設施營運者可聘用第三人負起執行網絡安全措施的責任。

根據第十二條（一）項的規定，關鍵基礎設施私人營運者可將其網絡及資訊系統所存在的安全及風險的評估事宜交由專業實體作出；第十六條（一）項一般規定私人營運者的網絡安全可由第三人確保。如果出現這種情況，私人營運者仍須承擔法律規定的違法責任，不會因此獲豁免，也就是說，即使可將不遵守網絡安全義務的責任歸咎於網絡安全私人服務提供者，但私人營運者仍可被處罰（或許該等私人營運者其後可向網絡安全私人服務提供者追究民事責任）。

至於關鍵基礎設施公共營運者，第十四條第一款（四）項規定，公共營運者與私人實體之間可訂立提供網絡安全服務的合同，但為此須獲得行政長官的預先許可（第十四條第三款）。在此情況下，即使存在提供勞務的合同，亦不免除公共實體檢視相關執行情況的責任，此外，在私人實體不履行合同時，公共實體還須執行相關服務，且不影響可向其追究第十四條第一款（四）項及（五）項所指的責任。法案還允許就公共部門、機關或實體的網絡安全事宜，可根據其組織法規或行政長官批示的規定，由其他公共實體負責作出規定。屬於此情況的部門、機關或實體被排除於《網絡安全法》的適用範圍內（第五條第一

款第一款）。向委員會提供的例子之一是保安司司長辦公室，其網絡安全是由澳門保安部隊事務局負責。[19]

（五）充性保安措施

法案對強制獲取電信服務客戶的身份資料，以及保存和提供通訊地址翻譯紀錄等內容作出規範。這“兩個實質問題，該等問題雖不直接涉及網絡安全，但與網絡安全息息相關，因為都是為了更好地保護資訊網絡及其廣大用戶。”[20]

5.1. 法案第二十五條規定電信網絡營運者，在訂立提供互聯網接入服務、域名註冊服務、固定或流動公用電信服務的合同或確認提供該等服務時，必須查核及登記客戶的身份資料。第二十四條，以過渡規定的形式，處理在法律生效前購買的無須預先提供身份資料的預付式 SIM 卡的情況。透過這兩條條文，本地區制定了一個識別流動電信服務使用者身份（實名制）的政策，目的是阻嚇透過流動電話終端機使用“用戶身份模塊卡”（SIM 卡）作犯罪用途。

[19] 根據第 9/2002 號行政法規《澳門保安部隊事務局的組織與運作》第二條（八）項的規定澳門保安部隊事務局的組織與運作。

[20] 理由陳述。

公開諮詢總結報告[21]指出，“按照澳門現時的電訊業務情況，除了預付卡外，現時澳門固網電話及手提電話用戶均以真實身份資料登記。‘實名制’旨在要求購買預付卡的人士同樣需要提供真實身份資料以作登記，防止不法之徒利用不記名預付卡作為犯案工具，以逃避警方進行的刑事偵查，從而更好地維護社會治安、保障市民大眾的合法權益。因此，要求預付卡用戶提供真實身份資料是‘實名制’一項基本要求，亦是交易行為上普遍的規則，世界各地早已遵循此規則以保障社會利益。”

委員會接納這一立法政策措施，並將之視為打擊電腦犯罪和透過傳播媒介犯罪的重要措施。資訊科技所提供的匿名行為在有助言論自由發揮的同時[22]，亦可以被利用於實施諸如詐騙、勒索、誹謗或不當查閱個人資料等犯罪[23]。因

[21] 報告第30頁。

[22] 參閱 Jyh-An Lee 及 Ching-Yi Liu, «Real-Name Registration Rules and the Fading Digital Anonymity in China», in Washington International Law Journal,第25冊，第一號，2016，4-10頁；Song Guangxing 及 Yang Pingfang, «The Influence of Network Real-name System on the Management of Internet Public Opinion», in *Public Administration in the Time of Regional Change - Proceedings of the Second International Conference on Public Management (ICPM 2013)*, 2013, 第47-53頁。

[23] 根據政府向委員會的說明，“有關與太空卡及外地SIM卡相關的犯罪數據雖未有正式統計，但經多年的案件偵辦情況和作案手法，因太空卡毋須進行實名登記，犯案成本相當低廉，廣泛應用在“偽基站”、“電話詐騙”、“電話勒索”、“裸聊”中，增加偵查難度。事實上，本局亦有發現很多犯罪分子來澳購買大批預付卡（太空卡），當中更有犯罪分子利用本澳的預付卡在境外詐騙當地華人，情況相當嚴重。另外，因作案分子可透過偽冒來電顯示，使來電區號不代表其真正所在地，案發時追查所得的外地號碼部門其實是由本澳太空卡打出，反之亦然。故此，在澳門實行電話實名制始終有打擊作用，否則會更易

此，必須確保現時採取的身份識別政策是打擊罪案的工具，既不會削弱使用者的隱私權，亦不會導致對數據內容有不當的控制。提案人保證，第二十四條及第二十五條所引入的身份識別制度，純粹是將現行適用於固網及流動電話用戶的規則擴大適用於預付式 SIM 卡的使用者。提案人亦表示，“對於電訊營運商與商店合作出售預付 SIM 卡，電訊商及有關商店應遵守《個人資料保護法》的規定，否則須負上法律責任。如不遵守法律關於這方一面的規定，則視乎具體情況，可根據行政違法行為（第 8/2005 號法律第三十條至第三十六條）或刑事違法行為（第 8/2005 號法律第三十七條至第四十二條）的規定，進行處罰，且針對這兩種情況亦可增加某些附加處罰（同上法律第四十三條及第四十四條）。”

委員會還詢問如何執行該政策，並關注如何核實使用者的身份。提案人解釋，對於預付卡電話的實名制的操作程序，將會考慮選擇電子認證的方式，這是用户最容易處理的方式。

5.2. 第二類補充性保安措施載於法案第二十六條，當中對保存及提供網絡地址轉換紀錄作出規範。根據現於第 11/2009 號法律《打擊電腦犯罪法》中新增的條文，互聯

成為犯罪地。”

網服務提供者必須將私人網絡地址轉換成公共網絡地址的紀錄保存一年。

為使互聯網有效運作，每個接入網絡的設備必須以數字代碼識別，以便適當發放和接收數據，並取得資訊。在當前使用的互聯網協議版本 4（IPv4），IP 地址由 32 位元組成，這使得這些地址的組合數量相對較少[24]。在 IPv6（IPv6 引入 128 位元組成）全面開發使用之前，必須限制用作網絡接入點的地址數量。因此，現時允許屬於同一私人網絡的多個不同設備（各自有本身的私人網絡地址）在網絡發出或接收數據時，共用一個公共網絡地址。為此，通過路由器將私人網絡地址轉換成公共網絡地址。基於 IPv4 的限制，該處理辦法是有着實際和技術上的需求，但當有需要識別私人網絡地址中的某一個設備時，例如某特定 IP 地址，尤其牽涉到犯罪調查時，則識別工作顯得較困難。保存網絡地址轉換紀錄的目的，是為了更便捷地識別涉及電腦犯罪的接入互聯網的終端機，從而識別行為人的身份。因此，對這些紀錄作出規定，並非為了瞭解通過電子途徑所作出的行為或用户曾瀏覽的網頁。

強制保存網絡地址轉換紀錄是透過在《打擊電腦犯罪法》中增加條文而落實。此舉導致使用該等紀錄的範圍受到限制：司法當局可根據第 11/2009 號法律第十五條的規

[24] IPv4 於全球提供約 42.9 億個 IP 地址。

定，在調查該法律所規定的犯罪及相關訴訟行為時，以及在針對用電子載體實施犯罪進行蒐證時，命令互聯網服務提供者提供有關紀錄。換言之，在調查其中一項犯罪時，刑事警察機關必須根據刑事訴訟法的規定，在法官許可後才可取得網絡地址轉換紀錄。

基於電腦犯罪或利用電腦系統犯罪的調查，及從電子載體中取證和蒐證的需要，委員會認為對保存及提供網絡地址轉換紀錄作強制規定是合理的。同時亦認為，透過補充適用《刑事訴訟法典》，市民的私隱已得到法律的保障。

四、細則性分析

委員會除了就法案進行上述的概括性審議工作外，亦已根據《立法會議事規則》第一百一十九條的規定，就法案所採納的具體解決方案與法案的立法原則的符合性作出審議，以及完善法律技術方面的內容。對於在小組會內曾分析的問題，以及對條文所引入的修改方面，須作特別說明的有以下的內容：

- **第一條：標的及宗旨**

在法案最初文本中，由於有關標的的條文以過於冗長的方式作出撰寫，因此，使人難以領會，而且與其他規定

相比較顯得重複。因此，致力簡化行文，刪除了第二條所規定的內容。另一方面，明確了法律的宗旨：保護關鍵基礎設施營運者的資訊網絡、電腦系統及電腦數據資料。這樣，行文明文規定了應受本法律維護的法益。行文確定後，有必要針對標題作出修改，改為“標的及宗旨”，以便更好地反映本條的內容。

最初文本	最後文本
第一條 **標的**	**第一條** **標的及宗旨**
本法律設立澳門特別行政區的網絡安全體系並規範其運作，旨在透過強化關鍵基礎設施營運者的網絡安全，維護福祉、公共安全及公共秩序等重大公共利益。	本法律建立及規範澳門特別行政區的網絡安全體系，以保護關鍵基礎設施營運者的資訊網絡、電腦系統及電腦數據資料。

- **第二條：定義**

在定義的條文中有多項修改。首先，對有關定義重新進行排序，作為整個法案的核心概念，首先定義“網絡安全”的事宜。

第一款（一）項：刪除了預防方法的例子[25]，認為沒有

[25] “……在以適當的技術工具，例如加密系統、“防火牆”、認證及防入侵機制等防毒應用程式及避免服務中斷的工具……”

需要在法律上有所規定。因為技術解決方法是不斷發展的。此外，根據第三條第一款（二）項及第二款的規定，該等解決方法將於技術規範上規定。

第一款（二）項：最初文本中對“資訊網絡”定義的技術準確性令人生疑。為了解決有關疑問，法案套用了國際使用的定義[26]及根據第七條第一款（三）項的規定，使用有關定義有助網絡安全領域的國際合作。

第一款（三）項：在“關鍵基礎設施”的定義中，最初文本中的“喪失功能”一詞被“停止運作或效能大幅降低”取代，作為顯示網絡和系統雖未完全不能使用但處於能力降低時亦會對社會造成損害，影響提供服務的效能。為避免出現不必要的重複，在這項還刪除了“不論其營運者屬公共性質或私人性質”的表述，因為該表述已經載於“關鍵基礎設施營運者”的定義上。

第一款（五）項：修訂了“未經許可的行為”的定義，作為與第 11/2009 號法律所規定和處罰的構成電腦犯罪的行為相聯繫。透過使用“進入、獲取、使用、提供、截取、損害或其他類型的干擾”的定義作聯繫。

[26] 尤其是二零一六年七月六日（歐盟）歐洲議會和理事會的第 2016/1148 號指令第四條 a）項關於“網絡和資訊系統”的定義。

第一款（六）項：在“網絡安全事故”的定義上，刪除了“未遂行為”的表述，從而排除在概念上屬輕微的情況，即使試圖攔截互聯網之間的傳輸或試圖傳播惡意程式，亦不會對網絡及資訊系統造成嚴重損害。受歐洲法律的啟發，“造成實際不利影響”一詞可限制概念的範圍，即排除對網絡及資訊系統安全性損害較小的行為。

第二款：法案最初文本的第二條（二）項援引了打擊電腦犯罪法有關“電腦系統”及“電腦數據資料”的定義。從技術角度來看，該援引實際上並不等於定義，因此採取了另外一種處理方法，將該定義的條文分為兩款，將第二款援引第 11/2009 號法律的有關“電腦系統”及“電腦數據資料”定義。該援引的缺點就是促使執法者須使用兩套法律工具來取得有關的法律定義，但是，亦提供了避免重複規範的好處及確保兩個法律中使用的定義具有相同的內容。因此，日後如有需要修改這些定義，只須在第 11/2009 號法律內作出修改就無須修改網絡安全法。

最初文本	最後文本
第二條 **定義**	**第二條** **定義**
為適用本法律，下列用語的含義為：	一、 為適用本法律，下列詞語的含義為：
（一）“資訊網絡”：是指一電腦系統的組件、支援	（一）“網絡安全”：是指澳門特別行政區為確保關

有關組件之間的通訊的網絡，以及該等組件所儲存、處理、交換或傳送的一組電腦數據資料，其目的是使有關組件及網絡得以運作、使用、受保護及維護；

（二）“電腦系統”及“電腦數據資料”：是指第11/2009號法律《打擊電腦犯罪法》規定的系統及數據資料；

（三）“網絡安全”：是指澳門特別行政區所推展的長期及多領域的活動，旨在確保關鍵基礎設施營運者所使用的資訊網絡及電腦系統的可操作性、完整性及可用性，以及電腦數據資料的保密性，並旨在以適當的技術工具，例如加密系統、“防火牆”、認證及防入侵機制等防毒應用程式及避免服務中斷的工具，防止該等資訊網絡、電腦系統及數據資料遭受未經許可的行為所損害或任何形式的影響；

（四）“關鍵基礎設施”：是指對社會利益及社會正常運作具有重要意義的鍵基礎設施營運者所使用的資訊網絡及電腦系統正常運作，以及電腦數據資料的完整性、保密性及可用性而開展的長期性跨領域活動，尤其防止該等網絡、系統及數據資料因未經許可的行為而受到不利影響；

（二）“資訊網絡”：

(1)互聯的電腦裝置或電腦系統；

(2)使電腦裝置及電腦系統互聯的電子通訊網絡，尤其是第14/2001號法律《電信綱要法》所指的電信網絡；

(3)於上兩分項所指的裝置、系統及網絡範圍內儲存、處理、交換或傳輸的電腦數據資料，以確保其運作、使用、保護及維護；

（三）“關鍵基礎設施”：是指對社會正常運作具有重要意義，且一旦遭到擾亂、破壞、數據資料洩漏、停止運作或效能大幅降低，可能嚴重危害社會福祉、公共安全、公共秩序或其他尤為重要的公共利益的資產、資訊

資產、網絡和系統，不論其營運者屬公共性質或私人性質，該等資產、網絡和系統一旦遭到破壞、數據資料洩漏或喪失功能，可能嚴重危害社會福祉、公共安全、公共秩序或其他尤為重要的公共利益； （五）“關鍵基礎設施營運者”：是指營運關鍵基礎設施及提供有關服務的公共或私人實體； （六）“未經許可的行為”：是指任何未經資訊網絡或電腦系統擁有者、該等網絡或系統的權利持有人同意或准許而存取或干擾的行為； （七）“網絡安全事故”：是指任何未經許可的行為或未遂行為所呈現的任何情況； （八）“網絡經營者”：是指具資格經營固定或流動的公共電信網絡及提供互聯網接入服務的實體。	網絡和電腦系統； （四）“關鍵基礎設施營運者”：是指營運關鍵基礎設施及提供有關服務的公共或私人實體； （五）“未經許可的行為”：是指未經資訊網絡、電腦系統或電腦數據資料的所有權人或其他權利人同意而對該等網絡、系統或數據資料實施進入、獲取、使用、提供、截取、損害或其他類型的干擾行為； （六）“網絡安全事故”：是指任何構成未經許可的行為的情況，以及通常對資訊網絡、電腦系統及電腦數據資料的安全造成實際不利影響的任何事件； （七）“網絡營運者”：是指具資格經營固定或流動的公共電信網絡及提供互聯網接入服務的實體。 二、為適用本法律的規定，“電腦系統”及“電腦數據資料”的含義，與第11/2009號法律《打擊電腦犯罪法》的相關定義規定相同。

● **第三條：網絡安全活動**

對該條的行文作了修改，以明確訂定發出技術規範是網絡安全活動的組成部分。為此，新的第一款（二）項提及："向關鍵基礎設施營運者發出具約束力的技術規範"；這種技術監管方式旨在"制定資訊網絡、電腦系統及電腦數據資料的安全程序和機制"（第二款第一部分）。根據提案人表示，將落實國際標準化組織和國際電工委員會的 ISO/IEC 27000 標準。技術規範以傳閱文件向全體關鍵基礎設施營運者發出，以及透過指引向特定類別的關鍵基礎設施營運者發出（第二款第二部分）。一般而言，技術規範須公佈於《澳門特別行政區公報》，但基於性質須進行保密時，則以簽收方式或以郵遞方式送交（第三款）。發出該等規範的權限賦予澳門特別行政區網安體系的任何實體，尤其是網絡安全委員會、網絡安全事故預警及應急中心及（十一個）監管實體。關於技術規範的部分制度載於最初文本第十一條第一款（二）項。

第一款第（五）項規定了檢視電腦數據資料的部分規定。基於其整體性質，該權力應在首次法律訂定時作出實質的界定。因此，關於檢視目的的表述（"以防止、偵測及打擊網絡安全事故"），是從最初文本第八條第二款（三）項搬移至現時的第三條第一款（五）項，並使用"網絡安全事故"這個概念及放棄採用"網絡入侵及攻擊

"這個表述，以避免引用新的法律用語。

最初文本	最後文本
第三條 **網絡安全活動**	**第三條** **網絡安全活動**
網絡安全活動按下列方式進行： （一）為實現網絡安全的宗旨，訂定總體方向、目的及策略； （二）由關鍵基礎設施營運者履行本法律及監察實體發出的指示或傳閱文件所規定的日常網絡安全義務及措施； （三） 為應對網絡安全事故，尤其是嚴重的事故，推行網絡安全例外性義務及措施； （四）監察關鍵基礎設施營運者的網絡安全數據資料； （五）監督網絡安全義務及措施的確切履行，以及提起相應的處罰程序。	一、網絡安全活動按下列方式進行： （一）為達至適切的網絡安全標準，訂定方針、目的及策略； （二）向關鍵基礎設施營運者發出具約束力的技術規範； （三）履行本法律及技術規範所定的義務； （四）為應對網絡安全事故，尤其是正在發生或即將發生的嚴重網絡安全事故，執行網絡安全例外措施； （五）檢視關鍵基礎設施營運者的資訊網絡與互聯網之間傳輸的電腦數據資料，以防止、偵測及打擊網絡安全事故； （六）監察網絡安全義務及措施的履行情況，以及提起相應的處罰程序。 二、技術規範旨在制定資訊網絡、電腦系統及電腦數

	據資料的安全程序和機制，由第二章所指的實體透過傳閱文件向全體關鍵基礎設施營運者發出，或透過指引向特定類別的關鍵基礎設施營運者發出。 三、傳閱文件及指引均須公佈於《澳門特別行政區公報》；但基於性質須進行保密者，則以簽收方式或以附收件回執的郵政掛號方式送交。

● **第四條：適用的主體範圍**

第一款：第一款的行文旨在清楚及簡要地識別該法律的兩類主體：關鍵基礎設施的公共營運者及私人營運者。另一方面，亦明確規範法律的適用範圍（“本法律適用於……”），而不是按最初文本的規定須遵守網絡安全義務（“下列實體須遵守網絡安全的義務”）。

第二款：最初文本規定“澳門特別行政區的所有公共部門、機關及實體”均被視為關鍵基礎設施的公共營運者，並提供了一般規則中包括的公共實體的附加列舉例子。基於該行文的內容曾引起過一些疑問，因此，在不修改其範圍下已對其進行修訂及完善。最後，在維持所有公

共實體均被視為關鍵基礎設施公共營運者的一般原則下，再由第二款各項以組別方式列舉。該一般原則尤其以概括形式作出，如第二款(二)項規定的："澳門特別行政區公共部門"。

於（一）項刪除了對廉政專員辦公室及審計長辦公室的提述，因為它們已納入《基本法》及第 24/2010 號行政法規《澳門特別行政區主要官員通則》中的主要官員的概念。另外，根據第 14/1999 號行政法規（《行政長官及司長辦公室通則》）規定，因不存在政府主要官員的辦公室及有關行政輔助部門，故刪除有關提述，以便形式上區分有關辦公室及行政輔助部門。

第三款（三）項：法案將行政公益法人視為關鍵基礎設施私人營運者。這規定載於法案最初文本第四條（二）項（3）分項。然而，立法原意曾是(而且仍然是）：並非是所有行政公益法人均受法律適用的約束，而是其當中涉及進行對網絡安全具重要性的活動的才被約束。這一立法取向在最初文本中以排除規定表達：第五條第一款（三）項排除了"由法規定性為行政公益法人的，且其宗旨與慈善、救濟、教育、文化或娛樂活動有關的私法人。"這種消極界定的法律適用範圍，在細則性審議時引起了疑問。首先，由於"其宗旨與……"這一表述與八月十二日第 11/96/M 號法律第三條第一款所規定的"推行目標"的標

準有所不同，所以標準模糊，因為法人的宗旨可與多於一項所指活動有關；其次，由於在描述目的時所使用的術語與八月十二日第 11/96/M 號法律並不完全相符，因此提出是否有意訂定有別於上述法律所規定的類別的質疑。最後，委員會得悉提案人就《網絡安全法》的執行方面，目前僅有兩個從事科學及技術研究的行政公益法人。因此，為免對將來法律的適用範圍產生疑問，故採取了正面的界定，規定只有科學及技術領域的行政公益法人才包含在網絡安全法的適用的主體範圍。

對法案與八月十二日第 11/96/M 號法律等其他法規進行了用語方面的統一。因此，“行政公益法人”這個法律概念取代了“依法被定性為行政公益法人的私法人”這一表述。

最初文本	最後文本
第四條 **適用的主體範圍**	**第四條** **適用的主體範圍**
下列實體須遵守網絡安全的義務： （一）關鍵基礎設施的公共營運者，包括澳門特別行政區的所有公共部門、機關及實體，包括： （1）行政長官辦公室、政府主要官員的辦公室及有關行政輔助部門、立法會輔助部門、終審法院院長辦公	一、本法律適用於關鍵基礎設施的公共及私人營運者。 二、關鍵基礎設施公共營運者包括： （一）行政長官辦公室、主要官員的辦公室、立法會輔助部門、終審法院院長辦公室及檢察長辦公室；

室、檢察長辦公室、廉政專員辦公室及審計長辦公室； （2） 以任何形式設立的公務法人及自治基金； （3） 無法律人格但具財產及財政自治權的其他公共部門及機構； （二）關鍵基礎設施的私人營運者，包括： （1） 住所設於澳門特別行政區或外地且具資格以經營批給、向行政當局提供服務、准照、執照或相同性質的憑證的方式在下列特定領域從事業務的所有私法實體： （i）供水； （ii）銀行、財務及保險業； （iii）在醫院提供衛生護理； （iv）污水處理和垃圾收集及處理； （v）燃料和受衛生檢疫及植物檢疫的食品的總批發供應； （vi）法定屠宰場宰殺動物； （vii）電力及天然氣的供應及分配； （viii）按預定路線或航線、班次、時間表及收費提供的定期海、陸、空運輸的公共服務；	（二）澳門特別行政區公共部門； （三）以任何形式設立的公務法人及自治基金。 三、關鍵基礎設施私人營運者包括： （一）住所設於澳門特別行政區或外地，且具資格以經營批給、向行政當局提供服務、准照、執照或相同性質的憑證的方式，在下列特定領域從事業務的私法實體： （1）供水； （2）銀行、財務及保險業； （3）在醫院提供衛生護理； （4）污水處理和垃圾收集及處理； （5）燃料和受衛生檢疫及植物檢疫的食品的總批發供應； （6）法定屠宰場宰殺動物； （7）電力及天然氣的供應及分配； （8）按預定路線或航線、班次、時間表及收費提供的定期海、陸、空運輸的公共服務； （9）港口、碼頭、機場及直升機場的營運； （10）視聽廣播； （11）經營娛樂場幸運博彩； （12）經營固定或流動的

(ix) 港口、碼頭、機場及直升機場的營運； (x) 視聽廣播； (xi) 經營娛樂場幸運博彩； (xii) 經營固定或流動的公共電信網絡，以及提供互聯網接入服務； (2) 全公共資本公司； (3) 依法被定性為行政公益法人的私法人。	公共電信網絡，以及提供互聯網接入服務； (二) 全公共資本公司； (三) 活動僅限於科學及技術領域的行政公益法人。

● **第七條：網絡安全委員會**

委員會與提案人就網絡安全委員會的角色及將之反映在法案條文中的形式進行討論。有關討論導致第七條的多項修改。

議員們認為最初文本所採用的“網絡安全常設委員會”這一名稱可能會弱化這一機關的角色，以及降低了其作為澳門特別行政區行政架構的份量。原則上，行政機關都是常設的，其名稱無須顯現這一特性。基於這一原因，修改了委員會的名稱，改稱為網絡安全委員會。

修改了本條的引文部分。最初文本採用了“政府的決策機關” 這一表述方式。用決策性質而非諮詢性質表述，

這與第三項規定的具有建議政府訂立協議、議定書或合同的權限不相符。最後文本改為規定網絡安全委員會由行政長官領導。

議員們建議把第二項規定的權限載入這一條，以釐清網絡安全委員會與納入由本法律創建的體系內的其他實體的關係。

最初文本	最後文本
第七條 **網絡安全常設委員會**	**第七條** **網絡安全委員會**
常設委員會是政府的決策機關，其負責： （一）確保第三條（一）項所指的活動； （二）建議政府與澳門特別行政區或外地的公共或私人實體訂立或修訂協議、協定書或合同，使澳門特別行政區達到更高的網絡安全標準。	委員會是由行政長官領導的機關，其負責： （一）確保第三條第一款（一）項所指的活動； （二）監督網絡安全體系內其他實體在本法律範圍內所開展的活動； （三） 建議政府與澳門特別行政區或外地的公共或私人實體訂立或修訂有助提高澳門特別行政區網絡安全標準的協議、議定書或合同。

● 第八條：網絡安全事故預警及應急中心

修改了第八條，以闡明網絡安全事故預警及應急中心的法律性質。提案人解釋，按照立法原意，該中心並非一個行政機關，而是一個由多個公共部門組成的具有技術性的快速回應小組。第一款起首部份反映了這一意圖，訂明“預警及應急中心是網絡安全事故預警及應急方面的專門技術性機構”。

第二款改為規範第一款（五）項規定的實施檢視的權限，該權限授予司法警察局，而且訂明有關檢視的範圍。本意見書的一般性分析已說明訂定有關範圍的原因。

最初文本	最後文本
第八條 **網絡安全事故預警及應急中心**	**第八條** **網絡安全事故預警及應急中心**
一、預警及應急中心由在網絡安全方面具特別技術職權的公共實體組成，並由司法警察局統籌。	一、預警及應急中心是網絡安全事故預警及應急方面的專門技術性機構，由司法警察局統籌，其負責： （一）集中接收與網絡安全事故有關的資訊； （二）擬定第三條第一款（四）項規定的網絡安全措施，並協調各參與實體的應對，以避免或減少網絡安全事故的影響； （三）確保並促進組織
二、預警及應急中心具下列職責，但不影響司法警察局職權及權力制度的適用： （一）確保第三條（三）項所指的活動，為此集中接收網絡安全事故預警信息，並協調不同參與實體之間的	

合作及適當行動，以及與外地的同類實體合作，以防止或減少網絡安全事故的影響； （二） 按照常設委員會制訂的指引，訂定網絡安全事故的嚴重性等級，以及事故預警及應急行動的指示和程序，並向網絡安全體系的所有參與者作出宣傳； （三） 透過司法警察局實時監察關鍵基礎設施營運者網絡與互聯網之間以機器語言方式傳輸的電腦數據資料的流量及特徵，以防止、偵察及打擊網絡入侵及攻擊； （四） 在必要時發出網絡安全事故預警信息。	間合作，包括與外地的同類實體合作； （四） 按嚴重性等級對網絡安全事故分級，並按有關等級制定預警及應對程序； （五） 根據第三條第一款（五）項的規定，實時檢視關鍵基礎設施營運者的資訊網絡與互聯網之間傳輸的電腦數據資料的流量及特徵； （六） 就網絡安全事故發出預警； （七） 應監管實體的要求，在其履行職責時給予技術支援。 二、上款（五）項所指的檢視由司法警察局進行，且僅涉及機器語言，不得收集電腦數據資料或以任何方式對該等資料解碼。 三、以上兩款的規定不影響司法警察局的職權及權力制度的適用。

● 第九條：網絡安全監管實體

在最初文本中，關於監管實體的權限存在缺口。因此，致力作出緻密的規範，把分散於條文中的各種權限匯集於這一條。形式上，權限的清單可讓所有與網絡安全體

系內的實體相關的所有條文具有一種相同的結構。

關於監管實體的性質，改為訂明是“公共行政部門或機構”，該等已存在的部門或機構將根據本法律的規定，履行新的職能。

最初文本	最後文本
第九條 **網絡安全監管實體**	**第九條** **網絡安全監管實體**
一、網絡安全監察實體是指對關鍵基礎設施營運者履行網絡安全監察職責的實體。	一、監管實體是公共行政部門或機構，在其職責範圍內具有下列權限： （一） 確保本法律及技術規範所定的義務獲履行，但不影響預警及應急中心在第三條第一款（四）項所指情況下的本身權限； （二） 監察關鍵基礎設施營運者有關其網絡安全的計劃及行動； （三） 行使本法律規定的處罰權限。
二、上款所指的職責以下列方式履行： （一） 由行政公職局對關鍵基礎設施的公共營運者履行監察職責； （二） 由以行政法規指定的其他公共實體對關鍵基礎設施的私人營運者履行監察職責。	二、上款所指的權限由下列者行使： （一） 對關鍵基礎設施公共營運者，由行政公職局行使； （二） 對關鍵基礎設施私人營運者，由行政法規指定的公共實體行使。

● **第十條：組織性義務**

關於組織性義務，除前文所述（一般性分析 4.1.，還需指出，對網絡安全主要負責人的替代人這一概念的理解有所改變。最初文本規定網絡安全主要負責人不在或因故不能視事時，有責任“確保由另一名具備資格且熟悉有關系統以及便於預警及應急中心聯絡的對話人替代，該對話人應在澳門特別行政區聽候安排”。規定的是主要負責人的一項義務。但是從嚴格意義上，本條規定的是私人營運者的義務。該規定推定這種替代是偶發且短暫的，因此替代人無需符合網絡安全主要負責人應具備的適當資格。經考慮，得出的結論是，既然需要進行任職資格審查，則應針對任何擔任此職務的人，不論是以主要負責人身份還是以代任制度擔任。因此，法案最後文本要求須同時指定兩個人，分別擔任網絡安全主要負責人及其替代人，兩者須符合同樣的規定和要件，包括以澳門特別行政區為常居地、具備適當資格及專業經驗、可隨時聯絡。

最初文本	最後文本
第十條 **組織性義務**	**第十條** **組織性義務**
一、關鍵基礎設施的私人營運者在組織方面的義務如下：	一、關鍵基礎設施私人營運者在組織方面的義務如下：
（一）配置網絡安全管理的單位的運作架構，並指定	（一）設立具能力執行網絡安全內部保護措施的網絡

相關的負責人運用人力資源、財政資源、物資資源及財產資源，落實維護網絡安全的內部措施； （二）審查關鍵基礎設施營運者的網絡安全主要負責人是否具備適當資格及專業經驗，為此必須徵求司法警察局的意見； （三）建立網絡安全的投訴和舉報的機制及渠道。 二、為適用上款（二）項的規定，因下列任一犯罪被澳門特別行政區或外地法院判罪者，且有關判決已轉為確定，則視為不具備適當資格擔任網絡安全主要負責人的職務： （一）第 2/2009 號法律《維護國家安全法》規定的犯罪； （二）電腦犯罪或偽造技術註記罪、損壞或取去技術註記罪、以資訊方法作侵入罪、不當利用秘密罪、違反函件或電訊保密罪或違反職業保密罪； （三）其他可處超過五年	安全管理單位； （二）為網絡安全管理單位配置合適的人力、財政、物力及財產資源； （三）從具備適當資格及專業經驗且以澳門特別行政區為常居地的人士中指定網絡安全主要負責人及其替代人； （四）採取措施確保預警及應急中心能隨時聯絡網絡安全主要負責人及其替代人； （五）建立網絡安全的投訴和舉報機制。 二、在審查適當資格時，應考慮任何基於其嚴重性、多發性或其他應予重視的情節而對確保網絡安全構成重大疑慮的事實。 三、在不影響上款規定的情況下，禁止關鍵基礎設施私人營運者指定因下列任一犯罪而透過確定判決被判刑的人在下款規定的期間內成為網絡安全主要負責人及其替代人：

徒刑的犯罪。 三、如屬上款（三）項規定的情況，澳門特別行政區以外地方的法院所宣示的判決，僅在有關行為根據澳門特別行政區法例亦構成犯罪時，方產生上款（二）及（三）項規定的效力。 四、網絡安全主要負責人在澳門特別行政區應有常居所，以便預警及應急中心可隨時聯絡該負責人；有關負責人不在或因故不能視事時，應確保由另一名具備資格且熟悉有關系統以及便於預警及應急中心聯絡的對話人替代，該對話人應在澳門特別行政區聽候安排。	（一）第 2/2009 號法律《維護國家安全法》規定的犯罪； （二）電腦犯罪或偽造技術註記罪、損壞或取去技術註記罪、以資訊方法作侵入罪、不當利用秘密罪、違反函件或電訊保密罪或違反職業保密罪； （三）其他可處超過五年徒刑的犯罪。 四、禁止期間如下： （一）如被判處五年或以下徒刑，自暫緩執行刑罰期滿、服刑終止或延長服刑終止之日起計五年； （二）如被判處超過五年的實際徒刑，自服刑終止或延長服刑終止之日起計十年。 五、由外地法院宣示的判決，對第三款（二）項及（三）項的效力而言具重要性；如屬該款（三）項的情況，則有關行為根據澳門特別行政區的法例規定亦構成犯罪。

	六、就擬指定為網絡安全主要負責人及其替代人的人士的適當資格及倘有的禁止情況，關鍵基礎設施私人營運者應徵求司法警察局的意見。

● **第十七條：附加處罰**

原第一款第（一）項規定了剝奪參與公開招標的權利這一附加處罰。委員會認為有同樣的理由禁止參與直接磋商和限定對象諮詢。七月十五日第 6/96/M 號法律《妨害公共衛生及經濟之違法行為之法律制度》第十條第一款 b）項有此類規定。因此，附加處罰的範圍得到擴大，包括了參與公共部門、機關及實體有關取得財貨或勞務的直接磋商和限定對象諮詢。

最初文本	最後文本
第十六條 **附加處罰**	**第十七條** **附加處罰**
一、關鍵基礎設施的私人營運者違反第十條第一款（一）及（二）項、第十一條第一款、第十二條（一）項及第十三條（一）項的規定，可單獨或合併科處下列附加處罰：	一、違反第十條第一款（一）至（三）項、第十一條（一）項、第十二條（一）項及第十三條（一）項的規定，可單獨或合併科處下列附加處罰： （一）剝奪參與公共部

（一）剝奪參與公共部門、機關及實體購置物品或取得服務的公開招標的權利； （二）剝奪獲公共部門、機關及實體發給津貼或利益的權利。 二、上款所指的附加處罰的最長期間，為自開始執行有關附加處罰之日起計兩年。	門、機關及實體有關取得財貨或勞務的直接磋商、限定對象諮詢或公開招標的權利； （二）剝奪獲公共部門、機關及實體發給津貼或利益的權利。 二、上款所指的附加處罰最長期間為兩年，自相關決定轉為不可申訴之日起計算。

● **第十八條：勸誡**

第四章規定的處罰制度包括勸誡。其目的是，對於履行義務時存在的不合規範情況，給予糾正的機會，而不科處針對行政違法行為的主要處罰和附加處罰。所以，對應的是可令違法程序消滅的初步階段。勸誡始於對行為人行為的不法性作出的判斷，但該行為不法性的程度較低。該行為僅是履行網絡安全義務上的不合規範，並非完全、絕對的不履行；此不合規範可以糾正；而且此不合規範未造成特別嚴重的後果，換言之，對網絡安全不構成嚴重危險。而且，行為人不是累犯也是不法性程度較低的原因。如符合這些要件，行為人須在指定期間內補正不合規範的情況，此後或程序完結，或因監管實體認為雖然已經得到補正，不合規範的情況仍不可免於申誡，而發出單純勸

誡。第十八條第二款規定："不合規範的情況已在指定期間內獲補正，監管實體可對違法者僅作出勸誡的決定"。如不合規範的情況在指定期間內未獲補正，則針對行政違法行為的處理程序繼續正常進行，科處相應的處罰（第三款）。本法案中的勸誡參考了本地法律體系中現行的類似規定，尤其是七月五日第 32/93/M 號法令通過的《澳門地區金融體系的法律制度》第一百三十條。

對最初文本進行的修改是為清晰作出勸誡的前提。因為如果僅是"涉嫌不遵守……義務"，不應受到勸誡。僅當實際出現不遵守的情況時，才可因其性質被視為單純的不合規範。另外，在最初文本中，勸誡的內容是在指定期限內糾正違規情況（"監察實體可勸誡其於指定期間內補正不合規範的情況"）。經過斟酌，認為在程序的最後階段發出勸誡較為恰當，在發現違規且糾正之後發出訓誡，避免此類情況再次發生。

最初文本	最後文本
第十七條 **勸誡**	**第十八條** **勸誡**
一、如發現關鍵基礎設施的私人營運者涉嫌不遵守第十條至第十三條規定的義務，監察實體可勸誡其於指定期間內補正不合規範的情	一、如發現在履行網絡安全義務時存在不合規範情況且屬下列者，監管實體可指定補正期間： （一）不合規範為可予

況，但屬下列情況則除外： （一）有關情況對網絡安全構成實質危險； （二）被針對的營運者不足一年內曾因相同性質的行政違法行為被處罰。 二、如關鍵基礎設施的私人營運者未有在上款所指的期間內補正不合規範的情況，監察實體須提起有關的行政違法處罰程序。	補正且對網絡安全不構成嚴重危險者； （二）非為累犯者。 二、不合規範的情況已在指定期間內獲補正，監管實體可對違法者僅作出勸誡的決定。 三、如不合規範的情況在指定期間內未獲補正，則針對違法行為的處罰程序繼續進行。

● **第二十四條：用戶身份模塊卡**

採用實名制的期限由原來的六十日延長至一百二十日，給予網絡營運者更多的時間履行第二十四條所規定的義務。這一延長同樣亦使到整個申請和提供身份識別資料的程序可以在該期限內完成。

第二款規定，當不提供所需資料時，則中止有關服務。同時亦規定，只要該卡仍有效，提供有關資料便可以重新激活服務。否則，中止便會變相成為一種損害消費者的處罰，但原意單純是為了勸導使用者合作，提供身份識別資料。

對於違反身份資料義務的處罰，最初文本準用“訂立准入及經營提供互聯網服務的業務的制度的法規作出處罰，並按該法規所定的最高罰款額處罰”。考慮到這一解決方案無法確保到必需的法律確定性和安定性，且可能會與第 13/2009 號法律《關於訂定內部規範的法律制度》第四條第二款規定的法律完整性原則相悖，因為當中並沒有充分地指出所適用的法規和有關違反行為的罰則，基於此，最後文本明文規定了所適用的處罰幅度，即澳門幣五萬元至十五萬元的罰款。同時亦規定了將有關的處罰權限賦予郵電局。第二十五條（客戶身份資料）亦採用了相同的解決方案。

最初文本	最後文本
第二十三條 **本法律生效前已購買的用戶身份模塊卡**	**第二十四條** **用戶身份模塊卡**
一、網絡經營者應在本法律生效後六十日內，採取措施獲取在本法律生效前已購買的無須預先提供身份資料的預付式“用戶身份模塊卡”（下稱“SIM卡”）用戶的身份資料並作出登記。	一、網絡營運者應自本法律生效之日起一百二十日內採取措施，以便對在本法律生效前售出的無須預先提供身份資料的預付式用戶身份模塊卡（下稱“SIM 卡”）用戶的身份資料進行登記。
二、SIM 卡的購買者或用戶應在網絡經營者要求提供身份資料後六十日內提供有	二、如 SIM 卡用戶在上款所指的期間屆滿時仍不提供其身份資料，網絡營運者應

關資料。 三、如 SIM 卡的用戶不履行提供身份資料的義務，網絡經營者應自上款所指的期間屆滿日起停止激活有關SIM卡，且不影響 SIM 卡有效期屆滿出現的服務暫停的情況。 四、如網絡經營者不履行第一款及第三款規定的義務，構成行政違法行為；對該行為可根據訂立准入及經營提供互聯網服務的業務的制度的法規作出處罰，並按該法規所定的最高罰款額處罰。	中止有關服務，但不影響在用戶提供身份資料之日重新激活該卡。 三、不履行以上兩款規定的義務構成行政違法行為，科澳門幣五萬元至十五萬元的罰款。 四、郵電局具權限就上款所指的行政違法行為提起處罰程序、指定預審員及作出處罰。

● **第二十六條：增加第 11/2009 號法律的條文**

強制保存和提供網絡地址轉換紀錄是透過在《打擊電腦犯罪法》中增加條文而落實。最初文本的解決方案是在第 11/2009 號法律第三章中增加第十五-A 條，而該章的內容乃涉及刑事程序的規定。然而，新增條文的內容不僅與程序事宜無關，而且更規定了一項違反該條所規定的義務時所構成的行政違法行為。這一系統編列會對上述法律的

內部連貫性構成影響。因此，最後文本轉為規定，透過新增一個標題為“行政違法行為”的獨立第三-A 章增加有關的條文。而且，亦將該處罰權限規定在新增的第十六-B 條內。

最初文本	最後文本
第二十五條 **增加第 11/2009 號法律的條文** 在第 11/2009 號法律內增加第十五-A 條，內容如下：	**第二十六條** **增加第 11/2009 號法律的條文** 在第 11/2009 號法律內增加由第十六-A 條及第十六-B 條組成的第三-A 章，標題為“行政違法行為”，內容如下：
“第十五-A 條 **保存及提供網絡地址轉換紀錄**	**“第十六-A 條** **保存及提供網絡地址轉換紀錄**
一、互聯網服務提供者必須將私人網絡地址轉換成公共網絡地址的紀錄保存一年。	一、互聯網服務提供者必須將私人網絡地址轉換成公共網絡地址的紀錄保存一年。
二、不履行上款規定的義務構成行政違法行為；對該行為可根據訂立准入及經營提供互聯網服務的業務的制度的法規作出處罰，並按該法規所定的最高罰款額處罰。	二、不履行上款規定的義務構成行政違法行為，科澳門幣五萬元至十五萬元的罰款。 三、具權限的司法當局在必要時可命令提供第一款所指的紀錄，為此須遵守第十五條第一款至第四款的規定。

三、具權限的司法當局在必要時可命令提供第一款所指的紀錄，為此須遵循上條第一款至第四款的規定。”	第十六-B條 **權限** 郵電局具權限就上條第二款所指的行政違法行為提起處罰程序、指定預審員及作出處罰。”

● **最初文本第二十六條——適用的補充法律**

該條原本規定對多項法規的補充適用，因認為沒有需要而被刪除了。《行政程序法典》的補充適用是源於該法典第二條的規定。此外，第二十六條第二款的規定與十月四日第 52/99/M 號法令（行政上之違法行為之一般制度及程序）第三條第三款規定的內容相對應。

最初文本	最後文本
第二十六條 **適用的補充法律** 一、《行政程序法典》和《行政訴訟法典》補充適用於本法律規定的行政行為。 二、十月四日第 52/99/M 號法令《行政上之違法行為之一般制度及程序》、經必要配合後的《行政程序法典》的規定、刑法及刑事訴訟的一般原則，依次補充適用於本法律規定的行政違法行為。	

● 第二十七條：補充規範

在補充規範中，最初文本只規定了監管實體的指定。此規定現擴大至受監管實體監管的關鍵基礎設施私人營運者的指定。期望能更準確地建立監管人員與私人經營者之間的關係。

此外，還簡化了行文，刪除了行政長官在制定補充法規時應考慮的法規的提述。

最初文本	最後文本
第二十七條 補充規範 執行本法律所需的補充規範，尤其關於下列事宜的規範，由行政長官以行政法規或對外規範性批示制定： （一）訂定常設委員會、預警及應急中心的組成、職權及運作方式； （二）經考慮第四條（二）項所指實體負責的活動的性質或範疇、第 2/1999 號法律《政府組織綱要法》及第 6/1999 號行政法規《政府部門及實體的組織、職權與運作》規定的指引，列出第九條第二款（二）項所指的監察實體。	第二十七條 補充規範 執行本法律所需的補充規範，尤其針對下列事宜，由行政長官以補充性行政法規或對外規範性批示制定： （一）委員會和預警及應急中心的組成、權限及運作方式； （二）指定監管實體及受該等實體監管的關鍵基礎設施私人營運者。

● 第二十八條：生效

最初文本規定本法律自公佈後滿一百八十日起生效，但此日期並不包括私人內聯網地址轉換成互聯網公共網絡地址（IP）的紀錄保存義務的生效。原第二十八條第二款規定，網絡經營者必須在另一日期起履行該義務，並希望是較後的日期，以便經營者可以為履行該義務作好必需的準備。

在細則性分析過程中，政府向委員會表示，認為沒有理由將法律生效與第二十五條的產生效力作不同的處理，因為一百八十日的待生效期已足以讓營運者具備履行全部法定義務所需的條件。

最初文本	最後文本
第二十八條 生效及產生效力 一、本法律自公佈後滿一百八十日起生效。 二、第二十五條的規定自二零一　年　月　日起產生效力。	第二十八條 生效 本法律自公佈後滿一百八十日起生效。

● **法律技術方面的調整**

除以上各點所述，委員會亦對多項規定的行文和系統編列作出改善，以使其在法律技術上更為完善，但實質內容不受影響。

五、結論

委員會經細則性審議及分析後認為：

（一） 本法案最後文本具備在全體會議作細則性審議及表決的必需要件；

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

二零一九年五月二十二日

委員會

何潤生
（主席）

馬志成
（秘書）

高開賢

區錦新

李靜儀

宋碧琪

葉兆佳

邱庭彪

馮家超

林倫偉