

四、在本法律生效之前取得憑證，應按照第十五條第一款申請登記但未登記的須登記的事實，可由利害關係人自本法律生效之日起十八個月內申請登記，且無須支付同條第四款所規定增加的手續費用。

第八十二條
補充法律

一、物業登記的相關規定經適當配合後，在不抵觸船舶商業登記的性質及本法律規定的前提下，適用於船舶的商業登記。

二、海事登記的相關規定，按上款所定的條件亦適用於船舶的商業登記。

第八十三條
生效

本法律自公佈後滿九十日起生效。

二零一九年六月十日通過。

立法會主席 賀一誠

二零一九年六月十三日簽署。

命令公佈。

行政長官 崔世安

澳門特別行政區
第 13/2019 號法律

網絡安全法

立法會根據《澳門特別行政區基本法》第七十一條（一）項，制定本法律。

第一章
一般規定

第一條
標的及宗旨

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。

4. Os registos de factos titulados em data anterior à entrada em vigor da presente lei, que devam ser requeridos nos termos do n.º 1 do artigo 15.º, e que ainda não tenham sido registados, podem ser requeridos pelos interessados dentro do prazo de 18 meses a contar da data da entrada em vigor desta lei, sem que lhes seja aplicado o acréscimo de emolumentos previsto no n.º 4 do mesmo artigo.

Artigo 82.º

Direito subsidiário

1. São aplicáveis ao registo comercial de embarcações, com as necessárias adaptações, as disposições legais relativas ao registo predial que não sejam contrárias à natureza daquele e às disposições da presente lei.

2. Ao registo comercial de embarcações são ainda aplicáveis, nos mesmos termos, as normas relativas ao registo marítimo.

Artigo 83.º

Entrada em vigor

A presente lei entra em vigor 90 dias após a data da sua publicação.

Aprovada em 10 de Junho de 2019.

O Presidente da Assembleia Legislativa, *Ho Iat Seng*.

Assinada em 13 de Junho de 2019.

Publique-se.

O Chefe do Executivo, *Chui Sai On*.

REGIÃO ADMINISTRATIVA ESPECIAL
DE MACAU

Lei n.º 13/2019

Lei da cibersegurança

A Assembleia Legislativa decreta, nos termos da alínea 1) do artigo 71.º da Lei Básica da Região Administrativa Especial de Macau, para valer como lei, o seguinte:

CAPÍTULO I

Disposições gerais

Artigo 1.º

Objecto e finalidade

A presente lei estabelece e regula o sistema de cibersegurança da Região Administrativa Especial de Macau, doravante designada por RAEM, visando a protecção das redes, sistemas e dados informáticos dos operadores de infra-estruturas críticas.

第二條

定義

一、為適用本法律，下列用語的含義為：

(一) “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；

(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

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；

Artigo 2.º

Definições

1. Para efeitos da presente lei, entende-se por:

1) «Cibersegurança», a actividade permanente e plurisectorial desenvolvida pela RAEM com o objectivo de assegurar o normal funcionamento das redes e sistemas informáticos utilizados pelos operadores de infra-estruturas críticas e a integridade, confidencialidade e disponibilidade dos dados informáticos, prevenindo, em especial, que tais redes, sistemas e dados sejam comprometidos por actos não autorizados;

2) «Redes informáticas»:

(1) Os dispositivos e ou sistemas informáticos interligados;

(2) As redes de comunicações electrónicas, através das quais se processa a interligação de dispositivos e sistemas, designadamente as redes de telecomunicações referidas na Lei n.º 14/2001 (Lei de Bases das Telecomunicações); e

(3) Os dados informáticos armazenados, tratados, trocados ou transmitidos no âmbito dos dispositivos, sistemas e redes referidos nas sublinéas anteriores, tendo em vista o seu funcionamento, utilização, protecção e manutenção;

3) «Infra-estruturas críticas», os patrimónios, redes e sistemas informáticos relevantes para o normal funcionamento da sociedade, e cuja perturbação, destruição, revelação de dados, suspensão de funcionamento ou diminuição significativa da eficiência é susceptível de causar prejuízos graves para o bem-estar, segurança ou ordem públicas ou outro interesse público especialmente relevante;

4) «Operadores de infra-estruturas críticas», as entidades, públicas ou privadas, que operam infra-estruturas críticas e que prestam serviços ligados às mesmas;

5) «Acto não autorizado», o acesso, obtenção, utilização, disponibilização, interceptação, dano ou outro tipo de interferência nas redes, sistemas e dados informáticos não consentidos pelos seus proprietários ou demais titulares de direitos sobre eles;

6) «Incidente de cibersegurança», qualquer situação que configure um acto não autorizado e, em geral, qualquer evento com um efeito real adverso na segurança das redes, sistemas e dados informáticos;

7) «Operadores de redes», as entidades habilitadas a explorar redes públicas de telecomunicações fixas ou móveis e a prestar serviços de acesso à *internet*.

2. Para efeitos do disposto na presente lei, as expressões «sistema informático» e «dados informáticos» são entendidas nos termos das respectivas definições constantes da Lei n.º 11/2009 (Lei de combate à criminalidade informática).

Artigo 3.º

Actividade de cibersegurança

1. A actividade de cibersegurança é prosseguida mediante:

1) A definição de orientações, objectivos e estratégias com vista à prossecução das finalidades da cibersegurança;

(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

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；

(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；

2) A emissão de normas técnicas vinculativas para os operadores de infra-estruturas críticas;

3) O cumprimento dos deveres previstos na presente lei e nas normas técnicas;

4) A execução de medidas de cibersegurança excepcionais que visem dar resposta a incidentes de cibersegurança, em especial quando ocorram ou estejam eminentes incidentes graves;

5) A monitorização dos dados informáticos transmitidos entre as redes dos operadores de infra-estruturas críticas e a internet, com a finalidade de prevenir, detectar e combater incidentes de cibersegurança;

6) A fiscalização do cumprimento dos deveres e medidas de cibersegurança e a instauração dos correspondentes procedimentos sancionatórios.

2. As normas técnicas visam definir processos e mecanismos de segurança das redes, sistemas e dados informáticos e são emitidas pelas entidades referidas no capítulo II através de circulares, dirigidas à generalidade dos operadores de infra-estruturas críticas ou de instruções, dirigidas a categorias específicas de operadores de infra-estruturas críticas.

3. As circulares e instruções são publicadas no *Boletim Oficial da Região Administrativa Especial de Macau* ou, quando a sua natureza reservada o justifique, entregues por protocolo ou expedidas sob registo postal com aviso de recepção.

Artigo 4.º

Âmbito subjectivo de aplicação

1. A presente lei aplica-se aos operadores públicos e privados de infra-estruturas críticas.

2. São operadores públicos de infra-estruturas críticas:

1) O Gabinete do Chefe do Executivo, os gabinetes dos titulares dos principais cargos, os serviços de apoio à Assembleia Legislativa, o Gabinete do Presidente do Tribunal de Última Instância e o Gabinete do Procurador;

2) Os serviços públicos da RAEM;

3) Os institutos públicos e fundos autónomos, qualquer que seja a modalidade que revistam.

3. São operadores privados de infra-estruturas críticas:

1) Todas as entidades de direito privado, com sede na RAEM ou no exterior, habilitadas a exercer actividades nos domínios a seguir especificados, seja a título de concessão de exploração, de prestação de serviços à Administração ou de licenciamento, alvará ou título de idêntica natureza:

(1) Abastecimento de água;

(2) Actividade bancária, financeira e seguradora;

(3) Prestação de cuidados de saúde em hospitais;

(4) Tratamento de águas residuais e recolha e tratamento de resíduos;

(5) Abastecimento público grossista de combustíveis e de produtos alimentares sujeitos a controlos sanitários e fitossanitários;

- (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。

第五條

不適用及豁免

一、本法律的規定不適用於下列者：

- (一) 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；
- (二) 其業務僅限於娛樂節目廣播的視聽廣播業營運者。

二、行政長官可應利害關係人的要求，以批示豁免以下關鍵基礎設施私人營運者履行網絡安全的義務：

- (一) 不從事獲發准照的業務者，但須已預先通知簽發准照的實體延遲開業或中止業務；
- (二) 其業務不使用資訊網絡或電腦系統者；
- (三) 顯示其業務的良好和常規表現不取決於資訊網絡及電腦系統長期操作者。

第二章 組織規定

第六條 組織框架

澳門特別行政區網絡安全體系由下列實體組成：

- (一) 網絡安全委員會（下稱“委員會”）；

- (6) Abate de animais em matadouros legais;
- (7) Fornecimento e distribuição de electricidade e gás natural;
- (8) Prestação de serviço público de transportes marítimos, terrestres e aéreos realizados com regularidade, segundo itinerários, frequência de viagens, horários e preços previamente definidos;
- (9) Exploração de portos, terminais marítimos, aeroportos e heliportos;
- (10) Radiodifusão televisiva e sonora;
- (11) Exploração de jogos de fortuna e azar em casino;
- (12) Exploração de redes públicas de telecomunicações fixas ou móveis e prestação de serviços de acesso à *internet*;
- 2) As sociedades comerciais de capitais exclusivamente públicos;
- 3) As pessoas colectivas privadas qualificadas de utilidade pública administrativa cuja actividade se cinja à área científica e tecnológica.

Artigo 5.º

Exclusões e isenção

1. O disposto na presente lei não se aplica:

- 1) Aos serviços, órgãos ou entidades públicos da RAEM que não utilizem redes ou sistemas informáticos, ou que apenas utilizem redes e sistemas cuja cibersegurança constitua responsabilidade de outras entidades públicas, nos termos das disposições dos diplomas orgânicos aplicáveis ou de despacho do Chefe do Executivo;
- 2) Aos operadores de radiodifusão televisiva e sonora cuja actividade se cinja à difusão de conteúdos de entretenimento.

2. O Chefe do Executivo, a pedido dos interessados e mediante despacho, pode isentar do cumprimento dos deveres de cibersegurança os operadores privados de infra-estruturas críticas que:

- 1) Não exerçam a actividade para a qual tenham sido licenciados, desde que o diferimento do início ou a suspensão da actividade tenha sido antecipadamente comunicado à entidade licenciadora;
- 2) Não usem sistemas e redes informáticas na sua actividade;
- 3) Demonstrem que o bom e regular desempenho da sua actividade não depende da permanente operacionalidade dos sistemas e redes informáticos.

CAPÍTULO II

Disposições institucionais

Artigo 6.º

Enquadramento institucional

Integram o sistema de cibersegurança da RAEM:

- 1) A Comissão para a Cibersegurança, doravante designada por CPC;

(二) 網絡安全事故預警及應急中心 (下稱“預警及應急中心”);

(三) 網絡安全監管實體 (下稱“監管實體”)。

第七條 網絡安全委員會

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

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。

2) O Centro de Alerta e Resposta a Incidentes de Cibersegurança, doravante designado por CARIC;

3) As Entidades de supervisão de cibersegurança, doravante designadas por entidades de supervisão.

Artigo 7.º

Comissão para a Cibersegurança

A CPC é o órgão presidido pelo Chefe do Executivo, à qual cabe:

1) Assegurar a actividade referida na alínea 1) do n.º 1 do artigo 3.º;

2) Supervisionar a actividade desenvolvida no âmbito da presente lei pelas demais entidades que integram o sistema de cibersegurança;

3) Propor ao Governo a celebração e revisão de acordos, protocolos ou contratos com entidades públicas ou privadas, da RAEM ou do exterior, que se mostrem adequados à elevação dos padrões de cibersegurança na RAEM.

Artigo 8.º

Centro de Alerta e Resposta a Incidentes de Cibersegurança

1. O CARIC é uma estrutura de natureza técnica especializada em matéria de alerta e resposta a incidentes de cibersegurança, coordenado pela Polícia Judiciária, ao qual cabe:

1) Centralizar a recepção de informações sobre incidentes de cibersegurança;

2) Definir as medidas de cibersegurança previstas na alínea 4) do n.º 1 do artigo 3.º e coordenar a resposta das diversas entidades intervenientes, de modo a evitar ou mitigar os efeitos dos incidentes de cibersegurança;

3) Assegurar e promover a cooperação institucional, incluindo com entidades congéneres do exterior;

4) Adoptar uma classificação dos incidentes de cibersegurança por níveis de gravidade e definir os procedimentos de alerta e resposta de acordo com esses níveis;

5) Monitorizar, em tempo real, o tráfego e as características dos dados informáticos transmitidos entre as redes dos operadores de infra-estruturas críticas e a *internet*, nos termos do disposto na alínea 5) do n.º 1 do artigo 3.º;

6) Emitir alertas sobre incidentes de cibersegurança;

7) Disponibilizar apoio técnico às entidades de supervisão, a pedido destas, no exercício das suas competências.

2. A monitorização referida na alínea 5) do número anterior é efectuada pela Polícia Judiciária e incide exclusivamente sobre a linguagem máquina, não podendo os dados informáticos ser recolhidos ou, por qualquer forma, descodificados.

3. O disposto nos números anteriores não prejudica o regime de competências e de autoridade da Polícia Judiciária.

第九條

網絡安全監管實體

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。

第三章

網絡安全義務

第十條

組織性義務

一、關鍵基礎設施私人營運者在組織方面的義務如下：

(一) 設立具能力執行網絡安全內部保護措施的網絡安全管理單位；

(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：

(一) 第2/2009號法律《維護國家安全法》規定的犯罪；

Artigo 9.º

Entidades de supervisão de cibersegurança

1. As entidades de supervisão são serviços e organismos da Administração Pública aos quais compete, no âmbito das suas atribuições:

1) Zelar pelo cumprimento dos deveres previstos na presente lei e nas normas técnicas, sem prejuízo das competências próprias do CARIC nas situações referidas na alínea 4) do n.º 1 do artigo 3.º;

2) Fiscalizar os planos e acções dos operadores de infra-estruturas críticas relativos à respectiva cibersegurança;

3) Exercer a competência sancionatória prevista na presente lei.

2. As competências referidas no número anterior são exercidas:

1) Pela Direcção dos Serviços de Administração e Função Pública, doravante designada pelos SAFP, relativamente aos operadores públicos de infra-estruturas críticas;

2) Pelas entidades públicas designadas por regulamento administrativo, relativamente aos operadores privados de infra-estruturas críticas.

CAPÍTULO III

Deveres de cibersegurança

Artigo 10.º

Deveres de carácter orgânico

1. Constituem deveres dos operadores privados de infra-estruturas críticas, no âmbito da respectiva organização:

1) Criar unidades de gestão de cibersegurança capazes de executar as respectivas medidas internas de protecção;

2) Dotar as unidades de gestão de cibersegurança com os meios humanos, financeiros, materiais e patrimoniais adequados;

3) Designar o principal responsável pela cibersegurança e respectivo substituto, de entre indivíduos com a idoneidade e experiência profissional adequadas e com residência habitual na RAEM;

4) Diligenciar para que o principal responsável pela cibersegurança e o seu substituto estejam permanentemente contactáveis pelo CARIC;

5) Estabelecer mecanismos de reclamação e denúncia relativas à cibersegurança.

2. Na apreciação da idoneidade, devem ser ponderados quaisquer factos que, pela sua gravidade, frequência ou outras circunstâncias atendíveis, indiquem que a pessoa suscita dúvidas sérias quanto à garantia da cibersegurança.

3. Sem prejuízo do disposto no número anterior, os operadores estão impedidos de designar como principal responsável pela cibersegurança e respectivo substituto, pelos períodos referidos no número seguinte, quem tiver sido condenado, por sentença transitada em julgado, por:

1) Crimes previstos na Lei n.º 2/2009 (Lei relativa à defesa da segurança do Estado);

(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。

第十一條

程序性、預防性及應變性義務

關鍵基礎設施私人營運者在程序、預防及應對網絡安全事故方面的義務如下：

(一) 制定網絡安全管理制度及相關的內部操作程序；

(二) 按照網絡安全管理制度及適用的技術規範，採取與網絡安全的保護、檢視、預警及應對有關的網絡安全事故內部措施；

(三) 在發生網絡安全事故時，通知預警及應急中心，並將有關事實告知相關監管實體，以及立即開展應對嚴重的網絡安全事故的行動；

(四) 檢視和記錄其資訊網絡的運作狀況。

第十二條

自行評估及報告義務

關鍵基礎設施私人營運者在自行評估及報告方面的義務如下：

(一) 就其資訊網絡及電腦系統的安全性及存在的風險，自行或由專業實體進行評估；

2) Crimes informáticos ou de falsificação de notação técnica, danificação ou subtração de notação técnica, devassa por meio de informática, aproveitamento indevido de segredo, violação de segredo de correspondência ou telecomunicações ou violação de segredo profissional;

3) Qualquer outro crime punível com pena de prisão superior a 5 anos.

4. Os períodos de impedimento são de:

1) 5 anos a contar do termo do período de suspensão de execução da pena ou da cessação do cumprimento da pena, ou das respectivas prorrogações, se a condenação foi em pena de prisão igual ou inferior a 5 anos;

2) 10 anos a contar da cessação do cumprimento da pena, ou das respectivas prorrogações, se a condenação foi em pena de prisão efectiva superior a 5 anos.

5. As sentenças proferidas por tribunal do exterior são relevantes para efeitos das alíneas 2) e 3) do n.º 3, contanto que, no caso da alínea 3), a conduta em causa também constitua crime nos termos da legislação da RAEM.

6. Os operadores devem solicitar parecer à Polícia Judiciária sobre a idoneidade e eventuais impedimentos relativos às pessoas que pretendam designar como principal responsável pela cibersegurança e o seu substituto.

Artigo 11.º

Deveres de carácter procedimental, preventivo e reactivo

Constituem deveres dos operadores privados de infra-estruturas críticas, em matéria de procedimentos e de prevenção e resposta a incidentes de cibersegurança:

1) Estabelecer um regime de gestão da cibersegurança e respectivos procedimentos operacionais internos;

2) Adoptar, conforme o regime de gestão da cibersegurança e as normas técnicas aplicáveis, medidas internas de protecção, monitorização, alerta e resposta a incidentes de cibersegurança;

3) Informar o CARIC da ocorrência de incidentes de cibersegurança e dar conhecimento do facto à respectiva entidade de supervisão, bem como iniciar, de imediato, as acções de resposta a incidentes graves;

4) Monitorizar e registar o estado de funcionamento da rede.

Artigo 12.º

Deveres de auto-avaliação e relato

Constituem deveres dos operadores privados de infra-estruturas críticas, em matéria de auto-avaliação e relato:

1) Proceder, por si próprios ou através de entidades especializadas, à avaliação da segurança e dos riscos existentes nas suas redes e sistemas;

(二) 每年向有關監管實體提交網絡安全報告，其中尤須指出倘有已記錄的網絡安全事故、上項所指評估的結果及已採取的改善措施。

第十三條 合作義務

關鍵基礎設施私人營運者及其行政管理機關成員、管理人員或受託人，在與預警及應急中心和監管實體的合作方面有如下義務：

(一) 在查核第十一條所指義務的履行情況屬必要的範圍內，允許該等部門的代表進入其設施及資訊網絡，並向該等人員提供所要求的資料；

(二) 提供確保網絡安全的妥善管理所需的支援與合作。

第十四條 關鍵基礎設施公共營運者的義務

一、關鍵基礎設施公共營運者的義務如下：

(一) 在領導及主管人員中，指定一名網絡安全負責人；

(二) 採取措施以取得合適的人力、財政、物力及財產資源，使有關的網絡安全管理制度能良好運作；

(三) 對內及在由其負責網絡安全的公共部門、機關或實體範圍內，履行和促使履行第十一條至第十三條規定的義務；

(四) 檢視與私人實體訂立的提供網絡安全服務合同的執行情況；

(五) 私人實體不履行有關合同時，在不影響可予歸責的情況下，執行與該私人實體以合同訂定的網絡安全服務。

二、非組成預警及應急中心的關鍵基礎設施公共營運者，每年須向行政公職局提交一份關於其資訊網絡及電腦系統的安全及存在風險的評估報告。

三、第一款(四)項所指的提供網絡安全服務合同的訂立，須經行政長官預先許可。

2) Submeter anualmente à respectiva entidade de supervisão um relatório de cibersegurança, mencionando, designadamente, os eventuais incidentes registados, os resultados da avaliação referida na alínea anterior e as medidas de melhoria tomadas.

Artigo 13.º Dever de colaboração

Constituem deveres dos operadores privados de infra-estruturas críticas, bem como dos respectivos administradores, gerentes ou mandatários, em matéria de colaboração com o CARIC e as entidades de supervisão:

1) Permitir a entrada nas suas instalações dos representantes daqueles serviços, facultar-lhes o acesso às suas redes e prestar-lhes as informações que estes solicitem, na medida necessária à verificação do cumprimento dos deveres referidos no artigo 11.º;

2) Prestar o apoio e a colaboração necessários para garantir a boa gestão da cibersegurança.

Artigo 14.º Deveres dos operadores públicos de infra-estruturas críticas

1. Constituem deveres dos operadores públicos de infra-estruturas críticas:

1) Designar um responsável pela cibersegurança, de entre o pessoal de direcção e chefia;

2) Diligenciar pela obtenção dos meios humanos, financeiros, materiais e patrimoniais adequados para o bom funcionamento do respectivo regime de gestão de cibersegurança;

3) Cumprir e fazer cumprir os deveres previstos nos artigos 11.º a 13.º, internamente e no âmbito dos serviços, órgãos ou entidades públicas cuja cibersegurança constitua sua responsabilidade;

4) Monitorizar a execução do contrato de prestação de serviços de cibersegurança celebrado com entidades privadas;

5) Assumir a execução dos serviços de cibersegurança contratados com entidades privadas, em caso de incumprimento por estas do respectivo contrato e sem prejuízo da responsabilidade que lhes vier a ser imputada.

2. Os operadores públicos de infra-estruturas críticas que não integrem o CARIC apresentam, anualmente, aos SAFP um relatório de avaliação da segurança e dos riscos existentes nas suas redes e sistemas.

3. A celebração do contrato de prestação de serviços de cibersegurança previsto na alínea 4) do n.º 1 depende de autorização prévia do Chefe do Executivo.

第四章 處罰制度

第十五條 行政違法行為

一、在不影響尚有的其他責任的情況下，因作為或不作為而違反第十條至第十三條規定的義務，科澳門幣十五萬元至五百萬元的罰款，但下款的規定除外。

二、因作為或不作為而違反第十條第一款（四）項、第十二條（二）項、第十三條（二）項以及技術規範規定的義務，科澳門幣五萬元至十五萬元的罰款。

第十六條 行政違法行為的責任

就上條所指的行政違法行為對關鍵基礎設施營運者的歸責：

（一）適用於由第三人確保網絡安全的情況；

（二）不取決於以作為或不作為方式實行政違法行為的行為人的身份識別；

（三）不取決於身份可被識別的行為人與關鍵基礎設施營運者或與合同訂定的網絡安全服務提供者的關係。

第十七條 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優惠的權利。

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

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）不合規範為可予補正且對網絡安全不構成嚴重危險者；

CAPÍTULO IV

Regime sancionatório

Artigo 15.º

Infracções administrativas

1. Sem prejuízo de outra responsabilidade que ao caso couber, a violação, por acção ou omissão, dos deveres previstos nos artigos 10.º a 13.º, é sancionada com multa de 150 000 a 5 000 000 patacas, salvo o disposto no número seguinte.

2. A violação, por acção ou omissão, dos deveres previstos na alínea 4) do n.º 1 do artigo 10.º, na alínea 2) do artigo 12.º, na alínea 2) do artigo 13.º e nas normas técnicas é sancionada com multa de 50 000 a 150 000 patacas.

Artigo 16.º

Responsabilidade por infracções administrativas

A imputação de responsabilidade pelas infracções administrativas previstas no artigo anterior aos operadores de infra-estruturas críticas:

1) Aplica-se às situações em que a cibersegurança é assegurada por terceiros;

2) Não depende da identificação do agente de cuja acção ou omissão resultou a prática da infracção administrativa;

3) Não depende da relação entre o agente, sendo este identificável, e o operador ou o prestador de serviços de cibersegurança por este contratado.

Artigo 17.º

Sanções acessórias

1. Pelas infracções ao disposto nas alíneas 1) a 3) do n.º 1 do artigo 10.º, na alínea 1) do artigo 11.º, na alínea 1) do artigo 12.º e na alínea 1) do artigo 13.º, podem ser aplicadas, isolada ou cumulativamente, as seguintes sanções acessórias:

1) Privação do direito de participar em ajustes directos, consultas restritas ou concursos públicos que tenham por objecto a aquisição de bens ou serviços por serviços, órgãos e entidades públicos;

2) Privação do direito a subsídios ou benefícios concedidos por serviços, órgãos e entidades públicos.

2. As sanções acessórias referidas no número anterior têm a duração máxima de dois anos, contada a partir da data em que a correspondente decisão se tenha tornado inimpugnável.

Artigo 18.º

Advertência

1. Caso se verifique uma irregularidade no cumprimento dos deveres de cibersegurança, a entidade de supervisão pode fixar um prazo para a sua sanção, quando:

1) A irregularidade seja sanável e dela não tenha resultado um perigo significativo para a cibersegurança;

(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。

第十九條

累犯

一、為適用本法律的規定，自行政處罰決定轉為不可申訴起一年內，且距上一次的行政違法行為實施日不足五年，再次實施第十五條規定的行政違法行為者，視為累犯。

二、如屬累犯的情況，罰款的最低限額提高四分之一，最高限額則維持不變。

第二十條

行政違法行為的合併

一、如行為同時構成違反本章規定的義務及其他法例規定的行政違法行為，則根據罰款上限較高的法例對違法者作出處罰。

二、上款的規定不影響單獨或一併適用：

(一) 就各種行政違法行為訂定的附加處罰；

(二) 訂定廢止或中止准照或其等同憑證，又或其他非處罰性措施的規範。

第二十一條

處罰權限

一、第九條所指的實體具權限對受其監管的關鍵基礎設施私人營運者就本法律規定的行政違法行為提起程序及組成相關卷宗。

二、監管實體的最高負責人員具權限決定提起處罰程序、指定預審員及作出處罰。

第二十二條

履行未履行的義務

如因不履行義務而構成違法行為，科處處罰及繳付罰款並不免除違法者履行仍屬可履行的義務。

2) Não haja reincidência.

2. Sendo a irregularidade sanada no prazo fixado, a entidade de supervisão pode decidir-se por uma simples advertência ao infractor.

3. A falta de sanção da irregularidade no prazo fixado determina o prosseguimento do procedimento para aplicação das sanções que couberem à infracção.

Artigo 19.º

Reincidência

1. Para efeitos da presente lei, considera-se reincidência a prática de infracção administrativa prevista no artigo 15.º no prazo de um ano após a decisão sancionatória administrativa se ter tornado inimpugnável e desde que entre a prática da infracção administrativa e a da anterior não tenham decorrido mais de cinco anos.

2. Em caso de reincidência, o valor mínimo da multa é elevado de um quarto e o valor máximo permanece inalterado.

Artigo 20.º

Cumulação de infracções administrativas

1. Quando a conduta constitua simultaneamente infracção administrativa aos deveres de cibersegurança e aos previstos noutra legislação, o infractor é punido de acordo com a legislação que estabeleça multa de limite máximo mais elevado.

2. O disposto no número anterior não prejudica a aplicação, isolada ou cumulativamente:

1) Das sanções acessórias previstas para as diversas infracções administrativas;

2) De normas que prevejam a revogação ou suspensão de licenças ou títulos equivalentes ou outras medidas de natureza não sancionatória.

Artigo 21.º

Competência sancionatória

1. Compete às entidades referidas no artigo 9.º, relativamente aos operadores privados de infra-estruturas críticas sujeitos à sua supervisão, instaurar os procedimentos pelas infracções administrativas previstas na presente lei e instruir os respectivos processos.

2. Compete ao responsável máximo da entidade de supervisão determinar a instauração do procedimento sancionatório, designar instrutor e aplicar as sanções.

Artigo 22.º

Cumprimento do dever omitido

Sempre que a infracção resulte da omissão de um dever, a aplicação da sanção e o pagamento da multa não dispensam o infractor do seu cumprimento, se este ainda for possível.

第二十三條

關鍵基礎設施公共營運者的工作人員的責任

一、關鍵基礎設施公共營運者的工作人員須對違反第十一條至第十四條規定的義務負紀律責任，且不影響倘有的其他責任。

二、對因違反程序性、預防性及應變性義務而構成的違紀行為，可科處強迫退休或撤職，又或停職處分。

第五章

過渡及最後規定

第二十四條

用戶身份模塊卡

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、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。

第二十五條

客戶身份資料

一、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，應查核及登記客戶的身份資料。

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、相應適用上條第四款的規定。

Artigo 23.º

Responsabilidade dos trabalhadores dos operadores públicos de infra-estruturas críticas

1. Sem prejuízo de outra responsabilidade que ao caso couber, os trabalhadores dos operadores públicos de infra-estruturas críticas são disciplinarmente responsáveis pelas infracções aos deveres previstos nos artigos 11.º a 14.º

2. As infracções disciplinares por violação dos deveres de carácter procedimental, preventivo e reactivo são puníveis com as penas de aposentação compulsiva ou demissão ou com pena de suspensão.

CAPÍTULO V

Disposições transitórias e finais

Artigo 24.º

Módulos de identificação de assinante

1. No prazo de 120 dias a contar da data de entrada em vigor da presente lei, os operadores de redes devem diligenciar no sentido de registar a identidade dos utilizadores de todos os módulos de identificação de assinante vendidos antes daquela data, sem prévia identificação, na modalidade de pré-pagos.

2. Os operadores de rede devem suspender o serviço relativamente aos módulos cujos utilizadores não forneçam os seus dados de identificação até ao termo do prazo referido no número anterior, sem prejuízo da posterior reactivação dos mesmos a partir da data em que os dados de identificação sejam fornecidos.

3. O incumprimento dos deveres previstos nos números anteriores constitui infracção administrativa, sancionada com multa de 50 000 a 150 000 patacas.

4. Compete à Direcção dos Serviços de Correios e Telecomunicações instaurar os procedimentos sancionatórios pela infracção referida no número anterior, designar instrutor e aplicar as sanções.

Artigo 25.º

Identificação de clientes

1. Os operadores de redes devem verificar e registar a identidade dos clientes no momento da celebração de contratos ou da confirmação da prestação de serviços para acesso à *internet*, registo de nomes de domínio ou serviços públicos de telecomunicações fixas ou móveis.

2. O incumprimento do dever previsto no número anterior constitui infracção administrativa, sancionada com multa de 50 000 a 150 000 patacas.

3. É correspondentemente aplicável o disposto no n.º 4 do artigo anterior.

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。

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。

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。”

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

本法律自公佈後滿一百八十日起生效。

二零一九年六月六日通過。

立法會主席 賀一誠

二零一九年六月十七日簽署。

命令公佈。

行政長官 崔世安

Artigo 26.º

Aditamento à Lei n.º 11/2009

É aditado à Lei n.º 11/2009 o capítulo III-A, denominado «Infracção administrativa», constituído pelos artigos 16.º-A e 16.º-B, com a seguinte redacção:

«Artigo 16.º-A

Conservação e fornecimento de registos de tradução de endereços de rede

1. Os prestadores de serviços de *internet* estão obrigados a conservar, por um ano, os registos de tradução de endereços de rede privada em endereços de rede pública.

2. O incumprimento do dever previsto no número anterior constitui infracção administrativa, sancionada com multa de 50 000 a 150 000 patacas.

3. A autoridade judiciária competente pode, quando necessário, ordenar o fornecimento dos registos referidos no n.º 1, observando-se, para o efeito, o disposto nos n.ºs 1 a 4 do artigo 15.º

Artigo 16.º-B

Competência

Compete à Direcção dos Serviços de Correios e Telecomunicações instaurar os procedimentos sancionatórios pela infracção administrativa prevista no n.º 2 do artigo anterior, designar instrutor e aplicar as sanções.»

Artigo 27.º

Regulamentação complementar

O Chefe do Executivo aprova os regulamentos administrativos complementares ou os despachos regulamentares externos que se mostrem necessários à execução da presente lei, nomeadamente em matéria de:

1) Composição, competências e modo de funcionamento da CPC e do CARIC;

2) Designação das entidades de supervisão e dos operadores privados de infra-estruturas críticas abrangidos pelo respectivo poder de supervisão.

Artigo 28.º

Entrada em vigor

A presente lei entra em vigor 180 dias após a sua publicação.

Aprovada em 6 de Junho de 2019.

O Presidente da Assembleia Legislativa, *Ho Iat Seng*.

Assinada em 17 de Junho de 2019.

Publique-se.

O Chefe do Executivo, *Chui Sai On*.