（供学术交流使用）

越南社会主义共和国
《网络安全法》

编译： 西北政法大学涉外刑事法治与国别检察司法研究中心

本件法律由西北政法大学涉外刑事法治与国别检察司法研究中心组织编译，如需详细法律查明，请与中心联系。

单位：西北政法大学涉外刑事法治与国别检察司法研究中心

联系电话：029-88182613

目录

第一章：总则

第 1 条 调整范围与适用对象

1. 本法规定网络安全及网络安全保障制度，明确相关机关、组织和个人在网络安全领域的权利、义务与责任。

2. 本法适用于：

a) 越南国家机关、组织和个人；

b) 在越南境内的外国机关、组织和个人，以及已取得身份证明文件并在越南居住的无国籍越南裔人士；

c) 外国机构、组织、个人事先参与，或者与在越南境内开展的网络安全、网络产品经营、网络安全服务相关的活动；

第 2 条 术语解释

在本法中，下列术语定义如下：

1. 网络安全，是指维护网络空间的稳定运行与安全状态，保护信息系统安全，防范网络空间内的信息、数据及活动对国家安全、国家主权、社会公共安全以及机关、组织、个人的合法权益造成危害。

2. 网络信息安全，是指保障网络空间中信息的完整性、保密性和可用性，防范信息被非法访问、使用、泄露、篡改、破坏以及其他非法侵害，防止上述行为危害国家安全、社会秩序和公共安全。

3. 数据安全，是指保障数据质量以及网络空间上的数据处理、使用活动的安全，以经济社会发展和国家数字化转型，防范数据被非法访问、使用、泄露、篡改、破坏或遭受其他威胁、损害国家安全、社会秩序与公共安全的行为。

4. 网络安全保护，是指采取必要措施，预防、发现、制止和处置网络安全违法侵害行为，维护网络空间安全秩序的活动。

5. 网络空间，是指由信息技术基础设施互联网络系统形成的环境，包括通信网络、互联网、计算机网络、信息系统、信息处理与控制系统、数据库；是人类开展不受时空限制的社会活动的场所。

6. 国家网络空间，是指越南社会主义共和国享有主权、管辖权和控制权的网络空间。

7. 信息系统，是指由硬件、软件和数据组成的系统，用于在网络空间中信息的创建、提供、传输、收集、处理、存储、以及交换。

8. 信息系统管理主体，是指对信息系统享有直接管理权限的机关、组织或个人。

9. 恶意软件，是指能够导致信息系统的部分或整体异常运行，或者对信息系统中存储的信息进行非法复制、篡改、删除的软件。

10. 恶意硬件，是指被故意设计或附加到标准硬件组件之外的物理部件，用于非法收集信息、数据，或干扰、导致计算机系统、信息系统停滞、瘫痪、受到破坏。

11. 系统日志是记录系统时间、用户、活动、系统状态的集合，用于系统管理、监控和安全防护。

12. 网络犯罪，是个人或组织在网络空间上通过使用信息技术或电子手段实施的，并在刑法典中规定的对社会具有危险的行为。

13. 网络攻击，是指在网络空间中利用信息技术或者电子手段，非法获取信息、造成系统混乱、干扰正常运行、瘫痪业务活动，破坏或控制信息系统、通信网络、互联网、计算机网络、信息处理与控制系统、数据库及其他电子设备的行为。

14网络恐怖主义，是指在网络空间中利用信息技术或者电子手段，传播虚假信息或者有害内容，造成公众恐慌或者破坏政治稳定的行为。

15. 网络间谍行为，是指利用信息技术或者电子手段，秘密侵入网络空间，窃取、收集、复制属于国家秘密范围的信息，以及非法获取机关、组织、个人重要数据，以危害国家安全、社会秩序和公共安全的行为。

16. 网络安全威胁，是指网络空间中出现的可能危害国家安全、严重破坏社会秩序、社会公共安全以及机关、组织或个人合法权益的潜在危险状态。

17. 危害网络安全的行为，是指在网络空间中实施的，危害国家安全、社会秩序和公共安全以及机关、组织或个人合法权益的行为。

18. 网络安全风险，是指在网络空间中，因存在攻击、入侵、煽动、信息泄露、信息丢失或者其他非法行为，可能严重威胁国家安全、社会秩序、社会公共安全以及机关、组织或个人合法权益的状态及其动态变化。

19. 数字账户，是用于在网络空间中对各类应用、服务进行认证、身份验证和授权使用的信息集合。

20. 民用密码，是指采用密码技术和密码产品，对不涉及国家秘密的信息进行加密保护或者安全认证，保障机关、组织或个人信息安全的密码。

21. 网络安全产品，是指具有保护网络安全、网络信息安全、数据安全、信息、数据、信息系统、信息技术基础设施功能的硬件和软件。

22. 网络安全服务，是指为网络安全、信息安全、数据安全、信息、数据、信息系统及信息技术基础设施提供安全保障的服务。

23. 关键信息系统，是指使用核心密码技术，用于处理涉及国家秘密的信息，支撑由相关组织直接管理运营的专业工作活动的信息系统。

第 3 条 国家网络安全政策

1. 建设健康清朗的网络空间，防范危害国家安全、国家利益和公共安全以及机关、组织和个人合法权益的行为。

2. 优先保障国防、国家安全、国家重要机关、经济社会发展、科学技术和对外交往领域的网络安全。

3. 优先配置资源建设和发展国家网络安全专业力量，保障高素质网络安全人才供给；提升国家网络安全防护能力以及参与网络安全保护的组织和个人的能力；优先支持网络安全科学研究和技术现代化发展；建立特殊机制和优惠政策，吸引、培养、调动和激励网络安全领域人才。

4. 加强协同配合，鼓励依法依规与网络安全相关单位开展合作；鼓励和引导各机关、组织或个人参与网络安全保护，防范和处理网络安全风险；支持网络安全技术、产品、服务和应用的研发与推广；优先使用越南国产网络安全产品和服务。

5. 深化国际网络安全合作，增强国家网络安全防护能力；预防和打击网络犯罪及跨国网络安全威胁；引进吸收国际先进技术，提升国家网络安全自主能力。

第 4 条 网络安全保护原则

1. 遵守宪法与法律，维护网络空间的国家安全、主权和利益。

2. 坚持越南共产党领导，在国家的统一管理之下，凝聚政治体系与全体民众的综合力量，发挥安全专职力量的骨干作用。

3. 坚持网络安全与经济社会发展相协调，保障人权与公民权利，保护个人数据，为机关、组织或个人在网络空间开展合法活动创造条件。

4. 采取措施守护国家网络空间，预防、发现、制止并处置网络空间内侵害国家安全、公共秩序、社会安全及合法权益的行为，及时、从严查处网络安全违法行为。

5. 实行网络安全常态化管理，持续强化国家网络空间基础设施防护，主动采取措施来保护事关国家安全的重要信息系统。

第 5 条 网络安全防护措施

1. 网络安全防护措施具体包括：

a) 开展网络安全评估；

b) 开展网络安全条件评估；

c) 实施网络安全检查；

d) 开展安全监测；

đ) 应对和处理网络安全事故。

e) 为保卫网络安全而斗争；

g) 运用密码保护网络信息；

h) 采取技术措施保障信息安全、数据安全与信息系统安全，拦截违法信息；

i) 制止、责令暂停或终止提供网络信息；依法中止、暂时中止设立、提供和使用各类通信服务、互联网服务，以及无线电信号发射、接收的相关活动；

k) 责令删除、访问并删除网络空间内侵害国家安全、公共秩序、社会安全和机关、组织、个人合法权益的违法信息、失实信息或虚假信息。

l) 收集与网络空间中危害国家安全、社会秩序及公共安全，侵害机关、组织、个人合法权益的行为相关的电子数据。

m) 封锁、限制信息系统活动；依法中止、暂时中止或要求停止信息系统活动，依法收回域名；

n) 依照《刑事诉讼法》的规定，立案、侦查、起诉、审判；

o) 依照《国家安全法》及《行政违法处理法》的规定采取的其他措施。

2. 政府制定颁布网络安全防护措施的适用范围、程序、手续和权限的施行细则，本条第1款n项及o项）规定的措施除外。

第 6 条 网络安全国际合作

1. 网络安全国际合作应当在尊重独立、主权和领土完整，互不干涉内政，平等互利，以及遵守越南宪法、法律及越南社会主义共和国作为缔约方的国际条约的基础上进行。

2. 网络安全国际合作的内容包括：

a) 共享信息、数据及关于影响网络安全的各类风险、威胁、网络攻击的早期预警；

b) 建立网络安全保护领域的法律框架、政策及合作与协调机制；谈判、签署并参与执行越南社会主义共和国作为缔约方的国际条约及国际协议；

c) 培训、咨询、经验交流以及提升网络安全领域的专业技术能力；

d) 预防和打击网络犯罪、利用高科技实施的犯罪；协调开展调查、处理违法行为、网络犯罪及利用高科技实施的犯罪；

đ) 研究、开发、转让技术、产品、方案以及提供服务于网络安全保护工作；

e) 组织国际会议、研讨会，并开展网络安全领域的国际合作项目、合作计划；

g) 其他网络安全国际合作活动。

3. 网络安全国际合作的责任规定如下：

a) 公安部对政府负责，牵头、协调实施网络安全领域的国际合作；

b) 国防部对政府负责，在管理范围内开展网络安全国际合作；

c) 外交部有责任与公安部、国防部在网络安全国际合作活动中进行协调。

d) 涉及多个部委、部门责任的网络安全国际合作事项，由政府总理决定；

đ) 各部委、各部门及地方开展的网络安全国际合作活动，必须在实施前取得公安部的书面意见；

第 7 条 关于网络安全的严禁行为

1. 在网络空间发布、传播含有下列内容的信息：

a) 宣传反对越南社会主义共和国包括：宣传歪曲、诽谤人民政权；心理战，煽动侵略战争，分裂、煽动民族、宗教及各国人民之间的仇恨；侮辱民族、国旗、国徽、国歌、伟人、领袖、名人、民族英雄；

b)歪曲历史、否认革命成果、破坏全民族大团结的基石、侮辱宗教、性别歧视、种族歧视；

c)编造、诬陷、传播虚假信息，侵犯他人的人格、名誉和信誉，或者对机关、组织或个人的合法权益造成损害的；

d）传播造成人民恐慌、损害经济社会活动，妨碍国家机关或执行公务人员的正常活动，侵害其他机关、组织、个人合法权益的失实消息；捏造、歪曲关于产品、商品、货币、债券、国库券、公债、支票及其他有价证券的失实信息；在金融、银行、电子商务、多层次经营、证券领域的捏造、虚假信息。

2.禁止在网络空间实施下列行为：

a)组织、活动、勾结、教唆、收买、欺骗、拉拢、培训、训练反对越南社会主义共和国的人员；

b)煽动、号召、鼓动、教唆、威胁、制造分裂，实施武装活动或使用暴力以对抗人民政权；号召、鼓动、教唆、威胁、拉拢聚众闹事，对抗执行公务的人员，阻碍国家机关、组织的活动，破坏公共安全和社会秩序稳定。

c)窃取、买卖、扣押、故意泄露属于国家秘密、工作秘密、商业秘密的信息；非法占有、买卖、扣押、故意泄露属于个人秘密、家庭秘密及私人生活秘密的信息，并影响其他机关、组织或个人的名誉、信誉、人格、合法权益；在网络空间非法窃听、录音、录像；泄露关于民用密码产品、合法使用民用密码产品客户的信息；使用、经营来源不明的民用密码产品；

d)卖淫活动、社会丑恶现象、买卖人口、人体器官；传播淫秽、堕落文化产品；煽动、鼓吹暴力、堕落、偏离正道的生活方式，破坏民族淳正风气和美好习俗、社会道德、公众健康；

đ)欺诈侵占财产；组织赌博、网络赌博；在互联网上窃取国际电信资费；宣传、广告、买卖法律法规禁止清单中的商品、服务；在网络空间侵犯版权和知识产权

e)伪造机关、组织、个人的电子信息门户网站；非法制作、流通、窃取、买卖、收集、交换他人的信用卡信息、银行账户、加密资产、数字资产；非法发行、提供、使用支付工具；伪造机关、组织的证件；

g)非法利用人工智能或新技术伪造他人的视频、图像、声音；创建、发布、传播本条第1款规定的信息；

h)非法收集、使用、传播、交换、转让、经营他人的个人信息、数据；

i)指导、教唆、拉拢、煽动他人实施犯罪或实施违法行为；

k)利用信息技术、电子手段在网络空间实施危害国家安全、社会秩序及公共安全的其他违法行为。

3.实施网络攻击、网络恐怖主义、网络间谍、网络犯罪、利用高科技实施的犯罪；造成信息系统部事故，攻击、入侵、非法控制、破坏、中断、瘫痪或摧毁信息系统。

4.生产、提供使用工具、设备、软件，或实施阻碍、干扰行为，或传播垃圾邮件、垃圾短信、垃圾电话、有害计算机程序，危害电信网络、互联网、计算机网络、信息系统、信息处理与控制系统、电子设备的运行。

5.非法侵入他人的电信网络、计算机网络、信息系统、信息处理与控制系统、数据库及电子设备。

6.对抗或阻碍网络安全保护力量的活动；非法攻击、破坏网络安全保护措施，使其失去效力。

7.利用或滥用网络安全保护活动，侵犯国家主权、利益、国家安全、社会秩序与安全，以及机关、组织或个人的合法权益，或从中牟利。

8.违反本法规定的其他行为。

第二章 信息系统的网络安全保护

第 8 条 信息系统安全保护级别分类

1.信息系统遭受安全事故或违反网络安全法的行为，对国家安全、社会秩序与公共安全及机关、组织、个人合法权益、公共利益所造成的危害程度，分为以下5个级别：

a)第1级，可能对机关、组织的合法权益及个人的合法权益造成损害；

b)第2级，可能对机关、组织的或个人的合法权益造成严重损害，或对公共利益造成损害；

c)第3级，可能对机关、组织或个人的合法权益造成特别严重损害；对公共利益造成严重损害；对社会秩序与安全造成损害或严重损害，或对国家安全造成损害；

d)第4级，可能对公共利益、社会秩序与公共安全造成特别严重损害，或对国家安全造成严重损害；

đ)第5级，可能对国家安全造成特别严重损害。

2.政府详细规定信息系统安全级别认定的具体标准；规定系统级别认定的权限、程序、手续，以及针对不同级别信息系统采取网络安全保障措施、承担相应责任及履行相关义务。

第9条 国家安全重要信息系统

1.国家安全重要信息系统，是指对政治、国防、安全、外交、经济、社会等领域具有战略性和特别重要作用的系统。在发生安全事故或出现违反网络安全法行为时，可能对国家安全、社会秩序与公共安全造成严重损害的，并属于政府总理决定颁布的名录范围之内。

2.国家安全重要信息系统属于下列领域：

a)军事、安全、外交、重要信息系统；

b)存储、处理属于国家秘密信息的重要信息系统；

c)服务于存管和保管具有特别重要价值的实物、档案材料的重要信息系统；

d)服务于保管对人类、环境具有极度危险的材料、物质的重要信息系统。

đ)服务于保管、制造、管理其他与国家安全相关特别重要的基础设施的重要信息系统；

e)服务于中央机关、组织活动的重要信息系统；

g)服务于地方机关、组织活动的重要信息系统；

h)政府总理规定的其他重要信息系统。

3.国家安全重要信息系统在投入运行使用前，必须经过网络安全评估，并获得符合网络安全条件的认证；在使用过程中须定期开展网络安全检查和网络安全监控，并及时应对、处置网络安全事故。

4.公安部牵头、协同各相关部委、部门、机关、组织或个人制定国家安全重要信息系统名录，并提请政府总理审议决定。

5.政府详细规定国家安全重要信息系统的认定标准。

第十条 信息系统的网络安全保护职责与措施

1.信息系统的网络安全保护职责包括：

a)确定信息系统的网络安全级别，并确定国家安全重要信息系统；

b)评估和管理信息系统的网络安全风险；

c)督促、监督、检查信息系统的网络安全保护工作；

d)组织实施信息系统的网络安全保护措施；

đ)按照规定执行报告制度；

e)组织开展网络安全宣传教育，提升网络安全意识。

2.信息系统的网络安全保护措施包括：

a)颁布信息系统在设计、建设、管理、运行、使用、升级、销毁等环节中保障网络安全的规定；

b)对信息系统的档案及设计进行网络安全评估；

c)对信息系统进行网络安全条件评估；

d)根据网络安全技术标准、技术规范采取管理措施，研究建设国家防火墙系统以预防、应对网络安全风险，处置网络安全事故事件；

đ)组织实施信息存储、备份等措施，以保护网络信息安全以及信息系统各组成部分的安全；

e)检查、监督各项规定的遵守情况，并评估所采取的管理措施与技术措施的有效性；

g)实施网络安全监控；

h)对信息系统进行网络安全事件的应对与处置修复。

3.第1级、第2级信息系统的管理方，应当全面执行本条第1款规定的各项任务，并根据实际需求与能力，选择适用本条第2款规定的各项措施。

4.属于第3级、第4级且不属于国家安全重要信息系统名录的信息系统管理方，应当全面执行本条第1款规定的各项任务，执行本条第2款a、d、đ、e、g、h项规定的各项措施，并根据实际需求与能力，选择适用本条第2款b和c规定的措施。

5.属于国家安全重要信息系统名录的信息系统管理方，应当全面执行本条第1款和第2款规定的各项任务与措施。

6.政府对本条第1款和第2款作出详细规定。

第十一条 国家安全重要信息系统的网络安全保护责任

1.国家安全重要信息系统的管理方负有下列责任：

a)执行本法第10条第5款的规定；

b)在设立、扩展或升级国家安全重要信息系统时，必须在投入运行、开发、使用前进行网络安全检查；每年定期自行检查网络安全，评估国家安全重要信

息系统的网络安全条件，并于每年10月之前将书面检查结果报送有管辖权的专职网络安全保护力量；

c)牵头、协同有管辖权的专职网络安全保护力量，在日常工作中实施网络安全监控；建立预警机制，接收网络安全威胁预警；制定紧急应对、处置修复方案；

d)制定网络安全事故应对、处置修复方案；在网络安全事故发生时应立即启动并执行应对与处置修复方案，并及时向有管辖权的专职网络安全保护力量报告；

đ)配合有管辖权的专职网络安全保护力量实施突击网络安全检查。

2.除法令规定的军事信息系统和政府机要局委的核心机密信息系统外，公安部对国家安全重要信息系统负有下列责任：

a)对国家安全重要信息系统进行网络安全评估；

b)评估并认证国家安全重要信息系统是否满足网络安全条件；

c)对国家安全重要信息系统进行突击网络安全检查。

d)实施网络安全监控；向信息系统管理方发出警报并协同其应对、处置修复针对国家安全重要信息系统的网络安全威胁风险、网络安全事故；

đ)牵头、协调针对国家安全重要信息系统发生的网络安全事件的应对、处置修复活动；在发现网络攻击、网络安全事件时通知信息系统管理方；

e)在使用政府机要委提供的密码解决方案、密码产品以保护国家秘密的国家安全重要信息系统中，牵头、协同政府机要委实施各项保护措施。

3.国防部牵头对国防部管理的军事信息系统进行网络安全评估、网络安全条件评估、突击网络安全检查、网络安全监控，并协调应对、处置修复网络安全事故。

4.政府机要委牵头组织实施核心机密密码解决方案，以保护国家安全重要信息系统中属于国家秘密的信息；对政府机要委主管的关键信息系统进行网络

安全评估、网络安全条件评估、突击网络安全检查、网络安全监控，并协调应对、处置修复网络安全事故。

第12条 对未列入国家安全重要信息系统名录的机关、组织的信息系统进行网络安全检查

1.对未列入国家安全重要信息系统名录的机关、组织的信息系统，在以下情形中进行网络安全检查：

a)当出现本法第2条第12、13、14和15款所规定的行为时；

b)当信息系统管理方提出建议时。

2.网络安全检查的对象包括：

a)信息系统中使用的硬件、软件、数字设备；

b)信息系统中存储、处理、传输的信息；

c)保护国家秘密以及通过技术渠道预防、打击泄露、丢失国家秘密的行为。

3.信息系统管理方发现其管辖范围内的信息系统存在违反网络安全法的行为时，有义务向公安部所属的专职网络安全保护力量报告。

4.公安部所属的专职网络安全保护力量在本条第1款所规定的情形下，对机关、组织的信息系统实施网络安全检查。网络安全检查结果依法予以保密。

5.政府规定本条所指网络安全检查的程序和操作规范。

第三章 危害网络安全行为的预防与处理

第 13 条 利用信息技术、电子手段侵犯的侵害国家安全、社会秩序与公共安全的信息与行为

1.具有宣传反对越南社会主义共和国、煽动制造暴乱、破坏安全、扰乱公共秩序内容的信息，包括：

a)传播含有歪曲、污蔑、诋毁人民政权内容的信息与资料；

b)开展心理战，煽动侵略战争、制造分裂，煽动民族、宗教对立及各国人民间的仇恨；

c)侮辱民族、国旗、国徽、国歌、伟人、领袖、名人、名誉、肖像及民族尊严。

d）鼓吹、煽动、教唆、胁迫、制造分裂，组织武装活动或使用暴力对抗人民政权；

đ)鼓吹、煽动、教唆、胁迫、纠集人员寻衅滋事、妨害机关与社会组织正常公务，扰乱安全与社会秩序；

e）歪曲、失实表述有关越南国界、国家主权的内容；刊登或传播歪曲、失实、内容残缺的越南地图，或以其他方式侵害越南国家主权。

2.包含破坏越南社会主义共和国大团结政策、经济社会政策的信息，包括：

a）在人民各阶层之间、人民与人民政权之间、人民武装力量之间或各政治社会组织之间制造矛盾和分裂；

b）煽动仇恨、制造歧视与分裂、实行民族分离，侵犯越南各民族共同体的平等权利；

c）煽动、制造、挑拨信教群众与非信教群众之间、不同宗教信徒之间，以及宗教信徒与人民政权、人民武装力量或各政治社会组织之间的对立；

d）破坏或阻碍国际团结政策的实施；

đ) 直接或间接传播损害国家在政治、经济、社会方面的合法权利和利益及国际声誉的内容；

e）鼓吹、煽动破坏各项经济社会政策实施，阻碍政策执行；

g）鼓吹、煽动破坏越南社会主义共和国国家物质与技术基础设施。

3. 侵害组织、个人合法权利与利益的信息，包括：

a）散布歪曲、诽谤、失实信息，损害主体声誉和正常经营活动；

b）鼓动、煽动、教唆抵制组织、企业的产品、服务、商品、商标、品牌，造成组织、企业物质损失与声誉损毁；

c）利用信息技术，冒充身份、伪造信息、图像，仿制产品、商品商标、品牌，侵害组织、企业声誉；

d）侮辱他人荣誉、声誉、人格；

đ) 歪曲事实损害他人名誉、声誉、人格

e）诽谤或者公然散布虚假信息，损害他人合法民事权利和利益；

g） 诽谤他人犯罪者，并在相关机构前举报； g）诬告陷害他人，致使被害人在有管辖权的机关遭受控告；

h）冒用身份、伪造个人信息、肖像、声音，侵害个人信誉、名誉、人格

4. 在网络空间利用信息技术、电子手段实施的危害国家安全、社会秩序与公共安全的行为包括：

a）在网络平台发布、散播本条第1、2、3款所列违法内容的信息

b）实施本法第15条第1款规定的违法行为；

c）侵占财产；组织赌博、通过互联网进行赌博；在互联网平台窃取国际电信资费；侵犯网络空间内知识产权；

d）伪造机关、组织、个人电子信息页面；伪造、流通、窃取、倒卖、收受、转借他人账户信息与银行账户；非法发行、提供、使用各类支付工具；伪造机关、组织印章、文件或其他证件；

đ)宣传、推广、非法买卖枪支、爆炸物、辅助工具、烟花爆竹；毒品、毒品前体、麻醉品或精神药品；珍稀野生动植物及其制品、法律法规明令禁售的其他商品与服务；卖淫；传播淫秽物品；儿童性虐待；性骚扰；

e）建立、提供服务或支持非法网络空间的交易、业务运营、买卖、在线营销的交易平台、电子信息网页、应用程序，包括：电子商务平台、电子信息网站、销售应用程序、提供电子商务服务、基于各种商品指数的交易平台；以多层次方式经营的数字资产交易平台

g）使用虚假身份、文件或档案，或非法利用他人信息设立企业，设立和注册银行账户、证券账户、保险账户、税务账户及其他数字账户;非法收集、存储、交换、交易、捐赠或披露银行账户、银行卡、电信账户、证券账户、保险账户、税务账户及其他类型数字账户的数据和信息；

h）广告宣传、售卖假冒产品、来源不明的进口货物、被国家采取应急管控措施的境内流通商品、已过使用有效期的产品；

i)引导他人实施违法犯罪行为。

k）在网络空间利用信息技术、电子手段实施的其他违反国家安全、社会治安与公共安全相关法律的行为。

第 14 条 预防、处置利用信息技术、电子手段在网络空间实施侵害国家安全、社会秩序、公共安全的信息与行为

1.信息系统管理方、国内外在电信网络、互联网上提供服务的以及提供网络空间增值服务的企业，有责任在其管理范围内的信息系统中，或在网络安全专业力量提出要求时，实施管理和技术措施，以预防、发现、拦截、删除本法第13条第1、2、3款规定内容的信息。

2.网络安全专业力量与法定职权部门，有权依照本法第5条第1款规定采取处置措施，清理网络中本法第13条第1、2、3款规定的违规信息，并防范、制止、

打击行为人借助信息技术、电子手段在网络空间实施危害国家安全、社会秩序、公共安全的违法活动。

3.境内外电信、互联网、增值电信服务经营者与信息系统管理方，应当配合网络安全专业力量，处置平台内本法第13条第1、2、3款列明的违规信息，并防范和打击利用信息技术、电子手段侵害国家安全、社会秩序和网络空间安全的行为

4. 组织、个人制作、发布、传播本法第13条第1、2、3款规定内容的网络信息，在接到网络安全专业力量通知后，必须删除相关信息，并依法承担法律责任。

5.政府应详细说明本条款。

第15条 预防、打击网络间谍行为；保护网络环境中的国家秘密、工作秘密、商业秘密、个人隐私与网络空间的隐私生活

1.网络间谍行为;网络窃密、窃取国家秘密、工作秘密、商业秘密、个人及家庭隐私的违法行为包括：

a）窃取、收购、收受、故意泄露国家秘密、工作秘密、商业秘密相关信息；窃取、买卖、留存、故意泄露个人隐私、家庭私密信息，损害机关、组织、个人的名誉、声誉、人格与合法财产权益；

b）故意删除、破坏、灭失、篡改已在网络空间存储、传输的国家秘密、工作秘密、商业秘密、个人隐私与家庭私生活信息；

c）故意篡改、废除、致使为保护国家秘密、工作秘密、商业秘密、个人隐私、家庭私生活信息而部署落地的技术防护措施失效；

d）违反法律规定，将国家秘密、工作秘密、商业秘密、个人隐私、家庭私生活信息上传至网络空间；

đ)非法窃听、录音、录像通话内容；

e）其他故意侵害国家秘密、工作秘密、商业秘密、个人隐私及家庭私生活秘密的行为

2.信息系统管理方负有下列责任

a）开展网络安全检查，查杀恶意软件、恶意硬件，修补安全短板与保密漏洞；排查、拦截、处置非法入侵及其他网络安全风险活动；

b）实施管理和技术措施，以预防、排查、拦截网络间谍行为，侵害国家秘密、工作秘密、商业秘密、个人隐私、家庭私生活秘密的违法行为，必要时对相关信息予以删除；

c）配合网络安全专业力量的工作要求，落实防范网络窃密、保护本系统内国家秘密、工作秘密、商业秘密、个人隐私、家庭私生活信息的相关工作。

3.制作、存储国家秘密信息资料的机关、组织，应当依照《国家机密保护法》规定，对在计算机、其他设备中编制、存储，或通过网络传输的国家秘密承担保密义务。

4.除本条第5、6款规定情形外，越南公安部承担下列职责：

a）对国家关键信息基础设施开展网络安全检查，排查清除恶意软件、恶意硬件，修补安全隐患与保密漏洞，排查、拦截、处置非法入侵活动；

b）在投入用于国家安全重要信息系统之前，对设备、产品、通信服务、数字设备、电子设备进行网络安全检查；

c）对国家关键信息基础设施实施网络安全监督，排查、处置非法窃取国家秘密信息的行为；

d）查处在网络空间违规发布、存储、传输涉密信息资料的行为；

đ)参与依法研究和生产存储和传播含国家机密信息及文件的产品，以及根据其分配的功能和任务在网络空间加密信息的产品

e）对国家机关网络保密工作、关键信息基础设施管理方的网络安全防护工作开展监督、检查；

g）面向本法第30条第1款规定的网络安全专业力量，组织开展提高对网络空间国家秘密保护、预防和防御网络攻击、网络安全防护的意识和知识的培训。

5.国防部就涉密军事信息系统，履行本条第4款所列全部法定职责

6.政府办公厅针对本级机要系统，落实本条第4款各项法定职责；并有责任组织实施法律规定中关于使用密码保护在网络空间上存储、传输的属于国家秘密的信息的相关规定。

第16条 预防、打击在网络空间上对儿童的侵害

1.未成年人依法享有在网络空间获取信息、参与社会活动、休闲娱乐、保护个人隐私及其他法定权利

2.未成年人使用增值网络服务的，由法定监护人依照法律规定完成账号注册；监护人负有监督、管理未成年人在各类服务平台访问、发布、分享网络信息内容的监护义务。

3.信息系统管理方、在电信网络、互联网上提供服务的以及提供网络空间增值服务的企业，承担以下责任：

a）管控自有系统与平台的信息内容，避免出现危害未成年人身心健康、侵害未成年人合法权益的内容；

b）屏蔽、删除含有侵害未成年人权益、危害未成年人身心健康等违法信息；

c）建设、部署技术防护系统，从技术层面拦截网络空间侵害未成年人的不良内容；

d）与各机关、组织、企业协调配合，封堵危害未成年人的不良信息源头；

đ）及时通报、配合公安部的专职网络安全保护力量进行处理。

4.机关、组织或个人参与网络活动的，应当配合主管机关落实未成年人权益保障工作，预防、打击在网络空间上对儿童的侵害。

5.机关、组织、父母、监护人、教师、儿童看护人及其他相关个人，负有依照儿童保护相关法律及本法规定，保障儿童权利、保护儿童参与网络空间活动安全的责任

6.网络安全专业力量与职能机关，依法采取防控措施，排查、拦截、从严处置利用网络危害未成年人身心健康、侵犯未成年人合法权益的违法行为。

第17条 预防、排查、阻止和处理恶意软件

1.机关、组织、个人有责任主动预防、排查、阻止恶意软件，并按照有权国家机关的指导和要求执行。

2.国家安全重要信息系统的主管单位部署技术系统，以预防、排查、阻止和及时处理恶意软件。

3.提供电子商务、信息传输、信息存储服务的组织和企业，在自身系统上发送、接收、存储信息的过程中，必须配备恶意软件过滤系统，并依照法律规定向有权国家机关报告。

4.互联网接入服务提供方，应当管理，预防、排查、拦截恶意软件的传播，并依照主管机关指令进行处理。

5.公安部牵头，会同国防部及相关部委统筹开展危害国家安全类恶意软件的预防、排查、拦截与处理工作。

第18条 预防与应对网络攻击

1.网络攻击行为及与网络攻击相关的行为包括：

a）传播能够对电信网络、互联网、计算机网络、信息系统、、信息处理和控制系统、数据库、电子设备造成危害的程序；

b）造成阻碍、扰乱、瘫痪、中断、停滞网络空间活动，非法阻止网络空间数据的传输；

c）非法侵入、破坏、窃取存储与传输于电信网络、互联网、计算机网络、信息系统、信息处理和控制系统、数据库、电子设备内的数据；

d）入侵、制造或利用系统的弱点、安全漏洞和服务，以窃取信息、牟取非法利益；

đ）生产、买卖、交换、赠与用于实施违法活动，可破坏电信网络、互联网、计算机网络、信息系统、信息处理和控制系统、数据库、电子设备的工具、设备、软件；

e）其他妨害电信网络、互联网、计算机网络、信息系统、信息处理和控制系统、数据库、电子设备正常运行的行为。

2.信息系统管理方应当在其管理范围内采取技术措施，预防、拦截本条第1款a、b、c、d、e项所列不法行为

3.当网络攻击侵犯或威胁国家主权、利益和安全，严重损害社会秩序和公共安全时，网络安全专业力量应牵头并协调信息系统主管方和组织、个人采取措施，以确定网络攻击的来源并收集证据;请求提供电信网络、互联网、网络增值服务的企业拦截和过滤信息，以防止和消除网络攻击，并提供充足且及时相关的信息和资料。

4.预防和打击网络攻击的职责划分如下：

a）公安部应牵头并协调，相关部委、行业、地方实施本条第1款规定侵犯或威胁国家主权、利益、安全，对全国范围内的社会秩序和公共安全造成严重损害行为的预防、排查和处理工作，但本款b项和c项规定的情况除外；

b）国防部应牵头并协调有关部委及行业管理方，对军事信息系统进行本条第1款规定行为的预防、排查和处理工作；；

c）政府办公厅应牵头并协调相关部委及行业，对政府办公厅所属的政府信息系统，实施本条第1款规定行为的预防、排查和处理工作。

第19条 预防、打击网络恐怖主义

1.有管辖权的国家机关有责任根据本法及《反恐怖主义法》的规定采取措施来处理网络恐怖活动。

2.信息系统管理方应定期排查、检查所辖系统，以排除网络恐怖主义的风险。

3.当发现网络恐怖主义的迹象或行为时，机关、组织、个人必须及时向网络安全保护力量报告。接收举报信息的机关有责任完整接收关于网络恐怖主义的举报信息，并及时通报给网络安全专业力量

4.公安部应牵头并协同各部委开展预防、打击网络恐怖主义的工作采取消除网络恐怖主义源头、处理网络恐怖主义的措施，最大限度降低信息系统受损后果，但本条第5款和第6款规定的情况除外。

5.国防部应牵头并协调相关部委和行业预防和打击网络恐怖主义，开展开展预防、打击网络恐怖主义的工作采取消除网络恐怖主义源头，处理网络恐怖行为，最大限度降低军事信息系统受损后果。

6.政府办公厅牵头、协调相关部委和部门，开展预防、打击网络恐怖主义的工作，采取消除网络恐怖主义源头、处理网络恐怖主义的措施，最大限度降低政府信息系统受损的后果。

第20条 预防和处理网络安全危险情况

1.网络安全危险情况包括：

a）在网络空间上出现煽动信息，存在发生暴乱、破坏安全、恐怖主义的风险；

b）攻击具有国家安全重要性的信息系统；

c）大规模、高强度攻击多套信息系统；

d）旨在破坏国家安全重要工程、重要目标的网络攻击

đ）严重侵犯国家主权、利益和安全；对机关、组织、个人的合法权益，以及社会秩序和安全造成特别严重损害的网络攻击

2.有关网络安全危险情况预防的责任规定如下：

a）网络安全专业力量与涉及国家安全重要信息系统的主管部门合作，实施技术和业务解决方案，以预防、发现和处理网络安全危险情况

b）电信、互联网、信息技术企业，以及提供电信网络、互联网、网络空间增值服务的企业以及相关的机关、组织、个人，有责任配合公安部所属的网络安全专业力量，开展预防、排查、处理网络安全危险情况的工作。

3.网络安全危险情况的处理措施包括：

a）立即启动网络安全预防和紧急应对方案，阻止、消除或减轻由网络安全危险情况造成的损害；

b）通知到相关的机关、组织、个人；

c）收集相关信息；对网络安全危险情形进行连续跟踪、监督；

d）分析、评估信息，预测由网络安全危险情形造成的风险、影响范围和损害程度；

đ)在特定区域停止提供网络信息，或切断国际网络连接；

e）部署力量、采取手段以阻止、消除网络安全危险情形；

g）根据《国家安全法》规定的其他措施。

4.网络安全相关危险情况的处理规定如下：

a）机关、组织或个人发现网络安全危险情况后，应当立即向网络安全专业力量报告，并即刻落实本条第3款a、b项所规定的措施；

b）总理审议、决定或授权公安部长审议、决定、处理全国范围内或各地方、或针对特定目标的网络安全危险情况。

总理审议、决定或授权国防部长审议、决定、处理归政府办公厅管理的军用信息系统和政府信息系统的网络安全危险情况；

c）网络安全专业力量应承担主要责任，并与相关机构、组织和个人协调，执行本条第3款规定的措施处理网络安全危险情况；

d）涉案相关机关、组织、个人，负有配合网络安全专业力量开展险情阻止、事件处置的法定义务。

第21条 网络安全防护行动

1.定义：网络安全防护行动，是由网络安全专业力量在网络空间组织实施的专项工作，目的是维护国家安全、社会秩序与公共安全。

2.网络安全防护工作内容包括：

a）开展网络信息监督，预防、处理利用网络实施危害国家安全、扰乱社会秩序的组织与个人；

b）运用技术措施拦截、封堵违法信息；

c）预防、抵御攻，保障国家关键信息基础设施平稳安全运行；

d）使网络空间使用活动瘫痪或受限，以危害国家安全或对社会秩序、安全造成特别严重的损害

đ)主动攻击，使境外网络攻击目标失效，以此维护国家安全、社会秩序与公共安全。

3.公安部牵头并协调相关部委和行业开展全域网络安全防护工作；国防部牵头、协同相关部委或行业，负责涉密军政信息系统的网络安全防护工作。

第22条 阻止网络空间中的信息冲突

1.网络信息冲突，是指境内外两个及以上主体，借助技术、信息技术手段在网络信息系统内实施信息攻击，进而危害国家安全、社会秩序与公共安全的行为。

2.阻止网络空间上的信息冲突，是指实施技术措施，以监督、排查、预防、确定源头、过滤、删除、应对、引导舆论、修复、处罚以及其他消除网络空间信息冲突的措施。

3.在权责范围内，有关组织、个人负有如下法定义务：

a）在自有信息系统上阻止网络空间中的信息冲突；通过国内外组织、个人的信息系统，合作确定源头、应对并修复网络攻击所造成的后果；

b）阻止境内外组织和个人蓄意制造网络信息冲突的活动；

c）排除国内外组织、个人组织实施的、在网络空间发布、传播对国防、国家安全、社会秩序和公共安全造成严重影响的信息的行。

4.政府应详细规定本条款

第四章 网络安全防护工作

第23条 中央与地方的国家机关、政治组织及政治社会团体开展网络安全防护工作

1.网络安全防护工作内容包括：

a）制定、完善内部局域网、与互联网连接的计算机网络的使用规定、章程；制定针对信息系统的网络安全保障方案；网络安全事故的应对、处置修复方案；

b）落实信息安全防护方案与法定安全措施，对本单位管辖范围内的系统中存储、发布、传输的信息与和文件的网络安全；

c）面向干部、公职人员、事业单位工作人员、企业劳动者开展网络安全知识培训，提升网络安全保护力量的防护能力；

d）保护网络安全包括在网络空间提供公共服务、与机关、组织或个人的信息提供、交换和收集信息，内部及与其他机构共享信息，或在政府规定的其他活动中共享信息；

d）投资、建设符合条件的基础设施，以确保针对信息系统的网络安全防护活动的开展；

e）对信息系统进行网络安全检查；防止和打击网络安全违法行为；应对和处理修复网络安全事故。

2. 机关、组织主要负责人，在自身权责范围内组织落实网络安全防护工作

第24条 国家网络空间基础设施、与国际网络连接的网络安全保护

1.对国家网络空间基础设施、国际网络连接的网络安全保护，必须确保将网络安全保护要求与经济社会发展要求紧密结合；鼓励在越南领土上设立国际连接；鼓励组织、个人参与投资建设国家网络空间基础设施。

2.负责管理、使用国家网络基础设施与国际互联关口的机关、组织、个人负有下列义务：

a）保护其管理下的网络安全；接受有权国家机关在网络安全保护方面的管理、监督、检查，并落实其提出的要求；

b）在有管辖权的国家机关提出要求时，为其执行网络安全防护工作创造条件，并采取必要的技术、业务措施。

第25条 保障网络信息安全

1.任何机关、组织、个人的电子信息页面、电子信息门户网站或社交网络专门页面不得提供、发布、传播含有本法第13条第1款、第2款、第3款及第15条第1款规定内容的信息，以及其他含有危害国家安全内容的信息。

2.国内或国外企业在越南境内电信网络、互联网及网络空间的增值服务上提供服务时，有下列责任：

a)核验用户注册数字账户时的信息；对用户的信息、账户予以保密；向公安部专职网络安全保护力量提供用户信息，自收到以书面、电子邮件、电话或者其他已确认形式的要求之时起，最迟不得超过24小时，以服务于核实、调查、处理危害网络安全违法行为。紧急情况下，涉及危害国家安全、危及人身安全的，提供信息最迟不得超过3小时。

b)自公安部专职网络安全保护力量提出要求之时起，最迟在24小时内阻止分享信息、删除信息、下架具有违反本法规定内容的服务或应用程序，并保存系统日志，用于在法律规定的期限内为核实、调查、处理违反网络安全法律的行为提供支持；在威胁国家安全的紧急情况下，要求最迟在6小时内阻止分享、删除信息。

c)根据公安部专职网络安全保护力量提出要求时，对在网络空间发布含有本法第13条第1款、第2款、第3款及第14条第1款、第2款规定内容信息的组织、个人，不予提供或者停止提供电信网络、互联网及网络空间增值服务。

d)在用户终止使用服务后，将根据法律规定的期限，存储服务用户的个人信息以及用户产生的数据，包括：账户名称、服务使用时间、服务费用支付信息、访问IP地址及其他相关数据。

3.在越南境内电信网络、互联网及网络空间提供增值服务的境内外企业，有收集、开发、分析、处理个人信息数据、用户关系数据、用户在越南使用服务所产生数据的活动的，应当依法采取数据保护措施，并在越南境内存储该数据，存储期限由政府规定。本条规定的境外企业，应当在越南设立分支机构或者代表处。

4.政府规定本条第2款和第3款的详细内容。

第26条：保障数据安全

1.保障数据安全，是指采取技术、组织和法律措施的整体，旨在保护数据，防范、打击危害数据安全的行为。

2.保障数据安全的内容包括：

a）制定数据安全保障政策，建立数据安全保障的流程；

b）依照网络安全法律规定，采取措施、标准和强制性技术规范；

c）使用弱密码、民用密码，以保障数据安全；

d）建立对直接参与数据处理的人员严格的管控机制；

đ）定期检查、评估风险，及时发现、阻止和处理威胁数据安全的潜在风险；

e）检查、评估数据跨境传输情况；确保涉及国家安全的重点信息系统、数据库、数据中心、数据存储系统中数据安全的条件；

g）法律规定的其他内容。

3.政府规定本条第2款的详细内容；规定保障数据安全的责任。

第五章 网络安全标准、技术规范、产品、服务

第27条：网络安全标准、技术规范

1.网络安全标准、技术规范适用于信息系统、硬件、软件、网络安全管理运营系统、网络安全产品、服务、信息技术及网络连接设备。

2.网络安全合规认证、合规申明、网络安全标准符合性认证、符合性申明，依照关于标准和强制性技术规范的法律规定执行。

3.服务于涉及国家安全重要信息系统以及网络安全国家管理活动的网络安全标准符合性评估、合规评估，，应当在公安部指定的标准合规认证、合规评估机构进行。

4.公安部负有下列职责：

a）制定、维护网络安全国家标准；

b）管理网络安全产品、服务质量，民用密码产品、服务除外；

c）对管理网络安全合规认证机构的活动进行登记、指定和管理，本条第6款规定的情形除外；

5.公安部部长颁布网络安全国家技术规范。

6.国防部登记、指定并管理军事领域网络安全合规认证机构的活动。

政府机要委协助国防部部长管理民用密码产品和服务质量；登记、指定并管理民用密码产品、服务网络安全合规认证机构的活动。

第28条 网络安全产品和服务

1.网络安全产品包括：

a）民用密码产品；

b）网络安全检查、评估产品；

c）网络安全监测产品

d）防范攻击和入侵的产品；

d）其他网络安全产品。

2.网络安全服务包括：

a）网络安全检查、评估服务；

b）不使用民用密码的信息安全服务；

c）民用密码服务；

d）网络安全咨询服务；

đ）网络安全监测服务；

e)网络安全事件应急响应服务；

g）数据恢复服务；

h）防范、抵御网络攻攻击服务；

I）其他网络安全服务

3.政府规定本条详细内容。

第29条 网络安全产品与服务经营

1.经营网络安全产品、服务的企业，应当取得网络安全产品、服务经营许可证。

2.经营网络安全产品、服务的企业，负有下列责任：

a）严格按照网络安全产品、服务经营许可证开展业务；遵守网络安全法律规定及其他相关法律规定；

b）在网络安全产品、服务在市场流通前，确保其质量符合公布的适用标准及相应技术规范，并遵守有关产品和商品质量、标准与技术规范的法律规定；

c）依照法律规定，建立、保存并保密客户信息，管理产品技术方案、技术文件及服务提供活动的档案文件。

d）发现组织、个人违法使用网络安全产品与服务相关法规，或者违反与企业就使用该产品、服务达成的承诺的，应拒绝提供网络安全产品和服务；；

đ）配合、创造条件并落实专职网络安全保护力量的要求，以实施网络安全保护措施。

3.政府规定网络安全产品、服务经营许可证的颁发、暂扣、吊销；规定网络安全产品进出口；规定网络安全产品、服务经营活动。

第六章 网络安全保护力量与保障条件

第30条 网络安全保护力量

1.网络安全保护力量包括：

a）专职网络安全保护力量，下设于公安部、国防部；

b）网络安全保护力量，设于部、行业、省级人民委员会，及直接管理涉及国家安全的重点信息系统的机关或组织；

c）被动员参与网络安全保护的组织、个人。

2.政府规定本条第1款的详细内容；规定各网络安全保护力量之间的协调事项。

第31条 网络安全保护的人力资源保障

1.国家培养、发展网络安全保护人力资源，保障数量、质量，满足国家网络安全保护能力需求。

2.专职网络安全保护力量按照岗位、职务标准优先配置人力资源，适用政府规定特殊政策，在招聘、考察录用、使用、培训、培养、待遇

和人才引进方面实行特殊机制。

3.涉及国家安全的重要信息系统主管单位负有下列责任：

a）按照系统保护等级，部署专门部门或者专门人员；

b）保障执行网络安全任务的人员符合专业、业务标准。

c）对涉及系统运行、监控、应急响应和事件处理的人员队伍，经常进行进修、技能更新。

第32条 网络安全保护力量的选拔、培养与发展

1. 越南公民具备良好的品德、健康、文化程度、网络安全和信息技术知识，有意愿的，可被选拔加入网络安全保护力量。

2. 优先培养、发展高质量网络安全保护力量；发现网络安全、信息技术青年人才，为其指明学习方向，并选拔、招录及任用，用于网络安全领域。

3. 优先发展达到国际标准的网络安全培训基地，鼓励在网络安全领域建立公私部门、国内外之间的联系和合作。

第33条 网络安全知识、业务的教育与培养

1. 网络安全知识教育与培养内容被纳入学校的国防与安全教育课程，并按照《国防安全教育法》的规定，纳入国防与安全知识培养计划。

2. 公安部牵头，有关部门、行业协调配合，组织对网络安全保护力量和参与网络安全保护的公务员、事业编制人员、劳动者进行网络安全业务培养。

国防部、政府机要委组织对其管理范围内的对象进行网络安全业务培养。

第34条 网络安全的专业知识和技能训练

1. 本法第30条第1款a）项、b）项规定的网络安全保护力量，须满足网络安全专业知识、技能要求。

2. 国家机关、组织、国有企业中直接管理、运行第3级、第4级、第5级信息系统的人员，须接受网络安全知识、技能专业训练并取得认证，已接受过网络安全专门培训的个人除外。

3. 公安部牵头，配合有关部委、行业组织网络安全专业知识、技能培训练，本条第4款规定的情形除外。

4. 国防部、政府机要委对其管理范围内的对象组织网络安全专业知识、技能训练。

5.政府规定网络安全专业知识、技能标准；以及网络安全专业知识、技能训练的计划、内容和认证事项。

第35条 网络安全知识的普及

1.国家制定在全国范围普及网络安全知识的政策，鼓励国家机关与私营组织、个人合作，实施网络安全教育和提高网络安全意识的计划；优先向儿童、老年人、认知困难人员普及、指导，以提高其在网络空间维护自身合法权益的能力。

2.各部委、行业、机关、组织有责任为部委、行业、机关、组织中的干部、公务员、事业编制人员、劳动者制定并开展普及网络安全知识活动。

3.省级人民委员会有责任为地方机关、组织、个人制定并开展普及网络安全知识、提高网络安全意识活动。

第36条 网络安全的研究与发展

1.网络安全研究、发展内容包括：

a）建设网络安全保护软件系统、设备；

b）对达到标准的网络安全保护软件、设备进行评审的办法，用于限制其存在的安全缺陷、漏洞、恶意软件；

c）检查所提供硬件、软件功能运行正确性的方法；

d）保护国家秘密、工作秘密、商业秘密、个人隐私、家庭秘密和私生活的方法；以及在网络空间传输信息时的保密能力；

d）确定在网络空间传播的信息来源；

e)解决网络安全威胁风险；

g）建设网络靶场、网络安全测试环境。

h）提高网络安全意识和技能的技术创新。

i）网络安全预测。

k）网络安全实践研究、理论发展。

2.有关机关、组织和个人有权研究、发展网络安全。

第37条 提高网络安全自主能力

1.国家鼓励、创造条件，使机关、组织、个人提高网络安全自主能力，提高数字设备、网络服务、网络应用的生产、检查、评估、认证能力。

2.政府采取下列措施，提高机关、组织、个人的网络安全自主能力：

a）指导制定网络安全产业发展政策、战略、规划；针对硬件、软件产品制定技术标准和规范，以便在产品形成之初主动消除网络安全风险。

b）推动网络安全产业技术、产品、服务的转移、研究、掌握和发展。

c）推动网络安全有关的新技术、先进技术的应用；

d）组织培训、发展、优化利用高素质网络安全人才；

đ）优化营商环境，改善竞争条件，支持企业研究、生产用于保护网络安全的产品、服务、应用。

3.网络安全产业基础设施发展的投资和资源引进活动，包括：

a）投资建设网络安全产业基础设施的活动，属于投资特别优惠行业、领域，依照投资、税收、土地及其他相关法律规定享受优惠、扶持。

b）国家优先安排财政资金，用于投资建设网络安全产业基础设施，包括：网络安全产品、服务研究、设计、生产、测试基地；网络安全国家重点实验室；网络安全产品、服务检测、测试、评估基地；大数据中心；网络安全产业集聚区；网络安全产业综合体。

c）本款b）项规定的国家投资的网络安全产业基础设施，属于基础设施资产，依照公有资产管理，根据法律规定管理、开发、运行。

d）组织、企业可以便利进口和转让用于网络安全产品、服务培训及发展活动的技术、设备、机器、工具。

đ）各机关、组织、国有企业优先使用国内生产的网络安全产品、服务。

4.公安部提供建议、协助政府建设、发展网络安全产业基础设施，以提高网络安全自主能力。

第38条 网络安全保护经费

1.由国家资金保障的国家机关、组织、国有企业、政治组织、政治-社会组织及公立事业单位，必须在其年度数字化转型、信息技术应用任务支出资金中安排网络安全保卫经费；并至少安排实施数字化转型、信息技术应用投资计划、方案、项目总经费的15%用于网络安全保护。

2.不属于本条第1款规定的机关、组织、单位，自行保障其网络安全保护经费。

第七章 机关、组织、个人在网络安全方面的责任

第39条 网络安全国家管理职责

1.政府统一进行网络安全国家管理。

2.公安部是协助政府实施网络安全国家管理的牵头机关；对政府负责，执行下列网络安全国家管理内容，本条第3款和第4款规定的内容除外：

a）颁布或者提请有权国家机关颁布网络安全法律规范性文件；

b）制定、提出网络安全保护战略、方针、政策、计划和方案；研究、制定、发展、使用安全密码，以保护公安部管理范围内的数据安全。

c）协调配合有关机关，组织宣传、批驳本法第13条第1款规定的含有反对越南社会主义共和国内容的信息

d）要求提供电信网络、互联网及网络空间增值服务的企业，以及信息系统的主管部门，在其企业、机关、组织直接管理的服务和信息系统上，删除含有违反网络安全法内容的信息

đ）防范、打击利用网络空间危害主权、利益、国家安全、社会秩序与安全活动并防范、打击网络犯罪。

e）保障网络空间信息安全、数据安全；建立IP地址标识管理机制；核验数字账户注册信息；预警、分享网络安全信息、网络安全威胁风险。

g）参谋、提请政府、政府总理审议、决定分工、配合实施网络安全保护措施，防范、处理危害网络安全行为，在国家管理内容涉及多部、行业管理范围的情形。

h）紧急情况下，动员专家、科学家、专门干部并征用系统、工具、设备，以保卫国家安全，保障网络空间社会秩序、社会安全。

i）组织演练防范、抵御网络攻击；组织涉及国家安全的重点信息系统网络安全应急响应、恢复演练。

k）检查、监察、解决投诉、举报并处理违反网络安全法律的行为。

3.国防部对政府负责，实施其管理范围内的网络安全国家管理，如下：

a）在其管理范围内，发布或者提请有权国家机关发布网络安全法律规范性文件；

b）在其管理范围内，制定、提出网络安全保护战略、方针、政策、计划和方案；

c）在其管理范围内，防范、打击利用网络空间危害国家安全的活动。

d）配合公安部，组织网络攻击防范、抵御演练，组织涉及国家安全的重要信息系统网络安全的应急响应及恢复演练，部署落实网络安全保护工作。

đ）在其管理范围内，检查、监察、解决投诉、举报并处理违反网络安全法律的行为。

4.政府机要委员会协助国防部部长，依照法律规定承担其管理范围内的民用密码和网络安全国家管理工作。

5.各部、部级同级机关、政府所属机关，在法定职权、职责范围内，开展网络安全保护工作；并配合公安机关实施网络安全国家管理工作。

6.省级人民委员会统筹辖区内网络安全保护工作；并配合公安部实施网络安全国家管理工作。

第40条 信息系统主管单位在网络安全保护中的责任

1.信息系统主管单位负有下列责任：

a）依照本法规定，落实信息系统安全防护工作。

b）将网络安全监控系统、恶意软件防护系统接入公安部国家网络安全中心或者省、市网络安全中心，以协助网络安全监控工作。

c）向公安部或者国防部的专门机关报告网络安全事件。

2.使用国家预算的信息系统主管单位，除本条第1款规定的责任外，还应承担以下责任：

a）在建立、扩建或升级信息系统时，须编制网络安全保障方案，并由主管国家机关进行网络安全审查。

b）指定负责网络安全的个人或部门。

第41条 网络空间服务提供企业的责任

1.遵守网络安全法律的规定。

2.警示使用其提供的网络空间服务时可能的网络安全风险情形，并指导用户采取防范措施；建立网络安全应急响应方案，以主动处理网络安全弱点、风险和事故。

3.发生网络安全事件时，立即启动网络安全紧急应急响应方案，同时依照本法规定立即向网络安全专业力量报告。

4.依照本法、数据法律、个人数据保护法律及其他相关法律规定，采取技术措施、技术解决方案，以保障数据处理、个人数据处理的网络安全。

5.有责任识别使用互联网服务的组织、个人IP地址；向网络安全专业力量提供IP地址识别信息，以实施网络安全保护措施。

6.依照公安部网络安全专业力量指导，建立链接系统、接入技术传输线路、传输数据，并满足实施网络安全保护解决方案和措施所需的其他条件，以在有要求时协助调查、核实和处理网络安全违法行为。

7.在越南境内提供电信网络、互联网及网络空间提供增值服务的企业，有责任执行本条、本法第25条第2款和第3款的规定。

第42条 使用网络空间的机关、组织、个人的责任

1.遵守网络安全法律规定。

2.有责任保密自己注册、开设、管理、使用的数字账户信息。如果使用数字账户实施违法行为，根据违法行为的性质、程度，数字账户所有人、使用人

将受到纪律处分、行政处罚或者追究其刑事责任；给国家利益、组织和个人合法权益造成损害的，应当依法赔偿损失。

3.及时向有权机关、网络安全专业力量提供与网络安全保护、网络安全威胁或危害网络的安全行为有关的信息。

4.执行有权机关在网络安全保护中的要求和指导；为机关、组织和有责任的人员实施网络安全保护措施提供帮助、创造条件。

第八章 实施条款

第43条 对若干法律条款的修正和补充

1.替换《档案法》（2024年第33号/QH15）中的若干表述，废止若干款项，如下：

a）将第35条第1款第b项的“信息安全”、第36条第2款第b项的“网络信息安全”及第60条第3款的“信息安全与保密”替换为“网络安全”；

b）废止第58条第4款。

2. 替换、废止《消费者权利保护法》（2023年第19号/QH15）若干表述，如下：

a）将第16条第1款第d项的“信息保密”替换为“信息安全”；将第15条第1款、第19条标题、第19条第1款和第3款的“信息安全与保密”替换为“网络安全”。

b）废止第19条第3款的“网络信息安全”一词。

3.替换《费用和手续费法》（2015年第97号/QH13）经2017年第09号/QH14、2018年第23号/QH14、2020年第72号/QH14、2023年第16号/QH15、2023年第20号/QH15、2023年第24号/QH15、2024年第33号/QH15、2024年第35号/QH15、2024年第47号/QH15、2024年第60号/QH15、2025年第74号/QH15、2025年第89号/QH15、2025年第94号/QH15、2025年第95号/QH15和2025年第118号/QH15法律修改、补充若干条款后的若干表述，如下：

a）在附录01《费用和手续费目录》A部分VI目第10子目和B部分III目第16子目，将“信息安全”替换为“网络安全”；

b）在附录01《费用和手续费目录》A部分VI目第11子目，将“网络信息安全”替换为“网络安全”。

4.替换、废止《数字技术工业法》（2025年第71号/QH15）若干表述，如下：

a）将第25条第1款第a）项的“信息安全”替换为“网络安全”；

b）废止第10条的“网络信息安全”一词。

5.替换、废止《数据法》（2024年第60号/QH15）若干表述，如下：

a）将第25条第4款的“信息安全与保密”替换为“数据安全”

b）将第33条第2款的“信息安全与保密”替换为“网络安全”；

c）废止第25条第4款的“信息安全”一词

d）废止第39条第4款的“网络信息安全”一词。

đ）废止第43条第4款的“网络信息安全法”一词。

6.替换、废止《文化遗产法》（2024年第45号/QH15）经2025年第84号/QH15法律修改、补充若干条款后的若干表述，如下：

a）将第59条第4款的“网络信息安全”替换为“网络安全”；

b）废止第86条第2款第c项的“网络信息安全”一词

7.替换、废止《电信法》（2023年第24号/QH15）经2024年第47号/QH15法律修改、补充若干条款后的若干表述，如下：

a）将第5条第8款的“网络信息安全”替换为“信息安全”

b）废止第5条标题和第5条第1款、第38条第2款第c项的“网络信息安全”一词。

c）废止第21条第2款和第29条第2款第b）项的“网络信息安全”一词。

8.替换、废止《电子交易法》第20/2023/QH15号经第60/2024/QH15号法律修改、补充若干条款后的若干表述，如下：

a）废止第5条标题的“网络和信息安全”一词。

b）废止第5条第1款的“网络信息安全法”一词。

c）将第20条第1款第c项、第21条第2款、第29条第1款第c项、第30条第6款、第44条第4款、第46条第4款第a项和第47条第1款第c项的“网络信息安全”替换为“网络安全”一词。

d）废止第42条第1款第d项和第47条第1款第a项的“网络信息安全”一词。

9.将《公司所得税法》第67/2025/QH15号第12条第2款第b）项和《土地法》第31/2024/QH15号经第43/2024/QH15号、第47/2024/QH15号、第58/2024/QH15号、第71/2025/QH15号、第84/2025/QH15号、第93/2025/QH15号和第95/2025/QH15号法律修改、补充若干条款后的第169条第1款的“网络信息安全”替换为“网络安全”。

10.将《水资源法》第28/2023/QH15号经第84/2023/QH15号法律修改、补充若干条款后的第7条第3款第a项的“信息安全与保密”替换为“网络安全”。

11.废止《行政违规处理法》第15/2012/QH13号经第54/2014/QH13号、第18/2017/QH14号、第67/2020/QH14号、第09/2022/QH15号、第11/2022/QH15号、第56/2024/QH15号和第88/2025/QH15号法律修改、补充若干条款后的第24条第1款第đ项的“网络信息安全”一词。

12.废止《人民公安法》第37/2018/QH14号第16条第6款中“网络信息安全”一词，该法已经第21/2023/QH15号法、第30/2023/QH15号法、第2024/QH15号法、第2024/QH15号法、第52/2024/QH15号及第86/2025/QH15号法修订补充；《国民议会代表选举法》第85/2015/QH13号第66条第1款已根据第83/2025/QH15号法律修订并补充的“网络信息安全”一词。

13.废止《人民法院组织法》第34/2024/QH15号经第81/2025/QH15号法律修改、补充若干条款后的第136条第3款的“信息安全”一词；废止《电力法》第61/2024/QH15号经第94/2025/QH15号法律修改、补充若干条款后的第26条第1款的“信息安全”一词。

14.废止《化学品法》第69/2025/QH15号第29条第8款的“信息安全”一词；废止第29条第2款和第7款的“信息和安全”一词。

15.废止《竞标法》第22/2023/QH15号经第57/2024/QH15号和第90/2025/QH15号法律修改、补充若干条款后的第51条第3款、第52条第1款和第5款的“信息安全”一词；废止《民防法》第18/2023/QH15号经第98/2025/QH15号法律修改、补充若干条款后的第23条第1款第e项的“信息安全”一词。

16. 废止《原子能法》94/2025/QH15第7条第4款的“信息安全保障法”一词。

17. 废止《图书馆法》46/2019/QH14第49条第3款。

第44条 施行效力

1. 本法自2026年7月1日起施行。

2. 《网络信息安全法》第86/2015/QH13号经35/2018/QH14法律修改、补充若干条款后；《网络信息安全法》24/2018/QH14号自本法施行之日起失效。

第45条：过渡条款

1. 依照《网络信息安全法》第86/2015/QH13号及35/2018/QH14号法律修改、补充若干条款后确定等级的信息系统，自本法施行之日起继续保留已确定等级；自本法施行之日起12个月内，应当保障符合本法规定的相应等级的网络安全保护条件、标准、措施。

2. 依照《网络信息安全法》第86/2015/QH13号法律及其经第35/2018/QH14号法律修改、补充若干条款后规定的信息安全产品、服务及民用密码产品与服务经营许可证，在本法施行之日前已颁发的，使用至许可证载明期限届满有效。

3. 依照《网络信息安全法》86/2015/QH13号法律及经第35/2018/QH14号法律修改、补充若干条款后规定的保障网络安全产品、服务、解决方案、技术工具，在本法施行之日前已投入使用的，继续使用；自本法施行之日起12个月内，应当符合本法规定的网络安全条件。

本法由越南社会主义共和国第十五届国会第十次会议于2025年12月10日通过。

第45条　过渡条款

1. 依照《网络信息安全法》第86/2015/QH13号及35/2018/QH14号法律修改、补充若干条款后确定等级的信息系统，自本法施行之日起继续保留已确定等级；

自本法施行之日起12个月内，应当保障符合本法规定的相应等级的网络安全保护条件、标准、措施。

2.依照《网络信息安全法》第86/2015/QH13号法律及其经第35/2018/QH14号法律修改、补充若干条款后规定的信息安全产品、服务及民用密码产品与服务经营许可证，在本法施行之日前已颁发的，使用至许可证载明期限届满有效。

3.依照《网络信息安全法》86/2015/QH13号法律及经第35/2018/QH14号法律修改、补充若干条款后规定的保障网络安全产品、服务、解决方案、技术工具，在本法施行之日前已投入使用的，继续使用；自本法施行之日起12个月内，应当符合本法规定的网络安全条件。

本法由越南社会主义共和国第十五届国会第十次会议于2025年12月10日通过。