

中華人民共和國網路安全法

(2016年11月7日第十二屆全國人民代表大會常務委員會第二十四次會議通過)

流覽字型大小： 大 中 小 來源： 中國人大網 2016年11月7日 17:31:34

目 錄

| | |
|-----|---------------|
| 第一章 | 總 則 |
| 第二章 | 網路安全支援與促進 |
| 第三章 | 網路運行安全 |
| 第一節 | 一般規定 |
| 第二節 | 關鍵資訊基礎設施的運行安全 |
| 第四章 | 網路資訊安全 |
| 第五章 | 監測預警與應急處置 |
| 第六章 | 法律責任 |
| 第七章 | 附 則 |

第一章 總 則

第一條 為了保障網路安全，維護網路空間主權和國家安全、社會公共利益，保護公民、法人和其他組織的合法權益，促進經濟社會資訊化健康發展，制定本法。

第二條 在中華人民共和國境內建設、運營、維護和使用網路，以及網路安全的監督管理，適用本法。

第三條 國家堅持網路安全與資訊化發展並重，遵循積極利用、科學發展、依法管理、確保安全的方針，推進網路基礎設施建設和互聯互通，鼓勵網路技術創新和應用，支援培養網路安全人才，建立健全網路安全保障體系，提高網路安全保護能力。

第四條 國家制定並不斷完善網路安全戰略，明確保障網路安全的基本要求和主要目標，提出重點領域的網路安全政策、工作任務和措施。

第五條 國家採取措施，監測、防禦、處置來源於中華人民共和國境內外的網路安全風險和威脅，保護關鍵資訊基礎設施免受攻擊、侵入、干擾和破壞，依法懲治網路違法犯罪活動，維護網路空間安全和秩序。

第六條 國家宣導誠實守信、健康文明的網路行為，推動傳播社會主義核心價值觀，採取措施提高全社會的網路安全意識和水準，形成全社會共同參與促進網路安全的良好環境。

第七條 國家積極開展網路空間治理、網路技術研發和標準制定、打擊網路違法犯罪等方面的國際交流與合作，推動構建和平、安全、開放、合作的網路空間，建立多邊、民主、透明的網路治理體系。

第八條 國家網信部門負責統籌協調網路安全工作和相關監督管理工作。國務院電信主管部門、公安部門和其他有關機關依照本法和有關法律、行政法規的規定，在各自職責範圍內負責網路安全保護和監督管理工作。

縣級以上地方人民政府有關部門的網路安全保護和監督管理職責，按照國家有關規定確定。

第九條 網路運營者開展經營和服務活動，必須遵守法律、行政法規，尊重社會公德，遵守商業道德，誠實信用，履行網路安全保護義務，接受政府和社會的監督，承擔社會責任。

第十條 建設、運營網路或者通過網路提供服務，應當依照法律、行政法規的規定和國家標準的強制性要求，採取技術措施和其他必要措施，保障網路安全、穩定運行，有效應對網路安全事件，防範網路違法犯罪活動，維護網路資料的完整性、保密性和可用性。

第十一條 網路相關行業組織按照章程，加強行業自律，制定網路安全行為規範，指導會員加強網路安全保護，提高網路安全保護水準，促進行業健康發展。

第十二條 國家保護公民、法人和其他組織依法使用網路的權利，促進網路接入普及，提升網路服務水準，為社會提供安全、便利的網路服務，保障網路資訊依法有序自由流動。

任何個人和組織使用網路應當遵守憲法法律，遵守公共秩序，尊重社會公德，不得危害網路安全，不得利用網路從事危害國家安全、榮譽和利益，煽動顛覆國家政權、推翻社會主義制度，煽動分裂國家、破壞國家統一，宣揚恐怖主義、極端主義，宣揚民族仇恨、民族歧視，傳播暴力、淫穢色情資訊，編造、傳播虛假

資訊擾亂經濟秩序和社會秩序，以及侵害他人名譽、隱私、智慧財產權和其他合法權益等活動。

第十三條 國家支援研究開發有利於未成年人健康成長的網路產品和服務，依法懲治利用網路從事危害未成年人身心健康的活動，為未成年人提供安全、健康的網路環境。

第十四條 任何個人和組織有權對危害網路安全的行為向網信、電信、公安等部門舉報。收到舉報的部門應當及時依法作出處理；不屬於本部門職責的，應當及時移送有權處理的部門。

有關部門應當對舉報人的相關資訊予以保密，保護舉報人的合法權益。

第二章 網路安全支援與促進

第十五條 國家建立和完善網路安全標準體系。國務院標準化行政主管部門和國務院其他有關部門根據各自的職責，組織制定並適時修訂有關網路安全管理以及網路產品、服務和運行安全的國家標準、行業標準。

國家支援企業、研究機構、高等學校、網路相關行業組織參與網路安全國家標準、行業標準的制定。

第十六條 國務院和省、自治區、直轄市人民政府應當統籌規劃，加大投入，扶持重點網路安全技術產業和專案，支援網路安全技術的研究開發和應用，推廣安全可信的網路產品和服務，保護網路技術智慧財產權，支援企業、研究機構和高等學校等參與國家網路安全技術創新專案。

第十七條 國家推進網路安全社會化服務體系建設，鼓勵有關企業、機構開展網路安全認證、檢測和風險評估等安全服務。

第十八條 國家鼓勵開發網路資料安全保護和利用技術，促進公共資料資源開放，推動技術創新和經濟社會發展。

國家支援創新網路安全管理方式，運用網路新技術，提升網路安全保護水準。

第十九條 各級人民政府及其有關部門應當組織開展經常性的網路安全宣傳教育，並指導、督促有關單位做好網路安全宣傳教育工作。

大眾傳播媒介應當有針對性地面向社會進行網路安全宣傳教育。

第二十條 國家支持企業和高等學校、職業學校等教育培訓機構開展網路安全相關教育與培訓，採取多種方式培養網路安全人才，促進網路安全人才交流。

第三章 網路運行安全

第一節 一般規定

第二十一條 國家實行網路安全等級保護制度。網路運營者應當按照網路安全等級保護制度的要求，履行下列安全保護義務，保障網路免受干擾、破壞或者未經授權的訪問，防止網路資料洩露或者被竊取、篡改：

（一）制定內部安全管理制度和操作規程，確定網路安全負責人，落實網路安全保護責任；

（二）採取防範電腦病毒和網路攻擊、網路侵入等危害網路安全行為的技術措施；

（三）採取監測、記錄網路運行狀態、網路安全事件的技術措施，並按照規定留存相關的網路日誌不少於六個月；

（四）採取資料分類、重要資料備份和加密等措施；

（五）法律、行政法規規定的其他義務。

第二十二條 網路產品、服務應當符合相關國家標準的強制性要求。網路產品、服務的提供者不得設置惡意程式；發現其網路產品、服務存在安全缺陷、漏洞等風險時，應當立即採取補救措施，按照規定及時告知用戶並向有關主管部門報告。

網路產品、服務的提供者應當為其產品、服務持續提供安全維護；在規定或者當事人約定的期限內，不得終止提供安全維護。

網路產品、服務具有收集使用者資訊功能的，其提供者應當向用戶明示並取得同意；涉及使用者個人資訊的，還應當遵守本法和有關法律、行政法規關於個人資訊保護的規定。

第二十三條 網路關鍵設備和網路安全專用產品應當按照相關國家標準的強制性要求，由具備資格的機構安全認證合格或者安全檢測符合要求後，方可銷售或者提供。國家網信部門會同國務院有關部門制定、公佈網路關鍵設備和網

路安全專用產品目錄，並推動安全認證和安全檢測結果互認，避免重複認證、檢測。

第二十四條 網路運營者為使用者辦理網路接入、功能變數名稱註冊服務，辦理固定電話、行動電話等入網手續，或者為使用者提供資訊發佈、即時通訊等服務，在與使用者簽訂協定或者確認提供服務時，應當要求使用者提供真實身份資訊。使用者不提供真實身份資訊的，網路運營者不得為其提供相關服務。

國家實施網路可信身份戰略，支援研究開發安全、方便的電子身份認證技術，推動不同電子身份認證之間的互認。

第二十五條 網路運營者應當制定網路安全事件應急預案，及時處置系統漏洞、電腦病毒、網路攻擊、網路侵入等安全風險；在發生危害網路安全的事件時，立即啟動應急預案，採取相應的補救措施，並按照規定向有關主管部門報告。

第二十六條 開展網路安全認證、檢測、風險評估等活動，向社會發佈系統漏洞、電腦病毒、網路攻擊、網路侵入等網路安全資訊，應當遵守國家有關規定。

第二十七條 任何個人和組織不得從事非法侵入他人網路、干擾他人網路正常功能、竊取網路資料等危害網路安全的活動；不得提供專門用於從事侵入網路、干擾網路正常功能及防護措施、竊取網路資料等危害網路安全活動的程式、工具；明知他人從事危害網路安全的活動的，不得為其提供技術支持、廣告推廣、支付結算等幫助。

第二十八條 網路運營者應當為公安機關、國家安全機關依法維護國家安全和偵查犯罪的活動提供技術支持和協助。

第二十九條 國家支援網路運營者之間在網路安全資訊收集、分析、通報和應急處置等方面進行合作，提高網路運營者的安全保障能力。

有關行業組織建立健全本行業的網路安全保護規範和協作機制，加強對網路安全風險的分析評估，定期向會員進行風險警示，支援、協助會員應對網路安全風險。

第三十條 網信部門和有關部門在履行網路安全保護職責中獲取的資訊，只能用於維護網路安全的需要，不得用於其他用途。

第二節 關鍵資訊基礎設施的運行安全

第三十一條 國家對公共通信和資訊服務、能源、交通、水利、金融、公共服務、電子政務等重要行業和領域，以及其他一旦遭到破壞、喪失功能或者資料洩露，可能嚴重危害國家安全、國計民生、公共利益的關鍵資訊基礎設施，在網路安全等級保護制度的基礎上，實行重點保護。關鍵資訊基礎設施的具體範圍和安全保護辦法由國務院制定。

國家鼓勵關鍵資訊基礎設施以外的網路運營者自願參與關鍵資訊基礎設施保護體系。

第三十二條 按照國務院規定的職責分工，負責關鍵資訊基礎設施安全保護工作的部門分別編制並組織實施本行業、本領域的關鍵資訊基礎設施安全規劃，指導和監督關鍵資訊基礎設施運行安全保護工作。

第三十三條 建設關鍵資訊基礎設施應當確保其具有支援業務穩定、持續運行的性能，並保證安全技術措施同步規劃、同步建設、同步使用。

第三十四條 除本法第二十一條的規定外，關鍵資訊基礎設施的運營者還應當履行下列安全保護義務：

（一）設置專門安全管理機構和安全管理負責人，並對該負責人和關鍵崗位的人員進行安全背景審查；

（二）定期對從業人員進行網路安全教育、技術培訓和技能考核；

（三）對重要系統和資料庫進行容災備份；

（四）制定網路安全事件應急預案，並定期進行演練；

（五）法律、行政法規規定的其他義務。

第三十五條 關鍵資訊基礎設施的運營者採購網路產品和服務，可能影響國家安全的，應當通過國家網信部門會同國務院有關部門組織的國家安全審查。

第三十六條 關鍵資訊基礎設施的運營者採購網路產品和服務，應當按照規定與提供者簽訂安全保密協定，明確安全和保密義務與責任。

第三十七條 關鍵資訊基礎設施的運營者在中華人民共和國境內運營中收集和產生的個人資訊和重要資料應當在境內存儲。因業務需要，確需向境外提供的，應當按照國家網信部門會同國務院有關部門制定的辦法進行安全評估；法律、行政法規另有規定的，依照其規定。

第三十八條 關鍵資訊基礎設施的運營者應當自行或者委託網路安全服務機構對其網路的安全性和可能存在的風險每年至少進行一次檢測評估，並將檢測評估情況和改進措施報送相關負責關鍵資訊基礎設施安全保護工作的部門。

第三十九條 國家網信部門應當統籌協調有關部門對關鍵資訊基礎設施的安全保護採取下列措施：

（一）對關鍵資訊基礎設施的安全風險進行抽查檢測，提出改進措施，必要時可以委託網路安全服務機構對網路存在的安全風險進行檢測評估；

（二）定期組織關鍵資訊基礎設施的運營者進行網路安全應急演練，提高應對網路安全事件的水準和協同配合能力；

（三）促進有關部門、關鍵資訊基礎設施的運營者以及有關研究機構、網路安全服務機構等之間的網路安全資訊共用；

（四）對網路安全事件的應急處置與網路功能的恢復等，提供技術支援和協助。

第四章 網路資訊安全

第四十條 網路運營者應當對其收集的使用者資訊嚴格保密，並建立健全使用者資訊保護制度。

第四十一條 網路運營者收集、使用個人資訊，應當遵循合法、正當、必要的原則，公開收集、使用規則，明示收集、使用資訊的目的、方式和範圍，並經被收集者同意。

網路運營者不得收集與其提供的服務無關的個人資訊，不得違反法律、行政法規的規定和雙方的約定收集、使用個人資訊，並應當依照法律、行政法規的規定和與用戶的約定，處理其保存的個人資訊。

第四十二條 網路運營者不得洩露、篡改、毀損其收集的個人資訊；未經被收集者同意，不得向他人提供個人資訊。但是，經過處理無法識別特定個人且不能復原的除外。

網路運營者應當採取技術措施和其他必要措施，確保其收集的個人資訊安全，防止資訊洩露、毀損、丟失。在發生或者可能發生個人資訊洩露、毀損、丟失的情況時，應當立即採取補救措施，按照規定及時告知用戶並向有關主管部門報告。

第四十三條 個人發現網路運營者違反法律、行政法規的規定或者雙方的約定收集、使用其個人資訊的，有權要求網路運營者刪除其個人資訊；發現網路運營者收集、存儲的其個人資訊有錯誤的，有權要求網路運營者予以更正。網路運營者應當採取措施予以刪除或者更正。

第四十四條 任何個人和組織不得竊取或者以其他非法方式獲取個人資訊，不得非法出售或者非法向他人提供個人資訊。

第四十五條 依法負有網路安全監督管理職責的部門及其工作人員，必須對在履行職責中知悉的個人資訊、隱私和商業秘密嚴格保密，不得洩露、出售或者非法向他人提供。

第四十六條 任何個人和組織應當對其使用網路的行為負責，不得設立用於實施詐騙，傳授犯罪方法，製作或者銷售違禁物品、管制物品等違法犯罪活動的網站、通訊群組，不得利用網路發佈涉及實施詐騙，製作或者銷售違禁物品、管制物品以及其他違法犯罪活動的資訊。

第四十七條 網路運營者應當加強對其使用者發佈的資訊的管理，發現法律、行政法規禁止發佈或者傳輸的資訊的，應當立即停止傳輸該資訊，採取消除等處置措施，防止資訊擴散，保存有關記錄，並向有關主管部門報告。

第四十八條 任何個人和組織發送的電子資訊、提供的應用軟體，不得設置惡意程式，不得含有法律、行政法規禁止發佈或者傳輸的資訊。

電子資訊發送服務提供者和應用軟體下載服務提供者，應當履行安全管理義務，知道其用戶有前款規定行為的，應當停止提供服務，採取消除等處置措施，保存有關記錄，並向有關主管部門報告。

第四十九條 網路運營者應當建立網路資訊安全投訴、舉報制度，公佈投訴、舉報方式等資訊，及時受理並處理有關網路資訊安全的投訴和舉報。

網路運營者對網信部門和有關部門依法實施的監督檢查，應當予以配合。

第五十條 國家網信部門和有關部門依法履行網路資訊安全監督管理職責，發現法律、行政法規禁止發佈或者傳輸的資訊的，應當要求網路運營者停止傳輸，採取消除等處置措施，保存有關記錄；對來源於中華人民共和國境外的上述資訊，應當通知有關機構採取技術措施和其他必要措施阻斷傳播。

第五章 監測預警與應急處置

第五十一條 國家建立網路安全監測預警和資訊通報制度。國家網信部門應當統籌協調有關部門加強網路安全資訊收集、分析和通報工作，按照規定統一發佈網路安全監測預警資訊。

第五十二條 負責關鍵資訊基礎設施安全保護工作的部門，應當建立健全本行業、本領域的網路安全監測預警和資訊通報制度，並按照規定報送網路安全監測預警資訊。

第五十三條 國家網信部門協調有關部門建立健全網路安全風險評估和應急工作機制，制定網路安全事件應急預案，並定期組織演練。

負責關鍵資訊基礎設施安全保護工作的部門應當制定本行業、本領域的網路安全事件應急預案，並定期組織演練。

網路安全事件應急預案應當按照事件發生後的危害程度、影響範圍等因素對網路安全事件進行分級，並規定相應的應急處置措施。

第五十四條 網路安全事件發生的風險增大時，省級以上人民政府有關部門應當按照規定的許可權和程式，並根據網路安全風險的特點和可能造成的危害，採取下列措施：

（一）要求有關部門、機構和人員及時收集、報告有關資訊，加強對網路安全風險的監測；

（二）組織有關部門、機構和專業人員，對網路安全風險資訊進行分析評估，預測事件發生的可能性、影響範圍和危害程度；

（三）向社會發佈網路安全風險預警，發佈避免、減輕危害的措施。

第五十五條 發生網路安全事件，應當立即啟動網路安全事件應急預案，對網路安全事件進行調查和評估，要求網路運營者採取技術措施和其他必要措施，消除安全隱患，防止危害擴大，並及時向社會發佈與公眾有關的警示資訊。

第五十六條 省級以上人民政府有關部門在履行網路安全監督管理職責中，發現網路存在較大安全風險或者發生安全事件的，可以按照規定的許可權和程式對該網路的運營者的法定代表人或者主要負責人進行約談。網路運營者應當按照要求採取措施，進行整改，消除隱患。

第五十七條 因網路安全事件，發生突發事件或者生產安全事故的，應當依照《中華人民共和國突發事件應對法》、《中華人民共和國安全生產法》等有關法律、行政法規的規定處置。

第五十八條 因維護國家安全和社會公共秩序，處置重大突發社會安全事件的需要，經國務院決定或者批准，可以在特定區域對網路通信採取限制等臨時措施。

第六章 法律責任

第五十九條 網路運營者不履行本法第二十一條、第二十五條規定的網路安全保護義務的，由有關主管部門責令改正，給予警告；拒不改正或者導致危害網路安全等後果的，處一萬元以上十萬元以下罰款，對直接負責的主管人員處五千元以上五萬元以下罰款。

關鍵資訊基礎設施的運營者不履行本法第三十三條、第三十四條、第三十六條、第三十八條規定的網路安全保護義務的，由有關主管部門責令改正，給予警告；拒不改正或者導致危害網路安全等後果的，處十萬元以上一百萬元以下罰款，對直接負責的主管人員處一萬元以上十萬元以下罰款。

第六十條 違反本法第二十二條第一款、第二款和第四十八條第一款規定，有下列行為之一的，由有關主管部門責令改正，給予警告；拒不改正或者導致危害網路安全等後果的，處五萬元以上五十萬元以下罰款，對直接負責的主管人員處一萬元以上十萬元以下罰款：

- (一) 設置惡意程式的；
- (二) 對其產品、服務存在的安全缺陷、漏洞等風險未立即採取補救措施，或者未按照規定及時告知用戶並向有關主管部門報告的；
- (三) 擅自終止為其產品、服務提供安全維護的。

第六十一條 網路運營者違反本法第二十四條第一款規定，未要求使用者提供真實身份資訊，或者對不提供真實身份資訊的使用者提供相關服務的，由有關主管部門責令改正；拒不改正或者情節嚴重的，處五萬元以上五十萬元以下罰款，並可以由有關主管部門責令暫停相關業務、停業整頓、關閉網站、吊銷相關業務許可證或者吊銷營業執照，對直接負責的主管人員和其他直接責任人員處一萬元以上十萬元以下罰款。

第六十二條 違反本法第二十六條規定，開展網路安全認證、檢測、風險評估等活動，或者向社會發佈系統漏洞、電腦病毒、網路攻擊、網路侵入等網路安全資訊的，由有關主管部門責令改正，給予警告；拒不改正或者情節嚴重的，處一萬元以上十萬元以下罰款，並可以由有關主管部門責令暫停相關業務、停業整頓、關閉網站、吊銷相關業務許可證或者吊銷營業執照，對直接負責的主管人員和其他直接責任人員處五千元以上五萬元以下罰款。

第六十三條 違反本法第二十七條規定，從事危害網路安全的活動，或者提供專門用於從事危害網路安全活動的程式、工具，或者為他人從事危害網路安全的活動提供技術支持、廣告推廣、支付結算等幫助，尚不構成犯罪的，由公安機關沒收違法所得，處五日以下拘留，可以並處五萬元以上五十萬元以下罰款；情節較重的，處五日以上十五日以下拘留，可以並處十萬元以上一百萬元以下罰款。

單位有前款行為的，由公安機關沒收違法所得，處十萬元以上一百萬元以下罰款，並對直接負責的主管人員和其他直接責任人員依照前款規定處罰。

違反本法第二十七條規定，受到治安管理處罰的人員，五年內不得從事網路安全管理和網路運營關鍵崗位的工作；受到刑事處罰的人員，終身不得從事網路安全管理和網路運營關鍵崗位的工作。

第六十四條 網路運營者、網路產品或者服務的提供者違反本法第二十二條第三款、第四十一條至第四十三條規定，侵害個人資訊依法得到保護的權利的，由有關主管部門責令改正，可以根據情節單處或者並處警告、沒收違法所得、處違法所得一倍以上十倍以下罰款，沒有違法所得的，處一百萬元以下罰款，對直接負責的主管人員和其他直接責任人員處一萬元以上十萬元以下罰款；情節嚴重的，並可以責令暫停相關業務、停業整頓、關閉網站、吊銷相關業務許可證或者吊銷營業執照。

違反本法第四十四條規定，竊取或者以其他非法方式獲取、非法出售或者非法向他人提供個人資訊，尚不構成犯罪的，由公安機關沒收違法所得，並處違法所得一倍以上十倍以下罰款，沒有違法所得的，處一百萬元以下罰款。

第六十五條 關鍵資訊基礎設施的運營者違反本法第三十五條規定，使用未經安全審查或者安全審查未通過的網路產品或者服務的，由有關主管部門責令

停止使用，處採購金額一倍以上十倍以下罰款；對直接負責的主管人員和其他直接責任人員處一萬元以上十萬元以下罰款。

第六十六條 關鍵資訊基礎設施的運營者違反本法第三十七條規定，在境外存儲網路資料，或者向境外提供網路資料的，由有關主管部門責令改正，給予警告，沒收違法所得，處五萬元以上五十萬元以下罰款，並可以責令暫停相關業務、停業整頓、關閉網站、吊銷相關業務許可證或者吊銷營業執照；對直接負責的主管人員和其他直接責任人員處一萬元以上十萬元以下罰款。

第六十七條 違反本法第四十六條規定，設立用於實施違法犯罪活動的網站、通訊群組，或者利用網路發佈涉及實施違法犯罪活動的資訊，尚不構成犯罪的，由公安機關處五日以下拘留，可以並處一萬元以上十萬元以下罰款；情節較重的，處五日以上十五日以下拘留，可以並處五萬元以上五十萬元以下罰款。關閉用於實施違法犯罪活動的網站、通訊群組。

單位有前款行為的，由公安機關處十萬元以上五十萬元以下罰款，並對直接負責的主管人員和其他直接責任人員依照前款規定處罰。

第六十八條 網路運營者違反本法第四十七條規定，對法律、行政法規禁止發佈或者傳輸的資訊未停止傳輸、採取消除等處置措施、保存有關記錄的，由有關主管部門責令改正，給予警告，沒收違法所得；拒不改正或者情節嚴重的，處十萬元以上五十萬元以下罰款，並可以責令暫停相關業務、停業整頓、關閉網站、吊銷相關業務許可證或者吊銷營業執照，對直接負責的主管人員和其他直接責任人員處一萬元以上十萬元以下罰款。

電子資訊發送服務提供者、應用軟體下載服務提供者，不履行本法第四十八條第二款規定的安全管理義務的，依照前款規定處罰。

第六十九條 網路運營者違反本法規定，有下列行為之一的，由有關主管部門責令改正；拒不改正或者情節嚴重的，處五萬元以上五十萬元以下罰款，對直接負責的主管人員和其他直接責任人員，處一萬元以上十萬元以下罰款：

- (一) 不按照有關部門的要求對法律、行政法規禁止發佈或者傳輸的資訊，採取停止傳輸、消除等處置措施的；
- (二) 拒絕、阻礙有關部門依法實施的監督檢查的；
- (三) 拒不向公安機關、國家安全機關提供技術支援和協助的。

第七十條 發佈或者傳輸本法第十二條第二款和其他法律、行政法規禁止發佈或者傳輸的資訊的，依照有關法律、行政法規的規定處罰。

第七十一條 有本法規定的違法行為的，依照有關法律、行政法規的規定記入信用檔案，並予以公示。

第七十二條 國家機關政務網路的運營者不履行本法規定的網路安全保護義務的，由其上級機關或者有關機關責令改正；對直接負責的主管人員和其他直接責任人員依法給予處分。

第七十三條 網信部門和有關部門違反本法第三十條規定，將在履行網路安全保護職責中獲取的資訊用於其他用途的，對直接負責的主管人員和其他直接責任人員依法給予處分。

網信部門和有關部門的工作人員怠忽職守、濫用職權、徇私舞弊，尚不構成犯罪的，依法給予處分。

第七十四條 違反本法規定，給他人造成損害的，依法承擔民事責任。

違反本法規定，構成違反治安管理行為的，依法給予治安管理處罰；構成犯罪的，依法追究刑事責任。

第七十五條 境外的機構、組織、個人從事攻擊、侵入、干擾、破壞等危害中華人民共和國的關鍵資訊基礎設施的活動，造成嚴重後果的，依法追究法律責任；國務院公安部門和有關部門並可以決定對該機構、組織、個人採取凍結財產或者其他必要的制裁措施。

第七章 附 則

第七十六條 本法下列用語的含義：

（一）網路，是指由電腦或者其他資訊終端及相關設備組成的按照一定的規則和程式對資訊進行收集、存儲、傳輸、交換、處理的系統。

（二）網路安全，是指通過採取必要措施，防範對網路的攻擊、侵入、干擾、破壞和非法使用以及意外事故，使網路處於穩定可靠運行的狀態，以及保障網路資料的完整性、保密性、可用性的能力。

（三）網路運營者，是指網路的所有者、管理者和網路服務提供者。

（四）網路資料，是指通過網路收集、存儲、傳輸、處理和產生的各種電子資料。

(五)個人資訊，是指以電子或者其他方式記錄的能夠單獨或者與其他資訊結合識別自然人個人身份의各種資訊，包括但不限於自然人的姓名、出生日期、身份證件號碼、個人生物識別資訊、住址、電話號碼等。

第七十七條 存儲、處理涉及國家秘密資訊的網路的運行安全保護，除應當遵守本法外，還應當遵守保密法律、行政法規的規定。

第七十八條 軍事網路的安全保護，由中央軍事委員會另行規定。

第七十九條 本法自 2017 年 6 月 1 日起施行。

責任編輯：馬冬瀟