中國大陸《網絡安全法》對資訊安全問題研究

A Study of Information Security Issues in China's "Cybersecurity Law"

陳銘聰（Chen, Ming-Tsung）
國立臺灣大學國家發展研究所博士生

壹、前言

近年來，中國大陸（以下簡稱大陸）高度重視資訊化發展在推動國家現代化建設的基礎性和戰略性作用，《網絡安全法》[1] 無疑是大陸第一部全面規範網路空間安全管理問題的基礎性法律，[2] 這是網路空間法治建設的重要里程碑，除了讓網際網路在法治軌道上健康運行提供法律保護，也為將來可能的制度創新做出原則性的法律規定，並為網路安全相關工作提供法律依據。這代表大陸在網路空間管理的道路上，堅持要走自己的路。根據大陸官方媒體報導，《網絡安全法》的公布施行至少突出了以下 6 大特點：一、明確了網路空間主權的原則；二、明確了網路產品和服務提供者的安全義務；三、明確了網路運營者的安全義務；四、完善了個人資訊保護規則；五、建立了關鍵資訊基礎設施安全保護制度；六、確立了關鍵資訊基礎設施重要數據跨境傳輸的規則。[3]

---

1 網路在大陸稱為網絡，網際網路在大陸稱為互聯網。

2 王靜、周向明，「網絡空間法律問題初探」，**現代情報**（北京），第 2 期（2003 年），頁 40-42。

3 「專家解讀《網絡安全法》，具有六大突出亮點」（2016 年 11 月 8 日），2018 年 5 月 20 日瀏覽，《**新華網**》，http://www.xinhuanet.com/info/2016-11/08/c_135813341.htm。

貳、《網絡安全法》的立法背景

資訊安全已經成為網路時代的最重大課題，尤其是網路空間中存在許多違法資訊，已經嚴重侵害人民、法人和其他團體的合法權益，尤其是大陸每年的「雙十一購物狂歡節」，[4] 更是網路詐騙的高峰期，詐騙手法更是層出不窮，如網路購物退貨詐騙、冒充網購平臺的中獎詐騙、謊稱網站人手不夠而兼職詐騙等，令不少網民受騙上當。[5] 在 2016 大陸網際網路大會上，「中國互聯網協會」與「中國互聯網協會 12321 網路不良與垃圾資訊舉報受理中心」聯合發布《中國網民權益保護調查報告 (2016)》的內容顯示，從 2015 年下半年到 2016 上半年的一年間，大陸網民因為遭受垃圾資訊、詐騙資訊和個人資訊洩露等各類侵害所造成經濟損失高達人民幣（下同）915 億元。[6] 2016 年上半年以來，大陸網民平均每週收到垃圾郵件 18.9 封、垃圾短信 20.6 條、騷擾電話 21.3 個，其中騷擾電話是網民最為反感的騷擾來源，另外，有 84% 的網民曾親身感受到由於個人資訊洩露帶來的不良影響。僅 2017 年一整年，大陸網民因垃圾資訊、詐騙資訊、個人資訊洩露等遭受的經濟損失為人均 133 元，比去年增加 9 元，其中，高達 9% 的網民由於各類侵害造成的經濟損失在 1,000 元以上。[7] 然而，在網路詐騙的案件中，受害者雖然可以通過法律途徑追回，但能夠成功追討被騙的財物，機率其實不大。[8]

當今世界各國政府正面對著日益嚴峻的電信網路犯罪形勢，這些犯罪

---

4 「雙十一購物狂歡節」，是指大陸每年 11 月 11 日的網絡促銷日，源於淘寶商城（天貓）2009 年 11 月 11 日舉辦的網絡促銷活動，當時參與的商家數量和促銷力度有限，但營業額遠超過預想的效果，於是 11 月 11 日成為天貓舉辦大規模促銷活動的固定日期。雙十一購物狂歡節已成為大陸電子商務行業的年度盛事，並且逐漸影響到國際電子商務行業。

5 「網絡安全法為公民個人隱私保護撐腰」（2016 年 11 月 28 日），2018 年 5 月 20 日瀏覽，《千龍網》，http://bbs.qianlong.com/thread-9887442-1-1.html。

6 大陸網民數量 6.88 億 × 網民平均經濟損失 133 元 = 915 億元。

7 「54% 的線民認為個人資訊洩露嚴重」（2016 年 6 月 20 日），2018 年 5 月 20 日瀏覽，《中國網民權益保護調查報告 2016》，http://www.isc.org.cn/zxzx/xhdt/listinfo-33759.html。

8 黃建軍，「網絡詐騙的損失也可以通過民事途徑追回」（2015 年 5 月 28 日），2018 年 5 月 20 日瀏覽，《華律網》，http://www.66law.cn/goodcase/32010.aspx。

集團不但組織相當嚴密，藏身更趨隱蔽，犯罪手法不斷升級，受害群體涵蓋各行各業和各個年齡階段，已經給社會造成巨大的財產損失，更嚴重影響人與人之間的信任感和對政府公權力失去信心。這類新型電信網路犯罪的典型特徵，就是利用電信通訊、網際網路等技術和工具，透過發送簡訊、網路資訊、撥打電話和植入木馬程序等手段，誘騙被害人將錢財匯（存）入其控制的銀行帳戶。[9] 過去，大陸網路保護的法律體系並不完備，甚至沒有真正意義上的網路安全法規，當發生網路侵權問題而造成損害之後，受害者想要維護自己權利，卻陷入無法可以主張的困境。因此，大陸迫切需要建立網路安全保護的法律制度，保護個人資訊安全，提高網路安全意識，淨化網路空間環境。[10]

2015 年 6 月 24 日，大陸第 12 屆全國人民代表大會常務委員會第 15 次會議對《網絡安全法》草案進行了首次審議，並向全社會徵求意見。2016 年 11 月 7 日，大陸第 12 屆全國人民代表大會常務委員會第 24 次會議，會議以 154 票贊成、1 票棄權，通過該法案，並自 2017 年 6 月 1 日起開始施行，該法的公布施行，這是網路時代發展的需求。

《網絡安全法》的立法目的，根據第 1 條規定，為了保護網路安全，維護網路空間主權和國家安全、社會公共利益，保護人民、法人和其他組織的合法權益，促進資訊時代的健康發展，[11] 由此可知，該法為「資訊安全」保護提供了法律依據。《網絡安全法》公布施行後，大陸全國人大常委會法工委經濟法室副主任楊合慶在新聞發布會上表示，制定《網絡安全法》是為了適應網路時代的要求，是落實國家總體安全觀的重要措施。[12]

---

[9]「對最新電信、網絡詐騙司法文件的理解」（2015 年 12 月 21 日），2018 年 5 月 20 日瀏覽，《搜狐網》，http://www.sohu.com/a/122145005_480606。

[10]「中國首部網絡安全法通過明確網絡空間主權原則」（2016 年 11 月 7 日），2018 年 5 月 20 日瀏覽，《觀察者網》，http://money.163.com/16/1107/20/C5A0TCFH002580S6_all.html。

[11] 資訊一詞在大陸稱為信息，為了行文和閱讀的方便，原本應該以信息表示的，除非必要維持之外，均以資訊一詞表示。

[12]「全國人大常委會法工委經濟法室副主任楊合慶回答記者提問」（2016 年 11 月 7 日），2018 年 5 月 20 日瀏覽，《人大新聞網》，http://www.npc.gov.cn/npc/zhibo/zzzb39/2016-11/07/content_2001477.htm。

截止 2013 年底，大陸網路用戶數已經是高居世界第一，[13] 大陸已經是一個網路大國，也是面臨網路安全威脅最嚴重的國家之一，因此，對於保護網路空間的合法權益，建構網路空間的安全秩序，也就顯得十分重要。《網絡安全法》充分體現網路安全立法的核心理念，符合大陸當前網路安全工作的實際和需要，也為今後大陸針對個人資訊的法律保護，奠定了堅實的上位法律基礎。[14]

參、《網絡安全法》的主要內容

《網絡安全法》總共有 7 章，79 個條文，幾乎將網路空間管理所面臨到的問題都加以規範，按大陸官方網站的說法，這是大陸第一部全面規範網路空間管理問題的基礎性法律，是大陸網路空間法治建設的重要里程碑，是依法治網、化解網路風險的法律重器，是讓網際網路在法治軌道上健康運行的重要保障。《網絡安全法》除了將過去一些網路安全管理的措施加以法制化，並為將來可能的技術創新做了原則性規定，為網路安全工作提供法律保障。[15] 由於該法內容十分豐富，以下將主要內容整理如下：

一、網路資訊

根據該法第 10 條規定，建設、運營網路或者透過網路提供服務，應當依照法律、行政命令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，保護網路安全、穩定運行，有效應對網路安全事件，防範網路違法犯罪活動，維護網路資訊的保密性、完整性和可用性，此即網路資訊最重要的 3 個屬性。保密性（confidentiality），指資訊不被洩露給未經授權者的特性；完整性（integrity），指資訊在儲存或傳輸過程中保持

---

[13]「網絡經濟規模逾 6000 億，互聯網思維改變經濟格局」（2014 年 5 月 20 日），2018 年 5 月 20 日瀏覽，《新華網》，http://finance.sina.com.cn/chanjing/cyxw/20140420/155418857057.shtml。

[14] 邵美彥，「個人信息的法律保護」，**法制博覽**（北京），第 1 期（2018 年），頁 229。

[15]「《網絡安全法》出臺是網絡空間法治建設重要里程碑」（2016 年 11 月 09 日），2018 年 5 月 18 日瀏覽，《中國網信網》，http://www.cac.gov.cn/2016-11/09/c_1119879953.htm。

未經授權不能改變的特性；可用性（availability），指資訊可被授權者訪問並使用的特性。

值得注意的是，《網絡安全法》還對「違法信息」特別定義，該法第 12 條第 2 項規定，任何個人和組織不得危害網路安全，不得利用網路從事宣揚恐怖主義、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。最終，第 70 條規定，發布或者傳輸違法資訊，依照相關法律和行政命令的規定處罰。[16]

二、網路運行安全的一般規定

網路運行安全的一般規定規範在《網絡安全法》第 3 章第 1 節，共用 10 個條文對網路產品和服務提供者的安全義務有了明確的規定，包括：國家實行網路安全等級保護制度（第 21 條），網路產品、服務應當符合相關國家標準的強制性要求（第 24 條），推動安全認證和安全檢測結果互認（第 23 條），要求使用者提供真實身分資訊（第 24 條），網路安全的事件處理（第 25 條）等。這些措施就短時間來看，一定程度上可以滿足保護國家網路安全的需求，應對來自從境內外可能實施的網路攻擊和威脅；但就中長期前景來看，大陸的網路戰略是如何在持續開放的全球網際網路空間內，有效預防來自擁有網路科技優勢能力的國家或組織對關鍵資訊基礎設施所構成的威脅，這也是後續修定相關法律，完善網路安全戰略，設計

[16] 大陸《刑法》第 120-3 條：「宣揚恐怖主義、極端主義、煽動實施恐怖活動罪：以製作、散發宣揚恐怖主義、極端主義的圖書、音頻視頻資料或者其他物品，或者通過講授、發布資訊等方式宣揚恐怖主義、極端主義的，或者煽動實施恐怖活動的，處五年以下有期徒刑、拘役、管制或者剝奪政治權利，並處罰金；情節嚴重的，處五年以上有期徒刑，並處罰金或者沒收財產。《刑法》291-2 條第 2 項：「製造虛假的險情、疫情、災情、警情，在信息網絡或者其他媒體上傳播，或者明知是上述虛假信息，故意在信息網絡或者其他媒體上傳播，嚴重擾亂社會秩序的，處三年以下有期徒刑、拘役或者管制；造成嚴重後果的，處三年以上七年以下有期徒刑。《治安管理處罰法》第 25 條：「有下列行為之一的，處五日以上十日以下拘留，可以並處五百元以下罰款；情節較輕的，處五日以下拘留或者五百元以下罰款：（一）散布謠言，謊報險情、疫情、警情或者以其他方法故意擾亂公共秩序的；（二）投放虛假的爆炸性、毒害性、放射性、腐蝕性物質或者傳染病病原體等危險物質擾亂公共秩序的；（三）揚言實施放火、爆炸、投放危險物質擾亂公共秩序的。

安全的操作程序，必須認真思考的問題。[17]

根據該法第 26 條規定，開展網路安全認證、檢測、風險評估等活動，向社會發布系統漏洞、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。安全認證、檢測和風險評估作為加強網路安全管理的手段，也在《網絡安全法》中有多處提及（如第 29 條、第 38 條、第 39 條、第 53 條、第 54 條、第 55 條等），為網路安全風險管理相關工作提供了法律依據。不過，大陸存在不少機構和個人在未獲得正式授權之前，即進行安全檢測、漏洞挖掘和披露的行為，其中不乏因為操作不當或是評估不足，導致對被檢測方造成危害的案例。[18] 另外，第 28 條規定，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。

三、關鍵資訊基礎設施的運行規定

關鍵資訊基礎設施的運行規定規範在《網絡安全法》第 3 章在第 2 節，專門用 9 個條文規範關鍵資訊基礎設施的安全。關鍵基礎設施是一個有機的綜合系統，內部各分類設施系統之間聯繫非常緊密，並且這個系統在其內部以及同外界環境之間均需協調一致，才能正常良好地運轉。[19] 過去，企業實施網路安全的風險管理，原本用意是基於保護企業資產和業務的角度，避免因為駭客入侵而遭受損失。然而，《網絡安全法》是從國家總體安全觀出發，將網路空間主權和國家安全、社會公共利益，公民、法人和其他組織的合法權益均納入保護對象，最大限度地擴展網路空間風險管理的適用範圍。其中，有 5 個方面值得注意：

（一）保護內容。第 31 條規定，強化了關鍵資訊基礎設施保護的內容，

---

[17] 趙亞娟，「專家解讀網絡安全法草案：為建設網絡強國提供制度保障」（2015 年 7 月 16 日），2018 年 5 月 20 日瀏覽，《東方網》，http://news.eastday.com/c/20150716/u1a8798407.html。

[18] 劉賢剛、何延哲，「《網絡安全法》對網絡安全風險管理提出更高要求」（2016 年 11 月 15 日），2018 年 5 月 15 日瀏覽，《中國網信網》，http://www.cac.gov.cn/2016-11/15/c_1119916836.htm。

[19] 王玥，「確立監測預警與應急處置制度正當時 - 從網絡安全法草案徵求意見談起」，法治週末（北京），2015 年 7 月 23 日。

明確列出關鍵資訊基礎設施的範圍，包括：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。因為關鍵資訊基礎設施保護的影響重大，在網路安全保護的等級上，屬於重點保護的對象。

（二）安全保護義務。除第 21 條規定之外，第 34 條還規定，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：1. 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；2. 定期對從業人員進行網路安全教育、技術培訓和技能考核 3. 對重要系統和資料庫進行容災備份；[20] 4. 制定網路安全事件應急預案，並定期進行演練；5. 法律、行政命令規定的其他義務。

（三）安全審查。第 35 條規定，關鍵資訊基礎設施運營者採購網路產品和服務，可能影響國家安全的，應透過安全審查，該措施即是針對國家安全層面實施安全風險管理的有效舉措。

（四）保密協議。第 36 條規定，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。

（五）資訊儲存。《網絡安全法》首次在法律層面上明確規定對特定個人資訊和重要資訊必須儲存在大陸境內。這裡的「特定」並非指一般的個人資訊，而是指收集主體和管道，即第 37 條規定的關鍵資訊基礎設施的運營者在大陸境內運營中收集和產生的個人資訊和重要資訊。

值得注意的是，列入關鍵資訊基礎設施的範圍，涵蓋國家安全、經濟安全和社會民生保護等領域，具體範圍包括基礎資訊網路、重要行業和領

[20] 容災備份實際上是兩個概念，容災是為了在遭遇災害時能保證資訊系統能正常運行，幫助企業實現業務連續性的目標，備份是為了應對災難來臨時造成的資料丟失問題。「容災備份」，2018 年 5 月 20 日瀏覽，《百度百科》，https://baike.baidu.com/item/ 容災備份。

域的重要資訊系統、重要政務網路、用戶數量眾多的商業網路等。[21] 從全球各國的實踐來看，保護關鍵資訊基礎設施的安全，已經是國家網路安全戰略中最重要的內容，這也與人們日常生活對關鍵資訊基礎設施的強烈依賴密不可分。[22]

四、網路資訊安全

網路資訊安全規定《網絡安全法》第 4 章，共 11 個條文。特別針對網路運營者收集和使用的個人資訊的安全進行規範（第 40 條至 50 條）。在個人資訊保護方面，該法不僅繼承了現有法律關於個人資訊保護的主要條款內容，而且根據新時代特徵、發展需求和保護理念，創造性地增加了部分規定，例如：第 40 條明確將收集和使用個人資訊的網路運營者，設定為個人資訊保護的責任主體；第 41 條增加了最少夠用原則；第 42 條增設了個人資訊共用的條件；第 43 條增加了個人在一定情形下刪除、更正其個人資訊的權利；第 44 條在法律層面首次給予個人資訊交易一定的合法空間。這 5 條關於個人資訊的規定，注重保護個人對自己資訊的自主權和支配權，顯示大陸正努力與現行國際規則及歐美個人資訊保護等方面的立法，實現理念上的接軌。[23]

網路運營者的個人資訊保護義務方面，《網絡安全法》很大程度上保持了與既有法律法規的一致，例如：第 41 條規定，要求網路運營者收集、使用個人資訊應當遵循合法、正當、必要的原則，明示收集、使用資訊的目的、方式和範圍，經被收集者同意，公開收集、使用規則。第 42 條規定，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，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、丟失等。

---

[21]「網絡安全法草案解讀符合中國網絡空間安全需求」（2015 年 7 月 17 日），2018 年 5 月 20 日瀏覽，《新華網》，http://www.xinhuanet.com/politics/2015-07/17/c_128030632.htm。

[22]「解讀網絡安全法草案：為建設網絡強國提供制度保護」（2015 年 7 月 16 日），2018 年 5 月 20 日瀏覽，《中國網》，http://big5.china.com.cn/news/2015-07/16/content_36078948.htm。

[23] 洪延青，「網絡安全為人民的實在舉措—評《網絡安全法》」（2016 年 11 月 10 日），2018 年 5 月 20 日瀏覽，《中國網信網》，http://www.cac.gov.cn/2016-11/10/c_1119889930.htm。

在網路和大數據時代，侵犯個人資訊和電信網路詐騙是兩大主要新型網路違法犯罪類型，其中違法犯罪活動的網站和通訊群組以及利用網路發布與施行詐騙是上述兩大犯罪的兩個終端。[24] 針對電信詐騙特別是新型網路違法犯罪呈多發態勢，因此，第 46 條規定，任何個人和組織不得設立用於施行詐騙，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，不得利用網路發布與施行詐騙，製作或者銷售違禁物品、管制物品以及其他違法犯罪活動有關的資訊，並在第 67 條增加相應法律責任的規定。

針對網路空間容易流傳許多的違法資訊，第 47 條規定，網路運營者必須自我審查網路的內容，應當加強對用戶發布的資訊進行管理，若發現法律、行政命令所禁止發布或傳輸的資訊，應當立即停止傳輸該資訊，採取立即消除措施，防止資訊擴散，保存相關記錄，並向相關主管部門報告。

「惡意程式」的威脅是現今網路資訊安全的頭痛問題，[25] 隨著惡意程式的快速成長與變種，資訊安全的防範手段也必須要跟上才行，不過，資安人員一般都是被動的立場去解決惡意程式的攻擊，例如當新的惡意程式展開攻擊時，資安人員才能想辦法去偵測，然後再去補救受到攻擊的損害，最後再建構出有效的防禦機制。第 48 條也對設置惡意程式做出規定，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、行政命令禁止發布或者傳輸的資訊。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，知道用戶有前述規定行為的，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。

網路舉報和投訴是近年來隨著網路科技的發展而新興起來的新事物，主要有兩個方面的作用。一是透過設立網上舉報視窗，開展廣泛的舉報宣

[24]「專家解讀《網絡安全法》，具有六大突出亮點」（2016 年 11 月 8 日），2018 年 5 月 20 日瀏覽，《新華網》，http://www.xinhuanet.com/info/2016-11/08/c_135813341.htm。

[25] 張濤，「互聯網惡意程式治理存困惑，立法亟待完善」，通信世界（北京），第 21 期（2017 年），頁 25。

傳，提供法律諮詢；二是在網上受理群眾的舉報。《網絡安全法》也規定舉報和投訴的制度，第 49 條第 1 項規定，網路運營者應當建立網路資訊安全投訴、舉報制度，公布投訴、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。

值得注意的是，針對網路監控部分，第 50 條規定分為 3 個部分來規範：第一，規定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；第二，若發現法律、行政命令禁止發布或者傳輸的資訊，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；第三，對來源於境外的上述資訊，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。

五、監測預警與應急處理

監測預警與應急處理規定《網絡安全法》第 5 章，共 8 個條文。建立的監測預警與應急處置制度，對大陸的網路安全保護具有十分重要的意義，大陸具有從國家層面增強對關鍵基礎設施資訊安全保護的迫切需要。例如要求國務院有關部門建立健全網路安全監測預警和資訊通報制度，加強網路安全資訊收集、分析和情況通報工作（第 51 條、第 52 條）；建立網路安全應急工作機制（第 53 條第 1 項），制定應急預案（第 53 條第 2 項）；規定預警資訊的發布及網路安全事件應急處置措施（第 54 條至 58 條）；為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，對網路管制作了規定（第 58 條）。

近年來，網路安全事件頻繁發生，呈現不確定性、全域性和連鎖性特點，加強監測預警已經成為國際社會的普遍共識，重視應急處理更是網路安全活動的基本措施。儘管大陸網路空間法治建設剛剛起步，但是所面臨的網路安全問題卻與世界同步，而且是全方位的，尤其是面臨錯綜複雜的國際環境下與國情相關的特殊網路資訊安全問題，在監測預警與應急處理方面，大陸迫切需要在立法中確立系統完善的網路資訊安全事件預警監測與應急處置制度，特別是針對國家關鍵基礎設施的相關制度，以法律的強制性來控制和消除網路資訊安全事件帶來的負面影響。這些措施對於有效

保護國家關鍵基礎設施網路資訊安全的實現，支撐整個社會持續穩定的正常運轉，是非常有必要的。

肆、《網絡安全法》的立法評析

一、《網絡安全法》值得關注之處

《網絡安全法》在確立保護網路安全基本制度，保護網路資訊依法有序自由流動以及促進網路技術創新和資訊化發展持續健康發展的基礎上，充分體現了保護各類網路主體的合法權利的立法原則，特別是把保護人民合法權益不受侵犯作為網路安全立法的基礎。

（一）提出網路安全戰略，明確網路空間治理

《網絡安全法》第 4 條明確提出了網路安全戰略的主要內容，明確保護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 7 條規定，致力於推動構建和平、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。這是大陸第 1 次透過國家法律的形式向世界宣示網路空間治理目標，明確表達對網路空間治理訴求，提高了大陸網路治理公共政策的透明度，符合作為網路大國的地位，這將有利於提升對網路空間的國際話語權和規則制定權，促成網路空間國際規則的制定。

（二）明確政府的職責許可權，完善網路安全監管體制

《網絡安全法》將現行有效的網路安全監管體制法制化，明確了網信部門與其他相關網路監管部門的職責分工。第 8 條規定，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法在各自職責範圍內負責網路安全保護和監督管理工作。這種「1+X」的監管體制，符合當前大陸網際網路與現實社會全面融合特點和監管需要。[26]

[26]「新網絡安全法內容主要有哪些」（2017 年 10 月 19 日），2018 年 5 月 20 日瀏覽，《華律網》，http://www.66law.cn/laws/421562.aspx。

（三）強化網路運行安全，重點保護關鍵資訊基礎設施

《網絡安全法》第 3 章用了近三分之一的篇幅規範網路運行安全，特別強調要保護關鍵資訊基礎設施的運行安全。關鍵資訊基礎設施是指那些一旦遭到破壞、喪失功能或者資料洩露，可能嚴重危害國家安全、國計民生、公共利益的系統和設施。網路運行安全是網路安全的重心，關鍵資訊基礎設施安全則是重中之重，與國家安全和社會公共利益息息相關。為此，在網路安全等級保護制度的基礎上，對關鍵資訊基礎設施實行重點保護，明確關鍵資訊基礎設施的運營者負有更多的安全保護義務，並配以國家安全審查、重要資料強制本機存放區等法律措施，確保關鍵資訊基礎設施的運行安全。

（四）完善網路安全義務，加大違法懲處力度

《網絡安全法》將原來散見於各種法規、規章中的規定上升到法律層面，對網路運營者等主體的法律義務和責任做了全面規定，包括守法義務，遵守社會公德、商業道德義務，誠實信用義務，網路安全保護義務，接受監督義務，承擔社會責任等，並在網路運行安全、網路資訊安全、監測預警與應急處置等章節中進一步明確和細化。在法律責任中則提高了違法行為的處罰標準，加大了處罰力度，有利於保護該法的執行。

（五）監測預警與應急處置措施制度化、法制化

《網絡安全法》第 5 章將監測預警與應急處置工作制度化、法制化，明確國家建立網路安全監測預警和資訊通報制度，建立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演練。這為建立統一高效的網路安全風險報告機制、情報共用機制、研判處置機制提供了法律依據，為深化網路安全防護體系，實現全天候全方位感知網路安全態勢提供了法律保護。[27]

二、《網絡安全法》對境外的規範

[27] 謝永江，「網絡安全法全文解讀」（2017 年 6 月 27 日），2018 年 5 月 20 日瀏覽，《天津政務網》，http://sww.tj.gov.cn/html/2017/tongzhigonggao_new_0627/43763.html。

《網絡安全法》除了規範大陸境內的個人、組織、網路運營者和關鍵資訊基礎設施的運營者，有些規定還涉及境外部分，主要涉及的問題包括要求向公安、國安機關提供技術支持和協助（第 28 條）特定公司通過國家安全審查（第 35 條），在大陸儲存使用者和經營數據（第 37 條），境外的機構、組織、個人的處罰（第 76 條）等，這將對外國企業在境內經營業務，產生廣泛影響。

（一）廣泛的適用性

《網絡安全法》對網路運營者和關鍵資訊基礎設施運營者皆施加義務。其中，網路運營者被定義為任何「網絡」的所有者或提供者，而網路在該法第 76 條（1）的定義，是指由電腦[28]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序對資訊進行收集、儲存、傳輸、交換、處理的系統。由於網路的定義相當廣泛，幾乎大多數的網路平臺，甚至任何兩臺相連接的電腦都包括在內，因此，所有的網路運營者都有可能被該條款的範圍所涵蓋。至於關鍵資訊基礎設施運營者，第 31 條明確定義包含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。

（二）檢測、認證和審查

法律對特定網路產品和服務的安全性提出了若干要求。例如，關鍵網路設備和網路安全產品需要符合大陸國家安全標準和強制性要求（第 23 條）。同時，在該類設備或產品可能在大陸適用之前，該設備和產品必須通過安全「檢測」或者獲得資質機構所頒發的「認證」。將來，大陸於 2017 年 6 月發布受到該要求限制的網路設備和產品的類型目錄，並且發布特定設備和產品必須滿足於國家標準的強制性要求。該要求有效地將公司可能使用的網路設備和服務的範圍縮小至限定範圍的預先批准技術。製作網路設備或產品的公司很有可能面臨確保其產品符合大陸尚未發布標準的挑戰，並且使用關鍵網路技術和產品的公司也將在通過安全檢查或獲得

[28] 電腦在大陸稱為電子計算機。

使用批准認證的問題上面臨類似的挑戰。不過，該法沒有明確規定認證程序的時間表，這可能會占有足夠長的時間，導致該產品在大陸的運營受到延遲。法律也沒有明確產品會在何種程度上被「檢測」，也可能涉及公司智慧財產權和商業秘密。

關鍵資訊基礎設備運營者，包括要求其在購買任何可能影響國家安全的產品或服務前進行國家安全審查（第 35 條）。該法沒有規定該國家安全審查的內容，也沒有規定可能影響國家安全的產品或服務類別。同樣存在問題的是國家安全「審查」的程度，例如是否會要求智慧財產權或商業秘密的披露。

（三）關鍵資訊的儲存

根據該法第 37 條規定，在大陸境內運營中收集和產生的個人資訊和重要數據應當在境內儲存。這要求其將個人資訊儲存在位於大陸的伺服器上。其中個人資訊包括公民和外國人的資訊。除運營者可以表明資訊出於商業原因為「確需」並且已經通過政府的「安全評估」的情況外，運營者不得將資訊發送至大陸境外。法律沒有明確「確需」，也沒有對通過「安全評估」寫明具體要求。值得注意的是，雖然原本的草案允許運營者在大陸境外「儲存」和「提供」這類資訊，最終的版本刪除了「儲存」。[29] 可見，《網絡安全法》還是禁止關鍵資訊基礎設施運營者在境外儲存任何資訊，儘管這樣的儲存是必要的，且通過安全評估。

因此，經常需要跨境傳輸資料的跨國企業會格外受到該要求的困擾，而必須將所有和大陸客戶有關資訊和交易記錄，分別儲存至大陸的伺服器，最終導致的結果是，跨國企業必須準備兩套資料庫系統，一套在大陸，另一套在其他國家。

（四）境外的機構、組織、個人的處罰

[29] 原本草案規定：「關鍵信息基礎設施的運營者應當在中華人民共和國境內儲存在運營中收集和產生的公民個人信息等重要數據；因業務需要，確需在境外儲存或者向境外的組織或者個人提供的，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從其規定。」

《網絡安全法》不只是規範境內機構，當境外的機構、組織、個人從事攻擊、侵入、干擾、破壞等危害大陸境內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；根據第 75 條規定，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。

應該注意的是，並非所有網路運營者收集的個人資訊都要儲存在大陸境內，而僅限於該法第 31 條所規範關鍵資訊基礎設施運營者在大陸境內的運營活動中所收集和產生的個人資訊。換言之，一旦落入關鍵資訊基礎設施運營者的範疇，該法將限制其將在大陸境內運營過程中收集和產生的個人資訊和業務資料向境外傳輸的行為。[30] 當前全球市場已經深度融合，「中資企業」想要走出去、「外資企業」想要走進來的大背景下，以企業為主體的業務數據的跨境流動，在現實中已經十分普遍，特別是透過網路提供資訊服務的企業而言更是如此。因此，關鍵資訊基礎設施的範圍及其資訊傳輸的限制，對部分企業的業務正常開展，可能會產生根本性影響，甚至造成實質性阻礙。

（五）與公安、國安機關的密切合作

該法第 28 條規定，網路運營者在維護國家安全或調查犯罪應當與公安機關和國家安全機關密切合作，在需要時應提供技術支援和協助。不過，該法沒有技術支援和協助類型的細節，日後大陸可能援引該條規定，要求技術公司提供與該技術相關的其他資訊，如原始程式碼等，為大陸「開後門」。不過，該法沒有技術支援和協助類型的細節，何謂國家安全？全憑大陸說了算，此舉將迫使在大陸境內的個人或企業必須與大陸密切合作，否則將無法在大陸立足或發展。

三、《網絡安全法》引發的爭議

《網絡安全法》作為「網路空間」問題的基礎性法律，旨在保護網路

[30]「網絡安全法來了！-- 企業應該知道的五件事」（2016 年 11 月 11 日），2018 年 5 月 20 日瀏覽，《搜狐網》，http://www.sohu.com/a/118703474_481465。

安全和網路用戶的個人資訊，確保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，或是不得用網路實施詐騙，傳授犯罪方法。值得注意的是，隨著該法施行之後，大陸的相關措施已經超越資訊安全保護的立法目的，而是開始進行無所不在的網路監控。

（一）網路實名制法律化

大陸對於網路實名制的討論由來已久，[31] 但透過行政命令推行網路實名制始於 2011 年北京市頒布的《北京市微博客發展管理若干規定》，提出「前臺自願，後臺實名」的管制手段，[32] 新微博用戶在註冊時 (後臺) 必須使用真實身分資訊，但用戶暱稱 (前臺) 可自願選擇，而在此期限內未進行實名認證的微博老用戶，只能瀏覽資訊，不能發言、轉發消息。隨後，總部位於北京的新浪、搜狐、網易等各大網站微博都在 2012 年 3 月 16 日開始全部實行實名制，[33] 也是採取「前臺自願，後臺實名」的方式。

根據該法第 24 條規定，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布、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分資訊。使用者不提供真實身分資訊的，網路運營者不得為其提供相關服務，換言之，網路運營者為用戶提供電話及網路等服務之前，必須要求用戶提供真實身分，才能夠提供相關服務，也就是要求網路服務落實「實名制」，[34] 這讓大陸可以控制所有網路運營者的入口，事實上也就掌握了所有網路使用者，這給予大陸合法監控網路言論的權力，只要有不符合國家安全和社會公共秩序的訊息或言論，都會被

---

[31] 朱詩慧，「淺談網絡實名制問題」，**法制博覽**（北京），第 6 期（2018 年），頁 177。

[32] 陳堅豪，「中國擬立法推行『網絡後臺實名制』」，**金融科技時代**（北京），第 1 期（2013 年），頁 14。

[33] 韓寧，「微博實名制之合法性探究 - 以言論自由為視角」，**法學**（北京），第 4 期（2012 年），頁 3-9。

[34] 聶躍宏，「網絡實名制下個人信息的法律保護問題初探」，**法制博覽**（北京），第 2 期（2018），頁 205。

強烈管制，可想而知，網路運營者都必須配合把訊息或言論刪除及封鎖。

（二）保護關鍵訊息基礎設施

關鍵資訊基礎設施保護制度是《網絡安全法》一項重要制度，該法第 31 條規定，針對公共通信和資訊服務、能源、交通、水利、金融、公共服務、電子政務等被列為關鍵資訊基礎設施的產業，會特別實行重點保護，原因在於其一旦遭到破壞、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。

另外，該法第 37 條規定，保護措施為儲存在境內和限制跨境傳輸。要求關鍵資訊基礎設施的運營者在境內運營中收集和產生的個人數據和重要數據應當在境內儲存。當某企業被認定為關鍵資訊基礎設施的運營者，政府會將其納入專門的保護體系，這樣可以在一定程度上避免將大量的個人資訊和國家的重要資訊傳輸到境外。但是此舉並不能完全杜絕像阿里巴巴這樣掌握大量個人基礎資訊的企業，將資訊轉賣至境內具有外資背景的企業。因此，這些企業不需要將資訊轉移至境外，只要在境內完成分析，就能在不違反《網絡安全法》的情況下，達到危害國家安全的目的。

不過，此舉被認為會讓外國企業（特別是科技企業）的運營成本變高，甚至無法進入大陸市場。特別是目前劃進去的行業和領域，涵蓋的範圍很廣，有些甚至是極隱私的領域，例如金融業。另外，什麼是關鍵資訊基礎設施、關鍵資訊基礎設施認定的標準和程序等，目前認定尚不一致，需要配套法規予以明確。另外，如何進行年度檢測評估、網路運營者和管理部門如何統一發布網路安全預警資訊、如何扶持網路安全自主智慧財產權等，也有待於配套法規予以明確。[35]

（三）重大突發事件限制通訊

根據該法第 58 條規定，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後，可以在特定區域對

[35] 全國人大常委會網絡安全法執法檢查報告建議，「加快個人信息保護法立法進程」，法制日報（北京），2017 年 12 月 24 日。

網路通信採取限制等臨時措施。但是，只要國務院認定是國家安全事件或違反社會公共秩序，就有權可以限制網路通訊，也就是斷網及封殺消息，證明大陸管制網路的決心，並透過法律把這些管制手段確立下來。由於該規定擴及對外國企業的管制，引起外國企業極大的不安，認為《網絡安全法》有許多條款是為了形成貿易壁壘，削弱外國企業在大陸市場競爭力，對網路安全其實並沒有實質幫助。[36]

然而，該規定很可能用會用來作為箝制言論自由及侵犯人權的手段，例如防堵「茉莉花革命」、「太陽花學運」、「雨傘革命」以及「鎮壓新疆獨立運動」等境內外的社會運動，經由網路快速傳播的特性散布對大陸不利的消息，此舉將迫使在大陸境內的眾多網路公司，必須配合大陸進行言論管制。另外，從 2016 年以來，大陸對於網路監控日趨嚴密，且動作相當頻繁，如掌管所有網路相關監管事項的「國家互聯網信息辦公室」，不但管制網路新聞頻道，更在 2016 年 11 月 4 日發布《互聯網直播服務管理規定》，直播網路新聞必須先審後發，[37] 還規定直播頻道必須設立總編輯。[38]

（四）言論自由的不當監控

在言論自由管制方面，該法第 47 條規定，網路運營者應當加強對用戶發布的資訊的管理，發現法律、行政命令禁止發布或者傳輸的資訊，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。網路安全的保護和管理，必須充分保障人權和言論自由，充分尊重人民的知情權、參與權、表達權和監督權。同時，任何人、任何機構都應該對自己在網上的言行負責，個人的自由不應以損害他人的自由和社會公共利益為代價。因此，這條規定有兩點理解：

---

[36] 郭芝榕，「中國強力通過網絡安全法，背後沒說的那些事」（2016 年 11 月 8 日），2018 年 5 月 20 日瀏覽，《數位時代》，https://www.bnext.com.tw/article/41730/china-approves-law-to-tighten-control-on-internet-use。

[37]「網絡直播不能任性 -- 聚焦《互聯網直播服務管理規定》」（2016 年 11 月 4 日），2018 年 5 月 20 日瀏覽，《新華社》，http://www.xinhuanet.com/politics/2016-11/04/c_1119853573.htm。

[38] 第 7 條：「互聯網直播服務提供者應當落實主體責任，配備與服務規模相適應的專業人員，健全信息審核、信息安全管理、值班巡查、應急處置、技術保護等制度。提供互聯網新聞信息直播服務的，應當設立總編輯。」

一是針對的是用戶公開發布的資訊，而不是個人通信資訊，不會損害個人隱私。二是要求停止是違法資訊，不存在妨礙言論自由問題。

（五）《網絡安全法》、《國家安全法》和《反恐怖主義法》的競合

從網路時代的誕生開始，就與網路空間結下了不解之緣，隨著網路持續深入人民生活的方方面面，同時也產生了國家安全的新問題。所謂國家安全，不僅僅侷限於以保護現實世界中有形的、以領土為代表的主權核心價值的安全，而且還要求能夠對關鍵資訊基礎設施、跨境數據流動、網路空間的各種行為等支撐社會生活正常運作保持必要的控制，確保國家的核心利益處於可持續發展和免受威脅的狀態。

網路空間安全 3 部法律，除《網絡安全法》之外，還有《國家安全法》和《反恐怖主義法》也有相關規定。《國家安全法》第 25 條關於加強網路管理，防範、制止和依法懲治網路攻擊、網路入侵、網路竊密、散布違法有害資訊等網路違法犯罪行為的規定。《反恐怖主義法》第 18 條和第 19 條規定如何規範網路空間中恐怖主義相關內容的傳輸、保存、刪除和報告的義務。第 21 條規定關於網路運營者、服務提供者在反恐中承擔的義務，如對客戶身分進行查驗。對身分不明或者拒絕身分查驗的，不得提供服務。

自 18 大以來，大陸加速啟動構建網路安全國家戰略能力體系的步伐，從頂層設計入手，迅速推進了相關的各項工作。其中最為重要的舉措之一，就是組建了中共中央網絡安全和信息化領導小組（2018 年 3 月改稱委員會）辦公室，而《網絡安全法》相關條文中提到的「網信部門」，就是指這一辦公室為代表的相關部門。之所以是大陸網路安全國家戰略能力體系最為重要的舉措，因為透過組建這個辦公室，整合原先分散於不同部門（如網信、工信、公安和國安）的職權，進一步建設完善大陸網路安全戰略能力體系，以因應網路時代的全新挑戰，從而實現在網路空間領域的資源整合與快速反應，而《網絡安全法》、《國家安全法》以及《反恐怖主義法》的相關規定，都將是關鍵而重要的步驟。

伍、結論

從《網絡安全法》的立法背景可知，大陸為解決當前網路空間存在的安全問題，應對網路安全所面臨的嚴峻形勢，保護人民的合法權益不受侵害，促使網路安全的法制化建設，淨化網路空間環境，保護個人資訊安全。雖然大陸官方媒體不斷強調，《網絡安全法》可以充分保障個人資訊，嚇阻電信網路詐騙和犯罪；不過，外國媒體分析認為，該法的立法目的就是透過網路監控通信來箝制言論自由，剝奪人民的知情權，侵犯人民的基本權利，例如：禁止網路用戶發表包括所謂的損害國家聲譽、擾亂經濟或社會秩序、或意圖推翻社會主義制度在內的資訊。另外，對網路資訊內容實行嚴格的審查，一些人權組織則擔憂，可能進一步限制人民的網路自由，並可以用來針對異議人士和疆獨、藏獨、港獨和臺獨分子。由於《網絡安全法》的許多規定都涉及外國企業，不但增加外國企業在大陸的經營成本，甚至從外國企業獲得營業秘密或智慧財產權，導致「中」方企業在不公平的情勢中，獲得競爭優勢。

另外，《網絡安全法》在制定之初，就已經引起了國際社會的高度矚目與擔憂，紛紛呼籲大陸在推動網路法制化措施的同時，也應該尊重人民表達意見和言論自由，以及使用網路的權益。如今，《網絡安全法》已經正式施行，相關網路安全措施陸續開展並不斷深入，引發在大陸境內的外國企業和個人的擔憂，尤其是兩岸人民交流往來日趨頻繁，已經呈現出不可逆轉的態勢，面對此一形勢，行政院大陸委員會副主委邱垂正公開呼籲，臺商赴陸投資時，應審慎評估可能的風險、資訊安全和商業機密保護等問題，以免觸法。[39] 因此，準備赴大陸的國人除了注意相關規定外，臺商赴陸投資時，應注意及審慎評估可能的投資風險、資訊安全，以及商業機密保護等問題。

[39]「中國網安法生效 陸委會籲臺商注意」（2017 年 6 月 2 日），《自由時報電子報》，https://news.ltn.com.tw/news/politics/paper/1107127。