中國行政評論 第 25 卷第 1 期
The Chinese Public Administration
Vol25 No.1 March.2019,pp.91~114
DOI:10.6635/cpar.201903_25(1).0004

中國大陸《網路安全法》規範與問題研究

陳銘聰*

摘要

《網路安全法》是中國大陸第一部全面規範網路安全方面的基礎性法律，本法除了對中國大陸境內的個人、組織、網路運營者、關鍵資訊基礎設施的運營者進行規範和處罰之外，不少規定還針對中國境外機構、組織和個人。網路安全和資訊化發展是網路空間存在的兩大基本命題，《網路安全法》正式對網路空間管理作出相關規定，以實現安全和發展要同步推進的總體要求。隨著網路時代的到臨，人民日常生活皆與網路脫不了關係，電信網路詐騙和侵犯個人資訊成為網路時代的新興犯罪，網路安全法正式在此背景下應運而生，不過，中國當局是否會以網路安全保護之名，進行網路監控之實，箝制言論自由，侵犯基本人權，產生寒蟬效應，值得關注。由於兩岸人民交流往來日趨頻繁，中國當局在採取相關措施時，應該考慮對雙方往來可能產生的負面影響。

關鍵字：網路安全法；資訊安全；個人資訊；網路空間；網路實名制

---

*國立臺灣大學國家發展研究所碩士生

收稿日期：2018 年 9 月 10 日　接受刊登日期：2019 年 4 月 28 日

壹、前言

2016 年 11 月 7 日，中國大陸第十二屆全國人民代表大會常務委員會第二十四次會議仍然依據原本草案內容通過《中華人民共和國網路安全法》[1]（下簡《網路安全法》或本法），並自 2017 年 6 月 1 日起開始施行。該法最重大意義在於中國當局[2]在網路安全工作終於有了基礎性的法律框架，代表中國當局在維護網路安全的道路上，堅持要走自己的路。該法具有兩個特點，一是全面性。該法全面和系統地確立了各個主體包括國家有關主管部門、網路運營者、網路使用者在網路安全保護方面的義務和責任。另外，也確立網路運行安全、網路資訊安全、保障網路的設備設施安全，以及等各方面的基本制度。二是涉外性。許多規定涉及境外部分，包括要求向中國當局提供技術支援和協助（第 28 條），特定產品和服務必須通過國家安全審查（第 35 條），在中國儲存使用者和經營資料（第 37 條），境外的機構、組織、個人的處罰（第 76 條）等。本法是中國大陸第一部全面規範網路空間安全方面問題的基礎性法律，賦予國家對網路管制手段的合法地位，充分發揮法律的強制性規範作用。本法代表中國當局在維護網路安全的道路上，堅持要走自己的路。

貳、《網路安全法》的立法背景

當前，網路世界中存在著一些違法資訊，嚴重侵害人民、法人和其它組織的合法權益，尤其是中國大陸每年的「雙十一購物狂歡節」[3]，更是網路詐騙的高峰期，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層出不窮，令不少人受騙上當。在 2016 所舉辦的中國互聯網大會上，「中國互聯網協會」與「12321 網路不良與垃圾資訊舉報受理中心」聯合發布的《中國網民權益保護調查報告》(2016)內容顯示，從 2015 年下半年到 2016 上半年的一年間，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高達 915 億元人民幣(以下皆同)。2016 年上半年以來，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個人資訊洩露帶來的不良影響。2017 年一整年，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，同比增加 9 元，因此而消耗的時間人均達 3.6 小時，其中，有 9%的網民經濟損失在 1000 元以上（中國新聞網，2016）。然而，在網路詐騙的案件中，受

[1] 網路在中國大陸稱為網絡，而網際網路（Internet）在中國大陸則稱為互聯網。

[2] 本文在探討國家層面議題時用中國大陸一詞，在探討政府層面或中國執政者議題時用中國當局一詞，以茲區別，合先敘明。

[3]「雙十一購物狂歡節」，是中國大陸每年 11 月 11 日的網路促銷日，源於淘寶商城（天貓）2009 年 11 月 11 日舉辦的網路促銷活動，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經成為中國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。

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(黃建軍,2015)。這促使中國當局加快網路安全的法制化建設,保護個人資訊安全,提高網路安全意識,淨化網路空間環境(網易,2016)。

2015 年 6 月,第十二屆全國人民代表大會常務委員會第十五次會議對《網路安全法》草案進行首次審議,並向全社會徵求意見。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,會議以 154 票贊成、1 票棄權,通過本法,並自 2017 年 6 月 1 日起施行。本法突出六大亮點:一是明確網路空間主權的原則;二是明確網路產品和服務提供者的安全義務;三是明確網路運營者的安全義務;四是完善個人資訊保護規則;五是建立關鍵資訊基礎設施安全保護制度;六是確立關鍵資訊基礎設施重要資料跨境傳輸的規則。由此可知,《網路安全法》將為網路空間管理提供法律依據(陳銘聰,2018,106)。

在《網路安全法》公布施行後,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,制定本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(中國人大網,2016)。中國將來必定是一個網路空間大國,也會是面臨網路安全威脅最嚴重的國家之一,因此迫切需要建立網路安全保護的法律制度(觀察者網,2016),本法的公布施行,這是呼應這個網路時代的要求。

參、《網路安全法》的基本內涵

一、理論基礎

網路空間已成為現代國家繼「陸、海、空、太空」之後的「第五疆域」(劉彥華,2017:48-53),且與其它疆域一樣,網路空間也需要體現國家主權,保護網路空間主權也就是保護國家主權。「網路空間主權」是進入網路時代後的新生名詞,是國家主權在網路空間的自然延伸,它沿襲國家主權概念內的四項基本權力:「在對內統治中,表現為一國對網路空間的最高管轄權;在對外權能中,表現為一國在網路空間的獨立權、平等權和自衛權。」網路空間管轄權,是一國對本國網路空間的最高管理權,包括對本國資訊系統的管理和對國土範圍內一切網路活動的管理,這種管轄由國家的物理空間逐漸延伸至網路空間,保障國家在網路空間的利益和公民在網路空間的合法權益。網路空間獨立權,即一國在網路空間中不受制於任何國家和組織,對其網路系統、資源以及應用技術等獨立自主地進行管理和控制的權力。獨立權的行使以不侵犯他國主權為前提,因此,現代各國的主權往往會體現出一定的相對性,這是各國對主權限制的自願接受,並非是對獨立權的放棄(李營輝,2016:10-11),這個規則同樣適用於網路空間,即網路空間獨立權的行使不應侵犯到他國的網路空間主權。網路空間平等權,即指各國在網路空間主權平等,對於網路空間的管理,主權國應在平等和互相尊重的基礎上進行協商,基於平等方式實現互聯互通,而不能因擁有網路資源的不平等造成主權國家網路空間地位的不平等,或由某一個國家憑藉技術優勢來控制網路空間。網路空間自衛權,是一國針對域外網路攻擊進行防衛的權力,主權國家可採

取必要的措施、手段保護本國網路以及在其中運行的軟體和硬體不受攻擊。

二、法律體系

自網路誕生開始，就與國家安全結下了不解之緣，隨著網路持續滲入生活的方方面面，同時也開啟國家安全的新領域。因此，國家安全不僅局限於保障現實世界中有形的和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、網路空間等支撐社會生活正常運作的各種行為，保持必要的控制，確保國家的核心利益處於免受威脅和可持續發展的狀態。關於網路安全管制體系，除《網路安全法》之外，還有《國家安全法》和《反恐怖主義法》的相關規定 。

這三部法律分別從國家層面（國家安全法）、社會層面（反恐怖主義法）和個人層面（網路安全法）共同落實國家總體安全的重要舉措。對此，這三部法律對網路安全保護提出「自主可控」的核心要求（倪光南，2018：6-7），即網路必須能夠自主可控，產品和服務就不存在惡意後門，並可以不斷改進或修補漏洞，資訊安全就獲得保護；反之，不能自主可控，就會受制於他國，產品和服務容易存在惡意後門，並難以改進或修補漏洞，資訊安全就難以獲得保護。《網路安全法》所闡述的網路安全風險管理範圍，就是在傳統網路資訊系統的基礎上，進一步擴展到個人資訊保護、國家關鍵資訊基礎設施等方面，同時提出「安全審查」等國家層面的治理手段。

例如《國家安全法》第 25 條規定，國家建設網路與資訊安全保障體系，提升網路和資訊安全保護能力，加強網路和資訊技術的創新研究和開發應用，實現網路和資訊核心技術、關鍵基礎設施和重要領域資訊系統及資料的安全可控；加強網路管理，防範和依法懲治網路攻擊、網路入侵、網路竊密、散佈違法有害資訊等網路違法犯罪行為，維護國家網路空間主權、安全和發展利益。《反恐怖主義法》第 18 條和第 19 條明確規定如何在網路空間防範恐怖主義相關內容的傳輸，第 21 條規定網路服務供應商在反恐中所承擔的義務。

自中共十八大以來，中國當局加速啟動構建網路安全國家戰略能力體系的步伐，並從頂層設計入手，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「中央網路安全和資訊化領導小組及其辦公室」（陳銘聰，2018：62），而《網路安全法》相關條文中的「網信部門」指的就是這一辦公室為代表的相關部門，之所以是最為重要的舉措，是因為透過組建這個辦公室，整合原先分散與不同部委（例如網信、工信、公安、國安）等相關部門的職權，進一步建設完善國家網路安全管制體系，以適應網路時代的全新挑戰，從而實現網路安全戰略領域的資源整合與快速反應。而三部法律的相關規定，都將是關鍵而重要的步驟。

三、三個層面

從《網路安全法》的理論基礎和法律體系的思路出發，並統整本法的相關規

範來看，可以建構出網路安全保護的三個層面：首先是最基礎的資訊安全，其次是個人資訊的保護，最終是國家層面的資訊保護。

（一）資訊安全保護

資訊對於現代人類文明發展具有特別重要的意義，資訊安全的內涵就是要保護網路資訊或資訊系統免受各種類型的威脅、干擾和破壞，換言之，資訊安全就是保護網路資訊或資訊系統免受未經授權的訪問、使用、披露、破壞、修改和銷毀等。資訊安全可以從不同層面來進行，如制度安全、技術安全、運算安全、儲存安全、傳輸安全、產品和服務安全等，任何國家、政府、企業、個人都必須重視的問題，它不僅關係到個人隱私、企業營業秘密，更直接關係到國家安全，是一個不容忽視的國家安全課題。因此，各國莫不完善與資訊安全相關的法規，尤其是隨著網路的快速發展和資訊化程度的不斷提高，網路深刻影響著政治、經濟、社會和文化等各個方面，加強管理網路上各類資訊，以及資訊安全保障的重要性日益明顯（聶證、曹燕，2018：47-48）。

資訊作為一種資源，根據「國際標準化組織」（ISO）的定義，資訊安全的涵義主要是指資訊的完整性、可用性、保密性和可靠性（張宏濤，2018：79-80），而《網路安全法》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（confidentiality）、完整性（integrity）和可用性（availability），此為網路資訊最重要的三個屬性。保密性，係指資訊不被洩露給未經授權者的特性；完整性，係指資訊在儲存或傳輸過程中保持未經授權不能改變的特性；可用性，係指資訊可被授權者訪問並使用的特性（胡潛、林鑫，2018：33-37）。

應該注意的是，除第 10 條外，第 21 條規定網路運營者（包括關鍵資訊基礎設施的運營者）的安全保護義務，明確提出防止網路資料洩露或者被竊取、篡改是安全保護的目的之一。第 27 條則是要求任何人不能提供專門用於竊取網路資料的程式和工具。第 31 條更是從資料洩露可能造成危害的角度來界定關鍵資訊基礎設施的範圍。上述相關法律規定，參見下表 1：

（表 1：資訊安全保護的相關法律規定）

第一層面	相關條文
資訊安全	第 10 條：維護網路資料的完整性、保密性和可用性。
	第 21 條：國家實行網路安全等級保護制度。防止網路資料洩露或者被竊取、篡改。
	第 27 條：不得提供專門用於竊取網路資料等危害網路安全活動的

	程式、工具。
	第 31 條：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。

（資料來源：作者自行整理）

（二）個人資訊保護

本法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，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。

為因應電腦科技發展和網路技術運用對個人資訊帶來各種風險，「個人資訊自決權理論」由此產生，這是一種管理資訊擴散和揭露的機制。該理論認為，為保護人格的自由發展，個人應當能自由地決定以何種方式實現人格的發展；而人格的發展，主要是透過人與人的交往過程中實現，因此個人需要掌控對外自我披露或表現的程度，以便合理維持自身與他人之間的人際關係，所以個人應當能自由地、自主地決定如何使用個人資訊（謝遠揚，2015：102-103）。也就是說，個人資訊保護賦予個人有權控制個人資訊用於何種用途，面向何種對象公開，透過何種途徑擴散和披露，亦即個人有權依照法律控制個人資訊，並決定是否被收集或利用（王利明，2013：64）。另外，個人資訊保護主要對個人資訊的自主使用，要求他人不得以違反本人意願的方式對個人資訊進行處理，因為若非經本人同意而進行個人資訊處理，可能會超出本人預期的結果，並對人格發展造成不可預料的影響，使得人格發展結果偏離原本的預期。因此，第一層面的資訊安全和第二層面的個人資訊保護是息息相關。如果用公式來表達兩者之間的關係，結果如下：

個人資訊保護 = 資訊安全 + 個人資訊自決權 + 資訊控制者滿足個人資訊自決權利的義務。

應該注意的是，《網路安全法》不僅繼受現有法律關於個人資訊保護的主要條款內容，而且根據網路時代特徵、發展需求和保護理念，創造性地增加了部分規定，例如，第 40 條增加健全用戶資訊保護制度；第 41 條增加最少夠用原則；第 42 條增設個人資訊共用的條件；第 43 條增加個人在一定情形下刪除、更正其個人資料的權利；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。由此可見，這五個條文除了注重保障個人對自己資訊的自主權和支配權之外，也與歐美各國關於個人資訊保護方面相接軌。相關法律規定，參見下表 2：

（表 2：個人資訊保護的相關法律規定）

第二層面	相關條文

個人資訊保護	第 40 條：網路運營者應當對其收集的用戶資訊嚴格保密，並建立健全用戶資訊保護制度。
	第 41 條：網路運營者不得收集與其提供的服務無關的個人資訊，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 42 條：網路運營者不得洩露、篡改、毀損其收集的個人資訊；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。
	第 43 條：個人發現網路運營者違反法律，有權要求網路運營者刪除其個人資訊，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 44 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。

（資料來源：作者自行整理）

由此可見，《網路安全法》針對個人資訊保護，提出許多具體的保護措施，除了彌補過去在個人資訊保護立法的不足，並將其納入網路運營者實施網路安全風險管理的必要內容。

（三）國家層面的資訊保護

《網路安全法》關於國家層面的資訊保護[4]，除了資訊安全之外，就是重要資訊的控制，而本法中重要資訊，係指「敏感資訊」，包括：身分證號碼、收入情況、住址、手機號碼、電子郵箱和個人生物識別資訊等個人依法享有的所有資訊。當敏感資訊遭惡意使用（即被不當使用或未經授權就被人接觸或修改），將會不利於國家利益。因此，第一層面的資訊安全和國家層面的資訊保護之間的關係：

國家層面的資訊保護 = 資訊安全 + 重要資訊的控制 + 防止敏感資訊遭惡意使用造成國家安全的威脅。

以人口基礎資訊為例，對一個國家來說，國家人口基礎資訊庫原則上是作為「重要資訊」來保護和「敏感資訊」來管理，一旦洩露將會對國家安全造成嚴重危害。根據阿里巴巴網路技術有限公司（以下簡稱阿里巴巴）於 2016 年 11 月 2 日公布的 2016 年 9 月底的業績顯示，其所經營的「淘寶中國」，其活躍買家高達 4.39 億戶，而根據淘寶的交易規範，淘寶買家至少需要提交以下個人資訊：姓

[4] 所謂國家層面的資訊保護，所保護的仍是個人資訊，只是其具有敏感性，因此必須由國家層面的思維去保護，《網路安全法》第 78 條規定，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。

名、性別、出生年月日、戶籍地址、身分證號碼、護照姓名、護照號碼、電話號碼、電子郵箱等（淘寶網，2018）。因此，阿里巴巴至少掌握 4 億中國人民的個人基礎資訊，再借助於買賣雙方的支付和收貨等情況，其掌握的個人基礎資訊的「真實性」並不輸給國家人口基礎資訊庫，另外，騰訊、百度、京東、順豐等私營企業皆擁有海量的客戶訂單資訊，這些個人資訊或客戶訂單資訊已經不能當作「基礎資訊」來看待，因為這些私營企業匯集如此巨量的個人基礎資訊，其規模和精密程度甚至可以比擬公安機關的「國家人口基礎資訊庫」（趙飛、伍曉玲、楊龍頻、孟群，2014：357-361），就網路安全保護的層面而言，顯然已經超過個人資訊保護，尤其是網路安全對國家發展和治理等方面越來越重要，再加上大數據的發展，就屬於國家層面的「重要資訊」，若是這些基礎資訊被有心人士利用，就有國家安全危害之虞，此時必須以國家手段來加以保護。

本法在國家層面的資訊保護，相比前面兩個層面，規定比較簡單，例如，重要資訊應當儲存在中國大陸境內（第 37 條），要求加強資訊安全的收集、分析和通報工作（第 51 條），以及要求及時報送安全資訊（第 52 條）。相關法律規定的內容，參見下表 3：

（表 3：國家層面的資訊保護的相關法律規定）

第三層面	相關條文
國家層面的資訊保護	第 37 條：關鍵資訊基礎設施的運營者在中國大陸境內運營中收集和產生的個人資訊和重要資訊應當在境內儲存。
	第 51 條：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。
	第 52 條：負責關鍵資訊基礎設施安全保護工作的部門，應當按照規定報送網路安全監測預警資訊。

（資料來源：作者自行整理）

應該注意的是，第 37 條要求關鍵資訊基礎設施的運營者在中國大陸境內運營中收集和產生的資訊應當儲存在中國境內，雖然避免了對大量的個人資訊和對國家的重要資訊流轉到境外，但是並不能完全杜絕像阿里巴巴、百度、京東和順豐這樣掌握大量「基礎資訊」的企業，將資訊移轉至中國大陸境內具有外資背景的企業，換言之，這些企業無需將資料轉移至國外，只要在中國大陸境內完成分析，就能在不違反《網路安全法》的情況下，達到危害國家安全的目的。

四、總體評價

綜上所述，《網路安全法》的保護主要著眼於三個方面：一是要求各種組織確實承擔起保障資訊安全的責任，即「保密性、完整性、可控性」。二是實現個人資訊自決權，並確保資訊控制者滿足個人資訊自決權利的義務。三是關鍵資訊基礎設施的運營者收集和產生的重要資訊應當儲存在中國大陸境內。

首先，沒有資訊安全，就沒有個人資訊保護，因為資訊系統被攻破，資訊遭到洩露，那要求的授權範圍和控制擴散的機制就無從談起。資訊安全的保護僅是資訊控制者和處理者的義務之一，其更重要的義務是在資訊的收集、儲存、使用、共用、公開、跨境傳輸等環節中提供服務，使得資訊主體可以行使其個人資訊的自決權。

其次，即使實現資訊安全，並非一定實現個人資訊保護，例如資訊雖然很安全地儲存在企業組織的資訊系統中，但如果沒有根據個人授權範圍來處理資訊，那就違背了個人的資訊保護。這也是為什麼在各國的個人資訊保護立法中，資訊安全部分的規定獨立成章，以《歐盟通用資料保護規則》（EU General Data Protection Regulation，GDPR）為例，立法重心在於規定個人資訊處理的基本原則、資訊主體的權利、資訊控制者和處理者的義務配置等，以充滿爭議的「被遺忘權」（范姜真媺，2016：61-106）為例，就是《歐盟通用資料保護規則》的一大創新，因為資訊所有者可以要求被遺忘，只要涉及個人資訊的部分就可以要求刪除，因此，在搜尋引擎、社群網站上輸入個人姓名，就不會連祖宗十八代都會搜尋到。可知雖然被遺忘權無關資訊安全，卻是賦予個人在特定情況下，可以刪除與其相關資訊的權利（張志偉，2017：1-68）。

最後，隨著資訊技術與經濟社會的發展，資訊已成為國家基礎性戰略資源。目前國務院及其所屬部會所公布的法規和行政命令中，冠上「戰略資源」的包括：土地、草原、稀土、石油、天然氣、糧食、水、森林、礦產和、煤炭等，而冠上「基礎性戰略資源」僅有「資訊」和「檔案」。從字面上來看，加上「基礎性」意味著更加重要，但是相對於檔案、土地、稀土、石油、森林等資源的管理體系相比，《網路安全法》對資訊的保護，尚未形成完整的體系，而僅是將構成基礎性戰略資源的資訊安全保護依附在關鍵資訊基礎設施的保護之上，資訊本身沒能構成獨立的保護對象。不過，對構成基礎性戰略資源的資訊的支配權，《網路安全法》僅要求儲存在境內，而且對於「敏感資訊」遭惡意使用時所造成對國家安全的威脅，本法完全沒有涉及。

總體來說，《網路安全法》對資訊安全和個人資訊保護給予足夠的關注，但從資訊作為國家基礎性戰略資源這個層面來看，並未在制度設計上做到通盤考慮，缺乏對保護國家基礎性戰略資源充分保護。這並非本法在制度設計上缺乏通盤考慮，而是本法立法重心在於個人資訊的保護，國家基礎性戰略資源則主要規定在《國家安全法》和其它相關法規。

肆、《網路安全法》的主要內容

《網路安全法》是中國大陸針對「網路空間」管理的基礎性法律（王靜、周向明，2003：40-42），與本法同時在 2017 年 6 月 1 日實施的還有《互聯網新聞資訊服務管理規定》、《互聯網新聞資訊服務許可管理實施細則》和《互聯網資訊內容管理行政執法程序規定》等法規，將新媒體納入了網路新聞的範圍，禁止微信公眾號和微博在未經許可的情況下，提供新聞資訊服務。以下將對本法的主要內容，進行探討：

一、網路空間主權原則

依據網路空間主權理論，各主權國家有權獨立自主地決定並採取一切防衛本國網路安全的正當措施，管理包括網路安全立法在內的一切與本國網路空間有關的事務，歸根到底，該理論為各國提供了在激烈的網路空間博弈中採取有效措施捍衛本國利益的法理依據。（陳銘聰，2018：63）。《網路安全法》第 1 條規定，開宗明義表示要維護中國的網路空間主權。網路空間主權是一國國家主權在網路空間中的自然延伸和表現。尤其是聯合國憲章確立的主權平等原則是當代國際關係的基本準則，覆蓋國與國交往各個領域，其原則和精神也應該適用於網路空間。各國自主選擇網路發展道路、網路管理模式、網際網路公共政策和平等參與國際網路空間治理的權利應當得到尊重（謝永江，2016）。

另外，2016 年 12 月 27 日，經中央網路安全和資訊化領導小組批准，國家網路資訊辦公室所發布《國家網路空間安全戰略》也指出：「網路空間主權不容侵犯，尊重各國自主選擇發展道路、網路管理模式、網路公共政策和平等參與國際網路空間治理的權利。」

網路空間主權是進入網路時代的新生名詞，是國家主權在網路空間的自然延伸，包括四項基本權力：一是網路空間「獨立權」，即一國在網路空間中不受制於任何國家和組織，對其網路系統、資源以及應用技術等獨立自主地進行管理和控制的權力。獨立權的行使以不侵犯他國主權為前提，在當代，各國的主權會體現出一定的相對性，這是各國對主權限制的自願接受，並非是對獨立權的放棄（李營輝，2016：10-11），這個規則同樣適用於網路空間，即網路空間獨立權的行使不應侵犯到他國的網路空間主權。二是網路空間「平等權」，即指各國在網路空間主權平等，對於網路空間的管理，主權國應在平等和互相尊重的基礎上進行協商，基於平等方式實現互聯互通，而不能因擁有網路資源的不平等造成主權國家網路空間地位的不平等，或由某一個國家憑藉技術優勢來控制網路空間。三是網路空間「自衛權」，即一國針對域外網路攻擊進行防衛的權力，主權國家可採取必要的措施、手段保護本國網路以及在其中運行的軟、硬體不受攻擊，同時，對外來攻擊可予以反擊。四是網路空間「管轄權」，即一國對其國內網路空間的最高管理權，包括對國內資訊系統的管理和對國土範圍內的一切網路活動（陳銘聰，2018：63）。

二、網路資訊

《網路安全法》所規範的網路資訊，包括個人資訊、重要資訊和違法資訊。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的各種資訊，包括但不限於自然人的姓名、出生日期、身分證件號碼、個人生物識別資訊、住址、電話號碼」(第 76 條)，與此前已經制定涉及個人資訊保護的法規一樣，例如《關於加強網路資訊保護的決定》、《消費者權益保護法(2013 修正）》及《電信和互聯網使用者個人資訊保護規定》等，皆強調其對個人身份的可識別性。重要資訊所保護的仍然是個人資訊，只是因為具有敏感性，必須從國家層面去保護。另外，無論是個人資訊和重要資訊，只要是關鍵資訊基礎設施的運營者在中國境內運營中收集和產生，應當在中國大陸境內儲存（第 37 條)。

另外，《網路安全法》還針對「違法資訊」特別定義，是指宣揚恐怖主義、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 12 條第 2 項)，並規定發布或者傳輸違法資訊，依照有關法律、行政命令的規定處罰（第 70 條)。

三、網路運行安全的一般規定

網路運行安全規定在《網路安全法》第三章，共十九個條文。第一節用十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 22 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份資訊（第 24 條)，網路安全的事件處理（第 25 條）等等。這些措施從短期來看，雖然在一定程度上可以應對來自國內外網路攻擊所帶來的威脅，並滿足網路安全保護的需求；但就中長期前景來看，中國大陸的戰略任務是如何在全球網路內持續開放其網路空間，並協同主要網路大國，共同預防來自網路所帶來的威脅，因此，未來中國大陸的網路空間戰略，應該是在構建新的網路安全秩序下，繼續修定相關法律，並完善相關配套措施。

《網路安全法》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(第 26 條)。其中，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《網路安全法》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充分的法律依據。不過，中國大陸境內尚存在不少機構和個人未獲得正式授權即進行安全檢測、漏洞挖掘和披露的行為，這當中不乏因操作不當或對後果估計不足，導致對被檢測方造成危害的案例。

另外，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。公安機關和國家安全機關在辦理案件過程中，

需要網路運營者提供技術支援和協助時，應當主動配合辦案，並提供相關資料和技術。任何單位、組織和個人均有法定義務配合公安機關和國家安全機關進行打擊各種犯罪活動和危害國家安全的活動（第 28 條）。

四、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在《網路安全法》第三章在第二節，專門用九個條文規範關鍵資訊基礎設施的安全，這是《網路安全法》從總體國家安全角度出發，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，極大擴展網路安全風險管理的適用範圍，其中有五個方面值得注意：

第一，保護內容。《網路安全法》進一步強化了關鍵資訊基礎設施保護的內容，明確列出關鍵資訊基礎設施的範圍(第 31 條)。因為關鍵資訊基礎設施保護的影響重大，是在網路安全等級保護基礎上，必須進一步重點保護，充分體現了安全風險管理的思想。

第二，安全保護義務。除第 21 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：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[5]；4.制定網路安全事件應急預案，並定期進行演練；5.法律、行政法規規定的其他義務(第 34 條)。

第三，安全審查。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(第 35 條)。

第四，保密協議。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 36 條)。

第五，資料儲存。本法首次在法律層級上對特定個人資訊和重要資料必須儲存在中國境內做出明確規定。這裡的「特定」並非指一般個人資訊的內容或類型，而是指向其收集主體和管道，即關鍵資訊基礎設施的運營者在中國境內運營中收集和產生的個人資訊（第 37 條）。

另外，此次列入關鍵資訊基礎設施範圍的，涵蓋涉及國家安全、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。保護關鍵資訊基礎設施的安全，從全球各國的實踐來看，這是國家網路安全戰略中最為重要和主要的內容，這與人們日常生活對網路關鍵基礎設施的強烈依賴密不可分。

[5] 「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。

五、網路資訊安全

網路資訊安全規定在《網路安全法》第四章，共十一個條文。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，本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，而且根據網路時代特徵、發展需求和保護理念，創造性地增加了部分規定，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。

網路運營者的個人資訊保護義務方面，《網路安全法》很大程度上保持與既有法律法規的一致，例如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，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（第 41 條、42 條）等等。

「電信網路詐騙」和「侵犯個人資訊」是網路時代兩大主要新型網路犯罪類型，並呈現出多發態勢，因此，《網路安全法》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（第 46 條），規定網路運營者必須自我審查網路的內容（第 47 條），並增加規定相應的法律責任（第 67 條）。

「惡意程式」（張濤，2017：25）的威脅是現代社會資訊安全的頭痛議題，隨著惡意程式的快速成長與變種，資訊安全的防範手段必須要跟上時代腳步，不過，資安人員一般都是被動地去解決惡意程式的攻擊，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。針對惡意程式所帶來的危害，《網路安全法》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、行政法規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（第 48 條）。

「網路舉報和投訴」是近年來隨著網路科技的發展而興起的，主要有兩個作用：一是透過設立網上舉報視窗，開展廣泛的舉報宣傳，提供法律諮詢；二是在網上受理民眾的舉報。因此，《網路安全法》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（第 49 條第 1 項）。

另外，針對網路監控部分，《網路安全法》第 50 條分為三個部分來規定，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，若發現法律和行政命令所禁止發布或傳輸的資訊，應當要求網路運營者立即停止傳輸，採取消除措施，並保存有關記錄；第三，對來源於中國大陸境外的上述資訊，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。

六、監測預警與應急處理

監測預警與應急處理規定在《網路安全法》第五章，共八個條文。包括：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和網路安全事件應急處置措施，以及有關法律、行政法規的規定（第 54 條至 57 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，採取限制等臨時措施（第 58 條）。

網路安全事件具有「不確定性」、「全域性」和「連鎖性」等特點，加強監測預警已經成為國際社會的普遍共識，重視應急響應更是網路安全活動的基本措施。因此，建立的監測預警與應急處置制度，對中國大陸的網路安全保護具有十分重要的意義，中國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。這些需要在立法中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。

七、法律責任

《網路安全法》第六章，共十七個條文規定法律責任。法律責任包括「個人」和「組織」，其中組織包括：網路運營者、關鍵資訊基礎設施的運營者、網路產品或者服務提供者、電子資訊發送服務提供者、運營軟體下載服務提供者、國家機關政務網路運營者、網信部門和有關部門等等。其中，個人處罰包括警告、罰款、拘留、不得從事網路安全管理和網路運營關鍵崗位的工作等等。組織處罰包括警告、罰款、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等等。

值得注意的是，《網路安全法》關於「信用檔案」（吳青麗，2002：9-10）的規定在第 71 條，其規定：「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。」信用檔案是中國企業徵信機構對企業信用資訊採集、整理、保存、加工而提供的信用記錄和信用報告，是企業整體信用狀況的真實體現，是企業獲得商業信任的綠色通行證，是大眾消費的指南和交易決策的重要參考，是安全消費、公平交易（信貸、借貸、賒銷、勞務等商務活動）的重要社會保護體系。其中最具代表性的就是「11315 全國企業徵信系統」，該

系統是具有合法主體資格的協力廠商公眾徵信平臺，這是中國大陸率先建起的大數據徵信新模式，既是政府職能部門監管資訊發布平臺又是消費者投訴維權平臺，同時還是企業信用查詢平臺。

伍、《網路安全法》的爭議問題

一、網路安全審查

《網路安全法》第 35 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。」根據中國當局官方媒體指出，當前中國大陸的網路安全問題為少數國家政府和企業利用產品的單邊壟斷和技術優勢，大規模收集敏感資訊，以及針對中國政府部門、機構、企業、大學及電信主幹網路侵入和違法監聽（南方日報，2014）。2014 年 5 月 22 日，「中國國家網路信息辦公室」（簡稱網信辦）發布公告稱，為維護國家網路安全、保障中國大陸用戶合法利益，並以此為目的，制定出「網路安全審查制度。」該審查制度是與資訊技術相關的產品和服務之審查，著重於國家安全和公共利益的重要技術產品和服務，審查重點是針對產品的安全性和可控性（張棉棉，2014）。因此，關係國家安全和公共利益系統使用的重要資訊技術產品和服務，都應該通過網路安全審查（中國廣播網，2014），而審查的具體內容，包括範圍、重點、目的和管理，相關內容如下表 4：

（表 4 ：網路安全審查具體內容）

審查範圍	關係國家安全和公共利益系統使用的重要資訊技術產品和服務
審查重點	產品的安全性和可控性
審查目的	防止產品提供者非法控制、干擾、中斷用戶系統，非法收集、儲存、處理和利用用戶有關資訊
如何管理	對不匹配安全要求的產品和服務，將不得在中國大陸境內使用

（資料來源：作者自行整理）

網路安全審查對象，根據《網路安全法》第 35 條的規定是「關鍵資訊基礎設施」，根據中國大陸當前對「關鍵資訊基礎設施」的界定，從字面意思理解，它是屬於「關係國家安 全和公共利益的系統」，再根據《網路安全法》第 31 條，關鍵資訊基礎設施應當「實行重 點保護」，可知關鍵資訊基礎設施是網路安全審查的重點領域。不過，《網路產品和服務安全審查辦法（試行）》第 2 條規定並未用「關鍵資訊基礎設施」一詞，而是用「關係國家安的網路和資訊系統採購的重要網路產品和服務」，後者的內涵其實就是關鍵資訊基礎設施（陳銘聰，2018：68）。

二、網路清理和舉報

2018 年 4 月 13 日，微博宣布為遵循《網路安全法》第 47 條的要求，將展開為期 3 個月的清理行動，對象包括涉及色情的、宣揚血腥暴力以及同性戀題材等相關漫畫、圖文、視頻和遊戲，並將違規嚴重的帳號關閉，也鼓勵民眾進行舉報。此舉引起廣大同性戀用戶及同性戀支持社群的反彈，同性戀支持者抗議微博將同性戀與涉黃及暴力畫上等號，也呼籲微博應尊重多元文化。4 月 16 日，微博清理政策急轉彎，宣布清理對象排除同性戀內容（陳曉莉，2018）。

《網路安全法》針對網路空間中容易流傳許多違法資訊，要求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的管理，發現法律所禁止發布或傳輸的資訊，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。

所謂發現法律禁止發布或者傳輸的資訊，係指第 12 條第 2 項的違法資訊，包括：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。但是，同性戀題材並不在上述違法資訊所包括的範圍之內，我們有理由相信，微博絕對不會是單一個案，未來網路運營者將不斷進行自我審查並自行擴張對違法資訊的範圍，可見《網路安全法》所引起的「寒蟬效應」。

三、資訊儲存境內和限制跨境傳輸

《網路安全法》第 37 條規定，要求關鍵資訊基礎設施的運營者在中國大陸境內運營中收集和產生的個人資訊和重要資訊應當在中國境內儲存。當某企業被認定為關鍵資訊基礎設施的運營者，政府會將其列入專門的管制對象，此舉將在一定程度上避免大量的個人資訊和國家的敏感資訊流通到境外。關鍵資訊基礎設施依本法規定，是指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、公共利益等。

2016 年 8 月 10 日，一共 46 家在華國際企業團體聯名致函中國國務院總理李克強，指出正在制定中的《網路安全法》將對資訊安全技術做出了嚴格的限制，並使得盜取資料將變得更容易，認為本法涉嫌貿易保護，將違反世界貿易組織規則，要求在符合國際貿易法規的相關規定（BBC 中文網，2016）。另外，媒體也指出中國當局試圖控制網路空間和網路技術，不能達到保證網路安全的目的，而且會形同在國家邊界設置貿易壁壘。因此，《網路安全法》有許多規定只是為了形成貿易壁壘，除了削弱外國企業在中國境內的競爭力，對網路安全並沒有實質幫助。

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中國大陸境內，僅限於關鍵資訊基礎設施的運營者在中國大陸境內運營活動中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的運營者的範疇，本法將直接影響其將在中國境內運營活動中收集和產生的個人資訊和業務資料向境外傳輸的行為。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資訊跨境流動已經十分普遍，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帶來的資料傳輸限制，將對部分企業業務的正常開展產生根本性的影響，甚至造成實質性阻礙，甚至形成貿易壁壘，限制外國企業和技術產品進入中國市場。

四、重大突發事件的限制通訊

《網路安全法》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，可以在特定區域對網路通信採取限制等臨時措施。換言之，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。過去，網路企業早已配合政府政策做過許多言論管制，但這次透過法律把這些管制手段確立下來，這證明中國當局管制網路安全的決心。

應該注意的是， 第 58 條規定很可能用來作為打壓言論自由及侵犯人權的手段，以維護政權的穩固，也就是說，該條就是為了防堵像「茉莉花革命」、「太陽花學運」、「雨傘革命」等境外社會運動，或是「天津倉庫爆炸」和「鎮壓新疆獨立運動」等境內重大社會事件，避免經由網路快速傳播對政府不利的消息。再者，掌管所有網路相關監管事項的「國家網際網路資訊辦公室」，先前不但管制網路新聞頻道，更在 2016 年 11 月 4 日發布網路直播服務管理規定，網路新聞直播必須先審後發，還要求直播頻道必須設立總編輯。根據《網路安全法》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，健全資訊審核、資訊安全管理、值班巡查、應急處置、技術保障等制度。提供互聯網新聞資訊直播服務的，應當設立總編輯。」可知，中國當局對網路的監控日趨嚴密，從 2016 年來動作頻頻，就可見端倪。

五、網路實名制的法制化

中國當局開始推行網路實名制始於北京市在 2011 年頒布的《北京市微博客發展管理若干規定》，按照「前臺自願，後臺實名」原則（周永坤，2013：1-7），微博用戶在註冊時(後臺)必須使用真實身份資訊，但用戶暱稱(前臺)可自願選擇。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，採取的都是「前臺自願，後臺實名」的方式，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。

網路實名制最主要是為了防止匿名在網上散布謠言，製造恐慌和惡意侵害他人名譽的一系列網路犯罪。網路實名制是網路空間安全管制中爭議較大的一種措

施，反對實名制者認為，若網路這種虛擬空間推動實名制將侵犯其個人隱私，並導致人們不敢在網路上輕易發言，無法勇於揭露弊案，造成寒蟬效應。贊成實名制者認為，實名制的推動具有公益性，將有效遏制網路假新聞和假消息，使得網友看到更多真實有責任的言論，有利於建立社會信用體系，提高個人資訊的準確度。世界第一個全面推行網路實名制的國家是韓國，不過已經在 2012 年宣布這一制度違憲，法院判決認為，網路實名制實行後網上的惡性言論和非法資訊並未明顯減少，卻使言論自由受到限制，個人資訊透過網路洩漏並被非法利用的風險增加，綜合權衡之下，最終認定該實名制的弊端遠勝於公益性（譚嘉玲，2016：10-14）。

《網路安全法》第 24 條規定，用戶辦理網路接入、域名註冊服務，辦理固定電話、移動電話等入網手續，或者為用戶提供資訊發布、即時通訊等服務，在與用戶簽訂協定或者確認提供服務時，應當要求用戶提供真實身份資訊。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，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份，才能夠提供相關服務，也就是要求網路服務使用者必須「實名制」，讓政府控管所有網路運營者的入口，事實上也就掌握所有網路使用者，這給予中國當局合法監管網路言論的權力，只要有不符合國家安全和社會公共秩序的訊息或言論，都會被強力管制，而網路運營者必須配合法律規定將訊息或言論刪除及封鎖。

六、兩套資訊儲存系統

《網路安全法》要求當地和外國企業通過中國當局的安全審查，並將用戶數據儲存在中國境內。第 37 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。」根據本條規定，關鍵資訊基礎設施的運營者同樣受制於資料定位的規定，這要求其將個人資訊儲存在位於中國大陸境內的伺服器上。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中國大陸境外。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，雖然之前的草案允許運營者在國外「發送」和「儲存」這類資訊，最終的版本刪除了「儲存」。因此，法律可能禁止運營者在境外儲存任何資訊，即使這樣的儲存是必要的，且通過安全評估。

因此，經常依賴於跨境資料流程的跨國企業會格外受到該要求困擾，即使在狹義的解釋下，一個跨國公司可能必須將所有和中國大陸客戶有關的資訊和交易劃分至中國大陸的伺服器上。例如該法要求外國電子商務公司和其他公司把中國客戶的數據儲存在中國大陸，這些公司就得建立兩套儲存系統，既增加成本，也增加運營的難度。事實上，跨國公司會被要求準備至少兩個全球資料系統：一個

在中國大陸境內，另一個在該公司的母國或世界其他國家。

由此可知，《網路安全法》第 37 條要求海外企業在中國蒐集的個資、數據都必須存放在境內伺服器，並經過安全檢查。隨後蘋果公司宣佈，配合《網路安全法》的要求，2018 年 1 月 11 日起，「中國 iCloud」服務將轉由合作的「雲上貴州」大資料產業發展公司負責（自由時報，2018），在 2017 年 7 月，蘋果公司與貴州省政府簽訂「iCloud 戰略合作框架協定」，授權雲上貴州做為蘋果在中國營運 iCloud 服務的唯一合作夥伴（貴州日報，2017）。自 2018 年 2 月 28 日起，iPhone 手機和 iPad 平板用戶的個人線上資訊，包含私人訊息、照片等，都將被轉移到中國大陸境內儲存，部分使用中國大陸的蘋果產品用戶已經被警告，藉設立海外 Apple ID 來迴避該法，將可能面臨喪失資料的風險。華碩雲端將於 2018 年 5 月起停止在中國大陸的服務，因為中國大陸的網路服務競爭激烈，以及新法令對外企提供的網路資訊服務功能的有限，所以決定將上海機房移出。另外，已經事先預告用戶並給予半年時間將資料備份或轉移，若消費者仍使用華碩雲端服務，可和客服聯繫更改設定，使用其他區域的機房（陳映璇，2018）。

不過，此舉被認為會讓外國企業（特別是科技企業）的營運成本變高，甚至無法進入中國大陸市場。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。

七、言論自由的侵害

2017 年 3 月 19 日，臺灣社區大學（非政府組織）工作者李明哲先生，因在網路與中國網友分享臺灣民主化等相關言論，從臺北飛往澳門後從廣東珠海市拱北口岸進入中國大陸再赴廣州，即被中國政府關押，並被迫認罪（風傳媒，2018）。臺灣人權促進會秘書長邱伊翎表示，這次針對李明哲所發起的國際連署，至今共有 136 個國內外團體連署，包括 Freedom House 自由之家、Human Rights Watch 人權觀察、FIDH 國際人權聯盟、鄭南榕基金會等團體都已經加入連署。李明哲失蹤之後，也引起許多國際媒體的報導，作為第一個臺灣 NGO 工作者被關押的個案，此案件凸顯國際社會對於中國當局任意逮捕人權工作者、打壓全球公民社會空間的嚴正抗議。李明哲在失蹤 177 天後被迫認罪，引發世界輿論譁然，因為李明哲所談的，不外乎是普世價值與政黨輪替，完全屬於言論自由的範疇。

《網路安全法》第 47 條中許多關於資訊禁止向境外傳輸、網路言論審查，且加重網路業者監控網路言論的責任，可能都會造成網路的貿易壁壘，提升營業成本，也侵害了個人隱私、言論自由與商業機密。其中該法規定，網路使用者禁止以匿名方式使用網路，且不得利用網路從事「危害國家安全、榮譽和利益」等

活動，且若發現使用者傳佈當局所禁止發布的訊息，會要求網路業者「斷網」並保存紀錄。

第 24 條規定，網路使用者應提供真實身分訊息，禁止以匿名方式使用網路。而在第 12 條及第 48 條規定，網路使用者不得利用網路從事危害國家安全、榮譽和利益等活動，或以電子或軟體發布或傳輸為當局所禁止發布的訊息。此法並對網路業者加上控管訊息與言論的責任，在第 21 條中，賦予網路營運業者安全保護的責任與義務，第 28 條則規定網路營運業者應當為公安機關、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。在言論自由管制方面，第 47 條規定網路運營者應當加強對其用戶發布的資訊的管理，發現法律、行政法規禁止發布或者傳輸的資訊的，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。而第 50 條更賦予有關部門若發現為當局所禁止發布的訊息，即得要求網路營運業者停止傳輸並保存紀錄。

雖然中國大陸官方媒體不斷報導指出，第 47 條規定可以充分保障個人資訊，並且嚇阻網路詐騙和犯罪。不過，外國媒體分析認為，美其名是維護網路安全的第三方監督機制，很可能會演變為政府專斷獨行的工具，進而遏制言論自由和通信自由，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。對網路資訊實行嚴格的審查，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，以及疆獨、藏獨、港獨和臺獨份子。

八、必須與中國當局的密切合作

《網路安全法》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大陸當局（主要是公安機關、國家安全機關）密切合作，在需要時為政府部門供技術支持和協助。不過，該法沒有技術支援和協助類型的細節，日後中國當局可以援引該條規定，要求技術公司對於其產品或和該技術相關的其他資訊（例如原始程式碼）為中國當局「開後門」。另外，網路運營者可能因此被捲入網路活動有關的爭議當中，特別是當該條和其他法律條款一併被引用的情況。例如：

1. 第 12 條禁止使用任何網路危害國家安全，破壞民族團結，煽動顛覆國家政權，煽動分裂國家，或推翻社會主義制度。

2. 第 21 條要求網路運營者監測和記錄其網路運營狀態和安全事件，並且留存網路日誌不少於六個月。

3. 第 24 條規定特定網路運營者，例如，網路和電話服務提供者，功能變數名稱註冊提供商，出版和博客平臺，和及時通訊服務商，在提供服務之前獲得其使用者的真實姓名。

4. 第 47 條和第 48 條規定網路運營者加強對其使用者發布資訊的管理，在發現使用者傳輸非法資訊時，運營者必須禁止其傳輸並刪除以防止傳播，保存有關記錄，並向有關主管部門報告。

5. 第 58 條允許政府在需要維護國家安全和社會公共秩序時，對網路通訊採取臨時措施，包括限制這些傳輸。

上述這些限制網路使用者的自主權並擴張公司監管和報告用戶義務的規定，可能會對企業的公共關係形成巨大的挑戰。還有一些企業擔心，該法中的一些規定非常模糊和寬泛，使得中國當局可以任意釋法，給企業定罪。

陸、結論

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，《網路安全法》對網路安全和資訊化發展做出了與其地位相匹配的安全保護規定，以實現「安全和發展要同步推進」的總體要求。可見，中國當局未來將加重網路監控和管制的力道，例如成立網路安全審查委員會，美其名是為維護網路安全的第三方監督機制，卻可能演變為政府專斷獨行的工具。尤其是中共十九大後，以中共總書記習近平為核心的中共領導體系，一手抓軟、另一手抓硬，無論在地緣戰略或者是網路空間上，都是不變的原則。不過，本法會造成貿易不公平的情事，也是不爭的事實，難怪會使在華外國企業間引起強烈反應，紛紛致函中國當局反對這項法律，認為法律會製造貿易壁壘，給外國企業帶來不公平待遇。另外，本法更可能有助於中國當局從外國企業竊取商業機密或智慧財產權，並將加大跨國企業的成本，使它們易遭商業間諜活動侵害，導致中國企業在不公平情勢中，獲得競爭優勢。

《網路安全法》已經引起國際社會的高度矚目與擔憂，呼籲中國當局在藉由法治化措施處理境內外網路安全挑戰的同時，也應尊重人民言論表達的自由，以及使用網路的權益。雖然中國官方媒體不斷報導指出，本法可以充分保障個人資訊，並且嚇阻網路詐騙和犯罪，不過，外國媒體分析認為，本法主要目的就是為了遏制言論自由和通信自由，剝奪人民的知情權，侵犯人民的基本權利。李明哲事件的殷鑑不遠，一些人權組織則擔憂，《網路安全法》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、港獨或臺獨份子。面對此一形勢，陸委會副主委邱垂正公開呼籲，台商赴陸投資時，應審慎評估可能的風險、資訊安全，以及商業機密保護等問題，以免觸法。隨著兩岸之間交流日益密切，臺資企業和臺灣人民在中國經商、旅遊、求學和生活日益頻繁，如何知道本法相關規定，事先規避風險，避免觸法，這都是必須學習的功課。

參考文獻

一、期刊論文

王利明，2013，〈論個人資訊權的法律保護--以個人資訊權與隱私權的界分為中心〉，《現代法學》，4：64。

王靜、周向明，2003，〈網路空間法律問題初探〉，《現代情報》，2：40-42。

倪光南，2018，〈自主可控是保障網路安全的一個必要條件〉，《資訊安全研究》，1：6-7。

吳青麗，2002，〈信用檔案與信用檔案管理〉，《中國檔案》，7：9-10。

周永坤，2013，〈網路實名制立法評析〉，《暨南學報(哲學社會科學版)》，2：1-7。

胡潛; 林鑫，2018，〈雲環境下國家學術資訊資源安全體制建設〉，《情報理論與實踐》，1：33-37。

范姜真媺，2016，〈網路時代個人資料保護之強化--被遺忘權利之主張〉，《興大法學》，19：61-106。

張志偉，2017，〈記憶或遺忘，抑或相忘於網路--從歐洲法院被遺忘權判決，檢視資訊時代下的個人資料保護〉，《政大法學評論》，148：1-68。

張濤，2017，〈網路惡意程式治理存困惑，立法亟待完善〉，通信世界》，21：25。

趙飛、伍曉玲、楊龍頻、孟群，2014，〈國家人口基礎資訊庫建設及其在人口健康資訊化中的應用思考〉，《中國衛生資訊管理雜誌》，4：357-361。

陳銘聰，2018，〈中國大陸網路安全審查制度研究〉，《前瞻科技與管理》，2:59-80。

陳銘聰，2018，〈中國大陸《網路安全法》對資訊安全問題研究〉，《展望與探索》，9：106-125。

譚嘉玲，2016，〈韓國憲法法院確認網路實名制違憲對我國的啟〉，《廣播電視大學學報(哲學社會科學版）》，2：193-196。

謝遠揚，2015，〈資訊理論視角下個人資訊的價值--兼對隱私權保護模式的檢討〉，《清華法學》，3：102-103。

劉彥華，2017，〈2017 中國平安小康指數:82.3，第五疆域急需安全屏障〉，《小康》，19：48-53。

聶證、曹燕，2018，〈大資料時代面臨的資訊安全機遇和挑戰〉，《資訊記錄材料》，2：47-48。

二、學位論文

李營輝，2016，《我國關鍵資訊基礎設施立法保護研究》，北京交通大學碩士論文。

三、報紙

網路安全審查乃順勢而為，人民日報，2014 年 5 月 23 日。

2018/1/13。中國網路監控，全民透明，**自由時報**。

四、網路資料

BBC 中文網， 46 在華外企團體呼籲北京修改網絡安全法，2016 年 8 月 12 日

http://www.bbc.com/zhongwen/trad/business/2016/08/160812_business_china_cyber_law_appeal，2018 年 8 月 28 日瀏覽。

中國新聞網，54%的網民認為個人資訊洩露嚴重，2016 年 6 月 26 日，http://www.isc.org.cn/zxzx/xhdt/listinfo-33759.html，2018 年 6 月 20 日瀏覽。

中國人大網,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，http://www.npc.gov.cn/npc/zhibo/zzzb39/2016-11/07/content_2001477.htm，2018 年 6 月 20 日瀏覽。

風傳媒，李明哲果然被認罪，在中國法庭承認觸犯顛覆國家政權罪，2017 年 9 月 11 日，http://www.storm.mg/article/329216，2018 年 6 月 20 日瀏覽。

謝永江，《網路安全法》解讀，2016 年 11 月 8 日，http://www.71.cn/2016/1108/919725.shtml，2018 年 8 月 28 日瀏覽。

黃建軍，網路詐騙的損失也可以通過民事途徑追回」，2015 年 4 月 28 日，http://www.66law.cn/goodcase/32010.aspx，2018 年 6 月 20 日瀏覽。

網易，中國首部《網路安全法》通過明確網路空間主權原則，2016 年 11 月 7 日，http://money.163.com/16/1107/20/C5A0TCFH002580S6_all.html，2018 年 6 月 20 日瀏覽。

觀察者網，中國首部《網路安全法》通過明確網路空間主權原則，2016 年 11 月 7 日，http://money.163.com/16/1107/20/C5A0TCFH002580S6_all.html，2018 年 6 月 20 日瀏覽。

張棉棉，中國將推出網路安全審查制度，外企入華門檻或提高，2014 年 5 月 22 日，http://news.163.com/14/0522/19/9SSFSPSF00014JB5.html，2018 年 6 月 20 日瀏覽。

淘寶網，法律聲明，2018 年 11 月 1 日，https://www.taobao.com/go/chn/tb-fp/2014/law.php?spm=a21bo.50862.1997523009.38.26IY3m，2018 年 6 月 20 日瀏覽。

中國廣播網，中國將推出網路安全審查制度，外企入華門檻或提高，2014 年 5 月 22 日，http://news.163.com/14/0522/19/9SSFSPSF00014JB5.html，2018 年 6 月 20 日瀏覽。

陳映璇，碩雲端決定撤出中國，上海機房 5 月停止服務」，2018 年 2 月 8 日，https://www.bnext.com.tw/article/48129/asus-stop-asuscloud-in-china，2018 年 6 月 20 日瀏覽。

陳曉莉，微博依《網路安全法》大力整頓，掃蕩同性戀內容引發反彈，急踩煞車，2018 年 4 月 16 日，iThome，https://www.ithome.com.tw/news/122465，2018 年 6 月 20 日瀏覽。

Research on the Norms and Problems of China's Network Security Law

Ming-tsung Chen＊

Abstract

The Law on Network Security is the first basic law in China to comprehensively regulate network security. In addition to regulating and punishing individuals organizations, network operators and operators of key information infrastructure in China, many provisions are also directed at organizations, organizations and individuals in China. Network security and information development are two basic propositions in cyberspace. The cybersecurity law formally stipulates cyberspace management in order to achieve the overall requirement of synchronous advancement of security and development. With the advent of the Internet era, people's daily life is closely related to the internet. Telecommunication network fraud and infringement of personal information have become new crimes in the Internet era. Under this background, the network security law came into being formally. However, whether the Chinese Communist authorities will monitor the Internet in the name of network security protection, suppress freedom of speech, infringe basic human rights and produce cold cicada effect? Should deserve attention. Due to the increasingly frequent exchanges between the people on both sides of the Straits, the Chinese Communist authorities should take into account the possible negative impact on the exchanges between the two sides when taking relevant measures.

Key words: Network Security Law; Information Security; Personal Information; Network Space; Network Real Name System

＊Graduate Institute of National Development,National Taiwan University.

Received: Sept 10, 2018. Accepted: April 28, 2019.