

圖／東方 IC

中國大陸修訂反間諜法規 對臺商的影響

中國大陸國家安全部公布反間諜新規，稱此舉是為了應對給大陸構成嚴重威脅的滲透竊密活動。

文《游智偉》

中央警察大學公共安全學系副教授

前言

近年中共陸續修訂了不少反間諜法規，從2014年（民國103年）的《反間諜法》（以下簡稱《該法》）開始，包括2017年的《反間諜法實施細則》（以下簡稱《實施細則》）、2021年的《反間諜安全防範工作規定》（以下簡稱《規定》），這些修法過程相當程度反應了中共改革開放後對和平演變或政治安全的擔憂——也就是擔心歐美國家以「民主化」為名侵蝕或撼動中共的統治正當性，但隨著這些法律或行政命令的制訂，同時也顯著地增加了在中國大陸生活的民眾或經商的企業必須負擔的義務，同時限縮了渠等能享有的權利。

從《該法》伊始，中共便逐步將反間諜或反

情報的責任加諸於在中國大陸生活的自然人身上，而在《規定》公布之前，中共的相關法規存在兩個問題：第一，較少關注網路間諜行為，僅將重點置於境外勢力／他國對中國大陸民眾的收買或派遣赴陸工作的情報人員；然而，隨著科技的發展與派遣或收買人員的成本及風險增加，來自網路或公開訊息的情報所佔比例本已快速提升。第二，在《規定》尚未公布之前，中國大陸不少省份（例如西藏、江蘇、浙江、黑龍江與四川等）頒布類似法令，而這些法令並未允許國安部門的成員直接介入，因而這類議題多由公安部門處理。

即便《規定》在某種程度上解決了前述的兩個問題，但由於威權體制對問責制（accountability）的界定不清與規範不明，卻反可能造成國安部門的



擴權，進而導致所涉社會團體或企業遭遇更多問題，例如相關部門配合其他法令勒索企業、抑或競爭對手以此增加企業經營成本與風險。本文嘗試透過回顧相關法律的修訂過程檢視企業可能被迫增加的義務與可能面臨的困境，並提出相應建議。

增加的義務與限縮的權利

中共陸續修訂的反間諜法規帶給在中國大陸生活的民眾與在陸企業更多的義務並限縮更多的權利，特別是當中共國安部頒布《規定》後。《該法》於 2014 年重新修訂後，後續相關法規均將反間諜、維

護國家主權與領土完整的責任賦予所有民眾——也包括臺灣民眾，而這便新增了三項義務，但同時也限縮了基本權利：第一，在陸民眾有義務支持「一中原則」，特別是舊三段論的版本，也就是在陸民眾在言談中必須「『抹除』中華民國的存在」與「『否定』臺灣作為政治實體」，實際上，這也部分解釋了為何近年中國大陸網民努力舉報違反「一中原則」之個人或廠商。而對在陸臺灣民眾或企業來說，這些法規的變化限縮了渠等的言論空間，特別是在與友人互動或與大陸境外企業往來之際，反而增加了牴觸法規的風險。

第二，在陸民眾有義務即時通報可疑行為，這點在《規定》中更被強調，並提出相應的具體作法與權責分工。先從「在陸民眾有義務即時通報可疑行為」來說，中共似乎希望仿造「朝陽群眾」在 1974 年「蘇聯間諜落網記」的角色與功能，將之拓展到全境，在反間諜與反情報業務的運作上打造「公私協力」的實踐。然而，分辨他人是否有蒐集情報意圖並不容易，可能導致民眾肆意檢舉，更進一步緊縮社會氛圍與言論空間。

第三，《規定》要求團體、企業與社會組織等為反間諜活動主體，並進行日常培訓與管理，這樣的規定帶給這些團體與其成員更多的義務與工作。

《規定》將國家安全機關的職責界定為業務指導與督促檢查責任，要求行業主管部門負責監督管理，團體、企業與社會組織則有義務執行規定，並進行相關人員的安全查核、強化日常防範、出國（境）安全防範、定期教育培訓、落實技術防範措施、定期工作自查等。因而團體、企業與社會組織肩負的義務更多。

對在陸臺商的可能影響

實際上，《規定》帶給在陸臺商的影響可能甚鉅，因為《規定》更偏重對網路間諜行為的防護，因而涉及資訊關鍵基礎設施的在陸臺商可能受到相當劇烈的影響，也就是業務集中在電腦設備、積體電路、電子與通訊設備等類別的相關企業。即便《該法》、《實施細則》或《規定》均未明確定義渠等內文提出的「重點單位」為何，但從過去大陸各省相關法令來看，重點單位可能至少包括：國防科研生產單位、高等院校、科研機構與涉及國家安全的企業。而從 2014 年以來相關法規的修法與立法趨勢來看，資訊相關的產業將被加倍關注，因為網路間諜行為的防範成為這一系列修法的最新重點。

在資訊相關的產業中，關鍵資訊基礎設施供應鏈又成為中共官方關注的重點，這些產業可能包括晶片製造與設計、網路設備及營運、通訊設備及營運、電信業者等。過去浙江省政府的實踐便已略透端倪，該省於 2019 年 10 月制訂公布的《浙江省反間諜安全防範辦法》便特別著重規範涉及國家安全的高新技術企業和境外投資企業、與網路安全密切相關企業。嚴格來說，網路間諜行為的防範與網路安全的防護不外乎要求團體——不論是政府部門、企業或社會團體——強化網路信箱與設備密碼防護、在單位內部透過實體隔離建構內外網、強化單位成員的安全意識等，但從《規定》本身與過去類似之地方政府頒布的法規內容來看，吾人宜更謹慎看待此一趨勢會否遭到曲解或無限上綱。

平心而論，政府設立反間諜法規一事舉世皆然，但由於這類行為的舉證困難，且很難一致性地平衡國家安全與個人安全的衝突，因而多數國家均相當嚴謹地定義這類法規所涉行為、負責單位與舉證責任。然而，清楚定義法律條文內容與釐清所涉



圖／歐新社

今年3月，中國大陸軍方指控特斯拉電動車搭載的攝影鏡頭，可能存在國安疑慮，因此禁止特斯拉接近部分軍事設施。

單位職責卻可能是整個中共政治體制中最弱一環，此係威權政體對問責制的定義不清與接受度不高所致。正因如此，中共自2014年以來修訂或制訂的反間諜法規，卻可能進一步造成國安部門的擴權與在陸企業（特別是臺商與外企）的困擾。

第一種可能產生的困擾為相關單位以此影響或騷擾廠商，要求廠商配合相關法律與國家安全政策。近年中共修訂不少與網路安全或關鍵資訊基礎設施相關的法律，包括《網路安全法》、《網路安全審查辦法》（2020）、《外商投資安全審查辦法》（2020）、《阻斷外國法律與措施不當域外適用辦法》（2021）與《數據安全法》（2021），這些法令均允許中共國家安全機關介入或主導執法過程，而這些法令與《該法》、《實施細則》或《規定》的混合搭配將相應提升中共國安部門對企業的影響力，要求渠等在經營方向或產品製程上配合特定政策，例如分享技術、或將資料庫建置在大陸境內等。

第二種可能產生的困擾為競爭對手以此展開騷擾。經濟起飛、海歸人才的增加與基本工資的提升本已增加企業在大陸的經營困難，而《該法》、《實施細則》或《規定》均未明確界定舉報責任與查緝標準，因而競爭對手（特別是本地陸企）很可能以這些規定逕行舉報造成企業的經營困擾與可

能的營業損失，因為《規定》允許中共國安人員在取得市國安單位負責人批准與具有相關法律文書後，在無須揭露舉報人資訊的情況下，逕行前往企業進行反間諜安全防範檢查。

結論與建議

綜言之，中共修訂反間諜法規以強化國家對社會的控制能力已屬既定趨勢。雖然中共制訂或修正反間諜法規並不是特例，站在國家安全的角度也屬合理，但問題在於威權體制對問責制的界定不清，賦予政府單位更多權力的同時，卻未相應提升對這些單位的獨立監督，因而容易造成相關單位（特別是地方單位）的濫權。

而近年中共對網路安全的重視與美中貿易戰下，美國對中國大陸高科技企業的箝制也迫使中共更重視涉及關鍵資訊基礎設施供應鏈之廠商，而這些法律會否成為中共相關部門要求廠商必須配合政策的工具實有疑慮。在維持在陸營運的前提下，未雨綢繆地防範這類議題或可能風險便是大陸臺商必須留意之處，大陸臺商也許可考慮儘速強化相關議題的法律顧問與服務，釐清這些法律可能的影響範圍與種類。