Luật an ninh mạng – Cán cân... cong lý

Hoàng Xuân Phú

Vâng, không phải công lý, mà quả là **cong lý**. Bởi ở xứ luật pháp đóng vai trò tượng trưng, nặng về chức năng trang trí, thì cán cân hay cong theo cái lý của đấng cầm cân. Đặc biệt, trong trường hợp của Luật an ninh mạng Việt Nam, thì chẳng phải đợi đến lúc kẻ cầm cân bẻ cán, mà nó đã bị cong từ khi chế tác. Để đẻ ra nó, đấng sinh thành đã vận dụng cả phép thần thông... lươn lẹo, nhằm thôi miên hơn mấy trăm vị được phép tham gia bấm nút, đồng thời ru ngủ cả bao triệu tâm hồn cả tin.

Để làm rõ một số nét của cái công nghệ thôi miên - ru ngủ đã được vận dụng, bài viết này trình bày mấy nội dung sau đây:

- Phần I bàn về ba khái niệm *"an toàn mạng"*, *"an ninh mạng"* và *"cybersecurity"*.
- Phần II bình luận về sự cần thiết ban hành Luật an ninh mạng.
- Phần III khảo sát mấy trường hợp được cho là Luật an ninh mạng điển hình.
- Phần IV phân tích cái được coi là Luật an minh mạng của Trung Quốc.
- Phần V tìm hiểu chân tướng của thông tin *"138 quốc gia đã ban hành Luật an ninh mạng"*.
- Phần VI là mấy lời nhắn nhủ.

Cuối cùng là phụ lục về mấy luật liên quan của Nhật Bản, Cộng hòa Séc, Hàn Quốc, Mỹ và Đức.

Bài này chỉ khảo sát cái *"cong lý"* đã được dùng để mê hoặc mọi người về tính bức thiết của Luật an ninh mạng. Còn nguy cơ *"cong lý"* trong quá trình thực thi Luật an ninh mạng sẽ được xem xét trong bài *"**Càng an ninh mạng dân càng bất an**"*.

I. An toàn mạng - An ninh mạng - Cybersecurity

Trước hết cần phải làm rõ, ba khái niệm đó có nghĩa là gì?

Theo Từ điển tiếng Việt của Viện Ngôn ngữ học do Hoàng Phê chủ biên, *"an toàn"* là tính từ, hoặc động từ, hay động ngữ. Khi là tính từ, *"an toàn"* có nghĩa là *"yên ổn hẳn, tránh được tai nạn, tránh được thiệt hại"*. Khi là động ngữ, *"an toàn"* có nghĩa là *"làm cho an toàn, bảo đảm sự an toàn"*. Vì vậy, *"an toàn mạng"* có nghĩa là *"làm cho mạng an toàn"*, hay *"bảo đảm sự an toàn của mạng"*. *"An toàn thông tin mạng"* cũng có ý nghĩa tương tự như *"an toàn mạng"*, vì thông tin mạng an toàn khi và chỉ khi mạng an toàn. Do đó, "***Luật an toàn mạng***" hay *"**Luật an toàn thông tin mạng**"* là **luật về biện pháp bảo đảm an toàn mạng** hay **an toàn thông tin mạng**.

Cũng theo Từ điển tiếng Việt của Viện Ngôn ngữ, *"an ninh"* là tính từ, hoặc danh từ, có nghĩa là *"yên ổn về mặt chính trị, về trật tự xã hội"*.

Theo giải thích từ ngữ tại Điều 3 Luật an toàn thông tin mạng của Việt Nam, *"mạng là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính"*.

Như vậy, khái niệm *"mạng"* chỉ thể hiện môi trường vật chất kỹ thuật thuần túy, không mang đặc tính chính trị, xã hội, nên nó không thể *"yên ổn về mặt chính trị, về trật tự xã hội"*. Do đó, *"an ninh mạng"* không thể là *"an ninh của mạng"*, hay *"an ninh đối với mạng"*, mà là *"an ninh trên mạng"*, tức vấn đề an ninh diễn ra trên môi trường mạng. Và ***"Luật an ninh mạng"*** là **luật** bảo đảm **an ninh** chính trị, xã hội, nhưng chỉ giới hạn trong khuôn khổ những gì diễn ra **trên không gian mạng**.

Trong tiếng Anh, động từ *"secure"* có nghĩa *"bảo vệ", "bảo đảm"*... Nó có nguồn gốc từ tiếng La-tinh *"securus"*, có nghĩa là *"không phải lo lắng". "Secure"* là bảo vệ để không phải lo lắng. Danh từ tương ứng *"security"* có mấy nghĩa khác nhau. Một nghĩa là *"sự bảo đảm"*, hay *"sự an toàn"*. Một nghĩa khác là *"biện pháp an toàn"*, tức *"biện pháp bảo đảm sự an toàn"*. Trong trường hợp đặc biệt, nếu đó là *an toàn về mặt chính trị, trật tự xã hội*, thì *"security"* có nghĩa là *"an ninh"*, hay *"biện pháp an ninh"*, tức là *"biện pháp bảo vệ an ninh"*.

"Cybersecurity" (còn được viết là *"cyber security"*) có nghĩa là *"an toàn mạng"*, hoặc *"biện pháp an toàn mạng"*, hay *"biện pháp bảo đảm an toàn mạng"*. Vì với tư cách môi trường môi trường vật chất kỹ thuật thuần túy, mạng chỉ có thể an toàn, yên ổn về mặt vật chất kỹ thuật, chứ không thể an toàn, yên ổn về mặt chính trị, trật tự xã hội, nên không thể dịch *"cybersecurity"* thành *"an ninh mạng"*, hoặc *"biện pháp an ninh mạng"*.

Vì lý do trên, ***"Cybersecurity Law"*** (tức *"Cyber Security Law"*) có nghĩa là tiếng Việt là ***"Luật an toàn mạng"***, hay ***"Luật biện pháp an toàn mạng"***. **Không thể dịch nó thành *"Luật an ninh mạng"***, hay ***"Luật biện pháp an ninh mạng"***.

Thực ra, đối với Cybersecurity Law, thì Cybersecurity thường có nghĩa là **biện pháp bảo đảm an toàn** hệ thống máy tính, mạng máy tính, phần mềm và dữ liệu, khỏi bị đánh cắp và phá hoại bởi các hoạt động tấn công và xâm nhập trái phép. Cho nên, tên *"Luật biện pháp an toàn mạng"* sát nghĩa hơn. Tuy nhiên, tên *"Luật an toàn mạng"* không khiến người đọc hiểu sai tinh thần, vì muốn bảo đảm an toàn thì đương nhiên phải đề ra các biện pháp cần thiết và thích hợp.

II. Về sự cần thiết ban hành Luật an ninh mạng

Để thuyết phục dư luận, tuyên truyền viên thường xoáy vào *"nguy cơ an toàn thông tin mạng đang gia tăng nhanh chóng"*. Chẳng hạn, Thiếu tướng GS TS Nguyễn Minh Đức, Viện trưởng Viện Khoa học cảnh sát - Học viện Cảnh sát nhân dân, đã liệt kê:

> *"Trong năm 2017, các hệ thống thông tin tại Việt Nam đã phải hứng chịu khoảng 15.000 cuộc tấn công mạng, gồm khoảng 3.000 cuộc tấn công lừa đảo (Phishing), 6.500 cuộc tấn công cài phần mềm độc hại (Malware) và 4.500 cuộc tấn công thay đổi giao diện*

(Deface)… Thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam đã lên tới 12.300 tỷ đồng (540 triệu USD), vượt xa mốc 10.400 tỷ đồng của năm 2016 và đã đạt kỷ lục trong nhiều năm trở lại đây."

Nghe như vậy, hẳn nhiều người muốn giơ cả hai tay, nhiệt liệt ủng hộ việc ban hành Luật an ninh mạng. Nhưng họ nhầm lẫn ở chỗ, **đó không phải là vấn đề an ninh trên mạng, mà là vấn đề an toàn của mạng**. Và **để bảo vệ an toàn của mạng, Quốc hội khóa XIII đã ban hành Luật an toàn thông tin mạng (số 86/2015/QH13) vào năm 2015**, trong đó Điều 3 Khoản 1 viết như sau:

*"**An toàn thông tin mạng** là **sự bảo vệ thông tin, hệ thống thông tin trên mạng** tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin."*

Lập luận về sự cần thiết ban hành Luật an ninh mạng, Tờ trình số 366/TTr-CP về Dự án Luật an ninh mạng của Chính phủ gửi Quốc hội (ngày 31 tháng 8 năm 2017) đưa ra năm lý do, trong đó lý do đầu tiên là:

"1. Đáp ứng yêu cầu của công tác an ninh mạng trong bảo vệ an ninh quốc gia, bảo đảm trật tự an toàn xã hội."

Cụ thể là mười yêu cầu sau:

"Thứ nhất, phòng ngừa, đấu tranh, làm thất bại hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, chống nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, tuyên truyền phá hoại tư tưởng, phá hoại nội bộ, phá hoại khối đại đoàn kết toàn dân tộc, kích động biểu tình, phá rối an ninh trên không gian mạng của các thế lực thù địch, phản động."

"Thứ hai, phòng ngừa, ngăn chặn, ứng phó, khắc phục hậu quả của các hoạt động tấn công mạng, khủng bố mạng, phòng, chống chiến tranh mạng."

"Thứ ba, phòng ngừa, ngăn chặn, loại bỏ tác nhân tiến hành hoạt động gián điệp mạng, chiếm đoạt thông tin, tài liệu bí mật nhà nước trên không gian mạng, tình trạng đăng tải thông tin, tài liệu bí mật nhà nước trên không gian mạng."

"Thứ tư, bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia theo cấp độ và áp dụng các biện pháp cần thiết, tương xứng."

"Thứ năm, quy định và thống nhất thực hiện phòng ngừa, ứng phó nguy cơ, sự cố an ninh mạng."

"Thứ sáu, quy định về tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng."

"Thứ bảy, triển khai công tác bảo vệ an ninh mạng trong hệ thống cơ quan nhà nước từ Trung ương đến địa phương."

"Thứ tám, đặt nền móng và triển khai công tác nghiên cứu, dự báo, phát triển các giải pháp bảo đảm an ninh mạng."

"Thứ chín, thường xuyên kiểm tra, đánh giá thực trạng an ninh mạng đối với hệ thống thông tin của các bộ, ngành, địa phương."

"Thứ mười, xây dựng cơ chế chia sẻ thông tin, thông báo tình hình an ninh mạng để nâng cao nhận thức về an ninh mạng, chủ động phòng ngừa các nguy cơ an ninh mạng có thể xảy ra."

Trong mười yêu cầu trên, **chỉ có yêu cầu thứ nhất là thuộc về an ninh trên mạng, còn lại đều là yêu cầu đảm bảo an toàn của mạng.** Nhiều nội dung thuộc về Luật an toàn thông tin mạng được huy động vào Luật an ninh mạng như vậy, phải chăng nhằm che đậy ý đồ đích thực? Và ý đồ đó được bộc lộ rõ ràng ở lý do thứ năm mà Tờ trình về Dự án Luật an ninh mạng đưa ra:

"5. Bảo đảm sự phù hợp với quy định của Hiến pháp năm 2013 về quyền con người, quyền cơ bản của công dân và bảo vệ Tổ quốc

***Theo quy định tại khoản 2 Điều 14 của Hiến pháp năm 2013** thì **Quyền con người, quyền công dân chỉ có thể bị hạn chế theo quy định của luật** trong trường hợp cần thiết vì lý do quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội, đạo đức xã hội, sức khỏe của cộng đồng. Dự kiến **Luật an ninh mạng sẽ quy định các biện pháp nghiệp vụ an ninh mạng**, trong đó có một số biện pháp có khả năng **ảnh hưởng tới quyền con người, quyền và nghĩa vụ cơ bản của công dân** như giám sát an ninh mạng, hạn chế thông tin mạng… Do vậy, việc ban hành Luật an ninh mạng để bảo đảm quyền con người, quyền công dân theo quy định của Hiến pháp là cần thiết."*

Vâng, vì Điều 14 Khoản 2 của Hiến pháp năm 2013 quy định **quyền con người, quyền công dân chỉ có thể bị hạn chế theo quy định của luật**, nên họ phải **ban hành Luật an ninh mạng để có thể hạn chế một số quyền con người, quyền công dân**. Mục đích sâu xa chỉ đơn giản như vậy.

Tất nhiên, để phục vụ nhu cầu bảo vệ an ninh chính trị và trật tự xã hội trong tình hình mới, có thể phải sửa đổi và bổ sung một số quy định của Luật an toàn thông tin mạng và Bộ luật hình sự, đó là một việc hết sức thông thường trong quá trình lập pháp và hoàn thiện pháp luật. Song, nếu tiến hành sửa đổi và bổ sung Luật an toàn thông tin mạng và Bộ luật hình sự, thì Luật an ninh mạng chỉ còn lại lơ thơ mấy điều đáng kể, khiến nó trở nên ngắn tủn, và điều khoản trao cho công an quyền hạn chế quyền con người và quyền công dân trở nên quá lộ liễu. Vì vậy, đành huy động cả những nội dung thuộc Luật an toàn thông tin mạng để làm hoa lá cành xum xuê, có tác dụng ngụy trang, hạn chế tai tiếng cho Luật an ninh mạng.

Có điều, cách làm luật tùy tiện đó khiến hai luật trở nên mâu thuẫn và chống lại nhau. Ví dụ, Điều 18 Khoản 1 của Luật an toàn thông tin mạng quy định:

*"**Chủ thể thông tin cá nhân có quyền yêu cầu tổ chức, cá nhân xử lý thông tin cá nhân** cập nhật, sửa đổi, **hủy bỏ thông tin cá nhân của mình mà tổ chức, cá nhân đó đã thu thập, lưu trữ hoặc ngừng cung cấp thông tin cá nhân của mình cho bên thứ ba**."*

Nhưng Luật an ninh mạng quy định ngược lại tại Điều 26 Khoản 2:

> *"**Doanh nghiệp** trong và ngoài nước khi cung cấp dịch vụ trên mạng viễn thông, mạng Internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam **có trách nhiệm** sau đây:*
> ***a) Xác thực thông tin khi người dùng đăng ký tài khoản s**ố; bảo mật thông tin, tài khoản của người dùng; **cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi có yêu cầu bằng văn bản** để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng."*

Thử hỏi, khi chủ thể thông tin cá nhân đã thực hiện *"quyền yêu cầu"* doanh nghiệp cung cấp dịch vụ trên mạng *"hủy bỏ thông tin cá nhân của mình"* mà doanh nghiệp đó *"đã thu thập, lưu trữ"* và *"ngừng cung cấp thông tin cá nhân của mình cho bên thứ ba"* (theo quy định tại Điều 18 Khoản 1 của Luật an toàn thông tin mạng), thì làm sao doanh nghiệp có thể *"cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi có yêu cầu"* (theo quy định tại Điều 26 Khoản 2 của Luật an ninh mạng)? Vậy thì doanh nghiệp cung cấp dịch vụ trên mạng phải tuân theo Luật an toàn thông tin mạng của Quốc hội khóa XIII (dưới sự lãnh đạo của Chủ tịch Nguyễn Sinh Hùng và Phó Chủ tịch Nguyễn Thị Kim Ngân), hay phải tuân theo Luật an ninh mạng của Quốc hội khóa XIV (dưới sự lãnh đạo của Chủ tịch Nguyễn Thị Kim Ngân)?

III. Mấy trường hợp được cho là Luật an ninh mạng điển hình

Lý do thứ sáu mà Tờ trình về Dự án Luật an ninh mạng của Chính phủ đưa ra để biện hộ cho sự cần thiết ban hành Luật an ninh mạng là:

> *"6. Bảo đảm sự phù hợp với thông lệ quốc tế*
>
> *Qua nghiên cứu cho thấy, hiện đã **có nhiều quốc gia trên thế giới ban hành các văn bản luật về an ninh mạng, điển hình** như: Nhật (Basic Act on cybersecurity - Đạo luật cơ bản về An ninh mạng), Trung Quốc (People's Republic of China Cybersecurity Law - An ninh mạng của CHND Trung Hoa), Cộng hòa Séc (Cyber Security Law of the Czech Republic - Luật an ninh mạng của Cộng hòa Séc), Hàn Quốc (National Anti - Cyberterrorism Act - Dự luật phòng chống khủng bố mạng quốc gia)… Riêng Mỹ, ngoài việc ban hành các đạo luật chung, Mỹ đã ban hành tới 06 đạo luật liên quan các vấn đề về an ninh mạng là: Đạo luật Đánh giá Lực lượng An ninh mạng, Đạo luật Tăng cường An ninh mạng năm 2014, Đạo luật Bảo vệ An ninh mạng Quốc gia 2014, Đạo luật hiện đại hóa An ninh thông tin Liên bang năm 2014, Dự luật Chia sẻ thông tin An ninh mạng năm 2015, Dự luật Tăng cường Bảo vệ An ninh mạng Quốc gia năm 2015. Ngày 7/12/2015, Hội đồng và Nghị viện Châu Âu đạt được sự thống nhất về các biện pháp thúc đẩy an ninh mạng tổng thể trong Liên minh Châu Âu tại Chỉ thị An ninh thông tin và mạng (Network and Information Security) nhằm tăng cường các khả năng an ninh mạng của các quốc gia thành viên, tăng cường sự hợp tác của các quốc gia thành viên trong lĩnh*

vực an ninh mạng. ***Việc xây dựng, ban hành Luật an ninh mạng sẽ bảo đảm công tác an ninh mạng của nước ta có sự phù hợp nhất định với thông lệ quốc tế và bảo đảm các điều kiện hội nhập quốc tế về an ninh mạng.****"*

Để gia tăng hiệu quả thuyết phục, Tờ trình của Chính phủ viết thêm tên tiếng Anh của một số luật. Nhờ thế, ta có thể tìm được đúng văn bản luật tương ứng, mà không lo nhầm lẫn (do tên dịch tiếng Việt gây ra). Thông tin về mấy đạo luật của Mỹ trong Tờ trình thì lộn xộn hơn và không có tiếng Anh, nhưng tên dịch ra tiếng Việt cũng đủ để định vị các đạo luật được đề cập.

Một số điểm mấu chốt của Basic Act on Cybersecurity của Nhật Bản, Cyber Security Law của Cộng hòa Séc, National Anti-Cyberterrorism Act của Hàn Quốc và mấy đạo luật của Mỹ được trình bày tương ứng trong Phụ lục 1, Phụ lục 2, Phụ lục 3 và Phụ lục 4. Qua đó có thể thấy, **các văn bản luật ấy đều về an toàn mạng, chứ không phải về an ninh mạng**. Cybersecurity Law of the People's Republic of China cũng tương tự như vậy, và điều này sẽ được trình bày kỹ trong phần IV.

Văn bản mà Tờ trình về Dự án Luật an ninh mạng viết là *"Chỉ thị An ninh thông tin và mạng (Network and Information Security)"* của Liên minh Châu Âu chính là EU Network and Information Security Directive (NIS Directive). Nguyên văn tên tiếng Anh của nó là:

"Directive (EU) 2016/1148 of the European Parliament and of the Council
of 6 July 2016
concerning measures for a high common level of security of network and information systems across the Union"

Để có thể dịch chính xác thì phải căn cứ vào định nghĩa sau đây tại Điều 4 Khoản 2 của Chỉ thị:

*"****'Security of network and information systems'*** *means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems."*

Tức là:

*"****'Security of network and information systems'*** *có nghĩa là khả năng kháng cự của các hệ thống mạng và thông tin, với mức độ tin cậy được xác định, chống lại mọi hành vi gây tổn hại cho tính khả dụng, tính xác thực, tính đáng tin hoặc tính bảo mật của dữ liệu được lưu trữ hay truyền tải hay xử lý, hoặc của các dịch vụ liên quan được cung cấp hay có thể tiếp cận qua các hệ thống mạng và hệ thống thông tin ấy."*

Như vậy, cần dịch tên của Chỉ thị EU 2016/1148 thành

"Chỉ thị (EU) 2016/1148 của Nghị viện và Hội đồng Liên minh Châu Âu
ngày 6 tháng 7 năm 2016
về các biện pháp nhằm đạt được mức độ ***an toàn*** *cao của hệ thống mạng và thông tin trong toàn Liên minh"*

Nói gọn hơn, đó là Chỉ thị về các biện pháp bảo vệ **an toàn** hệ thống mạng và thông tin. Không thể dịch thành *"Chỉ thị **An ninh** thông tin và mạng"*, như trong Tờ trình của Chính phủ.

Tóm lại, **tất cả *"các văn bản luật về an ninh mạng... điển hình"* được trích dẫn trong Tờ trình về Dự án Luật an ninh mạng của Chính phủ gửi Quốc hội đều không phải là luật về an ninh mạng, mà về an toàn mạng.**

Tuy không được trích dẫn trong Tờ trình về Dự án Luật an ninh mạng, nhưng cái gọi là Luật an ninh mạng của Đức hay được đề cập trên đài báo Việt Nam, ví dụ như Nhân dân (31/05/2018), ANTV (23/06/2018), An ninh Thủ đô (18/06/2018), Công an Thành phố Hồ Chí Minh (04/07/2018), Quân đội nhân dân (23/06/2018)... Nội dung đăng tải thường được xào xáo từ hai nguồn thông tin sau.

Nguồn thứ nhất là bài *"Đức thông qua Luật an ninh mạng"*, được đăng trên VTV vào ngày 18/12/2014. Bài ấy viết về IT-Sicherheitsgesetz, nhưng nó thuộc loại Luật an toàn mạng, chứ hoàn toàn không phải là Luật an ninh mạng (xem Phụ lục 5).

Nguồn thứ hai là bài *"Một số điều cần biết về luật an ninh mạng ở CHLB Đức"*, được đăng đồng thời vào lúc 15 giờ 11 phút ngày 24/5/2018 (tức là 19 ngày trước khi Quốc hội biểu quyết thông qua Luật an ninh mạng vào ngày 12/6/2018) trên hệ thống trang mạng đặc nhiệm:

http://quochoi.org/mot-so-dieu-can-biet-ve-luat-an-ninh-mang-o-chlb-duc.html
http://nguyenphutrong.org/mot-so-dieu-can-biet-ve-luat-an-ninh-mang-o-chlb-duc.html
http://trandaiquang.org/mot-so-dieu-can-biet-ve-luat-an-ninh-mang-o-chlb-duc.html
http://nguyenxuanphuc.org/mot-so-dieu-can-biet-ve-luat-an-ninh-mang-o-chlb-duc.html
http://nguyenthikimngan.org/mot-so-dieu-can-biet-ve-luat-an-ninh-mang-o-chlb-duc.html
http://tranquocvuong.org/mot-so-dieu-can-biet-ve-luat-an-ninh-mang-o-chlb-duc.html
http://phamminhchinh.org/mot-so-dieu-can-biet-ve-luat-an-ninh-mang-o-chlb-duc.html
http://hoangtrunghai.org/mot-so-dieu-can-biet-ve-luat-an-ninh-mang-o-chlb-duc.html
http://dinhthehuynh.org/mot-so-dieu-can-biet-ve-luat-an-ninh-mang-o-chlb-duc.html
http://tolam.org/mot-so-dieu-can-biet-ve-luat-an-ninh-mang-o-chlb-duc.html
http://nguyenthiennhan.org/mot-so-dieu-can-biet-ve-luat-an-ninh-mang-o-chlb-duc.html
http://vovanthuong.org/mot-so-dieu-can-biet-ve-luat-an-ninh-mang-o-chlb-duc.html
http://nguyentandung.org/mot-so-dieu-can-biet-ve-luat-an-ninh-mang-o-chlb-duc.html
...

Có điều, cái mà bài *"Một số điều cần biết về luật an ninh mạng ở CHLB Đức"* gọi là *"Luật an ninh mạng ở CHLB Đức"* không phải là IT-Sicherheitsgesetz, mà là NetzDG - Netzwerkdurchsetzungsgesetz, tức Luật chấp pháp trên mạng. Và như đã chỉ ra trong bài ***"Luật an ninh mạng - Tượng đài… cô đơn"***, NetzDG cũng không phải là Luật an ninh mạng.

Ấy vậy mà Tờ trình của Chính phủ lại viết: *"Qua nghiên cứu cho thấy, hiện **đã có nhiều quốc gia trên thế giới ban hành các văn bản luật về an ninh mạng**"*. Và nhiều đến mức, *"việc xây dựng, ban*

*hành Luật an ninh mạng sẽ bảo đảm công tác an ninh mạng của nước ta có sự **phù hợp** nhất định **với thông lệ quốc tế**".*

Trớ trêu thay, trong số *"các văn bản luật về an ninh mạng... điển hình"* được chọn lọc để đưa vào Tờ trình, phải tận thu cả **ba dự luật** (tức là dự thảo luật chưa được thông qua). Đó là Dự luật phòng chống khủng bố mạng quốc gia của Hàn Quốc, Dự luật Chia sẻ thông tin An ninh mạng năm 2015 và Dự luật Tăng cường Bảo vệ An ninh mạng Quốc gia năm 2015 của Mỹ. Điều đó cho thấy hoàn cảnh tìm kiếm dẫn chứng của họ bí bách đến mức nào.

Thực ra, hai cái được trích dẫn là dự luật của Mỹ đã được thông qua thành đạo luật từ năm 2015. Nhưng hai năm sau, khi viết Tờ trình vào năm 2017, thì họ tưởng chúng vẫn còn là dự luật. Hơn nữa, hai thứ ấy không phải là đạo luật độc lập, mà chỉ là tên quy ước được dùng để trích dẫn hai trong số bốn tiêu đề thuộc Cybersecurity Act of 2015 - Đạo luật an toàn mạng năm 2015. Và bản thân cái này cũng chỉ là tên quy ước được dùng để trích dẫn Phân đoạn N của Công luật số 114-113. Vì Công luật số 114-113 còn có nhiều nội dung khác không liên quan, nên khi bàn đến vấn đề an toàn mạng, có thể chỉ trích dẫn phần tương ứng bằng tên gọi Đạo luật an toàn mạng năm 2015. Thế nhưng, thay vì trích dẫn mỗi Đạo luật an toàn mạng năm 2015, họ lại trích dẫn riêng rẽ hai thành phần nhỏ của nó, nhờ thế mà dôi thêm được một đơn vị luật. Nếu biết rằng Đạo luật an toàn mạng năm 2015 còn có hai phần nữa cũng có tên trích dẫn riêng là đạo luật, thì có lẽ họ sẽ kể riêng rẽ cả bốn phần cho thêm phần rôm rả (xem Phụ lục 4).

Có thể ai đó sẽ ngụy biện, rằng dịch *"Cybersecurity Law"* thành *"Luật an ninh mạng"* cũng không sai. Vì theo tập quán ngôn ngữ hiện đại của chính trường, thì *"an ninh"* hay *"an toàn"* cũng như nhau, chỉ chưa kịp cập nhật trong Từ điển tiếng Việt của Viện Ngôn ngữ mà thôi. Và để minh họa, thì viện dẫn kiểu đại ngôn *"an ninh lương thực"*. Nếu vậy thì tại sao *"hệ thống chính trị"* lại không gọi *"Luật an toàn thông tin mạng"* (số 86/2015/QH13) là *"Luật an ninh thông tin mạng"* cho nhất quán?

IV. Luật Trung Quốc

Trong phần III, ta vẫn chưa xem xét cái được Tờ trình về Dự án Luật an ninh mạng của Chính phủ gọi là *"People's Republic of China Cybersecurity Law – Luật an ninh mạng của CHND Trung Hoa",* mà giữ lại để xét riêng trong phần này. Sở dĩ nó được ưu tiên như vậy là vì nhiều người cho rằng Luật an ninh mạng Việt Nam được sao chép từ Luật an ninh mạng Trung Quốc, và nhiều điều tệ hại từ đó mà ra. Vốn sẵn định kiến, nên nghe vậy thì người người đều tin. Chẳng mấy ai đặt câu hỏi, liệu kết luận ấy có chính xác hay không. Nhưng ta sẽ thấy, câu hỏi đó đáng được xem xét và trả lời một cách nghiêm túc.

Có **ba lý do** khiến ta **phải dịch Cybersecurity Law of the People's Republic of China** (được thông qua ngày 7/11/2016 và có hiệu lực thực hiện từ 1/6/2017) **thành Luật an toàn mạng của Cộng hòa Nhân dân Trung Hoa**.

Một là về thuật ngữ, Điều 76 Khoản 2 quy ước như sau:

> *"**Cybersecurity** có nghĩa là tiến hành các biện pháp cần thiết để ngăn ngừa tấn công, xâm nhập, gây nhiễu, phá hoại và sử dụng phi pháp mạng, cũng như ngăn chặn các rủi ro ngoài ý muốn; để mạng hoạt động ổn định và đáng tin cậy, đồng thời bảo đảm cho dung lượng thông tin mạng trọn vẹn, bí mật và khả dụng."*

Như vậy, *"cybersecurity"* trong Luật này có nghĩa là *"biện pháp an toàn mạng"*, hay *"biện pháp bảo đảm an toàn mạng"*, chứ không phải là *"an ninh mạng"*.

Hai là về mục đích của luật, Điều 2 viết như sau:

> *"**Luật này quy định việc xây dựng, vận hành, duy trì và sử dụng mạng, cũng như việc giám sát và quản lý an toàn mạng trên lãnh thổ đất liền của Cộng hòa Nhân dân Trung Hoa.**"*

Ba là về nội dung, Luật này chủ yếu đề cập đến vấn đề an toàn mạng, với ngoại lệ dành cho mấy loại hành vi sau đây:

> *"**Điều 46:** Mọi cá nhân và tổ chức phải chịu trách nhiệm về việc sử dụng trang mạng và không được dựng ra trang mạng hay nhóm liên lạc nhằm **lừa gạt, phổ biến phương pháp phạm tội, tạo ra hay bán những thứ bị cấm hay bị hạn chế, hoặc các hành động phạm pháp khác**, và trang mạng không được sử dụng để công bố thông tin liên quan tới lừa gạt, tạo ra hay bán những thứ bị cấm hay bị hạn chế, hoặc các hành động phạm pháp khác."*

Và hình phạt cho loại hành vi vi phạm trật tự xã hội này được quy định tại Điều 67. Có lẽ đó là mấy loại tội phạm nguy hiểm đặc trưng trên mạng, nhưng còn thiếu quy định pháp luật để xử lý chúng, nên mới nảy sinh ngoại lệ ấy.

Điều 12 quy định nghĩa vụ của Nhà nước đối với công dân và nghĩa vụ của công dân trong việc chấp hành Hiến pháp và pháp luật, trong đó đoạn 2 được viết như sau:

> *"Mọi người và tổ chức sử dụng mạng phải tuân theo Hiến pháp và pháp luật, tôn trọng trật tự công cộng và đạo đức xã hội; không được gây phương hại cho an toàn mạng, không được sử dụng internet để tổ chức các hoạt động gây tổn hại cho an ninh quốc gia, danh dự và quyền lợi dân tộc, kích động phá hoại chủ quyền dân tộc, lật đổ hệ thống xã hội chủ nghĩa, kích động ly khai, phá hoại sự thống nhất dân tộc, ủng hộ khủng bố hoặc chủ nghĩa cực đoan, kích động thù hằn và chia rẽ chủng tộc, phổ biến thông tin bạo lực, tục tĩu, khiêu dâm, tạo ra hay phổ biến thông tin sai trái nhằm phá vỡ trật tự kinh tế hay xã hội, hoặc thông tin xâm phạm uy tín, cuộc sống riêng tư, sở hữu trí tuệ, quyền và lợi ích hợp pháp của người khác, và các hành vi tương tự."*

Đọc xong đoạn vừa rồi dễ lầm tưởng, rằng ngăn chặn và trừng phạt các hành vi nêu trên cũng là mục đích của Luật an toàn mạng Trung Quốc. Nhưng hoàn toàn không phải như vậy. Các hành vi vi phạm ấy chỉ được nương nhờ chốc lát trong khuôn khổ Chương I về Quy định chung, để tập hợp các

nguyên tắc cần tôn trọng khi sử dụng mạng internet trở nên đầy đủ. Rồi lại bị khai trừ ngay khỏi vòng chiến của Luật tại Chương VI về Trách nhiệm pháp lý:

> *"**Điều 70:** Hành vi công bố hay chuyển tiếp thông tin bị cấm bởi đoạn 2 Điều 12 của Luật này, hay các luật khác, hay bị cấm bởi các quy định của nhà nước sẽ bị trừng phạt theo quy định của luật hay quy định nhà nước tương ứng."*

Tức là các hành vi vi phạm an ninh chính trị và trật tự xã hội được đề cập trong đoạn 2 Điều 12 không phải là đối tượng xử lý của Luật này, trong khi hình phạt đối với các hành vi thuộc đối tượng xử lý của Luật này được quy định rất cụ thể trong 11 điều của Chương VI (từ Điều 59 đến Điều 69). Riêng điều đó cũng đủ để chứng tỏ, **KHÔNG THỂ dịch Cybersecurity Law of the People's Republic of China thành Luật an ninh mạng**.

Ngoài phạt tù và phạt tiền, Luật an toàn mạng Trung Quốc còn quy định hình phạt đóng trang mạng, đóng nhóm liên lạc trên mạng... Nhưng do Điều 70 đã khai trừ loại thông tin bị cấm bởi bị cấm bởi đoạn 2 Điều 12 (ví dụ như *thông tin gây tổn hại cho an ninh quốc gia, kích động phá hoại chủ quyền dân tộc, lật đổ hệ thống xã hội chủ nghĩa; thông tin sai trái nhằm phá vỡ trật tự kinh tế hay xã hội; thông tin xâm phạm uy tín, cuộc sống riêng tư, sở hữu trí tuệ, quyền và lợi ích hợp pháp của người khác*) ra khỏi vòng chiến của Luật an toàn mạng Trung Quốc, nên không thể áp dụng Luật này để đóng trang mạng và đóng nhóm liên lạc trên mạng đăng nội dung như vậy.

Về năng lực sáng tạo hình phạt, các nhà làm luật Việt Nam đã tỏ ra còn cứng rắn hơn đồng nghiệp Trung Quốc. Luật an ninh mạng Việt Nam triển khai thêm loại hình phạt **đình chỉ sử dụng mạng viễn thông, mạng internet** và **phong tỏa, hạn chế hoạt động của hệ thống thông tin,** khiến không chỉ người bị kết tội, mà cả những người chung sống hoặc cùng làm việc cũng bị lao đao. Còn Luật an toàn mạng Trung Quốc thì không có những hình thức xử phạt ấy.

Quy định gây nhiều tranh luận và khiến một số nhà đầu tư nước ngoài quan ngại nhất trong Luật an toàn mạng Trung Quốc là:

> *"**Điều 37: Phải lưu trữ trên đất liền Trung Quốc** thông tin cá nhân và các dữ liệu quan trọng khác được thu thập hoặc sản sinh bởi những người điều khiển **hạ tầng thông tin quan trọng** trong lúc hoạt động trên lãnh thổ đất liền của Cộng hòa Nhân dân Trung Hoa. Nếu việc chuyển thông tin ra khỏi đất liền Trung Quốc là thực sự cần thiết cho công việc, thì phải thực hiện các biện pháp do cơ quan an toàn thông tin và thông tin hóa quốc gia và các cơ quan liên quan của Hội đồng quốc gia phối hợp ban hành để đánh giá an toàn; nhưng nếu pháp luật và quy định nhà nước cho phép làm khác thì tuân theo quy định ấy."*

Về phương diện này, Luật an ninh mạng Việt Nam cũng quy định tại Điều 26 Khoản 3 rằng:

> *"Doanh nghiệp trong nước và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu về thông tin cá nhân, dữ liệu về mối quan hệ của người*

sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra ***phải lưu trữ dữ liệu này tại Việt Nam*** *trong thời gian theo quy định của Chính phủ."*

Thoáng qua thì thấy na ná giống nhau, vì cả hai đều quy định phải lưu trữ dữ liệu trên lãnh thổ của nước mình. Song thực ra, **hai quy định ấy rất khác biệt**, trái ngược như nước với lửa.

Khác biệt thứ nhất là về hình thức lưu trữ.

Luật an toàn mạng Trung Quốc đòi hỏi phải lưu trữ dữ liệu trong máy chủ đặt trên đất liền Trung Quốc. Nếu vi phạm Điều 37, bằng cách lưu trữ thông tin ở ngoài lãnh thổ Trung Quốc, hoặc chuyển thông tin cho cá nhân hay tổ chức ở ngoài lãnh thổ Trung Quốc mà không thực hiện các biện pháp an toàn do phía Trung Quốc quy định, thì sẽ bị xử phạt theo quy định tại Điều 66**.**

Luật an ninh mạng Việt Nam thì chấp nhận lưu trữ dữ liệu trong máy chủ đặt ở ngoài lãnh thổ Việt Nam, chỉ đòi hỏi *"phải dịch chuyển đám mây điện toán (máy chủ ảo) về Việt Nam để mở trung tâm dữ liệu tại Việt Nam"*. Đại khái là chỉ phải sinh ra một phiên bản copy huyền ảo bồng bềnh trên *"đám mây điện toán"*, miễn là lấp ló trên bầu trời nước Việt, để bộ máy an ninh Việt Nam có thể tự do khai thác dữ liệu.

Để ngụy biện cho đòi hỏi ấy, họ tung ra thông tin hết sức vu vơ: *"Theo Thường vụ Quốc hội, đến nay, đã có hơn 18 quốc gia thành viên của WTO (trong đó có Hoa Kỳ, Canada, Úc, Đức, Pháp) quy định bắt buộc phải lưu trữ dữ liệu trong lãnh thổ quốc gia."* Vu vơ ở chỗ, nếu tồn tại ai đó trong Thường vụ Quốc hội có đủ trình độ cần thiết, thì người đó cũng không đầu tư thời gian tra cứu để tìm ra 18 quốc gia quy định bắt buộc phải lưu trữ dữ liệu trong lãnh thổ quốc gia; nhưng họ lại gán thành tích tìm kiếm ấy cho Thường vụ Quốc hội, để tăng thêm hiệu quả hù dọa muôn người. Vu vơ ở chỗ, không hề nêu đích danh tên văn bản pháp luật của 18 quốc gia để mọi người có thể kiểm chứng, bởi nếu kiểm chứng thì sẽ phát hiện ra quá nhiều thông tin là sai hoặc bịa đặt. Và vu vơ ở chỗ, nếu có quốc gia nào đó quy định phải lưu trữ dữ liệu trên lãnh thổ nước đó, thì chắc chắn phải quy định như Luật an toàn mạng Trung Quốc, tức là chỉ được lưu trữ trong máy chủ đặt trên lãnh thổ nước đó; chứ khó có chuyện được phép lưu trữ ở ngoài lãnh thổ và chỉ phải sinh ra một phiên bản ảo trong *"đám mây điện toán"* bay trên nước đó.

Khác biệt thứ hai là về đối tượng lưu trữ.

Luật an toàn mạng Trung Quốc đòi hỏi phải lưu trữ *"thông tin cá nhân và các dữ liệu quan trọng khác được thu thập hoặc sản sinh bởi những người điều khiển hạ tầng thông tin quan trọng".* Theo quy định tại Điều 31, **hạ tầng thông tin quan trọng** bao gồm thông tin trong các lĩnh vực truyền thông công cộng và dịch vụ thông tin, điện lực, giao thông, cung cấp nước, tài chính, dịch vụ công cộng, chính phủ điện tử... Cần lưu ý, thông tin cá nhân được đề cập ở đây không mang tính riêng tư, mà là thông tin nhân sự tham gia công việc do doanh nghiệp nước ngoài triển khai tại Trung Quốc.

Còn **Luật an ninh mạng Việt Nam thì đòi hỏi phải lưu trữ *"dữ liệu về thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra"*** khi sử dụng *"dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng"*.

Ví dụ, nếu đầu tư ở Trung Quốc vào các lĩnh vực với hạ tầng thông tin quan trọng thì Luật an toàn mạng Trung Quốc đòi hỏi các doanh nghiệp nước ngoài phải lưu trữ tại Trung Quốc các dữ liệu về nhân sự và các dữ liệu quan trọng khác mà họ thu thập hoặc sản sinh trong quá trình đầu tư. Nhưng nếu đầu tư ở Việt Nam, thì các doanh nghiệp nước ngoài có thể tự do lưu trữ dữ liệu ở nước ngoài, phía Việt Nam không quan tâm và cũng không thể can thiệp, khi các doanh nghiệp ấy không thuộc diện *"cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam"*, là đối tượng mà Khoản 3 Điều 26 Luật an ninh mạng Việt Nam đề cập.

Ví dụ ngược lại, nếu Facebook hoạt động ở Trung Quốc thì có thể lưu trữ dữ liệu tùy ý ở nước ngoài, vì dữ liệu của Facebook không thuộc vào hạ tầng thông tin quan trọng. Nhưng nếu hoạt động ở Việt Nam thì Facebook phải sinh ra một phiên bản lưu trữ (ảo) ở Việt Nam…

Khác biệt thứ ba là về thời gian lưu trữ.

Luật an toàn mạng Trung Quốc không có quy định về thời gian lưu trữ. Tức là, người lưu trữ có quyền xóa thông tin nếu không cần nó nữa.

Luật an ninh mạng Việt Nam thì quy định ngược lại: ***"Phải lưu trữ dữ liệu... trong thời gian theo quy định của Chính phủ."*** Tức là, cho dù bản thân phía lưu trữ không cần nữa, nhưng vẫn phải lưu trữ thông tin trong thời gian theo quy định của Chính phủ, để cung cấp cho cơ quan an ninh. Hệ quả là, nếu khách hàng đăng bài trên trang mạng thì nhà mạng phải phải lưu trữ một thời gian, kể cả khi người dùng đã xóa bài trên giao diện của mình thì nhà mạng vẫn phải lưu trữ tiếp cho hết thời gian theo quy định.

Khác biệt thứ tư là mục đích lưu trữ. Đó là nguyên nhân của mọi nguyên nhân, gây ra ba sự khác biệt kể trên.

Mục đích của Điều 37 Luật an toàn mạng Trung Quốc là đảm bảo an toàn thông tin thuộc các lĩnh vực quan trọng của nền kinh tế quốc gia. Vì vậy không được lưu trữ chúng ở ngoài lãnh thổ Trung Quốc, và nếu cần phải gửi chúng ra nước ngoài vì đòi hỏi của công việc thì phải tuân theo những quy định nghiêm ngặt. Và chỉ áp dụng với *"thông tin cá nhân và các dữ liệu quan trọng khác được thu thập hoặc sản sinh bởi những người điều khiển hạ tầng thông tin quan trọng"*, chứ **không áp dụng với thông tin của người dùng mạng xã hội**. Và cũng vì vậy mà phía lưu trữ có thể xóa thông tin nếu thấy không cần lưu trữ nữa.

Mục đích của Điều 26 Khoản 3 của Luật an ninh mạng Việt Nam là đảm bảo quyền của cơ quan an ninh mạng trong việc lục lọi thông tin của người dân để khống chế người dân. Vì vậy, tác giả và đồng tác giả (tức Quốc hội) của Luật an ninh mạng không quan tâm đến việc bảo đảm an toàn

cho thông tin quan trọng của các ngành kinh tế quan trọng, mà chỉ nhắm vào loại "*thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra"* trên không gian mạng. Và cũng vì vậy mà "*doanh nghiệp trong và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam... phải lưu trữ dữ liệu... trong thời gian theo quy định của Chính phủ"*, kể cả khi người tham gia mạng xã hội đã xóa thông tin mà mình đăng tải trên mạng.

Còn một khác biệt nữa đáng lưu ý. Luật an toàn mạng Trung Quốc quy định tại Điều 47, nếu phát hiện người dùng mạng công bố những thông tin bị pháp luật cấm, thì phía điều khiển mạng thông tin phải thông báo cho cơ quan có thẩm quyền thích hợp, tức là phải thực hiện trách nhiệm tố cáo tội phạm. Tất nhiên, điều này chỉ có thể áp dụng đối với những thông tin vi phạm pháp luật một cách rõ ràng. Còn đối với những vi phạm không đủ rõ ràng thì phía điều khiển mạng thông tin không có trách nhiệm phải phát hiện ra, và vì vậy không có trách nhiệm phải thông báo cho cơ quan có thẩm quyền. Điều quan trọng là, Luật an toàn mạng Trung Quốc đưa ra một số quy định cụ thể nhằm tăng cường bảo vệ thông tin của người dùng, ví dụ:

- Phía điều khiển mạng không được thu thập những thông tin cá nhân không liên quan đến dịch vụ mình cung cấp (Điều 41).
- Phía điều khiển mạng không được để lộ, giả mạo, hay hủy hoại thông tin cá nhân đã thu thập; không được cung cấp thông tin cá nhân cho bên thứ ba nếu không được cá nhân đó đồng ý; và nếu thông tin cá nhân bị đánh cắp, bị mất, hay bị phá hủy thì phải báo ngay chi cá nhân đó biết (Điều 42).
- Người dùng mạng có quyền yêu cầu phía điều khiển mạng xóa thông tin hoặc sửa chữa sai sót thông tin của mình (Điều 43).

Quy định nhằm bảo vệ thông tin của người dùng mạng không phải là mối bận tâm của tác giả Luật an ninh mạng Việt Nam. Trái lại, họ đòi hỏi doanh nghiệp cung cấp dịch vụ phải chủ động lưu trữ, để *"cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi có yêu cầu bằng văn bản"* (Khoản 2 Điều 26), cho dù văn bản ấy có thể được ký bởi loại tội phạm đeo quân hàm sĩ quan công an, tương tự như Thiếu tướng công an Nguyễn Thanh Hóa, kẻ đã sử dụng công nghệ cao để tổ chức hoạt động tội phạm, trong khi đang đảm đương chức vụ Cục trưởng Cảnh sát phòng chống tội phạm sử dụng công nghệ cao.

Hy vọng, thông tin như vậy đã quá đủ để mọi người xem xét lại định kiến, rằng Luật an ninh mạng Việt Nam là bản sao từ Trung Quốc, và rằng những cái xấu của giới cầm quyền Việt thường từ *"đồng chí tốt"* mà ra. Nghĩ như vậy là vô tình can tội... dìm hàng Việt, bởi vì xét về năng lực đầu têu cái xấu và làm điều xấu, giới cầm quyền xứ ta chẳng kém bất kỳ xứ nào.

V. Chiến dịch chi viện

Có lẽ vẫn chưa đủ yên tâm với những thứ đã được trưng ra để giả danh là *"Luật an ninh mạng"* (mà ta đã xem xét trong phần III và IV), họ lại tiếp tục tung thêm thông tin *"138 quốc gia đã ban hành Luật*

an ninh mạng". Tin đó được công bố vào ngày 14/06/2018 trên VTV, vào ngày 22/06/2018 trên Sài Gòn Giải phóng (trong mục *"Tin nóng trong ngày"*) và được đăng đồng loạt vào lúc 9 giờ 30 phút ngày 23/06/2018 trên hệ thống trang mạng đặc nhiệm:

> http://quochoi.org/138-quoc-gia-da-ban-hanh-luat-an-ninh-mang.html
> http://nguyenphutrong.org/138-quoc-gia-da-ban-hanh-luat-an-ninh-mang.html
> http://trandaiquang.org/138-quoc-gia-da-ban-hanh-luat-an-ninh-mang.html
> http://nguyenxuanphuc.org/138-quoc-gia-da-ban-hanh-luat-an-ninh-mang.html
> http://nguyenthikimngan.org/138-quoc-gia-da-ban-hanh-luat-an-ninh-mang.html
> http://phamminhchinh.org/138-quoc-gia-da-ban-hanh-luat-an-ninh-mang.html
> http://hoangtrunghai.org/138-quoc-gia-da-ban-hanh-luat-an-ninh-mang.html
> http://vuongdinhhue.org/138-quoc-gia-da-ban-hanh-luat-an-ninh-mang.html
> http://tolam.org/138-quoc-gia-da-ban-hanh-luat-an-ninh-mang.html
> http://nguyenthiennhan.org/138-quoc-gia-da-ban-hanh-luat-an-ninh-mang.html
> http://vovanthuong.org/138-quoc-gia-da-ban-hanh-luat-an-ninh-mang.html
> http://nguyentandung.org/138-quoc-gia-da-ban-hanh-luat-an-ninh-mang.html
> ...

Đặc biệt, lần này đích thân Chủ tịch nước tham gia chiến dịch. Theo báo Công an Thành phố Hồ Chí Minh, trong buổi tiếp xúc cử tri tại Thành phố Hồ Chí Minh vào ngày 19/06/2018, Chủ tịch nước Trần Đại Quang đã tuyên bố:

> *"Theo số liệu thống kê của Liên Hợp Quốc, 138 quốc gia (trong đó có 95 nước đang phát triển) đã ban hành Luật an ninh mạng."*

Và ông còn tuyên bố nhiều hơn thế về vấn đề an ninh mạng (xem Phụ lục 6).

Vẫn với lối khẳng định chắc nịch như đinh đóng cột, nhưng tuyệt nhiên không để lộ địa chỉ nguồn tin, khiến người đọc người nghe khó lòng phát hiện ra chân tướng sự thật.

Biết tìm thống kê nào trong hàng triệu thống kê? Và tìm kiếm ở bộ phận nào trong số rất nhiều tổ chức của Liên Hợp Quốc? Song dù rất khó cũng không phải là hoàn toàn vô vọng, nếu ta chịu đầu tư thời gian để tìm kiếm một cách nghiêm túc. Hãy vào trang mạng http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx của United Nations Conference on Trade and Development (UNCTAD, tức Hội nghị Liên Hiệp Quốc về Thương mại và Phát triển). Bạn sẽ tìm thấy dưới tiêu đề ***"Cybercrime Legislation Worldwide"*** câu sau đây:

> ***"138 countries (of which 95 are developing and transition economies) had enacted such legislation."***

Có thể nhận thấy, về hình thức thì câu này có vẻ khớp với lời tuyên bố của Chủ tịch nước Trần Đại Quang, rằng ***"138 quốc gia (trong đó có 95 nước đang phát triển) đã ban hành Luật an ninh mạng"***. Vâng, khớp *"138 quốc gia"*, khớp *"95 nước đang phát triển"*, và thậm chí khớp cả hai dấu ngoặc đơn. Nhưng về nội dung thì lại quá vênh nhau.

Để nhận ra sự vênh nhau, hãy nhấp chuột vào vị trí được ghi là ***"Download: Full Data"***, và tải về tệp thống kê mang tên CC.xlsx.

Tiếc rằng, khi rà soát tệp CC.xlsx thì chỉ tìm thấy bốn văn bản pháp luật, mà tên của chúng có chứa từ Cybersecurity hay Cyber Security. Đó là Cybersecurity and Cybercrime Law của Cameroon, Law on Cyber Security của Cộng hòa Séc, Computer Misuse and Cybersecurity Act của Singapore, và Cyber Security Agency Bill của Trinidad and Tobago. Nghĩa là, cho dù phát huy truyền thống dịch bừa *"cybersecurity"* thành *"an ninh mạng"*, thì cũng chỉ có được ba luật và một dự luật về an ninh mạng mà thôi. Song cũng cần nói luôn, **cả bốn văn bản ấy đều không phải là luật hay dự luật về an ninh mạng**.

Điều đáng nói là: Tất cả các luật hay dự luật về cybersecurity của Đức, Hàn Quốc, Mỹ, Nhật Bản và Trung Quốc đã được đề cập trong phần III và phần IV đều không được điểm danh trong tệp thống kê CC.xlsx. Trái lại, năm quốc gia ấy lại được điểm danh bởi những thành tích khác hẳn. Cụ thể là:

- Đức được điểm danh bởi Criminal Code - Strafgesetzbuch (Bộ luật hình sự).
- Hàn Quốc được điểm danh bởi Criminal Act (Bộ luật hình sự) và Act on Promotion of Information and Communications Network Utilization and Information Protection, etc (Luật về thúc đẩy thông tin, sử dụng mạng thông tin và bảo vệ thông tin…).
- Mỹ được điểm danh bởi Title 18 - Crimes and Criminal Procedure (Tiêu đề 18 - Tội phạm và thủ tục tố tụng hình sự) và Computer Fraud and Abuse Act (Đạo luật về gian lận và lạm dụng máy tính).
- Nhật Bản được điểm danh bởi Penal Code (Bộ luật hình sự).
- Trung Quốc được điểm danh bởi Criminal Law of the People's Republic of China (Bộ luật hình sự của Cộng hòa Nhân dân Trung Hoa).

Chỉ riêng với Bộ luật hình sự đã có 67 quốc gia được điểm danh, trong đó có 39 trường hợp với tên gọi Criminal Code, 22 trường hợp với tên gọi Penal Code, 5 trường hợp với tên gọi Criminal Law và 1 trường hợp với tên gọi Criminal Act.

Đặc biệt, mặc dù Quốc hội CHXHCN Việt Nam mới thông qua Luật an ninh mạng vào ngày 12/06/2018 và Văn phòng Chủ tịch nước mới họp báo công bố Lệnh của Chủ tịch nước về Luật an ninh mạng vào ngày 28/06/2018, nhưng từ 01/04/2018 Việt Nam đã được UNCTAD đánh giá là đã thực hiện *"Cybercrime Legislation"*, tức là đã lọt vào cái danh sách được phía Việt Nam gọi là *"138 quốc gia... đã ban hành Luật an ninh mạng"*. Có điều, không phải với thành tích ban hành Luật an ninh mạng, mà với Decree no. 55/2001/ND-CP of August 23, 2001 on the Management, Provision and Use of Internet Services, tức là Nghị định của Chính phủ số 55/2001/NĐ-CP ngày 23 tháng 8 năm 2001 về quản lý, cung cấp và sử dụng dịch vụ internet.

Đọc đến đây, chắc mọi người đã nhận ra, **cái danh sách *"138 quốc gia..."* ấy chỉ thống kê các quốc gia đã có văn bản pháp luật (kể cả dự thảo) đề cập ít nhiều đến tội phạm trên mạng, mà văn bản đặc trưng nhất chính là Bộ luật hình sự.** Danh sách ấy không chỉ dừng lại ở **luật** (vì

những thứ như nghị định của Việt Nam cũng được tính) và chẳng hề liên quan đến khái niệm **an ninh mạng** (theo kiểu Việt Nam). Vậy mà vị Đại tướng công an và đội đặc nhiệm lại dõng dạc tuyên bố *"138 quốc gia… đã ban hành Luật an ninh mạng".*

Nếu chỉ là luận điệu của nhà báo hạng xoàng hay cây bút nặc danh thì chẳng mấy ai bận tâm, và vì vậy cũng chẳng để lại hậu quả nào đáng kể. Nhưng đằng này lại là tuyên bố long trọng của **Chủ tịch nước**, với **chức danh Giáo sư và học vị Tiến sỹ Luật học**, trước bao cử tri và được đài báo truyền đi cả nước...

Bất hạnh thay cho Dân cho Nước, khi những thông tin sai trái như thế lại được dựa vào để lãnh đạo Quốc gia.

Vậy thì tránh sao khỏi lầm đường lạc lối?

VI. Mấy lời nhắn nhủ

Cũng là *"General Secretary"* và *"President"*, nhưng không thể dịch thành *"Tổng thư ký Nguyễn Phú Trọng"* và *"Tổng thống Nguyễn Phú Trọng"*. Tương tự như vậy, cũng là *"Security"*, nhưng không thể dịch *"Cyber Security"* (an toàn mạng) thành *"an ninh mạng"* hay *"an ninh trên mạng"*. Điều đó thì bộ máy khổng lồ với đủ thứ bằng cấp không thể không hiểu.

Như đã chỉ ra ở trên, **TẤT CẢ CÁC LUẬT NƯỚC NGOÀI MÀ HỌ ĐÃ TỪNG VIỆN DẪN** để biện hộ (cho Luật an ninh mạng Việt Nam) **ĐỀU KHÔNG PHẢI LÀ LUẬT AN NINH MẠNG**. Và cho đến lúc công bố bài viết này, vẫn chưa thấy họ chỉ ra được một quốc gia nào khác trên Thế giới cũng có Luật anh ninh mạng, với mục đích tương tự như nội dung Điều 1 Luật an ninh mạng Việt Nam, đó là:

> *"Luật này quy định về hoạt động **bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội trên không gian mạng**; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan."*

Thế nhưng, họ vẫn **dịch Cybersecurity Law (Luật an toàn mạng)** của một số quốc gia **thành Luật an ninh mạng**. Rồi **huy động cả dự thảo luật hay văn bản dưới luật và cả những thứ không hề dính đến cybersecurity, để tạo nên ảo giác Luật an ninh mạng đã hiện hữu muôn nơi**. Hơn nữa, họ **gán cho Luật an ninh mạng cả vai trò bảo vệ an toàn mạng**, mặc dù **Quốc hội khóa XIII đã ban hành Luật an toàn thông tin mạng (số 86/2015/QH13) vào năm 2015** để thực hiện chức năng bảo vệ sự an toàn của mạng. **Bằng cách ấy, họ lừa được bao người tán thành thông qua Luật an ninh mạng.** Cái **lý** cầm quyền **cong** là vậy.

Cái Luật an ninh mạng ấy thuộc loại *"chẳng giống ai"*, nhưng lại tạo ra ảo tưởng *"phù hợp nhất định với thông lệ quốc tế và bảo đảm các điều kiện hội nhập quốc tế về an ninh mạng"*, như đã viết trong Tờ trình về Dự án Luật an ninh mạng của Chính phủ gửi Quốc hội. Đấy là phép thôi miên, dắt nhau vào cõi u mê, tựa như sa vào xứ sở ma quỷ và rước về luật lệ của xứ ấy, mà vẫn đinh ninh vớ được một văn bản pháp lý của Thế giới văn minh.

Xin chúc mừng **15 Đại biểu Quốc hội đã biểu quyết *"KHÔNG TÁN THÀNH"*** thông qua Luật an ninh mạng. Với quyết định đúng đắn nhưng đầy khó khăn ấy, các vị đã thể hiện được trình độ, bản lĩnh và trách nhiệm với dân với nước.

Xin chia vui với **28 Đại biểu Quốc hội đã biểu quyết... *"KHÔNG BIỂU QUYẾT"***. Nhờ có đủ can đảm và tự trọng, các vị đã tránh được một vết nhơ, khỏi phải xấu hổ với gia đình, người thân, bạn bè và đồng nghiệp.

Đối với **423 Đại biểu Quốc hội đã biểu quyết *"TÁN THÀNH"*** thông qua Luật an ninh mạng, một khi đã viết ra bài "*Bầu cử kiểu gì khi tệ ngay từ luật*", tôi cũng chẳng còn ảo tưởng để tranh luận về những điều cao cả. Vẫn hiểu, các vị cũng có trách nhiệm, nhưng không nhất thiết là trách nhiệm với dân với nước, mà có thể chỉ là trách nhiệm với thế lực đã đưa mình vào Quốc hội, nhờ đó có được tiền tài, địa vị và danh vọng. Cũng hiểu, để duy trì vị trí được ban bằng mọi giá, nhiều vị phải chấp nhận làm mọi việc bị sai bảo, kể cả những việc sai, việc xấu. Nhưng nên tỉnh táo, để nhận ra điều sai là sai, điều xấu là xấu và điều ác là ác. Và nếu bị lừa sai là đúng, xấu là tốt, ác là thiện, thì cũng cần hiểu rằng mình đang bị lừa. Chứ đừng nên phụ họa, bằng cách tự huyễn hoặc, lừa dối bản thân, rằng đầy tớ có trung thành thì mới được... chủ lừa. Chẳng vinh quang gì cái thân phận phải nhắm mắt gật bừa, để được bề trên xoa đầu khen *"sáng suốt"***.**

Nếu nhận ra mình đã bị lừa khi bấm nút *"TÁN THÀNH"*, thì đừng vội trách kẻ lừa mình. **Trong cộng đồng mà dối trá đã trở thành tập quán, thậm chí là phương tiện ưa dùng, là vũ khí thông dụng, thì tin vào dối trá là lỗi của bản thân.**

Đừng ngạc nhiên, tại sao họ lại lừa cả Quốc hội. Bởi vì **nếu không lừa được Quốc hội, thì liệu có thể thông qua ngần ấy điều khoản sai trái trong Hiến pháp và pháp luật hay không**?

Đã bị lừa, đang bị lừa và sẽ còn tiếp tục bị lừa. Nhưng **có trở thành nạn nhân của lừa dối hay không, thì trách nhiệm và quyền hạn tự vệ thuộc về bản thân mỗi người**, không thể đổ lỗi cho ai khác.

Nếu để bị lừa mà chỉ có hại cho bản thân, thì cứ việc tự làm tự chịu. Nhưng **không ai có quyền vin vào cớ bị lừa đề bấm nút *"TÁN THÀNH"* những thứ khổ Dân hại Nước**.

Chỉ có thể tránh được những thứ luật sai trái, nếu đa số Đại biểu Quốc hội tư duy bằng đầu chứ không phải bằng mông, tức là vận dụng trí não để cân nhắc đúng sai trước khi bấm nút, chứ không chỉ chăm chăm tuân lệnh nhằm giữ cái ghế được ban. Dẫu chỉ đóng vai trò hợp pháp hóa ý đồ của thế lực cầm quyền, vẫn cần hiểu rằng sẽ không có ai chịu đứng ra gánh thay Quốc hội trách nhiệm trước Nhân dân và lịch sử Dân tộc.

Luật an ninh là khúc nhạc dạo đầu. Đoạn cao trào là Luật đặc khu. Sẽ tiếp tục vang lên bài ca *"theo thông lệ quốc tế"*, *"các nước khác cũng làm như vậy"*, vân vân và vân vân. Một khi Luật an ninh mạng đã được thuyết minh là cần để bảo vệ chế độ, thì có thể Luật đặc khu sẽ được lý giải là cần để

nuôi chế độ, nuôi đảng, và để trả lương hưu cho quan chức, trong đó đương nhiên có các đại biểu Quốc hội. Vậy thì lại bấm nút như xưa ư?

Hãy cân nhắc cẩn trọng. Luật an ninh mạng có thể sẽ không để lại nhiều hậu quả nặng nề, nếu giới cầm quyền nhận ra những khía cạnh sai trái và sự lạc lõng giữa Thế giới văn minh, nên chẳng thi hành, hoặc không thi hành triệt để. Nhưng với Luật đặc khu thì bút sa gà chết. Đất đai đã trao, dù 99 năm, hay 70 năm, hay 50 năm, đều không dễ lấy lại. Đừng quên bài học đau đớn mang tên Formosa... Cho nên, **hãy tỉnh táo để phân biệt đúng sai và quyết định có chấp nhận bị lừa tiếp hay không.**

* * *

Phụ lục 1. The Basic Act on Cybersecurity - Đạo luật cơ bản về an toàn mạng của Nhật Bản

The Basic Act on Cybersecurity là Đạo luật cơ bản về an toàn mạng của Nhật Bản, mang số 104 của năm 2014. Nó gồm năm phần sau:

Chương I: Các quy định chung (từ Điều 1 đến Điều 11)
Chương II: Chiến lược đảm bảo an toàn mạng (Điều 12)
Chương III: Chính sách cơ bản (từ Điều 13 đến Điều 23)
Chương IV: Các trung tâm chiến lược đảm bảo an toàn mạng (từ Điều 24 đến Điều 35)
Các quy định bổ sung

Điều 1 xác định:

> *"Mục đích của đạo luật này là thúc đẩy chính sách an toàn mạng một cách toàn diện và hiệu quả, thông qua: quy định các nguyên tắc cơ bản của chính sách an toàn mạng quốc gia; xác định trách nhiệm của chính quyền trung ương, chính quyền địa phương và các tổ chức công quyền liên quan khác; quy định các nội dung thiết yếu của các chính sách liên quan tới an toàn mạng, như xác định chiến lược an toàn mạng; và thiết lập các cơ quan đầu não chiến lược về an toàn mạng…"*

Điều 2 định nghĩa:

> *"Khái niệm "Cybersecurity" có nghĩa là các biện pháp cần được áp dụng để quản lý thông tin an toàn, như ngăn ngừa sự rò rỉ, biến mất hoặc hư hại của thông tin được lưu trữ, gửi đi, truyền hay tiếp nhận bằng phương tiện điện tử, từ tính, hoặc các phương tiện khác không thể nhận ra bởi những chức năng tri giác tự nhiên; và để đảm bảo sự an toàn và sự tin cậy của cá hệ thống tin, của thông tin và các mạng viễn thông (kể cả các biện pháp ngăn ngừa cần thiết để chống lại các hành vi ác ý đối với máy tính điện tử thông qua mạng lưới thông tin hay môi trường lưu trữ thông tin được tạo ra bởi phương tiện điện tử hay từ tính), và để các trạng thái được duy trì một cách hợp lý."*

Đặc biệt, một trong sáu nguyên tắc cơ bản được quy định tại Điều 3 là:

> *"Việc thúc đẩy chính sách an toàn mạng phải được thực hiện sao cho **không xâm phạm bất hợp pháp quyền con người**."*

Qua đó ta thấy rõ, đạo luật này không hề đề cập đến vấn đề an ninh chính trị, xã hội trên mạng, và **không hề hạn chế quyền con người**.

Các thông tin trên đã quá đủ để khẳng định rằng: **Không thể dịch The Basic Act on Cybersecurity thành Đạo luật cơ bản về an ninh mạng** (như trong Tờ trình về Dự án Luật an ninh mạng của Chính phủ gửi Quốc hội).

Phụ lục 2. Act on Cyber Security - Đạo luật an toàn mạng của Cộng hòa Séc

Thông qua trang https://www.cybersecurity.cz/basic_en.html, có thể xác định rằng cái mà Tờ trình về Dự án Luật an ninh mạng viết là Cyber Security Law of the Czech Republic chính là Act on Cyber Security (tên viết tắt của On Cyber Security and Change of Related Acts), tức là Đạo luật an toàn mạng của Cộng hòa Séc, mang số 181 của năm 2014 và có hiệu lực thi hành từ ngày 01/01/2015. Nó gồm các phần sau:

Phần một: Đảm bảo an toàn mạng
- Chương I: Các quy định chung (từ Điều 1 đến Điều 3)
- Chương II: Hệ thống bảo đảm an toàn mạng (từ Điều 4 đến Điều 20)
- Chương III: Tình trạng khẩn cấp mạng (Điều 21)
- Chương IV: Tiến hành quản lý nhà nước (Điều 22)
- Chương V: Kiểm tra, giám sát và các vi phạm quản lý (Điều 23 đến Điều 27)
- Chương VI: Các quy định cuối (Điều 28 đến Điều 33)

Phần hai: Sửa đổi Đạo luật về bảo vệ thông tin phân loại và tư cách đảm bảo an toàn
Phần ba: Sửa đổi Đạo luật thông tin điện tử
Phần bốn: Sửa đổi Đạo luật về tự do thông tin
Phần năm: Sửa đổi Đạo luật về phát thanh và truyền hình
Phần sáu: Hiệu lực thi hành

Về đối tượng của đạo luật, Điều 1 Khoản 1 viết:

> *"Đạo luật này quy định quyền và nghĩa vụ của thể nhân và pháp nhân, thẩm quyền và quyền lực của các cơ quan công quyền trong lĩnh vực an toàn mạng."*

Về khái niệm *"Security of information"*, Điều 2 viết:

> *"Security of information (bảo đảm an toàn thông tin) có nghĩa là đảm bảo sự bí mật, tính nguyên vẹn và tính khả dụng của thông tin."*

Về khái niệm *"Security measures"*, Điều 4 Khoản 1 viết:

"Security measures (biện pháp đảm bảo an toàn) có nghĩa là hệ thống các thao tác với mục đích đảm bảo an toàn của thông tin trong các hệ thống thông tin, tính khả dụng và tính đáng tin của các dịch vụ và các mạng truyền thông điện tử trong không gian mạng."

Trong bản dịch tiếng Anh (dài 18 trang) của Act on Cyber Security, từ *"the state"* xuất hiện 11 lần, nhưng luôn trong ngữ cảnh *"the state of emergency"* hay *"the state of cyber emergency"* để chỉ tình trạng khẩn cấp, chứ không có lần nào có nghĩa là *"nhà nước"* (để chỉ thứ tội *"chống nhà nước"*). Từ *"national security"* (anh ninh quốc gia) cũng chẳng xuất hiện lần nào. Viết thêm như vậy để thấy rằng: **Không thể dịch Act on Cyber Security thành Luật an ninh mạng** (như trong Tờ trình về Dự án Luật an ninh mạng của Chính phủ gửi Quốc hội).

Phụ lục 3. Dự luật của Hàn Quốc

Legislative Bill for National Anti-Cyberterrorism Act (2013) là Dự luật phòng chống khủng bố mạng quốc gia của Hàn Quốc. Nó gồm các phần sau:

Chương I: Các quy định chung (từ Điều 1 đến Điều 5)
Chương II: Phòng ngừa khủng bố mạng cấp quốc gia và hệ thống điều hành xử lý khủng hoảng (từ Điều 6 đến Điều 9)
Chương III: Chống khủng bố mạng và điều hành xử lý khủng hoảng mạng (từ Điều 10 đến Điều 17)
Chương IV: Nghiên cứu & phát triển, hỗ trợ (từ Điều 18 đến Điều 24)
Chương IV: Quy định về hình phạt (Điều 25 và Điều 26)

Thuật ngữ *"khủng bố mạng"* có thể khiến nhiều người nghĩ, dự luật này được dành cho vấn đề an ninh (chính trị, xã hội) trên mạng. Suy luận này khớp với giải thích từ *"khủng bố mạng"* tại Điều 2 Khoản 9 Luật an ninh mạng Việt Nam:

"Khủng bố mạng là việc sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện hành vi khủng bố, tài trợ khủng bố."

Nhưng các nhà làm luật Hàn Quốc lại định nghĩa khác hẳn tại Điều 2 Khoản 1 của Dự luật phòng chống khủng bố mạng quốc gia:

"Khủng bố mạng là mọi hành động tấn công xâm nhập, gây rối, làm tê liệt, hoặc phá hủy hạ tầng viễn thông thông tin, hoặc các hành động nhằm đánh cắp, hủy hoại thông tin và phát tán thông tin sai lệch, bằng các phương tiện điện tử như đột nhập, virut máy tính, từ chối dịch vụ và sóng điện từ."

Cũng tại Điều 2 Khoản 1 của Dự luật, khái niệm *"Cyber Security"* được định nghĩa như sau:

"*Cyber Security có nghĩa là các biện pháp và cách ứng phó bằng các phương tiện quản lý, vật chất và công nghệ nhằm bảo vệ hạ tầng truyền thông và thông tin trước khủng bố mạng, bao gồm cả việc điều hành xử lý khủng hoảng mạng."*

Theo nghĩa ấy, chỉ có thể dịch *"Cyber Security"* thành *"biện pháp bảo đảm an toàn mạng"*, chứ không thể dịch thành *"an ninh mạng"*.

Mục đích của Dự luật là bảo vệ sự an toàn của mạng quốc gia, và điều đó được xác định rõ ràng tại Điều 1:

> *"Mục đích của Đạo luật là đóng góp cho an ninh và lợi ích quốc gia bằng cách xác định các tình huống cơ bản trong việc ngăn ngừa khủng bố mạng quốc gia, nhằm đối phó khủng bố mạng đe dọa an ninh quốc gia và cho phép phản ứng nhanh bằng cách tập trung năng lực quốc gia trong các trường hợp khủng hoảng mạng."*

Tóm lại, **National Anti-Cyberterrorism Act của Hàn Quốc là một dự luật về an toàn mạng, chứ không phải là dự luật về an ninh mạng** (như Tờ trình về Dự án Luật an ninh mạng của Chính phủ gửi Quốc hội đã viết).

Phụ lục 4. Một số đạo luật của Mỹ về an toàn mạng

Trang Cyber Security Laws of Different Countries (Luật an toàn mạng của các nước) của International Commission on Cyber Security Law (Hội đồng Quốc tế về Luật an toàn mạng) liệt kê ba đạo luật của Hợp chúng quốc Hoa Kỳ về an toàn mạng, đó là Cybersecurity Enhancement Act of 2014, National Cybersecurity Protection Act of 2014, Cybersecurity Act of 2015.

Cybersecurity Enhancement Act of 2014 (Public Law 113-274) có nghĩa là Đạo luật tăng cường an toàn mạng năm 2014 (Công luật số 113-274), được Tờ trình về Dự án Luật an ninh mạng dịch thành Đạo luật tăng cường an ninh mạng năm 2014. *"Một đạo luật tạo mối liên kết công-tư tình nguyện tiếp diễn nhằm cải tiến biện pháp an toàn mạng và tăng cường nghiên cứu và phát triển an toàn mạng, phát triển và đào tạo lực lượng lao động, ý thức công cộng và sự sẵn sàng, và cho các mục đích khác"* - đó là tên đầy đủ, và cũng đủ để nói lên nội dung của đạo luật.

National Cybersecurity Protection Act of 2014 (Public Law 113-282) có nghĩa là Đạo luật bảo vệ an toàn mạng quốc gia năm 2014 (Công luật số 113-282), được Tờ trình về Dự án Luật an ninh mạng dịch thành Đạo luật bảo vệ an ninh mạng quốc gia 2014. *"Một đạo luật để lập điều lệ cho một trung tâm thao tác an toàn mạng đang tồn tại"* - đó là tên đầy đủ của đạo luật.

Cybersecurity Act of 2015 có nghĩa là Đạo luật an toàn mạng năm 2015. Nó là Phân đoạn N của Công luật số 114-113, và bản thân nó chứa bốn tiêu đề với tên trích dẫn riêng như sau:

- Tiêu đề I, có tên trích dẫn là Cybersecurity Information Sharing Act of 2015, tức Đạo luật chia sẻ thông tin an toàn mạng năm 2015. Tờ trình về Dự án Luật an ninh mạng gọi nó là Dự luật chia sẻ thông tin an ninh mạng năm 2015.
- Tiêu đề II.A, có tên trích dẫn là National Cybersecurity Protection Advancement Act of 2015, tức Đạo luật khuyến khích bảo vệ an toàn mạng quốc gia năm 2015. Có thể nó là cái mà Tờ

trình về Dự án Luật an ninh mạng gọi là Dự luật tăng cường bảo vệ an ninh mạng quốc gia năm 2015.

- Tiêu đề II.B, có tên trích dẫn là Federal Cybersecurity Enhancement Act of 2015, tức Đạo luật tăng cường bảo đảm an toàn mạng Liên bang năm 2015.
- Tiêu đề III, có tên trích dẫn là Federal Cybersecurity Workforce Assessment Act of 2015, tức Đạo luật đánh giá lực lượng bảo đảm an toàn mạng năm 2015. Tờ trình về Dự án Luật an ninh mạng gọi nó là Đạo luật đánh giá lực lượng an ninh mạng.

Ngoài ba công luật được thống kê trên trang Cyber Security Laws of Different Countries (Luật an toàn mạng của các nước) còn có Federal Information Security Modernization Act of 2014 (Public Law 113-283), có nghĩa là Đạo luật hiện đại hóa biện pháp an toàn thông tin Liên bang. Tờ trình về Dự án Luật an ninh mạng gọi nó là Đạo luật hiện đại hóa an ninh thông tin Liên bang năm 2014.

Tóm lại, **các đạo luật được liệt kê ở trên đều nhằm bảo đảm an toàn mạng, chứ không xử lý vấn đề an ninh trên mạng** (như Tờ trình về Dự án Luật an ninh mạng của Chính phủ gửi Quốc hội đã viết).

Phụ lục 5. IT-Sicherheitsgesetz - Luật an toàn mạng của CHLB Đức

IT-Sicherheitsgesetz là tên gọi tắt của Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, tức Luật tăng cường an toàn các hệ thống kỹ thuật thông tin. Ngày 17/12/2014 Chính phủ Liên bang Đức thông qua bản dự thảo của IT-Sicherheitsgesetz, và sáu tháng sau Quốc hội Đức mới thông qua Luật này vào ngày 12/06/2015. Vậy mà ngày 18/12/2014 VTV đã tung ra tin *"Đức thông qua Luật an ninh mạng"*.

Luật này có 11 điều. Điều 10 quy định về việc đánh giá lại ba khoản của Điều 1 sau 4 năm thực hiện. Điều 11 quy định về thời điểm có hiệu lực thi hành. 9 điều còn lại quy định về sửa đổi trong tám luật đã được ban hành từ trước, cụ thể như sau.

Điều 1 và Điều 8 quy định về một số sửa đổi trong BSI-Gesetz, tên gọi tắt của Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (Luật về Văn phòng Liên bang phụ trách an toàn kỹ thuật thông tin). Nội dung thay đổi là mở rộng vai trò của Văn phòng liên bang phụ trách an toàn kỹ thuật thông tin, đặc biệt là vai trò tư vấn.

Điều 2 quy định về sửa đổi Điều 44b của Atomgesetz (Luật nguyên tử), tên gọi tắt của Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (Luật về sử dụng năng lượng hạt nhân vì mục đích hòa bình và phòng chống hiểm họa của nó).

Điều 3 quy định về một số sửa đổi trong Energiewirtschaftsgesetz (Luật kinh tế năng lượng), tên gọi tắt của Gesetz über die Elektrizitäts- und Gasversorgung (Luật cung cấp điện năng và khí đốt).

Điều 4 quy định về sửa đổi Điều 13 và Điều 16 của Telemediengesetz (Luật dịch vụ thông tin liên lạc điện tử).

Điều 5 quy định về một số sửa đổi trong Telekommunikationsgesetz (Luật viễn thông).

Điều 6 quy định một thay đổi nhỏ trong Bundesbesoldungsgesetz (Luật tiền lương Liên bang), đó là chuyển Chủ tịch Trung tâm đào tạo Quân đội Đức từ nhóm lương B 6 sang nhóm lương B 7.

Điều 7 quy định một thay đổi nhỏ trong Điều 4 của Bundeskriminalamtgesetz (Luật Văn phòng cảnh sát hình sự Liên bang), tên gọi tắt của Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (tức Luật về Văn Văn phòng cảnh sát hình sự Liên bang và việc phối hợp giữa Liên bang và các bang trong công tác cảnh sát hình sự).

Điều 9 quy định về việc xóa Khoản 7 Điều 3 của Gesetz zur Strukturreform des Gebührenrechts des Bundes (Luật cải cách cơ cấu thu phí của Liên bang).

Kể chi tiết như vậy để thấy rằng, **IT-Sicherheitsgesetz thực sự là Luật an toàn mạng và hoàn toàn không liên quan đến cái gọi là Luật an ninh mạng**.

Hơn nữa, cũng để lưu ý một bài học, đáng để các nhà làm luật Việt Nam học hỏi. Đó là, để đáp ứng tình hình mới thì không nhất thiết phải ban hành một luật hoàn toàn mới, mà có thể chỉ cần sửa đổi một số quy định trong các luật hiện hành. Và để sửa đổi chúng thì không nên quy định trong nhiều luật lẻ tẻ, tương ứng với các luật phải sửa đổi, mà nên gói chung trong một luật mới, giống như Luật an toàn mạng của Đức. Nếu các nhà làm luật Việt Nam quy định trong Luật an ninh mạng về việc sửa đổi Khoản 1 Điều 18 Luật an toàn thông tin mạng, thì đã không dẫn đến mâu thuẫn giữa nó và Khoản 2 Điều 26 của Luật an ninh mạng.

Phụ lục 6

Trong buổi tiếp xúc với cử tri tại Thành phố Hồ Chí Minh vào ngày 19/06/2018, Chủ tịch nước Trần Đại Quang tuyên bố:

> *"Hiện nay, có 18 quốc gia yêu cầu nhà cung cấp dịch vụ mạng, nhất là mạng xã hội, phải lưu trữ dữ liệu tại quốc gia đó. Tháng 5/2018, Liên minh châu Âu chính thức yêu cầu Facebook phải lưu trữ dữ liệu tại các nước thuộc Liên minh."*

Thử hỏi, thông tin *"có 18 quốc gia yêu cầu nhà cung cấp dịch vụ mạng, **nhất là mạng xã hội**, phải lưu trữ dữ liệu tại quốc gia đó"* được lấy từ tài liệu nào? Chịu tai tiếng như Cybersecurity Law of the People's Republic of China, mà cũng không hề *"yêu cầu nhà cung cấp **dịch vụ**… **mạng xã hội** phải lưu trữ dữ liệu tại quốc gia đó"*, thì cái yêu cầu ấy có thể tồn tại ở 18 quốc gia nào?

Và thông tin *"Tháng 5/2018, Liên minh châu Âu chính thức yêu cầu Facebook phải lưu trữ dữ liệu tại các nước thuộc Liên minh"* được lấy từ đâu? Lưu ý rằng, General Data Protection Regulation of the European Union (tức Quy định chung về bảo vệ dữ liệu của Liên minh châu Âu, được viết tắt là GDPR) bắt đầu có hiệu lực thi hành từ ngày 25/05/2018. Khoản 1 Điều 3 GDPR khẳng định:

> *"Quy định này áp dụng cho việc xử lý thông tin cá nhân trong khuôn khổ hoạt động của một cơ sở kinh doanh của nhà quản lý hay nhà xử lý đặt tại EU, không phụ thuộc vào việc xử lý được thực hiện ở trong hay ngoài EU."*

Chương V (từ Điều 44 đến Điều 50) được dành để quy định về việc chuyển thông tin cá nhân sang nước thứ ba và các tổ chức quốc tế, với những điều kiện không hề ngặt nghèo, có thể thỏa mãn dễ dàng. Đặc biệt, trong khi thời gian lưu trữ dữ liệu được đề cập đến 10 lần, **thì GDPR không hề đề cập đến địa điểm lưu trữ dữ liệu**, tức là **không có bất kỳ đòi hỏi hay hạn chế nào về địa điểm lưu trữ dữ liệu**. Vậy thì dựa vào đâu để nói rằng *"Liên minh châu Âu chính thức yêu cầu Facebook phải lưu trữ dữ liệu tại các nước thuộc Liên minh"*?

Ngày 8 tháng 10 năm 2018

Cùng tác giả:

Luật an ninh mạng - Tượng đài... cô đơn
Một số điều cần trao đổi nhân vụ Trịnh Xuân Thanh
Mấy ý kiến trao đổi về tiêu chuẩn bổ nhiệm chức danh giáo sư
Bầu cử kiểu gì khi tệ ngay từ luật
Oan ức trĩu Hồn Cây
Sai phạm về tố tụng trong vụ án "Nguyễn Hữu Vinh cùng đồng bọn…"
Não lòng với Hiến pháp
Bắt mạch Hiến… nháp
Hiến pháp vi hiến
Hiến pháp 2013 - Sửa nhầm hay đổi thiệt?
Đảng và Nhân dân - Vị thế bị tráo
Uẩn khúc trong Điều 4 Hiến pháp
Rủi cho Phương Uyên - May cho Dimitrov
Quốc hiệu nào hội tụ lòng Dân?
Chỗ đứng của Nhân dân trong Hiến pháp
Teo dần quyền con người trong Hiến pháp
Hai tử huyệt của chế độ
Lực cản Nhà nước pháp quyền
Một số khía cạnh hình sự của vụ án Tiên Lãng - Hải Phòng
Nhân vụ Tiên Lãng bàn về công vụ
Quyền biểu tình của công dân
Bài học tồn vong từ thảm họa
Phiêu lưu điện hạt nhân
Về huyền thoại điện hạt nhân giá rẻ

Mạn bàn về an toàn điện hạt nhân

Bàn về qui mô đào tạo đại học từ góc độ chất lượng giảng viên