BỘ TƯ PHÁP
VỤ PHỔ BIẾN, GIÁO DỤC PHÁP LUẬT

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

ĐỀ CƯƠNG GIỚI THIỆU
LUẬT AN TOÀN THÔNG TIN MẠNG

Luật an toàn thông tin mạng đã được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam khóa XIII, kỳ họp thứ 10 thông qua ngày 19/11/2015. Luật có hiệu lực thi hành từ ngày 01/7/2016.

I. SỰ CẦN THIẾT BAN HÀNH LUẬT AN TOÀN THÔNG TIN MẠNG

Hiện nay, mạng Internet đã trở thành công cụ trung tâm để phát triển nền kinh tế và xã hội của mọi quốc gia. Đối với Việt Nam, mạng internet cũng được coi là công cụ, phương tiện quan trọng để thực hiện mục tiêu đưa Việt Nam trở thành nước công nghiệp hóa, hiện đại hóa, phát triển mạnh trong một thế giới cạnh tranh và toàn cầu hóa.

Tuy nhiên, tính hai mặt của công nghệ internet đang là thách thức đối với việc thực thi luật pháp, nhất là trong việc điều chỉnh những hành vi lợi dụng mạng internet nhằm truyền đưa, lưu trữ, phát tán thông tin sai trái, độc hại, vi phạm quyền và lợi ích hợp pháp của tổ chức, cá nhân. Các tổ chức, cá nhân luôn phải đối mặt với nhiều loại hình tấn công trên mạng với mức độ ngày càng thường xuyên hơn, như làm biến dạng trang tin, lừa đảo trên mạng, tấn công từ chối dịch vụ, phát tán mã độc hại và vi-rút máy tính, thư rác, đánh cắp thông tin, phá hoại dữ liệu, làm gián đoạn, phá rối hoạt động, thay đổi cấu hình của các hệ thống thông tin, phần mềm gián điệp, tấn công hệ thống ngân hàng và mạng lưới bán hàng trực tuyến, tin nhắn lừa đảo.

Bên cạnh đó, trên môi trường mạng đã và đang xuất hiện ngày càng nhiều tổ chức, cá nhân ở tầm quốc gia sử dụng mạng để đánh cắp, thỏa hiệp hoặc phá hủy dữ liệu quan trọng của quốc gia khác. Vì vậy, Việt Nam cũng như các nước trên thế giới đang đứng trước các mối đe dọa từ các tội phạm trên môi trường mạng. Một số tội phạm chỉ tồn tại trong thế giới kỹ thuật số, đặc biệt với mục tiêu phá hoại an toàn của mạng máy tính và dịch vụ trực tuyến; sử dụng mạng làm công cụ để mở rộng phạm vi ảnh hưởng; tiến hành hoạt động gián điệp hoặc gây ảnh hưởng đến hoạt động của Chính phủ để phá hoại nền kinh tế; truyền bá thông tin sai lệch, làm gián đoạn các dịch vụ quan trọng hoặc tìm kiếm lợi thế trong xung đột mạng. Mặt khác, lỗ hổng trên mạng có thể bị tội phạm khai thác

nhằm giảm lợi thế công nghệ quân sự hoặc sử dụng nó để tấn công cơ sở hạ tầng quan trọng của các quốc gia.

Các mối đe dọa đối với Việt Nam đến từ các nhóm hoạt động với động cơ chính trị hoạt động trên mạng. Việc tấn công vào các trang thông tin điện tử, cổng thông tin điện tử và dịch vụ trực tuyến ở Việt Nam được dàn dựng bởi các nhóm tội phạm đang ngày càng phổ biến hơn, nhằm làm gián đoạn, gây thiệt hại về uy tín chính trị và kinh tế của đất nước. Các nhóm tội phạm khác nhau như: khủng bố, tình báo nước ngoài và quân đội của một số nước đang hoạt động hiện nay nhằm mục đích xâm hại lợi ích của Việt Nam trên mạng.

Tất cả những vấn đề trên đã đặt ra cho công tác quản lý nhà nước về an toàn thông tin cần phải giải quyết để bảo đảm một môi trường phát triển ổn định.

Thực tiễn công tác quản lý, điều hành trong lĩnh vực thông tin, truyền thông cho thấy hành lang pháp lý về an toàn thông tin còn thiếu, không đồng bộ và chưa theo kịp với hiện trạng phát triển của xã hội cũng như hội nhập quốc tế. Các văn bản pháp quy được xây dựng mới chỉ tập trung vào nhiệm vụ quản lý của từng lĩnh vực đơn lẻ, đề cập đến công tác đảm bảo an toàn thông tin ở từng phạm vi hẹp như Luật viễn thông, Luật giao dịch điện tử, Luật công nghệ thông tin… Các văn bản pháp luật hiện hành có liên quan đến công tác bảo đảm an toàn thông tin còn có những vấn đề bất cập như: thiếu các quy định về phân loại cấp độ an toàn thông tin của hệ thống thông tin, quy định quản lý sản phẩm an toàn thông tin cũng như quản lý dịch vụ an toàn thông tin… Hơn nữa, Việt Nam chưa có một văn bản ở tầm luật để điều chỉnh toàn diện hoạt động an toàn thông tin trên mạng, bảo đảm một môi trường mạng an toàn phục vụ cho sự nghiệp công nghiệp hóa, hiện đại hóa đất nước.

Vì vậy, Việt Nam cần có các quy định pháp lý về an toàn thông tin để nội luật hóa các điều ước quốc tế mà Việt Nam là thành viên; phù hợp với thông lệ quốc tế, bảo đảm an toàn thông tin, tạo môi trường bình đẳng cho các tổ chức, doanh nghiệp hoạt động sản xuất, kinh doanh tại Việt Nam.

II. QUAN ĐIỂM CHỈ ĐẠO, MỤC TIÊU BAN HÀNH LUẬT AN TOÀN THÔNG TIN MẠNG

1. Quan điểm chỉ đạo

- Thể chế hóa các chủ trương, đường lối, chính sách của Đảng và Nhà nước về an toàn thông tin, đáp ứng yêu cầu phát triển bền vững kinh tế - xã hội, bảo vệ thông tin và hệ thống thông tin, góp phần bảo đảm quốc phòng, an ninh, chủ quyền và lợi ích quốc gia; phù hợp với điều kiện kinh tế, xã hội của đất nước trong giai đoạn hiện nay và các năm tiếp theo; đồng thời, đáp ứng yêu cầu hội nhập kinh tế quốc tế; bảo đảm phù hợp với quy định của Hiến pháp, đồng

bộ, thống nhất với hệ thống pháp luật của nước Cộng hòa xã hội chủ nghĩa Việt Nam;

- Đáp ứng yêu cầu đổi mới về cơ chế, chính sách trong hoạt động an toàn thông tin, tạo môi trường thuận lợi và an toàn cho các thành phần kinh tế, góp phần thúc đẩy phát triển ứng dụng công nghệ thông tin và truyền thông theo hướng chủ động hội nhập quốc tế; đồng thời, tạo môi trường an toàn và tin cậy cho các nhà đầu tư nước ngoài tham gia hoạt động đầu tư, thương mại tại Việt Nam;

- Bảo đảm an toàn thông tin theo hướng hiện đại, đồng bộ và ổn định lâu dài, đáp ứng các yêu cầu về an toàn thông tin phục vụ phát triển kinh tế, xã hội, quốc phòng, an ninh, góp phần thực hiện sự nghiệp công nghiệp hoá, hiện đại hoá đất nước và bảo đảm an ninh quốc gia;

- Tiếp thu có chọn lọc kinh nghiệm của các nước có hệ thống pháp luật về an toàn thông tin phát triển và vận dụng phù hợp với điều kiện kinh tế - xã hội ở Việt Nam.

2. Mục tiêu

- Hoàn thiện cơ sở pháp lý ổn định về an toàn thông tin theo hướng áp dụng các quy định pháp luật một cách đồng bộ, khả thi trong thực tiễn thi hành;

- Phát huy các nguồn lực của đất nước để bảo đảm an toàn thông tin, phát triển lĩnh vực an toàn thông tin đáp ứng yêu cầu phát triển kinh tế - xã hội, quốc phòng, an ninh, góp phần nâng cao chất lượng cuộc sống của nhân dân và bảo đảm quốc phòng, an ninh;

- Bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân tham gia hoạt động an toàn thông tin;

- Đẩy mạnh công tác giám sát, phòng, chống nguy cơ mất an toàn thông tin, đảm bảo hiệu quả công tác thực thi quản lý nhà nước trong lĩnh vực này;

- Mở rộng hợp tác quốc tế về an toàn thông tin trên cơ sở tôn trọng độc lập, chủ quyền, bình đẳng, cùng có lợi, phù hợp với pháp luật Việt Nam và điều ước quốc tế mà Việt Nam tham gia ký kết.

III. BỐ CỤC VÀ Ý NGHĨA BAN HÀNH LUẬT AN TOÀN THÔNG TIN MẠNG

1. Bố cục

Luật an toàn thông tin mạng gồm 08 Chương và 54 Điều, bao gồm:

Chương I. Những quy định chung (Điều 01 – Điều 08).

Chương II. Bảo đảm an toàn thông tin mạng (Điều 09 – Điều 29), bao gồm 04 mục: Bảo vệ thông tin mạng; Bảo vệ thông tin cá nhân; Bảo vệ hệ thống thông tin; Ngăn chặn xung đột thông tin trên mạng.

Chương III. Mật mã dân sự (Điều 30 – Điều 36).

Chương IV. Tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng (Điều 37 – Điều 39).

Chương V. Kinh doanh trong lĩnh vực an toàn thông tin mạng (Điều 40 – Điều 48), gồm 02 mục: Giấy phép kinh doanh sản phẩm an toàn thông tin mạng;Quản lý nhập khẩu sản phẩm an toàn thông tin mạng.

Chương VI. Phát triển nguồn nhân lực an toàn thông tin mạng (Điều 49 – Điều 50).

Chương VII. Quản lý nhà nước về an toàn thông tin mạng (Điều 51 – Điều 52).

Chương VIII. Điều khoản thi hành (Điều 53 – Điều 54).

2. Ý nghĩa của việc ban hành Luật an toàn thông tin mạng

Trước khi Luật an toàn thông tin mạng ra đời, các quy định về an toàn thông tin vẫn còn rải rác ở các văn bản pháp luật ở các phạm vi và mức độ khác nhau, chưa đầy đủ, chưa bao quát được lĩnh vực an toàn thông tin, còn gây chồng chéo trong lĩnh vực quản lý điều hành trong lĩnh vực an toàn thông tin, gây khó khăn nhất định khi áp dụng. Trong khi đó vẫn còn những khoảng trống chưa được điều chỉnh, khi xảy ra sự cố thì vẫn thiếu các quy định phối hợp thực thi tổng thể. Do đó, Luật an toàn thông tin mạng có thể xem là văn bản hoàn thiện, tổng hợp và bao quát nhất các nội dung có liên quan đến an toàn thông tin nhằm tránh được những hạn chế này.

Luật an toàn thông tin mạng đã đưa ra các chế tài mạnh hơn nhằm hạn chế các hành vi gây mất an toàn thông tin, thay vì việc trước đây các văn bản về xử phạt vi phạm hành chính trong lĩnh vực an toàn thông tin vẫn theo cách tiếp cận nhỏ lẻ, áp dụng với từng loại riêng biệt và cũng mới chỉ giới hạn ở một số loại như can thiệp vào hệ thống, phát tán mã độc, nên mức độ tác động còn hẹp.

Luật an toàn thông tin mạng đã đưa ra quy định về kinh doanh trong lĩnh vực an toàn thông tin mạng, các dịch vụ an toàn thông tin mạng được cho phép kinh doanh có thể kể đến như dịch vụ kiểm tra, đánh giá an toàn thông tin mạng, dịch vụ chứng thực chữ ký điện tử, dịch vụ tấn công an toàn thông tin mạng,... và các sản phẩm an toàn thông tin mạng như sản phẩm kiểm tra, đánh giá an toàn thông tin mạng, sản phẩm giám sát an toàn thông tin mạng.

Do sự phát triển nhanh của công nghệ và sự tăng trưởng đáng kể trong việc sử dụng ứng dụng điện thoại thông minh và các thiết bị điện tử đang tạo

ngày càng gia tăng các lỗ hổng gây mất an toàn thông tin tuy các văn bản pháp luật đã cho phép ngăn chặn và xử lý một số các hành vi gây mất an toàn thông tin, song việc ngăn chặn, xử lý còn gặp nhiều khó khăn. Luật an toàn thông tin mạng đã đưa ra quy định về việc bảo vệ mạng và hệ thống thông tin khỏi những nguy cơ bị tấn công, đồng thời có thể đáp ứng nhu cầu ngày càng cao của xã hội.

IV. NỘI DUNG CƠ BẢN CỦA LUẬT AN TOÀN THÔNG TIN MẠNG

Luật an toàn thông tin mạng tập trung vào các nội dung nhằm đảm bảo 03 thuộc tính của thông tin là tính bí mật, nguyên vẹn và khả dụng; ngăn chặn việc giả mạo, lợi dụng điểm yếu, lỗ hổng nhằm phát tán phần mềm độc hại, tấn công mạng làm ảnh hưởng đến thông tin và hệ thống thông tin, cụ thể như sau:

1. Chương I. Những quy định chung

Chương này quy định về phạm vi điều chỉnh, đối tượng áp dụng, giải thích từ ngữ, nguyên tắc bảo đảm an toàn thông tin mạng, chính sách của nhà nước, hợp tác quốc tế, những hành vi bị cấm trong hoạt động an toàn thông tin mạng và xử lý vi phạm pháp luật về an toàn thông tin mạng.

Về phạm vi điều chỉnh: Luật quy định về hoạt động an toàn thông tin mạng, quyền, trách nhiệm của cơ quan, tổ chức, cá nhân trong việc bảo đảm an toàn thông tin mạng; mật mã dân sự; tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin mạng; kinh doanh trong lĩnh vực an toàn thông tin mạng; phát triển nguồn nhân lực an toàn thông tin mạng; quản lý nhà nước về an toàn thông tin mạng.

Về đối tượng áp dụng: Do hoạt động an toàn thông tin có thể liên quan đến hợp tác quốc tế, đặc biệt là hoạt động tham gia đảm bảo an toàn thông tin của các cơ quan, tổ chức và cá nhân Việt Nam; tổ chức, cá nhân nước ngoài, đối tượng của Luật an toàn thông tin mạng được quy định gồm cơ quan, tổ chức, cá nhân Việt Nam và tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động an toàn thông tin tại Việt Nam.

Luật an toàn thông tin mạng đã giải thích một số từ ngữ như khái niệm an toàn thông tin mạng, mạng, hệ thống thông tin, hệ thống thông tin quan trọng quốc gia, chủ quản hệ thống thông tin, xâm phạm an toàn thông tin mạng, sự cố an toàn thông tin mạng, rủi ro an toàn thông tin mạng, đánh giá rủi ro an toàn thông tin mạng, quản lý rủi ro an toàn thông tin mạng, phần mềm độc hại, hệ thống lọc phần mềm độc hại, địa chỉ điện tử, xung đột thông tin, thông tin cá nhân, chủ thể thông tin cá nhân, xử lý thông tin cá nhân, mật mã dân sự, sản phẩm an toàn thông tin mạng, dịch vụ an toàn thông tin mạng.

Trong đó, khái niệm an toàn thông tin mạng tại Luật này được hiểu 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.

Trong Chương này, Luật an toàn thông tin mạng cũng quy định rõ 04 nguyên tắc cơ bản trong bảo đảm an toàn thông tin: Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng. Hoạt động an toàn thông tin của cơ quan tổ chức, cá nhân phải phù hợp với quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội; tổ chức, cá nhân tham gia hoạt động trên mạng không được xâm phạm an toàn thông tin của tổ chức, cá nhân khác; tổ chức, cá nhân tham gia hoạt động an toàn thông tin có trách nhiệm phối hợp với cơ quan quản lý nhà nước có thẩm quyền và với tổ chức, cá nhân khác trong việc bảo đảm an toàn thông tin; xử lý sự cố thông tin phải đảm bảo quyền và lợi ích hợp pháp của cá nhân, tổ chức, không xâm phạm đến đời sống riêng tư của cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức; hoạt động bảo đảm an toàn thông tin phải được thực hiện thường xuyên, liên tục, kịp thời và có hiệu quả.

Về chính sách của nhà nước về an toàn thông tin: Tập trung nguồn lực; đẩy mạnh đào tạo phát triển nguồn nhân lực; khuyến khích nghiên cứu và phát triển, hỗ trợ xuất khẩu, mở rộng thị trường cho sản phẩm, dịch vụ và chính sách bảo đảm môi trường cạnh tranh lành mạnh, khuyến khích, tạo điều kiện cho tổ chức, cá nhân thuộc mọi thành phần kinh tế trong nước và nước ngoài tham gia đầu tư nghiên cứu và phát triển sản phẩm và cung cấp dịch vụ an toàn thông tin.

Về hợp tác quốc tế: Hợp tác quốc tế về an toàn thông tin tôn trọng độc lập, chủ quyền và toàn vẹn lãnh thổ quốc gia, không can thiệp vào công tác nội bộ của nhau, bình đẳng và các bên cùng có lợi; phù hợp với luật pháp quốc tế và quy định của pháp luật, cam kết quốc tế của Việt Nam, thúc đẩy phát triển kinh tế, xã hội và bảo đảm an ninh quốc gia; và ưu tiên các hoạt động hợp tác trong các lĩnh vực nghiên cứu, ứng dụng khoa học, mở rộng hợp tác quốc tế trong việc phòng, chống hành vi vi phạm pháp luật về an toàn thông tin mạng, điều tra xử lý sự cố an toàn thông tin mạng, ngăn chặn lợi dụng mạng để khủng bố và các hoạt động động hợp tác quốc tế khác có liên quan.

Về các hành vi bị nghiêm cấm: Luật nghiêm cấm các hành vi ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy cập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật; Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới

khả năng truy nhập hệ thống thông tin của người sử dụng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin; phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo; thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin của người khác, lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân; Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của các cơ quan, tổ chức, cá nhân; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp.

2. Chương II. Bảo đảm an toàn thông tin mạng

Chương này gồm 04 mục và 21 Điều, trong đó có các mục đặc biệt quan trọng và đã được nghiên cứu kỹ là *Bảo vệ thông tin cá nhân* và *Bảo vệ hệ thống thông tin*, đây là hai vấn đề nhạy cảm được nhiều đại biểu Quốc hội quan tâm.

Về bảo vệ thông tin cá nhân: Cá nhân có trách nhiệm tự bảo vệ thông tin cá nhân của mình và có ý thức tuân thủ quy định của pháp luật về cung cấp thông tin cá nhân khi sử dụng dịch vụ trên mạng. Mục này còn quy định trách nhiệm của tổ chức, cá nhân trong việc xử lý thông tin cá nhân và trách nhiệm của cơ quan nhà nước trong việc bảo mật, lưu trữ thông tin cá nhân do mình thu thập.

Về nguyên tắc bảo vệ thông tin cá nhân: Cá nhân phải có ý thức tự bảo vệ thông tin cá nhân của mình và tuân thủ quy định của pháp luật về cung cấp thông tin cá nhân khi sử dụng dịch vụ trên mạng; tổ chức, cá nhân xử lý thông tin cá nhân có trách nhiệm bảo vệ an toàn thông tin đối với thông tin cá nhân do mình xử lý; việc bảo vệ thông tin cá nhân thực hiện theo quy định của Luật này và quy định của pháp luật liên quan. Ngoài ra, việc xử lý thông tin cá nhân phục vụ mục đích bảo đảm quốc phòng, an ninh, trật tự an toàn xã hội và chỉ để phục vụ nhu cầu sử dụng cá nhân đơn thuần không thuộc phạm vi điều chỉnh của luật này.

Về bảo vệ hệ thống thông tin: Để có thể đảm bảo an toàn thông tin một cách hiệu quả thì trước hết cần phải xác định cấp độ của hệ thống thông tin, bao gồm 5 cấp độ (từ cấp 1 đến 5). Trong đó, cấp độ 1 là cấp độ nhẹ nhất, khi bị phá hoại sẽ làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân nhưng không làm tổn hại tới lợi ích công cộng, trật tự, an toàn xã hội, quốc phòng, an ninh quốc gia; còn cấp độ 05 là cấp độ nặng nhất, khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia.

3. Chương III. Mật mã dân sự

Chương này quy định các nội dung liên quan đến sản phẩm, dịch vụ mật mã dân sự và các hoạt động có liên quan đến kinh doanh sản phẩm, dịch vụ mật mã dân sự.

Kinh doanh sản phẩm mật mã dân sự là ngành nghề sản xuất cần có sự quản lý của nhà nước. Vì vậy, doanh nghiệp sản xuất sản phẩm mật mã dân sự phải được cơ quan quản lý mật mã dân sự cấp phép.

4. Chương IV. Tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng

Chương này quy định các nội dung về tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng; quản lý tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng và chứng nhận, công bố hợp quy và đánh giá, kiểm định an toàn thông tin mạng.

Trong đó, tiêu chuẩn an toàn thông tin mạng bao gồm tiêu chuẩn quốc tế, tiêu chuẩn khu vực, tiêu chuẩn nước ngoài, tiêu chuẩn quốc gia và tiêu chuẩn cơ sở đối với hệ thống thống tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an toàn thông tin mạng được công bố, thừa nhận áp dụng tại Việt Nam. Quy chuẩn kỹ thuật an toàn thông tin mạng gồm quy chuẩn kỹ thuật quốc gia và quy chuẩn kỹ thuật địa phương đối với hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an toàn thông tin mạng phù hợp với quy chuẩn ký thuật an toàn thông tin mạng.

Trên cơ sở phân loại tiêu chuẩn kĩ thuật và quy chuẩn kĩ thuật, Luật quy định cụ thể quy trình chứng nhận hợp chuẩn, quy trình chứng nhận hợp quy đồng thời xác định rõ trách nhiệm của các Bộ, ngành, địa phương trong việc quản lý tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng. Trong đó, Bộ khoa học công nghệ đóng vai trò là cơ quan chủ trì, phối hợp với các cơ quan có liên quan tổ chức thẩm định và công bố tiêu chuẩn quốc gia về an toàn thông tin mạng theo quy định của pháp luật về tiêu chuẩn, quy chuẩn kĩ thuật.

5. Chương V. Kinh doanh trong lĩnh vực an toàn thông tin mạng

Đây là lĩnh vực rất mới, hành lang pháp lý cho hoạt động kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng còn chưa đầy đủ, nên Luật an toàn thông tin mạng hướng tới việc hoàn thiện hành lang pháp lý đảm bảo thông thoáng, công bằng, phù hợp với thông lệ quốc tế, thúc đẩy thị trường phát triển bền vững. Chương này gồm có 02 mục là:

- Cấp giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng. Theo đó kinh doanh trong lĩnh vực an toàn thông tin được quy định tại Điều 40 là loại hình kinh doanh có điều kiện bao gồm kinh doanh sản phẩm an toàn thông tin và kinh doanh dịch vụ an toàn thông tin cần phải tuân thủ theo pháp

luật về ngành nghề kinh doanh có điều kiện. Quy định về sản phẩm an toàn thông tin lưu hành trên thị trường là yếu tố quan trọng nhằm đảm bảo an toàn thông tin và hệ thống thông tin vì vậy đối với mọi sản phẩm an toàn thông tin được lưu hành trên thị trường đều phải được Bộ Thông tin và Truyền thông cấp giấy chứng nhận lưu hành, đây là biện pháp nhằm quản lý chặt các sản phẩm có tính chuyên dụng.

Hoạt động sản xuất, kinh doanh, dịch vụ cũng như trong các hoạt động sinh hoạt của đời sống xã hội ít nhiều đều có liên quan đến công nghệ, hệ thống, ngay cả sinh hoạt hàng ngày của người dân. Các cá nhân, tổ chức luôn phải đối mặt với nhiều loại hình tấn công trên mạng, mức độ ngày càng thường xuyên hơn như làm biến dạng trang tin, lừa đảo trên mạng, tấn công từ chối dịch vụ, phát tán mã độc hại và vi-rút máy tính, thư rác, đánh cắp thông tin, phá hoại dữ liệu, làm gián đoạn và phá rối hoạt động của các hệ thống thông tin, phần mềm gián điệp, tấn công hệ thống ngân hàng và mạng bán hàng trực tuyến, tin nhắn lừa đảo và ý thức về bảo vệ thông tin, dữ liệu của tổ chức, cá nhân trên môi trường mạng chưa cao nên cần phải có các cơ quan chuyên môn kiểm soát qua các thủ tục cấp phép, giấy chứng nhận...

Các loại giấy phép, giấy chứng nhận đủ điều kiện quy định trong Luật sẽ giảm dần hoặc khoanh hẹp hơn với một số đối tượng nhất định với điều kiện ý thức của người dân đã tăng lên hoặc hoạt động kiểm soát của cơ quan nhà nước tốt hơn về lĩnh vực an toàn thông tin. Các thủ tục này là các quy định ràng buộc các tổ chức, cá nhân có ý thức chủ động bảo vệ thông tin của mình trên môi trường mạng. Tuy nhiên, thủ tục này cũng có những nguy cơ nhất định như làm cho cơ quan quản lý "lơ là" và tin tưởng, thiếu kiểm soát thường xuyên đối với những tổ chức, cá nhân đã được cấp phép.

- Quản lý nhập khẩu sản phẩm an toàn thông tin mạng: Mục này quy định về nguyên tắc quản lý nhập khẩu sản phẩm an toàn thông tin mạng; sản phẩm nhập khẩu theo giấy phép an toàn thông tin mạng.

6. Chương VI. Phát triển nguồn nhân lực an toàn thông tin mạng

Chương này quy định về các hoạt động đào tạo, bồi dưỡng nghiệp vụ về an toàn thông tin mạng, văn bằng, chứng chỉ đào tạo về an toàn thông tin mạng tại Việt Nam, thể hiện đúng đường lối chủ trương của Đảng và Nhà nước ta trong thời gian vừa qua.

Để có kiến thức chuyên ngành về an toàn thông tin và nâng cao trình độ cho cán bộ quản lý kỹ thuật về an toàn thông tin thì chủ quản hệ thống thông tin sử dụng nguồn vốn ngân sách nhà nước phải có trách nhiệm đào tạo, bồi dưỡng kiến thức nghiệp vụ cho các đối tượng này. Đồng thời các Bộ chức năng phải

xây dựng kế hoạch và tổ chức thực hiện đào tạo, bồi dưỡng kiến thức, nghiệp vụ về an toàn thông tin cho cán bộ, công chức, viên chức trong cơ quan, tổ chức nhà nước. Ngoài quy định chung về đào tạo, bồi dưỡng nghiệp vụ an toàn thông tin mạng, Điều 50 quy định cụ thể về văn bằng, chứng chỉ đào tạo an toàn thông tin mạng, trong đó xác định rõ thẩm quyền của các cơ sở giáo dục đại học, cơ sở giáo dục nghề nghiệp trong phạm vi nhiệm vụ, quyền hạn của mình cấp văn bằng, chứng chỉ đào tạo về an toàn thông tin mạng và quy định trách nhiệm của các Bộ, ngành liên quan trong việc cấp văn bằng giáo dục đại học, văn bằng chứng chỉ giáo dục nghề nghiệp về an toàn thông tin mạng do tổ chức nước ngoài cấp.

7. Chương VII. Quản lý nhà nước về an toàn thông tin mạng

Mặc dù các Chương, Điều của Luật đã có những quy định về phân công trách nhiệm cụ thể của các Bộ, ngành, địa phương trong việc chỉ đạo, phối hợp tổ chức các biện pháp đảm bảo an toàn thông tin, Chương VII của Luật vẫn hệ thống hoá thẩm quyền và trách nhiệm của cơ quan quản lý nhà nước các cấp, qua đó giúp các cơ quan này có thể tham chiếu một cách hệ thống, cơ bản về các quyền hạn và trách nhiệm của mình trong quá trình đảm bảo an toàn thông tin bên cạnh việc xác định các nội dung cụ thể xoay quanh nội dung quản lý nhà nước về an toàn thông tin mạng, bao gồm các hoạt động xây dựng chiến lược, quy hoạch, kế hoạch; hoạt động xây dựng và hoàn thiện thể chế; tổ chức thực thi các văn bản; quản lý nhà nước trên các lĩnh vực; hoạt động thanh tra kiểm tra; hợp tác quốc tế...

V. TỔ CHỨC THỰC HIỆN

1. Ban hành văn bản quy định chi tiết và hướng dẫn thi hành Luật:

Ngay sau khi Luật an toàn thông tin mạng được Quốc hội thông qua, Bộ Thông tin và Truyền thông, Bộ Quốc phòng, Bộ Công an và các đơn vị có liên quan đã và đang xây dựng các văn bản dưới Luật nhằm triển khai và thực hiện các nội dung đã được quy định tại Luật an toàn thông tin mạng, bao gồm:

- Nghị định quy định bảo vệ hệ thống thông tin theo cấp độ an toàn thông tin.

- Nghị định quy định về điều kiện cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng.

- Nghị định quy định chi tiết về ngăn chặn xung đột thông tin trên mạng.

- Nghị định quy định chi tiết về trách nhiệm thực hiện và các biện pháp ngăn chặn hoạt động sử dụng mạng để khủng bố.

- Nghị định quy định danh mục sản phẩm, dịch vụ mật mã dân sự và quy định chi tiết về kinh doanh sản phẩm, dịch vụ mật mã dân sự.

- Nghị định quy định danh mục sản phẩm mật mã dân sự xuất khẩu, nhập khẩu theo giấy phép và quy định chi tiết về xuất khẩu, nhập khẩu sản phẩm mật mã dân sự.

- Nghị định quy định danh mục sản phẩm, dịch vụ an toàn thông tin mạng. Nghị định quy định danh mục sản phẩm an toàn thông tin mạng nhập khẩu.

Quyết định của Thủ tướng Chính phủ về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

- Quyết định của Thủ tướng Chính phủ về danh mục hệ thống thông tin quan trọng quốc gia.

- Thông tư của Bộ Thông tin và Truyền thông quy định chi tiết về điều phối ứng cứu sự cố an toàn thông tin mạng.

- Thông tư của Bộ Thông tin và Truyền thông quy định chi tiết về trình tự, thủ tục, hồ sơ cấp giấy phép nhập khẩu sản phẩm an toàn thông tin mạng theo giấy phép.

- Định hướng về công tác triển khai áp dụng, thi hành sau khi Luật có hiệu lực và các văn bản dưới luật được ban hành

Tiếp tục triển khai Quy hoạch về phát triển an toàn thông tin số quốc gia đến năm 2020, mục tiêu của Quy hoạch là đến năm 2020 các ứng dụng về Chính phủ điện tử và thương mại điện tử đều được đảm bảo an toàn thông tin ở mức cao nhất;

Triển khai Đề án đào tạo và phát triển nguồn nhân lực an toàn, an ninh thông tin đến năm 2020. Theo đó, triển khai các hoạt động nhằm thúc đẩyvà phát triển nguồn nhân lực về an toàn thông tin trong nước thông qua các hoạt động đã được đề ra như cử cán bộ đi đào tạo, tập huấn nhằm nâng cao trình độ tại các nước phát triển về an toàn thông tin bên cạnh đó tập trung đầu tư phát triển các cơ sở đào tạo về an toàn thông tin đã được nêu ra trong Đề án này;

Thực hiện Đề án Tuyên truyền nâng cao nhận thức và trách nhiệm về an toàn thông tin mục tiêu đến năm 2020 qua các hình thức tuyên truyền, phổ biến sẽ giúp tăng cường nhận thức và ý thức chấp hành về an toàn thông tin tại Việt Nam. Giảm thiểu số sự cố mất an toàn thông tin xảy ra vì lí do bắt nguồn từ nhận thức yếu kém về các nguy cơ mất an toàn thông tin của con người. Đồng thời tuyên truyền, phổ biến kiến thức cơ bản cho người sử dụng trong việc phòng tránh mất an toàn thông tin.

2. Dự kiến kế hoạch phổ biến, giáo dục pháp luật

Nhằm triển khai thực hiện Luật an toàn thông tin mạng một cách đồng bộ, thống nhất, hiệu quả, nâng cao nhận thức về an toàn thông tin mạng, Bộ Thông

tin và Truyền thông là đơn vị trực tiếp chịu trách nhiệm phổ biến Luật an toàn thông tin mạng, gồm các nhiệm vụ cụ thể như sau:

- Đăng tải toàn văn nội dung Luật an toàn thông tin mạng trên trang thông tin điện tử của Chính phủ và Bộ Thông tin và Truyền thông.

- Tổ chức biên soạn tài liệu và đề cương phổ biến Luật.

- Tổ chức các hội nghị phổ biến và tập huấn các nội dung cơ bản của Luật cho các đối tượng có liên quan trên phạm vi cả nước.

- Tổ chức tập huấn chuyên sâu các nội dung và tinh thần của Luật.

- Chỉ đạo, hướng dẫn các cơ quan báo chí, thông tin và truyền thông tiến hành tuyên truyền, phổ biến nội dung, tinh thần và ý nghĩa của Luật an toàn thông tin mạng.

- Hỗ trợ giải đáp, hướng dẫn về các nội dung cơ bản của Luật an toàn thông tin mạng.