TÀI LIỆU TUYÊN TRUYỀN VỀ LUẬT AN NINH MẠNG

1. Sự cần thiết phải ban hành Luật An ninh mạng

Với sự phát triển như vũ bão của khoa học công nghệ, không gian mạng trở thành một bộ phận cấu thành không thể thiếu và đóng vai trò quan trọng trong xây dựng xã hội thông tin và phát triển kinh tế tri thức. Sự phát triển bùng nổ của công nghệ mang tính đột phá như trí tuệ nhân tạo, Internet của vạn vật, máy tính lượng tử, điện toán đám mây, hệ thống dữ liệu lớn, hệ thống dữ liệu nhanh… đã làm không gian mạng thay đổi sâu sắc cả về chất và lượng, được dự báo sẽ mang lại những lợi ích chưa từng có cho xã hội loài người nhưng cũng làm xuất hiện những nguy cơ tiềm ẩn vô cùng lớn. Nhiều quốc gia đã nhận thức rõ về những mối đe dọa đối với an ninh mạng, coi đây là thách thức mới, mối đe dọa mới có tầm quan trọng và nguy hiểm cao nên đã cụ thể hóa thành các văn bản chính sách, văn bản pháp luật như luật hoặc văn bản dưới luật tại hơn 80 quốc gia, tổ chức, liên minh quốc tế như Mỹ, Anh, Đức, Hà Lan, Pháp, Canada, Hàn Quốc, NATO… nhằm tạo ra các thiết chế, cơ sở pháp lý chống lại các nguy cơ đe dọa đến an ninh quốc gia từ không gian mạng; thành lập các lực lượng chuyên trách về an ninh mạng, tình báo mạng, chiến tranh mạng, phòng chống khủng bố mạng và tội phạm mạng. Chỉ trong vòng 06 năm trở lại đây, đã có 23 quốc gia trên thế giới ban hành trên 40 văn bản luật về an ninh mạng.

Ở nước ta, ứng dụng và phát triển mạnh mẽ công nghệ thông tin trong các lĩnh vực của đời sống đã góp phần to lớn đẩy nhanh quá trình công nghiệp hóa, hiện đại hóa đất nước, phát triển kinh tế, văn hóa, xã hội, nâng cao chất lượng y tế, giáo dục, phát huy sức sáng tạo và quyền làm chủ của nhân dân, giữ vững an ninh, quốc phòng. Tuy nhiên, vẫn còn những tồn tại, hạn chế về an ninh mạng cần khắc phục như: **(1)** Tiềm lực quốc gia về an ninh mạng của nước ta chưa đủ mạnh, chưa huy động, khai thác được sức mạnh tổng hợp để đối phó với các mối đe dọa trên không gian mạng. **(2)** Không gian mạng và một số loại hình dịch vụ, ứng dụng công nghệ thông tin đang bị các thế lực thù địch, phản động sử dụng để thực hiện âm mưu tiến hành "cách mạng màu", "cách mạng đường phố", "diễn biến hòa bình" nhằm xóa bỏ chế độ chính trị ở nước ta. Tình trạng đăng tải thông tin sai sự thật, làm nhục, vu khống tổ chức, cá nhân tràn lan trên không gian mạng nhưng chưa có biện pháp quản lý hữu hiệu, dẫn tới nhiều hậu quả đáng tiếc về nhân mạng, tinh thần, thậm chí ảnh hưởng tới chủ quyền, lợi ích, an ninh quốc gia, trật tự an toàn xã hội. **(3)** Ngày càng xuất hiện nhiều cuộc tấn công mạng với quy mô lớn, cường độ cao, gia tăng về tính chất nghiêm trọng, mức độ nguy hiểm đe dọa trực tiếp đến an ninh quốc gia và trật tự an toàn xã hội. Khủng bố mạng nổi lên như một thách thức đe dọa nghiêm trọng tới an ninh quốc gia. Hoạt động phạm tội trên không gian mạng ngày càng gia

tăng về số vụ, thủ đoạn tinh vi gây thiệt hại nghiêm trọng về kinh tế, ảnh hưởng đến tư tưởng, văn hóa, xã hội. **(4)** Hệ thống thông tin quan trọng về an ninh quốc gia chưa được xác định và bảo vệ bằng các biện pháp tương xứng. Do chưa xác định nội hàm sự cố an ninh mạng nên khi xảy ra các sự cố nguy hại, ảnh hưởng tới chủ quyền, lợi ích, an ninh quốc gia, trật tự an toàn xã hội, việc triển khai hoạt động ứng phó, xử lý, khắc phục hậu quả của cơ quan chức năng có liên quan rất lúng túng, chưa có quy trình thống nhất, cơ quan có trách nhiệm bảo vệ an ninh mạng chưa thể chủ động triển khai các biện pháp, phương án phù hợp. **(5)** Tình hình lộ, lọt bí mật nhà nước qua không gian mạng rất đáng lo ngại, nhiều văn bản thuộc bí mật nhà nước bị đăng tải trên không gian mạng. Một trong những nguyên nhân quan trọng dẫn tới tình trạng trên là do nhận thức của các cơ quan, doanh nghiệp và cá nhân về bảo vệ bí mật nhà nước trên không gian mạng còn hạn chế, ý thức trách nhiệm của nhiều cán bộ, nhân viên trong bảo mật thông tin trên không gian mạng còn chưa cao, chế tài xử phạt chưa đủ răn đe. **(6)** Sự phụ thuộc vào thiết bị công nghệ thông tin có nguồn gốc từ nước ngoài. Không gian mạng đang ứng dụng sâu rộng vào mọi lĩnh vực của đời sống xã hội, tuy nhiên, sự phụ thuộc vào trang thiết bị công nghệ thông tin xuất xứ từ nước ngoài là mối đe dọa tiềm tàng đối với an ninh mạng nếu xảy ra xung đột. Để tránh bị tin tặc tấn công, thu thập thông tin, hoạt động tình báo, một số sản phẩm, dịch vụ mạng cần đáp ứng các tiêu chuẩn, quy chuẩn nhất định, nhất là khi các sản phẩm, dịch vụ này được sử dụng trong hệ thống thông tin quan trọng và an ninh quốc gia, địa điểm cơ yếu, bảo mật, chứa đựng bí mật nhà nước. **(7)** Hệ thống văn bản quy phạm pháp luật về an ninh mạng chưa được xây dựng, các văn bản hiện hành chưa đáp ứng được yêu cầu phòng ngừa, đấu tranh, xử lý các hành vi sử dụng không gian mạng vi phạm pháp luật.

Thực trạng trên đã đặt đất nước ta trước những nguy cơ:

Một là, sự phát triển của mạng xã hội góp phần quan trọng phát triển kinh tế - xã hội, song cũng tạo môi trường thuận lợi cho các hoạt động tác động, chuyển hóa chính trị, khủng bố.

Hai là, sự phát triển của trí tuệ nhân tạo đã và đang tạo ra những thành tựu khoa học công nghệ vượt trội, đóng vai trò ngày càng quan trọng trong nhiều lĩnh vực của đời sống xã hội nhưng cũng được dự báo sẽ gây nên "thảm họa" nếu không được kiểm soát chặt chẽ.

Ba là, các thiết bị kết nối internet ngày càng phổ biến không chỉ mang lại những lợi ích to lớn cho cuộc sống con người, phát triển kinh tế - xã hội, bảo đảm quốc phòng - an ninh mà còn có thể bị sử dụng để tiến hành các cuộc tấn công mạng quy mô lớn.

Bốn là, các cuộc tấn công mạng có chủ đích (Advanced Peristent Threat - APT) không chỉ có thể phá hoại các mục tiêu, công trình quan trọng về an

ninh quốc gia mà còn chiếm đoạt thông tin, tài liệu bí mật, chiếm đoạt để sử dụng các hệ thống dữ liệu lớn, dữ liệu nhanh phục vụ các ý đồ chính trị và hoạt động phạm tội.

Thực trạng, nguy cơ trên đã đặt ra yêu cầu bức thiết phải xây dựng và ban hành văn bản luật về an ninh mạng để phòng ngừa, đấu tranh, xử lý các hành vi sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

2. Mục đích xây dựng Luật An ninh mạng

- Hoàn thiện cơ sở pháp lý ổn định về an ninh mạng 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 ninh mạng, phát triển lĩnh vực an ninh mạng 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 chủ quyền, lợi ích, an ninh quốc gia, quyền và lợi ích hợp pháp của tổ chức, cá nhân tham gia hoạt động trên không gian mạng, xây dựng môi trường không gian mạng lành mạnh.

- Triển khai công tác an ninh mạng trên phạm vi toàn quốc, đẩy mạnh công tác giám sát, dự báo, ứng phó và diễn tập ứng phó sự cố an ninh mạng, bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia; đảm bảo hiệu quả công tác quản lý nhà nước trong lĩnh vực này.

- Nâng cao năng lực tự chủ về an ninh mạng, hoàn thiện chính sách nghiên cứu, phát triển chiến lược, chia sẻ thông tin về an ninh mạng.

- Mở rộng hợp tác quốc tế về an ninh mạng trên cơ sở tôn trọng độc lập, chủ quyền, bình đẳng, cùng có lợi, phù hợp với pháp luật trong nước và điều ước quốc tế mà nước ta tham gia ký kết.

3. Nội dung cơ bản của Luật An ninh mạng

Luật An ninh mạng gồm 07 chương, 43 điều, quy định những nội dung cơ bản về bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh mạng; triển khai hoạt động bảo vệ an ninh mạng và quy định trách nhiệm của cơ quan, tổ chức, cá nhân.

Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia là một trong những nội dung đặc biệt quan trọng của Luật An ninh mạng. Quy định đầy đủ các biện pháp, hoạt động bảo vệ tương xứng với mức độ quan trọng của hệ thống thông tin này, trong đó nêu ra tiêu chí xác định, lĩnh vực liên quan, quy định các biện pháp như thẩm định an ninh mạng, đánh giá

điều kiện, kiểm tra, giám sát an ninh và ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.

Để bảo vệ tối đa quyền và lợi ích hợp pháp của tổ chức, cá nhân, Luật An ninh mạng đã dành 01 chương (Chương III) quy định đầy đủ các biện pháp phòng ngừa, đấu tranh, xử lý nhằm loại bỏ các nguy cơ đe dọa, phát hiện và xử lý hành vi vi phạm pháp luật, bao gồm: phòng ngừa, xử lý thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế; phòng, chống gián điệp mạng, bảo vệ thông tin bí mật nhà nước, bí mật công tác, thông tin cá nhân trên không gian mạng; phòng ngừa, xử lý hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh, trật tự; phòng, chống tấn công mạng; phòng, chống khủng bố mạng; phòng, chống chiến tranh mạng; phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng; đấu tranh bảo vệ an ninh mạng. Đây là hành lang pháp lý vững chắc để người dân có thể yên tâm buôn bán, kinh doanh hay hoạt động trên không gian mạng.

Chương IV của Luật An ninh mạng tập trung quy định về triển khai hoạt động bảo vệ an ninh mạng một cách đồng bộ, thống nhất từ Trung ương tới địa phương, trọng tâm là các cơ quan nhà nước và tổ chức chính trị, quy định rõ các nội dung triển khai, hoạt động kiểm tra an ninh mạng đối với hệ thống thông tin của các cơ quan, tổ chức này. Cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế cũng là một trong những đối tượng được bảo vệ trọng điểm. Với các quy định chặt chẽ, sự tham gia đồng bộ của cơ quan nhà nước, doanh nghiệp và tổ chức, cá nhân, việc sử dụng thông tin để vu khống, làm nhục, xâm phạm danh dự, nhân phẩm, uy tín của người khác sẽ được xử lý nghiêm minh. Các hoạt động nghiên cứu, phát triển an ninh mạng, phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng nhằm bảo vệ an ninh mạng, nâng cao năng lực tự chủ về an ninh mạng và bảo vệ trẻ em trên không gian mạng cũng được quy định chi tiết trong Chương này.

Hiện nay, dữ liệu của nước ta trên không gian mạng đã và đang bị sử dụng tràn lan với mục đích lợi nhuận mà Nhà nước chưa có đủ hành lang pháp lý để quản lý, thậm chí là bị sử dụng vào các âm mưu chính trị hoặc vi phạm pháp luật. Để quản lý chặt chẽ, bảo vệ nghiêm ngặt dữ liệu của nước ta trên không gian mạng, Luật An ninh mạng đã quy định doanh nghiệp trong và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ giá trị 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.

Nguồn nhân lực bảo vệ an ninh mạng là một trong những yếu tố quyết định sự thành bại của công tác bảo vệ an ninh mạng. Chương V Luật An ninh mạng đã quy định đầy đủ các nội dung bảo đảm triển khai hoạt động bảo vệ an ninh mạng, xác định lực lượng chuyên trách bảo vệ an ninh mạng, ưu tiên đào tạo nguồn nhân lực an ninh mạng chất lượng cao, chú trọng giáo dục, bồi dưỡng, phổ biến kiến thức về an ninh mạng.

Trách nhiệm của cơ quan, tổ chức, cá nhân cũng được quy định rõ trong Luật An ninh mạng, tập trung vào trách nhiệm của lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Bộ Công an, Bộ Quốc phòng. Theo chức năng, nhiệm vụ được giao, các bộ, ngành chức năng, ủy ban nhân dân cấp tỉnh có trách nhiệm thực hiện đồng bộ các biện pháp được phân công để hướng tới một không gian mạng ít nguy cơ, hạn chế tối đa các hành vi vi phạm pháp luật trên không gian mạng.

Mặc dù được chuẩn bị kỹ lưỡng, được đa số Đại biểu Quốc hội tán thành, nhưng do đây là đạo luật có quy định về phòng ngừa, đấu tranh, xử lý trực tiếp các hoạt động xâm phạm an ninh quốc gia trên không gian mạng nên vẫn còn có những ý kiến băn khoăn về nội dung Luật. Một số đối tượng chống đối đã có hoạt động tuyên truyền, xuyên tạc với những luận điệu như "chống lại loài người", "bịt miệng dân chủ", "đàn áp bất đồng chính kiến", "tạo rào cản kinh doanh", "tăng chi phí cho doanh nghiệp", "thêm giấy phép con", "lạm quyền", "cấm sử dụng Facebook, Google". Đây là những thông tin hoàn toàn bịa đặt, xuyên tạc, với mục đích cản trở hoặc gây tâm lý hoang mang, nghi ngờ trong quần chúng nhân dân đối với chủ trương của Đảng, chính sách, pháp luật của Nhà nước về an ninh mạng. Luật An ninh mạng không có những quy định nêu trên, không tạo rào cản, không tăng thủ tục hành chính, không cấp giấy phép con và không cản trở hoạt động bình thường, đúng luật của các tổ chức, cá nhân.

4. Ý nghĩa, tác dụng của Luật An ninh mạng

Luật An ninh mạng được thông qua có ý nghĩa, tác dụng sau đây:

Thứ nhất, là cơ sở pháp lý quan trọng để bảo vệ an ninh quốc gia; xử lý đối với các hành vi vi phạm pháp luật, như: (*) Chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, bao gồm sử dụng không gian mạng tổ chức, hoạt động, cấu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, ví dụ như thông tin kích động lôi kéo tụ tập đông người, gây rối an ninh trật tự, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức, gây mất ổn định về an ninh trật tự... (*) Các hành vi xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc; (*) Các hành vi phát tán thông tin gây hại cho tổ chức, cá nhân, gồm: thông tin sai sự thật gây hoang mang trong nhân dân, gây

thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác; (*) Các hành vi xâm phạm trật tự an toàn xã hội như sử dụng không gian mạng để hoạt động mại dâm, tệ nạn xã hội, mua bán người; đăng tải thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe cộng đồng, xúi giục, lôi kéo, kích động người khác phạm tội. (Những hành vi này đã được quy định rải rác, cụ thể trong 29 Điều của Bộ luật Hình sự năm 2015, sửa đổi năm 2017). (*) Các hành vi tấn công mạng, gián điệp mạng, khủng bố mạng và liên quan như sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoạt động của mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử...

Thứ hai, nhằm bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia. Hệ thống thông tin quan trọng về an ninh quốc gia được quy định trong Luật An ninh mạng là hệ thống thông tin khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ xâm phạm nghiêm trọng an ninh mạng. Với tiêu chí như trên, hệ thống thông tin quan trọng về an ninh quốc gia được xác định trong các lĩnh vực quan trọng đặc biệt đối với quốc gia như quân sự, an ninh, ngoại giao, cơ yếu; trong lĩnh vực đặc thù như lưu trữ, xử lý thông tin thuộc bí mật nhà nước; phục vụ hoạt động của các công trình quan trọng liên quan tới an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia hoặc những hệ thống thông tin quan trọng trong các lĩnh vực năng lượng, tài chính, ngân hàng, viễn thông, giao thông vận tải, tài nguyên và môi trường, hóa chất, y tế, văn hóa, báo chí. Chính phủ sẽ quy định cụ thể những hệ thống thông tin nào trong các lĩnh vực nêu trên thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia được giao cho lực lượng chuyên trách bảo vệ an ninh mạng, trực tiếp là lực lượng An ninh mạng thuộc Bộ Công an, lực lượng Tác chiến Không gian mạng thuộc Bộ Quốc phòng. Để bảo đảm phù hợp với hệ thống pháp luật trong nước, Luật An ninh mạng cũng giao Chính phủ quy định cụ thể việc phối hợp giữa Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông, Ban Cơ yếu Chính phủ, các bộ, ngành chức năng trong việc thẩm định, đánh giá, kiểm tra, giám sát, ứng phó, khắc phục sự cố đối với hệ thống thông tin quan trọng về an ninh quốc gia.

Thứ ba, nhằm phòng, chống tấn công mạng. Luật An ninh mạng là văn bản Luật đầu tiên quy định khái niệm của hoạt động "tấn công mạng". Theo đó *"Tấn công mạng* là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để phá hoại, gây gián đoạn hoạt động của mạng viễn thông,

mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử". Đồng thời, quy định các nhóm hành vi cụ thể liên quan tới tấn công mạng tại Điều 17, 18, 19, 20 và Điều 21; quy định cụ thể các nhóm giải pháp cụ thể để phòng, chống tấn công mạng, quy định trách nhiệm cụ thể của cơ quan chức năng, chủ quản hệ thống thông tin. Như vậy:

- Hệ thống thông tin của cơ quan, tổ chức, cá nhân được bảo vệ trước hoạt động tấn công mạng theo quy định của Luật An ninh mạng.

- Các hệ thống thông tin quan trọng về an ninh quốc gia được bảo vệ tương xứng với tầm quan trọng đối với an ninh quốc gia, trật tự an toàn xã hội.

- Quyền và lợi ích hợp pháp của tổ chức, cá nhân được bảo vệ trước các hành vi tấn công mạng.

- Luật An ninh mạng cũng quy định cụ thể cơ chế phối hợp phòng, chống tấn công mạng của các bộ, ngành chức năng, xác định trách nhiệm cụ thể của Bộ Công an, Bộ Quốc phòng, Ban Cơ yếu Chính phủ trong phòng, chống tấn công mạng.

BAN TUYÊN GIÁO TRUNG ƯƠNG