**THUYẾT TRÌNH VỀ LUẬT AN NINH MẠNG**

 ***Kính thưa các đồng chí đại biểu!***

 ***Thưa toàn thể hội nghị!***

Trong bối cảnh cuộc cách mạng công nghiệp 4.0, không gian mạng trở thành một bộ phận cấu thành và đóng vai trò quan trọng trong việc xây dựng một xã hội thông tin và kinh tế tri thức. Trong năm 1995, dưới 1% dân số thế giới kết nối mạng. Internet chỉ được sử dụng chủ yếu tại các nước phương Tây. Hơn 20 năm sau, con số đó đã lên đến 3,5 tỷ người, chiếm gần một nửa dân số thế giới và đang tăng với tốc độ khoảng 10 người mỗi giây. 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… đã làm không gian mạng thay đổi sâu sắc, và 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. Vì vậy, an toàn môi trường mạng đang là mối quan tâm hàng đầu của nhiều quốc gia trên thế giới.

**I. Tình hình An ninh mạng trước khi ban hành Luật An ninh mạng**

**1. Tình hình thế giới**

Trong những năm gần đây, hàng loạt vụ tấn công mạng quy mô lớn diễn ra trên toàn cầu, điển hình như vụ việc vào tháng 10/2013, Adobe đã công bố về việc hãng bị thất thoát dữ liệu bởi các Hacker. Cụ thể, có đến 2,9 triệu thông tin cá nhân từ các tài khoản bị đánh cắp từ mạng internet (bao gồm tên đăng nhập, các mật khẩu, tên thật, số thẻ tín dụng và ngày hết hạn). Ngay sau đó, tệp dữ liệu này được các tin tặc công khai trên internet với con số khủng lên đến 150 triệu (trong đó có 38 triệu tài khoản vẫn còn đang hoạt động); tin tặc Triều Tiên đã cố gắng đột nhập vào hệ thống máy tính của công ty dược phẩm Pfizer để lấy thông tin về vắc-xin và phương pháp điều trị COVID-19; hay sự việc tin tặc Trung Quốc đã nhắm mục tiêu vào phần mềm email doanh nghiệp của Microsoft để đánh cắp dữ liệu từ hơn 30.000 tổ chức trên khắp thế giới;… Mới đây nhất vào ngày 4/4/2021, Forbes cho biết số điện thoại và dữ liệu cá nhân của 533 triệu người dùng Facebook đã bị rò rỉ. Bên cạnh đó, các cuộc tấn công gần đây chống lại FireEye và SolarWinds nhấn mạnh mức độ nhạy cảm của các vấn đề chuỗi cung ứng và sự phụ thuộc vào các nhà cung cấp chức năng và dịch vụ công nghệ thông tin.

**2. Tình hình Việt Nam**

Việt Nam nằm trong nhóm các quốc gia có tốc độ phát triển Internet nhanh nhất thế giới, không gian mạng ở nước ta cũng xuất hiện nhiều nguy cơ, thách thức lớn tác động đến an ninh quốc gia và trật tự an toàn xã hội, cụ thể là:

- Các thế lực thù địch, phản động tăng cường sử dụng không gian mạng để phá hoại tư tưởng, phá hoại nội bộ, thực hiện âm mưu “diễn biến hòa bình”, gây mâu thuẫn dân tộc, kích động biểu tình, bạo loạn nhằm chuyển hóa thể chế chính trị tại Việt Nam. ***(Dẫn chứng ví dụ trong Sline)***

- Vấn nạn tin giả, thông tin sai sự thật, tin xấu, độc, làm tổn hại đến quyền và lợi ích hợp pháp của các tổ chức, cá nhân đang diễn ra nghiêm trọng.

***(Dẫn chứng ví dụ trong Sline)***

- Hệ thống mạng của nước ta nằm trong nhóm các quốc gia phải đối mặt với hoạt động tấn công mạng quy mô lớn, cường độ cao, tính chất nghiêm trọng và ngày càng nguy hiểm. Nước ta xếp thứ 20 trong các nước trên thế giới có hệ thống mạng bị tấn công bởi phần mềm độc hại, đứng thứ 8 trong số 10 quốc gia hàng đầu thế giới về tình trạng lây nhiễm mã độc cục bộ. Từ cuối năm 2015 đến nay, đã có 12.360 trang tin, cổng thông tin điện tử tên miền quốc gia (.vn) của Việt Nam bị tin tặc tấn công, thay đổi giao diện, trong đó có trên 400 trang tin, cổng thông tin điện tử của cơ quan nhà nước; có 9.763 trang tin bị tấn công bởi tin tặc nước ngoài và 2.597 trang tin bị tấn công bởi các đối tượng, nhóm tin tặc trong nước (chiếm 21%).

- Tình hình chiếm đoạt thông tin, làm lộ bí mật nhà nước, lộ thông tin cá nhân của người dùng internet diễn ra đáng lo ngại. ***(Dẫn chứng ví dụ trong Sline)***

- Hoạt động tội phạm sử dụng công nghệ cao gia tăng về số vụ, thủ đoạn tinh vi, gây thiệt hại nghiêm trọng về nhiều mặt và hệ lụy lâu dài cho xã hội, trong đó có các hoạt động tội phạm, như lừa đảo, tổ chức đánh bạc trực tuyến.

***(Dẫn chứng ví dụ trong Sline)***

- Công tác quản lý nhà nước về không gian mạng đối mặt với nhiều thách thức trước những dịch vụ mới trên mạng, như thanh toán trực tuyến, thương mại điện tử, trò chơi trực tuyến, kinh doanh tiền ảo, kinh doanh đa cấp. Đồng thời, đặt ra một số vấn đề về an ninh quốc gia, nguy cơ mất an ninh thanh toán, an ninh thông tin mạng, như nguy cơ mất an ninh thông tin mạng tạo điều kiện cho đối phương tiến hành thu thập tin tức tình báo; nguy cơ thất thu thuế, mất chủ quyền không gian thanh toán; tình trạng cạnh tranh không bình đẳng giữa các doanh nghiệp hoạt động trong lĩnh vực thanh toán, trung gian thanh toán trong và ngoài nước tạo môi trường lý tưởng cho tội phạm sử dụng công nghệ cao hoạt động phạm tội, xâm phạm trật tự quản lý kinh tế, trật tự xã hội.

- Công tác đào tạo chuyên gia an ninh mạng còn hạn chế, chưa đáp ứng yêu cầu thực tiễn đặt ra.

Dữ liệu từ Cục An ninh mạng (Bộ Công an) cho thấy thời gian qua Việt Nam chịu nhiều đợt tấn công nhằm vào các hệ thống thông tin quốc gia, phát tán thông tin sai sự thật để lừa đảo, chiếm đoạt tài sản. Các thiết bị dễ bị tấn công nhất thường là điện thoại di động, IoT *(*Internet of Things: Thuật ngữ với ý nghĩa về việc mở rộng sức mạnh của internet vượt ra ngoài khỏi phạm vi máy tính và điện thoại thông minh, kết nối tới vạn vật, các quy trình và môi trường khác).

Cục An ninh mạng - Bộ Công an đã phát hiện được 1.555 vụ tấn công vào trang/cổng thông tin điện tử có tên miền .vn (bị chèn thông điệp của tin tặc). Trong đó, 412 trang thuộc quản lý của cơ quan Nhà nước. Một số điểm khác biệt về xu hướng tấn công mạng trong năm 2021 so với trước là xuất hiện tình trạng địa chỉ IP của các khách hàng, nhà cung cấp dịch vụ Internet trong nước bị nhiễm mã độc. 6 tháng đầu năm nay, Bộ Công an đã phát hiện 2.551 vụ tấn công mạng, 5,4 triệu lượt địa chỉ IP của các cơ quan Nhà nước bị tấn công với 15 biến thể mã độc.

Ngoài ra, trên không gian mạng, các thông tin giả, tin xấu độc liên tục được đăng tải và chia sẻ tràn lan. Trong quý I và II/2021 khi dịch có diễn biến phức tạp, Bộ Công an rà soát được 221 ngàn tin, bài chứa thông tin xấu, sai sự thật được đăng trên các trang thông tin điện tử, diễn đàn, blog. Đáng chú ý, hệ lụy của những tin giả này lớn hơn nhiều khi chúng được lan truyền nhanh chóng trên mạng xã hội.

Bên cạnh đó, hoạt động của những đối tượng xấu lợi dụng không gian mạng để xâm phạm trật tự, an toàn xã hội diễn ra phức tạp ở các địa phương. Tội phạm mạng thực hiện nhiều thủ đoạn tinh vi như lập giả mạo website, trang thông tin điện tử cơ quan, doanh nghiệp; thiết lập trạm BTS giả mạo để chặn, chuyển hướng thuê bao di động người dùng nhằm thu thập dữ liệu…

Ngoài ra, tình trạng lộ lọt, mua bán thông tin, dữ liệu của người dùng cũng ghi nhận diễn biến phức tạp, điển hình là vụ lộ lọt thông tin của 35,6 triệu khách hàng của một tập đoàn lớn ở Việt Nam trong đó có cả các nhà cung cấp dịch vụ viễn thông, nhiều ngân hàng và công ty bảo hiểm, bất động sản, du lịch…gây bức xúc và thu hút sự quan tâm lớn trong nhân dân. Trong đó, có khoảng 100 triệu lượt dữ liệu người dùng Internet, tổ chức doanh nghiệp Việt Nam lộ lọt. Cùng với đó hơn 100 nghìn tài khoản mật khẩu rao bán trên chợ đen.

**II. Vị trí, vai trò của Luật An ninh mạng**

**1. Tính cấp thiết**

**Tại thời điểm Việt Nam chưa ban hành Luật An ninh mạng vẫn còn những tồn tại hạn chế về an ninh mạng cần khắc phục là:**

 **- Về thể chế: Chưa có văn bản QPPL riêng điều chỉnh về an ninh mạng. *(Chỉ có Luật An toàn thông tin, một số Nghị định về quản lý Internet…)***

 **- Chế tài xử phạt chưa đủ sức răn đe, chưa quy định biện pháp thu thập chứng cứ, dữ liệu điện tử… gây khó khăn cho thu thập, xử lý vi phạm. *(Nghị định 174/2013/NĐ-CP ngày 13/11/2013 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, công nghệ thông tin và tần số vô tuyến điện thì người có hành vi “Cung*** *cấp, trao đổi, truyền đưa hoặc lưu trữ, sử dụng thông tin số nhằm đe dọa, quấy rối, xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự, nhân phẩm, uy tín của người khác;” sẽ bị phạt tiền từ 5.000.000 đồng đến 10.000.000 đồng).*

 **- Quản lý Nhà nước đối với báo chí điện tử, mạng xã hội chưa chặt chẽ.**

 **- Cổng *(Trang)* thông tin điện tử chưa theo một tiêu chuẩn thống nhất, thiếu thẩm định về an ninh mạng. Việc sử dụng phần mềm, hệ điều hành bẻ khoá *(Crack)* diễn ra phổ biến.**

 **- Cơ sở hạ tầng công nghệ kỹ thuật không gian mạng phần lớn lệ thuộc nước ngoài *(mối đe doạ an ninh nếu xảy ra xung đột).***

**- Công tác đào tạo nguồn nhân lực, chuyên gia an ninh mạng chưa theo kịp yêu cầu về số lượng và chất lượng: Đội ngũ chuyên gia an ninh mạng chưa có *(mới chỉ có ở mảng dân sự, phục vụ an toàn thông tin).* Đội ngũ quản trị Cổng *(Trang)* thông tin điện tử chưa được quan tâm.**

 **- Công tác đấu tranh an ninh mạng còn hạn chế: Chưa huy động được sức mạnh tổng hợp; công tác bảo vệ bí mật nhà nước trên không gian mạng, phòng chống tấn công mạng còn hạn chế.**

 **- Các quốc gia trên thế giới đều đồng loạt ban hành Luật An ninh mạng:**

 **Mỹ:** Ngày 27/10/2015, với 74 phiếu thuận và 21 phiếu chống, Thượng viện Mỹ thông qua dự Luật Chia sẻ Thông tin An ninh mạng (CISA) nhằm tạo hệ thống phòng thủ vững chắc không gian mạng, bất chấp phản đối của đại gia công nghệ và nhà hoạt động bảo mật. Thực tế ở Mỹ, các hành vi bị coi là phạm pháp được ghi rất rõ trong Bộ Pháp điển Mỹ như trộm cắp danh tính, xâm nhập vào các hệ thống máy tính, vi phạm sở hữu trí tuệ...

 **Đức:** Tháng 7/2015, Quốc hội Đức thông qua Luật An ninh mạng nhằm bảo vệ tốt hơn cho công dân và các doanh nghiệp trong kỷ nguyên số. Luật An ninh mạng của Đức yêu cầu các công ty và cơ quan liên bang phải có tiêu chuẩn bảo mật mạng tối thiểu và phải được bằng Văn phòng Bảo mật Thông tin Liên bang (BSI) chứng nhận. Các công ty cũng phải thông báo cho Văn phòng về các vụ tấn công mạng bị nghi ngờ trên hệ thống của họ.

**Liên minh Châu Âu (EU):** Với những "kho" dữ liệu khổng lồ, ngày 9/5, Liên minh châu Âu (EU) đã bắt đầu thực thi Luật An ninh mạng đầu tiên. Theo đó, các doanh nghiệp cung cấp những dịch vụ “thiết yếu” như: cấp nước, năng lượng, vận tải, y tế và ngân hàng, phải thông báo đến chính quyền quốc gia nếu bị tấn công mạng nghiêm trọng.

**Singapore:** Dự Luật An ninh mạng được trình lên Quốc hội Singapore ngày 1/4/2018**,**cho phép Cơ quan An ninh mạng nước này theo dõi và quản lý an toàn không gian mạng của quốc gia. Cơ quan An ninh mạng được phép thực hiện các biện pháp chủ động để bảo vệ cơ sở hạ tầng thông tin quan trọng và nhanh chóng ứng phó với các mối đe dọa và sự cố. Chính phủ Singapore đã liệt kê 11 lĩnh vực được xem là cơ sở hạ tầng thông tin quan trọng, trong đó có nước, y tế, hàng hải, truyền thông, thông tin, năng lượng và hàng không.

**Thái Lan:**Ngày 16/12/2016, với 167 phiếu ủng hộ và 5 phiếu trắng, Quốc hội Thái Lan đã nhất trí thông qua Luật Tội phạm máy tính. Luật Tội phạm máy tính quy định mức phạt tới 5 năm tù đối với những người đăng tải những thông tin sai lên hệ thống máy tính nhằm phá hoại an ninh quốc gia, an toàn công cộng, sự ổn định kinh tế quốc dân hay hạ tầng cơ sở công cộng hoặc gây hoang mang…

**Nhật bản:** Từ tháng 11/2014 Nhật Bản đã ban hành đạo Luật cơ sở về an ninh mạng. Theo đó, chính phủ xây dựng một chiến lược an ninh, cũng như Bộ Chỉ huy chiến lược an ninh mạng được thành lập trực thuộc Nội các Nhật Bản, nhằm mục đích thúc đẩy toàn diện và hiệu quả các chính sách an ninh mạng.

**Australia:** Australia là quốc gia có khung văn bản pháp lý tương đối hoàn thiện về an ninh mạng, bao gồm: Luật về tội phạm mạng; Luật về thư điện tử rác; Luật về viễn thông và Luật bảo mật. Luật về tội phạm mạng cung cấp các quy định toàn diện về các tội liên quan đến Internet và máy tính như truy cập, xâm nhập máy tính trái phép, làm hỏng dữ liệu và cản trở truy cập đến máy tính, ăn cắp dữ liệu, gian lận máy tính, rình rập trên mạng, quấy rối và sở hữu các nội dung khiêu dâm về trẻ em.

**Trước tình hình trên,** đã đặt ra yêu cầu cấp thiết đối với công tác an ninh mạng trong bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội. Việc ban hành Luật an ninh mạng góp phần phòng ngừa, đấu tranh làm thất bại hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, chống Nhà nước, 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; Phòng ngừa, ngăn chặn, ứng phó, khắc phục hậu quả của các hoạt động tấn công mạng, khủng bố mạng, chiến tranh mạng khi hoạt động tấn công mạng nhằm vào hệ thống thông tin nước ta gia tăng về số lượng và mức độ nguy hiểm, ảnh hưởng nghiêm trọng tới chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội; Phòng ngừa, ngăn chặn, loại bỏ tác nhân tiến hành hoạt động gián điệp mạng, sử dụng không gian mạng để chiếm đoạt thông tin, tài liệu bí mật nhà nước, đặc biệt là hoạt động xâm nhập, tấn công vào hệ thống thông tin quan trọng về an ninh quốc gia; đồng thời, hạn chế và tiến tới không còn tình trạng đăng tải bí mật nhà nước trên mạng Internet do chủ quan hoặc thiếu kiến thức an ninh mạng. Bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia và áp dụng các biện pháp cần thiết, tương xứng. Đây là hệ thống thông tin của các mục tiêu, cơ sở hạ tầng quan trọng quốc gia, cơ quan chứa đựng bí mật nhà nước, nếu bị tấn công, xâm nhập, phá hoại, chiếm đoạt thông tin có thể gây hậu quả nghiêm trọng, ảnh hưởng chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội.

Việc ban hành Luật an ninh mạng có tác dụng phòng ngừa, ứng phó với các nguy cơ đe dọa an ninh mạng: Các nguy cơ đe dọa an ninh mạng hiện đang tồn tại là: Thông qua không gian mạng thực hiện âm mưu “diễn biến hòa bình”, phá hoại tư tưởng, chuyển hóa chế độ chính trị nước ta. Đối mặt với các cuộc tấn công mạng trên quy mô lớn, cường độ cao. Mất kiểm soát về an ninh, an toàn thông tin mạng. Khắc phục tồn tại, hạn chế liên quan bảo vệ an ninh mạng. Các quy định hiện nay về an toàn thông tin mạng chưa đủ sức răn đe, ngăn chặn các hành vi vi phạm trên không gian mạng; chưa đáp ứng được yêu cầu thực tiễn của công tác an ninh mạng đặt ra trong tình hình mới. Thực trạng này đã gây khó khăn, vướng mắc trong tổ chức, triển khai các phương án bảo đảm an ninh thông tin, an ninh mạng cũng như trong công tác phòng ngừa, đấu tranh ngăn chặn các hoạt động sử dụng Internet để xâm phạm an ninh quốc gia, trật tự, an toàn xã hội.

Việc ban hành Luật An ninh mạng nhằm thể chế hóa đầy đủ, kịp thời chủ trương, đường lối của Đảng về an ninh mạng quy định tại một số văn kiện, đó là: Nghị quyết số 13-NQ/TW ngày 16/01/2012 của Hội nghị Trung ương 4 Khóa XI về xây dựng hệ thống kết cấu hạ tầng đồng bộ nhằm đưa nước ta cơ bản trở thành nước công nghiệp theo hướng hiện đại vào năm 2020; Nghị quyết số 28-NQ/TW ngày 25/10/2013 của Hội nghị Trung ương 8 Khóa XI về chiến lược bảo vệ Tổ quốc trong tình hình mới; Chỉ thị số 46-CT/TW ngày 22/6/2015 của Bộ Chính trị về tăng cường sự lãnh đạo của Đảng đối với công tác bảo đảm an ninh, trật tự trong tình hình mới; Chỉ thị số 28-CT/TW ngày 16/9/2013 của Ban Bí thư Trung ương Đảng về tăng cường công tác bảo đảm an toàn thông tin mạng trong tình hình mới. Cụ thể hóa 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. 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. Bên cạnh đó, việc ban hành Luật góp phần cụ thể hóa tinh thần và nội dung mới của Hiến pháp về bảo vệ Tổ quốc, đặc biệt là quy định “Tổ quốc Việt Nam là thiêng liêng, bất khả xâm phạm” và “mọi hành vi chống lại độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ, chống lại sự nghiệp xây dựng và bảo vệ Tổ quốc đều bị nghiêm trị”. Đồng thời, tạo cơ sở pháp lý để hội nhập 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: Mỹ, Nhật Bản, Trung Quốc, Anh, Úc, Séc, Hàn Quốc… 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.

**2. Mục đích xây dựng Luật An ninh mạng**

Việc xây dựng và ban hành Luật An ninh mạng nhằm mục đích hoàn thiện cơ sở pháp lý để 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. 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.

Luật An ninh mạng 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 trên không gian mạng. Bảo vệ 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. Luật An ninh mạng ra đời 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”. Đồng thời, quy định các nhóm hành vi cụ thể liên quan tới tấn công mạng; 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, việc ban hành Luật An ninh mạng sẽ giúp Hệ thống thông tin của cơ quan, tổ chức, cá nhân được bảo vệ trước hoạt động tấn công 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.

**III. Luật An ninh mạng**

Luật An Ninh mạng đã được Quốc hội Việt Nam thông qua và có hiệu lực từ ngày 1 tháng 1 năm 2019 tại Việt Nam. Không chỉ cung cấp các biện pháp bảo vệ môi trường mạng mà ở một mức độ nào đó đã được quy định bởi Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015, Luật An Ninh Mạng cũng bao gồm nhiều điều khoản khác nhau để kiểm soát nội dung được đăng hoặc xuất bản trên mạng. Dưới đây là một số vấn đề nổi bật luật an ninh mạng.

Luật An ninh mạng áp dụng cho tất cả các cơ quan, tổ chức, cá nhân liên quan đến bảo vệ an ninh mạng, được định nghĩa rộng rãi là đảm bảo rằng các hoạt động trong không gian mạng không gây tổn hại đến an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của các cơ quan, tổ chức và cá nhân. Đặc biệt, Luật An ninh mạng sẽ áp dụng cho các tổ chức ở nước ngoài, có người dùng cư trú tại Việt Nam như Google hoặc Facebook.

Luật An ninh mạng bao gồm tất cả các mạng về cơ sở hạ tầng CNTT, viễn thông, Internet, hệ thống máy tính, cơ sở dữ liệu, xử lý thông tin, hệ thống lưu trữ và kiểm soát và điều chỉnh các hoạt động của mọi doanh nghiệp cung cấp dịch vụ trong không gian mạng và người dùng Internet bao gồm thương mại điện tử, trang web, diễn đàn trực tuyến, mạng xã hội và blog.

Luật An ninh mạng áp đặt các nghĩa vụ khác nhau đối với người vận hành hệ thống thông tin. Theo Luật An toàn thông tin mạng theo đó, người vận hành hệ thống thông tin có nghĩa là bất kỳ cơ quan, tổ chức hoặc cá nhân nào có quyền quản lý trực tiếp đối với hệ thống thông tin.

 **Những nội dung cơ bản**

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 4 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. 5 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, UBND 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 (khóa XIV) 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. (\*) Các hành vi tấn công mạng, gián điệp mạng, khủng bố mạng và liên quan như 6 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. 7 - 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.

 **IV. Định hướng công tác tuyên truyền**

Để tạo sự thống nhất trong cán bộ, đảng viên, sự đồng thuận trong xã hội về Luật An ninh mạng; góp phần đấu tranh, phản bác lại các luận điệu tuyên truyền
xuyên tạc, kích động của các thế lực thù địch, phần tử phản động, số cơ hội chính
trị, không bị lôi kéo, tham gia vào các hoạt động tụ tập đông người, gây mất trật
tự an ninh, công tác tuyên truyền cần tập trung làm tốt một số việc sau:

**1.** Triển khai nghiêm túc, bài bản công tác tuyên truyền theo Kế hoạch số
207-KH/BTGTW ngày 16/6/2018 của Ban Tuyên giáo Trung ương về “Côngtác tuyên truyền góp phần ổn định an ninh trật tự trong thời gian tới.

**2.** Thông tin, tuyên truyền, giải thích rõ những nội dung cơ bản của Luật
An ninh mạng. Làm rõ sự cần thiết, mục đích ban hành và ý nghĩa của Luật An
ninh mạng; đấu tranh, phản bác lại các luận điệu bịa đặt, xuyên tạc các nội dung
của Luật An ninh mạng.

**3.** Tuyên truyền, vạch trần các âm mưu, hoạt động lợi dụng việc ban hành
Luật An ninh mạng (và dự thảo Luật Đơn vị hành chính - kinh tế đặc biệt) để
kích động biểu tình, bạo loạn chống phá Đảng, Nhà nước ta của các thế lực thù
địch, tổ chức phản động, các phần tử cơ hội chính trị; qua đó, nâng cao tinh thần
cảnh giác, không mắc mưu các phần tử xấu, không bị kích động, xúi giục tham
gia vào các hoạt động tụ tập đông người, tuần hành hoặc có hành vi quá khích
gây mất an ninh trật tự, an toàn xã hội, vi phạm pháp luật.

**4.** Tăng cường bám sát cơ sở, nắm bắt tâm tư, nguyện vọng, nhất là những
vấn đề bức xúc của nhân dân để chủ động, kịp thời xử lý và tham mưu cho cấp
trên biện pháp giải quyết.

**5.** Định hướng và quản lý tốt thông tin trên báo chí, mạng viễn thông, mạng
xã hội, bảo đảm đưa tin đúng định hướng, thông tin chính xác, đúng đắn, kịp thời
để nhân dân hiểu rõ; xử lý nghiêm các tổ chức, cá nhân có thông tin, bình luận,
phát ngôn thiếu căn cứ, sai lệch nội dung Luật An ninh mạng, kích động, tụ tập
đông người, tuần hành, gây rối an ninh trật tự, bạo loạn và chống phá Đảng, Nhà
nước trên báo chí, mạng xã hội.

**V. Liên hệ thực tế**

Trước thời điểm Luật An ninh mạng được ban hành, không ít ý kiến bày tỏ lo ngại luật này có thể gây cản trở tới sự phát triển kinh tế - xã hội... Tuy nhiên, những gì diễn ra trên môi trường mạng trong thời gian qua cho thấy, luật không những bảo vệ, bảo đảm an toàn, an ninh thông tin cho tổ chức, doanh nghiệp, người dân, mà còn góp phần nâng cao ý thức của người sử dụng khi tương tác, chia sẻ thông tin trên mạng.

Có thể thấy, ảnh hưởng rõ nhất của Luật An ninh mạng - có hiệu lực từ ngày 1-1-2019 là cảnh tỉnh, nâng cao nhận thức của người sử dụng internet, đặc biệt là mạng xã hội (Facebook, Youtube, Zalo...). Trước đây, cộng đồng mạng tự cho mình hoạt động hoàn toàn tự do, bất chấp pháp luật, đến nay hầu hết đều hiểu rằng, dù là trên mạng thì họ vẫn phải tuân thủ pháp luật và quy phạm đạo đức của người Việt Nam.

Tình trạng tung tin giả, sai sự thật, tin bịa đặt lên mạng xã hội, trong suốt một thời gian dài, không chỉ làm thiệt hại cho cá nhân, tổ chức bị tung tin, mà còn gây tâm lý hoang mang, sự bất ổn cho cộng đồng, xã hội. Gần đây nhất, trong khi cả nước cùng vào cuộc quyết liệt phòng, chống dịch Covid-19, thì có không ít đối tượng tung tin sai lệch trên Facebook cá nhân về dịch bệnh này.

Ở quy mô toàn quốc, Phó Cục trưởng Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao (Bộ Công an), Thiếu tướng Nguyễn Văn Giang thông tin, Bộ Công an đã lập danh sách hàng trăm đối tượng, tổ chức đấu tranh với gần 200 trường hợp và xử lý vi phạm hành chính hơn 30 trường hợp đưa tin sai sự thật về dịch Covid-19.

Trong năm 2021, Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao Công an tỉnh Hưng Yên đã tham mưu, đề xuất Giám đốc Công an tỉnh ra quyết định xử phạt vi phạm hành chính 09 trường hợp, nhắc nhở hàng chục trường hợp liên quan đến việc đăng tin giả mạo, sai sự thật, xúc phạm uy tín, danh dự của các đồng chí lãnh đạo Đảng, Nhà nước, ảnh hưởng đến công tác phòng, chống dịch Covid-19…

Rõ ràng, khi có hành lang pháp lý đầy đủ, các cơ quan thực thi pháp luật có thể triển khai hiệu quả hơn Luật An ninh mạng. Cùng với đó, ý thức và trách nhiệm của mỗi người dân, của cộng đồng cần tiếp tục được nâng cao hơn nữa để môi trường mạng ngày càng lành mạnh, an toàn hơn.

Trên đây, tôi đã trình bày tới toàn thể các đồng chí một số nội dung cơ bản về Luật An ninh mạng *(Sự cần thiết phải ban hành Luật An ninh mạng, vị trí, vai trò của Luật An ninh mạng và nội dung cơ bản của Luật).* Trân trọng cảm ơn các đồng chí đã lắng nghe, chúc các đồng chí và gia đình luôn mạnh khoẻ, hạnh phúc và thành công. Xin trân trọng cảm ơn!