UBND TỈNH BẮC GIANG
SỞ TƯ PHÁP

TÌM HIỂU
LUẬT AN NINH MẠNG
NĂM 2018

Bắc Giang, năm 2019

LỜI NÓI ĐẦU

Thể chế hóa đầy đủ, kịp thời chủ trương, đường lối của Đảng về an ninh mạng được nêu tại một số văn bản như: Nghị quyết số 13-NQ/TW ngày 16/01/2012 của Hội nghị TW4 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 của Hội nghị TW VIII khóa XI về chiến lược bảo vệ Tổ quốc trong tình hình mới; Chỉ thị số 46-CT/TW 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, trong đó khẳng định vấn đề an ninh mạng đang là vấn đề rất phức tạp, cần được chú trọng giải quyết đồng bộ, hiệu quả; Chỉ thị số 28-CT/TW của Ban Bí thư Trung ương Đảng, Chỉ thị số 15-CT/TTg của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an toàn thông tin mạng; Chỉ thị số 30-CT/TW của Bộ Chính trị ban hành về phát triển và tăng cường quản lý báo chí điện tử, mạng xã hội và các loại hình truyền thông khác trên Internet; Nghị định 101/2016/NĐ-CP của Chính phủ quy định chi tiết trách nhiệm thực hiện và các biện pháp ngăn chặn hoạt động sử dụng không gian mạng để khủng bố, Luật An ninh mạng đã được Quốc hội khóa XIV, kỳ họp thứ 5 thông qua ngày 12/6/2018. Chủ tịch nước ký Lệnh công bố ngày 25/6/2018 (Lệnh số 06/2018/L-CTN), Luật có hiệu lực thi hành từ ngày 01/01/2019.

Để góp phần trang bị phổ biến những quy định của Luật An ninh mạng năm 2018 đến các báo cáo viên pháp luật, tuyên truyền viên pháp luật, cán bộ, công chức, viên chức và toàn thể Nhân dân trên địa bàn tỉnh, Sở Tư pháp tỉnh Bắc Giang biên soạn và phát hành cuốn sách "***Tìm hiểu Luật An ninh mạng năm 2018".***

Cuốn tài liệu gồm 2 phần:

Phần I: Giới thiệu chung.

Phần II: Những nội dung cơ bản của Luật.

Trong quá trình biên soạn tài liệu không tránh khỏi những thiếu sót, rất mong nhận được sự trao đổi, chỉa sẻ và góp ý của quý bạn đọc để chúng tôi hoàn chỉnh tài liệu hơn, phục vụ tốt nhất cho nhân dân ở cơ sở.

Sở Tư pháp trân trọng giới thiệu !

SỞ TƯ PHÁP TỈNH BẮC GIANG

Phần I:
GIỚI THIỆU CHUNG

1. Sự cần thiết ban hành Luật

1.1. 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

Cùng với quá trình hội nhập quốc tế, phát triển công nghệ thông tin, đặc biệt là cuộc cách mạng công nghệ 4.0, thực trạng, tình hình diễn ra trên không gian mạng 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, cụ thể:

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 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. Trong khi đó, khủng bố mạng nổi lên như một thách thức toàn cầu, chiến tranh mạng là một trong những nguy cơ đe dọa an ninh

quốc gia. Những vấn đề trên đặt vấn đề phải chủ động phòng ngừa, ngăn chặn, ứng phó, có phương án và sự chuẩn bị sẵn sàng để kịp thời xử lý các tình huống xấu có thể xảy ra.

Thứ ba, 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.

Thứ tư, 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 quan trọng quốc gia, 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, gây rối loạn trật tự an toàn xã hội nên cần có biện pháp bảo vệ chặt chẽ, tương xứng và ở mức độ cao hơn so với những mục tiêu cần bảo vệ ít quan trọng hơn. Việc bảo vệ những hệ thống thông tin này không chỉ bao gồm hoạt động kiểm tra, đánh giá quá trình vận hành, áp dụng các tiêu chuẩn an ninh mạng phù hợp, riêng biệt mà phải tiến hành hoạt động thẩm định ngay từ khi xây dựng hồ sơ thiết kế, vận hành hệ thống thông tin để sớm phát hiện, loại bỏ các nguy cơ đe dọa an ninh mạng.

Để góp phần cải cách thủ tục hành chính, tránh trùng lặp về thẩm quyền quản lý nhà nước, hướng tới mục tiêu chỉ

một cơ quan quản lý nhà nước đối với một hệ thống thông tin, Luật An ninh mạng đã quy định Chính phủ quy định chi tiết Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, trường hợp hệ thống thông tin được phân loại theo quy định của luật khác mà trùng với hệ thống thông tin thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia theo quy định của Luật An ninh mạng thì áp dụng quy định của Luật an ninh mạng; Bộ Công an thẩm định về năng lực, điều kiện đối với doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.

Thứ năm, quy định và thống nhất thực hiện phòng ngừa, ứng phó nguy cơ, sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia. Hoạt động ứng cứu sự cố an toàn thông tin mạng theo quy định của Luật An toàn thông tin mạng hiện nay chỉ phát huy được vai trò bảo đảm 03 thuộc tính của thông tin là tính nguyên vẹn, tính bảo mật và tính khả dụng, chưa đáp ứng được yêu cầu bảo vệ quốc phòng, an ninh, trật tự an toàn xã hội, xử lý sự cố, huy động lực lượng ứng phó, cũng như loại bỏ các tác nhân gây hại tồn tại sẵn bên trong hệ thống thông tin hoặc hành vi vi phạm pháp luật trên không gian mạng ảnh hưởng tới hệ thống thông tin quan trọng về an ninh quốc gia. Phòng ngừa, ứng phó nguy cơ, sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia là một quy trình thống nhất. Việc phân tích các sự cố an ninh mạng liên quan trực tiếp tới dấu vết hiện trường và các dấu hiệu phạm tội, góp phần vào công tác điều tra, xử lý hành vi vi phạm của cơ quan chức

năng Bộ Công an, Bộ Quốc phòng. Do đó, thống nhất đầu mối trong giám sát, dự báo, ứng phó và diễn tập ứng phó khẩn cấp sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia là cấp bách, cần thiết, không trùng dẫm với ứng cứu sự cố an toàn thông tin mạng.

Thứ sáu, quy định về tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia. Tham khảo kinh nghiệm nước ngoài cho thấy, một số quốc gia trên thế giới đã xây dựng các bộ tiêu chuẩn, quy chuẩn kỹ thuật về an ninh mạng để áp dụng cho các mục tiêu, đối tượng và yêu cầu bảo vệ an ninh mạng cụ thể. Ở nước ta, tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng được ban hành rộng rãi, được áp dụng chung cho toàn xã hội, mang tính phổ thông, đại chúng. Tuy nhiên, đối với hệ thống thông tin quan trọng về an ninh quốc gia, ngoài những tiêu chuẩn an toàn thông tin mạng, cần có những quy định về tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng ở mức độ cao hơn để đáp ứng yêu cầu đặt ra.

Thứ bảy, triển khai công tác bảo vệ an ninh mạng trong hệ thống cơ quan nhà nước từ Trung ương đến địa phương. Hiện nay, hệ thống thông tin của cơ quan nhà nước tồn tại nhiều lỗ hổng bảo mật không được khắc phục, nhận thức của cán bộ, nhân viên còn nhiều hạn chế, chưa nhận thức được mức độ cần thiết của công tác an ninh mạng. Trong khi đó, công nghệ thông tin đã được ứng dụng rộng rãi từ Trung ương đến địa phương, chính phủ điện tử và các hệ thống điều khiển, xử lý tự động đã xuất hiện ở mọi ngành, cấp, lĩnh vực. Hệ

thống thông tin của cơ quan nhà nước đang là đối tượng của hoạt động tấn công mạng, xâm nhập mạng, gián điệp mạng; tình trạng đăng tải thông tin, tài liệu bí mật nhà nước trên mạng internet vẫn còn tồn tại. Do đó, tình hình thực tiễn đã đặt ra yêu cầu triển khai công tác bảo vệ an ninh mạng và lực lượng an ninh mạng 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. Hiện nay, công tác này chưa được chú trọng, nhà nước cũng chưa có định hướng quản lý, bảo đảm an ninh mạng đối với các xu hướng công nghệ có khả năng thay đổi tương lai như cuộc cách mạng công nghiệp lần thứ 4, điện toán đám mây, dữ liệu lớn, dữ liệu nhanh. Tham khảo kinh nghiệm nước ngoài cho thấy, một số quốc gia đã xây dựng nhiều đạo luật chuyên ngành của an ninh mạng, tập trung nâng cao năng lực dự báo, chia sẻ thông tin và tăng cường năng lực 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. Mặc dù Chính phủ đã giao Bộ Công an đã chủ trì, phối hợp với các bộ, ngành liên quan triển khai nhiều kế hoạch kiểm tra, đánh giá thực trạng an ninh mạng tại hàng chục bộ, ngành, địa phương nhưng đây là hoạt động đột xuất, chưa được triển khai hằng năm, không tạo thành được trách nhiệm và ý thức kiểm tra, đánh giá an ninh mạng định kỳ. Trong khi đó, cơ quan chủ quản hệ thống thông tin chưa nhận thức rõ trách nhiệm của mình, chưa chủ động hoặc triển khai các hoạt động bảo vệ an ninh mạng một cách chiếu lệ, hình

thức. Để phòng ngừa, hạn chế nguy cơ an ninh mạng, cần xây dựng quy trình, cơ chế kiểm tra, đánh giá thực trạng an ninh mạng phù hợp, thống nhất trên phạm vi cả nước.

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. Việc chia sẻ thông tin, thông báo tình hình an ninh mạng có thể được thực hiện bởi cơ quan chức năng để tổ chức, cá nhân nâng cao nhận thức, áp dụng biện pháp phòng tránh hoặc nghiên cứu, tham khảo.

1.2. 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: *(1)* 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; *(2)* Đối mặt với các cuộc tấn công mạng trên quy mô lớn, cường độ cao; *(3)* Mất kiểm soát về an ninh, an toàn thông tin mạng.

1.3. Khắc phục tồn tại, hạn chế liên quan bảo vệ an ninh mạng

Một là, chồng chéo, trùng dẫm trong thực hiện chức năng, nhiệm vụ bảo vệ an ninh mạng giữa các bộ, ngành chức năng; tồn tại cách hiểu chưa rõ ràng giữa an ninh mạng và an toàn thông tin mạng. Cần thống nhất nhận thức rằng, an ninh mạng bao gồm hoạt động bảo vệ an ninh quốc gia, trật tự an toàn xã hội theo chức năng, nhiệm vụ của Bộ Công

an; hoạt động tác chiến trên không gian mạng theo chức năng, nhiệm vụ của Bộ Quốc phòng và bảo đảm an toàn thông tin mạng theo chức năng, nhiệm vụ của Bộ Thông tin và Truyền thông. An toàn thông tin mạng là điều kiện cho bảo đảm an ninh mạng được thực thi có hiệu quả, bền vững.

Hai là, chưa có văn bản luật quy định về công tác 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.

1.4. Thể chế hóa đầy đủ, kịp thời các chủ trương, đường lối của Đảng về an ninh mạng

Quan điểm, tư tưởng chỉ đạo của Đảng, Nhà nước về an ninh mạng đã thể hiện rõ, nhất quán, có hệ thống và phù hợp với từng thời kỳ, kịp thời điều chỉnh, đưa ra các quan điểm, tư tưởng chỉ đạo về vấn đề an ninh mạng trong tình hình mới. Việc ban hành Luật An ninh mạng là nhằm thể chế hóa đầy đủ, kịp thời chủ trương, đường lối của Đảng về an ninh mạng được nêu tại một số văn bản như: Nghị quyết số 13-NQ/TW ngày 16/01/2012 của Hội nghị TW4 khóa XI; Nghị quyết số 28-NQ/TW của Hội nghị TW VIII khóa XI; Chỉ thị số 46-CT/TW của Bộ Chính trị; Chỉ thị số 28-

CT/TW của Ban Bí thư Trung ương Đảng, Chỉ thị số 15-CT/TTg của Thủ tướng Chính phủ; Chỉ thị số 30-CT/TW của Bộ Chính trị; Nghị định 101/2016/NĐ-CP; Nghị định 66/2017/NĐ-CP.

1.5. 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. Luật An ninh mạng 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. Bên cạnh đó, việc ban hành Luật này cũng 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".

1.6. 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: Mỹ, Nhật, Trung Quốc, Anh, Úc, Cộng hòa 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 tiêu, quan điểm chỉ đạo của Luật

2.1. Mục tiêu

- Hoàn thiện cơ sở pháp lý ổn định về an ninh mạng theo hướng áp dụng các quy định pháp luật 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 Việt Nam và điều ước quốc tế mà Việt Nam tham gia ký kết.

2.2. Quan điểm

Luật An ninh mạng được xây dựng trên cơ sở các quan điểm chỉ đạo sau:

Một là, thể chế hóa đầy đủ, kịp thời các chủ trương, đường lối, chính sách của Đảng, Nhà nước về an ninh mạng. Xác định bảo đảm an ninh mạng là một bộ phận cấu thành đặc biệt quan trọng của sự nghiệp bảo vệ Tổ quốc Việt Nam xã hội chủ nghĩa; là nhiệm vụ vừa cấp bách vừa lâu dài của cả hệ thống chính trị, giao Bộ Công an chủ trì, đặt dưới sự lãnh đạo xuyên suốt của Đảng và sự quản lý thống nhất của Nhà nước.

Hai là, bảo đảm phù hợp với quy định của Hiến pháp năm 2013; cụ thể hóa các quy định của Hiến pháp, nhất là quy định về bảo vệ Tổ quốc và quy định về quyền con người, quyền và nghĩa vụ cơ bản của công dân.

Ba là, bảo đảm tính đồng bộ, thống nhất của hệ thống pháp luật, xác định hợp lý mối quan hệ giữa Luật này và các luật liên quan.

Bốn là, kế thừa các quy định hiện hành còn phù hợp, sửa đổi, bổ sung các quy định đã bộc lộ những hạn chế.

Năm là, tham khảo có chọn lọc kinh nghiệm của các nước trong khu vực và trên thế giới để vận dụng linh hoạt vào điều kiện thực tiễn của Việt Nam; bảo đảm sự phù hợp với các quy định, cam kết quốc tế mà Việt Nam tham gia ký kết hoặc là thành viên.

3. Bố cục của Luật

Luật An ninh mạng gồm 7 chương, 43 điều. Bố cục của Luật cụ thể như sau:

Chương I. Những quy định chung:

Gồm 9 điều, (từ Điều 1 đến Điều 9) quy định về phạm vi điều chỉnh; giải thích từ ngữ; chính sách của Nhà nước về an ninh mạng; nguyên tắc bảo vệ an ninh mạng; biện pháp bảo vệ an ninh mạng; bảo vệ không gian mạng quốc gia; hợp tác quốc tế về an ninh mạng; các hành vi bị nghiêm cấm về an ninh mạng; xử lý vi phạm pháp luật về an ninh mạng.

Chương II. Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

Gồm 6 điều (từ Điều 10 đến Điều 15), quy định về hệ thống thông tin quan trọng về an ninh quốc gia; thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; giám sát an ninh mạng đối với hệ thống thông tin

quan trọng về an ninh quốc gia; ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.

Chương III. Phòng ngừa, xử lý hành vi xâm phạm an ninh mạng

Gồm 7 điều (từ Điều 16 đến Điều 22), quy định về 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 thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng; phòng, chống hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội; phòng, chống tấn công mạng; phòng, chống khủng bố mạng; phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng; đấu tranh bảo vệ an ninh mạng.

Chương IV. Hoạt động bảo vệ an ninh mạng

Gồm 7 điều (từ Điều 23 đến Điều 29), quy định về triển khai hoạt động bảo vệ an ninh mạng trong cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương; kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia; bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia; cổng kết nối mạng quốc tế; bảo

đảm an ninh thông tin trên không gian mạng; nghiên cứu, phát triển an ninh mạng; nâng cao năng lực tự chủ về an ninh mạng; bảo vệ trẻ em trên không gian mạng.

Chương V. Bảo đảm hoạt động bảo vệ an ninh mạng

Gồm 6 điều (từ Điều 30 đến Điều 35), quy định về lực lượng bảo vệ an ninh mạng; bảo đảm nguồn nhân lực bảo vệ an ninh mạng; tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng; giáo dục, bồi dưỡng kiến thức, nghiệp vụ an ninh mạng; phổ biến kiến thức về an ninh mạng; kinh phí bảo vệ an ninh mạng.

Chương VI. Trách nhiệm của cơ quan, tổ chức, cá nhân

Gồm 7 điều (từ Điều 36 đến Điều 42), quy định về trách nhiệm của Bộ Công an; trách nhiệm của Bộ Quốc phòng; trách nhiệm của Bộ Thông tin và Truyền thông; trách nhiệm của Ban Cơ yếu Chính phủ; trách nhiệm của Bộ, ngành, Ủy ban nhân dân cấp tỉnh; trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng; trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng.

Chương VII. Điều khoản thi hành

Gồm 01 điều (Điều 43), quy định về hiệu lực thi hành.

Phần II

Những nội dung cơ bản của Luật

1. Những quy định chung (Chương 1)

Chương 1 bao gồm những quy định về phạm vi điều chỉnh; giải thích từ ngữ; chính sách của Nhà nước về an ninh mạng; nguyên tắc bảo vệ an ninh mạng; biện pháp bảo vệ an ninh mạng; bảo vệ không gian mạng quốc gia; hợp tác quốc tế về an ninh mạng; các hành vi bị nghiêm cấm về an ninh mạng; xử lý vi phạm pháp luật về an ninh mạng.

1.1. Về phạm vi điều chỉnh (Điều 1)

Luật An ninh mạng 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.

1.2. Một số khái niệm

- *An ninh mạng* là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

- *Bảo vệ an ninh mạng* là phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng.

- *Không gian mạng* là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm 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; là nơi con người thực

hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian.

- *Không gian mạng quốc gia* là không gian mạng do Chính phủ xác lập, quản lý và kiểm soát.

- *Tội phạm mạng* là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện tội phạm được quy định tại Bộ luật Hình sự.

- *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.

- *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.

- *Gián điệp mạng* là hành vi cố ý vượt qua cảnh báo, mã truy cập, mật mã, tường lửa, sử dụng quyền quản trị của người khác hoặc bằng phương thức khác để chiếm đoạt, thu thập trái phép thông tin, tài nguyên thông tin trên 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 của cơ quan, tổ chức, cá nhân.

- *Tài khoản số* là thông tin dùng để chứng thực, xác thực, phân quyền sử dụng các ứng dụng, dịch vụ trên không gian mạng.

- *Nguy cơ đe dọa an ninh mạng* là tình trạng không gian mạng xuất hiện dấu hiệu đe dọa xâm phạm an ninh quốc gia,

gây tổn hại nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

- *Sự cố an ninh mạng* là sự việc bất ngờ xảy ra trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

- *Tình huống nguy hiểm về an ninh mạng* là sự việc xảy ra trên không gian mạng khi có hành vi xâm phạm nghiêm trọng an ninh quốc gia, gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

1. 3. Về chính sách của Nhà nước về an ninh mạng (Điều 3)

Về chính sách của Nhà nước về an ninh mạng, Luật An ninh mạng quy định:

- Ưu tiên, bảo vệ an ninh mạng trong quốc phòng, an ninh, phát triển kinh tế - xã hội, khoa học, công nghệ và đối ngoại;

- Xây dựng không gian mạng lành mạnh, không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân;

- Ưu tiên nguồn lực xây dựng lực lượng chuyên trách bảo vệ an ninh mạng; nâng cao năng lực cho lực lượng bảo vệ an ninh mạng và tổ chức, cá nhân tham gia bảo vệ an ninh mạng; ưu tiên đầu tư cho nghiên cứu, phát triển khoa học, công nghệ để bảo vệ an ninh mạng;

- Khuyến khích, tạo điều kiện để tổ chức, cá nhân tham gia bảo vệ an ninh mạng, xử lý các nguy cơ đe dọa an ninh mạng; nghiên cứu, phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng nhằm bảo vệ an ninh mạng; phối hợp với cơ quan chức năng trong bảo vệ an ninh mạng;

- Tăng cường hợp tác quốc tế về an ninh mạng.

1.4. Về nguyên tắc bảo vệ an ninh mạng (Điều 4)

Luật An ninh mạng quy định việc bảo vệ an ninh mạng phải tuân thủ 07 nguyên tắc sau:

- Tuân thủ Hiến pháp và pháp luật; bảo đảm lợi ích của Nhà nước, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân;

- Đặt dưới sự lãnh đạo của Đảng Cộng sản Việt Nam, sự quản lý thống nhất của Nhà nước; huy động sức mạnh tổng hợp của hệ thống chính trị và toàn dân tộc; phát huy vai trò nòng cốt của lực lượng chuyên trách bảo vệ an ninh mạng;

- Kết hợp chặt chẽ giữa nhiệm vụ bảo vệ an ninh mạng, bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia với nhiệm vụ phát triển kinh tế - xã hội, bảo đảm quyền con người, quyền công dân, tạo điều kiện cho cơ quan, tổ chức, cá nhân hoạt động trên không gian mạng;

- Chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh, làm thất bại mọi hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; sẵn sàng ngăn chặn các nguy cơ đe dọa an ninh mạng;

- Triển khai hoạt động bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia; áp dụng các biện pháp 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 thẩm định, chứng nhận đủ điều kiện về an ninh mạng trước khi đưa vào vận hành, sử dụng; thường xuyên kiểm tra, giám sát về an ninh mạng trong quá trình sử dụng và kịp thời ứng phó, khắc phục sự cố an ninh mạng;

- Mọi hành vi vi phạm pháp luật về an ninh mạng phải được xử lý kịp thời nghiêm minh.

1.5. Về biện pháp bảo vệ an ninh mạng (Điều 5)

Luật quy định chi tiết, cụ thể các biện pháp bảo vệ an ninh mạng. Đây là những biện pháp hành chính, kỹ thuật chung, vừa bảo vệ an ninh quốc gia, trật tự, an toàn xã hội, vừa bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng. Khoản 1 Điều 5 của Luật quy định các biện pháp bảo vệ an ninh mạng bao gồm:

- Thẩm định an ninh mạng;

- Đánh giá điều kiện an ninh mạng;

- Kiểm tra an ninh mạng;

- Giám sát an ninh mạng;

- Ứng phó, khắc phục sự cố an ninh mạng;

- Đấu tranh, bảo vệ an ninh mạng;

- Sử dụng mật mã để bảo vệ thông tin mạng;

- Ngăn chặn, yêu cầu tạm ngừng, ngừng cung cấp thông tin mạng; đình chỉ, tạm đình chỉ các hoạt động thiết

lập, cung cấp và sử dụng mạng viễn thông, mạng Internet, sản xuất và sử dụng thiết bị phát, thu phát sóng vô tuyến theo quy định của pháp luật;

- Yêu cầu xóa bỏ, truy cập xóa bỏ thông tin trái pháp luật hoặc thông tin quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng;

- Phong tỏa, hạn chế hoạt động của hệ thống thông tin; đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, thu hồi tin miền theo quy định của pháp luật;

- Khởi tố, điều tra, truy tố, xét xử theo quy định của Bộ luật tố tụng hình sự;

- Biện pháp khác theo quy định của pháp luật về an ninh quốc gia, pháp luật về xử lý vi phạm hành chính.

Bên cạnh đó, Luật giao Chính phủ quy định trình tự, thủ tục áp dụng biện pháp bảo vệ an ninh mạng, trừ biện pháp khởi tố, điều tra, truy tố, xét xử theo quy định của Bộ luật Tố tụng hình sự và biện pháp khác theo quy định của pháp luật về an ninh quốc gia, pháp luật về xử lý vi phạm hành chính.

1.6. Về hợp tác quốc tế về an ninh mạng (Điều 7)

Luật quy định hợp tác quốc tế về an ninh mạng được thực hiện trên cơ sở tôn trọng độc lập, chủ quyền và toàn vẹn lãnh thổ, không can thiệp vào công việc nội bộ của nhau, bình đẳng và cùng có lợi. Trên cơ sở đó, Luật quy định cụ thể nội dung hợp tác quốc tế về an ninh mạng, đồng thời giao Bộ Công an chịu trách nhiệm trước Chính phủ chủ trì,

phối hợp thực hiện hợp tác quốc tế về an ninh mạng, trừ hoạt động hợp tác quốc tế của Bộ Quốc phòng; Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện hợp tác quốc tế về an ninh mạng trong phạm vụ quản lý; Bộ Ngoại giao có trách nhiệm phối hợp với Bộ Công an, Bộ Quốc phòng trong hoạt động hợp tác quốc tế về an ninh mạng; trường hợp hợp tác quốc tế về an ninh mạng có liên quan đến trách nhiệm của nhiều Bộ, ngành do Chính phủ quyết định.

Bên cạnh đó, Luật quy định hoạt động hợp tác quốc tế về an ninh mạng của Bộ, ngành khác, của địa phương phải có văn bản tham gia ý kiến của Bộ Công an trước khi triển khai, trừ hoạt động hợp tác quốc tế của Bộ Quốc phòng.

1.7. Các hành vi bị nghiêm cấm về an ninh mạng và xử lý vi phạm pháp luật về an ninh mạng (Điều 8, Điều 9)

Luật An ninh mạng chỉ nghiêm cấm sử dụng không gian mạng để thực hiện các hành vi vi phạm pháp luật đã được pháp luật (Bộ luật hình sự, Bộ luật dân sự và các văn bản quy phạm pháp luật khác liên quan) quy định. Theo đó, Điều 8 Luật An ninh mạng đã liệt kê cụ thể, rõ ràng các hành vi bị nghiêm cấm về an ninh mạng, góp phần thuận lợi trong việc thực hiện và xử lý hành vi vi phạm điều cấm, bao gồm:

- Sử dụng không gian mạng để thực hiện hành vi sau đây: Hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự an toàn xã hội; Tổ chức, hoạt động, câu 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;

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; 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; 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 của cộng đồng; Xúi giục, lôi kéo, kích động người khác phạm tội;

- Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin quan trọng về an ninh quốc gia;

- 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; phát tán chương trình tin học gây hại cho 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; xâm nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác;

- Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng;

- Lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi;

- Hành vi khác vi phạm quy định của Luật này.

Như vậy, Luật An ninh mạng không có quy định cấm Facebook, Google hoặc các nhà cung cấp dịch vụ nước ngoài hoạt động tại Việt Nam; không ngăn cản quyền tự do ngôn luận, quyền bày tỏ quan điểm của công dân; không cấm công dân sử dụng các dịch vụ mạng xã hội như Facebook, Google; không cấm công dân tham gia hoạt động trên không gian mạng hoặc truy cập, sử dụng thông tin trên không gian mạng; cấm công dân khởi nghiệp, sáng tạo hay trao đổi, triển khai ý tưởng sáng tạo của mình trên không gian mạng.

Bên cạnh đó, Luật quy định người nào có hành vi vi phạm quy định của Luật này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử lý vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật (Điều 9).

2. Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia (Chương II)

Chương II Luật An ninh mạng quy định về bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia. Đây là một trong những nội dung đặc biệt quan

trọng của Luật an ninh mạng, quy định về hệ thống thông tin quan trọng về an ninh quốc gia và thể hiện đầy đủ các biện pháp, hoạt động bảo vệ tương xứng với mực độ quan trọng của hệ thống thông tin, 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 mạng và ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.

2.1. Về hệ thống thông tin quan trọng về an ninh quốc gia

"*Hệ thống thông tin quan trọng về an ninh quốc gia được hiểu 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*".

Hệ thống thông tin quan trọng về an ninh quốc gia được xác định trong các lĩnh vực đặc biệt quan trọng đối với quốc gia hay trong lĩnh vực đặc thù, bao gồm:

- Hệ thống thông tin quân sự, an ninh, ngoại giao, cơ yếu;

- Hệ thống thông tin lưu trữ, xử lý thông tin thuộc bí mật nhà nước;

- Hệ thống thông tin phục vụ lưu giữ, bảo quản hiện vật, tài liệu có giá trị đặc biệt quan trọng;

- Hệ thống thông tin phục vụ bảo quản, chế tạo, quản lý cơ sở vật chất đặc biệt quan trọng khác liên quan đến an ninh quốc gia;

- Hệ thống thông tin bảo quản, chế tạo, quản lý cơ sở vật chất đặc biệt quan trọng khác liên quan đến an ninh quốc gia;

- Hệ thống thông tin quan trọng phục vụ hoạt động của cơ quan, tổ chức ở trung ương;

- Hệ thống thông tin quốc gia thuộc 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;

- Hệ thống điều khiển và giám sát tự động tại công trình quan trọng liên quan đến an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia.

Luật giao Thủ tướng Chính phủ ban hành và sửa đổi, bổ sung Danh mục hệ thống thông tin quan trọng về an ninh quốc gia. Đồng thời, để tạo thuận lợi cho các chủ quản hệ thống thông tin trong việc thực hiện các nội dung quản lý nhà nước có liên quan đến thẩm quyền của nhiều bộ khác nhau, Luật giao Chính phủ quy định việc phối hợp giữa 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. (Điều 10)

2.2. Về hoạt động thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia (Điều 11)

Thẩm định an ninh mạng là hoạt động xem xét, đánh giá những nội dung về an ninh mạng để làm cơ sở cho việc quyết định xây dựng hoặc nâng cấp hệ thống thông tin. Điều 11 của Luật quy định cụ thể đối tượng, nội dung và thẩm quyền thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, cụ thể:

** Về đối tượng, bao gồm:*

- Báo cáo nghiên cứu tiền khả thi, hồ sơ thiết kế thi công dự án đầu tư xây dựng hệ thống thông tin trước khi phê duyệt;

- Đề án nâng cấp hệ thống thông tin trước khi phê duyệt.

** Về nội dung, bao gồm:*

- Việc tuân thủ quy định, điều kiện an ninh mạng trong thiết kế;

- Sự phù hợp với phương án bảo vệ, ứng phó, khắc phục sự cố và bố trí nhân lực bảo vệ an ninh mạng.

** Về thẩm quyền, bao gồm:*

- Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ trường hợp quy định tại điểm b và điểm c khoản này;

- Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng thẩm định an ninh mạng đối với hệ thống thông tin quân sự;

- Ban Cơ yếu Chính phủ thẩm định an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

2.3. Đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia (Điều 12)

Đánh giá điều kiện về an ninh mạng là hoạt động xem xét sự đáp ứng về an ninh mạng của hệ thống thông tin trước khi đưa vào vận hành, sử dụng. Hoạt động kiểm tra, đánh giá an ninh mạng do cơ quan chủ quản hệ thống thông tin thực hiện trước khi vận hành, sử dụng hoặc khi có thay đổi hiện

trạng; còn lực lượng chuyên trách bảo vệ an ninh mạng sẽ tiến hành kiểm tra, đánh giá trong trường hợp đột xuất khi xảy ra sự cố an ninh mạng, hành vi xâm phạm an ninh mạng, khi có yêu cầu quản lý nhà nước về an ninh mạng hoặc khi có đề nghị của cơ quan chủ quản hệ thống thông tin.

** Các điều kiện của hệ thống thông tin quan trọng về an ninh quốc gia, bao gồm:*

- Quy định, quy trình và phương án bảo đảm an ninh mạng; nhân sự vận hành, quản trị hệ thống;

- Bảo đảm an ninh mạng đối với trang thiết bị, phần cứng, phần mềm là thành phần hệ thống;

- Biện pháp kỹ thuật để giám sát, bảo vệ an ninh mạng; biện pháp bảo vệ hệ thống điều khiển và giám sát tự động, Internet vạn vật, hệ thống phức hợp thực - ảo, điện toán đám mây, hệ thống dữ liệu lớn, hệ thống dữ liệu nhanh, hệ thống trí tuệ nhân tạo;

- Biện pháp bảo đảm an ninh vật lý bao gồm cách ly cô lập đặc biệt, chống rò rỉ dữ liệu, chống thu tin, kiểm soát ra vào.

Đồng thời, Luật quy định cụ thể thẩm quyền đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc các Bộ Công an, Bộ Quốc phòng; Ban Cơ yếu Chính phủ.

2.4. Kiểm tra, giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia (Điều 13, 14)

Kiểm tra an ninh mạng là hoạt động xác định thực trạng an ninh mạng của hệ thống thông tin, cơ sở hạ tầng hệ

thống thông tin hoặc thông tin được lưu trữ, xử lý, truyền đưa trong hệ thống thông tin nhằm phòng ngừa, phát hiện, xử lý nguy cơ đe dọa an ninh mạng và đưa ra các phương án, biện pháp bảo đảm hoạt động bình thường của hệ thống thông tin.

** Các trường hợp, đối tượng kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, cụ thể:*

- Về trường hợp kiểm tra an ninh mạng, bao gồm:

+ Khi đưa phương tiện điện tử, dịch vụ an toàn thông tin mạng vào sử dụng trong hệ thống thông tin;

+ Khi có thay đổi hiện trạng hệ thống thông tin;

+ Kiểm tra định kỳ hằng năm;

+ Kiểm tra đột xuất khi xảy ra sự cố an ninh mạng, hành vi xâm phạm an ninh mạng; khi có yêu cầu quản lý nhà nước về an ninh mạng; khi hết thời hạn khắc phục điểm yếu, lỗ hỏng bảo mật theo khuyến cáo của lực lượng chuyên trách bảo vệ an ninh mạng.

- Về đối tượng bao gồm:

+ Hệ thống phần cứng, phần mềm, thiết bị số được sử dụng trong hệ thống thông tin;

+ Quy định, biện pháp bảo vệ an ninh mạng;

+ Thông tin được lưu trữ, xử lý, truyền đưa trong hệ thống thông tin;

+ Phương án ứng phó, khắc phục sự cố an ninh mạng của chủ quản hệ thống thông tin;

+ Biện pháp bảo vệ bí mật nhà nước và phòng, chống lộ, bí mật nhà nước qua các kênh kỹ thuật;

+ Nhân lực bảo vệ an ninh mạng.

Bên cạnh đó Luật quy định cụ thể về việc kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quan trọng về an ninh quốc gia.

- Hoạt động giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia sẽ do cơ quan chủ quản hệ thống thông tin chủ trì, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thực hiện trong suốt quá trình hoạt động; còn lực lượng chuyên trách bảo vệ an ninh mạng tiến hành giám sát chung đối với toàn bộ hệ thống thông tin quan trọng về an ninh quốc gia trong cả nước (Điều 14).

2.5. Ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia (Điều 15)

Để ứng phó, khắc phục các sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, Điều 15 của Luật quy định cụ thể các hoạt động ứng phó, khắc phục, đồng thời giao trách nhiệm cho cơ quan chủ quản trong việc xây dựng, triển khai phương án ứng phó, khắc phục và kịp thời báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền. Việc điều phối hoạt động ứng phó, khắc phục sự cố 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 thuộc Bộ Công an, lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng, Ban Cơ yếu Chính phủ. Cơ quan, tổ chức, cá nhân có trách nhiệm tham gia ứng

phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia khi có yêu cầu của lực lượng chủ trì điều phối

3. Phòng ngừa, xử lý hành vi xâm phạm an ninh mạng (Chương III)

Để bảo vệ tối đa quyền và lợi ích hợp pháp của tổ chức, cá nhân, Chương III Luật An ninh mạng 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 hoại an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế; phòng, chống gián điệm 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.

3.1. Phòng ngừa, xử lý thông tin trên không gia 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

Điều 16 của Luật An ninh mạng quy định:

- Thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm: *(1)* Tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân; *(2)* Chiến tranh tâm lý, kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước; *(3)* Xúc phạm dân dộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc.

- Thông tin trên không gian mạng có nội dung kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng bao gồm: *(1)* Kêu gọi, vận động, xúi giục, đe dọa, lôi kéo, tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tư; *(2)* Kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự.

- Thông tin trên không gian mạng có nội dung làm nhục, vu khống bao gồm: *(1)* Xúc phạm nghiêm trọng danh dự, uy tín, nhân phẩm của người khác; *(2)* Thông tin bịa đặt, sai sự thật xâm phạm danh dự, uy tín, nhân phẩm hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác.

- Thông tin trên không gian mạng có nội dung xâm phạm trật tự quản lý kinh tế bao gồm: *(1)* Thông tin bịa đặt, sai sự

thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá khác; *(2)* Thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp, chứng khoán.

- Thông tin trên không gian mạng có nội dung bịa đặt, sai sự thật gây hoang mạng 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.

Bên cạnh đó, Luật quy định trách nhiệm của cơ quan chủ quản hệ thống thông tin trong việc triển khai biện pháp quản lý, kỹ thuật trên hệ thống thông tin thuộc phạm vi quản lý khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng; trách nhiệm của lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền trong việc xử lý thông tin trên không gian mạng; trách nhiệm của doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng và chủ quản hệ thống thông tin và trách nhiệm của tổ chức,cá nhân đối với thông tin trên không gian mạng.

3.2. Phòng, chống gián điệp mạng; bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng

Điều 17 của Luật An ninh mạng quy định chi tiết các hành vi gián điệp mạng xâm phạm bí mật nhà nước, bí mật

công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng bao gồm:

- Chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân;

- Cố ý xóa, làm hư hỏng, thất lạc, thay đổi thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư được truyền đưa, lưu trữ trên không gian mạng;

- Cố ý thay đổi, hủy bỏ hoặc làm vô hiệu hóa biện pháp kỹ thuật được xây dựng, áp dụng để bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư;

- Đưa lên không gian mạng những thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trái quy định của pháp luật;

- Cố ý nghe, ghi âm, ghi hình trái phép các cuộc đàm thoại;

- Hành vi khác cố ý xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư.

Luật quy định trách nhiệm của chủ quản hệ thống thông tin gồm: Kiểm tra an ninh mạng nhằm phát hiện, loại bỏ mã độc, phần cứng độc hại, khắc phục điểm yếu, lỗ hổng

bảo mật; phát hiện, ngăn chặn và xử lý các hoạt động xâm nhập bất hợp pháp hoặc nguy cơ khác đe dọa an ninh mạng; Triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn hành vi gián điệp mạng, xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin và kịp thời gỡ bỏ thông tin liên quan đến hành vi này; Phối hợp, thực hiện yêu cầu của lực lượng chuyên trách an ninh mạng về phòng, chống gián điệp mạng, bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin.

Bên cạnh đó, quy định trách nhiệm đối với cơ quan soạn thảo, lưu trữ thông tin, tài liệu thuộc bí mật nhà nước; Bộ Công an; Bộ Quốc phòng; Ban Cơ yếu Chính phủ.

3.3. Phòng, chống hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội

Điều 18 Luật An ninh mạng quy định cụ thể, rõ ràng các hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội bao gồm:

- Đăng tải, phát tán thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam (*Tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân; Chiến tranh tâm lý, kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và*

nhân dân các nước; Xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc); Thông tin trên không gian mạng có nội dung kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng (*Kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân; Kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự*); Thông tin trên không gian mạng có nội dung làm nhục, vu khống (*Xúc phạm nghiêm trọng danh dự, uy tín, nhân phẩm của người khác; Thông tin bịa đặt, sai sự thật xâm phạm danh dự, uy tín, nhân phẩm hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác*); Thông tin trên không gian mạng có nội dung xâm phạm trật tự quản lý kinh tế (*Thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá khác; Thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp, chứng khoán*); Thông tin trên không gian mạng có nội dung bịa đặt, 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. Và hành vi gián điệp mạng; xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh

doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng (*Chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; Cố ý xóa, làm hư hỏng, thất lạc, thay đổi thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư được truyền đưa, lưu trữ trên không gian mạng; Cố ý thay đổi, hủy bỏ hoặc làm vô hiệu hóa biện pháp kỹ thuật được xây dựng, áp dụng để bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư; Đưa lên không gian mạng những thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trái quy định của pháp luật; Cố ý nghe, ghi âm, ghi hình trái phép các cuộc đàm thoại; Hành vi khác cố ý xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư*).

- Chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua mạng Internet; trộm cắp cước viễn thông quốc tế trên nền Internet; vi phạm bản quyền và sở hữu trí tuệ trên không gian mạng;

- Giả mạo trang thông tin điện tử của cơ quan, tổ chức, cá nhân; làm giả, lưu hành, trộm cắp, mua bán, thu thập, trao đổi trái phép thông tin thẻ tín dụng, tài khoản ngân hàng của

người khác; phát hành, cung cấp, sử dụng trái phép các phương tiện thanh toán;

- Tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật;

- Hướng dẫn người khác thực hiện hành vi vi phạm pháp luật;

- Hành vi khác sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội.

Luật giao trách nhiệm cho lực lượng chuyên trách bảo vệ an ninh mạng trong việc phòng, chống hành vi sử dựng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc giam trật tự, an toàn xã hội (khoản 2 Điều 18).

3.4. Phòng, chống tấn công mạng

Luật An ninh mạng quy định cụ thể các hành vi tấn công mạng và hành vi có liên quan đến tấn công mạng (Điều 19) bao gồm:

- Phát tán chương trình tin học gây hại cho 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;

- Gây cản trở, rối loạn, làm tê liệt, gián đoạn, ngưng trệ hoạt động, ngăn chặn trái phép việc truyền đưa dữ liệu 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;

- Xâm nhập, làm tổn hại, chiếm đoạt dữ liệu được lưu trữ, truyền đưa qua 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;

- Xâm nhập, tạo ra hoặc khai thác điểm yếu, lỗ hổng bảo mật và dịch vụ hệ thống để chiếm đoạt thông tin, thu lợi bất chính;

- Sản xuất, mua bán, trao đổi, tặng cho công cụ, thiết bị, phần mềm có tính năng tấn công 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 để sử dụng vào mục đích trái pháp luật;

- Hành vi khác gây ảnh hưởng đến hoạt động bình thường 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, giao trách nhiệm cho cơ quan chủ quản hệ thống thông tin trong việc áp dụng biện pháp kỹ thuật để phòng ngừa, ngăn chặn hành vi theo quy định đối với hệ thống thông tin thuộc phạm vi quản lý.

Khi xảy ra tấn công mạng xâm phạm hoặc đe dọa xâm phạm chủ quyền, lợi ích, an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội, lực lượng chuyên trách bảo vệ an ninh mạng chủ trì, phối hợp với chủ quản hệ thống thông tin và tổ chức, cá nhân có liên quan áp dụng biện pháp xác định nguồn gốc tấn công mạng, thu thập chứng cứ; yêu cầu doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet,

các dịch vụ gia tăng trên không gian mạng chặn lọc thông tin để ngăn chặn, loại trừ hành vi tấn công mạng và cung cấp đầy đủ, kịp thời thông tin, tài liệu liên quan.

Bên cạnh đó, Luật quy định cụ thể trách nhiệm của Bộ Công an, Bộ Quốc phòng, Ban Cơ yếu Chính phủ đối với phòng, chống tấn công mạng.

3.5. Phòng, chống khủng bố mạng

Cơ quan nhà nước có thẩm quyền có trách nhiệm áp dụng biện pháp theo quy định của Luật này, Điều 20 của Luật An toàn thông tin mạng (Vô hiệu hóa nguồn Internet sử dụng để thực hiện hành vi khủng bố; Ngăn chặn việc thiết lập và mở rộng trao đổi thông tin về các tín hiệu, nhân tố, phương pháp và cách sử dụng Internet để thực hiện hành vi khủng bố, về mục tiêu và hoạt động của các tổ chức khủng bố trên mạng; Trao đổi kinh nghiệm và thực tiễn kiểm soát các nguồn Internet, tìm và kiểm soát nội dung của trang tin điện tử có mục đích khủng bố) và pháp luật về phòng, chống khủng bố để xử lý khủng bố mạng.

Chủ quản hệ thống thông tin thường xuyên rà soát, kiểm tra hệ thống thông tin thuộc phạm vi quản lý nhằm loại trừ nguy cơ khủng bố mạng.

Khi phát hiện dấu hiệu, hành vi khủng bố mạng, cơ quan, tổ chức, cá nhân phải kịp thời báo cho lực lượng bảo vệ an ninh mạng. Cơ quan tiếp nhận tin báo có trách nhiệm tiếp nhận đầy đủ tin báo về khủng bố mạng và kịp thời thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng.

Bên cạnh đó, Luật quy định cụ thể trách nhiệm của Bộ Công an, Bộ Quốc phòng, Ban Cơ yếu Chính phủ trong phòng, chống khủng bố mạng.

3.6. Phòng, ngừa, xử lý tình huống nguy hiểm về an ninh mạng

Điều 21 Luật An ninh mạng quy định cụ thể các tình huống nguy hiểm về an ninh mạng, bao gồm:

- Xuất hiện thông tin kích động trên không gian mạng có nguy cơ xảy ra bạo loạn, phá rối an ninh, khủng bố;

- Tấn công vào hệ thống thông tin quan trọng về an ninh quốc gia;

- Tấn công nhiều hệ thống thông tin trên quy mô lớn, cường độ cao;

- Tấn công mạng nhằm phá hủy công trình quan trọng về an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia;

- Tấn công mạng xâm phạm nghiêm trọng chủ quyền, lợi ích, an ninh quốc gia; gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

Để phòng ngừa tình huống nguy hiểm về an ninh mạng, Luật đã giao trách nhiệm đối với lực lượng chuyên trách bảo vệ an ninh mạng; doanh nghiệp viễn thông, Internet, công nghệ thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng và cơ quan, tổ chức, cá nhân có liên quan.

- Biện pháp xử lý tình huống nguy hiểm về an ninh mạng bao gồm: Triển khai ngay phương án phòng ngừa, ứng phó khẩn cấp về an ninh mạng, ngăn chặn, loại trừ hoặc giảm nhẹ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra; Thông báo đến cơ quan, tổ chức, cá nhân có liên quan; Thu thập thông tin liên quan; theo dõi, giám sát liên tục đối với tình huống nguy hiểm về an ninh mạng; Phân tích, đánh giá thông tin, dự báo khả năng, phạm vi ảnh hưởng và mức độ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra; Ngừng cung cấp thông tin mạng tại khu vực cụ thể hoặc ngắt cổng kết nối mạng quốc tế; Bố trí lực lượng, phương tiện ngăn chặn, loại bỏ tình huống nguy hiểm về an ninh mạng; Biện pháp khác theo quy định của Luật An ninh quốc gia.

- Việc xử lý tình huống nguy hiểm về an ninh mạng được quy định như sau: Khi phát hiện tình huống nguy hiểm về an ninh mạng, cơ quan, tổ chức, cá nhân kịp thời thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng và áp dụng ngay các biện pháp triển khai ngay phương án phòng ngừa, ứng phó khẩn cấp về an ninh mạng, ngăn chặn, loại trừ hoặc giảm nhẹ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra và thông báo đến cơ quan, tổ chức, cá nhân có liên quan; Thủ tướng Chính phủ xem xét, quyết định hoặc ủy quyền cho Bộ trưởng Bộ Công an xem xét, quyết định, xử lý tình huống nguy hiểm về an ninh mạng trong phạm vi cả nước hoặc từng địa phương hoặc đối với một mục tiêu cụ thể. Thủ tướng Chính phủ xem xét, quyết định hoặc ủy quyền cho Bộ trưởng Bộ Quốc phòng xem xét, quyết định,

xử lý tình huống nguy hiểm về an ninh mạng đối với hệ thống thông tin quân sự và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ; Lực lượng chuyên trách bảo vệ an ninh mạng chủ trì, phối hợp với cơ quan, tổ chức, cá nhân có liên quan áp dụng các biện pháp quy định tại khoản 3 Điều này để xử lý tình huống nguy hiểm về an ninh mạng; Cơ quan, tổ chức, cá nhân có liên quan có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thực hiện biện pháp nhằm ngăn chặn, xử lý tình huống nguy hiểm về an ninh mạng.

3.7. Đấu tranh bảo vệ an ninh mạng

Điều 22 Luật An ninh mạng quy định, đấu tranh bảo vệ an ninh mạng là hoạt động có tổ chức do lực lượng chuyên trách bảo vệ an ninh mạng thực hiện trên không gian mạng nhằm bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội (khoản 1 Điều 22). Theo đó, Luật quy định cụ thể nội dung đấu tranh bảo vệ an ninh mạng bao gồm:

- Tổ chức nắm tình hình có liên quan đến hoạt động bảo vệ an ninh quốc gia;

- Phòng, chống tấn công và bảo vệ hoạt động ổn định của hệ thống thông tin quan trọng về an ninh quốc gia;

- Làm tê liệt hoặc hạn chế hoạt động sử dụng không gian mạng nhằm gây phương hại an ninh quốc gia hoặc gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội;

- Chủ động tấn công vô hiệu hóa mục tiêu trên không gian mạng nhằm bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội.

Đồng thời, Luật giao Bộ Công an chủ trì, phối hợp với Bộ, ngành có liên quan thực hiện đấu tranh bảo vệ an ninh mạng.

4. Hoạt động bảo vệ an ninh mạng

Chương IV 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.

4.1. Triển khai hoạt động bảo vệ an ninh mạng trong cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương

Điều 23 Luật An ninh mạng quy định nội dung triển khai hoạt động bảo vệ an ninh mạng bao gồm:

- Xây dựng, hoàn thiện quy định, quy chế sử dụng mạng máy tính nội bộ, mạng máy tính có kết nối mạng Internet; phương án bảo đảm an ninh mạng đối với hệ thống thông tin; phương án ứng phó, khắc phục sự cố an ninh mạng;

- Ứng dụng, triển khai phương án, biện pháp, công nghệ bảo vệ an ninh mạng đối với hệ thống thông tin và thông tin, tài liệu được lưu trữ, soạn thảo, truyền đưa trên hệ thống thông tin thuộc phạm vi quản lý;

- Tổ chức bồi dưỡng kiến thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động; nâng cao năng lực bảo vệ an ninh mạng cho lực lượng bảo vệ an ninh mạng;

- Bảo vệ an ninh mạng trong hoạt động cung cấp dịch vụ công trên không gian mạng, cung cấp, trao đổi, thu thập thông tin với cơ quan, tổ chức, cá nhân, chia sẻ thông tin trong nội bộ và với cơ quan khác hoặc trong hoạt động khác theo quy định của Chính phủ;

- Đầu tư, xây dựng hạ tầng cơ sở vật chất phù hợp với điều kiện bảo đảm triển khai hoạt động bảo vệ an ninh mạng đối với hệ thống thông tin;

- Kiểm tra an ninh mạng đối với hệ thống thông tin; phòng, chống hành vi vi phạm pháp luật về an ninh mạng; ứng phó, khắc phục sự cố an ninh mạng.

Theo đó, Luật quy định người đứng đầu cơ quan, tổ chức có trách nhiệm triển khai hoạt động bảo vệ an ninh mạng thuộc quyền quản lý.

4.2. Kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia (Điều 24)

Việc kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia được tiến hành trong các trường hợp sau đây:

- Khi có hành vi vi phạm pháp luật về an ninh mạng xâm phạm an ninh quốc gia hoặc gây tổn hại nghiêm trọng trật tự, an toàn xã hội;

- Khi có đề nghị của chủ quản hệ thống thông tin.

Theo đó, đối tượng kiểm tra an ninh mạng được Luật quy định bao gồm:

- Hệ thống phần cứng, phần mềm, thiết bị số được sử dụng trong hệ thống thông tin;

- Thông tin được lưu trữ, xử lý, truyền đưa trong hệ thống thông tin;

- Biện pháp bảo vệ bí mật nhà nước và phòng, chống lộ, mất bí mật nhà nước qua các kênh kỹ thuật.

Đồng thời, Luật giao trách nhiệm cho chủ quản hệ thống thông tin, lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an và các quy định trước thời điểm kiểm tra và sau khi kết thúc kiểm tra. Kết quả kiểm tra an ninh mạng được bảo mật theo quy định của pháp luật.

4.3. Bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế

Điều 25 Luật an ninh mạng quy định bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế phải bảo đảm kết hợp chặt chẽ giữa yêu cầu bảo vệ an ninh mạng với yêu cầu phát triển kinh tế - xã hội; khuyến khích cổng kết nối quốc tế đặt trên lãnh thổ Việt Nam; khuyến khích tổ chức, cá nhân tham gia đầu tư xây dựng cơ sở hạ tầng không gian mạng quốc gia. Theo đó, Luật quy định trách nhiệm cho cơ quan, tổ chức, cá nhân quản lý, khai thác cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế.

4.4. Bảo đảm an ninh thông tin trên không gian mạng

Để đảm bảo an ninh thông tin trên không gian mạng, Điều 26 Luật An ninh mạng quy định đối với Trang thông tin điện tử, cổng thông tin điện tử hoặc chuyên trang trên mạng xã hội của cơ quan, tổ chức, cá nhân không được cung cấp, đăng tải, truyền đưa thông tin có nội dung thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; Thông tin trên không gian mạng có nội dung kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; Thông tin trên không gian mạng có nội dung làm nhục, vu khống; Thông tin trên không gian mạng có nội dung xâm phạm trật tự quản lý kinh tế; Thông tin trên không gian mạng có nội dung bịa đặt, 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 và thông tin khác có nội dung xâm phạm an ninh quốc gia.

Luật An ninh mạng quy định đối với 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 trách nhiệm:

- Xác thực thông tin khi người dùng đăng ký tài khoản số; 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;

- Ngăn chặn việc chia sẻ thông tin, xóa bỏ thông tin có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; Thông tin trên không gian mạng có nội dung kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; Thông tin trên không gian mạng có nội dung làm nhục, vu khống; Thông tin trên không gian mạng có nội dung xâm phạm trật tự quản lý kinh tế; Thông tin trên không gian mạng có nội dung bịa đặt, 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 và thông tin khác có nội dung xâm phạm an ninh quốc gia trên dịch vụ hoặc hệ thống thông tin do cơ quan, tổ chức trực tiếp quản lý chậm

nhất là 24 giờ kể từ thời điểm có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an hoặc cơ quan có thẩm quyền của Bộ Thông tin và Truyền thông và lưu nhật ký hệ thống để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng trong thời gian theo quy định của Chính phủ;

- Không cung cấp hoặc ngừng cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng cho tổ chức, cá nhân đăng tải trên không gian mạng thông tin có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; Thông tin trên không gian mạng có nội dung kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; Thông tin trên không gian mạng có nội dung làm nhục, vu khống; Thông tin trên không gian mạng có nội dung xâm phạm trật tự quản lý kinh tế; Thông tin trên không gian mạng có nội dung bịa đặt, 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 và thông tin khác có nội dung xâm phạm an ninh quốc gia khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an hoặc cơ quan có thẩm quyền của Bộ Thông tin và Truyền thông.

Đối với 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. Đối với doanh nghiệp ngoài nước quy định tại khoản này phải đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam.

Như vậy, doanh nghiệp trong nước 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 xác thực thông tin khi người dùng đăng ký tài khoản số; bảo mật thông tin, tài khoản của người dùng và chỉ trong trường hợp phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng, lực lượng chuyên trách bảo vệ an ninh mạng mới được quyền yêu cầu cung cấp thông tin người dùng.

Mặt khác, thông tin cá nhân vi phạm pháp luật là một trong những loại dữ liệu quan trọng phục vụ điều tra, xử lý hành vi vi phạm pháp luật. Lực lượng bảo vệ pháp luật chỉ được phép yêu cầu cung cấp thông tin trong trường hợp phục vụ xử lý vi phạm pháp luật. Các quy định trong Bộ luật Tố tụng hình sự năm 2015 và các văn bản có liên quan đã quy định rõ về việc quản lý, sử dụng thông tin được cung cấp để phục vụ điều tra, xử lý các hành vi vi phạm pháp luật. Trước các hoạt động vi phạm pháp luật trên không gian mạng đang diễn ra nghiêm trọng, phức tạp, yêu cầu bảo đảm cơ sở, điều kiện để điều tra, xử lý nhanh chóng, hiệu quả của lực lượng bảo vệ pháp luật là cần thiết, cấp bách, trong đó có trách nhiệm của các doanh nghiệp cung cấp dịch vụ trong và ngoài nước.

Có thể thấy, tất cả các quốc gia trên thế giới đều coi an ninh quốc gia là điều kiện tiên quyết hàng đầu. Do đó, các doanh nghiệp cung cấp dịch vụ trên không gian mạng đã và đang phải phối hợp với các cơ quan chức năng của các quốc gia trên thế giới trong bảo vệ an ninh quốc gia, phòng chống tội phạm. Khoản 2 Điều 26 Luật An ninh mạng đã quy định rõ các trường hợp phải cung cấp thông tin cho lực lượng chuyên trách bảo vệ an ninh mạng. Đây là hai điều kiện đồng thời, tức là khi có hành vi vi phạm pháp luật về an ninh mạng xảy ra, khi lực lượng chuyên trách bảo vệ an ninh mạng sẽ có văn bản yêu cầu các doanh nghiệp nêu trên cung cấp thông tin về hành vi vi phạm pháp luật đó. Cần đặc biệt lưu ý rằng, những thông tin cung cấp là thông tin liên quan tới hành vi vi phạm pháp luật.

Doanh nghiệp phải chịu điều chỉnh theo quy định này là những 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 có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu người dùng Việt Nam. Quy định này không áp dụng đối với toàn bộ các doanh nghiệp mà là những doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam, nhưng phải kèm theo điều kiện có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu người dùng Việt Nam. Quy định này là phù hợp với yêu cầu bảo vệ an ninh mạng hiện nay.

Đồng thời, Luật An ninh mạng đã quy định cụ thể 03 loại dữ liệu cần lưu trữ là: Thông tin cá nhân người sử

dụng dịch vụ; 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.

Như vậy, không phải toàn bộ các dữ liệu được truyền đưa trên không gian mạng phải lưu trữ tại Việt Nam. Quy định này không làm ảnh hưởng tới lưu thông dữ liệu số, cản trở hoạt động của doanh nghiệp.

4.5. Nghiên cứu, phát triển an ninh mạng

Điều 27 Luật An ninh mạng quy định, nội dung nghiên cứu, phát triển an ninh mạng bao gồm:

- Xây dựng hệ thống phần mềm, trang thiết bị bảo vệ an ninh mạng;

- Phương pháp thẩm định phần mềm, trang thiết bị bảo vệ an ninh mạng đạt chuẩn và hạn chế tồn tại điểm yếu, lỗ hổng bảo mật, phần mềm độc hại;

- Phương pháp kiểm tra phần cứng, phần mềm được cung cấp thực hiện đúng chức năng;

- Phương pháp bảo vệ bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư; khả năng bảo mật khi truyền đưa thông tin trên không gian mạng;

- Xác định nguồn gốc của thông tin được truyền đưa trên không gian mạng;

- Giải quyết nguy cơ đe dọa an ninh mạng;

- Xây dựng thao trường mạng, môi trường thử nghiệm an ninh mạng;

- Sáng kiến kỹ thuật nâng cao nhận thức, kỹ năng về an ninh mạng;

- Dự báo an ninh mạng;

- Nghiên cứu thực tiễn, phát triển lý luận an ninh mạng.

Bên cạnh đó, Luật quy định cơ quan, tổ chức, cá nhân có liên quan có quyền nghiên cứu, phát triển an ninh mạng.

4.6. Nâng cao năng lực tự chủ về an ninh mạng

Điều 28 Luật An ninh mạng quy định Chính phủ thực hiện các biện pháp nâng cao năng lực tự chủ về an ninh mạng cho cơ quan, tổ chức, cá nhân, gồm: Thúc đẩy chuyển giao, nghiên cứu, làm chủ và phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng để bảo vệ an ninh mạng; Thúc đẩy ứng dụng công nghệ mới, công nghệ tiên tiến liên quan đến an ninh mạng; Tổ chức đào tạo, phát triển và sử dụng nhân lực an ninh mạng; Tăng cường môi trường kinh doanh, cải thiện điều kiện cạnh tranh hỗ trợ doanh nghiệp nghiên cứu, sản xuất sản phẩm, dịch vụ, ứng dụng để bảo vệ an ninh mạng.

4.7. Bảo vệ trẻ em trên không gian mạng

Để đáp ứng yêu cầu thực tiễn, đồng thời thể hiện chính sách bảo vệ trẻ em của Nhà nước ta, Điều 29 Luật An ninh mạng quy định, trẻ em có quyền được bảo vệ, tiếp cận thông tin, tham gia hoạt động xã hội, vui chơi, giải trí, giữ bí mật cá nhân, đời sống riêng tư và các quyền khác khi tham gia trên không gian mạng. Đây là quy định rất tiến bộ trong Luật an ninh mạng. Theo đó, Luật quy định cụ thể trách nhiệm của chủ quản hệ thống thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia

tăng trên không gian mạng; cơ quan, tổ chức cá nhân tham gia hoạt động không gian mạng; cơ quan, tổ chức, cha mẹ, giáo viên, người chăm sóc trẻ em và cá nhân khác liên quan; lực lượng chuyên trách bảo vệ an ninh mạng và các cơ quan chức năng.

5. Bảo đảm hoạt động bảo vệ an ninh mạng

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

Về lực lượng bảo vệ an ninh mạng: Lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Bộ Công an, Bộ Quốc phòng. Lực lượng bảo vệ an ninh mạng được bố trí tại Bộ, ngành, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia. Tổ chức, cá nhân được huy động tham gia bảo vệ an ninh mạng (Điều 30).

Về bảo đảm nguồn nhân lực bảo vệ an ninh mạng: Công dân Việt Nam có kiến thức về an ninh mạng, an toàn thông tin mạng, công nghệ thông tin là nguồn lực cơ bản, chủ yếu bảo vệ an ninh mạng; Nhà nước có chương trình, kế hoạch xây dựng, phát triển nguồn nhân lực bảo vệ an ninh mạng; Khi xảy ra tình huống nguy hiểm về an ninh mạng, khủng bố mạng, tấn công mạng, sự cố an ninh mạng hoặc

nguy cơ đe dọa an ninh mạng, cơ quan nhà nước có thẩm quyền quyết định huy động nhân lực bảo vệ an ninh mạng. Luật quy định thẩm quyền, trách nhiệm, trình tự, thủ tục huy động nhân lực bảo vệ an ninh mạng được thực hiện theo quy định của Luật An ninh quốc gia, Luật Quốc phòng, Luật Công an nhân dân và quy định khác của pháp luật có liên quan (Điều 31).

Theo đó, Luật quy định cụ thể về việc tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh; giáo dục, bồi dưỡng kiến thức, nghiệp vụ an ninh mạng; phổ biến kiến thức về an ninh mạng và kinh phí bảo vệ an ninh mạng.

6. Trách nhiệm của cơ quan, tổ chức, cá nhân

Trách nhiệm của cơ quan, tổ chức, cá nhân cũng được quy định rõ trong Chương VI, 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 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 tí nguy cơ, hạn chế tối đa các hành vi vi phạm pháp luật trên không gian mạng.

6.1. Trách nhiệm của Bộ Công an

Bộ Công an được giao nhiệm vụ tại Điều 36 Luật và được giao các nhiệm vụ cụ thể tại 16 điều luật trong Luật. Theo đó, Điều 36 Luật An ninh mạng quy định Bộ Công an chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an ninh mạng và có nhiệm vụ, quyền hạn sau đây,

trừ nội dung thuộc trách nhiệm của Bộ Quốc phòng và Ban Cơ yếu Chính phủ:

- Ban hành hoặc trình cơ quan nhà nước có thẩm quyền ban hành và hướng dẫn thi hành văn bản quy phạm pháp luật về an ninh mạng;

- Xây dựng, đề xuất chiến lược, chủ trương, chính sách, kế hoạch và phương án bảo vệ an ninh mạng;

- Phòng ngừa, đấu tranh với hoạt động sử dụng không gian mạng xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội và phòng, chống tội phạm mạng;

- Bảo đảm an ninh thông tin trên không gian mạng; xây dựng cơ chế xác thực thông tin đăng ký tài khoản số; cảnh báo, chia sẻ thông tin an ninh mạng, nguy cơ đe dọa an ninh mạng;

- Tham mưu, đề xuất Chính phủ, Thủ tướng Chính phủ xem xét, quyết định việc phân công, phối hợp thực hiện các biện pháp bảo vệ an ninh mạng, phòng ngừa, xử lý hành vi xâm phạm an ninh mạng trong trường hợp nội dung quản lý nhà nước liên quan đến phạm vi quản lý của nhiều Bộ, ngành;

- Tổ chức diễn tập phòng, chống tấn công mạng; diễn tập ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia;

- Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về an ninh mạng.

6.2. *Trách nhiệm của Bộ Quốc phòng*

Điều 37 Luật An ninh mạng quy định Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà

nước về an ninh mạng trong phạm vi quản lý và có nhiệm vụ, quyền hạn sau đây:

- Ban hành hoặc trình cơ quan nhà nước có thẩm quyền ban hành và hướng dẫn thi hành văn bản quy phạm pháp luật về an ninh mạng trong phạm vi quản lý;

- Xây dựng, đề xuất chiến lược, chủ trương, chính sách, kế hoạch và phương án bảo vệ an ninh mạng trong phạm vi quản lý;

- Phòng ngừa, đấu tranh với các hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia trong phạm vi quản lý;

- Phối hợp với Bộ Công an tổ chức diễn tập phòng, chống tấn công mạng, diễn tập ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, triển khai thực hiện công tác bảo vệ an ninh mạng;

- Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về an ninh mạng trong phạm vi quản lý.

6.3. Trách nhiệm của Bộ Thông tin và Truyền thông

Điều 38 Luật An ninh mạng quy định Bộ Thông tin và Truyền thông có trách nhiệm:

- Phối hợp với Bộ Công an, Bộ Quốc phòng trong bảo vệ an ninh mạng;

- Phối hợp với các cơ quan liên quan tổ chức tuyên truyền, phản bác thông tin có nội dung chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam;

- Yêu cầu doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng, chủ quản hệ thống thông tin loại bỏ thông tin có nội dung vi phạm pháp luật về an ninh mạng trên dịch vụ, hệ thống thông tin do doanh nghiệp, cơ quan, tổ chức trực tiếp quản lý.

6.4. Trách nhiệm của Ban Cơ yếu Chính phủ

Điều 39 Luật An ninh mạng quy định Ban Cơ yếu Chính phủ có trách nhiệm:

- Tham mưu, đề xuất Bộ trưởng Bộ Quốc phòng ban hành hoặc trình cơ quan có thẩm quyền ban hành và tổ chức thực hiện văn bản quy phạm pháp luật, chương trình, kế hoạch về mật mã để bảo vệ an ninh mạng thuộc phạm vi Ban Cơ yếu Chính phủ quản lý;

- Bảo vệ an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ và sản phẩm mật mã do Ban Cơ yếu Chính phủ cung cấp theo quy định của Luật này;

- Thống nhất quản lý nghiên cứu khoa học, công nghệ mật mã; sản xuất, sử dụng, cung cấp sản phẩm mật mã để bảo vệ thông tin thuộc bí mật nhà nước được lưu trữ, trao đổi trên không gian mạng.

6.5. Trách nhiệm của Bộ, ngành, Ủy ban nhân dân cấp tỉnh

Điều 40 Luật An ninh mạng quy định trong phạm vi nhiệm vụ, quyền hạn của mình, Bộ, ngành, Ủy ban nhân dân cấp tỉnh có trách nhiệm thực hiện công tác bảo vệ an ninh mạng đối với thông tin, hệ thống thông tin thuộc phạm vi

quản lý; phối hợp với Bộ Công an thực hiện quản lý nhà nước về an ninh mạng của Bộ, ngành, địa phương.

6.6. Trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng

Điều 41 Luật An ninh mạng quy định cụ thể trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng tại Việt Nam, bao gồm:

- Cảnh báo khả năng mất an ninh mạng trong việc sử dụng dịch vụ trên không gian mạng do mình cung cấp và hướng dẫn biện pháp phòng ngừa;

- Xây dựng phương án, giải pháp phản ứng nhanh với sự cố an ninh mạng, xử lý ngay điểm yếu, lỗ hổng bảo mật, mã độc, tấn công mạng, xâm nhập mạng và rủi ro an ninh khác; khi xảy ra sự cố an ninh mạng, ngay lập tức triển khai phương án khẩn cấp, biện pháp ứng phó thích hợp, đồng thời báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng theo quy định của Luật này;

- Áp dụng các giải pháp kỹ thuật và các biện pháp cần thiết khác nhằm bảo đảm an ninh cho quá trình thu thập thông tin, ngăn chặn nguy cơ lộ, lọt, tổn hại hoặc mất dữ liệu; trường hợp xảy ra hoặc có nguy cơ xảy ra sự cố lộ, lọt, tổn hại hoặc mất dữ liệu thông tin người sử dụng, cần lập tức đưa ra giải pháp ứng phó, đồng thời thông báo đến người sử dụng và báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng theo quy định của Luật này;

- Phối hợp, tạo điều kiện cho lực lượng chuyên trách bảo vệ an ninh mạng trong bảo vệ an ninh mạng.

Đồng thời quy định trách nhiệm của Doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam.

6.7. Trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng

Điều 42 Luật An ninh mạng quy định trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng bao gồm:

- Tuân thủ quy định của pháp luật về an ninh mạng;

- Kịp thời cung cấp thông tin liên quan đến bảo vệ an ninh mạng, nguy cơ đe dọa an ninh mạng, hành vi xâm phạm an ninh mạng cho cơ quan có thẩm quyền, lực lượng bảo vệ an ninh mạng;

- Thực hiện yêu cầu và hướng dẫn của cơ quan có thẩm quyền trong bảo vệ an ninh mạng; giúp đỡ, tạo điều kiện cho cơ quan, tổ chức và người có trách nhiệm tiến hành các biện pháp bảo vệ an ninh mạng.

MỤC LỤC

Chịu trách nhiệm xuất bản
ĐẶNG VĂN NGUYÊN
Giám đốc Sở Tư pháp

Chịu trách nhiệm nội dung
LÊ ANH TUẤN
Phó Giám đốc Sở Tư pháp

Biên soạn
NGUYỄN THỊ PHƯƠNG LINH

In cuốn, khổ 14,5cm x 20,5cm
Tại Công ty TNHH Tính toán, In và Thương mại Bắc Giang
Số 22, đường Ngô Văn Cảnh, phường Ngô Quyền, TP Bắc Giang
Giấy phép xuất bản số:
Do Sở TT&TT tỉnh Bắc Giang cấp
In xong và nộp lưu chiểu năm 2019.