SỞ TƯ PHÁP TỈNH TUYÊN QUANG

ĐỀ CƯƠNG GIỚI THIỆU
Luật An ninh mạng và Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ Quy định chi tiết một số điều của Luật An ninh mạng

Ngày 12 tháng 6 năm 2018, tại kỳ họp thứ 5, Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam khóa XIV đã thông qua Luật An ninh mạng số 24/2018/QH14; Chủ tịch nước ký Lệnh công bố số 06/2018/L-CTN ngày 25/6/2018; Luật có hiệu lực thi hành từ ngày 01/01/2019. Ngày 15/8/2022 Chính phủ đã ban hành Nghị định số 53/2022/NĐ-CP Quy định chi tiết một số điều của Luật An ninh mạng, có hiệu lực từ ngày 01/10/2022.

Sở Tư pháp tỉnh Tuyên Quang giới thiệu một số nội dung của Luật An ninh mạng và Nghị định số 53/2022/NĐ-CP.

I. NHỮNG QUY ĐỊNH CHUNG

1. Giải thích từ ngữ

**** Điều 2 Luật An ninh mạng giải thích 14 từ ngữ, cụ thể như sau:***

(1) 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.

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

(3) 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.

(4) Không gian mạng quốc gia là không gian mạng do Chính phủ xác lập, quản lý và kiểm soát.

(5) Cơ sở hạ tầng không gian mạng quốc gia là hệ thống cơ sở vật chất, kỹ thuật để tạo lập, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên không gian mạng quốc gia, bao gồm:

- Hệ thống truyền dẫn bao gồm hệ thống truyền dẫn quốc gia, hệ thống truyền dẫn kết nối quốc tế, hệ thống vệ tinh, hệ thống truyền dẫn của doanh

nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng;

- Hệ thống các dịch vụ lõi bao gồm hệ thống phân luồng và điều hướng thông tin quốc gia, hệ thống phân giải tên miền quốc gia (DNS), hệ thống chứng thực quốc gia (PKI/CA) và hệ thống cung cấp dịch vụ kết nối, truy cập Internet của doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng;

- Dịch vụ, ứng dụng công nghệ thông tin bao gồm dịch vụ trực tuyến; ứng dụng công nghệ thông tin có kết nối mạng phục vụ quản lý, điều hành của cơ quan, tổ chức, tập đoàn kinh tế, tài chính quan trọng; cơ sở dữ liệu quốc gia.

Dịch vụ trực tuyến bao gồm chính phủ điện tử, thương mại điện tử, trang thông tin điện tử, diễn đàn trực tuyến, mạng xã hội, blog;

- Cơ sở hạ tầng công nghệ thông tin của đô thị thông minh, Internet vạn vật, hệ thống phức hợp thực - ảo, điện toán đám mây, hệ thống dữ liệu lớn, hệ thống dữ liệu nhanh và hệ thống trí tuệ nhân tạo.

(6) Cổng kết nối mạng quốc tế là nơi diễn ra hoạt động chuyển nhận tín hiệu mạng qua lại giữa Việt Nam và các quốc gia, vùng lãnh thổ khác.

(7) 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.

(8) 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.

(9) 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.

(10) 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.

(11) 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.

(12) 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.

(13) 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.

(14) 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.

**** Điều 2 Nghị định số 53/2022/NĐ-CP giải thích từ ngữ 12 từ ngữ sau:***

(1) Dữ liệu về thông tin cá nhân là dữ liệu về thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự để xác định danh tính một cá nhân.

(2) Người sử dụng dịch vụ là tổ chức, cá nhân tham gia sử dụng dịch vụ trên không gian mạng.

(3) Người sử dụng dịch vụ tại Việt Nam là tổ chức, cá nhân sử dụng không gian mạng trên lãnh thổ nước Cộng hòa xã hội chủ nghĩa Việt Nam.

(4) Dữ liệu về mối quan hệ của người sử dụng dịch vụ là dữ liệu về thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự phản ánh, xác định mối quan hệ của người sử dụng dịch vụ với người khác trên không gian mạng.

(5) Dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra là dữ liệu về thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự phản ánh quá trình tham gia, hoạt động, sử dụng không gian mạng của người sử dụng dịch vụ và các thông tin về thiết bị, dịch vụ mạng sử dụng để kết nối với không gian mạng trên lãnh thổ nước Cộng hòa xã hội chủ nghĩa Việt Nam.

(6) Dịch vụ trên mạng viễn thông là dịch vụ viễn thông, dịch vụ ứng dụng viễn thông theo quy định của pháp luật.

(7) Dịch vụ trên mạng Internet là dịch vụ Internet và dịch vụ cung cấp nội dung trên nền internet theo quy định của pháp luật.

(8) Dịch vụ gia tăng trên không gian mạng là dịch vụ viễn thông giá trị gia tăng theo quy định của pháp luật.

(9) Lực lượng chuyên trách bảo vệ an ninh mạng bao gồm:

- Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an;

- Cục Bảo vệ an ninh Quân đội, Tổng cục Chính trị và Bộ Tư lệnh Tác chiến không gian mạng thuộc Bộ Quốc phòng.

(10) Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia là cơ quan, tổ chức có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin quan trọng về an ninh quốc gia, gồm những trường hợp sau:

- Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;

- Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương;

- Các tổ chức chính trị ở Trung ương;

- Cấp có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin quan trọng về an ninh quốc gia.

(11) Doanh nghiệp trong nước là doanh nghiệp được thành lập hoặc đăng ký thành lập theo pháp luật Việt Nam và có trụ sở chính tại Việt Nam.

(12) Doanh nghiệp nước ngoài là doanh nghiệp được thành lập hoặc đăng ký thành lập theo pháp luật nước ngoài.

2. Chính sách của Nhà nước về an ninh mạng

Điều 3 Luật An ninh mạng quy định Nhà nước có những chính sách sau về an ninh mạng:

Một là, 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;

Hai là, 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;

Ba là, 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;

Bốn là, 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;

Năm là, tăng cường hợp tác quốc tế về an ninh mạng.

3. 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:

(1) 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;

(2) 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;

(3) 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;

(4) 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;

(5) 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;

(6) 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;

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

4. Biện pháp bảo vệ an ninh mạng

Luật An ninh mạng 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 An ninh mạng quy định các biện pháp bảo vệ an ninh mạng bao gồm:

(1) Thẩm định an ninh mạng;

(2) Đáng giá điều kiện an ninh mạng;

(3) Kiểm tra an ninh mạng;

(4) Giám sát an ninh mạng;

(5) Ứng phó, khắc phục sự cố an ninh mạng;

(6) Đấu tranh, bảo vệ an ninh mạng;

(7) Sử dụng mật mã để bảo vệ thông tin mạng;

(8) 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;

(9) 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;

(10) 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;

(11) Khởi tố, điều tra, truy tố, xét xử theo quy định của Bộ luật Tố tụng hình sự;

(12) 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.

**** Nghị định số 53/2022/NĐ-CP quy định cụ thể 09 biện pháp bảo vệ an ninh mạng, gồm:***

4.1. Trình tự, thủ tục thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia (Điều 13 Nghị định số 53/2022/NĐ-CP)

- Về thẩm quyền: Thẩm định an ninh mạng đối với hệ thống thông tin thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia do **lực lượng chuyên trách bảo vệ an ninh mạng** thực hiện theo quy định.

- Trình tự thực hiện thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

+ Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia nộp hồ sơ đề nghị thẩm định an ninh mạng cho lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền;

+ Lực lượng chuyên trách bảo vệ an ninh mạng tiếp nhận, kiểm tra, hướng dẫn hoàn thiện hồ sơ đề nghị thẩm định an ninh mạng và cấp giấy tiếp nhận ngay sau khi nhận đủ hồ sơ hợp lệ trong thời gian 03 ngày làm việc;

+ Lực lượng chuyên trách bảo vệ an ninh mạng tiến hành thẩm định an ninh mạng và thông báo kết quả trong thời hạn 30 ngày, kể từ ngày cấp giấy tiếp nhận hồ sơ cho chủ quản hệ thống thông tin quan trọng về an ninh quốc gia.

- Hồ sơ đề nghị thẩm định đối với hệ thống thông tin quan trọng về an ninh quốc gia, bao gồm:

+ Văn bản đề nghị thẩm định an ninh mạng (Mẫu số 06 Phụ lục);

+ 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 trong trường hợp nâng cấp hệ thống thông tin quan trọng về an ninh quốc gia.

- Trường hợp cần xác định sự phù hợp giữa hiện trạng của hệ thống thông tin quan trọng về an ninh quốc gia và hồ sơ đề nghị thẩm định, lực lượng chuyên trách bảo vệ an ninh mạng tiến hành khảo sát, đánh giá hiện trạng thực tế của hệ thống thông tin quan trọng về an ninh quốc gia để đối chiếu với hồ sơ đề nghị thẩm định. Việc khảo sát, đánh giá thực tế bảo đảm không gây ảnh hưởng tới hoạt động bình thường của chủ quản cũng như hệ thống thông tin quan trọng về an ninh quốc gia. Thời gian khảo sát, đánh giá thực tế không quá 07 ngày làm việc.

- Kết quả thẩm định an ninh mạng được bảo vệ theo quy định của pháp luật.

4.2. Trình tự, thủ tục đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia (Điều 14 Nghị định số 53/2022/NĐ-CP)

- Về thẩm quyền: Đánh giá điều kiện an ninh mạng đối với hệ thống thông tin thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia **do lực lượng chuyên trách bảo vệ an ninh mạng** thực hiện theo quy định.

- Trình tự đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia:

+ Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia nộp hồ sơ đề nghị đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia cho lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền đánh giá điều kiện an ninh mạng;

+ Lực lượng chuyên trách bảo vệ an ninh mạng tiếp nhận, kiểm tra, hướng dẫn hoàn thiện hồ sơ đề nghị đánh giá điều kiện an ninh mạng và cấp giấy tiếp nhận ngay sau khi nhận đủ hồ sơ hợp lệ;

+ Sau khi tiếp nhận đủ hồ sơ hợp lệ, lực lượng chuyên trách bảo vệ an ninh mạng tiến hành đánh giá điều kiện an ninh mạng và thông báo kết quả trong thời hạn 30 ngày, kể từ ngày cấp giấy tiếp nhận đủ hồ sơ hợp lệ của chủ quản hệ thống thông tin quan trọng về an ninh quốc gia;

+ Trường hợp đủ điều kiện an ninh mạng, Thủ trưởng cơ quan đánh giá điều kiện an ninh mạng cấp Giấy chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia trong vòng 03 ngày làm việc kể từ khi kết thúc đánh giá điều kiện an ninh mạng.

- Hồ sơ đề nghị chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm:

+ Văn bản đề nghị chứng nhận điều kiện an ninh mạng (Mẫu số 07 Phụ lục);

+ 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;

+ Hồ sơ giải pháp bảo đảm an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.

- Trường hợp không bảo đảm điều kiện an ninh mạng, lực lượng chuyên trách bảo vệ an ninh mạng yêu cầu chủ quản hệ thống thông tin quan trọng về an ninh quốc gia bổ sung, nâng cấp hệ thống thông tin quan trọng về an ninh quốc gia đê bảo đảm đủ điều kiện.

4.3. Trình tự, thủ tục giám sát an ninh mạng (Điều 15 Nghị định số 53/2022/NĐ-CP)

- Về thẩm quyền: Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an, Bộ Tư lệnh Tác chiến Không gian mạng thuộc Bộ Quốc phòng có trách nhiệm thực hiện giám sát an ninh mạng đối với không gian mạng quốc gia, hệ thống thông tin quan trọng về an ninh quốc gia theo chức năng, nhiệm vụ được giao. Ban Cơ yếu Chính phủ thực hiện giám sát an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ theo chức năng, nhiệm vụ được giao.

- Trình tự giám sát an ninh mạng của lực lượng chuyên trách bảo vệ an ninh mạng:

+ Gửi thông báo bằng văn bản yêu cầu triển khai biện pháp giám sát an ninh mạng tới chủ quản hệ thống thông tin; trong văn bản nêu rõ lý do, thời gian, nội dung và phạm vi tiến hành giám sát an ninh mạng;

+ Triển khai biện pháp giám sát an ninh mạng;

+ Định kỳ thống kê, báo cáo kết quả giám sát an ninh mạng.

- Trách nhiệm của chủ quản hệ thống thông tin quan trọng về an ninh quốc gia:

+ Xây dựng, triển khai hệ thống giám sát an ninh mạng, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thực hiện hoạt động giám sát an ninh mạng đối với hệ thống thông tin thuộc thẩm quyền quản lý;

+ Bố trí mặt bằng, điều kiện kỹ thuật, thiết lập, kết nối hệ thống, thiết bị giám sát của lực lượng chuyên trách bảo vệ an ninh mạng vào hệ thống thông tin do mình quản lý để phục vụ giám sát an ninh mạng;

+ Cung cấp và cập nhật thông tin về hệ thống thông tin thuộc thẩm quyền quản lý, phương án kỹ thuật triển khai hệ thống giám sát cho lực lượng chuyên trách bảo vệ an ninh mạng theo định kỳ hoặc đột xuất khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền;

+Thông báo với lực lượng chuyên trách bảo vệ an ninh mạng về hoạt động giám sát của chủ quản hệ thống thông tin định kỳ 03 tháng một lần;

+ Bảo mật các thông tin liên quan trong quá trình phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng.

- Doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ công nghệ thông tin, viễn thông, internet có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng trong giám sát an ninh mạng theo thẩm quyền nhằm bảo vệ an ninh mạng.

- Kết quả giám sát an ninh mạng được bảo mật theo quy định của pháp luật.

4.4. Trình tự, thủ tục kiểm tra an ninh mạng (Điều 16 Nghị định số 53/2022/NĐ-CP)

- Về thẩm quyền: Lực lượng chuyên trách bảo vệ an ninh mạng tiến hành kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quan trọng về an ninh quốc gia và 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.

- Nội dung kiểm tra an ninh mạng, bao gồm: kiểm tra việc tuân thủ các quy định của pháp luật về bảo đảm an ninh mạng, bảo vệ bí mật nhà nước trên

không gian mạng; kiểm tra, đánh giá hiệu quả các phương án, biện pháp bảo đảm an ninh mạng, phương án, kế hoạch ứng phó, khắc phục sự cố an ninh mạng; kiểm tra, đánh giá phát hiện lỗ hổng, điểm yếu bảo mật, mã độc và tấn công thử nghiệm xâm nhập hệ thống; kiểm tra, đánh giá khác do chủ quản hệ thống thông tin quy định.

- Trình tự, thủ tục kiểm tra an ninh mạng của lực lượng chuyên trách bảo vệ an ninh mạng:

+ Thông báo về kế hoạch kiểm tra an ninh mạng theo quy định;

+ Thành lập Đoàn kiểm tra theo chức năng, nhiệm vụ được giao;

+ Tiến hành kiểm tra an ninh mạng, phối hợp chặt chẽ với chủ quản hệ thống thông tin trong quá trình kiểm tra;

+ Lập biên bản về quá trình, kết quả kiểm tra an ninh mạng và bảo quản theo quy định của pháp luật;

+ Thông báo kết quả kiểm tra an ninh mạng trong 03 ngày làm việc kể từ ngày hoàn thành kiểm tra.

- Trường hợp cần giữ nguyên hiện trạng hệ thống thông tin, phục vụ điều tra, xử lý hành vi vi phạm pháp luật, phát hiện điểm yếu, lỗ hổng bảo mật; hướng dẫn hoặc tham gia khắc phục khi có đề nghị của chủ quản hệ thống thông tin, lực lượng chuyên trách bảo vệ an ninh mạng gửi văn bản đề nghị chủ quản hệ thống thông tin tạm ngừng tiến hành kiểm tra an ninh mạng. Nội dung văn bản phải ghi rõ lý do, mục đích, thời gian tạm ngừng hoạt động kiểm tra an ninh mạng.

4.5. Trình tự, thủ tục ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia (Điều 17 Nghị định số 53/2022/NĐ-CP)

- Đối với các hệ thống thông tin quan trọng về an ninh quốc gia khi gặp sự cố an ninh mạng thì thực hiện trình tự, thủ tục ứng phó, khắc phục sự cố như sau:

+ Lực lượng chuyên trách bảo vệ an ninh mạng thông báo bằng văn bản và hướng dẫn biện pháp tạm thời để ngăn chặn, xử lý hoạt động tấn công mạng, khắc phục hậu quả do tấn công mạng, sự cố an ninh mạng cho chủ quản hệ thống thông tin quan trọng về an ninh quốc gia.

Trường hợp khẩn cấp, thông báo bằng điện thoại hoặc các hình thức khác trước khi thông báo bằng văn bản;

+ Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm thực hiện các biện pháp theo hướng dẫn và các biện pháp phù hợp khác để ngăn chặn, xử lý, khắc phục hậu quả ngay sau khi nhận được thông báo, trừ quy định tại điểm c khoản này.

Trường hợp vượt quá khả năng xử lý, kịp thời thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng để điều phối, ứng phó khắc phục sự cố an ninh mạng;

+ Trường hợp cần ứng phó ngay để ngăn chặn hậu quả xảy ra có khả năng gây nguy hại cho an ninh quốc gia, lực lượng chuyên trách bảo vệ an ninh mạng quyết định trực tiếp điều phối, ứng phó khắc phục sự cố an ninh mạng.

- Điều phối, ứng phó khắc phục sự cố an ninh mạng của lực lượng chuyên trách bảo vệ an ninh mạng:

+ Đánh giá, quyết định phương án ứng phó, khắc phục sự cố an ninh mạng;

+ Điều hành công tác ứng phó, khắc phục sự cố an ninh mạng;

+ Chủ trì tiếp nhận, thu thập, xử lý, trao đổi thông tin về ứng phó, khắc phục sự cố an ninh mạng;

+ Huy động, phối hợp với các tổ chức, cá nhân trong và ngoài nước có liên quan tham gia ứng phó, khắc phục sự cố an ninh mạng trong trường hợp cần thiết;

+ Chỉ định đơn vị đầu mối phối hợp với các đơn vị chức năng của các quốc gia khác hoặc các tổ chức quốc tế trong hoạt động ứng phó, xử lý các sự cố liên quốc gia trên cơ sở thỏa thuận quốc tế hoặc điều ước quốc tế mà Việt Nam là thành viên;

+ Kiểm tra, giám sát, đôn đốc việc thực hiện của các đơn vị liên quan ứng phó, khắc phục sự cố an ninh mạng;

+ Lập biên bản quá trình ứng cứu sự cố an ninh mạng.

- Tổ chức, cá nhân tham gia ứng phó, khắc phục sự cố an ninh mạng có trách nhiệm thực hiện các biện pháp, hoạt động ứng phó, khắc phục sự cố theo sự điều phối của lực lượng chuyên trách bảo vệ an ninh mạng.

- Trường hợp bảo vệ an ninh quốc gia, trật tự an toàn xã hội, doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ Internet bố trí mặt bằng, cổng kết nối và các biện pháp kỹ thuật cần thiết để Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an thực hiện nhiệm vụ bảo đảm an ninh mạng. Thủ tục, quy trình cụ thể, doanh nghiệp viễn thông,

doanh nghiệp cung cấp dịch vụ Internet phối hợp với Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an thực hiện.

4.6. Trình tự, thủ tục thực hiện biện pháp sử dụng mật mã để bảo vệ thông tin mạng (Điều 18 Nghị định số 53/2022/NĐ-CP)

- Lực lượng chuyên trách bảo vệ an ninh mạng sử dụng các biện pháp mã hóa bằng mật mã của cơ yếu để bảo vệ thông tin mạng khi truyền đưa thông tin, tài liệu có nội dung thuộc bí mật nhà nước trên không gian mạng. Các biện pháp mã hóa phải bảo đảm các yêu cầu theo quy định của pháp luật về cơ yếu, bảo vệ bí mật nhà nước, an ninh mạng.

- Trường hợp cần thiết vì lý do an ninh quốc gia, trật tự an toàn xã hội, bảo vệ quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân, lực lượng chuyên trách bảo vệ an ninh mạng gửi văn bản yêu cầu các cơ quan, tổ chức, cá nhân có liên quan thực hiện mã hóa các thông tin không nằm trong phạm vi bí mật nhà nước trước khi tiến hành lưu trữ, truyền đưa trên mạng Internet. Nội dung văn bản phải nêu rõ lý do yêu cầu, nội dung cần mã hóa.

4.7. Trình tự, thủ tục thực hiện biện pháp yêu cầu xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật 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 (Điều 19 Nghị định số 53/2022/NĐ-CP)

- Trường hợp áp dụng biện pháp:

+ Khi thông tin trên không gian mạng được cơ quan có thẩm quyền xác định là có nội dung xâm phạm an ninh quốc gia, 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 theo quy định của pháp luật;

+ Khi có căn cứ pháp luật xác định thông tin trên không gian mạng có nội dung làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế; bịa đặt, sai sự thật gây hoang mang trong nhân dân, gây thiệt hại nghiêm trọng cho hoạt động kinh tế - xã hội đến mức phải yêu cầu xóa bỏ thông tin;

+ Các thông tin trên không gian mạng khác có nội dung 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; 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.

- Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an, Thủ trưởng cơ quan có thẩm quyền của Bộ Thông tin và Truyền thông:

+ Quyết định áp dụng biện pháp yêu cầu xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật 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;

+ Gửi văn bản yêu cầu các doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, dịch vụ trên mạng Internet, dịch vụ gia tăng trên không gian mạng, chủ quản hệ thống thông tin xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật 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;

+ Kiểm tra việc chấp hành thực hiện biện pháp của các chủ thể có liên quan được yêu cầu;

+ Trao đổi, chia sẻ thông tin về việc thực hiện biện pháp này, trừ trường hợp nội dung thuộc phạm vi bí mật nhà nước hoặc yêu cầu nghiệp vụ của Bộ Công an.

- Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng quyết định áp dụng biện pháp yêu cầu xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên không gian mạng xâm phạm an ninh quốc gia, an ninh quân đội đối với hệ thống thông tin quân sự.

4.8. Trình tự, thủ tục thực hiện biện pháp thu thập dữ liệu điện tử liên quan đến hoạt động 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 trên không gian mạng (Điều 20 Nghị định số 53/2022/NĐ-CP)

- Dữ liệu điện tử là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự.

- Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an quyết định tiến hành biện pháp thu thập dữ liệu điện tử để phục vụ điều tra, xử lý các hành vi 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 trên không gian mạng.

- Việc thu thập dữ liệu điện tử liên quan đến hoạt động 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 trên không gian mạng được thực hiện theo quy định của pháp luật; đồng thời bảo đảm các yêu cầu sau:

+ Giữ nguyên hiện trạng của thiết bị số, dữ liệu điện tử;

+ Việc sao ghi dữ liệu điện tử phải được thực hiện đúng quy trình bằng các thiết bị, phần mềm được công nhận, có thể kiểm chứng được, phải bảo vệ được tính nguyên vẹn của dữ liệu điện tử lưu trong thiết bị;

+ Quá trình khôi phục dữ liệu, tìm kiếm dữ liệu điện tử phải được ghi nhận lại bằng biên bản, hình ảnh, video, khi cần thiết có thể lặp lại quá trình đi tới kết quả tương tự để trình bày tại tòa án;

+ Người thực hiện thu thập dữ liệu điện tử phải là cán bộ chuyên trách được giao thực hiện nhiệm vụ thu thập dữ liệu điện tử.

- Nguyên tắc sao chép, phục hồi dữ liệu điện tử liên quan đến hoạt động 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 trên không gian mạng:

+ Trường hợp dữ liệu điện tử được cho là có giá trị chứng minh tội phạm mà cần phải sao chép, phục hồi hoặc nếu muốn sao chép, phục hồi dữ liệu điện tử, người thực hiện sao chép, phục hồi phải có thẩm quyền để sao chép, phục hồi và phải quyết định của cấp có thẩm quyền theo quy định của pháp luật;

+ Lập biên bản cho các hoạt động sao chép, phục hồi chứng cứ điện tử, trường hợp cần thiết có thể mời một bên thứ ba độc lập tham gia, chứng kiến, xác nhận quy trình này.

- Thu giữ phương tiện lưu trữ, truyền đưa, xử lý dữ liệu điện tử liên quan đến hoạt động 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 trên không gian mạng được thực hiện theo quy định pháp luật.

- Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng quyết định áp dụng biện pháp thu thập dữ liệu điện tử để phục vụ điều tra các vụ việc vi phạm, tội phạm gây mất an ninh, an toàn thông tin, xâm phạm an ninh quốc gia, an ninh quân đội trên không gian mạng.

4.9. Trình tự, thủ tục thực hiện biện pháp đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, thu hồi tên miền (Điều 21 Nghị định số 53/2022/NĐ-CP)

- Trường hợp áp dụng biện pháp:

+ Có tài liệu chứng minh hoạt động của hệ thống thông tin là vi phạm pháp luật về an ninh quốc gia, an ninh mạng;

+ Hệ thống thông tin đang được sử dụng vào mục đích xâm phạm an ninh quốc gia, trật tự an toàn xã hội.

- Thẩm quyền áp dụng biện pháp:

+ Bộ trưởng Bộ Công an trực tiếp quyết định đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, tạm ngừng, thu hồi tên miền có hoạt động vi phạm pháp luật về an ninh mạng.

+ Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an có trách nhiệm thực hiện quyết định đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, tạm ngừng, thu hồi tên miền.

- Trình tự, thủ tục thực hiện biện pháp:

+ Báo cáo về việc áp dụng biện pháp đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, tạm ngừng, thu hồi tên miền;

+ Quyết định đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, tạm ngừng, thu hồi tên miền;

+ Gửi văn bản yêu cầu các cơ quan, tổ chức, cá nhân có liên quan thực hiện đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin hoặc gửi Trung tâm Internet Việt Nam đề nghị tạm ngừng, thu hồi tên miền theo trình tự, thủ tục được pháp luật quy định; văn bản yêu cầu nêu rõ lý do, thời gian, nội dung và kiến nghị;

+ Trong trường hợp cấp bách, cần ngăn chặn kịp thời hoạt động của hệ thống thông tin tránh gây nguy hại cho an ninh quốc gia hoặc cần ngăn chặn hậu quả tác hại có thể xảy ra, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an yêu cầu trực tiếp hoặc bằng văn bản qua fax, email để yêu cầu cơ quan, tổ chức, cá nhân đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin;

Trong thời gian chậm nhất là 24 giờ kể từ khi có yêu cầu, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an phải gửi văn bản yêu cầu đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin. Trường hợp quá thời hạn trên mà không có quyết định bằng văn bản thì hệ thống thông tin được tiếp tục hoạt động. Tùy theo tính chất, mức độ, hậu quả xảy ra do việc chậm trễ gửi văn bản yêu cầu, cán bộ thực hiện và những người có liên quan phải chịu trách nhiệm theo quy định của pháp luật;

+ Việc đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin phải được lập thành biên bản. Biên bản phải ghi rõ thời gian, địa điểm, căn cứ và được lập thành 02 bản. Cơ quan chức năng có thẩm quyền giữ một bản, cơ quan, tổ chức, cá nhân sở hữu, quản lý hệ thống thông tin giữ một bản;

+ Việc tạm ngừng, thu hồi tên miền quốc gia trong các trường hợp này, cơ quan chức năng có thẩm quyền gửi văn bản đề nghị Trung tâm Internet Việt Nam tạm ngừng, thu hồi tên miền theo trình tự, thủ tục được pháp luật quy định.

- Việc đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin mà không có căn cứ thì Thủ trưởng, Phó Thủ trưởng cơ quan chức năng có thẩm quyền và cán bộ có liên quan phải chịu trách nhiệm trước pháp luật, nếu gây thiệt hại cho cơ quan, tổ chức, cá nhân có liên quan thì phải bồi thường theo quy định của pháp luật.

5. Hợp tác quốc tế về an ninh mạng

Luật An ninh mạng 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 (khoản 1 Điều 7). Trên cơ sở đó, Luật quy định cụ thể nội dung hợp tác quốc tế về an ninh mạng (khoản 2 Điều 7), 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 (khoản 3 Điều 7).

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 (khoản 4 Điều 7).

6. 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)

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:

(1) Sử dụng không gian mạng để thực hiện hành vi sau đây: (a) Hành vi quy định tại khoản 1 Điều 18 của Luật *(Đăng tải, phát tán thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều 16 và hành vi quy định tại khoản 1 Điều 17 của Luật; 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); (b) 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; (c) 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; (d) 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; (đ) 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; (e) Xúi giục, lôi kéo, kích động người khác phạm tội;

(2) 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;

(3) 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;

(4) 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;

(5) 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; (6) 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; không 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 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).

II. BẢO VỆ AN NINH MẠNG ĐỐI VỚI HỆ THỐNG THÔNG TIN QUAN TRỌNG VỀ AN NINH QUỐC GIA

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.

1. Về hệ thống thông tin quan trọng về an ninh quốc gia (Điều 10 Luật An ninh mạng)

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 (khoản 1 Điều 10).

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: (1) Hệ thống thông tin quân sự, an ninh, ngoại giao, cơ yếu; (2) Hệ thống thông tin lưu trữ, xử lý thông tin thuộc bí mật nhà nước; (3) Hệ thống thông tin phục vụ lưu giữ, bảo quản hiện vật, tài liệu có giá trị đặc biệt quan trọng; (4) 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; (5) 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; (6) Hệ thống thông tin quan trọng phục vụ hoạt động của cơ quan, tổ chức ở trung ương; (7) 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; (8) 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 (khoản 2 Điều 10).

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 (khoản 3 Điều 10). 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.

**** Nghị định số 53/2022/NĐ-CP hướng dẫn thực hiện các nội dung được Luật giao (Mục I Chương II), cụ thể:***

1.1. Quy định về xác lập danh mục hệ thống thông tin quan trọng về an ninh quốc gia (Điều 3, 4 và 5 Nghị định số 53/2022/NĐ-CP)

Nghị định số 53/2022/NĐ-CP quy định cụ thể về căn cứ xác lập hệ thống thông tin quan trọng về an ninh quốc gia; lập hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia; thẩm định hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia

1.2. Đưa hệ thống thông tin ra khỏi danh mục hệ thống thông tin quan trọng về an ninh quốc gia (Điều 6 Nghị định số 53/2022/NĐ-CP)

Nghị định số 53/2022/NĐ-CP quy định cụ thể các trường hợp, hồ sơ, trình tự, thủ tục đưa hệ thống thông tin ra khỏi danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

1.3. Phối hợp 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 7 Nghị định số 53/2022/NĐ-CP)

- Việc bảo vệ an ninh mạng, an toàn thông tin mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia được thực hiện theo quy định của pháp luật về an ninh mạng, an toàn thông tin mạng.

- Nguyên tắc phối hợp

+ Áp dụng quy định của pháp luật về an ninh mạng, an toàn thông tin mạng đối với 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;

+ Trường hợp cần có sự phối hợp của nhiều bên liên quan, Bộ Công an, Bộ Quốc phòng, Ban Cơ yếu Chính phủ căn cứ Luật An ninh mạng chủ trì, phối hợp với Bộ Thông tin và Truyền thông, các bộ, ngành có liên quan tổ chức thẩm định, đánh giá, kiểm tra, giám sát, ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia theo chức năng, nhiệm vụ được giao;

+ Quá trình phối hợp bảo đảm tuân thủ quy định của các điều ước quốc tế và các quy định của tổ chức quốc tế mà Việt Nam tham gia, Luật An ninh mạng và pháp luật có liên quan, chủ động, thường xuyên, kịp thời và đúng chức năng, nhiệm vụ, quyền hạn được giao.

- Phương thức phối hợp

+ Bộ Công an gửi văn bản đề nghị các bộ, ngành có liên quan cử thành viên tham gia thẩm định, đánh giá, kiểm tra, giám sát, ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia;

+ Các bộ, ngành có liên quan có trách nhiệm cử thành viên tham gia đầy đủ các hoạt động trong quá trình thẩm định, đánh giá, kiểm tra, giám sát, ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia theo nội dung đề nghị;

+ Hồ sơ, văn bản tài liệu phục vụ thẩm định, đánh giá, kiểm tra, giám sát, ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia được Bộ Công an sao gửi tới thành viên tham gia theo quy định.

- Việc phối hợp giám sát đối với hệ thống thông tin quan trọng về an ninh quốc gia phục vụ công tác bảo vệ an ninh mạng, an toàn thông tin mạng:

+ Các lực lượng chuyên trách bảo vệ an ninh mạng có trách nhiệm chia sẻ với nhau và với Cục An toàn thông tin, Bộ Thông tin và Truyền thông về dữ liệu giám sát an ninh mạng, an toàn thông tin mạng phục vụ thực hiện chức năng, nhiệm vụ được giao;

+ Trường hợp đã thực hiện giám sát an toàn thông tin mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, dữ liệu giám sát được chia sẻ, dùng chung phục vụ công tác bảo vệ an ninh mạng, an toàn thông tin mạng;

+ Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm bố trí mặt bằng, điều kiện kỹ thuật, thiết lập, kết nối hệ thống, thiết bị

giám sát của lực lượng chuyên trách bảo vệ an ninh mạng vào hệ thống thông tin do mình quản lý nhằm phát hiện, cảnh báo sớm nguy cơ an ninh mạng.

2. Về hoạt động thẩm định, đánh giá điều kiện, kiểm tra, giám sát, ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia (từ Điều 11 đến Điều 15 Luật An ninh mạng)

Luật An ninh mạng quy định:

- *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 *(khoản 1 Điều 11)*. Đối tượng thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm: (1) 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; (2) Đề án nâng cấp hệ thống thông tin trước khi phê duyệt *(khoản 2 Điều 11)*. Nội dung thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm: (1) Việc tuân thủ quy định, điều kiện an ninh mạng trong thiết kế; (2) Sự phù hợp với phương án bảo vệ, ứng phó, khắc phục sự cố và bố trí nhân lực bảo vệ an ninh mạng *(khoản 3 Điều 11)*. Thẩm quyền thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia được quy định như sau: (1) 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; (2) 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; (3) Ban Cơ yếu Chính phủ thẩm định an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ *(khoản 4 Điều 11)*.

- *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 (khoản 1 Điều 12).

- *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 (khoản 1 Điều 13).

- *Giám sát an ninh mạng* là hoạt động thu thập, phân tích tình hình nhằm xác định nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại để cảnh báo, khắc phục, xử lý (khoản 1 Điều 14).

Trên cơ sở đó, Luật quy định đầy đủ đối tượng, nội dung, quy trình, cơ quan chủ trì, cơ quan phối hợp thẩm định, thẩm quyền thẩm định, kiểm tra, đánh giá, giám sát an ninh mạng. Luật quy định:

- Hoạt động thẩm định an ninh mạng do lực lượng chuyên trách bảo vệ an ninh mạng thực hiện, áp dụng đối với hệ thống thông tin quan trọng về an ninh quốc gia. Đây là những hệ thống thông tin thuộc các bộ, ban, ngành, tập đoàn, doanh nghiệp của nhà nước, có vị trí, vai trò, tầm quan trọng đối với an ninh quốc gia, cần được bảo vệ bằng biện pháp tương xứng. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia phải bảo đảm cho hệ thống của mình đáp ứng các nội dung thẩm định để làm cơ sở cho việc quyết định xây dựng hoặc nâng cấp hệ thống thông tin. Các doanh nghiệp muốn cung cấp thiết bị, sản phẩm cho hệ thống thông tin quan trọng về an ninh quốc gia phải đáp ứng đủ các tiêu chuẩn chất lượng theo đề nghị của chủ quản hệ thống thông tin quan trọng về an ninh quốc gia, không phải đáp ứng yêu cầu từ lực lượng chuyên trách bảo vệ an ninh mạng. 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: (1) 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; (2) Đề án nâng cấp hệ thống thông tin trước khi phê duyệt (khoản 2 Điều 11).

+ Về nội dung, bao gồm: (1) Việc tuân thủ quy định, điều kiện an ninh mạng trong thiết kế; (2) Sự phù hợp với phương án bảo vệ, ứng phó, khắc phục sự cố và bố trí nhân lực bảo vệ an ninh mạng (khoản 3 Điều 11).

+ Về thẩm quyền, bao gồm: (1) 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; (2) 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; (3) Ban Cơ yếu Chính phủ thẩm định an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ (khoản 3 Điều 11).

- 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.

+ Luật quy định cụ thể các điều kiện của hệ thống thông tin quan trọng về an ninh quốc gia, bao gồm: (1) Quy định, quy trình và phương án bảo đảm an ninh mạng; nhân sự vận hành, quản trị hệ thống; (2) Bảo đảm an ninh mạng đối với trang thiết bị, phần cứng, phần mềm là thành phần hệ thống; (3) 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; (4) 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 và (khoản 2 Điều 12). 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 (khoản 3 Điều 12).

+ Luật cũng quy định cụ thể 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: (1) Khi đưa phương tiện điện tử, dịch vụ an toàn thông tin mạng vào sử dụng trong hệ thống thông tin; (2) Khi có thay đổi hiện trạng hệ thống thông tin; (3) Kiểm tra định kỳ hằng năm; (d) 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 hổng bảo mật theo khuyến cáo của lực lượng chuyên trách bảo vệ an ninh mạng (khoản 2 Điều 13). Về đối tượng bao gồm: (1) Hệ thống phần cứng, phần mềm, thiết bị số được sử dụng trong hệ thống thông tin; (2) Quy định, biện pháp bảo vệ an ninh mạng; (3) Thông tin được lưu trữ, xử lý, truyền đưa trong hệ thống thông tin; (4) Phương án ứng phó, khắc phục sự cố an ninh mạng của chủ quản hệ thống thông tin; (5) Biện pháp bảo vệ bí mật nhà nước và phòng, chống lộ, bí mật nhà nước qua các kênh kỹ thuật; (5) Nhân lực bảo vệ an ninh mạng (khoản 3 Điều 13). 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 (khoản 5 Điều 13).

- 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).

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 ninah 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 (Điều 15).

III. PHÒNG NGỪA, XỬ LÝ HÀNH VI XÂM PHẠM ANN NINH MẠNG

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 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 lỹ vững chắc để người dân có thể yên tâm buôn bán, kinh doanh hay hoạt động trên không gian mạng.

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)

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 (khoản 1 Điều 16).

- 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 (khoản 2 Điều 16).

- 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 (khoản 3 Điều 16).

- 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 (khoản 4 Điều 16).

- 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 (khoản 5 Điều 16).

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 (khoản 6 Điều 16); 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 (khoản 7 Điều 16); 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 (khoản 8 Điều 16) và trách nhiệm của tổ chức, cá nhân đối với thông tin trên không gian mạng (khoản 9 Điều 16).

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)

Điều 17 của Luật An ninh mạng quy định 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: (1) 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; (2) 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; (3) 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; (4) 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; (5) Cố ý nghe, ghi âm, ghi hình trái phép các cuộc đàm thoại; (6) 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 (khoản 1 Điều 17).

Luật quy định chủ quản hệ thống thông tin có trách nhiệm sau đây: (1) 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; (2) 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; (3) 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.

Cơ quan soạn thảo, lưu trữ thông tin, tài liệu thuộc bí mật nhà nước có trách nhiệm bảo vệ bí mật nhà nước được soạn thảo, lưu giữ trên máy tính, thiết bị khác hoặc trao đổi trên không gian mạng theo quy định của pháp luật về bảo vệ bí mật nhà nước.

Bộ Công an có trách nhiệm sau: (1) Kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia nhằm phát hiện, loại bỏ mã độc, phần cứng độc hại, khắc phục điểm yếu, lỗ hổng bảo mật; phát hiện, ngăn chặn, xử lý hoạt động xâm nhập bất hợp pháp; (2) Kiểm tra an ninh mạng đối

với thiết bị, sản phẩm, dịch vụ thông tin liên lạc, thiết bị kỹ thuật số, thiết bị điện tử trước khi đưa vào sử dụng trong hệ thống thông tin quan trọng về an ninh quốc gia; (3) Giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia nhằm phát hiện, xử lý hoạt động thu thập trái phép thông tin thuộc bí mật nhà nước; (4) Phát hiện, xử lý các hành vi đăng tải, lưu trữ, trao đổi trái phép thông tin, tài liệu có nội dung thuộc bí mật nhà nước trên không gian mạng; (5) Tham gia nghiên cứu, sản xuất sản phẩm lưu trữ, truyền đưa thông tin, tài liệu có nội dung thuộc bí mật nhà nước; sản phẩm mã hóa thông tin trên không gian mạng theo chức năng, nhiệm vụ được giao; (6) Thanh tra, kiểm tra công tác bảo vệ bí mật nhà nước trên không gian mạng của cơ quan nhà nước và bảo vệ an ninh mạng của chủ quản hệ thống thông tin quan trọng về an ninh quốc gia; (7) Tổ chức đào tạo, tập huấn nâng cao nhận thức và kiến thức về bảo vệ bí mật nhà nước trên không gian mạng, phòng, chống tấn công mạng, bảo vệ an ninh mạng đối với lực lượng bảo vệ an ninh mạng 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.

Bộ Quốc phòng có trách nhiệm thực hiện đối với hệ thống thông tin quân sự, gồm: (1) Kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia nhằm phát hiện, loại bỏ mã độc, phần cứng độc hại, khắc phục điểm yếu, lỗ hổng bảo mật; phát hiện, ngăn chặn, xử lý hoạt động xâm nhập bất hợp pháp; (2) Kiểm tra an ninh mạng đối với thiết bị, sản phẩm, dịch vụ thông tin liên lạc, thiết bị kỹ thuật số, thiết bị điện tử trước khi đưa vào sử dụng trong hệ thống thông tin quan trọng về an ninh quốc gia; (3) Giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia nhằm phát hiện, xử lý hoạt động thu thập trái phép thông tin thuộc bí mật nhà nước; (4) Phát hiện, xử lý các hành vi đăng tải, lưu trữ, trao đổi trái phép thông tin, tài liệu có nội dung thuộc bí mật nhà nước trên không gian mạng; (5) Tham gia nghiên cứu, sản xuất sản phẩm lưu trữ, truyền đưa thông tin, tài liệu có nội dung thuộc bí mật nhà nước; sản phẩm mã hóa thông tin trên không gian mạng theo chức năng, nhiệm vụ được giao; (6) Thanh tra, kiểm tra công tác bảo vệ bí mật nhà nước trên không gian mạng của cơ quan nhà nước và bảo vệ an ninh mạng của chủ quản hệ thống thông tin quan trọng về an ninh quốc gia.

Ban Cơ yếu Chính phủ có trách nhiệm tổ chức thực hiện các quy định của pháp luật trong việc sử dụng mật mã để bảo vệ thông tin thuộc bí mật nhà nước được lưu trữ, trao đổi trên không gian mạng.

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)

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: (1) Đăng tải, phát tán thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều 16 và hành vi quy định tại khoản 1 Điều 17 của Luật An ninh mạng; (2) 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; (3) 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; (4) Tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật; (5) Hướng dẫn người khác thực hiện hành vi vi phạm pháp luật; (6) 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 (khoản 1 Điều 18). Đồng thời, Luật giao trách nhiệm cho lực lượng chuyên trách bảo vệ an ninh mạng trong việc 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 giam trật tự, an toàn xã hội (khoản 2 Điều 18).

4. Phòng, chống tấn công mạng; phòng, chống khủng bố mạng (Điều 19, Điều 20 Luật An ninh 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 bao gồm: (1) 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; (2) 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; (3) 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; (4) 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; (5) 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; (6) 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 (Khoản 1 Điều 19). 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 vi phạm đối với hệ thống thông tin thuộc phạm vi quản lý (khoản 2 Điều 19). Trong trường hợp 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, Luật giao 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 (khoản 3 Điều 19). 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 (khoản 4 Điều 19).

Đối với quy định về phòng, chống khủng bố mạng, Điều 20 Luật An ninh mạng quy định cụ thể trách nhiệm của cơ quan nhà nước có thẩm quyền; chủ thể hệ thống thông tin; Bộ Công an, Bộ Quốc phòng, Ban cơ yếu Chính phủ. Trong trường hợp 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.

5. Phòng, ngừa, xử lý tình huống nguy hiểm về an ninh mạng (Điều 21 Luật An ninh mạng)

Điều 21 Luật An ninh mạng quy định cụ thể các tình huống nguy hiểm về an ninh mạng, bao gồm: (1) Xuất hiện thông tin kích động trên không gian mạng có nguy cơ xảy ra bạo loạn, phá rối an ninh, khủng bố; (2) Tấn công vào hệ thống thông tin quan trọng về an ninh quốc gia; (3) Tấn công nhiều hệ thống thông tin trên quy mô lớn, cường độ cao; (4) Tấn công mạng nhằm phá hủy công trình quan trọng về an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia; (5) 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 (khoản 1 Điều 21). Theo đó, 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 (khoản 2 Điều 21). Đồng thời, Luật quy định các biện pháp xử lý tình huống nguy hiểm về an ninh mạng (khoản 3 Điều 21) và giao trách nhiệm cho cơ quan, tổ chức, cá nhân; Thủ tướng Chính phủ; lực lượng chuyên

trách bảo vệ an ninh mạng trong việ xử lý tình huống nguy hiểm về an ninh mạng (khoản 4 Điều 21).

6. Đấu tranh bảo vệ an ninh mạng (Điều 22 Luật 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: (1) Tổ chức nắm tình hình có liên quan đến hoạt động bảo vệ an ninh quốc gia; (2) Phòng, chống tấn công và bảo vệ hoạt động ổn định của hệ thống thông tin quan trọng về an ninh quốc gia;(3) 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; (4) 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 (khoản 2 Điều 22). 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.

IV. 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.

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)

Điều 23 Luật An ninh mạng quy định nội dung triển khai hoạt động bảo vệ an ninh mạng bao gồm: (1) 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; (2) 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; (3) 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; (4) 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; (5) 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; (6) 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 (khoản 1 Điều 23). 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 (khoản 2 Điều 23).

**** Nghị định số 53/2022/NĐ-CP quy định một số hoạt động bảo vệ ann ninh mạng trong cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương, gồm:***

1.1. Xây dựng, hoàn thiện quy định sử dụng mạng máy tính của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương (Điều 23 Nghị định số 53/2022/NĐ-CP)

- Cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương phải xây dựng quy định sử dụng, quản lý và bảo đảm an ninh mạng máy tính nội bộ, mạng máy tính có kết nối mạng Internet do cơ quan, tổ chức mình quản lý. Nội dung các quy định về bảo đảm an toàn, an ninh mạng căn cứ vào những quy định về bảo vệ an ninh mạng, bảo vệ bí mật nhà nước, tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng và các tiêu chuẩn kỹ thuật chuyên ngành khác có liên quan.

- Quy định sử dụng, bảo đảm an ninh mạng máy tính của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương phải bao gồm các nội dung cơ bản sau:

+ Xác định rõ hệ thống mạng thông tin và thông tin quan trọng cần ưu tiên bảo đảm an ninh mạng;

+ Quy định rõ các điều cấm và các nguyên tắc quản lý, sử dụng và bảo đảm an ninh mạng, mạng máy tính nội bộ có lưu trữ, truyền đưa bí mật nhà nước phải được tách biệt vật lý hoàn toàn với mạng máy tính, các thiết bị,

phương tiện điện tử có kết nối mạng Internet, trường hợp khác phải bảo đảm quy định của pháp luật về bảo vệ bí mật nhà nước;

+ Quy trình quản lý, nghiệp vụ, kỹ thuật trong vận hành, sử dụng và bảo đảm an ninh mạng đối với dữ liệu, hạ tầng kỹ thuật, trong đó phải đáp ứng các yêu cầu cơ bản bảo đảm an toàn hệ thống thông tin;

+ Điều kiện về nhân sự làm công tác quản trị mạng, vận hành hệ thống, bảo đảm an ninh mạng, an toàn thông tin và liên quan đến hoạt động soạn thảo, lưu trữ, truyền đưa bí mật nhà nước qua hệ thống mạng máy tính;

+ Quy định rõ trách nhiệm của từng bộ phận, cán bộ, nhân viên trong quản lý, sử dụng, bảo đảm an ninh mạng, an toàn thông tin;

+ Chế tài xử lý những vi phạm quy định về đảm bảo an ninh mạng.

1.2. Xây dựng, hoàn thiện phương án bảo đảm an ninh mạng đối với hệ thống thông tin của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương (Điều 24 Nghị định số 53/2022/NĐ-CP)

- Người đứng đầu cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương có trách nhiệm ban hành phương án bảo đảm an ninh mạng đối với hệ thống thông tin do mình quản lý, bảo đảm đồng bộ, thống nhất, tập trung, có sự chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư trùng lặp.

- Phương án bảo đảm an ninh mạng đối với hệ thống thông tin bao gồm:

+ Quy định bảo đảm an ninh mạng trong thiết kế, xây dựng hệ thống thông tin, đáp ứng yêu cầu cơ bản như yêu cầu quản lý, kỹ thuật, nghiệp vụ;

+ Thẩm định an ninh mạng;

+ Kiểm tra, đánh giá an ninh mạng;

+ Giám sát an ninh mạng;

+ Dự phòng, ứng phó, khắc phục sự cố, tình huống nguy hiểm về an ninh mạng;

+ Quản lý rủi ro;

+ Kết thúc vận hành, khai thác, sửa chữa, thanh lý, hủy bỏ.

1.3. Xây dựng, hoàn thiện phương án bảo đảm an ninh mạng đối với hệ thống thông tin của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương (Điều 25 Nghị định số 53/2022/NĐ-CP)

- Phương án ứng phó, khắc phục sự cố an ninh mạng bao gồm:

+ Phương án phòng ngừa, xử lý thông tin 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 bị đăng tải trên hệ thống thông tin;

+ Phương án 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;

+ Phương án 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;

+ Phương án phòng, chống tấn công mạng;

+ Phương án phòng, chống khủng bố mạng;

+ Phương án phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng.

- Nội dung phương án ứng phó, khắc phục sự cố an ninh mạng

+ Các quy định chung;

+ Đánh giá các nguy cơ, sự cố an ninh mạng;

+ Phương án ứng phó, khắc phục đối với một số tình huống cụ thể;

+ Nhiệm vụ, trách nhiệm của các cơ quan trong tổ chức, điều phối, xử lý, ứng phó, khắc phục sự cố;

+ Huấn luyện, diễn tập, phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, khắc phục sự cố;

+ Các giải pháp đảm bảo, tổ chức triển khai phương án, kế hoạch và kinh phí thực hiện.

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 Luật An ninh mạng)

Theo quy định tại 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: (1) 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; (2) Khi có đề nghị của chủ quản hệ thống thông tin (khoản 1 Điều 24).

Đối tượng kiểm tra an ninh mạng được Luật quy định bao gồm: (1) Hệ thống phần cứng, phần mềm, thiết bị số được sử dụng trong hệ thống thông tin; (2) Thông tin được lưu trữ, xử lý, truyền đưa trong hệ thống thông tin; (3) Biện pháp bảo vệ bí mật nhà nước và phòng, chống lộ, mất bí mật nhà nước qua các

kênh kỹ thuật (khoản 2 Điều 24). Đồng thời, Luật giao trách nhiệm cho chủ quản hệ thống thông tin (khoản 3 Điều 24), lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an (khoản 4 Điều 24) và các quy định trước thời điểm kiểm tra và sau khi kết thúc kiểm tra (khoản 5 Điều 24). Kết quả kiểm tra an ninh mạng được bảo mật theo quy định của pháp luật (khoản 6 Điều 24). Luật giao Chính phủ quy định trình tự, thủ tục kiểm tra an ninh mạng quy định tại Điều này (khoản 7 Điều 24).

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)

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 (khoản 1 Điều 25).

Luật quy định 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 có trách nhiệm: (1) Bảo vệ an ninh mạng thuộc quyền quản lý; chịu sự quản lý, thanh tra, kiểm tra và thực hiện các yêu cầu về bảo vệ an ninh mạng của cơ quan nhà nước có thẩm quyền; (2) Tạo điều kiện, thực hiện các biện pháp kỹ thuật, nghiệp vụ cần thiết để cơ quan nhà nước có thẩm quyền thực hiện nhiệm vụ bảo vệ an ninh mạng khi có đề nghị (khoản 2 Điều 25).

4. Bảo đảm an ninh thông tin trên không gian mạng (Điều 26 Luật An ninh 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 quy định tại các khoản 1, 2, 3, 4 và 5 Điều 16 của Luật và thông tin khác có nội dung xâm phạm an ninh quốc gia (khoản 1 Điều 16), bao gồm:

+ 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 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 bao gồm: (1) 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; (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; (1) 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 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.

- 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: (1) 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; (2) Ngăn chặn việc chia sẻ thông tin, xóa bỏ thông tin có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều 16 Luật An ninh mạng 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; (3) 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 quy định tại các khoản 1, 2, 3, 4 và 5 Điều 16 của Luật 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 (khoản 2 Điều 26). 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 (khoản 3 Điều 26). Luật giao Chính phủ quy định chi tiết khoản 3 Điều này.

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.

Đối với quy định tại khoản 3 Điều 26 Luật An ninh mạng, 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: (1) Thông tin cá nhân người sử dụng dịch vụ; (2) Dữ liệu về mối quan hệ của người sử dụng dịch vụ; (3) 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.

**** Nghị định số 53/2022/NĐ-CP quy định về lưu trữ dữ liệu và đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam, cụ thể:***

4.1. Lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam (Điều 26 Nghị định số 53/2022/NĐ-CP)

- Các Dữ liệu phải lưu trữ tại Việt Nam, gồm:

+ Dữ liệu về thông tin cá nhân của người sử dụng dịch vụ tại Việt Nam;

+ Dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra: Tên tài khoản sử dụng dịch vụ, thời gian sử dụng dịch vụ, thông tin thẻ tín dụng, địa chỉ thư điện tử, địa chỉ mạng (IP) đăng nhập, đăng xuất gần nhất, số điện thoại đăng ký được gắn với tài khoản hoặc dữ liệu;

+ Dữ liệu về mối quan hệ của người sử dụng dịch vụ tại Việt Nam: bạn bè, nhóm mà người sử dụng kết nối hoặc tương tác.

Doanh nghiệp trong nước lưu trữ các dữ liệu nêu trên này tại Việt Nam.

- Việc lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam của doanh nghiệp nước ngoài:

+ Doanh nghiệp nước ngoài có hoạt động kinh doanh tại Việt Nam thuộc một trong những lĩnh vực sau: Dịch vụ viễn thông; lưu trữ, chia sẻ dữ liệu trên không gian mạng; cung cấp tên miền quốc gia hoặc quốc tế cho người sử dụng dịch vụ tại Việt Nam; thương mại điện tử; thanh toán trực tuyến; trung gian thanh toán; dịch vụ kết nối vận chuyển qua không gian mạng; mạng xã hội và truyền thông xã hội; trò chơi điện tử trên mạng; dịch vụ cung cấp, quản lý hoặc vận hành thông tin khác trên không gian mạng dưới dạng tin nhắn, cuộc gọi

thoại, cuộc gọi video, thư điện tử, trò chuyện trực tuyến phải lưu trữ dữ liệu nêu trên và đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam trong trường hợp dịch vụ do doanh nghiệp cung cấp bị sử dụng thực hiện hành vi vi phạm pháp luật về an ninh mạng đã được Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an thông báo và có yêu cầu phối hợp, ngăn chặn, điều tra, xử lý bằng văn bản nhưng không chấp hành, chấp hành không đầy đủ hoặc ngăn chặn, cản trở, vô hiệu hóa, làm mất tác dụng của biện pháp bảo vệ an ninh mạng do lực lượng chuyên trách bảo vệ an ninh mạng thực hiện;

+ Trường hợp bất khả kháng mà việc chấp hành yêu cầu của pháp luật về an ninh mạng của doanh nghiệp nước ngoài không thể thực hiện, doanh nghiệp nước ngoài thông báo cho Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an trong vòng 03 ngày làm việc để kiểm tra tính xác thực của việc bất khả kháng. Trong trường hợp này, doanh nghiệp có thời gian 30 ngày làm việc để tìm phương án khắc phục.

- Trường hợp dữ liệu do doanh nghiệp thu thập, khai thác, phân tích, xử lý không đầy đủ theo quy định, doanh nghiệp phối hợp với Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an để xác nhận và tiến hành lưu trữ các loại dữ liệu hiện đang thu thập, khai thác, phân tích, xử lý.

Trường hợp doanh nghiệp tiến hành thu thập, khai thác, phân tích, xử lý bổ sung các loại dữ liệu, doanh nghiệp có trách nhiệm phối hợp với Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an để bổ sung vào danh sách dữ liệu phải lưu trữ tại Việt Nam.

- Hình thức lưu trữ dữ liệu tại Việt Nam do doanh nghiệp quyết định.

- Trình tự, thủ tục yêu cầu lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện của doanh nghiệp nước ngoài tại Việt Nam:

+ Bộ trưởng Bộ Công an ra quyết định yêu cầu lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam;

+ Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an thông báo, hướng dẫn, theo dõi, giám sát, đôn đốc doanh nghiệp thực hiện yêu cầu lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam; đồng thời, thông báo cho các cơ quan liên quan để thực hiện chức năng quản lý nhà nước theo thẩm quyền;

+ Trong thời hạn 12 tháng kể từ ngày Bộ trưởng Bộ Công an ra quyết định, các doanh nghiệp nước ngoài có hoạt động kinh doanh tại Việt Nam phải hoàn thành lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam.

- Trình tự, thủ tục đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam được thực hiện theo các quy định của pháp luật về kinh doanh, thương mại, doanh nghiệp và các quy định khác có liên quan.

- Các doanh nghiệp không chấp hành quy định tại nêu trên thì tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định của pháp luật.

4.2. Thời gian lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam (Điều 27 Nghị định số 53/2022/NĐ-CP)

- Thời gian lưu trữ dữ liệu bắt đầu từ khi doanh nghiệp nhận được yêu cầu lưu trữ dữ liệu đến khi kết thúc yêu cầu. Thời gian lưu trữ tối thiểu là 24 tháng.

- Thời gian đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam bắt đầu từ khi doanh nghiệp nhận được yêu cầu đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam đến khi doanh nghiệp không còn hoạt động tại Việt Nam hoặc dịch vụ được quy định không còn cung cấp tại Việt Nam.

- Nhật ký hệ thống để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng được lưu trữ tối thiểu là 12 tháng.

5. Nghiên cứu, phát triển an ninh mạng (Điều 27 Luật An ninh mạng)

Điều 27 Luật An ninh mạng quy định nội dung nghiên cứu, phát triển an ninh mạng bao gồm: (1) Xây dựng hệ thống phần mềm, trang thiết bị bảo vệ an ninh mạng; (2) 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;(3) Phương pháp kiểm tra phần cứng, phần mềm được cung cấp thực hiện đúng chức năng; (4) 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; (5) Xác định nguồn gốc của thông tin được truyền đưa trên không gian mạng; (6) Giải quyết nguy cơ đe dọa an ninh mạng; (7) Xây dựng thao trường mạng, môi trường thử nghiệm an ninh mạng; (8) Sáng kiến kỹ thuật nâng cao nhận thức, kỹ năng về an ninh mạng; (9) Dự báo an ninh mạng; (10) Nghiên cứu thực tiễn, phát triển lý luận an ninh mạng (khoản 1 Điều 27). Bên cạnh đó, Luật quy định cơ quan, tổ chức, cá nhân có liên quan có quyền nghiên cứu, phát triển an ninh mạng.

6. Nâng cao năng lực tự chủ về an ninh mạng (Điều 28 Luật An ninh mạng)

Điều 28 Luật An ninh mạng quy định Nhà nước khuyến khích, tạo điều kiện để cơ quan, tổ chức, cá nhân nâng cao năng lực tự chủ về an ninh mạng và nâng cao khả năng sản xuất, kiểm tra, đánh giá, kiểm định thiết bị số, dịch vụ mạng, ứng dụng mạng. Chính phủ thực hiện các biện pháp nâng cao năng lực tự

chủ về an ninh mạng cho cơ quan, tổ chức, cá nhân, bao gồm: (1) 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; (2) Thúc đẩy ứng dụng công nghệ mới, công nghệ tiên tiến liên quan đến an ninh mạng; (3) Tổ chức đào tạo, phát triển và sử dụng nhân lực an ninh mạng; (4) 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.

7. Bảo vệ trẻ em trên không gian mạng (Điều 29 Luật An ninh mạng)

Để đáp ứng yêu cầu thực tiễn, đồng thời thể hiện chính sách bảo vệ trẻ em của Nhà nước ta, khoản 1 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.

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 có trách nhiệm kiểm soát nội dung thông tin trên hệ thống thông tin hoặc trên dịch vụ do doanh nghiệp cung cấp để không gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em; ngăn chặn việc chia sẻ và xóa bỏ thông tin có nội dung gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em; kịp thời thông báo, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an để xử lý.

Cơ quan, tổ chức, cá nhân tham gia hoạt động trên không gian mạng có trách nhiệm phối hợp với cơ quan có thẩm quyền trong bảo đảm quyền của trẻ em trên không gian mạng, ngăn chặn thông tin có nội dung gây nguy hại cho trẻ em theo quy định của Luật An ninh mạng và pháp luật về trẻ em.

Cơ quan, tổ chức, cha mẹ, giáo viên, người chăm sóc trẻ em và cá nhân khác liên quan có trách nhiệm bảo đảm quyền của trẻ em, bảo vệ trẻ em khi tham gia không gian mạng theo quy định của pháp luật về trẻ em.

Lực lượng chuyên trách bảo vệ an ninh mạng và các cơ quan chức năng có trách nhiệm áp dụng biện pháp để phòng ngừa, phát hiện, ngăn chặn, xử lý nghiêm hành vi sử dụng không gian mạng gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em.

V. ĐẢM BẢO 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, Điều 30 Luật An ninh mạng quy định: (1) Lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Bộ Công an, Bộ Quốc phòng; (2) 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. (3) Tổ chức, cá nhân được huy động tham gia bảo vệ an ninh mạng.

Về bảo đảm nguồn nhân lực bảo vệ an ninh mạng, Điều 31 Luật An ninh mạng quy định: (1) 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; (2) Nhà nước có chương trình, kế hoạch xây dựng, phát triển nguồn nhân lực bảo vệ an ninh mạng; (3) 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.

Theo đó, Luật quy định cụ thể về việc tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng (Điều 32); giáo dục, bồi dưỡng kiến thức, nghiệp vụ an ninh mạng (Điều 33); phổ biến kiến thức về an ninh mạng (Điều 34) và kinh phí bảo vệ an ninh mạng (Điều 35).

VI. 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 của Luật, 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.

1. Trách nhiệm của Bộ Công an (Điều 36 Luật An ninh mạng)

Trách nhiệm của Bộ Công an được quy định cụ thể tại Điều 36 và Điều 16. 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: (1) 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;

(2) Xây dựng, đề xuất chiến lược, chủ trương, chính sách, kế hoạch và phương án bảo vệ an ninh mạng; (3) 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; (4) 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; (5) 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; (6) 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; (7) Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về an ninh mạng.

2. Trách nhiệm của Bộ Quốc phòng (Điều 37 Luật An ninh mạng)

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: (1) 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; (2) 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; (3) Phòng ngừa, đấu tranh với các hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia trong phạm vi quản lý; (4) 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; (5). 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.

3. Trách nhiệm của Bộ Thông tin và Truyền thông (Điều 38 Luật An ninh mạng)

Điều 38 Luật An ninh mạng quy định Bộ Thông tin và Truyền thông có trách nhiệm: (1) Phối hợp với Bộ Công an, Bộ Quốc phòng trong bảo vệ an ninh mạng; (2) 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 quy định tại khoản 1 Điều 16 của Luật này; (3) 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.

4. Trách nhiệm của Ban Cơ yếu Chính phủ (Điều 39 Luật An ninh mạng)

Điều 39 Luật An ninh mạng quy định Ban Cơ yếu Chính phủ có trách nhiệm: (1) 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; (2) 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; (3) 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.

5. Trách nhiệm của Bộ, ngành, Ủy ban nhân dân cấp tỉnh (Điều 40 Luật An ninh mạng)

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. Trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng (Điều 41 Luật An ninh 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: (1) 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; (2) 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; (3) 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; (4) Phối hợp, tạo điều kiện cho lực lượng chuyên trách bảo vệ an ninh mạng trong bảo vệ an ninh mạng (khoản 1 Điều 41). 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 (khoản 2 Điều 41).

7. Trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng (Điều 42 Luật An ninh 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: (1) Tuân thủ quy định của pháp luật về an ninh mạng; (2) 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; (3) 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./.