TTĐT

CHÍNH PHỦ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1173/BC-CP	*Hà Nội, ngày 07 tháng 12 năm 2025*

BÁO CÁO
Về việc giải trình, tiếp thu, chỉnh lý và hoàn thiện dự thảo Luật An ninh mạng

Kính gửi: Quốc hội

Trên cơ sở Tờ trình số 815/TTr-CP ngày 22/9/2025 của Chính phủ về dự án Luật An ninh mạng, ngày 17/10/2025, Ủy ban Quốc phòng, An ninh và Đối ngoại đã ban hành Báo cáo thẩm tra số 1124/BC-UBQPANĐN15 đối với dự án Luật An ninh mạng.

Ngày 07/11/2025, Tổng thư ký Quốc hội ban hành Báo cáo số 4205/BC-VPQH tổng hợp ý kiến các vị đại biểu Quốc hội thảo luận tại Tổ về dự án Luật An ninh mạng; tiếp đó, ngày 13/11/2025, Tổng thư ký Quốc hội ban hành Báo cáo số 4344/BC-VPQH tổng hợp ý kiến các vị đại biểu Quốc hội thảo luận tại Hội trường về dự án Luật An ninh mạng. Theo đó, đã có **90** lượt ý kiến tham gia gồm **70** lượt ý kiến phát biểu tại Tổ, **15** lượt ý kiến phát biểu tại Hội trường và **05** ý kiến góp ý bằng văn bản.

Ngày 23/11/2025, Chính phủ đã có Báo cáo số 1079/BC-CP về việc tiếp thu, giải trình ý kiến của Đại biểu Quốc hội, chỉnh lý dự thảo Luật An ninh mạng. Ngày 24/11/2025, Ủy ban Thường vụ Quốc hội đã họp cho ý kiến về dự án Luật; tiếp đó, ngày 27/11/2025, Văn phòng Quốc hội ban hành Thông báo số 4658/TB-VPQH thông báo kết luận của Ủy ban Thường vụ Quốc hội về dự thảo Luật An ninh mạng.

Chính phủ đã chỉ đạo Bộ Công an chủ trì, phối hợp với Ủy ban Quốc phòng, An ninh và Đối ngoại, Ủy ban Pháp luật và Tư pháp và các bộ, ngành liên quan tiếp thu, giải trình đầy đủ ý kiến của đại biểu Quốc hội và ý kiến kết luận của Ủy ban Thường vụ Quốc hội. Đồng thời, Chính phủ chỉ đạo Bộ Tư pháp chủ trì, phối hợp với Bộ Công an và các bộ, ngành liên quan rà soát tính hợp hiến, hợp pháp, tính thống nhất của dự thảo Luật với hệ thống pháp luật hiện hành, cũng như ngôn ngữ, thể thức, kỹ thuật trình bày văn bản theo quy định của Luật Ban hành văn bản quy phạm pháp luật năm 2025.

Trên cơ sở đó, Chính phủ đã tiếp thu, giải trình, chỉnh lý và hoàn thiện dự thảo Luật An ninh mạng với **08** chương, **45** điều cụ thể như sau:

I. ĐỐI VỚI Ý KIẾN THAM GIA CỦA ĐẠI BIỂU QUỐC HỘI

1. Về sự phù hợp với chủ trương, đường lối của Đảng; tính hợp hiến, tính thống nhất với hệ thống pháp luật; tính tương thích với điều ước quốc tế có liên quan mà Việt Nam là thành viên; tính khả thi của dự thảo Luật

- Hầu hết ý kiến nhất trí sự cần thiết ban hành Luật An ninh mạng (89 ý kiến).

Tuy nhiên, có ý kiến băn khoăn việc hợp nhất Luật An ninh mạng 2018 và An toàn thông tin mạng năm 2015 đi ngược xu thế chuyên sâu (01 ý kiến).

Về ý kiến nêu trên, Chính phủ báo cáo như sau: Việc hợp nhất Luật An toàn thông tin mạng năm 2015, Luật An ninh mạng năm 2018 và lấy tên là Luật An ninh mạng là phù hợp với thực tiễn do Luật An ninh mạng có phạm vi điều chỉnh rộng hơn, không dừng lại ở bảo vệ thông tin mà còn bao quát các vấn đề liện quan đến bảo vệ an ninh quốc gia và trật tự, an toàn xã hội trên không gian mạng, trong khi Luật An toàn thông tin mạng chủ yếu điều chỉnh các nội dung mang tính kỹ thuật và bảo vệ thông tin mạng, hệ thống thông tin. Bên cạnh đó, an ninh mạng là lĩnh vực mang tính chiến lược, gắn với chủ quyền và an ninh quốc gia, nên việc thống nhất tên gọi theo hướng này thể hiện mức độ ưu tiên về chính sách pháp luật của Nhà nước trong giai đoạn hiện tại. Ngoài ra, trong bối cảnh các mối đe dọa trên không gian mạng ngày càng phức tạp, xu hướng chung của nhiều quốc gia cũng đang tập trung xây dựng pháp luật theo hướng toàn diện về an ninh mạng.

- Một số ý kiến đề nghị rà soát dự thảo Luật này trong mối quan hệ với các dự thảo Luật có liên quan sẽ được Quốc hội xem xét thông qua tại Kỳ họp thứ 10 như Luật Bảo vệ bí mật nhà nước (sửa đổi), Luật Chuyển đổi số, Luật Trí tuệ nhân tạo, Luật Công nghệ cao... để bảo đảm đồng bộ, thống nhất; cụ thể hóa Nghị quyết số 57 của Bộ Chính trị về đột phá khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia và các quan điểm chỉ đạo khác liên quan của Đảng (08 ý kiến).

Tiếp thu các ý kiến của Đại biểu Quốc hội, Chính phủ đã rà soát và quy định tại các điều khoản cụ thể trong dự thảo Luật.

- Một số ý kiến đề nghị rà soát để nội luật hóa Công ước của Liên hợp quốc về chống tội phạm mạng (Công ước Hà Nội) (03 ý kiến); đề nghị nội luật hóa một số nội dung cụ thể như sau: (1) Bổ sung Chương mới về các hành vi tội phạm mạng và hình sự hóa hành vi vi phạm an ninh mạng; (2) Bổ sung cơ chế điều tra xuyên biên giới, ủy thác tư pháp điện tử hoặc dẫn độ điện tử; hợp tác quốc tế; cho phép truy xuất, tịch thu tài sản do phạm tội; (3) Bổ sung quy định cơ quan đầu mối quốc gia chịu trách nhiệm điều phối mạng lưới 24/7, thiết lập trung tâm điều phối hợp tác quốc tế về tội phạm mạng; bổ sung điều khoản công nhận chứng cứ điện tử và dữ liệu số do nước ngoài cung cấp phù hợp với chuẩn mực quốc tế; (4) Tích hợp các chương trình nâng cao năng lực chuyển đổi số, chuyển giao công nghệ, đào tạo kỹ thuật số, pháp y điện tử; (5) Bổ sung quy định Chính phủ định kỳ hai năm một lần, báo cáo Quốc hội về tình hình an ninh mạng quốc gia (01 ý kiến)

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát để nội luật hoá các nội dung Công ước Hà Nội cho phù hợp với phạm vi điều chỉnh của dự thảo Luật.

2. Về ngôn ngữ, kỹ thuật soạn thảo

- Có ý kiến đề nghị đổi tên Luật thành "Luật An ninh, An toàn mạng" để tích hợp triệt để Luật An toàn thông tin mạng và Luật An ninh mạng, vì tên Luật do Chính phủ trình chỉ tập trung vào an ninh, bỏ sót nội dung an toàn thông tin (phân cấp độ, bảo vệ dữ liệu...) (02 ý kiến).

Về ý kiến nêu trên, Chính phủ báo cáo như sau: Việc sử dụng tên gọi "Luật An ninh mạng" giúp tạo sự thống nhất, dễ hiểu và thuận tiện cho người dân, doanh nghiệp khi tiếp cận và thực thi pháp luật. An ninh mạng là lĩnh vực mang tính chiến lược, gắn với chủ quyền và an ninh quốc gia, nên việc đặt tên theo hướng này thể hiện sự ưu tiên cao trong chính sách pháp luật của Nhà nước trong giai đoạn hiện tại. Ngoài ra, trong bối cảnh các mối đe dọa trên không gian mạng ngày càng phức tạp, nhiều quốc gia cũng đang tập trung xây dựng pháp luật theo hướng toàn diện về an ninh mạng.

- Có ý kiến đề nghị gộp Chương II (Bảo vệ an ninh mạng đối với hệ thống thông tin và hệ thống thông tin quan trọng về an ninh quốc gia) và Chương IV (Hoạt động về bảo vệ an ninh mạng) thành 01 chương để thống nhất quy định về an ninh dữ liệu, an ninh thông tin trên không gian mạng, bảo vệ an ninh mạng đối với hệ thống thông tin và cơ sở hạ tầng thiết yếu; gộp Chương V (Tiêu chuẩn, quy chuẩn kỹ thuật về an ninh mạng) và Chương VI (Kinh doanh sản phẩm, dịch vụ an ninh mạng) thành 01 chương quy định về "Tiêu chuẩn, quy chuẩn kỹ thuật, sản phẩm, dịch vụ an ninh mạng" (02 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát chỉnh lý và biên tập thành: Chương II (mới) Bảo vệ an ninh mạng đối với hệ thống thông tin; Chương V (mới) Tiêu chuẩn, quy chuẩn kỹ thuật, sản phẩm dịch vụ an ninh mạng trong dự thảo Luật.

3. Một số nội dung cụ thể của dự thảo Luật

3.1. Về những quy định chung (Chương I)

- Điều 1 (Phạm vi điều chỉnh)

Có ý kiến đề nghị bổ sung nội dung: "bảo vệ không gian mạng quốc gia, phòng ngừa, ứng phó, khắc phục sự cố an ninh mạng quan trọng về an ninh quốc gia" (02 ý kiến); bỏ nội dung: "bảo đảm an ninh thông tin, an ninh dữ liệu, an toàn hệ thống thông tin" vì đã bao hàm trong bảo vệ an ninh quốc gia, trật tự, an toàn xã hội, quyền lợi hợp pháp (01 ý kiến); làm rõ "an ninh dữ liệu" tránh chồng chéo với Luật Bảo vệ dữ liệu cá nhân (01 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát, chỉnh lý điều khoản này thành khoản 1 Điều 1 (mới) về phạm vi điều chỉnh và đối tượng áp dụng, như sau:

"1. Luật này quy định về an ninh mạng, bảo vệ an ninh mạng; quyền, nghĩa vụ, trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan".

- Điều 2 (Đối tượng áp dụng)

Có ý kiến đề nghị bỏ Điều này vì Luật Ban hành văn bản quy phạm pháp luật đã quy định rõ hiệu lực về không gian, thời gian, đối tượng (mọi cơ quan, tổ chức, cá nhân trên lãnh thổ Việt Nam); bỏ cụm từ "có liên quan" (01 ý kiến); rà soát kỹ đối tượng áp dụng để tránh trùng lặp, bỏ sót; hiện quy định chỉ giới hạn "tại Việt Nam" và "trực tiếp tham gia hoặc có liên quan" nhưng Chương V (Điều 36 - 40) có quy định nhập khẩu, kinh doanh sản phẩm, dịch vụ an ninh mạng cần mở rộng, làm rõ bao quát đầy đủ các chủ thể tham gia kinh doanh, cung cấp dịch vụ (01 ý kiến); mở rộng đối tượng áp dụng đối với cơ quan, tổ chức, cá nhân Việt

Nam ở nước ngoài (02 ý kiến), các nền tảng số xuyên biên giới cung cấp dịch vụ tại Việt Nam (01 ý kiến), cá nhân nước ngoài (01 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát, chỉnh lý điều khoản này thành khoản 2 Điều 1 (mới) về phạm vi điều chỉnh và đối tượng áp dụng), như sau:

"2. Luật này áp dụng đối với:

a) Cơ quan, tổ chức, cá nhân Việt Nam;

b) Cơ quan, tổ chức, cá nhân nước ngoài tại Việt Nam và người gốc Việt Nam chưa xác định được quốc tịch đang sinh sống tại Việt Nam đã được cấp giấy chứng nhận căn cước;

c) Cơ quan, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động bảo vệ an ninh mạng, kinh doanh sản phẩm, dịch vụ an ninh mạng tại Việt Nam".

- Điều 3 (Giải thích từ ngữ)

+ Có ý kiến đề nghị chuẩn hóa hệ thống khái niệm theo 3 hướng cơ bản để thuận tiện cho việc áp dụng thực tiễn: (1) An ninh mạng là khái niệm bao trùm; (2) An ninh thông tin mạng và an ninh dữ liệu; (3) Các khái niệm khác (01 ý kiến); làm rõ nội hàm, ranh giới an toàn thông tin (kỹ thuật, công nghệ); an ninh mạng (chính trị, pháp lý, chủ quyền) (01 ý kiến); quy định thống nhất hệ thống khái niệm, tránh mâu thuẫn, chồng chéo với các luật liên quan (ví dụ: phần mềm độc hại, mã độc, chương trình độc hại, chương trình tin học gây hại) (02 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát để chỉnh lý, hoàn thiện các thuật ngữ, khái niệm trong dự thảo Luật. Riêng các thuật ngữ phần mềm độc hại, mã độc, chương trình độc hại, chương trình tin học gây hại đang được sử dụng đúng với bản chất công nghệ trong từng trường hợp cụ thể.

+ Có ý kiến đề nghị bổ sung giải thích từ ngữ đối với các cụm từ: "An ninh thông tin", "an toàn hệ thống thông tin", "thông tin riêng", "phương tiện điện tử", "hệ thống lưu trữ dữ liệu chuyên ngành", "hệ thống trí tuệ nhân tạo tác động lớn", "hệ thống trí tuệ nhân tạo rủi ro cao", "tội phạm công nghệ cao", "xuyên tạc", "phủ nhận", "tuyên truyền" (02 ý kiến); "chiến tranh không gian mạng" (01 ý kiến); "dịch vụ mật mã dân sự" (01 ý kiến).

Về ý kiến nêu trên, Chính phủ báo cáo như sau: Các thuật ngữ trên đã và sẽ được định nghĩa hoặc chuẩn hóa trong luật chuyên ngành hiện hành hoặc các văn bản dưới luật. Việc bổ sung các khái niệm này trong dự thảo Luật sẽ dẫn đến trùng lặp. Vì vậy, dự thảo Luật chỉ quy định theo hướng dẫn chiếu đến khái niệm đã được xác định trong luật chuyên ngành và giao Chính phủ quy định chi tiết việc áp dụng để bảo đảm đồng bộ và rõ ràng trong hệ thống pháp luật.

*+ **Khoản 1**: Có ý kiến đề nghị bổ sung cụm từ "hệ thống thông tin và dữ liệu" vì các đối tượng này cần được bảo đảm tương tự như không gian mạng và chỉnh sửa như sau: "An ninh mạng là sự bảo đảm hoạt động trên không gian mạng, hệ thống thông tin và dữ liệu..." (01 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát, chỉnh lý nội dung này thành khoản 1 Điều 2 về giải thích từ ngữ, như sau:

"1. An ninh mạng là sự ổn định, an ninh, an toàn của không gian mạng; bảo vệ hệ thống thông tin và bảo đảm thông tin, dữ liệu, 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".

+ ***Khoản 2:*** *Có ý kiến đề nghị bổ sung cụm từ "truy cập" để bổ sung tình huống cần bảo đảm thông tin và viết lại theo hướng: "An ninh thông tin mạng là bảo đảm thông tin trên không gian mạng không bị truy cập, sử dụng..." (01 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát, chỉnh lý nội dung này thành khoản 2 Điều 2 về giải thích từ ngữ, như sau:

"2. An ninh thông tin mạng là sự bảo đảm tính nguyên vẹn, tính bảo mật, tính khả dụng của thông tin trên không gian mạng, tránh bị truy cập, sử dụng, tiết lộ, sửa đổi trái phép, phá hoại hoặc hành vi khác đe dọa hoặc gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội".

+ ***Khoản 3:*** *Có ý kiến đề nghị sửa như sau: "An ninh dữ liệu là việc bảo vệ dữ liệu thông qua biện pháp quản lý kỹ thuật và pháp lý nhằm phòng ngừa, ngăn chặn truy cập, thu thập, sử dụng, tiết lộ, sửa đổi, phá hủy dữ liệu trái phép; phục vụ chuyển đổi số, kinh tế số gắn với quốc phòng, an ninh, đối ngoại." (01 ý kiến); đề nghị bổ sung các cụm từ "lưu trữ", "chính phủ số", "xã hội số" để bảo đảm đầy đủ 3 trụ cột của chuyển đổi số (01 ý kiến). Có ý kiến cho rằng khoản này chỉ mới tập trung mục tiêu phục vụ chuyển đổi số quốc gia và phát triển kinh tế số, chưa thể hiện rõ bản chất cốt lõi của an ninh dữ liệu là bảo vệ tính bí mật, toàn vẹn của dữ liệu và phòng chống truy cập trái phép hoặc sự cố (01 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát, chỉnh lý nội dung này thành khoản 3 Điều 2 về giải thích từ ngữ, như sau:

"3. An ninh dữ liệu là sự bảo đảm chất lượng dữ liệu và các hoạt động xử lý, sử dụng dữ liệu trên không gian mạng phục vụ phát triển kinh tế - xã hội, chuyển đổi số quốc gia, tránh bị truy cập, sử dụng, tiết lộ, sửa đổi trái phép, phá hoại hoặc hành vi khác đe dọa hoặc gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội".

+ ***Khoản 5:*** *Có ý kiến đề nghị thay từ "đưa" bằng từ "dẫn" để bảo đảm đúng tính chất của truyền thông tin (01 ý kiến).*

Chính phủ đã rà soát và loại bỏ thuật ngữ "mạng" để đồng nhất với thuật ngữ "không gian mạng" trong toàn bộ dự thảo Luật.

+ ***Khoản 9:*** *Có ý kiến đề nghị thay từ "xâm phạm" bằng cụm từ "gây tổn hại nghiêm trọng đến an ninh mạng" để làm rõ quan hệ nhân quả (hành vi - hậu quả) (01 ý kiến); đề nghị bổ sung cụm từ "và an ninh quốc gia" để bảo đảm thống nhất, đầy đủ nội dung (01 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát, chỉnh lý và chuyển nội dung này thành khoản 1 Điều 9 về hệ thống thông tin quan trọng về an ninh quốc gia, như sau:

"1. Hệ thống thông tin quan trọng về an ninh quốc gia là hệ thống thông tin có vai trò chiến lược, đặc biệt quan trọng đối với quốc phòng, an ninh, ngoại giao, kinh tế, xã hội khi bị sự cố hoặc có hành vi vi phạm pháp luật về an ninh mạng có

thể gây tổn hại nghiêm trọng đến an ninh quốc gia, trật tự, an toàn xã hội, thuộc danh mục do Thủ tướng Chính phủ ban hành".

+ ***Khoản 11:*** *Có ý kiến đề nghị bổ sung các từ "xâm nhập", "kiểm soát" và cụm từ "khai thác tài nguyên hoặc thực hiện hành vi trái phép khác" để bảo đảm đầy đủ các mục đích của phần mềm độc hại (01 ý kiến).*

Về ý kiến nêu trên, Chính phủ báo cáo nhận thấy rằng việc bổ sung các thuật ngữ "xâm nhập", "kiểm soát", "khai thác tài nguyên hoặc thực hiện hành vi trái phép khác" vào khoản 11 sẽ làm thu hẹp phạm vi áp dụng, không theo kịp với sự phát triển của khoa học, kỹ thuật và chồng lấn với quy định, thuật ngữ tại luật chuyên ngành và Bộ luật Hình sự.

+ ***Khoản 14:*** *Có ý kiến đề nghị bỏ hoặc chỉnh sửa khái niệm này để tránh nhầm lẫn với các tội danh đã quy định rõ trong Bộ luật Hình sự; không nên định nghĩa như một tội danh mới gây khó khăn cho thực hiện (02 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát, chỉnh lý nội dung này thành khoản 12 Điều 2 về giải thích từ ngữ, như sau:

"12. Tội phạm mạng là hành vi nguy hiểm cho xã hội, được quy định trong Bộ luật Hình sự, do cá nhân hoặc tổ chức thực hiện trên không gian mạng bằng việc sử dụng công nghệ thông tin hoặc phương tiện điện tử".

+ ***Khoản 15:*** *Có ý kiến đề nghị bổ sung các hành vi như: trộm, sao chép trái phép thông tin mạng (01 ý kiến); đề nghị bổ sung từ "xâm nhập", các cụm từ "chiếm quyền điều khiển", "hoặc làm sai lệch" để bảo đảm bao quát các hình thức tấn công mạng hiện nay (01 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát, chỉnh lý nội dung này thành khoản 13 Điều 2 về giải thích từ ngữ, như sau:

"13. Tấn công mạng là hành vi thực hiện trên không gian mạng bằng việc sử dụng công nghệ thông tin hoặc phương tiện điện tử để chiếm đoạt thông tin, gây rối loạn, gián đoạn, tê liệt hoạt động, phá hoại hoặc kiểm soát hệ thống 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 16****: Có ý kiến đề nghị cân nhắc định nghĩa: "Sử dụng không gian mạng để thực hiện hành vi khủng bố hoặc tài trợ khủng bố" vì gộp hai tội riêng biệt trong Bộ luật Hình sự (khủng bố và tài trợ khủng bố), cần phân tách để phù hợp cấu thành tội danh (01 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát, chỉnh lý nội dung này thành khoản 14 Điều 2 về giải thích từ ngữ, như sau:

"14. Khủng bố mạng là hành vi thực hiện trên không gian mạng bằng việc sử dụng công nghệ thông tin hoặc phương tiện điện tử nhằm gây hoảng sợ trong công chúng hoặc làm mất ổn định chính trị".

+ ***Khoản 17:*** *Có ý kiến cho rằng khái niệm này còn thiếu nội dung "bí mật đời tư, bí mật cá nhân" đề nghị rà soát, thống nhất với Luật hiện hành (01 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát, chỉnh lý nội dung này thành khoản 15 Điều 2 về giải thích từ ngữ, như sau:

"15. Gián điệp mạng là hành vi thực hiện trên không gian mạng bằng việc sử dụng công nghệ thông tin, phương tiện điện tử bí mật xâm nhập để chiếm đoạt, thu thập, sao chép thông tin thuộc phạm vi bí mật nhà nước, dữ liệu quan trọng của cơ quan, tổ chức, cá nhân nhằm mục đích gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội".

+ ***Khoản 21:*** *Có ý kiến đề nghị thay từ "hành vi" bằng từ "mức độ" để làm rõ tính chất, vượt trên sự cố thông thường (01 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát, chỉnh lý nội dung này thành khoản 18 Điều 2 về giải thích từ ngữ, như sau:

"18. Tình huống nguy hiểm về an ninh mạng là trạng thái hoặc diễn biến trên không gian mạng khi có yếu tố tấn công, xâm nhập, kích động, làm lộ, mất thông tin hoặc hành vi khác đe dọa xâm phạm nghiêm trọng đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân".

- Điều 4 (Chính sách của Nhà nước về an ninh mạng)

+ Có ý kiến đề nghị rà soát, bổ sung chính sách khuyến khích doanh nghiệp công nghệ trong nước phát triển sản phẩm, dịch vụ an ninh mạng; khuyến khích sử dụng sản phẩm, dịch vụ an ninh mạng Việt Nam (02 ý kiến); bổ sung cơ chế cụ thể huy động, sử dụng nguồn lực tài chính cho chương trình đào tạo, nghiên cứu, phát triển sản phẩm an ninh mạng (01 ý kiến); đề nghị bổ sung chính sách mang tính nguyên tắc nền tảng của an ninh mạng là phục vụ phát triển kinh tế số, bảo vệ quyền dữ liệu của công dân số (01 ý kiến).

+ ***Khoản 2:*** *Có ý kiến đề nghị chuyển nội dung về nguyên tắc bảo vệ an ninh mạng sang Điều 5 để phù hợp hơn (01 ý kiến); đề nghị đổi vị trí khoản 1 và khoản 2 để bảo đảm tính logic (01 ý kiến).*

+ ***Khoản 3:*** *Có ý kiến đề nghị rà soát, dẫn chiếu Luật Khoa học, công nghệ và đổi mới sáng tạo (đã có chính sách đột phá); nếu ưu đãi cao hơn thì quy định rõ, tránh trùng lặp (01 ý kiến); đề nghị bổ sung "và có cơ chế đặc thù" tại đầu khoản (01 ý kiến).*

+ ***Khoản 5:*** *Có ý kiến đề nghị làm rõ khái niệm "công nghiệp an ninh mạng" (02 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát, chỉnh lý điều khoản này thành Điều 3 về chính sách của Nhà nước về an ninh mạng, như sau:

"Điều 3. Chính sách của Nhà nước về an ninh mạng

1. 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.

2. Ưu tiên bảo vệ an ninh mạng trong các lĩnh vực quốc phòng, an ninh, cơ yếu, phát triển kinh tế - xã hội, khoa học, công nghệ và đối ngoại.

3. Ưu tiên bố trí nguồn lực xây dựng, phát triển lực lượng chuyên trách bảo vệ an ninh mạng, bảo đảm nguồn nhân lực chất lượng cao phục vụ 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 hoạt động nghiên cứu, phát triển khoa học, công nghệ hiện đại phục vụ bảo vệ an ninh mạng; có cơ chế đặc thù,

chính sách ưu đãi để huy động, thu hút, đào tạo và sử dụng nhân tài trong lĩnh vực an ninh mạng.

4. Đẩy mạnh liên kết, hợp tác công - tư trong bảo vệ an ninh mạng; khuyến khích, tạo điều kiện để cơ quan, 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; sử dụng sản phẩm, dịch vụ an ninh mạng của Việt Nam.

5. Mở rộng hợp tác quốc tế về an ninh mạng để tăng cường khả năng bảo vệ an ninh mạng; phòng, chống tội phạm mạng và các mối đe dọa về an ninh mạng xuyên quốc gia; tiếp thu công nghệ hiện đại nhằm nâng cao năng lực tự chủ an ninh mạng quốc gia".

- Điều 5 (Nguyên tắc bảo vệ an ninh mạng)

+ Có ý kiến đề nghị bổ sung nguyên tắc: "bảo đảm quyền tiếp cận thông tin và quyền riêng tư hợp pháp của công dân", "bảo vệ quyền con người, quyền công dân trên không gian mạng" để tạo sự cân bằng giữa yêu cầu quản lý nhà nước và quyền con người trên không gian mạng, bảo đảm hài hòa giữa bảo vệ an ninh quốc gia và bảo vệ quyền, lợi ích hợp pháp của công dân (02 ý kiến); bổ sung nguyên tắc "phòng ngừa chủ động với hạ tầng trọng yếu về hệ thống thông tin quan trọng" (01 ý kiến); bảo đảm phù hợp với pháp luật chuyên ngành và điều ước quốc tế mà Việt Nam là thành viên; kết hợp chặt chẽ giữa bảo vệ an ninh mạng với phát triển kinh tế - xã hội, đổi mới sáng tạo; chủ động phòng ngừa, phát hiện, ngăn chặn, ứng phó, khắc phục sự cố và xử lý nghiêm vi phạm pháp luật về an ninh mạng (01 ý kiến); khuyến khích, giải phóng sáng tạo, thử nghiệm công nghệ mới có kiểm soát và bảo đảm an ninh mạng (01 ý kiến); áp dụng theo 4 tiêu chí bảo vệ an ninh mạng là "cần thiết, tương xứng, có thời hạn và có kiểm soát" (01 ý kiến).

+ ***Khoản 3:*** *Có ý kiến đề nghị quy định rõ thẩm quyền kiểm tra, giám sát, xử lý để bảo đảm tính pháp lý khi phát sinh các vấn đề đối với các hệ thống thông tin, nền tảng có máy chủ ở nước ngoài nhưng tác động trực tiếp đến người dùng ở Việt Nam (01 ý kiến); đề nghị rà soát loại bỏ một số nội dung không phải nguyên tắc trong điều này (01 ý kiến).*

+ ***Khoản 6:*** *Có ý kiến đề nghị bổ sung cụm từ "và theo đúng quy định của pháp luật" để bảo đảm đầy đủ và viết lại như sau: "Mọi hành vi vi phạm pháp luật về an ninh mạng phải được xử lý kịp thời, nghiêm minh và theo đúng quy định của pháp luật" (01 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát, chỉnh lý điều khoản này thành Điều 4 về nguyên tắc bảo vệ an ninh mạng, như sau:

"Điều 4. Nguyên tắc bảo vệ an ninh mạng

1. Tuân thủ Hiến pháp và pháp luật; bảo đảm an ninh, chủ quyền và lợi ích quốc gia trên không gian mạng.

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 bảo vệ an ninh mạng với phát triển kinh tế - xã hội, bảo đảm quyền con người, quyền công dân, bảo vệ dữ liệu cá nhân tạo điều kiện cho cơ quan, tổ chức, cá nhân hoạt động hợp pháp trên không gian mạng.

4. Áp dụng các biện pháp để bảo vệ không gian mạng quốc gia; chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh làm thất bại mọi hoạt động 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; xử lý kịp thời, nghiêm minh các hành vi vi phạm pháp luật về an ninh mạng.

5. Triển khai hoạt động bảo vệ an ninh mạng thường xuyên, liên tục đối với cơ sở hạ tầng không gian mạng quốc gia; chủ động áp dụng các biện pháp bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia".

Đối với ý kiến về việc áp dụng theo 4 tiêu chí bảo vệ an ninh mạng là "cần thiết, tương xứng, có thời hạn và có kiểm soát, Chính phủ sẽ nghiên cứu tiếp thu và chi tiết hóa nội dung này trong văn bản quy định chi tiết, hướng dẫn thi hành Luật này.

- Điều 6 (Biện pháp bảo vệ an ninh mạng)

+ Có ý kiến đề nghị bỏ từ "Biện pháp" trong tiêu đề và sửa thành "Bảo vệ an ninh mạng" để thống nhất với Điều 7"Bảo vệ không gian mạng quốc gia" và Chương II "Bảo vệ an ninh mạng đối với hệ thống thông tin" (01 ý kiến); làm rõ cơ quan nào có thẩm quyền ra quyết định ngừng cung cấp thông tin, tạm đình chỉ hoạt động mạng, trình tự, thủ tục thực hiện và cơ chế kiểm tra, giám sát để tránh lạm quyền, bảo đảm minh bạch và bảo đảm quyền công dân (01 ý kiến); bổ sung khoản 3 quy định nguyên tắc tôn trọng quyền con người, quyền công dân về đời sống riêng tư, bí mật cá nhân, gia đình theo Hiến pháp và pháp luật (01 ý kiến); khái quát các biện pháp thành 3 nhóm: biện pháp kỹ thuật (các điểm a,b,c...), biện pháp pháp luật (điểm m,n...), biện pháp hành chính (các điểm e,i,k...) (01 ý kiến); giao Chính phủ quy định chi tiết bằng Nghị định để linh hoạt, đúng Nghị quyết số 66-NQ/TW của Bộ Chính trị về đổi mới công tác xây dựng và thi hành pháp luật đáp ứng yêu cầu phát triển đất nước trong kỷ nguyên mới và Luật Ban hành văn bản quy phạm pháp luật (01 ý kiến); bổ sung quy định Chính phủ cập nhật định kỳ (theo quý) danh mục rủi ro về an ninh mạng và tiêu chuẩn bảo vệ để phù hợp với sự phát triển nhanh chóng của khoa học công nghệ (01 ý kiến).

Về ý kiến đề nghị bỏ từ "Biện pháp" trong tiêu đề Điều này để thống nhất với Điều 7 và Chương II, Chính phủ thấy rằng: Điều 7 quy định mang tính nguyên tắc, còn Điều 6 là các biện pháp cụ thể để áp dụng; đổi tên dễ làm mờ ranh giới giữa nguyên tắc và chính sách, công cụ và biện pháp.

Đối với các ý kiến còn lại, Chính phủ sẽ nghiên cứu tiếp thu trên cơ sở kế thừa quy định của Luật An ninh mạng năm 2018, tuy nhiên, có rà soát để chỉnh lý cho phù hợp với tinh thần Nghị quyết số 66-NQ/TW của Bộ Chính trị về đổi mới công tác xây dựng và thi hành pháp luật đáp ứng yêu cầu phát triển đất nước trong kỷ nguyên mới (sau đây gọi tắt là Nghị quyết số 66) và Luật Ban hành văn bản quy phạm pháp luật.

*+ **Khoản 1:** Có ý kiến đề nghị bổ sung biện pháp "tăng cường hợp tác quốc tế về an ninh mạng" để nâng cao hiệu quả trong hoạt động bảo vệ an ninh mạng (01 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát, bổ sung quy định tại Điều 6 về hợp tác quốc tế về an ninh mạng.

*+ **Khoản 2:** Có ý kiến đề nghị bổ sung "điều kiện áp dụng" biện pháp bảo vệ an ninh mạng (02 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ sẽ rà soát, bổ sung quy định về điều kiện áp dụng các biện pháp bảo vệ an ninh mạng tại văn bản quy định chi tiết hướng dẫn thi hành Luật.

- Điều 7 (Bảo vệ không gian mạng quốc gia)

Có ý kiến đề nghị bổ sung một khoản về "quyền tự vệ mạng" cho phép lực lượng chuyên trách được áp dụng các biện pháp kỹ thuật tương ứng để vô hiệu hóa hoặc cô lập nguồn tấn công gây tổn hại nghiêm trọng, tương tự quyền tự vệ an ninh truyền thống (01 ý kiến); xem xét gộp Điều 6 (Biện pháp bảo vệ an ninh mạng) với Điều 7 (Bảo vệ không gian mạng quốc gia); rà soát 14 nhóm biện pháp tại Điều 6 để tránh chồng chéo với Điều 7 vì không gian mạng không rõ ranh giới thời gian, không gian (01 ý kiến); bổ sung cụm từ "ứng phó, khắc phục các sự cố" vì ngoài việc phòng ngừa cần phải kịp thời ứng phó, khắc phục sự cố an ninh mạng (01 ý kiến).

Chính phủ đã rà soát và loại bỏ Điều khoản này khỏi dự thảo Luật và tập trung quy định bảo vệ không gian mạng quốc gia tại Điều 24 về bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế.

- Điều 8 (Hợp tác quốc tế về an ninh mạng)

+ Có ý kiến đề nghị bổ sung giao Chính phủ quy định cụ thể về cơ chế điều phối liên ngành để nâng cao hiệu quả phối hợp giữa Bộ Công an (chủ trì) với Bộ Khoa học và Công nghệ, Bộ Quốc phòng, Bộ Ngoại giao và Bộ Tư pháp, đặc biệt trong việc chia sẻ dữ liệu và cảnh báo sớm (01 ý kiến); yêu cầu "bảo đảm tuân thủ quy định của pháp Luật về bảo vệ bí mật Nhà nước" vào cuối quy định để bảo đảm chặt chẽ (01 ý kiến); bổ sung quy định"Việc thực hiện thỏa thuận quốc tế về an ninh mạng phải bảo đảm không trái Hiến pháp, giữ vững chủ quyền số quốc gia" nhằm bảo đảm tính độc lập, tự chủ và kiểm soát việc nội luật hóa cam kết quốc tế (01 ý kiến). Ý kiến khác cho rằng hợp tác quốc tế về an ninh mạng hiện nay chỉ quy định cụ thể tại điểm n khoản 1 Điều 49, đề nghị bổ sung 01 khoản riêng về hợp tác quốc tế (các loại tội phạm xuyên biên giới phổ biến) và giao Chính phủ quy định chi tiết (01 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ sẽ rà soát, nghiên cứu chỉnh lý quy định liên quan trong dự thảo Luật và văn bản quy định chi tiết, hướng dẫn thi hành Luật.

*+ **Khoản 2:** Có ý kiến đề nghị tại điểm d mở rộng phạm vi không chỉ công nghệ cao mà toàn bộ an ninh mạng (01 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát, nghiên cứu chỉnh lý quy định liên quan trong quá trình hoàn thiện dự thảo Luật.

*+ **Khoản 3, 4:** Có ý kiến đề nghị cân nhắc chuyển 2 khoản này về Điều 44 hoặc Chương VIII (quản lý nhà nước/trách nhiệm cơ quan) để thống nhất, tránh phân tán (01 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát, nghiên cứu chỉnh lý trong dự thảo Luật.

- Điều 9 (Hành vi bị nghiêm cấm về an ninh mạng)

+ Có ý kiến đề nghị rà soát, loại bỏ sự trùng lặp về nội dung giữa Điều 9 và các điều khoản trong Chương III của dự thảo Luật (01 ý kiến).

Về ý kiến nêu trên, Chính phủ báo cáo như sau: Những hành vi bị nghiêm cấm quy định tại Điều 9 là quy định của Luật chuyên ngành về an ninh mạng nói chung. Việc xác định hành vi nào là tội phạm thì sẽ căn cứ vào quy định của Bộ luật Hình sự; hành vi nào bị xử phạt hành chính thì căn cứ vào pháp luật xử lý vi phạm hành chính... bảo đảm tính thống nhất, không mâu thuẫn, chồng chéo; tương tự như quy định của Luật Phòng chống tham nhũng, Luật Phòng chống ma túy...Các nội dung tại Chương III của dự thảo Luật phục vụ cho hoạt động phòng ngừa, xử lý vi phạm của lực lượng chuyên trách bảo vệ an ninh mạng. Do vậy, nội hàm các nội dung này là khác nhau.

+ Có ý kiến đề nghị chỉ quy định nguyên tắc chính (vi phạm an ninh quốc gia, trật tự xã hội) và giao Chính phủ quy định chi tiết để linh hoạt, phù hợp Nghị quyết số 66 (Luật khung, ổn định) tránh chồng chéo, khó cập nhật công nghệ mới (02 ý kiến); phân nhóm các hành vi thành các nhóm vấn đề: nhóm vấn đề liên quan đến an ninh quốc gia; nhóm vấn đề liên quan đến tổ chức, cá nhân; nhóm vấn đề liên quan đến trật tự, an toàn xã hội (01 ý kiến); chỉ quy định hành vi bị nghiêm cấm khi có mục đích chống Nhà nước, gây bạo loạn, xâm phạm an ninh quốc gia (02 ý kiến); rà soát kỹ để thống nhất với quy định của Bộ luật Hình sự, Luật Xử lý vi phạm hành chính; cân nhắc các quy định tại điểm c khoản 1: "Bịa đặt, vu khống, vu cáo sai sự thật", vì "vu khống" đã bao hàm "vu cáo"; điểm d khoản 2: "Tuyên truyền văn hóa phẩm dâm ô", vì "dâm ô" là hành vi con người, không phải văn hóa phẩm; nên giữ "văn hóa phẩm đồi trụy"; hành vi nghe lén cho thống nhất với quy định của Luật Viễn thông (02 ý kiến).

Về ý kiến chỉ quy định nguyên tắc chính và giao Chính phủ quy định chi tiết, Chính phủ thấy rằng: Dự thảo Luật đã tham khảo quy định của các luật hiện hành thì việc quy định ngay trong Luật cụ thể những hành vi bị nghiêm cấm về an ninh mạng là phù hợp với kỹ thuật lập pháp hiện nay.

Đối với các ý kiến còn lại, tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ sẽ rà soát, nghiên cứu chỉnh lý trong dự thảo Luật.

+ Nhiều ý kiến đề nghị bổ sung hành vi sử dụng AI deepfake để tạo lập, chỉnh sửa, lan truyền video, hình ảnh, giọng nói giả nhằm vu cáo, bôi nhọ, lừa đảo (12 ý kiến); đề nghị làm rõ, giới hạn phạm vi hành vi AI bị cấm, tránh bao trùm ứng dụng AI có ích (học tập, y tế, sáng tạo); tránh hình sự hóa nghiên cứu AI (01 ý kiến); đề nghị bổ sung hành vi lạm dụng, cung cấp, cho thuê VPN để che giấu IP, vượt tường lửa, truy cập trái phép hoặc phát tán thông tin xâm phạm an ninh quốc gia, trật tự, an toàn xã hội (01 ý kiến); bổ sung trách nhiệm doanh nghiệp cung

cấp dịch vụ mạng phải định danh địa chỉ IP người dùng, truy vết hành vi trên không gian mạng (01 ý kiến); bổ sung nghiêm cấm hành vi xem trộm, xâm nhập trái phép tin nhắn, hình ảnh, văn bản trao đổi trên mạng (01 ý kiến); thu thập, khai thác, phân tích, bán dữ liệu cá nhân trẻ em không có sự đồng ý của cha mẹ hoặc người giám hộ; sử dụng tiền mã hóa, ví ẩn danh, hệ thống tài chính phi tập trung để lừa đảo chiếm đoạt tài sản, rửa tiền, buôn bán bất hợp pháp; sản xuất, nhập khẩu, sử dụng thiết bị IoT không được chứng nhận an ninh mạng tạo lỗ hổng, rò rỉ dữ liệu, công cụ tấn công (02 ý kiến); thao túng thuật toán trích xuất dữ liệu cá nhân từ dữ liệu tập thể (01 ý kiến); bổ sung hành vi xuyên tạc đường lối, chính sách của Đảng, pháp Luật của Nhà nước; hành vi xúc phạm Đảng kỳ (01 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội đối với nội dung bổ sung các hành vi liên quan đến công nghệ trí tuệ nhân tạo, Chính phủ thiết kế lại điều khoản này thành điểm g khoản 2 Điều 7 về các hành vi bị nghiêm cấm về an ninh mạng, như sau:

"g) Sử dụng trí tuệ nhân tạo hoặc công nghệ mới để giả mạo video, hình ảnh, giọng nói của người khác trái quy định của pháp luật; tạo lập, đăng tải, phát tán thông tin quy định tại khoản 1 Điều này".

Đối với các ý kiến còn lại, Chính phủ báo cáo như sau: (1) Mọi hành vi dùng VPN để xâm nhập trái phép, phát tán thông tin vi phạm đã bị cấm tại điểm k, khoản 2 và khoản 4 Điều 7 dự thảo Luật. Do vậy, cấm "VPN" nói chung không phù hợp cách tiếp cận của dự thảo Luật là không ấn định công nghệ cụ thể; (2) Nội hàm hành vi xem trộm, xâm nhập trái phép tin nhắn, hình ảnh, văn bản trao đổi trên mạng nằm trong hành vi cố tình làm lộ thông tin thuộc bí mật công tác, bí mật kinh doanh, bí mật cá nhân...(3) Điều 20 dự thảo Luật quy định chi tiết về phòng, chống xâm hại trẻ em trên mạng và trách nhiệm của doanh nghiệp/chủ quản hệ thống; (4) Thiết bị IoT không chứng nhận: Nhóm này xử lý bằng công cụ tiêu chuẩn, quy chuẩn, kiểm định, điều kiện kinh doanh (Chương V và VI), không nên chuyển thành hành vi cấm chung trong Điều 7 để tránh đánh đồng mọi vi phạm kỹ thuật thành cấm đoán tuyệt đối; (5) Nội hàm của hành vi thao túng thuật toán trích xuất dữ liệu cá nhân từ dữ liệu tập thể đã được quy định tại điểm g khoản 2 Điều này; (6) Đối với các hành vi "xuyên tạc đường lối, chính sách của Đảng" và "xúc phạm Đảng kỳ" nếu nhằm mục đích chống chính quyền nhân dân đã được quy định tại điểm a khoản 1 Điều 7 dự thảo Luật và sẽ bị xử lý theo quy định của Bộ luật Hình sự; nếu nhằm mục đích khác thì đã được quy định cụ thể tại các điểm b, c và d khoản 1 Điều 7 dự thảo Luật và bị xử lý theo quy định của pháp luật có liên quan.

+ ***Khoản 1:*** *Có ý kiến đề nghị tại điểm c bổ sung: "Bịa đặt, vu khống, sử dụng công nghệ trí tuệ nhân tạo (AI) để giả mạo âm thanh, giọng nói, video của cá nhân, tổ chức nhằm xuyên tạc sự thật, gây hiểu lầm, làm tổn hại danh dự, uy tín, quyền lợi hợp pháp hoặc gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội" (01 ý kiến); đề nghị tại điểm d bổ sung nội dung "tài sản số, tiền, tiền số, tiền mã hóa, trí tuệ nhân tạo, Blockchain, IoT" để bao quát các công nghệ mới xuất hiện thời gian gần đây (01 ý kiến); và làm rõ tiêu chí xác định thế nào*

là thông tin sai sự thật gây thiệt hại trong lĩnh vực kinh tế, đặc biệt là sự khác biệt giữa phân tích, nhận định thị trường (01 ý kiến); bổ sung hành vi xử lý dữ liệu suy luận để xác thực, xác định danh tính cá nhân khi chưa có sự đồng ý rõ ràng của chủ thể dữ liệu (01 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội đối với nội dung bổ sung các hành vi liên quan đến công nghệ trí tuệ nhân tạo, Chính phủ thiết kế lại điều khoản này thành điểm g khoản Điều 7 về các hành vi bị nghiêm cấm về an ninh mạng.

Đối với ý kiến cần làm rõ thông tin sai sự thật gây thiệt hại về kinh tế, Chính phủ nhận thấy đây là việc thông tin mang tính cố ý, biết rõ là sai sự thật. Còn việc phân tích, nhận định mang tính dự báo thị trường trên cơ sở sử dụng, phân tích các nguồn dữ liệu hợp pháp thì không bị coi là hành vi tung tin thất thiệt có chủ đích mang tính thao túng thị trường. Do vậy, quy định của dự thảo Luật không cản trở việc tự do phân tích, trao đổi thông tin trên thị trường. Bên cạnh đó, Bộ Công an đang tham mưu, trình Chính phủ ban hành Nghị định quy định một số biện pháp, công tác bảo đảm an ninh, trật tự trong phòng, chống tin giả, tin sai sự thật, trong đó có dự kiến quy định khái niệm về thông tin sai sự thật.

Với ý kiến về việc cấm xử lý dữ liệu suy luận để xác thực, xác định danh tính cá nhân khi chưa có sự đồng ý rõ ràng của chủ thể dữ liệu, Chính phủ thấy rằng hành vi này đã được điều chỉnh theo Luật Bảo vệ dữ liệu cá nhân. Do vậy việc quy định trong Luật này là không phù hợp.

*+ **Khoản 2:** Có ý kiến đề nghị tại điểm d bổ sung "các bộ phận cơ thể người" sau cụm từ "mua bán người" để phù hợp với thực tế hiện nay (01 ý kiến); có ý kiến đề nghị tại điểm e bổ sung cụm từ đó "tài sản mã hóa, tài sản số" sau cụm từ "thông tin thẻ tín dụng, tài khoản ngân hàng" (01 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ sẽ nghiên cứu rà soát để chỉnh lý, hoàn thiện trong dự thảo Luật.

- Điều 10 (Xử lý vi phạm pháp luật về an ninh mạng)

Một số ý kiến đề nghị bỏ Điều này vì không có nội dung (03 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã chuyển nội dung điều khoản này vào khoản 4 Điều 4 quy định về nguyên tắc bảo vệ an ninh mạng.

3.2. Về bảo vệ an ninh mạng đối với hệ thống thông tin (Chương II)

- Điều 11 (Phân loại cấp độ hệ thống thông tin)

+ Có ý kiến đề nghị bổ sung làm rõ kết quả tổ chức hệ thống thông tin ở các cấp độ (01 ý kiến); đề nghị quy định cụ thể hơn về thẩm định định kỳ và nâng cấp cấp độ an toàn (01 ý kiến); đề nghị bổ sung khoản 4 giao Chính phủ quyết định chi tiết và công khai tiêu chí đánh giá, thẩm quyền, trình tự phân loại cấp độ hệ thống thông tin (02 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ thiết kế lại điều khoản này thành Điều 8 về hệ thống thông tin quan trọng về an ninh quốc gia, như sau:

"**Điều 8. Phân loại cấp độ hệ thống thông tin**

1. Hệ thống thông tin được phân loại theo 5 cấp độ căn cứ vào mức độ tổn hại tới an ninh quốc gia, trật tự, an toàn xã hội, quyền, lợi ích hợp pháp của tổ chức, cá

nhân, lợi ích công cộng khi bị sự cố hoặc có hành vi vi phạm pháp luật về an ninh mạng như sau:

a) Cấp độ 1 có thể làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân;

b) Cấp độ 2 có thể làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng;

c) Cấp độ 3 có thể làm tổn hại đặc biệt nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân; tổn hại nghiêm trọng tới lợi ích công cộng; tổn hại hoặc tổn hại nghiêm trọng tới trật tự, an toàn xã hội hoặc làm tổn hại tới an ninh quốc gia;

d) Cấp độ 4 có thể làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng, trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới an ninh quốc gia;

đ) Cấp độ 5 có thể làm tổn hại đặc biệt nghiêm trọng tới an ninh quốc gia.

2. Chính phủ quy định chi tiết tiêu chí xác định cấp độ hệ thống thông tin; quy định thẩm quyền, trình tự, thủ tục xác định cấp độ hệ thống thông tin và biện pháp, trách nhiệm, nghĩa vụ bảo đảm an ninh mạng theo từng cấp độ của hệ thống thông tin.".

+ Khoản 2: tại điểm đ, đề nghị bổ sung bộ tiêu chí xác định "tổn hại đặc biệt nghiêm trọng tới chủ quyền" (03 ý kiến).

Về ý kiến nêu trên, Chính phủ báo cáo nhận thấy nội dung liên quan đến chủ quyền đã nằm trong nội hàm an ninh quốc gia.

- Điều 13 (Biện pháp bảo vệ hệ thống thông tin)

Có ý kiến đề nghị bổ sung quy định về đánh giá rủi ro cụ thể cho các hệ thống sử dụng công nghệ mới như AI, IoT và quy định về kiểm tra chuỗi cung ứng phần mềm, phần cứng để đối phó với các nguy cơ bị khai thác và tấn công chuỗi cung ứng (01 ý kiến).

Về ý kiến nêu trên, Chính phủ báo cáo như sau: Các biện pháp bảo vệ hệ thống thông tin trong dự thảo Luật được xây dựng theo hướng nguyên tắc, áp dụng cho mọi công nghệ bao gồm cả công nghệ mới, có thể trong tương lai sẽ xuất hiện. Các quy định về thẩm định, kiểm tra, đánh giá an ninh mạng; quản lý theo tiêu chuẩn, quy chuẩn kỹ thuật; sao lưu dữ liệu; giám sát an ninh mạng và ứng phó, khắc phục sự cố không phụ thuộc vào từng loại công nghệ cụ thể, do đó đã bao quát đầy đủ yêu cầu đối với các công nghệ như AI, IoT cũng như nguy cơ tấn công chuỗi cung ứng. Việc liệt kê hoặc bổ sung riêng cho từng công nghệ có thể dẫn đến trùng lặp và không theo kịp sự phát triển nhanh của công nghệ.

- Điều 14 (Hệ thống thông tin quan trọng về an ninh quốc gia)

+ Có ý kiến cho rằng, dự thảo Luật xác định cấp độ 4, 5 hoặc cấp 3 khi đáp ứng tiêu chí nhất định là quan trọng về an ninh quốc gia, do đó đề nghị quy định rõ tiêu chí để tránh gây lúng túng khi xác định hệ thống thông tin quan trọng về an ninh quốc gia (01 ý kiến); bổ sung lĩnh vực dân tộc, tôn giáo vào nhóm hệ thống thông tin quan trọng về an ninh quốc gia (01 ý kiến).

Về ý kiến nêu trên, Chính phủ thấy rằng, trong 08 hệ thống thông tin quan trọng về an ninh quốc gia quy định tại Điều 9 đã bao gồm lĩnh vực dân tộc, tôn giáo; do vậy, quy định như dự thảo Luật là phù hợp. Đối với tiêu chí để xác định là hệ thống thông tin quan trọng về an ninh quốc gia, tiếp thu ý kiến của Đại biểu Quốc hội, Chính phủ sẽ quy định trong văn bản quy định chi tiết và hướng dẫn thi

hành Luật.

+ ***Khoản 1:*** *Có ý kiến đề nghị bổ sung từ "Hệ thống thông tin được phân loại thuộc cấp độ 5, hoặc cấp độ 3, 4 khi đáp ứng tiêu chí nhất định" cho rõ ràng, thống nhất với quy định tại Điều 11 về phân loại cấp độ (01 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát, đưa nội dung này vào văn bản quy định chi tiết và hướng dẫn thi hành Luật.

+ ***Khoản 3:*** *Có ý kiến đề nghị bổ sung quy định: "Việc thẩm định, đánh giá, chứng nhận đủ điều kiện phải đảm bảo nguyên tắc công khai, minh bạch, khách quan, đúng thời hạn, tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật và không gây cản trở hoạt động bình thường của cơ quan, tổ chức, doanh nghiệp" (01 ý kiến).*

Tiếp thu ý kiến của Đại biểu Quốc hội về việc thẩm định, đánh giá, chứng nhận đủ điều kiện hệ thống thông tin quan trọng về an ninh quốc gia, Chính phủ sẽ quy định trong văn bản quy định chi tiết và hướng dẫn thi hành Luật.

- Điều 15 (Trách nhiệm bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia)

+ Nhiều ý kiến đề nghị thay thế cụm từ "hệ thống thông tin quân sự" bằng cụm từ "hệ thống thông tin quan trọng về an ninh quốc gia thuộc phạm vi quản lý của Bộ Quốc phòng" tại Điều này và các điều khoản liên quan khác tại các điều 18, 22, 23, 24, 25 32, 34 và 35 (20 ý kiến).

Về ý kiến nêu trên, Chính phủ báo cáo như sau: dự thảo Luật An ninh mạng 2025 được xây dựng trên cơ sở hợp nhất Luật An ninh mạng năm 2018 và Luật An toàn thông tin mạng năm 2015 theo nguyên tắc không làm thay đổi chức năng, nhiệm vụ của các bộ, ngành, không tạo ra chính sách mới; bảo đảm thực hiện đúng tinh thần Nghị quyết số 18-NQ/TW ngày 25/10/2017 của Ban Chấp hành Trung ương về một số vấn đề tiếp tục đổi mới, sắp xếp tổ chức bộ máy của hệ thống chính trị tinh gọn, hoạt động hiệu lực, hiệu quả (sau đây viết tắt là Nghị quyết số 18) là "một việc chỉ giao cho một cơ quan chủ trì, chịu trách nhiệm chính", bảo đảm phân công, phân cấp rõ ràng, tránh chồng chéo chức năng, nhiệm vụ, phạm vi quản lý.

Trong giai đoạn hiện nay, không một quốc gia nào có thể tự mình bảo đảm an ninh mạng vì đây là thách thức mang tính toàn cầu. Bởi vậy, tăng cường hợp tác quốc tế, chia sẻ thông tin và phối hợp hành động giữa các quốc gia là yêu cầu tất yếu để nâng cao năng lực bảo đảm an ninh mạng. Ở Việt Nam, không một bộ, ngành, địa phương, tổ chức, doanh nghiệp nào có thể tự mình bảo vệ an ninh mạng mà cần có sự tham gia, phối hợp, cộng tác, trách nhiệm của tất cả bộ, ngành, địa phương, tổ chức, doanh nghiệp, cá nhân dưới sự chủ trì, điều phối của một đầu mối thống nhất.

Hiện nay, Bộ Công an được Chính phủ giao là cơ quan giữ vai trò chủ trì, điều phối Liên minh ứng phó, khắc phục sự cố an ninh mạng quốc gia gồm các cơ quan, doanh nghiệp (tính đến nay đã có hàng chục cơ quan, doanh nghiệp tham gia liên minh), sẵn sàng được huy động để ứng phó kịp thời các sự cố, tình huống nguy hiểm về an ninh mạng xảy ra tại các hệ thống thông tin của bộ, ngành, địa phương, tập đoàn, doanh nghiệp kinh tế trọng yếu; đồng thời đảm bảo việc thu

thập dữ liệu, chứng cứ điện tử, tuân thủ các quy định của pháp luật về tố tụng hình sự để xử lý tội phạm mạng theo quy định của pháp luật.

Công ước của Liên hợp quốc về chống tội phạm mạng được 72 quốc gia ký kết tại Hà Nội vừa qua với tính ràng buộc pháp lý trên toàn cầu đã ghi nhận mỗi quốc gia thành viên chỉ định một đầu mối liên lạc sẵn sàng 24/7 nhằm bảo đảm việc cung cấp sự hỗ trợ ngay lập tức cho các hoạt động điều tra, truy tố, xét xử hoặc cho việc thu thập chứng cứ là dữ liệu điện tử. Theo phân công, Bộ Công an là cơ quan đầu mối của Việt Nam có nhiệm vụ tổ chức thực hiện Công ước.

Bản chất của bảo đảm an ninh mạng là đấu tranh phòng, chống tội phạm trên không gian mạng, trong khi đó, việc chia sẻ thông tin, thu thập chứng cứ, dữ liệu điện tử giữa các quốc gia là yếu tố quyết định hiệu quả công tác này. Cơ quan đầu mối của Việt Nam về đấu tranh, phòng, chống tội phạm trên không gian mạng cần phối hợp chặt chẽ với các quốc gia khác để chia sẻ thông tin, thu thập chứng cứ, dữ liệu điện tử, tổ chức công tác phòng ngừa và điều tra, xử lý loại tội phạm này. Bộ Công an là cơ quan đầu mối thực thi Công ước Liên hợp quốc về chống tội phạm mạng và là cơ quan chủ trì phòng ngừa và điều tra tội phạm mạng.

Thực tế hiện nay, hệ thống thông tin liên quan đến dân sự (y tế, giáo dục, năng lượng, giao thông, viễn thông, ngân hàng, tài chính, ...) của các cơ quan, tổ chức, doanh nghiệp có sự kết nối, liên thông với nhau để thực hiện các giao dịch. Do vậy, hệ thống thông tin của các cơ quan, tổ chức, doanh nghiệp chỉ được đảm bảo an ninh, an toàn khi tất cả các hệ thống thông tin phải được bảo đảm an ninh, an toàn. Chỉ một hệ thống thông tin bị tấn công, chiếm quyền điều khiển thì không chỉ ảnh hưởng đến hệ thống thông tin của cơ quan, tổ chức, doanh nghiệp đó mà còn ảnh hưởng đến an ninh, an toàn của toàn bộ hệ thống thông tin trong phạm vi cả nước hoặc toàn cầu. Thực hiện quy định của Luật An ninh mạng năm 2018, Bộ Công an đã thực hiện giám sát, cảnh báo, phát hiện nhiều lỗ hổng bảo mật, nhiều phần mềm gián điệp đối với các hệ thống thông tin. Do vậy, để bảo đảm an ninh mạng thì tất cả các hệ thống thông tin liên quan đến dân sự cơ quan, tổ chức, doanh nghiệp đều phải kết nối về Trung tâm An ninh mạng Quốc gia để giám sát, kịp thời phát hiện, cảnh báo, hướng dẫn khắc phục, bảo vệ ngay từ khi có dấu hiệu bị tấn công, không để lan rộng, làm tê liệt cả hệ thống thông tin.

Do đó, Bộ Công an là cơ quan đầu mối có trách nhiệm quản lý về bảo đảm an ninh mạng trong phạm vi cả nước, chủ trì xây dựng tiêu chuẩn, quy chuẩn kỹ thuật quốc gia, hướng dẫn tổ chức, cá nhân bảo đảm an ninh mạng cho các hệ thống thông tin quan trọng về an ninh quốc gia thuộc các lĩnh vực (bao gồm các hệ thống thông tin liên quan dân sự), trừ hệ thống thông tin quân sự, cơ yếu. Theo quy định hiện hành, lực lượng chuyên trách bảo vệ an ninh mạng của Bộ Quốc phòng chủ trì bảo đảm an ninh mạng đối với hệ thống thông tin quân sự, hướng dẫn tổ chức, cá nhân bảo vệ an ninh mạng đối với hệ thống thông tin quân sự.

*+ **Khoản 2, 3:** Có ý kiến đề nghị bổ sung quy định "Bộ Công an chủ trì phối hợp với Bộ Quốc phòng và các cơ quan, tổ chức có liên quan" (03 ý kiến); ý kiến khác đề nghị viết lại như sau:*

"2. Bộ Công an chủ trì phối hợp với Bộ Quốc phòng và các cơ quan, tổ chức có liên quan có trách nhiệm sau đây đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ hệ thống thông tin quan trọng về an ninh quốc gia thuộc phạm vi quản lý của Bộ Quốc phòng và hệ thống thông tin cơ yếu do Ban Cơ yếu Chính phủ quản lý theo quy định của pháp luật.

3. Bộ Quốc phòng chủ trì thẩm định, đánh giá, kiểm tra an ninh đột xuất, giám sát an ninh mạng và điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia thuộc phạm vi quản lý của Bộ Quốc phòng" (01 ý kiến).

Về ý kiến nêu trên, Chính phủ kế thừa quy định của Luật An ninh mạng năm 2018 và Luật An toàn thông tin mạng năm 2015 và có bổ sung quy định cho phù hợp với việc tiếp nhận chức năng, nhiệm vụ quản lý nhà nước về an toàn thông tin mạng của Bộ Công an. Do vậy, quy định như trong dự thảo Luật là phù hợp.

+ ***Khoản 4:*** *Có ý kiến đề nghị chỉnh sửa như sau: "Ban Cơ yếu Chính phủ chủ trì tổ chức triển khai giải pháp dùng mật mã bảo vệ thông tin bí mật Nhà nước trên hệ thống thông tin quan trọng quốc gia; thẩm định, đánh giá, chứng nhận đủ điều kiện an ninh mạng; kiểm tra đột xuất, giám sát an ninh mạng và điều phối ứng phó, khắc phục sự cố đối với hệ thống thông tin cơ yếu; phối hợp chủ quản hệ thống thông tin quan trọng quốc gia giám sát an ninh mạng theo pháp luật"; bỏ cụm từ "do Ban Cơ yếu Chính phủ quản lý" tránh bỏ trống pháp lý, thống nhất với khoản 26 Điều 3 (01 ý kiến); đề nghị bổ sung quy định về việc loại trừ việc kết nối hệ thống thông tin cơ yếu với hệ thống giám sát an ninh mạng, hệ thống phòng, chống mã độc tập trung về Trung tâm an ninh mạng quốc gia của Bộ Công an (03 ý kiến).*

Về ý kiến đề nghị bổ sung nội dung phối hợp chủ quản hệ thống thông tin quan trọng quốc gia giám sát an ninh mạng theo pháp luật và bỏ cụm từ "do Ban Cơ yếu Chính phủ quản lý", Chính phủ thấy rằng nội dung điều khoản này được kế thừa từ các nguyên tắc, chính sách đã áp dụng trên thực tiễn theo quy định của Luật An ninh mạng và Luật An toàn thông tin mạng, không làm phát sinh chính sách mới, không làm thay đổi chức năng, nhiệm vụ của các bộ, ngành. Do vậy, việc bổ sung như trên là không phù hợp.

Đối với ý kiến đề nghị loại trừ việc kết nối hệ thống thông tin cơ yếu với hệ thống giám sát an ninh mạng, thực tế hiện nay, hệ thống thông tin liên quan đến dân sự của các cơ quan, tổ chức, doanh nghiệp được kết nối với nhau, khi một hệ thống thông tin bị tấn công, chiếm quyền điều khiển sẽ ảnh hưởng đến an ninh, an toàn của toàn bộ hệ thống thông tin trong phạm vi cả nước hoặc toàn cầu. Theo đó, việc kết nối với Trung tâm An ninh mạng quốc gia của tất cả các hệ thống thông tin của cơ quan, tổ chức, doanh nghiệp liên quan đến dân sự để được giám sát tập trung, bảo vệ ngay từ khi có dấu hiệu bị tấn công, không để lan rộng, làm tê liệt cả hệ thống thông tin.

Bên cạnh đó, việc kết nối hệ thống thông tin cơ yếu với hệ thống giám sát an ninh mạng sẽ giúp bảo vệ hệ thống thông tin của Ban Cơ yếu Chính phủ tốt hơn.

- Điều 16 (Kiểm tra an ninh mạng với hệ thống không thuộc danh mục quan trọng)

+ ***Khoản 3:*** *Có ý kiến đề nghị bổ sung thời gian và hình thức thông báo để bảo đảm rõ ràng, thống nhất; bổ sung nội dung giao Chính phủ quy định chi tiết tại khoản 7 (01 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ sẽ bổ sung quy định tại văn bản quy định chi tiết, hướng dẫn thi hành Luật.

+ ***Khoản 4:*** *Một số ý kiến đề nghị bổ sung quy định "Bộ Quốc phòng kiểm tra an ninh mạng đối với các đơn vị thuộc quyền" nhằm bảo đảm trách nhiệm quản lý toàn diện, không để khoảng trống (05 ý kiến).*

Về ý kiến nêu trên, Chính phủ báo cáo như sau: Theo tinh thần Nghị quyết số 18 thì "một việc chỉ giao cho một cơ quan chủ trì, chịu trách nhiệm chính", bảo đảm phân công, phân cấp rõ ràng, tránh chồng chéo chức năng, nhiệm vụ, phạm vi quản lý. Mặt khác, quan điểm, mục tiêu khi xây dựng dự án Luật An ninh mạng năm 2025 là hợp nhất Luật An ninh mạng năm 2018 và Luật An toàn thông tin mạng năm 2015 theo nguyên tắc không làm thay đổi chức năng, nhiệm vụ của các bộ, ngành, không tạo ra chính sách mới. Do vậy, quy định như dự thảo Luật là phù hợp chủ trương, chính sách của Đảng và quan điểm, mục tiêu xây dựng; tránh phát sinh thêm trách nhiệm tuân thủ của chủ quản hệ thống thông tin liên quan dân sự đối với hoạt động kiểm tra an ninh mạng (một việc nhưng phải thực hiện 2 lần đối với 02 cơ quan quản lý nhà nước).

3.3. Về phòng ngừa, xử lý hành vi xâm phạm an ninh mạng (Chương III)

- Điều 17 (Phòng ngừa, xử lý thông tin xâm phạm trật tự an toàn xã hội)

+ Có ý kiến đề nghị bổ sung thời hạn gỡ thông tin cụ thể (ví dụ: tối đa 24 giờ) hoặc giao Chính phủ quy định, đồng thời nghiên cứu quy định trách nhiệm doanh nghiệp cung cấp dịch vụ xuyên biên giới để quản lý hiệu quả nền tảng ở nước ngoài (01 ý kiến); bổ sung quy định ngăn việc chính trị hóa các diễn đàn, hội nhóm (01 ý kiến); bổ sung biện pháp kỹ thuật và nghiệp vụ (AI tự động phát hiện) buộc các nhà mạng, doanh nghiệp có cơ chế tự động ngăn chặn các hành vi như xúc phạm danh dự, uy tín, nhân phẩm, lan truyền, bịa đặt, mạo danh, giả mạo thông tin, giả giọng nói (01 ý kiến); nghiên cứu hình sự hóa các hành vi này theo Công ước Hà nội (01 ý kiến); đề nghị quy định tiêu chí, quy trình xác định nội dung xuyên tạc tránh áp dụng tùy tiện, bảo vệ quyền tự do ngôn luận của công dân (01 ý kiến); có ý kiến đề nghị bổ sung cơ chế rõ ràng về việc thực hiện yêu cầu gỡ bỏ, ngăn chặn thông tin; bảo đảm quyền khiếu nại, khởi kiện của các tổ chức, cá nhân bị yêu cầu gỡ bỏ, ngăn chặn thông tin; bổ sung cơ chế giám sát độc lập đối với các hoạt động yêu cầu gỡ bỏ, ngăn chặn thông tin tránh việc lạm quyền và đảm bảo kiểm soát quyền lực (01 ý kiến).

Về ý kiến bổ sung thời hạn gỡ thông tin cụ thể, Chính phủ cho rằng quy định ràng buộc trách nhiệm đối với các doanh nghiệp cung cấp dịch vụ xuyên biên giới, để quản lý hiệu quả nền tảng ở nước ngoài đã được quy định chi tiết tại Điều 27 (Trách nhiệm bảo đảm an ninh mạng) và Điều 43 (Trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng).

Đối với các ý kiến còn lại, giữ nguyên như dự thảo Luật để đảm bảo tính kế thừa các quy định của Luật An ninh mạng năm 2018 phù hợp với quan điểm của Chính phủ và kết luận của Ủy ban Thường vụ Quốc hội trong quá trình xây dựng dự án Luật, không làm thay đổi trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan. Các ý kiến này, Chính phủ sẽ nghiên cứu tiếp tục rà soát để chỉnh lý, hoàn thiện trong văn bản quy định chi tiết và hướng dẫn thi hành Luật này.

*+ **Khoản 7:** Có ý kiến đề nghị quy định theo hướng phân loại hai nhóm thông tin về nội dung xâm hại nghiêm trọng buộc gỡ bỏ ngay (kêu gọi bạo lực, khủng bố, xâm hại trẻ em); nội dung còn vướng mắc, tranh cãi (vu khống, xúc phạm) chỉ gỡ bỏ khi có quyết định của cơ quan có thẩm quyền (02 ý kiến).*

Tiếp thu ý kiến của Đại biểu Quốc hội, Chính phủ sẽ quy định trong văn bản quy định chi tiết hướng dẫn thi hành Luật.

- Điều 18 (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)

Có ý kiến đề nghị bổ sung quy định trường hợp tiếp cận dữ liệu cá nhân của công dân phải có quyết định của Tòa án hoặc Viện kiểm sát; đối với bí mật nhà nước thì cần công bố rõ danh mục, tránh việc làm mở rộng khái niệm dẫn đến việc khó bảo quản các việc quyền tiếp cận thông tin (02 ý kiến).

Về ý kiến nêu trên, Chính phủ nhận thấy các nội nay nêu này không thuộc phạm vi điều chỉnh của Luật An ninh mạng mà đã được quy định tại Luật Bảo vệ bí mật Nhà nước, Luật Bảo vệ dữ liệu cá nhân, Luật Dữ liệu, Bộ luật Hình sự và các văn bản hướng dẫn thi hành các Luật này.

- Điều 20 (Phòng, chống xâm hại trẻ em trên không gian mạng)

+ Một số ý kiến đề nghị bổ sung quy định bảo vệ đối với các nhóm yếu thế khác như người cao tuổi, phụ nữ đơn thân, phụ nữ vùng sâu vùng xa, người mất năng lực hành vi dân sự (10 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã bổ sung một số nhóm yếu thế vào quy định tại khoản 1 Điều 35 dự thảo Luật về phổ biến kiến thức về an ninh mạng, như sau:

"1. Nhà nước có chính sách phổ biến kiến thức về an ninh mạng trong phạm vi cả nước, khuyến khích cơ quan nhà nước phối hợp với tổ chức tư nhân, cá nhân thực hiện chương trình giáo dục và nâng cao nhận thức về an ninh mạng; ưu tiên phổ biến, hướng dẫn trẻ em, người cao tuổi, người khó khăn trong nhận thức để nâng cao khả năng tự bảo vệ quyền và lợi ích hợp pháp của mình trên không gian mạng".

+ Có ý kiến đề nghị bổ sung quy định giao cơ quan quản lý nhà nước yêu cầu doanh nghiệp viễn thông, Internet, nền tảng mạng xã hội ngăn chặn hoặc gỡ bỏ thông tin xâm hại trẻ em (chậm nhất là 24h) thống nhất với Luật Quảng cáo, Luật Báo chí (01 ý kiến); yêu cầu doanh nghiệp viễn thông, Internet phải xây dựng hệ thống kỹ thuật cho phép người dùng báo cáo nội dung vi phạm, xâm hại, bạo lực trẻ em gửi đến cơ quan chức năng (01 ý kiến); nghiên cứu có cơ chế lọc nội dung, xác định độ tuổi, thiết lập đầu mối liên hệ (02 ý kiến); bổ sung quy định độ tuổi trẻ em trong không gian mạng (đồng bộ Luật Trẻ em - dưới 16 tuổi); xác thực

độ tuổi nền tảng mạng xã hội, ứng dụng trực tuyến (01 ý kiến); dẫn chiếu và hài hòa với các Luật chuyên ngành liên quan đến nhóm yếu thế cơ bản như Luật Người cao tuổi, Luật Bình đẳng giới, Luật Trẻ em, bảo đảm tính tương thích pháp luật, tránh chồng chéo và vượt quá nội dung của Luật chuyên ngành (01 ý kiến); bổ sung nguyên tắc: "Mọi hoạt động nghiệp vụ liên quan đến dữ liệu trẻ em phải tuân thủ nguyên tắc tối thiểu hóa và bảo mật dữ liệu cá nhân" (01 ý kiến).

***Khoản 1:** Có ý kiến đề nghị bỏ cụm từ "khi tham gia tương tác trên không gian mạng", bởi vì có nhiều trường hợp trẻ em mầm non bị sử dụng hình ảnh ngay cả khi trẻ em không tương tác (01 ý kiến).*

***Khoản 2:** Có ý kiến đề nghị rà soát, chỉnh lý ngắn gọn, dễ hiểu; bổ sung trách nhiệm chủ quản hệ thống thông tin, doanh nghiệp viễn thông, Internet, dịch vụ gia tăng trên không gian mạng trong ngăn chặn thông tin xâm hại trẻ em (02 ý kiến); bổ sung tiêu chí, mức độ để nhận diện nội dung gây hại cho trẻ em; áp dụng theo cấp độ rủi ro và quy mô dịch vụ để giảm gánh nặng về chi phí tuân thủ pháp luật cho doanh nghiệp nhỏ, giao Chính phủ quy định danh mục dịch vụ rủi ro để quy định chi tiết về nội dung này (01 ý kiến).*

***Khoản 4:** Có ý kiến đề nghị bổ sung cụm từ "giáo dục kiến thức, hướng dẫn kỹ năng" vào trước cụm từ "có trách nhiệm" để bảo đảm đầy đủ và tương thích với Luật Trẻ em năm 2015 (01 ý kiến).*

***Khoản 5:** Có ý kiến đề nghị giao Chính phủ quy định chi tiết về chế tài xử phạt đối với tổ chức, cá nhân không thực hiện hoặc thực hiện chậm quy định tại các khoản 2, 3 và 4 của Điều này (01 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ thiết kế lại điều khoản này thành các khoản 1, 2, 3, 4 và 5 Điều 16 về phòng, chống xâm hại trẻ em trên không gian mạng), như sau:

"1. Trẻ em có quyền được tiếp cận thông tin, tham gia hoạt động xã hội, vui chơi, giải trí, bảo vệ bí mật cá nhân, đời sống riêng tư và các quyền khác trên không gian mạng theo quy định của pháp luật.

2. Trẻ em sử dụng dịch vụ giá trị gia tăng trên không gian mạng thì cha, mẹ hoặc người giám hộ theo pháp luật dân sự đăng ký tài khoản bằng thông tin của cha, mẹ hoặc người giám hộ và có trách nhiệm giám sát, quản lý nội dung trẻ em truy cập, đăng tải và chia sẻ thông tin trên các nền tảng dịch vụ đó.

3. Chủ quản hệ thống thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ giá trị gia tăng trên không gian mạng có các trách nhiệm sau đây:

a) 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 hoặc xâm phạm đến trẻ em hoặc xâm phạm quyền trẻ em;

b) Ngăn chặn việc chia sẻ và xóa bỏ thông tin có nội dung gây nguy hại cho trẻ em hoặc xâm phạm đến trẻ em hoặc xâm phạm đến quyền trẻ em;

c) Xây dựng, triển khai các hệ thống kỹ thuật hỗ trợ hoạt động ngăn chặn nội dung xâm hại trẻ em trên không gian mạng;

d) Phối hợp với các cơ quan, tổ chức, doanh nghiệp thực hiện ngăn chặn các nguồn phát tán thông tin xâm hại trẻ em trên không gian mạng;

đ) Kịp thời thông báo, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an để xử lý.

4. 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; phòng, chống xâm hại trẻ em trên không gian mạng.

5. Cơ quan, tổ chức, cha mẹ, người giám hộ, 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 và quy định của Luật này".

- Điều 21 (Phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại)

+ Một số ý kiến đề nghị giao Bộ Quốc phòng tổ chức phòng ngừa, phát hiện, ngăn chặn, xử lý phần mềm độc hại gây ảnh hưởng đến quốc phòng, an ninh thuộc phạm vi quản lý (03 ý kiến).

Về ý kiến nêu trên, Chính phủ báo cáo như sau: Quan điểm, mục tiêu xây dựng dự án Luật An ninh mạng 2025 được cấp có thẩm quyền xác định là: việc xây dựng dự án Luật An ninh mạng 2025 trên cơ sở hợp nhất Luật An ninh mạng năm 2018 và Luật An toàn thông tin mạng năm 2015, không làm thay đổi chức năng, nhiệm vụ của các bộ, ngành; đảm bảo thực hiện đúng tinh thần Nghị quyết số 18 là "một việc chỉ giao cho một cơ quan chủ trì, chịu trách nhiệm chính", bảo đảm phân công, phân cấp rõ ràng, tránh chồng chéo chức năng, nhiệm vụ, phạm vi quản lý. Do vậy, Chính phủ giữ nguyên như dự thảo Luật.

+ Có ý kiến đề nghị thay vì giao Bộ Công an chủ trì, phối hợp thì nên xem xét thành lập một tổ chức với cơ chế độc lập có thẩm quyền trực tiếp hoặc điều phối để tránh chậm trễ trong tổ chức thực hiện (01 ý kiến).

Về ý kiến nêu trên, Chính phủ thấy rằng việc thành lập một tổ chức độc lập để "trực tiếp hoặc điều phối" phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại sẽ làm phát sinh thêm tổ chức bộ máy, biên chế, thêm tầng nấc trung gian không phù hợp tinh thần Nghị quyết số 18 về tinh gọn tổ chức, tinh giản biên chế và phân định rõ thẩm quyền.

- Điều 22 (Phòng, chống tấn công mạng)

+ Có ý kiến đề nghị gộp các điểm a, b và c của khoản 4 thành một nội dung về chức năng, nhiệm vụ của Bộ Công an và Bộ Quốc phòng (03 ý kiến).

Về việc gộp các điểm a, b và c khoản 4 thành một khoản, Chính phủ thấy rằng chưa phù hợp với quan điểm xây dựng dự án luật, cụ thể: Dự thảo Luật An ninh mạng được xây dựng trên cơ sở hợp nhất Luật An ninh mạng năm 2018 và Luật An toàn thông tin mạng năm 2015 theo nguyên tắc không làm thay đổi chức năng, nhiệm vụ của các bộ, ngành, không tạo ra chính sách mới.

+ Có ý kiến đề nghị thay vì giao Bộ Công an chủ trì, phối hợp thì nên xem xét thành lập một tổ chức với cơ chế độc lập có thẩm quyền trực tiếp hoặc điều phối để tránh chậm trễ trong tổ chức thực hiện (01 ý kiến).

Về ý kiến này, Chính phủ cho rằng nếu tiếp thu sẽ dẫn tới phát sinh thêm tổ chức bộ máy, biên chế, thêm tầng nấc trung gian không phù hợp tinh thần Nghị quyết số 18.

- Điều 23 (Phòng, chống khủng bố mạng)

+ Có ý kiến đề nghị làm rõ khái niệm "nguồn khủng bố mạng" để thuận lợi cho việc tổ chức thực hiện, bảo đảm minh bạch và thống nhất trong áp dụng pháp luật (01 ý kiến); đề nghị gộp các khoản 4, 5 và 6 thành một khoản quy định thống nhất trách nhiệm giữa Bộ Công an, Bộ Quốc phòng và Ban Cơ yếu Chính phủ trong công tác phòng, chống khủng bố mạng (02 ý kiến).

Về ý kiến đề nghị bổ sung định nghĩa *"nguồn khủng bố mạng"* trong dự thảo Luật này, Chính phủ cho rằng sẽ dẫn tới xung đột với luật hiện hành, trong khi thẩm quyền, nhiệm vụ đã rõ.

Đối với ý kiến về việc gộp các khoản 4, 5 và 6 thành một khoản, Chính phủ thấy rằng chưa phù hợp với quan điểm xây dựng dự án luật, cụ thể: Dự thảo Luật An ninh mạng được xây dựng trên cơ sở hợp nhất Luật An ninh mạng năm 2018 và Luật An toàn thông tin mạng năm 2015 theo nguyên tắc không làm thay đổi chức năng, nhiệm vụ của các bộ, ngành, không tạo ra chính sách mới.

+ Có ý kiến đề nghị bổ sung quy định cụ thể về hành vi khủng bố mạng như phát tán dữ liệu nhạy cảm, gây hỗn loạn, tống tiền, đe dọa an toàn tính mạng, sức khỏe, xâm hại đến các đối tượng có nhược điểm về thể chất, tinh thần trên không gian mạng (01 ý kiến).

Về ý kiến này, Chính phủ báo cáo như sau: tại khoản 14 Điều 2 dự thảo Luật đã giải thích thuật ngữ "khủng bố mạng", đối với những hành vi cụ thể Đại biểu Quốc hội đã nêu thuộc phạm vi những hành vi bị nghiêm cấm tại Điều 7 dự thảo Luật.

- Điều 25 (Đấu tranh bảo vệ an ninh mạng)

Khoản 3: *Một số ý kiến đề nghị giao Bộ Công an và Bộ Quốc phòng chủ trì phối hợp với bộ, ngành có liên quan thực hiện đấu tranh bảo vệ an ninh mạng thuộc phạm vi quản lý (04 ý kiến).*

Về ý kiến này, Chính phủ báo cáo như sau: Nghị quyết số 18 là "một việc chỉ giao cho một cơ quan chủ trì, chịu trách nhiệm chính", bảo đảm phân công, phân cấp rõ ràng, tránh chồng chéo chức năng, nhiệm vụ, phạm vi quản lý. Mặt khác, nguyên tắc trong quá trình xây dựng dự thảo Luật An ninh mạng 2025 được xây dựng trên cơ sở hợp nhất Luật An ninh mạng năm 2018 và Luật An toàn thông tin mạng năm 2015 theo nguyên tắc không làm thay đổi chức năng, nhiệm vụ của các bộ, ngành, không tạo ra chính sách mới. Do vậy, Chính phủ đề nghị giữ nguyên như quy định của dự thảo Luật.

3.4. Về hoạt động bảo vệ an ninh mạng (Chương IV)

- Điều 27 (Phân loại thông tin)

Có ý kiến đề nghị bỏ Điều này hoặc giao Chính phủ quy định chi tiết để tránh trùng lặp, xung đột với quy định của Luật Bảo vệ bí mật Nhà nước, Luật Dữ liệu và Luật Bảo vệ dữ liệu cá nhân (01 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát và lược bỏ nội dung này.

- Điều 28 (Quản lý gửi thông tin trên mạng)

Khoản 2: *Có ý kiến đề nghị làm rõ "thông tin mang tính thương mại", nếu phòng chống thư rác quảng cáo thì cần thiết kế lại cho rõ nội hàm, tránh nhầm lẫn với bảo vệ bí mật kinh doanh (02 ý kiến); đề nghị giới hạn phạm vi thông tin xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, mà không nên điều chỉnh truyền thông thương mại thông thường tránh gây khó khăn doanh nghiệp (01 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát và không sử dụng thuật ngữ "thông tin mang tính thương mại" tại dự thảo Luật.

- Điều 30 (Bảo vệ an ninh mạng đối với hạ tầng không gian mạng quốc gia, cổng kết nối quốc tế)

Có ý kiến đề nghị bổ sung vai trò của Bộ Quốc phòng tại cổng kết nối tuyến cáp, trạm trục quốc tế khi nâng mức cảnh báo, quy định rõ quy trình phối hợp, chia sẻ chỉ số tấn công (IOC) thời gian thực (01 ý kiến).

Về ý kiến này, Chính phủ cho rằng cần thiết kế thừa nội dung "Bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế" quy định tại Luật An ninh mạng năm 2018 theo nguyên tắc không làm thay đổi chức năng, nhiệm vụ của các bộ, ngành, không tạo ra chính sách mới.

- Điều 31 (Bảo đảm an ninh thông tin mạng)

Khoản 2: Có ý kiến đề nghị sửa đổi khoản 2 (điểm a, b, c) yêu cầu doanh nghiệp trong nước và nước ngoài cung cấp dịch vụ tại Việt Nam có trách nhiệm cung cấp thông tin người dùng, ngăn chặn, xóa bỏ thông tin vi phạm và ngừng cung cấp dịch vụ khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an và Bộ Quốc phòng (bổ sung Bộ Quốc phòng vào tất cả các điểm) (02 ý kiến); đề nghị bỏ quy định về giới hạn 24 giờ để bảo đảm tính khả thi (01 ý kiến).

Về các ý kiến trên, Chính phủ báo cáo như sau: Việc đấu tranh phòng, chống tội phạm trên không gian mạng là trách nhiệm của tất cả các quốc gia, không một quốc gia nào đứng ngoài cuộc, mặt khác, nội hàm của bảo đảm an ninh mạng là đấu tranh phòng, chống tội phạm mạng, theo đó, việc tăng cường hợp tác quốc tế, chia sẻ thông tin và phối hợp hành động giữa các quốc gia là yêu cầu tất yếu để nâng cao năng lực bảo đảm an ninh mạng. Để tạo ra khung pháp lý ràng buộc trong phòng, chống tội phạm mạng trên phạm vi toàn cầu thì ra đời của Công ước của Liên hợp quốc về chống tội phạm mạng có ý nghĩa rất quan trọng (Công ước đã được 72 quốc gia ký kết tại Hà Nội); theo Công ước này, mỗi quốc gia thành viên chỉ định một đầu mối liên lạc sẵn sàng 24/7 nhằm bảo đảm việc cung cấp sự hỗ trợ ngay lập tức cho các hoạt động điều tra, truy tố, xét xử hoặc cho việc thu thập chứng cứ là dữ liệu điện tử và theo phân công Bộ Công an là cơ quan đầu mối chủ trì triển khai các trách nhiệm, nghĩa vụ của Việt Nam theo tinh thần của Công ước Liên hợp quốc về chống tội phạm mạng.

- Điều 32 (Bảo đảm an ninh dữ liệu)

+ Có ý kiến đề nghị gộp Điều 31 và Điều 32 thành một điều quy định rõ về nguyên tắc, đầu mối quản lý, trách nhiệm phối hợp nhằm giảm song trùng thủ tục hành chính; bổ sung điều khoản chuyển tiếp nhằm tránh xáo trộn khi Luật Dữ liệu đang triển khai (01 ý kiến).

Về ý kiến trên, Chính phủ cho rằng nội hàm an ninh thông tin (khoản 2 Điều 2) và an ninh dữ liệu (khoản 3 Điều 2) là khác nhau nên cần có quy định riêng để đảm bảo khả năng thực thi sau khi Luật được ban hành.

+ Khoản 2: Có ý kiến đề nghị bổ sung điểm c như sau: "Ban Cơ yếu Chính phủ kiểm tra, đánh giá điều kiện đảm bảo an ninh dữ liệu trong hệ thống thông tin cơ yếu, các cơ sở dữ liệu, trung tâm dữ liệu, hệ thống lưu trữ dữ liệu thuộc Ban Cơ yếu Chính phủ quản lý" (01 ý kiến); đề nghị quy định việc cung cấp thông tin phải được thực hiện bằng văn bản điện tử có xác thực hoặc hệ thống kết nối chính thức giữa doanh nghiệp và cơ quan nhà nước, đảm bảo nguyên tắc bảo vệ dữ liệu cá nhân (01 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ sẽ quy định nội dung trên tại văn bản quy định chi tiết, hướng dẫn thi hành Luật.

+ Có ý kiến đề nghị bổ sung 2 khoản như sau:

"Khoản 3. Dữ liệu thuộc sở hữu nhà nước, dữ liệu hình thành trong quá trình hoạt động của các cơ quan, tổ chức, doanh nghiệp Việt Nam có giá trị chiến lược phải được quản lý thống nhất theo quy định của Chính phủ và việc lưu trữ, xử lý, chuyển dữ liệu ra nước ngoài phải được thẩm định về an ninh mạng đối với doanh nghiệp nước ngoài cung cấp dịch vụ tại Việt Nam phải lưu trữ dữ liệu người dùng Việt Nam tại Việt Nam, chấp hành kiểm tra, giám sát.

Khoản 4. Doanh nghiệp nước ngoài cung cấp dịch vụ trên không gian mạng tại Việt Nam có trách nhiệm lưu trữ dữ liệu người sử dụng Việt Nam trên lãnh thổ Việt Nam và chấp hành yêu cầu kiểm tra, giám sát của cơ quan có thẩm quyền theo quy định" (01 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ thiết kế lại điều khoản này thành Điều 26 về trách nhiệm bảo đảm an ninh dữ liệu, như sau:

"Điều 26. Bảo đảm an ninh dữ liệu

1. Bảo đảm an ninh dữ liệu là tổng thể các biện pháp kỹ thuật, tổ chức và pháp lý nhằm bảo vệ dữ liệu, phòng, chống xâm phạm an ninh dữ liệu.

2. Nội dung bảo đảm an ninh dữ liệu bao gồm:

a) Xây dựng chính sách, thiết lập quy trình về bảo đảm an ninh dữ liệu;

b) Áp dụng biện pháp, tiêu chuẩn, quy chuẩn kỹ thuật theo quy định của pháp luật về an ninh mạng;

c) Sử dụng mật mã cơ yếu, mật mã dân sự để bảo đảm an ninh dữ liệu;

d) Triển khai cơ chế kiểm soát chặt chẽ nhân sự trực tiếp tham gia xử lý dữ liệu;

đ) Kiểm tra, đánh giá rủi ro định kỳ nhằm phát hiện, ngăn chặn và xử lý kịp thời các nguy cơ đe dọa an ninh dữ liệu;

e) Kiểm tra, đánh giá việc chuyển dữ liệu xuyên biên giới; điều kiện đảm bảo an ninh dữ liệu trong hệ thống thông tin quan trọng về an ninh quốc gia, các cơ sở dữ liệu, trung tâm dữ liệu, hệ thống lưu trữ dữ liệu;

g) Các nội dung khác theo quy định của pháp luật.

3. Chính phủ quy định chi tiết khoản 2 Điều này; quy định trách nhiệm bảo đảm an ninh dữ liệu.".

3.5. Về tiêu chuẩn, quy chuẩn kỹ thuật, sản phẩm, dịch vụ an ninh mạng

(Chương V)

- Ý kiến chung

+ Có ý kiến đề nghị không quy định lại nội dung về tiêu chuẩn và quy chuẩn kỹ thuật trong dự thảo Luật An ninh mạng vì Luật Tiêu chuẩn và quy chuẩn kỹ thuật đã quy định rõ trách nhiệm của các bộ, ngành (01 ý kiến). Ý kiến khác cho rằng quy định tại dự thảo Luật thiên về tiền kiểm (giấy phép kinh doanh, chứng nhận hành nghề) làm tăng thủ tục hành chính, chi phí tuân thủ, sẽ gây bất lợi doanh nghiệp khởi nghiệp công nghệ, nên đề nghị chuyển sang hậu kiểm để cho doanh nghiệp tự do kinh doanh nếu đáp ứng tiêu chuẩn, quy chuẩn và Nhà nước kiểm tra khi có dấu hiệu vi phạm, bảo đảm phù hợp Nghị quyết số 66 để phục vụ cải cách thể chế, phát triển kinh tế số (01 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ không quy định cụ thể về tiêu chuẩn, quy chuẩn kỹ thuật trong dự thảo Luật; việc quản lý tiêu chuẩn, quy chuẩn kỹ thuật được thực hiện theo quy định của quy định pháp luật về tiêu chuẩn, quy chuẩn kỹ thuật.

Với ý kiến cho rằng, dự thảo Luật thiên về tiền kiểm, Chính phủ thấy rằng, Luật Đầu tư quy định kinh doanh sản phẩm, dịch vụ an ninh mạng (an toàn thông tin mạng trước đây) là ngành nghề kinh doanh có điều kiện do vậy, Chính phủ giữ nguyên như dự thảo để bảo đảm tính kế thừa quy định tại Luật An toàn thông tin mạng năm 2015.

+ Có ý kiến đề nghị bổ sung quy định về mạng riêng ảo (VPN) vào Chương VI về kinh doanh sản phẩm, dịch vụ an ninh mạng nhằm chủ động kiểm soát hạ tầng truy cập xuyên biên giới (01 ý kiến); bổ sung một điều khuyến khích doanh nghiệp trong nước tăng cường nội lực, làm chủ công nghệ; được ưu tiên trong mua sắm, đấu thầu, tiếp cận nguồn vốn Chính phủ đối với các doanh nghiệp, các sản phẩm, dịch vụ do tổ chức, doanh nghiệp, người Việt Nam sản xuất đạt tiêu chuẩn quốc gia được cấp chứng nhận an ninh mạng quốc gia (01 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát và quy định những nội dung trên tại các điều khoản cụ thể.

- Điều 34 (Tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng)

Có ý kiến đề nghị bổ sung quy định "Nhà nước cho phép thử nghiệm có kiểm soát (sandbox) đối với công nghệ mới trong an ninh mạng, khoa học dữ liệu, AI, nông nghiệp thông minh trước khi ban hành tiêu chuẩn chính thức" bảo đảm linh hoạt để khuyến khích đổi mới sáng tạo; thử nghiệm trong môi trường an toàn cung cấp dữ liệu thực tiễn để xây dựng tiêu chuẩn phù hợp (01 ý kiến); đề nghị quy định mở và mang tính nguyên tắc, bảo đảm tương thích với các điều ước quốc tế, phù hợp với phát triển công nghệ; giao Chính phủ công bố danh mục tiêu chuẩn bắt buộc theo từng cấp độ của hệ thống thông tin, đồng thời thừa nhận tiêu chuẩn quốc tế khi đáp ứng yêu cầu (01 ý kiến).

***Khoản 6:** Có ý kiến đề nghị chỉnh sửa như sau: "Bộ Công an trình Chính phủ quy định tiêu chuẩn quốc gia về an ninh mạng" phù hợp thẩm quyền ban hành (01 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ chỉnh lý dự thảo Luật theo hướng các nội dung có liên quan đến tiêu chuẩn, quy chuẩn được quy định tại 01 điều khoản, cụ thể như sau:

"Điều 27. Tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng

1. Tiêu chuẩn an ninh mạng, quy chuẩn kỹ thuật an ninh mạng được áp dụng đối với hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng, sản phẩm, dịch vụ an ninh mạng, công nghệ thông tin và thiết bị kết nối mạng.

2. Việc chứng nhận hợp quy về an ninh mạng, công bố hợp quy về an ninh mạng, chứng nhận hợp chuẩn về an ninh mạng, công bố hợp chuẩn về an ninh mạng thực hiện theo quy định của pháp luật về tiêu chuẩn và quy chuẩn kỹ thuật.

3. Việc đánh giá hợp chuẩn, hợp quy về an ninh mạng phục vụ hệ thống thông tin quan trọng về an ninh quốc gia và phục vụ hoạt động quản lý nhà nước về an ninh mạng được thực hiện tại tổ chức chứng nhận hợp chuẩn, hợp quy do Bộ trưởng Bộ Công an chỉ định.

4. Bộ Công an có trách nhiệm sau đây:

a) Xây dựng dự thảo tiêu chuẩn quốc gia về an ninh mạng;

b) Xây dựng và ban hành quy chuẩn kỹ thuật quốc gia về an ninh mạng;

c) Quản lý chất lượng sản phẩm, dịch vụ an ninh mạng, trừ sản phẩm, dịch vụ mật mã dân sự;

d) Đăng ký, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp về an ninh mạng, trừ trường hợp quy định tại khoản 5 và khoản 6 Điều này.

5. Bộ Quốc phòng đăng ký, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp về an ninh mạng trong lĩnh vực quân sự.

6. Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng thực hiện quản lý chất lượng sản phẩm, dịch vụ mật mã dân sự; đăng ký, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp về an ninh mạng đối với sản phẩm, dịch vụ mật mã dân sự".

Đối với các ý kiến khác, tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ nghiên cứu bổ sung trong văn bản quy định chi tiết, hướng dẫn thi hành Luật.

- Điều 35 (Đánh giá hợp chuẩn, hợp quy)

Có ý kiến đề nghị bổ sung thẩm quyền của Bộ trưởng Bộ Quốc phòng vào khoản 2 (01 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ không quy định cụ thể về tiêu chuẩn, quy chuẩn kỹ thuật trong dự thảo Luật. Hiện tại các nội dung có liên quan đến tiêu chuẩn, quy chuẩn đã quy định tại Điều 27 (mới).

- Điều 37 (Điều kiện Cấp giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng)

Có ý kiến đề nghị bổ sung quy định về thẩm quyền cấp phép (cấp, sửa đổi, gia hạn...) ngay trong Điều này trước khi giao Chính phủ quy định chi tiết (01 ý kiến); cần làm rõ ý nghĩa của việc "trừ doanh nghiệp có vốn đầu tư nước ngoài", mở rộng khái niệm "doanh nghiệp" thành "Tổ chức kinh tế" để bao gồm hợp tác xã, liên hiệp hợp tác xã (01 ý kiến); bổ sung quy định về thời hạn giải quyết thủ tục cấp Giấy phép kinh doanh sản phẩm dịch vụ an ninh mạng (02 ý kiến); bổ

sung khoản 5 quy định: "Giao Chính phủ quy định chi tiết điều kiện, thẩm quyền cấp, sửa đổi, gia hạn, tạm đình chỉ, thu hồi giấy phép" (01 ý kiến).

***Khoản 1:** Có ý kiến đề nghị sửa điều khoản dẫn chiếu thành "điểm a, khoản 2, Điều 36 của Luật này" (02 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ sẽ rà soát, bổ sung tại văn bản quy định chi tiết, hướng dẫn thi hành Luật.

- Điều 38 (Doanh nghiệp kinh doanh sản phẩm/dịch vụ an ninh mạng)

Có ý kiến đề nghị quy định giao Bộ Quốc phòng quản lý đối với các doanh nghiệp thuộc Bộ Quốc phòng (01 ý kiến).

***Khoản 3:** Có ý kiến cho rằng quy định doanh nghiệp báo cáo Ủy ban nhân dân tỉnh, thành phố là chưa thống nhất với Luật Tổ chức chính quyền địa phương, đề nghị sửa thành "Ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương" (01 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ sẽ rà soát, bổ sung tại văn bản quy định chi tiết, hướng dẫn thi hành Luật.

- Điều 39. Xuất khẩu, nhập khẩu sản phẩm an ninh mạng

Có ý kiến đề nghị bỏ khoản 4 giao "Chính phủ quy định chi tiết" vì đã được quy định cụ thể tại các khoản 1, 2 và 3 (01 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ thiết kế lại các điều khoản về kinh doanh sản phẩm, dịch vụ thành Điều 29 về kinh doanh sản phẩm, dịch vụ an ninh mạng, như sau:

"Điều 29. Kinh doanh sản phẩm, dịch vụ an ninh mạng

1. Doanh nghiệp kinh doanh sản phẩm, dịch vụ an ninh mạng phải có Giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng.

2. Doanh nghiệp kinh doanh sản phẩm, dịch vụ an ninh mạng có trách nhiệm sau đây:

a) Thực hiện đúng Giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng; tuân thủ quy định của pháp luật về an ninh mạng và quy định khác của pháp luật có liên quan.

b) Bảo đảm về chất lượng sản phẩm, dịch vụ an ninh mạng đúng với tiêu chuẩn công bố áp dụng, quy chuẩn kỹ thuật tương ứng theo quy định của pháp luật về chất lượng sản phẩm, pháp luật về tiêu chuẩn và quy chuẩn kỹ thuật trước khi lưu thông trên thị trường.

c) Lập, lưu giữ và bảo mật thông tin của khách hàng, quản lý hồ sơ, tài liệu về giải pháp kỹ thuật, công nghệ của sản phẩm, hoạt động cung cấp dịch vụ theo quy định của pháp luật.

d) Từ chối cung cấp sản phẩm, dịch vụ an ninh mạng khi phát hiện tổ chức, cá nhân vi phạm pháp luật về sử dụng sản phẩm, dịch vụ an ninh mạng, vi phạm cam kết đã thỏa thuận về sử dụng sản phẩm, dịch vụ do doanh nghiệp cung cấp.

đ) Phối hợp, tạo điều kiện, thực hiện yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng để thực hiện các biện pháp bảo vệ an ninh mạng.

3. Chính phủ quy định việc cấp, tạm đình chỉ, thu hồi Giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng; quy định việc nhập khẩu, xuất khẩu sản phẩm an ninh mạng; quy định việc kinh doanh sản phẩm, dịch vụ an ninh mạng".

3.6. Về lực lượng, điều kiện bảo đảm an ninh mạng (Chương VI)

- Về thẩm quyền của lực lượng chuyên trách bảo vệ an ninh mạng

+ Một số ý kiến đề nghị rà soát toàn bộ các điều quy định trách nhiệm cụ thể của bộ, ngành theo hướng chỉ giữ lại trong Luật nội dung quản lý, còn trách nhiệm thì giao Chính phủ phân công cụ thể (05 ý kiến); đề nghị phân định rõ chức năng, thẩm quyền và cơ chế phối hợp thực hiện nhiệm vụ giữa các bộ, ngành, các cơ quan liên quan được xác định trong dự thảo Luật (04 ý kiến).

Tiếp thu ý kiến của Đại biểu Quốc hội, Chính phủ sẽ nghiên cứu rà soát, bổ sung tại văn bản quy định chi tiết, hướng dẫn thi hành Luật.

+ Có ý kiến đề nghị rà soát, chỉnh lý theo hướng giao lực lượng chuyên trách bảo vệ an ninh mạng của Bộ Công an chịu trách nhiệm chủ trì bảo đảm an ninh mạng trong phạm vi cả nước. Các lực lượng, cơ quan khác theo chức năng, nhiệm vụ có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng của Bộ Công an thực hiện công tác bảo vệ an ninh mạng (01 ý kiến).

Tiếp thu ý kiến của Đại biểu Quốc hội, Chính phủ sẽ nghiên cứu rà soát, chỉnh lý hoàn thiện dự thảo Luật.

+ Có ý kiến đề nghị bổ sung cơ chế bắt buộc phải có sự phê chuẩn của Tòa án hoặc Viện kiểm sát đối với biện pháp xâm nhập dữ liệu cá nhân, nghe lén hoặc giám sát đặc biệt để phù hợp thông lệ quốc tế, bảo đảm quyền con người (02 ý kiến).

Về ý kiến trên, Chính phủ thấy rằng nội dung dự thảo Luật không quy định chi tiết về vấn đề này do việc xâm nhập dữ liệu cá nhân, nghe lén hoặc giám sát đặc biệt để thu thập được thực hiện theo quy định của pháp luật có liên quan.

+ Có ý kiến đề nghị về một số nội dung liên quan đến trách nhiệm của Bộ Quốc phòng như sau (02 ý kiến):

Bộ Quốc phòng quản lý và bảo vệ hệ thống thông tin Bộ Quốc phòng sẽ quản lý và bảo vệ hệ thống thông tin, dữ liệu quốc phòng, bí mật Nhà nước và hạ tầng trọng yếu, xây dựng tổ chức chỉ huy, điều hành lực lượng tác chiến không gian mạng, xây dựng quản lý mạng riêng để phục vụ quốc phòng, ban hành tiêu chuẩn, quy chuẩn kỹ thuật an toàn mạng trong Quân đội, kiểm tra, kiểm định, đánh giá an toàn hệ thống thông tin thuộc phạm vi quản lý nhà nước về quốc phòng.

Bộ Quốc phòng được triển khai các biện pháp kỹ thuật, nghiệp vụ để phát hiện, ngăn chặn, vô hiệu hóa tấn công mạng có yếu tố xâm phạm chủ quyền, đồng thời phối hợp chặt chẽ với Bộ Công an, Bộ Khoa học và Công nghệ trong phòng ngừa, điều tra, xử lý và khắc phục các hậu quả.

Bộ Quốc phòng xây dựng và triển khai Chiến lược quốc phòng mạng quốc gia, tham mưu Chính phủ thành lập trung tâm chỉ huy tác chiến mạng quốc gia và làm đầu mối thống nhất chỉ huy khi có tình huống.

Bộ Quốc phòng là cơ quan thường trực tác chiến mạng quốc gia, Bộ Công An chủ trì điều tra, xử lý tội phạm mạng, cơ chế phối hợp liên ngành cần được thể chế theo nguyên tắc phân định rõ vai trò chủ trì nhưng không có nghĩa phân

chia để cắt khúc mà để xác định trách nhiệm chính trong từng lĩnh vực, từ đó làm cơ sở cho sự phối hợp có hiệu quả giữa các lực lượng, các bên có liên quan.

Quy định rõ nguyên tắc, nội dung, hình thức trách nhiệm phối hợp, cơ chế chia sẻ thông tin, đánh giá tình hình, cảnh báo sớm các nguy cơ, cơ chế chỉ huy hiệp đồng thống nhất trong các tình huống phức tạp, các tình huống khẩn cấp về an ninh mạng, đặc biệt khi đất nước chuyển sang các trạng thái phức tạp về quốc phòng, ví dụ khẩn cấp về quốc phòng hoặc tình trạng có chiến tranh, tránh tình trạng chồng chéo khi có sự việc xảy ra hoặc tạo ra những khoảng trống về trách nhiệm mà không có lực lượng nào tham gia xử lý.

Đối với những ý kiến này của Đại biểu Quốc hội, Chính phủ đã tiếp thu, giải trình tại từng điều khoản cụ thể.

+ Về nguồn nhân lực an ninh mạng, có ý kiến đề nghị bổ sung chính sách đặc thù sau đây: Ưu tiên hỗ trợ kinh phí đào tạo, thu hút chuyên gia, chuyển giao công nghệ cho vùng sâu, vùng xa, đồng bào dân tộc thiểu số, kinh tế khó khăn để xây dựng lực lượng tại chỗ (01 ý kiến); xây dựng Chiến lược quốc gia phát triển nhân lực an ninh mạng; đào tạo chuyên sâu, nghiên cứu, cấp chứng chỉ nghề, xây dựng mô hình hợp tác Nhà nước - đại học - doanh nghiệp; tuyên truyền giáo dục nhận thức hình thành Văn hóa an ninh mạng toàn xã hội (02 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ sẽ tiếp tục nghiên cứu rà soát để chỉnh lý, hoàn thiện trong dự thảo Luật.

- Điều 40 (Nghiên cứu phát triển)

Có ý kiến đề nghị không quy định cụ thể nội dung nghiên cứu vì sẽ không thích ứng khi công nghệ thay đổi nhanh; chỉ quy định chính sách Nhà nước khuyến khích, tạo điều kiện cho cơ quan, tổ chức, cá nhân nghiên cứu phát triển (01 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ sẽ tiếp tục rà soát để chỉnh lý, hoàn thiện trong dự thảo Luật.

- Điều 41 (Nâng cao năng lực tự chủ)

Có ý kiến đề nghị bỏ điểm a khoản 2, vì thuộc trách nhiệm Bộ Công an (đầu mối quản lý nhà nước) trong xây dựng, phối hợp ban hành (01 ý kiến).

Về ý kiến trên, Chính phủ báo cáo như sau: Nguồn lực xây dựng tiêu chuẩn, quy chuẩn kỹ thuật trước nay đều phụ thuộc vào cơ quan quản lý nhà nước, sự tham gia của các tổ chức khoa học công nghệ, xã hội nghề nghiệp như: viện, trường, hội, hiệp hội, doanh nghiệp, tư nhân vẫn còn rất hạn chế. Do vậy, để bảo đảm thực hiện thì quy định như dự thảo Luật.

- Điều 42 (Lực lượng bảo vệ an ninh mạng)

+ Có ý kiến đề nghị quy định cụ thể thành phần, số lượng từng cấp (bộ, ngành, địa phương) để triển khai dễ dàng, đồng bộ, tránh chồng chéo (01 ý kiến); bổ sung các quy định về chức năng, nhiệm vụ đào tạo chuyên sâu về công nghệ, trang thiết bị, chế độ, chính sách đãi ngộ làm cơ sở xây dựng lực lượng chuyên trách tại Bộ Công an và Bộ Quốc phòng, chuyên nghiệp, hiện đại (01 ý kiến).

Tiếp thu ý kiến của Đại biểu Quốc hội, Chính phủ sẽ nghiên cứu bổ sung các quy định trên trong văn bản quy định chi tiết, hướng dẫn thi hành Luật.

*+ **Khoản 2:** Có ý kiến đề nghị làm rõ tính chất, thẩm quyền, chủ trì, phối hợp, chuyên trách tránh chồng chéo, triển khai hiệu quả (01 ý kiến).*

Tiếp thu ý kiến của Đại biểu Quốc hội, Chính phủ sẽ quy định trong văn bản quy định chi tiết, hướng dẫn thi hành Luật.

*+ **Khoản 3:** Có ý kiến đề nghị bổ sung cơ chế huy động để làm cơ sở cho các cơ quan, lực lượng có thẩm quyền khi thực hiện việc điều động những lúc cần thiết (01 ý kiến).*

Về ý kiến trên, Chính phủ báo cáo như sau: Bổ sung cơ chế huy động vào Luật An ninh mạng là không cần thiết và không phù hợp với phạm vi điều chỉnh của Luật, do nội dung này đã được quy định đầy đủ trong các luật chuyên ngành như Luật An ninh quốc gia, Luật Quốc phòng, Luật Công an nhân dân và các văn bản quy định về huy động lực lượng, phương tiện phục vụ nhiệm vụ bảo đảm an ninh, trật tự. Việc đưa quy định này vào Luật An ninh mạng sẽ dẫn tới trùng lặp, chồng chéo trong hệ thống pháp luật, đồng thời có thể tạo ra cách hiểu mở rộng, làm phát sinh nguy cơ lạm dụng hoặc can thiệp vượt quá thẩm quyền. Bên cạnh đó, công tác bảo vệ an ninh mạng đòi hỏi tính linh hoạt, bí mật, và được thực hiện theo cơ chế điều phối tập trung. Việc bổ sung một cơ chế huy động riêng trong Luật An ninh mạng sẽ gây phân tán đầu mối, ảnh hưởng tới công tác chỉ đạo, điều hành và làm phức tạp hóa quy trình ứng phó trong thực tiễn. Vì những lý do nêu trên, Chính phủ đề xuất giữ nguyên quy định hiện hành, không bổ sung cơ chế huy động vào dự thảo Luật, nhằm bảo đảm tính thống nhất của hệ thống pháp luật, đồng thời nâng cao hiệu quả thực thi trong lĩnh vực bảo vệ an ninh mạng.

- Điều 44 (Tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng)

Có ý kiến đề nghị bổ sung quy định người quản lý kỹ thuật an ninh mạng tại cơ quan nhà nước, doanh nghiệp nhà nước phải có chứng chỉ hành nghề hoặc chứng nhận năng lực chuyên môn (01 ý kiến); bổ sung một khoản quy định về cá nhân, tổ chức hành nghề an ninh mạng phải tuân thủ quy tắc đạo đức, không lợi dụng kiến thức, quyền hạn để xâm nhập, thay đổi, công bố trái phép dữ liệu (01 ý kiến); bổ sung quy định về chính sách đặc thù của Nhà nước để thu hút các chuyên gia chất lượng cao về an ninh mạng tham gia nghiên cứu, đào tạo, chuyển giao công nghệ và ứng cứu sự cố an ninh mạng (01 ý kiến); quy định cụ thể về tiêu chí, tiêu chuẩn về phẩm chất, sức khỏe, trình độ để bảo đảm tính thống nhất trong áp dụng điều luật (01 ý kiến).

Tiếp thu ý kiến của Đại biểu Quốc hội, Chính phủ đã bổ sung nội dung "phát hiện tài năng trẻ về công nghệ thông tin để định hướng học tập, tuyển chọn, thu hút và sử dụng trong lĩnh vực an ninh mạng" vào khoản 2 Điều 32 về tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng.

Đối với các ý kiến khác, tiếp thu ý kiến của Đại biểu Quốc hội, Chính phủ sẽ quy định trong văn bản quy định chi tiết, hướng dẫn thi hành Luật.

- Điều 45 (Giáo dục bồi dưỡng kiến thức, nghiệp vụ an ninh mạng)

Có ý kiến đề nghị bổ sung nội dung giáo dục bồi dưỡng kiến thức an ninh mạng vào chương trình giáo dục quốc phòng, an ninh (02 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ sẽ tiếp tục rà soát, chỉnh lý nội dung vào khoản 1 Điều 33 về giáo dục bồi dưỡng kiến thức, nghiệp vụ an ninh mạng.

- Điều 46 (Phổ biến kiến thức về an ninh mạng)

Có ý kiến đề nghị bổ sung trách nhiệm Mặt trận Tổ quốc Việt Nam trong tuyên truyền, giáo dục, vận động toàn dân, toàn xã hội (01 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ sẽ tiếp tục nghiên cứu rà soát, chỉnh lý nội dung vào Điều 35 của dự thảo Luật.

- Điều 47 (Yêu cầu về kiến thức, kỹ năng bảo đảm an ninh mạng đối với người đứng đầu, lãnh đạo cơ quan, tổ chức, doanh nghiệp nhà nước, lực lượng chuyên trách bảo vệ an ninh mạng và cán bộ phụ trách bảo vệ an ninh mạng)

Có ý kiến đề nghị viết gọn tên điều là: "Yêu cầu về kiến thức, kỹ năng bảo đảm an ninh mạng" (không liệt kê đối tượng) (01 ý kiến).

Khoản 3: *Có ý kiến đề nghị giao Bộ Quốc phòng là cơ quan chủ trì phối hợp đào tạo, đánh giá, cấp chứng chỉ cho đối tượng thuộc phạm vi quản lý (01 ý kiến); cân nhắc bỏ đánh giá, cấp chứng chỉ hoặc quy định thuận lợi (thực hiện trên môi trường điện tử, tránh hình thức, tiết kiệm chi phí) (01 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ thiết kế lại điều khoản này thành Điều 34 về tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng, như sau:

"Điều 34. Tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng

1. Lực lượng bảo vệ an ninh mạng quy định tại khoản 1 và khoản 2 Điều 42 Luật này phải đáp ứng yêu cầu kiến thức, kỹ năng chuyên sâu về an ninh mạng.

2. Người trực tiếp quản trị, vận hành hệ thống thông tin cấp độ 3, 4 và 5 trong cơ quan, tổ chức, doanh nghiệp Nhà nước phải được tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng và được cấp giấy chứng nhận, trừ các cá nhân đã được đào tạo chuyên ngành an ninh mạng.

3. Bộ Công an chủ trì, phối hợp với các bộ, ngành liên quan tổ chức tập huấn về kiến thức, kỹ năng chuyên sâu về an ninh mạng.

4. Bộ Quốc phòng tổ chức tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng đối với đối tượng thuộc phạm vi quản lý.

5. Chính phủ quy định về chuẩn kiến thức, kỹ năng chuyên sâu về an ninh mạng; chương trình, nội dung tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng".

- Điều 48 (Kinh phí Bảo vệ an ninh mạng)

Một số ý kiến đề nghị không quy định cứng tối thiểu 10%, cần linh hoạt, phù hợp với thực tiễn (06 ý kiến). Có ý kiến đề nghị giải trình rõ và đánh giá tính khả thi của quy định này (02 ý kiến); đề nghị quy định nguyên tắc, giao Chính phủ linh hoạt theo điều kiện kinh tế - xã hội, yêu cầu nhiệm vụ (01 ý kiến); bổ sung cơ chế kiểm tra, giám sát việc bố trí và sử dụng kinh phí để bảo đảm tính thực thi của quy định (01 ý kiến).

Về ý kiến trên, Chính phủ báo cáo như sau: Mức 10% là mức thông lệ chung trên thế giới và cũng đã được nêu tại Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam. Nội dung này đã tiếp tục được nhắc lại tại

Quyết định số 964/QĐ-TTg ngày 10/8/2022 của Thủ tướng Chính phủ, phê duyệt Chiến lược an toàn, an ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030. Đồng thời cũng được thể hiện tại Công điện số 33/CĐ-TTg ngày 7/4/2024 của Thủ tướng Chính phủ yêu cầu các bộ, ngành, địa phương tăng cường bảo đảm an toàn thông tin mạng. Căn cứ Kết luận số 06-TB/CQTTBCĐ ngày 27/9/2025 của đồng chí Tổng Bí thư Tô Lâm, Trưởng Ban Chỉ đạo Trung ương về phát triển khoa học công nghệ, đổi mới sáng tạo và chuyển đổi số tại Phiên họp Thường trực Ban Chỉ đạo về công tác bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu, Chính phủ thiết kế lại điều khoản này thành Điều 40 (Kinh phí bảo vệ an ninh mạng), như sau:

"**Điều 40. Kinh phí bảo vệ an ninh mạng**

1. Cơ quan, tổ chức, doanh nghiệp nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội và các đơn vị sự nghiệp công lập do ngân sách nhà nước bảo đảm phải bố trí kinh phí bảo vệ an ninh mạng trong dự toán chi thực hiện nhiệm vụ chuyển đổi số, ứng dụng công nghệ thông tin hàng năm của cơ quan, tổ chức, đơn vị mình; bố trí tối thiểu 15% tổng kinh phí thực hiện chương trình, đề án, dự án đầu tư chuyển đổi số, ứng dụng công nghệ thông tin để bảo vệ an ninh mạng.

2. Cơ quan, tổ chức, đơn vị không thuộc quy định tại khoản 1 Điều này tự bảo đảm kinh phí bảo vệ an ninh mạng cho cơ quan, tổ chức, đơn vị mình".

3.7. Về trách nhiệm của cơ quan, tổ chức, cá nhân trong bảo vệ an ninh mạng (Chương VII)

- Ý kiến chung

+ Có ý kiến đề nghị làm rõ cơ chế phối hợp và phân định trách nhiệm trong việc xây dựng, thẩm định, công bố tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng giữa Bộ Công an (đầu mối quản lý nhà nước) và Bộ Khoa học và Công nghệ (chủ trì thẩm định, công bố tiêu chuẩn quốc gia) (01 ý kiến). Ý kiến khác đề nghị bỏ Điều này, gộp toàn bộ nội dung vào các điều về trách nhiệm của các bộ, ngành (02 ý kiến).

+ Ý kiến của Đại biểu Quốc hội tại Điều 50 (Trách nhiệm của Bộ Công an):

***Khoản 6:** Có ý kiến cho rằng cần có cơ chế phối hợp giữa Bộ Công an với Bộ Khoa học và Công nghệ để vừa bảo đảm được an ninh quốc gia, trật tự, an toàn xã hội, không kìm hãm sự phát triển kinh tế số, sử dụng nhân lực một cách hiệu quả, bảo đảm quyền riêng tư và bảo vệ dữ liệu cá nhân (01 ý kiến).*

***Khoản 8:** Có ý kiến đề nghị bổ sung dẫn chiếu quy định pháp luật về huy động, trưng dụng hoặc giao Chính phủ quy định chi tiết (01 ý kiến).*

+ Ý kiến của Đại biểu Quốc hội tại Điều 51 (Trách nhiệm của Bộ Quốc phòng):

Có ý kiến đề nghị giao Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng quản lý nhà nước về mật mã dân sự (07 ý kiến);); tổ chức bồi dưỡng nghiệp vụ an ninh mạng cho đối tượng thuộc phạm vi quản lý (01 ý kiến).

***Khoản 3:** Một số ý kiến đề nghị bổ sung quy định: "Bộ Quốc phòng chủ trì bảo vệ chủ quyền, phòng chống xâm phạm an ninh quốc gia, tội phạm mạng thuộc phạm vi quản lý" (03 ý kiến).*

Khoản 4: *Một số ý kiến đề nghị bổ sung quy định: "Bộ Quốc phòng có quyền yêu cầu doanh nghiệp viễn thông, Internet, chủ quản hệ thống gỡ bỏ nội dung vi phạm trên hệ thống do mình quản lý" (03 ý kiến).*

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ thiết kế lại các điều khoản này thành Điều 39 (mới) về trách nhiệm quản lý nhà nước về an ninh mạng, như sau:

"1. Chính phủ thống nhất quản lý nhà nước về an ninh mạng.

2. Bộ Công an là cơ quan đầu mối giúp Chính phủ thực hiện quản lý nhà nước về an ninh mạng; chịu trách nhiệm trước Chính phủ thực hiện các nội dung quản lý nhà nước về an ninh mạng sau đây, trừ nội dung quy định tại khoản 3 và khoản 4 Điều này:

a) 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;

b) Xây dựng, đề xuất chiến lược, chủ trương, chính sách, kế hoạch và phương án bảo vệ an ninh mạng; nghiên cứu, xây dựng, phát triển, sử dụng mật mã an ninh để bảo vệ an ninh dữ liệu thuộc phạm vi quản lý của Bộ Công an;

c) 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 13 của Luật này;

d) 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;

đ) 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;

e) Bảo đảm an ninh thông tin trên không gian mạng, an ninh dữ liệu; xây dựng cơ chế quản lý định danh địa chỉ IP; 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;

g) 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;

h) Trưng dụng chuyên gia, nhà khoa học, cán bộ chuyên sâu và hệ thống trong trường hợp khẩn cấp để bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội trên không gian mạng;

i) 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;

k) Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về an ninh mạng, an ninh thông tin, an ninh dữ liệu.

3. Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an ninh mạng thuộc phạm vi quản lý như sau:

a) 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;

b) 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;

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

d) 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;

đ) 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.

4. Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng thực hiện quản lý nhà nước về mật mã dân sự và an ninh mạng thuộc phạm vi quản lý theo quy định của pháp luật.

5. Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, trong phạm vi chức năng, nhiệm vụ, quyền hạn của mình, thực hiện công tác bảo vệ an ninh mạng; phối hợp với Bộ Công an thực hiện quản lý nhà nước về an ninh mạng.

6. Ủy ban nhân dân cấp tỉnh thực hiện công tác bảo vệ an ninh mạng tại địa phương; phối hợp với Bộ Công an thực hiện quản lý nhà nước về an ninh mạng".

- Điều 54 (Trách nhiệm chủ quản hệ thống thông tin)

Khoản 2: *Có ý kiến đề nghị bổ sung quy định: "trừ hệ thống thông tin cơ yếu", "chủ quản hệ thống thông tin thuộc Bộ Quốc phòng quản lý có trách nhiệm kết nối về hệ thống thông tin của Bộ Quốc phòng" vì hệ thống thông tin quốc phòng cần phải yêu cầu bí mật, tách biệt, tránh lộ lọt khi kết nối bên ngoài (02 ý kiến).*

Về ý kiến trên, Chính phủ báo cáo như sau: Trong bối cảnh chuyển đổi số diễn ra mạnh mẽ, hệ thống thông tin của các cơ quan, tổ chức, doanh nghiệp có sự kết nối, liên thông với nhau để trao đổi, chia sẻ thông tin, hình thành mạng lưới liên kết. Do vậy, để bảo đảm an ninh mạng thì tất cả các hệ thống thông tin liên quan đến dân sự thuộc cơ quan, tổ chức, doanh nghiệp cần kết nối về Trung tâm An ninh mạng Quốc gia để giám sát, kịp thời phát hiện, cảnh báo, hướng dẫn khắc phục, bảo vệ ngay từ khi có dấu hiệu bị tấn công, không để lan rộng, làm tê liệt cả hệ thống thông tin. Thực hiện quy định của Luật An ninh mạng năm 2018, Bộ Công an đã giám sát, cảnh báo, phát hiện nhiều lỗ hổng bảo mật, nhiều phần mềm gián điệp đối với các hệ thống thông tin. Vì vậy, Chính phủ đề nghị giữ nguyên nội dung dự thảo Luật.

- Điều 55 (Trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng)

+ Có ý kiến đề nghị bổ sung các quy định sau: "Trách nhiệm về phòng ngừa hành vi xâm phạm chủ quyền không gian mạng Việt Nam", "Doanh nghiệp cung cấp dịch vụ xuyên biên giới tại Việt Nam phải lưu giữ thông tin định danh điện tử của người dùng Việt Nam và chia sẻ với cơ quan quản lý khi có yêu cầu phục vụ điều tra" (01 ý kiến); bổ sung cơ chế cấp phép, chứng nhận năng lực cho doanh nghiệp cung cấp dịch vụ an ninh mạng; xây dựng cơ chế giám sát, xử lý vi phạm (01 ý kiến); bổ sung lộ trình áp dụng phân theo quy mô doanh nghiệp, chính sách hỗ trợ nhà nước (cung cấp bộ công cụ bảo mật cơ bản miễn phí, đào tạo miễn

phí) để không cản trở đổi mới sáng tạo (01 ý kiến); quy định rõ trách nhiệm doanh nghiệp mạng xã hội, đặc biệt nền tảng xuyên biên giới cần phải phối hợp cơ quan Việt Nam kiểm soát, gỡ bỏ nội dung độc hại, (01 ý kiến); bổ sung quy định chặt chẽ hơn về cơ chế phối hợp liên ngành về bảo vệ an ninh mạng, bảo đảm tính thống nhất trong chỉ đạo, phối hợp và huy động lực lượng khi xảy ra tấn công mạng diện rộng (01 ý kiến).

Về ý kiến bổ sung nội dung "Trách nhiệm về phòng ngừa hành vi xâm phạm chủ quyền không gian mạng Việt Nam", Chính phủ báo cáo như sau: Dự thảo Luật An ninh mạng 2025 được xây dựng trên cơ sở hợp nhất Luật An ninh mạng năm 2018 và Luật An toàn thông tin mạng năm 2015 theo nguyên tắc không làm thay đổi trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan. Do vậy, việc đề xuất bổ sung này sẽ làm phát sinh trách nhiệm, chi phí tuân thủ của các doanh nghiệp cung cấp dịch vụ trên không gian mạng.

Đối với ý kiến bổ sung cơ chế cấp phép, chứng nhận năng lực, Chính phủ thấy rằng việc kinh doanh dịch vụ an ninh mạng là ngành nghề kinh doanh có điều kiện theo pháp luật về đầu tư, các nội dung liên quan đến cấp phép, chứng nhận năng lực doanh nghiệp đã được quy định chi tiết tại Chương VI (Kinh doanh sản phẩm, dịch vụ an ninh mạng).

Đối với ý kiến áp dụng quy định phân theo quy mô doanh nghiệp, Chính phủ cho rằng đối với bất kỳ doanh nghiệp nào kể cả doanh nghiệp khởi nghiệp, doanh nghiệp siêu nhỏ khi bị sự cố gây mất an ninh mạng đều có nguy cơ ảnh hưởng đến an ninh mạng quốc gia.

Đối với các ý kiến khác, tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ đã rà soát để chỉnh lý, hoàn thiện trong dự thảo Luật.

+ Có ý kiến đề nghị bổ sung khoản 8 quy định đối với doanh nghiệp cung cấp dịch vụ viễn thông, Internet thuộc Bộ Quốc phòng phối hợp theo hướng dẫn lực lượng chuyên trách Bộ Quốc phòng thực hiện Điều 55, khoản 2 và khoản 3 Điều 31 để tránh tốn kém, phức tạp tái thiết hạ tầng lõi, bảo vệ bí mật quân sự, quốc phòng (01 ý kiến). Ý kiến khác đề nghị cân nhắc quy định này vì sẽ tạo gánh nặng về chi phí tuân thủ pháp luật của các doanh nghiệp vừa và nhỏ, doanh nghiệp khởi nghiệp (01 ý kiến).

Về ý kiến trên, Chính phủ cho rằng cơ bản nội dung dự thảo Luật An ninh mạng năm 2025 kế thừa các nguyên tắc, chính sách đã áp dụng trong thực tiễn của Luật An ninh mạng năm 2018 và Luật An toàn thông tin mạng năm 2015, không làm phát sinh chính sách mới, không làm thay đổi chức năng, nhiệm vụ của các bộ, ngành và bám sát quan điểm chỉ đạo tại Nghị quyết số 18 là "một việc chỉ giao cho một cơ quan chủ trì, chịu trách nhiệm chính".

Đối với ý kiến đề nghị cân nhắc quy định tại Điều này vì sẽ tạo gánh nặng về chi phí tuân thủ pháp luật của các doanh nghiệp vừa và nhỏ, doanh nghiệp khởi nghiệp, Chính phủ cho rằng đối với bất kỳ doanh nghiệp nào kể cả doanh nghiệp khởi nghiệp, doanh nghiệp siêu nhỏ khi bị sự cố gây mất an ninh mạng đều có nguy cơ ảnh hưởng đến an ninh mạng quốc gia.

*+ **Khoản 5:** Có ý kiến đề nghị quy định doanh nghiệp phải định danh IP người dùng để cung cấp khi cần trừ: doanh nghiệp phục vụ quốc phòng, an ninh sẽ do Chính phủ quy định riêng (03 ý kiến); đề nghị quy định "Cung cấp theo quy trình, thủ tục, thẩm quyền pháp luật quy định" để tránh lạm quyền, bảo vệ quyền riêng tư, quy định giới hạn trách nhiệm, thời hạn lưu trữ để giảm áp lực chi phí doanh nghiệp vừa và nhỏ (01 ý kiến).*

Đối với ý kiến đề nghị quy định doanh nghiệp phải định danh IP người dùng để cung cấp khi cần trừ: doanh nghiệp phục vụ quốc phòng, an ninh sẽ do Chính phủ quy định riêng, Chính phủ cho rằng: Dự thảo Luật An ninh mạng 2025 được xây dựng trên cơ sở hợp nhất Luật An ninh mạng năm 2018 và Luật An toàn thông tin mạng năm 2015 theo nguyên tắc không làm thay đổi chức năng, nhiệm vụ của các bộ, ngành, không tạo ra chính sách mới; bảo đảm thực hiện đúng tinh thần Nghị quyết số 18 là "một việc chỉ giao cho một cơ quan chủ trì, chịu trách nhiệm chính", bảo đảm phân công, phân cấp rõ ràng, tránh chồng chéo chức năng, nhiệm vụ, phạm vi quản lý. Đồng thời, đảm bảo kết nối, định danh đầy đủ, thống nhất, đồng bộ mới có khả năng bảo vệ tổng thể, ứng phó kịp thời, phục vụ nhiệm vụ bảo đảm an ninh mạng. Thực tế, các doanh nghiệp viễn thông, Internet và dịch vụ gia tăng trên không gian mạng đều hoạt động theo giấy phép và cơ chế quản lý thống nhất của cơ quan nhà nước có thẩm quyền. Do đó, quy định tại dự thảo đã phù hợp, bảo đảm nguyên tắc một đầu mối thống nhất về an ninh mạng, đúng định hướng theo Nghị quyết số 18.

Đối với ý kiến còn lại, tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ sẽ quy định cụ thể nội dung cung cấp theo quy trình, thủ tục, thẩm quyền tại văn bản quy định chi tiết, hướng dẫn thi hành Luật.

*+ **Khoản 6:** Có ý kiến đề nghị quy định doanh nghiệp thuộc Bộ Quốc phòng phối hợp theo yêu cầu lực lượng chuyên trách Bộ Quốc phòng để thiết lập kết nối, truyền tải dữ liệu, triển khai biện pháp bảo vệ (01 ý kiến); làm rõ "các điều kiện cần thiết khác", cần liệt kê cụ thể hoặc giao Chính phủ quy định chi tiết tiêu chí (01 ý kiến).*

Việc bổ sung thiết lập kết nối, truyền tải dữ liệu, triển khai biện pháp bảo vệ đặt nhiều trách nhiệm, tạo gánh nặng lớn về chi phí tuân thủ cho doanh nghiệp.

Đối với ý kiến còn lại, tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ sẽ quy định tại văn bản quy định chi tiết, hướng dẫn thi hành Luật.

- Điều 56 (Trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng)

+ Có ý kiến đề nghị bổ sung nghĩa vụ thông báo vi phạm; bổ sung quyền người dùng được tiếp cận, khiếu nại khi dữ liệu bị thu thập trái phép; cơ chế tiếp nhận, phản hồi báo cáo vi phạm (01 ý kiến); bổ sung cơ chế phối hợp với Mặt trận Tổ quốc và các tổ chức chính trị - xã hội; bổ sung chính sách đào tạo kỹ năng số cho cán bộ Mặt trận để nâng cao tuyên truyền, giám sát, phản biện tại cơ sở (01 ý kiến); đề nghị bổ sung một điều quy định về vai trò của Mặt trận Tổ quốc Việt Nam các cấp và các tổ chức thành viên (01 ý kiến).

Ý kiến tiếp thu, giải trình:

Nội dung về nghĩa vụ thông báo vi phạm bổ sung quyền người dùng được tiếp cận, khiếu nại khi dữ liệu bị thu thập trái phép; cơ chế tiếp nhận, phản hồi báo cáo vi phạm, báo cáo, khiếu nại vi phạm dữ liệu cá nhân không thuộc phạm vi điều chỉnh Luật An ninh mạng.

Các ý kiến khác, tiếp thu ý kiến của đại biểu Quốc hội, Chính phủ sẽ tiếp tục rà soát để chỉnh lý, hoàn thiện trong văn bản quy định chi tiết, hướng dẫn thi hành Luật.

+ ***Khoản 2:*** *Có ý kiến đề nghị nghiên cứu để bổ sung quy định, xử lý trong trường hợp tài khoản bị "hack" hay bị xâm nhập trái phép, dù đã áp dụng các biện pháp hợp lý (01 ý kiến).*

Ý kiến tiếp thu, giải trình:

Tiếp thu ý kiến Đại biểu Quốc hội, sẽ nghiên cứu bổ sung, chỉnh lý nội dung này thành khoản 2 Điều 42 về trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng, như sau:

"2. Có trách nhiệm bảo mật thông tin đăng ký, mở, quản lý, sử dụng tài khoản số của mình. Trường hợp sử dụng tài khoản số để thực hiện hành vi vi phạm pháp luật, tùy theo tính chất, mức độ của hành vi vi phạm, chủ tài khoản số, người sử dụng tài khoản số bị xử lý kỷ luật, xử phạt vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự; nếu gây thiệt hại đến lợi ích của Nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân thì phải bồi thường thiệt hại theo quy định pháp luật".

3.8. Một số nội dung khác

- Một số ý kiến đề nghị thống nhất sử dụng cụm từ "hệ thống thông tin cơ yếu" thay cho các cụm từ không đồng nhất như "hệ thống thông tin cơ yếu của Ban Cơ yếu Chính phủ,", "hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ" và "hệ thống thông tin cơ yếu do Ban Cơ yếu Chính phủ quản lý" tại các điều 15, 18, 22, 23, 24 và Điều 52 (04 ý kiến).

Về ý kiến trên, Chính phủ đã nghiên cứu, bổ sung, chỉnh lý nội hàm thuật ngữ hệ thống thông tin cơ yếu tại khoản 26 Điều 2 theo hướng "Hệ thống thông tin cơ yếu là hệ thống thông tin dùng mật mã cơ yếu để bảo vệ thông tin thuộc phạm vi bí mật nhà nước để phục vụ hoạt động chuyên môn nghiệp vụ cơ yếu do tổ chức cơ yếu trực tiếp quản lý, vận hành".

Bên cạnh đó, dự thảo Luật thống nhất sử dụng thuật ngữ "hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ" tại các điều khoản trên để phù hợp với quan điểm chỉ đạo của Chính phủ, Ủy ban Thường vụ Quốc hội trong quá trình xây dựng dự thảo.

- Về điều khoản thi hành, điều khoản chuyển tiếp: Có ý kiến đề nghị giao Chính phủ ban hành Nghị định hướng dẫn chuyển đổi thuật ngữ pháp lý trong thời hạn 12 tháng kể từ ngày Luật có hiệu lực nhằm bảo đảm tính đồng bộ, thống nhất của hệ thống pháp luật trong giai đoạn chuyển tiếp (01 ý kiến); cân nhắc các quy định tại khoản 2 và khoản 4 Điều 58 để bảo đảm tính khả thi, đề nghị nâng lên 24 tháng hoặc thực hiện theo lộ trình tùy quy mô hệ thống (03 ý kiến).

Về ý kiến kéo dài thời gian chuyển tiếp, Chính phủ cho rằng thời gian 24 tháng hoặc lộ trình theo quy mô hệ thống sẽ làm kéo dài trạng thái không đồng bộ, đặc biệt với hệ thống thông tin quan trọng về an ninh quốc gia, làm tăng rủi

ro phát sinh sự cố.

Đối với ý kiến còn lại, Tiếp thu ý kiến của Đại biểu Quốc hội, Chính phủ đã thiết kế lại nội dung này thành Điều 45 về điều khoản chuyển tiếp, như sau:

"**Điều 45. Điều khoản chuyển tiếp**

1. Hệ thống thông tin đã được xác định cấp độ theo quy định của Luật An toàn thông tin mạng số 86/2015/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 35/2018/QH14 thì tiếp tục được xác định cấp độ tương ứng theo quy định của Luật này; trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành phải bổ sung điều kiện, tiêu chuẩn, biện pháp bảo vệ an ninh mạng tương ứng với cấp độ theo quy định của Luật này; trường hợp điều chỉnh cấp độ hệ thống thông tin thực hiện theo quy định của Luật này.

2. Các loại giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng, mật mã dân sự theo quy định của Luật An toàn thông tin mạng số 86/2015/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 35/2018/QH14 đã được cấp trước ngày Luật này có hiệu lực thi hành có giá trị sử dụng đến hết thời hạn được ghi trên giấy phép; trường hợp cấp đổi sau ngày Luật này có hiệu lực thi hành thực hiện theo quy định của Luật này.

3. Các sản phẩm, dịch vụ, giải pháp, phương tiện kỹ thuật bảo đảm an toàn thông tin mạng theo quy định của Luật An toàn thông tin mạng số 86/2015/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 35/2018/QH14 đã được đưa vào sử dụng trước ngày Luật này có hiệu lực thi hành thì tiếp tục được sử dụng; trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành phải thay thế hoặc nâng cấp để đáp ứng các điều kiện an ninh mạng theo quy định của Luật này".

- Có ý kiến đề nghị bổ sung quy định cụ thể, chặt chẽ quản lý, bảo vệ dữ liệu từ nguồn (cơ quan nhà nước, doanh nghiệp); nghiên cứu bổ sung biện pháp ngăn chặn khai thác, đánh cắp, lạm dụng dữ liệu nhằm bảo vệ người dân, doanh nghiệp hiệu quả hơn (01 ý kiến); bổ sung cơ chế triển khai cụ thể việc ứng dụng công nghệ trong giám sát không gian mạng, tích hợp trí tuệ nhân tạo để phân tích hành vi, dự báo tấn công và cảnh báo tự động (02 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ sẽ tiếp tục nghiên cứu rà soát để chỉnh lý, hoàn thiện trong dự thảo Luật.

- Có ý kiến đề nghị nghiên cứu thành lập "Quỹ an ninh mạng quốc gia" để đầu tư nâng cấp hạ tầng kỹ thuật, đào tạo bồi dưỡng nguồn nhân lực chuyên sâu, hỗ trợ các doanh nghiệp vừa và nhỏ, triển khai nghiên cứu, hợp tác quốc tế (02 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ sẽ tiếp tục nghiên cứu rà soát để chỉnh lý, hoàn thiện trong dự thảo Luật.

- Có ý kiến đề nghị rà soát hoàn thiện dự thảo Luật trên cơ sở các nguyên tắc sau đây: Thống nhất trách nhiệm quản lý nhà nước; thận trọng với những chính sách mới; giao lực lượng chuyên trách bảo vệ an ninh mạng của Bộ Công an chịu trách nhiệm chủ trì bảo đảm an ninh mạng trong phạm vi cả nước, còn các lực lượng, cơ quan khác có trách nhiệm phối hợp (01 ý kiến); hạn chế tối đa quy định công khai trong Luật việc sử dụng lực lượng quân sự, quốc phòng để đấu tranh với hành vi gián điệp mạng, tấn công mạng, tác chiến mạng nhằm vào

Việt Nam (01 ý kiến). Có ý kiến đề nghị xây dựng cơ chế phối hợp liên ngành, Bộ Quốc phòng là cơ quan thường trực tác chiến mạng quốc gia, Bộ Công an chủ trì điều tra, xử lý tội phạm mạng (02 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ sẽ tiếp tục nghiên cứu rà soát để chỉnh lý, hoàn thiện trong dự thảo Luật.

Đối với ý kiến đề nghị xây dựng cơ chế phối hợp liên ngành giữa Bộ Quốc phòng và Bộ Công an, nội dung này đã được quy định tại Nghị định 03/2019/NĐ-CP ngày 05/9/2019 của Chính phủ về phối hợp giữa Bộ Quốc phòng và Bộ Công an trong thực hiện nhiệm vụ bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội, đấu tranh phòng, chống tội phạm và nhiệm vụ quốc phòng.

- Về kỹ thuật lập pháp: Có ý kiến đề nghị gộp khoản 3 và khoản 4 của Điều 36 (đều quy định về việc giao Chính phủ quy định chi tiết) thành một khoản; Sửa lỗi dẫn chiếu trong Khoản 1, Điều 47 vì nội dung về lực lượng bảo vệ an ninh mạng được quy định tại Điều 42 của dự thảo; tiếp tục rà soát, chỉnh sửa các lỗi kỹ thuật lập pháp khác (01 ý kiến).

Tiếp thu ý kiến Đại biểu Quốc hội, Chính phủ sẽ tiếp tục nghiên cứu rà soát để chỉnh lý, hoàn thiện trong dự thảo Luật.

II. ĐỐI VỚI Ý KIẾN CỦA ỦY BAN THƯỜNG VỤ QUỐC HỘI

1. Tiếp tục rà soát kỹ các ý kiến của Đại biểu Quốc hội, ý kiến của Ủy ban Thường vụ Quốc hội để tiếp thu, giải trình và chỉnh lý dự thảo Luật và hoàn thiện dự thảo Báo cáo tiếp thu, giải trình và chỉnh lý dự thảo Luật

- Đề nghị bổ sung phòng chống xâm hại đối với nhóm người yếu thế trên không gian mạng

Tiếp thu ý kiến nêu trên, Chính phủ đã bổ sung quy định một số nhóm yếu thế (trẻ em, người cao tuổi, người khó khăn về nhận thức) vào quy định tại khoản 1 Điều 35 dự thảo Luật.

- Đề nghị bổ sung giải trình thuyết phục hơn đối với kinh phí bảo vệ an ninh mạng, nhất là việc nâng mức tối thiểu từ 10% - 15% tổng kinh phí thực hiện chương trình, đề án, dự án đầu tư chuyển đổi số, ứng dụng công nghệ thông tin.

Tiếp thu ý kiến nêu trên, Chính phủ báo cáo như sau:

Về cơ sở chính trị, căn cứ Thông báo Kết luận số 06-TB/CQTTBCĐ ngày 27/9/2025 của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số đã xác định rõ: an ninh mạng, bảo mật thông tin và an toàn dữ liệu là cấu phần bắt buộc của mọi dự án công nghệ thông tin, đồng thời yêu cầu bố trí tối thiểu **15%** tổng kinh phí triển khai cho các sản phẩm, dịch vụ an ninh mạng nhằm bảo đảm hiệu quả, tránh lãng phí.

Về cơ sở thực tiễn:

Thứ nhất, quy định về tỷ lệ tối thiểu kinh phí bảo vệ an ninh mạng chỉ áp dụng đối với các chương trình, đề án, dự án chuyển đổi số và ứng dụng công nghệ thông tin của cơ quan nhà nước, tổ chức chính trị, tổ chức chính trị – xã hội, doanh nghiệp nhà nước và đơn vị sự nghiệp công lập sử dụng ngân sách nhà nước. Các cơ quan, tổ chức và đơn vị ngoài khu vực nhà nước tự bảo đảm kinh phí cho công tác bảo vệ an ninh mạng.

Thứ hai, xu hướng quốc tế cho thấy các quốc gia đều tăng mạnh đầu tư cho an ninh mạng, coi đây là ưu tiên hàng đầu trong bảo vệ hạ tầng số và dữ liệu quốc gia. Mặc dù nhiều nước chưa quy định tỷ lệ % cố định trong luật, mức chi tiêu thực tế và các khuyến nghị chính phủ đang hướng tới ngưỡng cao: Hàn Quốc đặt mục tiêu và khuyến khích dành 10 - 15% ngân sách công nghệ thông tin cho an ninh mạng trong các dự án chuyển đổi số trọng điểm (dù mức chi thực tế của khối doanh nghiệp hiện dao động khoảng 6% - 13%). Trung Quốc áp dụng các quy định nghiêm ngặt về bảo vệ hạ tầng thông tin trọng yếu (CII) với mức phạt cao, thúc đẩy đầu tư tuân thủ ước tính chiếm tỷ trọng lớn trong ngân sách công nghệ. Singapore, Estonia và Nhật Bản duy trì mức chi tiêu thực tế hoặc định hướng ngân sách ở mức 10 - 15% trong các dự án công nghệ quan trọng để đảm bảo vị thế quốc gia thông minh. Liên minh châu Âu cũng bố trí 7,5 tỷ EUR cho toàn bộ Chương trình Digital Europe, trong đó gói đầu tư chuyên biệt cho năng lực an ninh mạng và niềm tin số chiếm khoảng 1,6 tỷ EUR.

Thứ ba, mức 10% kinh phí dành cho bảo đảm an toàn, an ninh mạng vốn là mức thông lệ đã được Chính phủ quy định và áp dụng trong nhiều năm qua, thể hiện tại Chỉ thị số 14/CT-TTg ngày 07/6/2019, tiếp tục được nhấn mạnh trong Quyết định số 964/QĐ-TTg ngày 10/8/2022 phê duyệt Chiến lược an toàn, an ninh mạng quốc gia và Công điện số 33/CĐ-TTg ngày 7/4/2024 của Thủ tướng Chính phủ yêu cầu các bộ, ngành, địa phương tăng cường bảo đảm an toàn thông tin mạng. Tuy nhiên, trước yêu cầu mới của giai đoạn chuyển đổi số quốc gia, mức 10% không còn đáp ứng được yêu cầu bảo vệ hệ thống thông tin và dữ liệu quan trọng.

Từ các căn cứ nêu trên, Chính phủ nhận thấy việc nâng tỷ lệ tối thiểu kinh phí bảo vệ an ninh mạng lên 15% là phù hợp, có cơ sở chính trị, thực tiễn và kỹ thuật vững chắc; đồng thời đáp ứng yêu cầu tăng cường năng lực bảo vệ an ninh mạng quốc gia, bảo vệ dữ liệu và hạ tầng số trọng yếu, tạo động lực phát triển kinh tế số và thị trường an ninh mạng trong nước. Đây là khoản đầu tư cần thiết để bảo đảm tiến trình chuyển đổi số quốc gia được triển khai an toàn, hiệu quả và bền vững.

- Đề nghị bổ sung quy định về bảo vệ dữ liệu cá nhân trên không gian mạng và các Luật có liên quan.

Tiếp thu ý kiến nêu trên, Chính phủ đã nghiên cứu, đánh giá và bổ sung nội dung này vào khoản 3 Điều 4 dự thảo Luật về nguyên tắc bảo vệ an ninh mạng. Theo đó, dự thảo đã chỉnh lý theo hướng nhấn mạnh trách nhiệm bảo vệ dữ liệu cá nhân, bảo đảm tính thống nhất với Luật Bảo vệ dữ liệu cá nhân, thể hiện rõ tại quy định: "Kết hợp chặt chẽ giữa bảo vệ an ninh mạng với phát triển kinh tế - xã hội; bảo đảm quyền con người, quyền công dân; bảo vệ dữ liệu cá nhân; tạo điều kiện cho cơ quan, tổ chức, cá nhân hoạt động hợp pháp trên không gian mạng". Việc bổ sung này vừa đáp ứng yêu cầu của Ủy ban Thường vụ Quốc hội, vừa bảo đảm tính thống nhất của hệ thống pháp luật và phù hợp với định hướng hoàn thiện thể chế về bảo vệ dữ liệu cá nhân trong bối cảnh chuyển đổi số quốc gia.

2. Rà soát, bổ sung các quy định có liên quan vào dự thảo Luật để tạo sự thống nhất, đồng bộ với Luật Dữ liệu, Luật Bảo vệ dữ liệu cá nhân, dự thảo Luật Trí tuệ nhân tạo, dự thảo Luật Chuyển đổi số và các Luật khác về khoa học, công nghệ, đổi mới sáng tạo phục vụ hiệu quả quá trình phát triển kinh tế - xã hội

Về ý kiến trên, Chính phủ đã tiến hành rà soát toàn diện, nghiên cứu các quy định của dự thảo Luật An ninh mạng đảm bảo thống nhất, đồng bộ với hệ thống pháp luật hiện hành và các dự thảo Luật đang được xây dựng (bao gồm: Luật Dữ liệu, Luật Bảo vệ dữ liệu cá nhân, dự thảo Luật Trí tuệ nhân tạo, dự thảo Luật Chuyển đổi số, dự thảo Luật Thương mại điện tử, dự thảo Luật Công nghệ cao (sửa đổi) và dự thảo Luật Bảo vệ bí mật nhà nước). Dự thảo Luật An ninh mạng phù hợp với xu thế phát triển của khoa học - công nghệ, hỗ trợ hiệu quả tiến trình chuyển đổi số và phát triển kinh tế - xã hội của đất nước.

- Tiếp tục rà soát dự thảo Luật để bảo đảm sự thống nhất về nội dung và kỹ thuật văn bản; bảo đảm tính thuyết phục của Báo cáo tiếp thu, giải trình và chỉnh lý dự thảo Luật để trình Quốc hội xem xét, thông qua.

Tiếp thu ý kiến nêu trên, Chính phủ đã phối hợp với Thường trực Ủy ban Quốc phòng, An ninh và Đối ngoại cùng các cơ quan, tổ chức có liên quan rà soát toàn bộ ý kiến của các đại biểu Quốc hội tại phiên thảo luận tổ và thảo luận tại hội trường; đồng thời bổ sung đầy đủ các luận điểm và cơ sở để giải trình từng ý kiến. Kết quả rà soát dự thảo Luật đã đảm bảo sự thống nhất về nội dung và kỹ thuật văn bản.

- Đề nghị kịp thời chuẩn bị văn bản quy định chi tiết để bảo đảm hiệu lực thi hành sau khi ban hành Luật.

Tiếp thu ý kiến nêu trên, Chính phủ cơ bản xác lập được khung bố cục và dự thảo của 06 văn bản hướng dẫn thi hành Luật An ninh mạng, cụ thể là: (1) Nghị định quy định chi tiết một số điều của Luật An ninh mạng; (2) Nghị định quy định về bảo vệ an ninh mạng với hệ thống thông tin theo cấp độ; (3) Nghị định về ngăn chặn xung đột thông tin trên mạng; (4) Nghị định quy định điều kiện kinh doanh sản phẩm, dịch vụ an ninh mạng; (5) Nghị định quy định về biện pháp bảo vệ an ninh mạng; (6) Nghị định quy định xử phạt vi phạm hành chính về an ninh mạng và bảo vệ dữ liệu cá nhân. Chính phủ sẽ ban hành các văn bản hướng dẫn trên để kịp thời với hiệu lực thi hành Luật.

3. Chính phủ thống nhất các nội dung cụ thể về phạm vi, thẩm quyền, nhiệm vụ, trách nhiệm của Bộ Công an, Bộ Quốc phòng và Ban Cơ yếu Chính phủ trong bảo đảm an ninh mạng theo đúng tinh thần Nghị quyết 66/NQ-TW ngày 30/4/2025 của Bộ Chính trị về đổi mới công tác xây dựng và thi hành pháp luật đáp ứng yêu cầu phát triển đất nước trong kỷ nguyên mới.

- Đề nghị nghiên cứu, rà soát, bỏ các quy định cụ thể về trách nhiệm quản lý nhà nước tại 11 điều (bao gồm Điều 7, 13, 16, 19, 20, 21, 22, 29, 36, 42, 43) để quy định nguyên tắc chung ở Điều 41 về quản lý nhà nước và giao Chính phủ quy định chi tiết bảo đảm thống nhất với Luật Tổ chức Chính phủ.

Với ý kiến nêu trên, Chính phủ báo cáo như sau:

Thứ nhất, Luật An ninh mạng năm 2018 quy định cụ thể trách nhiệm của Bộ, ngành, địa phương tại 05 Điều[1] và nhiều điều khoản quy định các nội dung thuộc thẩm quyền của Chính phủ. Quán triệt tinh thần Nghị quyết số 66-NQ/TW ngày 30/4/2025 của Bộ Chính trị về đổi mới công tác xây dựng và thi hành pháp luật đáp ứng yêu cầu phát triển đất nước trong kỷ nguyên mới, dự thảo Luật An ninh mạng hiện tại đã lược bỏ toàn bộ các điều, khoản nêu trên, đồng thời rà soát những nội dung thuộc thẩm quyền của Chính phủ thì chỉ quy định mang tính nguyên tắc và giao Chính phủ quy định chi tiết tại 12 Điều[2].

Dự thảo Luật.tiếp tục quy định trách nhiệm quản lý nhà nước tại 11 Điều là cần thiết nhằm bảo đảm "rõ người, rõ việc, rõ trách nhiệm, rõ thẩm quyền". Đặc biệt, các điều này có chứa nội dung liên quan đến việc giới hạn quyền con người, quyền công dân (như quy định về phòng, chống gián điệp mạng; phòng, chống tấn công mạng; phòng, chống khủng bố mạng; phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng...), nên phải quy định ngay trong dự thảo Luật để phù hợp với quy định của Hiến pháp.

Thứ hai, các nội dung quy định tại 11 điều nêu trên là kế thừa Luật An ninh mạng năm 2018 và Luật An toàn thông tin mạng năm 2015, sau khi rà soát, nghiên cứu tiếp thu ý kiến của các đại biểu Quốc hội tại Tổ và Hội trường, hầu hết không đề cập đến các quy định cụ thể về trách nhiệm quản lý nhà nước tại 11 điều, còn lại các ý kiến về các nội dung khác, Chính phủ đã chỉ đạo Cơ quan soạn thảo tiếp thu tối đa, để hoàn thiện dự thảo Luật. Chính phủ nhận thấy những quy định tại 11 điều nêu trên không làm thay đổi chức năng, nhiệm vụ của các bộ, ngành, không tạo ra chính sách mới. Bên cạnh đó, thực tiễn thi hành đã chứng minh tính hiệu quả, ổn định và khả thi, không gây khó khăn, vướng mắc. Nếu chuyển sang chỉ quy định nguyên tắc, sẽ gây khó khăn trong triển khai, phát sinh yêu cầu ban hành nhiều văn bản hướng dẫn, tạo khoảng trống pháp lý trong giai đoạn chuyển tiếp.

Thứ ba, dự thảo Luật đã tham khảo kỹ thuật lập pháp của các luật hiện hành, đặc biệt là các luật được thông qua tại Kỳ họp thứ 9, Quốc hội khóa XV, trong đó vẫn duy trì các điều khoản quy định trách nhiệm Bộ, ngành theo từng nhiệm vụ quản lý nhà nước (như Luật Tham gia lực lượng gìn giữ hòa bình của Liên hợp quốc năm 2025; Luật Bảo vệ dữ liệu cá nhân năm 2025; Luật Công nghiệp công

---

[1] Điều 36 (Trách nhiệm của Bộ Công an); Điều 37 (Trách nhiệm của Bộ Quốc phòng); Điều 38 (Trách nhiệm của Bộ Thông tin và Truyền thông); Điều 39 (Trách nhiệm của Ban Cơ yếu Chính phủ) và Điều 40 (Trách nhiệm của Bộ, ngành, Ủy ban nhân dân tỉnh).

[2] Điều 8 (Phân loại cấp độ hệ thống thông tin); Điều 9 (Hệ thống thông tin quan trọng về an ninh quốc gia); Điều 10 (Nhiệm vụ, biện pháp bảo vệ an ninh mạng); Điều 12 (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 14 (Phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng); Điều 22 (Ngăn chặn xung đột thông tin trên không gian mạng); Điều 25 (Bảo đảm an ninh thông tin mạng); Điều 26 (Bảo đảm an ninh dữ liệu); Điều 28 (Sản phẩm, dịch vụ an ninh mạng); Điều 29 (Kinh doanh sản phẩm, dịch vụ an ninh mạng); Điều 30 (Lực lượng bảo vệ an ninh mạng); Điều 34 (Tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng).

nghệ số năm 2025; Luật Đường sắt năm 2025...). Do đó, việc tiếp tục quy định trách nhiệm tại 11 điều của Dự thảo Luật An ninh mạng hoàn toàn phù hợp với kỹ thuật lập pháp, bảo đảm rõ ràng, minh bạch, không mâu thuẫn với Luật Tổ chức Chính phủ.

Thứ tư, quy định rõ trách nhiệm của từng bộ, ngành trong một số điều luật là cần thiết để xác định chính xác cơ quan chủ trì, cơ quan phối hợp, đặc biệt đối với hoạt động bảo đảm an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia. Nếu không quy định rõ, sẽ dẫn đến lúng túng, chồng chéo hoặc bỏ sót trách nhiệm trong các trường hợp khẩn cấp, như: tình huống nguy hiểm về an ninh mạng, tấn công mạng, khủng bố mạng, ứng cứu, khắc phục sự cố an ninh mạng...

Thứ năm, đặc thù lĩnh vực an ninh mạng đòi hỏi phải phản ứng nhanh và cơ chế phối hợp liên ngành theo thời gian thực. Các điều khoản cụ thể, đặc biệt là Điều 19 (Phòng, chống khủng bố mạng) và Điều 20 (Phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng)..., đóng vai trò như "kịch bản pháp lý" để kích hoạt ngay các biện pháp ứng phó khi xảy ra tấn công mạng. Nếu chỉ quy định nguyên tắc chung, các cơ quan phải xác định lại phạm vi trách nhiệm, dẫn đến chậm trễ trong ứng cứu, gia tăng rủi ro thiệt hại cho hệ thống thông tin quan trọng, an ninh quốc gia, trật tự, an toàn xã hội.

Thứ sáu, việc quy định chi tiết trách nhiệm của từng cơ quan còn nhằm bảo đảm quyền và lợi ích hợp pháp của công dân trong bối cảnh tội phạm mạng, xâm phạm dữ liệu cá nhân, lừa đảo trực tuyến, xâm hại trẻ em gia tăng. Các điều như Điều 14 (Phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng) và Điều 16 (Phòng, chống xâm hại trẻ em trên không gian mạng) chỉ có thể phát huy tác dụng khi gắn trách nhiệm cụ thể của cơ quan chủ trì và cơ quan phối hợp, giúp người dân biết rõ nơi tiếp nhận, xử lý vụ việc, từ đó bảo đảm hiệu quả thực thi quyền.

Từ các căn cứ nêu trên, Chính phủ nhận thấy việc quy định cụ thể trách nhiệm quản lý nhà nước tại 11 điều của Dự thảo Luật là cần thiết, đúng thẩm quyền của Quốc hội, phù hợp Hiến pháp, bảo đảm tính minh bạch, khả thi và hiệu lực thi hành, đồng thời bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng.

- Đề nghị bổ sung giải trình thuyết phục hơn, bám sát chức năng, nhiệm vụ của các cơ quan được pháp luật quy định và bảo đảm nguyên tắc không làm thay đổi chức năng, nhiệm vụ của các bộ, ngành, không tạo ra chính sách mới và trên cơ sở kế thừa, hợp nhất Luật An ninh mạng năm 2018 và Luật An toàn thông tin mạng năm 2015, bảo đảm quan điểm chỉ đạo, nhiệm vụ, giải pháp mà Nghị quyết số 18-NQ/TW ngày 25/10/2017 của Ban Chấp hành Trung ương về một số vấn đề tiếp tục đổi mới, sắp xếp tổ chức bộ máy của hệ thống chính trị tinh gọn, hoạt động hiệu lực, hiệu quả. Những vấn đề phát sinh chính sách mới, thay đổi chức năng, nhiệm vụ của các bộ, ngành, cơ quan, tổ chức, cá nhân

cần nghiên cứu, đánh giá tác động kỹ lưỡng và đề xuất sửa đổi, bổ sung vào thời điểm thích hợp.

Tiếp thu ý kiến của Thường vụ Quốc hội, Chính phủ đã rà soát toàn diện dự thảo Luật và xin báo cáo, làm rõ như sau:

Thứ nhất, dự thảo Luật được xây dựng bám sát chức năng, nhiệm vụ của các cơ quan theo quy định pháp luật hiện hành, bảo đảm nguyên tắc không làm thay đổi chức năng và không tạo ra thẩm quyền mới. Dự thảo Luật An ninh mạng năm 2025 kế thừa mô hình phân công trách nhiệm đã được xác lập tại Luật An ninh mạng năm 2018 và Luật An toàn thông tin mạng năm 2015, đồng thời cập nhật phù hợp với việc sắp xếp lại tổ chức bộ máy, trong đó toàn bộ chức năng quản lý nhà nước về an toàn thông tin mạng đã được chuyển giao thống nhất về Bộ Công an. Các quy định về trách nhiệm của Bộ Công an, Bộ Quốc phòng và các bộ, ngành, địa phương được giữ nguyên về bản chất, chỉ làm rõ hơn để tránh chồng chéo, bảo đảm phù hợp chức năng của từng cơ quan theo luật định. Dự thảo không làm phát sinh thay đổi chức năng của các bộ, ngành và không hình thành thêm tổ chức mới.

Thứ hai, dự thảo Luật không đặt ra chính sách mới mà chỉ hoàn thiện các biện pháp bảo vệ an ninh mạng cho phù hợp với tình hình hiện nay. Các nội dung sửa đổi, bổ sung tập trung vào việc chuẩn hóa, hiện đại hóa biện pháp giám sát, kiểm tra, ứng phó sự cố; làm rõ trách nhiệm bảo vệ dữ liệu cá nhân, an ninh dữ liệu; và tăng cường cơ chế phối hợp giữa các cơ quan trong bối cảnh tội phạm mạng, lừa đảo trực tuyến gia tăng, diễn biến phức tạp. Những nội dung này không mở rộng thẩm quyền, không bổ sung nghĩa vụ mới vượt quá khuôn khổ pháp luật hiện hành, mà chỉ hướng tới nâng cao hiệu quả thực thi.

Thứ ba, dự thảo Luật bảo đảm giữ nguyên mô hình tổ chức bộ máy, không phát sinh thêm đầu mối quản lý, phù hợp tinh thần Nghị quyết 18-NQ/TW về tinh gọn, hiệu lực, hiệu quả. Cách tiếp cận này duy trì sự tinh gọn của bộ máy, không tạo chồng chéo chức năng, không phát sinh tổ chức mới. Những vấn đề mới làm phát sinh chính sách mới tiếp tục nghiên cứu, đánh giá kỹ lưỡng và đề xuất trong các lần sửa đổi tiếp theo. Dự thảo Luật chỉ hoàn thiện các nội dung đang triển khai hiệu quả; không mở rộng thẩm quyền hoặc bổ sung nhiệm vụ mới nếu chưa có đánh giá tác động đầy đủ. Những vấn đề có ảnh hưởng lớn đến tổ chức bộ máy hoặc chức năng cơ quan sẽ được Chính phủ tiếp tục nghiên cứu theo đúng quy trình xây dựng pháp luật.

Như vậy, dự thảo Luật An ninh mạng năm 2025 được xây dựng trên nguyên tắc tiếp thu nghiêm túc ý kiến của Thường vụ Quốc hội, bảo đảm không làm thay đổi chức năng, nhiệm vụ của các bộ, ngành; không tạo chính sách mới; kế thừa và hợp nhất các luật hiện hành; phù hợp tinh thần Nghị quyết 18-NQ/TW về tinh gọn bộ máy. Các nội dung chỉnh lý bảo đảm tính khả thi, phù hợp thực tiễn và góp phần hoàn thiện khung pháp lý bảo vệ an ninh mạng quốc gia trong bối cảnh chuyển đổi số toàn diện.

Trên đây là nội dung Báo cáo tiếp thu, giải trình ý kiến về dự án Luật An ninh mạng, Chính phủ trình Quốc hội xem xét, thông qua./.

Nơi nhận:
- Như trên;
- Thủ tướng Chính phủ;
- Các Phó Thủ tướng Chính phủ;
- Ủy ban Thường vụ Quốc hội;
- Ủy ban Quốc phòng, An ninh và Đối ngoại của Quốc hội;
- Văn phòng Quốc hội;
- Bộ Công an;
- Bộ Quốc phòng;
- Bộ Tư pháp;
- Tòa án nhân dân tối cao;
- Viện kiểm sát nhân dân tối cao;
- Văn phòng Chính phủ: BTCN, các PCN, trợ lý TTg, TGĐ cổng TTĐT;
Các vụ, cục: NC, QHĐP, PL, TH;
- Lưu: VT, KSTT! C (02).24

TM. CHÍNH PHỦ
TUQ. THỦ TƯỚNG
BỘ TRƯỞNG BỘ CÔNG AN

Đại tướng Lương Tam Quang

QUỐC HỘI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Luật số: /2025/QH15	**Độc lập - Tự do - Hạnh phúc**

LUẬT
AN NINH MẠNG

Căn cứ Hiến pháp nước Cộng hòa xã hội chủ nghĩa Việt Nam đã được sửa đổi, bổ sung một số điều theo Nghị quyết số 203/2025/QH15;

Quốc hội ban hành Luật An ninh mạng.

Chương I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Luật này quy định về an ninh mạng, bảo vệ an ninh mạng; quyền, nghĩa vụ, trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan.

2. Luật này áp dụng đối với:

a) Cơ quan, tổ chức, cá nhân Việt Nam;

b) Cơ quan, tổ chức, cá nhân nước ngoài tại Việt Nam và người gốc Việt Nam chưa xác định được quốc tịch đang sinh sống tại Việt Nam đã được cấp giấy chứng nhận căn cước;

c) Cơ quan, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động bảo vệ an ninh mạng, kinh doanh sản phẩm, dịch vụ an ninh mạng tại Việt Nam.

Điều 2. Giải thích từ ngữ

Trong Luật này, các từ ngữ dưới đây được hiểu như sau:

1. *An ninh mạng* là sự ổn định, an ninh, an toàn của không gian mạng; bảo vệ hệ thống thông tin và bảo đảm thông tin, dữ liệu, 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. *An ninh thông tin mạng* là sự bảo đảm tính nguyên vẹn, tính bảo mật, tính khả dụng của thông tin trên không gian mạng, tránh bị truy cập, sử dụng, tiết lộ, sửa đổi trái phép, phá hoại hoặc hành vi khác đe dọa hoặc gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội.

3. *An ninh dữ liệu* là sự bảo đảm chất lượng dữ liệu và các hoạt động xử lý, sử dụng dữ liệu trên không gian mạng phục vụ phát triển kinh tế - xã hội, chuyển đổi số quốc gia, tránh bị truy cập, sử dụng, tiết lộ, sửa đổi trái phép, phá hoại hoặc hành vi khác đe dọa hoặc gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội.

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

5. *Không gian mạng* là môi trường được hình thành bởi hệ thống 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.

6. *Không gian mạng quốc gia* là phần không gian mạng thuộc chủ quyền, quyền tài phán và quyền kiểm soát của Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam.

7. *Hệ thống thông tin* là tập hợp phần cứng, phần mềm và dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên không gian mạng.

8. *Chủ quản hệ thống thông tin* là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

9. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hoặc toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

10. *Phần cứng độc hại* là các bộ phận vật lý được thiết kế có chủ đích hoặc được gắn thêm ngoài cấu thành của phần cứng tiêu chuẩn nhằm thu thập thông tin, dữ liệu trái phép hoặc can thiệp, gây ngừng trệ, tê liệt, phá hoại hệ thống máy tính, hệ thống thông tin.

11. *Nhật ký hệ thống* là tập hợp các bản ghi phản ánh thời gian, người dùng, hoạt động, trạng thái của hệ thống phục vụ cho quản lý, giám sát và bảo mật hệ thống.

12. *Tội phạm mạng* là hành vi nguy hiểm cho xã hội được quy định trong Bộ luật Hình sự, do cá nhân hoặc tổ chức thực hiện trên không gian mạng bằng việc sử dụng công nghệ thông tin hoặc phương tiện điện tử.

13. *Tấn công mạng* là hành vi thực hiện trên không gian mạng bằng việc sử dụng công nghệ thông tin hoặc phương tiện điện tử để chiếm đoạt thông tin, gây rối loạn, gián đoạn, tê liệt hoạt động, phá hoại hoặc kiểm soát hệ thống 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.

14. *Khủng bố mạng* là hành vi thực hiện trên không gian mạng bằng việc sử dụng công nghệ thông tin hoặc phương tiện điện tử nhằm gây hoảng sợ trong công chúng hoặc làm mất ổn định chính trị.

15. *Gián điệp mạng* là hành vi thực hiện trên không gian mạng bằng việc sử dụng công nghệ thông tin, phương tiện điện tử bí mật xâm nhập để chiếm đoạt, thu thập, sao chép thông tin thuộc phạm vi bí mật nhà nước, dữ liệu quan trọng của cơ quan, tổ chức, cá nhân nhằm mục đích gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội.

16. *Nguy cơ đe dọa an ninh mạng* là trạng thái không gian mạng xuất hiện dấu hiệu đe dọa xâm phạm an ninh quốc gia, gây tổn hại nghiêm trọng đến trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

17. *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.

18. *Tình huống nguy hiểm về an ninh mạng* là trạng thái hoặc diễn biến trên không gian mạng khi có yếu tố tấn công, xâm nhập, kích động, làm lộ, mất thông tin hoặc hành vi khác đe dọa xâm phạm nghiêm trọng đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

19. *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.

20. *Mật mã dân sự* là kỹ thuật mật mã và sản phẩm mật mã được sử dụng để bảo mật hoặc xác thực đối với thông tin không thuộc phạm vi bí mật nhà nước nhằm bảo đảm an ninh thông tin cho cơ quan, tổ chức, cá nhân.

21. *Sản phẩm an ninh mạng* là phần cứng, phần mềm có chức năng bảo vệ an ninh mạng, an ninh thông tin, an ninh dữ liệu, thông tin, hệ thống thông tin, cơ sở hạ tầng công nghệ thông tin.

22. *Dịch vụ an ninh mạng* là dịch vụ được cung cấp để bảo vệ an ninh mạng, an ninh thông tin, an ninh dữ liệu, thông tin, hệ thống thông tin, cơ sở hạ tầng công nghệ thông tin.

23. *Hệ thống thông tin cơ yếu* là hệ thống thông tin dùng mật mã cơ yếu để bảo vệ thông tin thuộc phạm vi bí mật nhà nước để phục vụ hoạt động chuyên môn nghiệp vụ cơ yếu do tổ chức cơ yếu trực tiếp quản lý, vận hành.

Điều 3. Chính sách của Nhà nước về an ninh mạng

1. 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.

2. Ưu tiên bảo vệ an ninh mạng trong các lĩnh vực quốc phòng, an ninh, cơ yếu, phát triển kinh tế - xã hội, khoa học, công nghệ và đối ngoại.

3. Ưu tiên bố trí nguồn lực xây dựng, phát triển lực lượng chuyên trách bảo vệ an ninh mạng, bảo đảm nguồn nhân lực chất lượng cao phục vụ 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 hoạt động nghiên cứu, phát triển khoa học, công nghệ hiện đại phục vụ bảo vệ an ninh mạng; có cơ chế đặc thù, chính sách ưu đãi để huy động, thu hút, đào tạo và sử dụng nhân tài trong lĩnh vực an ninh mạng.

4. Đẩy mạnh liên kết, hợp tác công - tư trong bảo vệ an ninh mạng; khuyến khích, tạo điều kiện để cơ quan, 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; sử dụng sản phẩm, dịch vụ an ninh mạng của Việt Nam.

5. Mở rộng hợp tác quốc tế về an ninh mạng để tăng cường khả năng bảo vệ an ninh mạng; phòng, chống tội phạm mạng và các mối đe dọa về an ninh mạng xuyên quốc gia; tiếp thu công nghệ hiện đại nhằm nâng cao năng lực tự chủ an ninh mạng quốc gia.

Điều 4. Nguyên tắc bảo vệ an ninh mạng

1. Tuân thủ Hiến pháp và pháp luật; bảo đảm an ninh, chủ quyền và lợi ích quốc gia trên không gian mạng.

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 bảo vệ an ninh mạng với phát triển kinh tế - xã hội, bảo đảm quyền con người, quyền công dân, bảo vệ dữ liệu cá nhân, tạo điều kiện cho cơ quan, tổ chức, cá nhân hoạt động hợp pháp trên không gian mạng.

4. Áp dụng các biện pháp để bảo vệ không gian mạng quốc gia; chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh làm thất bại mọi hoạt động 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; xử lý kịp thời, nghiêm minh các hành vi vi phạm pháp luật về an ninh mạng.

5. Triển khai hoạt động bảo vệ an ninh mạng thường xuyên, liên tục đối với cơ sở hạ tầng không gian mạng quốc gia; chủ động áp dụng các biện pháp bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia.

Điều 5. Biện pháp bảo vệ an ninh mạng

1. Biện pháp bảo vệ an ninh mạng bao gồm:

a) Thẩm định an ninh mạng;

b) Đánh giá điều kiện an ninh mạng;

c) Kiểm tra an ninh mạng;

d) Giám sát an ninh mạng;

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

e) Đấu tranh bảo vệ an ninh mạng;

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

h) Sử dụng giải pháp kỹ thuật để bảo vệ an ninh dữ liệu, an ninh thông tin, hệ thống thông tin; ngăn chặn thông tin vi phạm pháp luật;

i) 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;

k) Yêu cầu xóa bỏ, truy cập xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật, tin giả 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;

l) 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;

m) 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 tên miền theo quy định của pháp luật;

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

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

2. Chính phủ quy định chi tiết nội dung, trình tự, thủ tục, thẩm quyền áp dụng biện pháp bảo vệ an ninh mạng, trừ biện pháp quy định tại điểm n và điểm o khoản 1 Điều này.

Điều 6. Hợp tác quốc tế về an ninh mạng

1. Hợp tác quốc tế về an ninh mạng được thực hiện trên cơ sở tôn trọng độc lập, chủ quyền, toàn vẹn lãnh thổ, không can thiệp vào công việc nội bộ của nhau, bình đẳng, cùng có lợi và tuân thủ Hiến pháp, pháp luật Việt Nam, điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên.

2. Nội dung hợp tác quốc tế về an ninh mạng bao gồm:

a) Chia sẻ thông tin, dữ liệu và cảnh báo sớm về nguy cơ, sự cố, tấn công mạng ảnh hưởng đến an ninh mạng;

b) Xây dựng khuôn khổ pháp lý, chính sách và cơ chế hợp tác, phối hợp trong bảo vệ an ninh mạng; đàm phán, ký kết, tham gia thực hiện điều ước quốc tế, thỏa thuận quốc tế về an ninh mạng;

c) Đào tạo, tư vấn, chia sẻ kinh nghiệm và nâng cao năng lực chuyên môn, kỹ thuật trong lĩnh vực an ninh mạng;

d) Phòng, chống tội phạm mạng, tội phạm sử dụng công nghệ cao; phối hợp điều tra, xử lý vi phạm pháp luật, tội phạm mạng và tội phạm sử dụng công nghệ cao;

đ) Nghiên cứu, phát triển, chuyển giao công nghệ, sản phẩm, giải pháp kỹ thuật phục vụ công tác bảo vệ an ninh mạng;

e) Tổ chức hội nghị, hội thảo quốc tế và triển khai các chương trình, dự án hợp tác quốc tế về an ninh mạng;

g) Hoạt động hợp tác quốc tế khác về an ninh mạng.

3. Trách nhiệm hợp tác quốc tế về an ninh mạng được quy định như sau:

a) Bộ Công an chịu trách nhiệm trước Chính phủ chủ trì, phối hợp thực hiện hợp tác quốc tế về an ninh mạng;

b) Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện hợp tác quốc tế về an ninh mạng trong phạm vi quản lý;

c) 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;

d) Trường hợp hợp tác quốc tế về an ninh mạng có liên quan đến trách nhiệm của nhiều Bộ, ngành do Thủ tướng Chính phủ quyết định;

đ) 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.

Điều 7. Các hành vi bị nghiêm cấm về an ninh mạng

1. Đăng tải, phát tán thông tin có nội dung sau trên không gian mạng:

a) Tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm: tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân; chiến tranh tâm lý, kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước; xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc;

b) 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;

c) Bịa đặt, vu khống, thông tin sai sự thật, xâm phạm nhân phẩm, danh dự, uy tín của người khác hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác;

d) 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 bình thường 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; thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá khác; thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, kinh doanh đa cấp, chứng khoán.

2. Thực hiện hành vi sau trên không gian mạng:

a) 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;

b) Kích động, kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân; kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự;

c) Chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật Nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời

sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; cố ý nghe lén, ghi âm, ghi hình trái phép các cuộc đàm thoại trên không gian mạng; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc;

d) Hoạt động mại dâm, tệ nạn xã hội, mua bán người, các bộ phận cơ thể người; tuyên truyền văn hóa phẩm dâm ô, đồi trụy; kích động, cổ xúy bạo lực, lối sống trụy lạc, lệch chuẩn, phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng;

đ) Lừa đảo chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua mạng Internet; trộm cắp cước viễn thông quốc tế trên nền Internet; tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật; vi phạm bản quyền và sở hữu trí tuệ trên không gian mạng;

e) 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, tài sản mã hóa, tài sản số của người khác; phát hành, cung cấp, sử dụng trái phép các phương tiện thanh toán; giả mạo giấy tờ của cơ quan, tổ chức;

g) Sử dụng trí tuệ nhân tạo hoặc công nghệ mới để giả mạo video, hình ảnh, giọng nói của người khác trái quy định của pháp luật; tạo lập, đăng tải, phát tán thông tin quy định tại khoản 1 Điều này;

h) Thu thập, sử dụng, phát tán, trao đổi, chuyển nhượng, kinh doanh trái pháp luật thông tin, dữ liệu cá nhân của người khác;

i) Hướng dẫn, xúi giục, lôi kéo, kích động người khác phạm tội hoặc thực hiện hành vi vi phạm pháp luật;

k) Thực hiện hành vi khác trên không gian mạng bằng việc sử dụng công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội.

3. Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng, tội phạm sử dụng công nghệ cao; 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.

4. Sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoặc phát tán thư rác, tin nhắn rác, cuộc gọi rác, chương trình tin học gây hại đến 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.

5. 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.

6. 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.

7. 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.

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

Chương II

BẢO VỆ AN NINH MẠNG ĐỐI VỚI HỆ THỐNG THÔNG TIN

Điều 8. Phân loại cấp độ hệ thống thông tin

1. Hệ thống thông tin được phân loại theo 5 cấp độ căn cứ vào mức độ tổn hại tới an ninh quốc gia, trật tự, an toàn xã hội, quyền, lợi ích hợp pháp của tổ chức, cá nhân, lợi ích công cộng khi bị sự cố hoặc có hành vi vi phạm pháp luật về an ninh mạng như sau:

a) Cấp độ 1 có thể làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân;

b) Cấp độ 2 có thể làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng;

c) Cấp độ 3 có thể làm tổn hại đặc biệt nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân; tổn hại nghiêm trọng tới lợi ích công cộng; tổn hại hoặc tổn hại nghiêm trọng tới trật tự, an toàn xã hội hoặc làm tổn hại tới an ninh quốc gia;

d) Cấp độ 4 có thể làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng, trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới an ninh quốc gia;

đ) Cấp độ 5 có thể làm tổn hại đặc biệt nghiêm trọng tới an ninh quốc gia.

2. Chính phủ quy định chi tiết tiêu chí xác định cấp độ hệ thống thông tin; quy định thẩm quyền, trình tự, thủ tục xác định cấp độ hệ thống thông tin và biện pháp, trách nhiệm, nghĩa vụ bảo đảm an ninh mạng theo từng cấp độ của hệ thống thông tin.

Điều 9. Hệ thống thông tin quan trọng về an ninh quốc gia

1. Hệ thống thông tin quan trọng về an ninh quốc gia là hệ thống thông tin có vai trò chiến lược, đặc biệt quan trọng đối với chính trị, quốc phòng, an ninh, ngoại giao, kinh tế, xã hội khi bị sự cố hoặc có hành vi vi phạm pháp luật về an ninh mạng có thể gây tổn hại tới an ninh quốc gia, tổn hại nghiêm trọng đến trật tự, an toàn xã hội, thuộc danh mục do Thủ tướng Chính phủ quyết định.

2. Hệ thống thông tin quan trọng về an ninh quốc gia thuộc các lĩnh vực sau đây:

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

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

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

d) Hệ thống thông tin phục vụ bảo quản vật liệu, chất đặc biệt nguy hiểm đối với con người, môi trường sinh thái;

đ) 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;

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

g) Hệ thống thông tin quốc gia thuộc lĩnh vực năng lượng, tài chính, ngân hàng, viễn thông, giao thông vận tải, nông nghiệp, tài nguyên và môi trường, hóa chất, y tế, văn hóa;

h) 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.

3. Hệ thống thông tin quan trọng về an ninh quốc gia phải được thẩm định an ninh mạng, chứng nhận đủ điều kiện về an ninh mạng trước khi đưa vào vận hành, sử dụng; thường xuyên kiểm tra an ninh mạng, giám sát an ninh mạng trong quá trình sử dụng và kịp thời ứng phó, khắc phục sự cố an ninh mạng.

4. Bộ Công an chủ trì, phối hợp với các Bộ, ngành, cơ quan, tổ chức, cá nhân có liên quan lập, trình Thủ tướng Chính phủ xem xét, quyết định danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

5. Chính phủ quy định chi tiết tiêu chí xác định hệ thống thông tin quan trọng về an ninh quốc gia.

Điều 10. Nhiệm vụ, biện pháp bảo vệ an ninh mạng đối với hệ thống thông tin

1. Nhiệm vụ bảo vệ an ninh mạng đối với hệ thống thông tin bao gồm:

a) Xác định cấp độ an ninh mạng của hệ thống thông tin và hệ thống thông tin quan trọng về an ninh quốc gia;

b) Đánh giá và quản lý rủi ro an ninh mạng hệ thống thông tin;

c) Đôn đốc, giám sát, kiểm tra công tác bảo vệ an ninh mạng hệ thống thông tin;

d) Tổ chức triển khai các biện pháp bảo vệ an ninh mạng hệ thống thông tin;

đ) Thực hiện chế độ báo cáo theo quy định;

e) Tổ chức tuyên truyền, nâng cao nhận thức về an ninh mạng.

2. Biện pháp bảo vệ an ninh mạng đối với hệ thống thông tin bao gồm:

a) Ban hành quy định về bảo đảm an ninh mạng trong thiết kế, xây dựng, quản lý, vận hành, sử dụng, nâng cấp, hủy bỏ hệ thống thông tin;

b) Thẩm định an ninh mạng đối với hồ sơ, thiết kế của hệ thống thông tin;

c) Đánh giá điều kiện an ninh mạng đối với hệ thống thông tin;

d) Áp dụng biện pháp quản lý theo tiêu chuẩn, quy chuẩn kỹ thuật về an ninh mạng, nghiên cứu xây dựng hệ thống tường lửa quốc gia để phòng, chống nguy cơ, khắc phục sự cố an ninh mạng;

đ) Tổ chức triển khai các biện pháp lưu trữ, sao lưu bảo vệ an ninh thông tin mạng và an ninh của các thành tố cấu thành hệ thống thông tin;

e) Kiểm tra, giám sát việc tuân thủ quy định và đánh giá hiệu quả của các biện pháp quản lý và kỹ thuật được áp dụng;

g) Thực hiện giám sát an ninh mạng;

h) Ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin.

3. Chủ quản hệ thống thông tin thuộc Cấp độ 1, Cấp độ 2 thực hiện đầy đủ các nhiệm vụ quy định tại khoản 1 Điều này và theo nhu cầu, khả năng thực tế lựa chọn áp dụng biện pháp quy định tại khoản 2 Điều này.

4. Chủ quản hệ thống thông tin thuộc Cấp độ 3, Cấp độ 4 không thuộc danh mục hệ thống thông tin quan trọng về an ninh quốc gia thực hiện đầy đủ các nhiệm vụ quy định tại khoản 1 Điều này, các biện pháp quy định tại các điểm a, d, đ, e, g và h khoản 2 Điều này và theo nhu cầu, khả năng thực tế lựa chọn áp dụng biện pháp quy định tại điểm b và điểm c khoản 2 Điều này.

5. Chủ quản hệ thống thông tin thuộc danh mục hệ thống thông tin quan trọng về an ninh quốc gia thực hiện đầy đủ các nhiệm vụ, biện pháp quy định tại khoản 1 và khoản 2 Điều này.

6. Chính phủ quy định chi tiết khoản 1 và khoản 2 Điều này.

Điều 11. Trách nhiệm bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

1. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm sau đây:

a) Thực hiện quy định tại khoản 5 Điều 10 của Luật này;

b) Khi thiết lập, mở rộng hoặc nâng cấp hệ thống thông tin quan trọng về an ninh quốc gia phải thực hiện kiểm tra an ninh mạng trước khi đi vào vận hành, khai thác; định kỳ hằng năm, tự kiểm tra an ninh mạng, đánh giá điều kiện an ninh mạng hệ thống thông tin quan trọng về an ninh quốc gia và thông báo kết quả kiểm tra bằng văn bản trước tháng 10 hằng năm cho lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền;

c) Chủ trì, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền trong việc thường xuyên thực hiện giám sát an ninh mạng; xây dựng cơ chế tự cảnh báo và tiếp nhận cảnh báo về nguy cơ đe dọa an ninh mạng; đề ra phương án ứng phó, khắc phục khẩn cấp;

d) Xây dựng phương án ứng phó, khắc phục sự cố an ninh mạng; triển khai phương án ứng phó, khắc phục khi sự cố an ninh mạng xảy ra và kịp thời báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền;

đ) Phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng trong việc thực hiện kiểm tra an ninh mạng đột xuất.

2. Bộ Công an có trách nhiệm sau đây đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ hệ thống thông tin quân sự và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ theo quy định của pháp luật:

a) Thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia;

b) Đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia;

c) Kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quan trọng về an ninh quốc gia;

d) Thực hiện giám sát an ninh mạng; cảnh báo và phối hợp với chủ quản hệ thống thông tin để khắc phục, xử lý các nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia;

đ) Chủ trì điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia; thông báo cho chủ quản hệ thống thông tin khi phát hiện có tấn công mạng, sự cố an ninh mạng;

e) Chủ trì, phối hợp Ban Cơ yếu Chính phủ trong triển khai các biện pháp bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia có sử dụng giải pháp, sản phẩm mật mã do Ban Cơ yếu Chính phủ cung cấp để bảo vệ bí mật nhà nước.

3. Bộ Quốc phòng chủ trì thẩm định an ninh mạng, đánh giá điều kiện an ninh mạng, kiểm tra an ninh mạng đột xuất, giám sát an ninh mạng và điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quân sự do Bộ Quốc phòng quản lý.

4. Ban Cơ yếu Chính phủ chủ trì tổ chức triển khai giải pháp dùng mật mã cơ yếu để bảo vệ thông tin bí mật nhà nước trong hệ thống thông tin quan trọng về an ninh quốc gia; thẩm định an ninh mạng, đánh giá điều kiện an ninh mạng, kiểm tra an ninh mạng đột xuất, giám sát an ninh mạng và điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

Điều 12. 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

1. 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 trong trường hợp sau đây:

a) Khi có hành vi được quy định tại các khoản 12, 13, 14 và 15 Điều 2 của Luật này;

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

2. Đối tượng kiểm tra an ninh mạng bao gồm:

a) Phần cứng, phần mềm, thiết bị số được sử dụng trong hệ thống thông tin;

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

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

3. Chủ quản hệ thống thông tin có trách nhiệm thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi phát hiện hành vi vi phạm pháp luật về an ninh mạng trên hệ thống thông tin thuộc phạm vi quản lý.

4. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an tiến hành kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức trong các trường hợp quy định tại khoản 1 Điều này. Kết quả kiểm tra an ninh mạng được bảo mật theo quy định của pháp luật.

5. Chính phủ quy định trình tự, thủ tục kiểm tra an ninh mạng quy định tại Điều này.

Chương III

PHÒNG NGỪA, XỬ LÝ HÀNH VI XÂM PHẠM AN NINH MẠNG

Điều 13. Các thông tin và hành vi sử dụng công nghệ thông tin, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng

1. 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 bao gồm:

a) Tuyên truyền thông tin, tài liệu có nội dung xuyên tạc, bôi nhọ, phỉ báng chính quyền nhân dân;

b) 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;

c) Xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc;

d) 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;

đ) 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 bình thường của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự;

e) Phản ánh sai lệch, không chính xác về đường biên giới quốc gia, chủ quyền lãnh thổ quốc gia Việt Nam; đăng tải, truyền đưa hình ảnh sai lệch, không chính xác, không đầy đủ về bản đồ Việt Nam hoặc thể hiện sai chủ quyền quốc gia Việt Nam.

2. Thông tin có nội dung phá hoại chính sách đoàn kết, chính sách kinh tế - xã hội nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm:

a) Gây mâu thuẫn, chia rẽ giữa các tầng lớp nhân dân, giữa nhân dân với chính quyền nhân dân, với lực lượng vũ trang nhân dân hoặc các tổ chức chính trị - xã hội;

b) Kích động, gây hận thù, kỳ thị, chia rẽ, ly khai dân tộc, xâm phạm quyền bình đẳng trong cộng đồng các dân tộc Việt Nam;

c) Kích động, gây mâu thuẫn, chia rẽ người theo tôn giáo với người không theo tôn giáo, giữa người theo các tôn giáo khác nhau, chia rẽ các tín đồ tôn giáo với chính quyền nhân dân, với lực lượng vũ trang nhân dân hoặc các tổ chức chính trị - xã hội;

d) Phá hoại, cản trở việc thực hiện chính sách đoàn kết quốc tế;

đ) Tuyên truyền gây tổn hại trực tiếp hoặc gián tiếp đến quyền, lợi ích hợp pháp của Nhà nước về chính trị, kinh tế, xã hội, uy tín quốc tế;

e) Kêu gọi, kích động phá hoại việc thực hiện các chính sách kinh tế - xã hội, gây cản trở việc thực thi các chính sách;

g) Kêu gọi, kích động phá hoại cơ sở vật chất - kỹ thuật của nước Cộng hòa xã hội chủ nghĩa Việt Nam.

3. Thông tin có nội dung xâm phạm quyền, lợi ích hợp pháp của tổ chức, cá nhân bao gồm:

a) Lan truyền thông tin xuyên tạc, bịa đặt, sai sự thật, gây ảnh hưởng đến uy tín, hoạt động bình thường của tổ chức;

b) Kêu gọi, vận động, xúi giục tẩy chay sản phẩm, dịch vụ, hàng hóa, nhãn hàng, thương hiệu của tổ chức, doanh nghiệp, gây thiệt hại về vật chất, uy tín của tổ chức, doanh nghiệp;

c) Mạo danh, giả mạo thông tin, hình ảnh, làm nhái sản phẩm, nhãn hiệu hàng hóa, thương hiệu của tổ chức, doanh nghiệp bằng cách sử dụng các tiện ích công nghệ, gây ảnh hưởng đến uy tín của tổ chức, doanh nghiệp;

d) Xúc phạm danh dự, uy tín, nhân phẩm của người khác;

đ) Xuyên tạc sai sự thật, gây ảnh hưởng đến danh dự, uy tín, nhân phẩm của người khác;

e) Bịa đặt hoặc lan truyền thông tin biết rõ là sai sự thật gây thiệt hại đến quyền, lợi ích hợp pháp của người khác;

g) Bịa đặt người khác phạm tội và tố cáo họ trước cơ quan có thẩm quyền;

h) Mạo danh, giả mạo thông tin, hình ảnh, giọng nói của cá nhân, gây ảnh hưởng đến uy tín, danh dự, nhân phẩm của cá nhân.

4. Các hành vi thực hiện trên không gian mạng bằng việc sử dụng công nghệ thông tin, phương tiện điện tử xâm phạm an ninh quốc gia và trật tự, an toàn xã hội bao gồm:

a) Đăng tải, phát tán thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2 và 3 Điều này;

b) Thực hiện hành vi quy định tại khoản 1 Điều 15 của Luật này;

c) 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;

d) 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; làm giả con dấu, tài liệu hoặc giấy tờ khác của cơ quan, tổ chức;

đ) Tuyên truyền, quảng cáo, mua bán trái phép vũ khí, vật liệu nổ, công cụ hỗ trợ, pháo nổ; ma túy, tiền chất ma túy, chất gây nghiện, chất hướng thần; động vật hoang dã, nguy cấp, quý, hiếm và các hàng hóa, dịch vụ khác thuộc danh mục cấm theo quy định của pháp luật; môi giới mại dâm; truyền bá văn hóa phẩm đồi trụy; lạm dụng tình dục trẻ em; quấy rối tình dục;

e) Thiết lập, cung cấp dịch vụ hoặc hỗ trợ vận hành, kinh doanh, giao dịch, mua bán, tiếp thị trực tuyến cho sàn giao dịch, trang thông tin điện tử, ứng dụng trái phép trên không gian mạng, bao gồm: sàn thương mại điện tử, trang thông tin điện tử, ứng dụng bán hàng, cung cấp dịch vụ thương mại điện tử; sàn giao dịch dựa trên chỉ số các loại hàng hóa; sàn giao dịch tài sản số, kinh doanh theo phương thức đa cấp;

g) Sử dụng danh tính giả, giấy tờ, hồ sơ giả hoặc sử dụng trái phép thông tin của người khác để thành lập doanh nghiệp, thiết lập, đăng ký tài khoản ngân hàng, tài khoản chứng khoán, tài khoản bảo hiểm, tài khoản thuế và tài khoản số khác; thu thập, tàng trữ, trao đổi, mua bán, tặng cho, công khai trái phép dữ liệu, thông tin tài khoản ngân hàng, thẻ ngân hàng, tài khoản ví điện tử, tài khoản chứng khoán, tài khoản bảo hiểm, tài khoản thuế và các loại tài khoản số khác;

h) Quảng cáo, buôn bán hàng giả, hàng hóa nhập lậu, không rõ nguồn gốc, xuất xứ; hàng hóa lưu thông trong nước bị áp dụng biện pháp khẩn cấp; hàng hóa quá hạn sử dụng;

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

k) Hành vi khác thực hiện trên không gian mạng bằng việc sử dụng công nghệ thông tin, phương tiện điện tử vi phạm pháp luật về trật tự, an toàn xã hội.

Điều 14. Phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng

1. Chủ quản hệ thống thông tin, doanh nghiệp trong nước và nước ngoài cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng có trách nhiệm triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn, gỡ bỏ thông tin có nội dung quy định tại các khoản 1, 2 và 3 Điều 13 của Luật này trên hệ thống thông tin thuộc phạm vi quản lý hoặc khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng.

2. Lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền áp dụng biện pháp quy định tại khoản 1 Điều 5 của Luật này để xử lý thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2 và 3 Điều 13 của Luật này và đấu tranh, phòng, chống hành vi sử dụng công nghệ thông tin, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng.

3. Doanh nghiệp trong nước và nước ngoài 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 phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng xử lý thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2 và 3 Điều 13 của Luật này và phòng, chống hành vi sử dụng công nghệ thông tin, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng.

4. Tổ chức, cá nhân soạn thảo, đăng tải, phát tán thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2 và 3 Điều 13 của Luật này phải gỡ bỏ thông tin khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng và chịu trách nhiệm theo quy định của pháp luật.

5. Chính phủ quy định chi tiết Điều này.

Điều 15. 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

1. 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:

a) 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;

b) 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;

c) 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;

d) 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;

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

e) 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.

2. Chủ quản hệ thống thông tin có trách nhiệm sau đây:

a) 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;

b) 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;

c) Phối hợp, thực hiện yêu cầu của lực lượng chuyên trách bảo vệ 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.

3. Cơ quan, tổ chức 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.

4. Bộ Công an có trách nhiệm sau đây, trừ quy định tại khoản 5 và khoản 6 Điều này:

a) 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;

b) 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;

c) 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;

d) 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;

đ) Tham gia nghiên cứu, sản xuất sản phẩm lưu trữ, truyền đưa thông tin, tài liệu có nội dung thuộc bí mật nhà nước theo quy định của pháp luật và sản phẩm mã hóa thông tin trên không gian mạng theo chức năng, nhiệm vụ được giao;

e) 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;

g) 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 quy định tại khoản 1 Điều 30 của Luật này.

5. Bộ Quốc phòng có trách nhiệm thực hiện các nội dung quy định tại các điểm a, b, c, d, đ và e khoản 4 Điều này đối với hệ thống thông tin quân sự.

6. Ban Cơ yếu Chính phủ có trách nhiệm thực hiện các nội dung quy định tại các điểm a, b, c, d, đ và e khoản 4 Điều này đối với hệ thống thông tin cơ yếu thuộc 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.

Điều 16. Phòng, chống xâm hại trẻ em trên không gian mạng

1. Trẻ em có quyền được tiếp cận thông tin, tham gia hoạt động xã hội, vui chơi, giải trí, bảo vệ bí mật cá nhân, đời sống riêng tư và các quyền khác trên không gian mạng theo quy định của pháp luật.

2. Trẻ em sử dụng dịch vụ giá trị gia tăng trên không gian mạng thì cha, mẹ hoặc người giám hộ theo pháp luật dân sự đăng ký tài khoản bằng thông tin của cha, mẹ hoặc người giám hộ và có trách nhiệm giám sát, quản lý nội dung trẻ em truy cập, đăng tải và chia sẻ thông tin trên các nền tảng dịch vụ đó.

3. Chủ quản hệ thống thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ giá trị gia tăng trên không gian mạng có các trách nhiệm sau đây:

a) 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 hoặc xâm hại trẻ em hoặc xâm phạm quyền trẻ em;

b) Ngăn chặn việc chia sẻ và xóa bỏ thông tin có nội dung gây nguy hại cho trẻ em hoặc xâm hại trẻ em hoặc xâm phạm quyền trẻ em;

c) Xây dựng, triển khai các hệ thống kỹ thuật hỗ trợ hoạt động ngăn chặn nội dung xâm hại trẻ em trên không gian mạng;

d) Phối hợp với các cơ quan, tổ chức, doanh nghiệp thực hiện ngăn chặn các nguồn phát tán thông tin xâm hại trẻ em trên không gian mạng;

đ) Kịp thời thông báo, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an để xử lý.

4. 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; phòng, chống xâm hại trẻ em trên không gian mạng.

5. Cơ quan, tổ chức, cha mẹ, người giám hộ, 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 và quy định của Luật này.

6. 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 hại trẻ em, xâm phạm quyền trẻ em.

Điều 17. Phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại

1. Cơ quan, tổ chức, cá nhân có trách nhiệm chủ động phòng ngừa, phát hiện, ngăn chặn phần mềm độc hại và thực hiện theo hướng dẫn, yêu cầu của cơ quan nhà nước có thẩm quyền.

2. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia triển khai hệ thống kỹ thuật nhằm phòng ngừa, phát hiện, ngăn chặn và xử lý kịp thời phần mềm độc hại.

3. Tổ chức, doanh nghiệp cung cấp dịch vụ thư điện tử, truyền đưa, lưu trữ thông tin phải có hệ thống lọc phần mềm độc hại trong quá trình gửi, nhận, lưu trữ thông tin trên hệ thống của mình và báo cáo cơ quan nhà nước có thẩm quyền theo quy định của pháp luật.

4. Doanh nghiệp cung cấp dịch vụ Internet có biện pháp quản lý, phòng ngừa, phát hiện, ngăn chặn phát tán phần mềm độc hại và xử lý theo yêu cầu của cơ quan nhà nước có thẩm quyền.

5. Bộ Công an chủ trì, phối hợp với Bộ Quốc phòng và bộ, ngành có liên quan tổ chức phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại gây tổn hại tới an ninh quốc gia.

Điều 18. Phòng, chống tấn công mạng

1. Hành vi tấn công mạng và hành vi có liên quan đến tấn công mạng bao gồm:

a) 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;

b) Gây cản trở, rối loạn, làm tê liệt, gián đoạn, ngưng trệ hoạt động, ngăn chặn trái phép việc truyền đưa dữ liệu của không gian mạng;

c) 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;

d) 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;

đ) Sản xuất, mua bán, trao đổi, tặng cho công cụ, thiết bị, phần mềm có tính năng gây hại 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;

e) 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.

2. Chủ quản hệ thống thông tin có trách nhiệm áp dụng biện pháp kỹ thuật để phòng ngừa, ngăn chặn hành vi quy định tại các điểm a, b, c, d và e khoản 1 Điều này đối với hệ thống thông tin thuộc phạm vi quản lý.

3. Khi xảy ra tấn công mạng xâm phạm hoặc đe dọa xâm phạm chủ quyền, lợi ích, an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội, lực lượng chuyên trách bảo vệ an ninh mạng chủ trì, phối hợp với chủ quản hệ thống thông tin và tổ chức, cá nhân có liên quan áp dụng biện pháp xác định nguồn gốc tấn công mạng, thu thập chứng cứ; yêu cầu doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng chặn lọc thông tin để ngăn chặn, loại trừ hành vi tấn công mạng và cung cấp đầy đủ, kịp thời thông tin, tài liệu liên quan.

4. Trách nhiệm phòng, chống tấn công mạng được quy định như sau:

a) Bộ Công an chủ trì, phối hợp với bộ, ngành, địa phương có liên quan thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi quy định tại khoản 1 Điều này 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 trên phạm vi cả nước, trừ trường hợp quy định tại điểm b và điểm c khoản này;

b) Bộ Quốc phòng chủ trì, phối hợp với Bộ, ngành có liên quan thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi quy định tại khoản 1 Điều này đối với hệ thống thông tin quân sự;

c) Ban Cơ yếu Chính phủ chủ trì, phối hợp với Bộ, ngành có liên quan thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi quy định tại khoản 1 Điều này đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

Điều 19. Phòng, chống khủng bố mạng

1. Cơ quan nhà nước có thẩm quyền có trách nhiệm áp dụng biện pháp theo quy định của Luật này và pháp luật về phòng, chống khủng bố để xử lý khủng bố mạng.

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

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

4. Bộ Công an chủ trì, phối hợp với Bộ, ngành có liên quan triển khai công tác phòng, chống khủng bố mạng, áp dụng biện pháp vô hiệu hóa nguồn khủng bố mạng, xử lý khủng bố mạng, hạn chế đến mức thấp nhất hậu quả xảy ra đối với hệ thống thông tin, trừ trường hợp quy định tại khoản 5 và khoản 6 Điều này.

5. Bộ Quốc phòng chủ trì, phối hợp với Bộ, ngành có liên quan triển khai công tác phòng, chống khủng bố mạng, áp dụng biện pháp xử lý khủng bố mạng xảy ra đối với hệ thống thông tin quân sự.

6. Ban Cơ yếu Chính phủ chủ trì, phối hợp với Bộ, ngành có liên quan triển khai công tác phòng, chống khủng bố mạng, áp dụng biện pháp xử lý khủng bố mạng xảy ra đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

Điều 20. Phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng

1. Tình huống nguy hiểm về an ninh mạng bao gồm:

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

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

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

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

đ) 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.

2. Trách nhiệm phòng ngừa tình huống nguy hiểm về an ninh mạng được quy định như sau:

a) Lực lượng chuyên trách bảo vệ an ninh mạng phối hợp với chủ quản hệ thống thông tin quan trọng về an ninh quốc gia triển khai các giải pháp kỹ thuật, nghiệp vụ để phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng;

b) 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 có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an trong phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng.

3. Biện pháp xử lý tình huống nguy hiểm về an ninh mạng bao gồm:

a) Triển khai ngay phương án phòng ngừa, ứng phó khẩn cấp về an ninh mạng, ngăn chặn, loại trừ hoặc giảm nhẹ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra;

b) Thông báo đến cơ quan, tổ chức, cá nhân có liên quan;

c) Thu thập thông tin liên quan; theo dõi, giám sát liên tục đối với tình huống nguy hiểm về an ninh mạng;

d) Phân tích, đánh giá thông tin, dự báo khả năng, phạm vi ảnh hưởng và mức độ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra;

đ) Ngừng cung cấp thông tin mạng tại khu vực cụ thể hoặc ngắt cổng kết nối mạng quốc tế;

e) Bố trí lực lượng, phương tiện ngăn chặn, loại bỏ tình huống nguy hiểm về an ninh mạng;

g) Biện pháp khác theo quy định của Luật An ninh quốc gia.

4. Việc xử lý tình huống nguy hiểm về an ninh mạng được quy định như sau:

a) Khi phát hiện tình huống nguy hiểm về an ninh mạng, cơ quan, tổ chức, cá nhân kịp thời thông báo cho lực lượng chuyên trách bảo vệ an ninh

mạng và áp dụng ngay các biện pháp quy định tại điểm a và điểm b khoản 3 Điều này;

b) Thủ tướng Chính phủ xem xét, quyết định hoặc ủy quyền cho Bộ trưởng Bộ Công an xem xét, quyết định, xử lý tình huống nguy hiểm về an ninh mạng trong phạm vi cả nước hoặc từng địa phương hoặc đối với một mục tiêu cụ thể.

Thủ tướng Chính phủ xem xét, quyết định hoặc ủy quyền cho Bộ trưởng Bộ Quốc phòng xem xét, quyết định, xử lý tình huống nguy hiểm về an ninh mạng đối với hệ thống thông tin quân sự và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ;

c) Lực lượng chuyên trách bảo vệ an ninh mạng chủ trì, phối hợp với cơ quan, tổ chức, cá nhân có liên quan áp dụng các biện pháp quy định tại khoản 3 Điều này để xử lý tình huống nguy hiểm về an ninh mạng;

d) Cơ quan, tổ chức, cá nhân có liên quan có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thực hiện biện pháp nhằm ngăn chặn, xử lý tình huống nguy hiểm về an ninh mạng.

Điều 21. Đấu tranh bảo vệ an ninh mạng

1. 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.

2. Nội dung đấu tranh bảo vệ an ninh mạng bao gồm:

a) Giám sát thông tin mạng và phòng ngừa, đấu tranh, xử lý tổ chức, cá nhân có hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội;

b) Sử dụng giải pháp kỹ thuật để ngăn chặn thông tin vi phạm pháp luật;

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

d) 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;

đ) 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.

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

Điều 22. Ngăn chặn xung đột thông tin trên không gian mạng

1. Xung đột thông tin là việc hai hoặc nhiều tổ chức trong nước và nước ngoài sử dụng biện pháp công nghệ, kỹ thuật thông tin gây tổn hại đến thông tin, hệ thống thông tin trên không gian mạng làm ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội.

2. Ngăn chặn xung đột thông tin trên không gian mạng là việc thực hiện các biện pháp công nghệ, kỹ thuật để giám sát, phát hiện, cảnh báo, xác định nguồn gốc, chặn lọc, gỡ bỏ, phản bác, định hướng dư luận, khắc phục, xử phạt và các biện pháp khác loại trừ xung đột thông tin trên không gian mạng.

3. Tổ chức, cá nhân trong phạm vi nhiệm vụ, quyền hạn của mình có trách nhiệm sau đây:

a) Ngăn chặn xung đột thông tin trên không gian mạng từ hệ thống thông tin của mình; hợp tác xác định nguồn, đẩy lùi, khắc phục hậu quả tấn công mạng được thực hiện thông qua hệ thống thông tin của tổ chức, cá nhân trong nước và nước ngoài;

b) Ngăn chặn hoạt động của tổ chức, cá nhân trong nước và nước ngoài có mục đích tạo xung đột thông tin trên không gian mạng;

c) Loại trừ việc tổ chức thực hiện đăng tải, phát tán thông tin trên không gian mạng có ảnh hưởng nghiêm trọng đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội của tổ chức, cá nhân trong nước và nước ngoài.

4. Chính phủ quy định chi tiết Điều này.

Chương IV

HOẠT ĐỘNG BẢO VỆ AN NINH MẠNG

Điều 23. Triển khai hoạt động bảo vệ an ninh mạng trong cơ quan nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội ở trung ương và địa phương

1. Nội dung triển khai hoạt động bảo vệ an ninh mạng bao gồm:

a) 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;

b) 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;

c) 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;

d) 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;

đ) 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;

e) 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.

2. Người đứng đầu cơ quan, tổ chức có trách nhiệm triển khai hoạt động bảo vệ an ninh mạng thuộc quyền quản lý.

Điều 24. Bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế

1. 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.

2. 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 sau đây:

a) 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;

b) 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.

Điều 25. Bảo đảm an ninh thông tin mạng

1. 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 Điều 13 và khoản 1 Điều 15 của Luật này và thông tin khác có nội dung xâm phạm an ninh quốc gia.

2. Doanh nghiệp trong nước và nước ngoài khi 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 sau đây:

a) 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 chậm nhất là 24 giờ kể từ thời điểm có yêu cầu bằng văn bản hoặc thư điện tử, điện thoại hoặc hình thức trao đổi khác đã được xác nhận để phục vụ xác minh, điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng; trường hợp khẩn cấp đe dọa xâm hại an ninh quốc gia, đe dọa tính mạng con người, yêu cầu cung cấp thông tin chậm nhất là 03 giờ;

b) Ngăn chặn việc chia sẻ thông tin, xóa bỏ thông tin, gỡ bỏ dịch vụ, ứng dụng có nội dung vi phạm quy định của Luật này 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 và lưu nhật ký hệ thống để phục vụ xác minh, điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng trong thời gian theo quy định của pháp luật; trường hợp khẩn cấp đe dọa xâm hại an ninh quốc gia, yêu cầu ngăn chặn, xóa bỏ thông tin chậm nhất là 06 giờ;

c) 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 đối với thông tin có nội dung quy định tại các khoản 1, 2 và 3 Điều 13, khoản 1 và khoản 2 Điều 14 của Luật này khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an;

d) Lưu trữ thông tin cá nhân của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tạo ra, bao gồm: tên tài khoản, thời gian sử dụng dịch vụ, thông tin thanh toán phí sử dụng dịch vụ, địa chỉ IP truy cập và các dữ liệu liên quan khác trong thời gian theo quy định của pháp luật sau khi người dùng kết thúc việc sử dụng dịch vụ.

3. 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 áp dụng các biện pháp bảo vệ dữ liệu theo quy định của pháp luật và lưu trữ dữ liệu này tại Việt Nam trong thời gian theo quy định của Chính phủ.

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

4. Chính phủ quy định chi tiết khoản 2 và khoản 3 Điều này.

Điều 26. Bảo đảm an ninh dữ liệu

1. Bảo đảm an ninh dữ liệu là tổng thể các biện pháp kỹ thuật, tổ chức và pháp lý nhằm bảo vệ dữ liệu, phòng, chống xâm phạm an ninh dữ liệu.

2. Nội dung bảo đảm an ninh dữ liệu bao gồm:

a) Xây dựng chính sách, thiết lập quy trình về bảo đảm an ninh dữ liệu;

b) Áp dụng biện pháp, tiêu chuẩn, quy chuẩn kỹ thuật theo quy định của pháp luật về an ninh mạng;

c) Sử dụng mật mã cơ yếu, mật mã dân sự để bảo đảm an ninh dữ liệu;

d) Triển khai cơ chế kiểm soát chặt chẽ nhân sự trực tiếp tham gia xử lý dữ liệu;

đ) Kiểm tra, đánh giá rủi ro định kỳ nhằm phát hiện, ngăn chặn và xử lý kịp thời các nguy cơ đe dọa an ninh dữ liệu;

e) Kiểm tra, đánh giá việc chuyển dữ liệu xuyên biên giới; điều kiện đảm bảo an ninh dữ liệu trong hệ thống thông tin quan trọng về an ninh quốc gia, các cơ sở dữ liệu, trung tâm dữ liệu, hệ thống lưu trữ dữ liệu;

g) Các nội dung khác theo quy định của pháp luật.

3. Chính phủ quy định chi tiết khoản 2 Điều này; quy định trách nhiệm bảo đảm an ninh dữ liệu.

Chương V

TIÊU CHUẨN, QUY CHUẨN KỸ THUẬT, SẢN PHẨM, DỊCH VỤ AN NINH MẠNG

Điều 27. Tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng

1. Tiêu chuẩn an ninh mạng, quy chuẩn kỹ thuật an ninh mạng được áp dụng đối với hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng, sản phẩm, dịch vụ an ninh mạng, công nghệ thông tin và thiết bị kết nối mạng.

2. Việc chứng nhận hợp quy về an ninh mạng, công bố hợp quy về an ninh mạng, chứng nhận hợp chuẩn về an ninh mạng, công bố hợp chuẩn về an ninh mạng thực hiện theo quy định của pháp luật về tiêu chuẩn và quy chuẩn kỹ thuật.

3. Việc đánh giá hợp chuẩn, hợp quy về an ninh mạng phục vụ hệ thống thông tin quan trọng về an ninh quốc gia và phục vụ hoạt động quản lý nhà nước về an ninh mạng được thực hiện tại tổ chức chứng nhận hợp chuẩn, hợp quy do Bộ trưởng Bộ Công an chỉ định.

4. Bộ Công an có trách nhiệm sau đây:

a) Xây dựng dự thảo tiêu chuẩn quốc gia về an ninh mạng;

b) Xây dựng và ban hành quy chuẩn kỹ thuật quốc gia về an ninh mạng;

c) Quản lý chất lượng sản phẩm, dịch vụ an ninh mạng, trừ sản phẩm, dịch vụ mật mã dân sự;

d) Đăng ký, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp về an ninh mạng, trừ trường hợp quy định tại khoản 5 và khoản 6 Điều này.

5. Bộ Quốc phòng đăng ký, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp về an ninh mạng trong lĩnh vực quân sự.

6. Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng thực hiện quản lý chất lượng sản phẩm, dịch vụ mật mã dân sự; đăng ký, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp về an ninh mạng đối với sản phẩm, dịch vụ mật mã dân sự.

Điều 28. Sản phẩm, dịch vụ an ninh mạng

1. Sản phẩm an ninh mạng bao gồm:

a) Sản phẩm mật mã dân sự;

b) Sản phẩm kiểm tra, đánh giá an ninh mạng;

c) Sản phẩm giám sát an ninh mạng;

d) Sản phẩm chống tấn công, xâm nhập;

đ) Sản phẩm an ninh mạng khác.

2. Dịch vụ an ninh mạng bao gồm:

a) Dịch vụ kiểm tra, đánh giá an ninh mạng;

b) Dịch vụ bảo mật thông tin không sử dụng mật mã dân sự;

c) Dịch vụ mật mã dân sự;

d) Dịch vụ tư vấn an ninh mạng;

đ) Dịch vụ giám sát an ninh mạng;

e) Dịch vụ ứng cứu sự cố an ninh mạng;

g) Dịch vụ khôi phục dữ liệu;

h) Dịch vụ phòng ngừa, chống tấn công mạng;

i) Dịch vụ an ninh mạng khác.

3. Chính phủ quy định chi tiết Điều này.

Điều 29. Kinh doanh sản phẩm, dịch vụ an ninh mạng

1. Doanh nghiệp kinh doanh sản phẩm, dịch vụ an ninh mạng phải có giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng.

2. Doanh nghiệp kinh doanh sản phẩm, dịch vụ an ninh mạng có trách nhiệm sau đây:

a) Thực hiện đúng giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng; tuân thủ quy định của pháp luật về an ninh mạng và quy định khác của pháp luật có liên quan;

b) Bảo đảm về chất lượng sản phẩm, dịch vụ an ninh mạng đúng với tiêu chuẩn công bố áp dụng, quy chuẩn kỹ thuật tương ứng theo quy định của pháp luật về chất lượng sản phẩm, hàng hóa, pháp luật về tiêu chuẩn và quy chuẩn kỹ thuật trước khi lưu thông trên thị trường;

c) Lập, lưu giữ và bảo mật thông tin của khách hàng, quản lý hồ sơ, tài liệu về giải pháp kỹ thuật, công nghệ của sản phẩm, hoạt động cung cấp dịch vụ theo quy định của pháp luật;

d) Từ chối cung cấp sản phẩm, dịch vụ an ninh mạng khi phát hiện tổ chức, cá nhân vi phạm pháp luật về sử dụng sản phẩm, dịch vụ an ninh mạng, vi phạm cam kết đã thỏa thuận về sử dụng sản phẩm, dịch vụ do doanh nghiệp cung cấp;

đ) Phối hợp, tạo điều kiện, thực hiện yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng để thực hiện các biện pháp bảo vệ an ninh mạng.

3. Chính phủ quy định việc cấp, tạm đình chỉ, thu hồi giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng; quy định việc nhập khẩu, xuất khẩu sản phẩm an ninh mạng; quy định việc kinh doanh sản phẩm, dịch vụ an ninh mạng.

Chương VI

LỰC LƯỢNG, ĐIỀU KIỆN BẢO ĐẢM AN NINH MẠNG

Điều 30. Lực lượng bảo vệ an ninh mạng

1. Lực lượng bảo vệ an ninh mạng bao gồm:

a) Lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Bộ Công an, Bộ Quốc phòng;

b) 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;

c) Tổ chức, cá nhân được huy động tham gia bảo vệ an ninh mạng.

2. Chính phủ quy định chi tiết khoản 1 Điều này; quy định việc phối hợp giữa các lực lượng bảo vệ an ninh mạng.

Điều 31. Bảo đảm nguồn nhân lực bảo vệ an ninh mạng

1. Nhà nước đào tạo, phát triển nguồn nhân lực bảo vệ an ninh mạng bảo đảm số lượng, chất lượng, đáp ứng yêu cầu năng lực bảo vệ an ninh mạng quốc gia.

2. Lực lượng chuyên trách bảo vệ an ninh mạng được ưu tiên bố trí nhân lực theo vị trí việc làm, tiêu chuẩn chức danh, được áp dụng cơ chế tuyển dụng, xét tuyển, sử dụng, đào tạo, bồi dưỡng, đãi ngộ và thu hút nhân tài theo chính sách đặc thù do Chính phủ quy định.

3. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm sau đây:

a) Bố trí bộ phận hoặc nhân sự chuyên trách phù hợp với cấp độ bảo vệ của hệ thống;

b) Bảo đảm người thực hiện nhiệm vụ an ninh mạng đáp ứng tiêu chuẩn chuyên môn, nghiệp vụ;

c) Thường xuyên bồi dưỡng, cập nhật kỹ năng cho đội ngũ nhân sự liên quan đến vận hành, giám sát, ứng cứu và xử lý sự cố mạng.

Điều 32. Tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng

1. Công dân Việt Nam có đủ tiêu chuẩn về phẩm chất đạo đức, sức khỏe, trình độ, kiến thức về an ninh mạng, công nghệ thông tin, có nguyện vọng thì có thể được tuyển chọn vào lực lượng bảo vệ an ninh mạng.

2. Ưu tiên đào tạo, phát triển lực lượng bảo vệ an ninh mạng có chất lượng cao; phát hiện tài năng trẻ về an ninh mạng, công nghệ thông tin để định hướng học tập, tuyển chọn, thu hút và sử dụng trong lĩnh vực an ninh mạng.

3. Ưu tiên phát triển cơ sở đào tạo an ninh mạng đạt tiêu chuẩn quốc tế; khuyến khích liên kết, tạo cơ hội hợp tác về an ninh mạng giữa khu vực nhà nước và khu vực tư nhân, trong nước và nước ngoài.

Điều 33. Giáo dục, bồi dưỡng kiến thức, nghiệp vụ an ninh mạng

1. Nội dung giáo dục, bồi dưỡng kiến thức an ninh mạng được đưa vào môn học giáo dục quốc phòng và an ninh trong nhà trường, chương trình bồi dưỡng kiến thức quốc phòng và an ninh theo quy định của Luật Giáo dục quốc phòng và an ninh.

2. Bộ Công an chủ trì, phối hợp với Bộ, ngành có liên quan tổ chức bồi dưỡng nghiệp vụ an ninh mạng cho lực lượng bảo vệ an ninh mạng và công chức, viên chức, người lao động tham gia bảo vệ an ninh mạng.

Bộ Quốc phòng tổ chức bồi dưỡng nghiệp vụ an ninh mạng cho đối tượng thuộc phạm vi quản lý.

Điều 34. Tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng

1. Lực lượng bảo vệ an ninh mạng quy định tại điểm a và điểm b khoản 1 Điều 30 của Luật này phải đáp ứng yêu cầu kiến thức, kỹ năng chuyên sâu về an ninh mạng.

2. Người trực tiếp quản trị, vận hành hệ thống thông tin Cấp độ 3, Cấp độ 4, Cấp độ 5 trong cơ quan, tổ chức, doanh nghiệp Nhà nước phải được tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng và được cấp chứng nhận, trừ các cá nhân đã được đào tạo chuyên ngành an ninh mạng.

3. Bộ Công an chủ trì, phối hợp với các bộ, ngành liên quan tổ chức tập huấn về kiến thức, kỹ năng chuyên sâu về an ninh mạng.

4. Bộ Quốc phòng tổ chức tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng đối với đối tượng thuộc phạm vi quản lý.

5. Chính phủ quy định về chuẩn kiến thức, kỹ năng chuyên sâu về an ninh mạng; chương trình, nội dung tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng.

Điều 35. Phổ biến kiến thức về an ninh mạng

1. Nhà nước có chính sách phổ biến kiến thức về an ninh mạng trong phạm vi cả nước, khuyến khích cơ quan nhà nước phối hợp với tổ chức tư nhân, cá nhân thực hiện chương trình giáo dục và nâng cao nhận thức về an ninh mạng; ưu tiên phổ biến, hướng dẫn trẻ em, người cao tuổi, người khó khăn trong nhận thức để nâng cao khả năng tự bảo vệ quyền và lợi ích hợp pháp của mình trên không gian mạng.

2. Bộ, ngành, cơ quan, tổ chức có trách nhiệm xây dựng và triển khai hoạt động phổ biến kiến thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động trong Bộ, ngành, cơ quan, tổ chức.

3. Ủy ban nhân dân cấp tỉnh có trách nhiệm xây dựng và triển khai hoạt động phổ biến kiến thức, nâng cao nhận thức về an ninh mạng cho cơ quan, tổ chức, cá nhân của địa phương.

Điều 36. Nghiên cứu, phát triển an ninh mạng

1. Nội dung nghiên cứu, phát triển an ninh mạng bao gồm:

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

b) 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;

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

d) 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;

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

e) Giải quyết nguy cơ đe dọa an ninh mạng;

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

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

i) Dự báo an ninh mạng;

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

2. Cơ quan, tổ chức, cá nhân có liên quan có quyền nghiên cứu, phát triển an ninh mạng.

Điều 37. Nâng cao năng lực tự chủ về an ninh mạng

1. 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.

2. Chính phủ thực hiện các biện pháp sau đây để nâng cao năng lực tự chủ về an ninh mạng cho cơ quan, tổ chức, cá nhân:

a) Chỉ đạo xây dựng chính sách, chiến lược, quy hoạch phát triển công nghiệp an ninh mạng; tiêu chuẩn, quy chuẩn kỹ thuật đối với các sản phẩm phần cứng, phần mềm nhằm chủ động loại bỏ các nguy cơ về an ninh mạng ngay từ khi hình thành sản phẩm;

b) Thúc đẩy chuyển giao, nghiên cứu, làm chủ và phát triển công nghệ, sản phẩm, dịch vụ công nghiệp an ninh để bảo vệ an ninh mạng;

c) Thúc đẩy ứng dụng công nghệ mới, công nghệ tiên tiến liên quan đến an ninh mạng;

d) Tổ chức đào tạo, phát triển, tối ưu hóa sử dụng nguồn nhân lực an ninh mạng chất lượng cao;

đ) 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.

3. Hoạt động đầu tư, thu hút nguồn lực phát triển hạ tầng công nghiệp an ninh mạng bao gồm:

a) Hoạt động đầu tư xây dựng hạ tầng công nghiệp an ninh mạng là ngành, nghề đặc biệt ưu đãi đầu tư, được hưởng ưu đãi, hỗ trợ theo quy định của pháp luật về đầu tư; thuế; đất đai và pháp luật khác có liên quan;

b) Nhà nước ưu tiên bố trí nguồn vốn ngân sách để đầu tư xây dựng hạ tầng công nghiệp an ninh mạng gồm: Cơ sở nghiên cứu, thiết kế, sản xuất, thử nghiệm sản phẩm, dịch vụ an ninh mạng; Phòng thí nghiệm trọng điểm quốc gia về an ninh mạng; Cơ sở đo kiểm, thử nghiệm, đánh giá sản phẩm, dịch vụ an

ninh mạng; Trung tâm dữ liệu lớn; Khu công nghiệp an ninh mạng tập trung; Tổ hợp công nghiệp an ninh mạng;

c) Hạ tầng công nghiệp an ninh mạng được nhà nước đầu tư quy định tại điểm b khoản này là một loại tài sản kết cấu hạ tầng và được quản lý, khai thác, vận hành theo quy định của pháp luật về quản lý, sử dụng tài sản công;

d) Tổ chức, doanh nghiệp được nhập khẩu dây chuyền công nghệ, thiết bị, máy móc, công cụ phục vụ hoạt động đào tạo, nghiên cứu và phát triển sản phẩm, dịch vụ an ninh mạng;

đ) Các cơ quan, tổ chức, doanh nghiệp nhà nước ưu tiên sử dụng các sản phẩm, dịch vụ an ninh mạng nội địa.

4. Bộ Công an tham mưu Chính phủ quy hoạch, xây dựng, phát triển hạ tầng công nghiệp an ninh mạng nhằm nâng cao năng lực tự chủ về an ninh mạng.

Điều 38. Kinh phí bảo vệ an ninh mạng

1. Cơ quan, tổ chức, doanh nghiệp nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội và các đơn vị sự nghiệp công lập do ngân sách nhà nước bảo đảm phải bố trí kinh phí bảo vệ an ninh mạng trong dự toán chi thực hiện nhiệm vụ chuyển đổi số, ứng dụng công nghệ thông tin hàng năm của cơ quan, tổ chức, đơn vị mình; bố trí tối thiểu 15% tổng kinh phí thực hiện chương trình, đề án, dự án đầu tư chuyển đổi số, ứng dụng công nghệ thông tin để bảo vệ an ninh mạng.

2. Cơ quan, tổ chức, đơn vị không thuộc quy định tại khoản 1 Điều này tự bảo đảm kinh phí bảo vệ an ninh mạng cho cơ quan, tổ chức, đơn vị mình.

Chương VII
TRÁCH NHIỆM CỦA CƠ QUAN, TỔ CHỨC, CÁ NHÂN VỀ AN NINH MẠNG

Điều 39. Trách nhiệm quản lý nhà nước về an ninh mạng

1. Chính phủ thống nhất quản lý nhà nước về an ninh mạng.

2. Bộ Công an là cơ quan đầu mối giúp Chính phủ thực hiện quản lý nhà nước về an ninh mạng; chịu trách nhiệm trước Chính phủ thực hiện các nội dung quản lý nhà nước về an ninh mạng sau đây, trừ nội dung quy định tại khoản 3 và khoản 4 Điều này:

a) 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;

b) Xây dựng, đề xuất chiến lược, chủ trương, chính sách, kế hoạch và phương án bảo vệ an ninh mạng; nghiên cứu, xây dựng, phát triển, sử dụng mật mã an ninh để bảo vệ an ninh dữ liệu thuộc phạm vi quản lý của Bộ Công an;

c) 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 13 của Luật này;

d) 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;

đ) 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;

e) Bảo đảm an ninh thông tin trên không gian mạng, an ninh dữ liệu; xây dựng cơ chế quản lý định danh địa chỉ IP; 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;

g) 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;

h) Trưng dụng chuyên gia, nhà khoa học, cán bộ chuyên sâu và hệ thống trong trường hợp khẩn cấp để bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội trên không gian mạng;

i) 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;

k) Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về an ninh mạng, an ninh thông tin, an ninh dữ liệu.

3. Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an ninh mạng thuộc phạm vi quản lý như sau:

a) 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;

b) 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;

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

d) 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;

đ) 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.

4. Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng thực hiện quản lý nhà nước về mật mã dân sự và an ninh mạng thuộc phạm vi quản lý theo quy định của pháp luật.

5. Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, trong phạm vi chức năng, nhiệm vụ, quyền hạn của mình, thực hiện công tác bảo vệ an ninh mạng;

phối hợp với Bộ Công an thực hiện quản lý nhà nước về an ninh mạng.

6. Ủy ban nhân dân cấp tỉnh thực hiện công tác bảo vệ an ninh mạng tại địa phương; phối hợp với Bộ Công an thực hiện quản lý nhà nước về an ninh mạng.

Điều 40. Trách nhiệm của chủ quản hệ thống thông tin trong bảo vệ an ninh mạng

1. Chủ quản hệ thống thông tin có trách nhiệm sau đây:

a) Thực hiện bảo vệ hệ thống thông tin theo quy định tại Luật này;

b) Kết nối hệ thống giám sát an ninh mạng, hệ thống phòng chống mã độc tập trung về Trung tâm An ninh mạng quốc gia của Bộ Công an hoặc Trung tâm An ninh mạng của tỉnh, thành phố để hỗ trợ giám sát an ninh mạng;

c) Báo cáo sự cố an ninh mạng với cơ quan chuyên trách của Bộ Công an hoặc Bộ Quốc phòng.

2. Chủ quản hệ thống thông tin sử dụng ngân sách nhà nước thực hiện trách nhiệm quy định tại khoản 1 Điều này và trách nhiệm sau đây:

a) Có phương án bảo đảm an ninh mạng được cơ quan nhà nước có thẩm quyền thẩm định an ninh mạng khi thiết lập, mở rộng hoặc nâng cấp hệ thống thông tin;

b) Chỉ định cá nhân, bộ phận phụ trách về an ninh mạng.

Điều 41. Trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng

1. Tuân thủ quy định của pháp luật về an ninh mạng.

2. 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 đối với người sử dụng dịch vụ; xây dựng phương án ứng cứu khẩn cấp bảo đảm an ninh mạng để chủ động xử lý điểm yếu, rủi ro và sự cố an ninh mạng.

3. Khi xảy ra sự cố an ninh mạng, ngay lập tức triển khai phương án ứng cứu khẩn cấp bảo đảm an ninh mạng, đồng thời báo cáo ngay với lực lượng chuyên trách bảo vệ an ninh mạng theo quy định của Luật này.

4. Áp dụng các biện pháp, giải pháp kỹ thuật để bảo đảm an ninh mạng cho hoạt động xử lý dữ liệu, xử lý dữ liệu cá nhân theo quy định của Luật này, pháp luật về dữ liệu, pháp luật về bảo vệ dữ liệu cá nhân và quy định khác của pháp luật có liên quan.

5. Có trách nhiệm định danh địa chỉ IP của tổ chức, cá nhân sử dụng dịch vụ internet; cung cấp thông tin định danh địa chỉ IP cho lực lượng chuyên trách bảo vệ an ninh mạng để thực hiện biện pháp bảo vệ an ninh mạng.

6. Phối hợp thực hiện theo hướng dẫn của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an để thiết lập hệ thống kết nối, đấu nối đường truyền kỹ thuật, truyền tải dữ liệu và đáp ứng các điều kiện cần thiết khác để triển khai các giải pháp, biện pháp bảo vệ an ninh mạng khi có yêu cầu để phục vụ điều tra, xác minh, xử lý hành vi vi phạm pháp luật về an ninh mạng.

7. Doanh nghiệp 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 thực hiện quy định tại Điều này, khoản 2 và khoản 3 Điều 25 của Luật này.

Điều 42. Trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng

1. Tuân thủ quy định của pháp luật về an ninh mạng.

2. Có trách nhiệm bảo mật thông tin đăng ký, mở, quản lý, sử dụng tài khoản số của mình. Trường hợp sử dụng tài khoản số để thực hiện hành vi vi phạm pháp luật, tùy theo tính chất, mức độ của hành vi vi phạm, chủ tài khoản số, người sử dụng tài khoản số bị xử lý kỷ luật, xử phạt vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự; nếu gây thiệt hại đến lợi ích của Nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân thì phải bồi thường thiệt hại theo quy định pháp luật.

3. 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.

4. 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.

Chương VIII

ĐIỀU KHOẢN THI HÀNH

Điều 43. Sửa đổi, bổ sung, thay thế, bãi bỏ một số điều của các luật có liên quan

1. Thay thế một số cụm từ, bãi bỏ khoản tại Luật Lưu trữ số 33/2024/QH15 như sau:

a) Thay thế cụm từ "an toàn thông tin" tại điểm b khoản 1 Điều 35; cụm từ "an toàn thông tin mạng" tại điểm b khoản 2 Điều 36; cụm từ "an toàn, an ninh thông tin" tại khoản 3 Điều 60 bằng cụm từ "an ninh mạng";

b) Bãi bỏ khoản 4 Điều 58.

2. Thay thế, bỏ một số cụm từ tại Luật Bảo vệ quyền lợi người tiêu dùng số 19/2023/QH15 như sau:

a) Thay thế cụm từ "an toàn thông tin" tại điểm d khoản 1 Điều 16; cụm từ "an toàn, an ninh thông tin" tại khoản 1 Điều 15, tên Điều 19, khoản 1 và 3 Điều 19 bằng cụm từ "an ninh mạng";

c) Bỏ cụm từ "an toàn thông tin mạng," khoản 3 Điều 19.

3. Thay thế một số cụm từ tại Luật Phí và lệ phí số 97/2015/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 09/2017/QH14, Luật số 23/2018/QH14, Luật số 72/2020/QH14, Luật số 16/2023/QH15, Luật số 20/2023/QH15, Luật số 24/2023/QH15, Luật số 33/2024/QH15, Luật số 35/2024/QH15, Luật số 47/2024/QH15, Luật số 60/2024/QH15, Luật số

74/2025/QH15, Luật số 89/2025/QH15, Luật số 94/2025/QH15 và Luật số 95/2025/QH15 như sau:

a) Thay thế cụm từ "an toàn thông tin" bằng cụm từ "an ninh mạng" tại tiểu mục 10 mục VI thuộc phần A và tiểu mục 16 mục III thuộc phần B Phụ lục số 01 - Danh mục phí và lệ phí;

b) Thay thế cụm từ "an toàn thông tin mạng" bằng cụm từ "an ninh mạng" tại tiểu mục 11 mục VI thuộc phần A Phụ lục số 01 - Danh mục phí và lệ phí.

4. Thay thế, bỏ một số cụm từ tại Luật Công nghiệp công nghệ số 71/2025/QH15 như sau:

a) Thay thế cụm từ "an toàn thông tin" bằng cụm từ "an ninh mạng" tại điểm a khoản 1 Điều 25;

b) Bỏ cụm từ "an toàn thông tin mạng," tại Điều 10.

5. Thay thế, bỏ một số cụm từ tại Luật Dữ liệu số 60/2024/QH15 như sau:

a) Thay thế cụm từ "an ninh, an toàn thông tin" bằng cụm từ "an ninh mạng" tại khoản 2 Điều 33;

b) Thay thế cụm từ "an toàn, an ninh dữ liệu" bằng cụm từ "an ninh dữ liệu" tại khoản 4 Điều 25;

c) Bỏ cụm từ "an toàn thông tin mạng," tại khoản 4 Điều 39;

d) Bỏ cụm từ ", an toàn thông tin" tại khoản 4 Điều 25, khoản 2 Điều 33;

đ) Bỏ cụm từ "pháp luật về an toàn thông tin mạng," tại khoản 4 Điều 43.

6. Thay thế, bỏ một số cụm từ tại Luật Di sản văn hoá số 45/2024/QH15 đã được sửa đổi, bổ sung một số điều theo Luật số 84/2025/QH15 như sau:

a) Thay thế cụm từ "an toàn thông tin mạng" bằng cụm từ "an ninh mạng" tại khoản 4 Điều 59;

b) Bỏ cụm từ "an toàn thông tin mạng," tại điểm c khoản 2 Điều 86.

7. Thay thế, bỏ một số cụm từ tại Luật Viễn thông số 24/2023/QH15 đã được sửa đổi, bổ sung một số điều theo Luật số 47/2024/QH15 như sau:

a) Thay thế cụm từ "an toàn thông tin mạng" bằng cụm từ "an ninh mạng" tại khoản 8 Điều 5;

b) Bỏ cụm từ ", an toàn thông tin mạng" tại khoản 1 Điều 5, điểm c khoản 2 Điều 38;

c) Bỏ cụm từ "an toàn thông tin mạng," tại khoản 2 Điều 21, điểm b khoản 2 Điều 29.

8. Thay thế, bỏ một số cụm từ tại Luật Giao dịch điện tử số 20/2023/QH15 đã được sửa đổi, bổ sung một số điều theo Luật số 60/2024/QH15 như sau:

a) Thay thế cụm từ "an toàn thông tin mạng" bằng cụm từ "an ninh mạng" tại điểm c khoản 1 Điều 20, khoản 2 Điều 21, điểm c khoản 1 Điều 29,

khoản 6 Điều 30, khoản 4 Điều 44, điểm a khoản 4 Điều 46, điểm c khoản 1 Điều 47;

b) Bỏ cụm từ "an toàn thông tin mạng và" tại tên Điều 5;

c) Bỏ cụm từ "an toàn thông tin mạng," tại điểm d khoản 1 Điều 42, điểm a khoản 1 Điều 47;

d) Bỏ cụm từ "pháp luật về an toàn thông tin mạng," tại khoản 1 Điều 5.

9. Thay thế cụm từ "an toàn thông tin mạng" bằng cụm từ "an ninh mạng" tại điểm b khoản 2 Điều 12 của Luật Thuế thu nhập doanh nghiệp số 67/2025/QH15; tại khoản 1 Điều 169 của Luật Đất đai số 31/2024/QH15 đã được sửa đổi, bổ sung một số điều theo Luật số 43/2024/QH15, Luật số 47/2024/QH15 và Luật số 58/2024/QH15.

10. Thay thế cụm từ "an toàn thông tin" bằng cụm từ "an ninh mạng" tại điểm c khoản 3 Điều 36 của Luật Cư trú số 68/2020/QH14 đã được sửa đổi, bổ sung một số điều theo Luật số 59/2024/QH15:

11. Thay thế cụm từ "an toàn, an ninh thông tin" bằng cụm từ "an ninh mạng" tại điểm a khoản 3 Điều 7 của Luật Tài nguyên nước số 28/2023/QH15.

12. Bỏ cụm từ "an toàn thông tin mạng;" tại điểm đ khoản 1 Điều 24 của Luật Xử lý vi phạm hành chính số 15/2012/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 54/2014/QH13, Luật số 18/2017/QH14, Luật số 67/2020/QH14, Luật số 09/2022/QH15, Luật số 11/2022/QH15, Luật số 56/2024/QH15 và Luật số 88/2025/QH15.

13. Bỏ cụm từ "an toàn thông tin mạng," tại khoản 6 Điều 16 của Luật Công an nhân dân số 37/2018/QH14 đã được sửa đổi, bổ sung một số điều theo Luật số 21/2023/QH15, Luật số 30/2023/QH15, Luật số 38/2024/QH15, Luật số 52/2024/QH15 và Luật số 86/2025/QH15; tại khoản 1 Điều 66 của Luật Bầu cử đại biểu Quốc hội và đại biểu Hội đồng nhân dân số 85/2015/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 83/2025/QH15.

14. Bỏ cụm từ ", an toàn thông tin" tại khoản 3 Điều 136 của Luật Tòa án nhân dân số 34/2024/QH15 đã được sửa đổi, bổ sung một số điều theo Luật số 81/2025/QH15; tại khoản 1 Điều 26 của Luật Điện lực số 61/2024/QH15.

15. Bỏ cụm từ "an toàn thông tin," tại khoản 8 Điều 29 và cụm từ "an toàn thông tin và" tại khoản 2, khoản 7 Điều 29 của Luật Hóa chất số 69/2025/QH15

16. Bỏ cụm từ "an toàn thông tin," tại khoản 3 Điều 51 khoản 1 và khoản 5 Điều 52 của Luật Đấu thầu số 22/2023/QH15 đã được sửa đổi, bổ sung một số điều theo Luật số 90/2025/QH15; tại điểm e khoản 1 Điều 23 của Luật Phòng thủ dân sự số 18/2023/QH15 đã được sửa đổi, bổ sung một số điều theo Luật số 98/2025/QH15.

17. Bỏ cụm từ ", pháp luật về bảo đảm an toàn thông tin" tại khoản 4 Điều 7 của Luật Năng lượng nguyên tử số 94/2025/QH15.

18. Bãi bỏ khoản 3 Điều 49 của Luật Thư viện số 46/2019/QH14.

Điều 44. Hiệu lực thi hành

1. Luật này có hiệu lực thi hành từ ngày 01 tháng 7 năm 2026.

2. Luật An toàn thông tin mạng số 86/2015/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 35/2018/QH14 và Luật An ninh mạng số 24/2018/QH14 hết hiệu lực kể từ ngày Luật này có hiệu lực thi hành, trừ trường hợp quy định tại Điều 45 của Luật này.

Điều 45. Điều khoản chuyển tiếp

1. Hệ thống thông tin đã được xác định cấp độ theo quy định của Luật An toàn thông tin mạng số 86/2015/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 35/2018/QH14 tiếp tục được xác định cấp độ tương ứng theo quy định của Luật này; trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành phải bổ sung điều kiện, tiêu chuẩn, biện pháp bảo vệ an ninh mạng tương ứng với cấp độ theo quy định của Luật này; trường hợp điều chỉnh cấp độ hệ thống thông tin thì thực hiện theo quy định của Luật này.

2. Các loại giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng, mật mã dân sự theo quy định của Luật An toàn thông tin mạng số 86/2015/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 35/2018/QH14 đã được cấp trước ngày Luật này có hiệu lực thi hành có giá trị sử dụng đến hết thời hạn được ghi trên giấy phép; trường hợp cấp đổi sau ngày Luật này có hiệu lực thi hành thì thực hiện theo quy định của Luật này.

3. Các sản phẩm, dịch vụ, giải pháp, phương tiện kỹ thuật bảo đảm an toàn thông tin mạng theo quy định của Luật An toàn thông tin mạng số 86/2015/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 35/2018/QH14 đã được đưa vào sử dụng trước ngày Luật này có hiệu lực thi hành tiếp tục được sử dụng; trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành phải thay thế hoặc nâng cấp để đáp ứng các điều kiện an ninh mạng theo quy định của Luật này.

Luật này được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam khóa XV, Kỳ họp thứ 10 thông qua ngày tháng 12 năm 2025.

CHỦ TỊCH QUỐC HỘI

Trần Thanh Mẫn