LUẬT
AN TOÀN THÔNG TIN MẠNG

Luật này đã được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam khóa XIII, kỳ họp thứ 10 thông qua ngày 19 tháng 11 năm 2015 và có hiệu lực thi hành từ ngày 01 tháng 7 năm 2016.

Điều 1. Phạm vi điều chỉnh

Luật này quy định về hoạt động an toàn thông tin mạng, quyền, trách nhiệm của cơ quan, tổ chức, cá nhân trong việc bảo đảm an toàn thông tin mạng; mật mã dân sự; tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin mạng; kinh doanh trong lĩnh vực an toàn thông tin mạng; phát triển nguồn nhân lực an toàn thông tin mạng; quản lý nhà nước về an toàn thông tin mạng.

Điều 4. Nguyên tắc bảo đảm an toàn thông tin mạng

1. Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng. Hoạt động an toàn thông tin mạng của cơ quan, tổ chức, cá nhân phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội.

2. Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác.

3. Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức.

4. Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

Điều 5. Chính sách của Nhà nước về an toàn thông tin mạng

1. Đẩy mạnh đào tạo, phát triển nguồn nhân lực và xây dựng cơ sở hạ tầng, kỹ thuật an toàn thông tin mạng đáp ứng yêu cầu ổn định chính trị, phát triển kinh tế - xã hội, bảo đảm quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội.

2. Khuyến khích nghiên cứu, phát triển, áp dụng biện pháp kỹ thuật, công nghệ, hỗ trợ xuất khẩu, mở rộng thị trường cho sản phẩm, dịch vụ an toàn thông tin mạng do tổ chức, cá nhân trong nước sản xuất, cung cấp; tạo điều kiện nhập khẩu sản phẩm, công nghệ hiện đại mà tổ chức, cá nhân trong nước chưa có năng lực sản xuất, cung cấp.

3. Bảo đảm môi trường cạnh tranh lành mạnh trong hoạt động kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng; khuyến khích, tạo điều kiện cho tổ chức, cá nhân tham gia đầu tư, nghiên cứu, phát triển và cung cấp sản phẩm, dịch vụ an toàn thông tin mạng.

4. Nhà nước bố trí kinh phí để bảo đảm an toàn thông tin mạng của cơ quan nhà nước và an toàn thông tin mạng cho hệ thống thông tin quan trọng quốc gia.

Điều 7. Các hành vi bị nghiêm cấm

1. Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật.

2. Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng.

3. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin.

4. Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

5. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

6. Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; 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.

Điều 8. Xử lý vi phạm pháp luật về an toàn thông tin mạng

Người nào có hành vi vi phạm quy định của Luật này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử phạt vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự; nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật.

Điều 10. Quản lý gửi thông tin

1. Việc gửi thông tin trên mạng phải bảo đảm các yêu cầu sau đây:

a) Không giả mạo nguồn gốc gửi thông tin;

b) Tuân thủ quy định của Luật này và quy định khác của pháp luật có liên quan.

2. Tổ chức, cá nhân không được gửi thông tin mang tính thương mại vào địa chỉ điện tử của người tiếp nhận khi chưa được người tiếp nhận đồng ý hoặc khi người tiếp nhận đã từ chối, trừ trường hợp người tiếp nhận có nghĩa vụ phải tiếp nhận thông tin theo quy định của pháp luật.

3. Doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ ứng dụng viễn thông và doanh nghiệp cung cấp dịch vụ công nghệ thông tin gửi thông tin có trách nhiệm sau đây:

a) Tuân thủ quy định của pháp luật về lưu trữ thông tin, bảo vệ thông tin cá nhân, thông tin riêng của tổ chức, cá nhân;

b) Áp dụng biện pháp ngăn chặn, xử lý khi nhận được thông báo của tổ chức, cá nhân về việc gửi thông tin vi phạm quy định của pháp luật;

c) Có phương thức để người tiếp nhận thông tin có khả năng từ chối việc tiếp nhận thông tin;

d) Cung cấp điều kiện kỹ thuật và nghiệp vụ cần thiết để cơ quan nhà nước có thẩm quyền thực hiện nhiệm vụ quản lý, bảo đảm an toàn thông tin mạng khi có yêu cầu.

Điều 15. Trách nhiệm của cơ quan, tổ chức, cá nhân trong bảo đảm an toàn thông tin mạng

1. Cơ quan, tổ chức, cá nhân tham gia hoạt động an toàn thông tin mạng có trách nhiệm phối hợp với cơ quan nhà nước có thẩm quyền và tổ chức, cá nhân khác trong việc bảo đảm an toàn thông tin mạng.

2. Cơ quan, tổ chức, cá nhân sử dụng dịch vụ trên mạng có trách nhiệm thông báo kịp thời cho doanh nghiệp cung cấp dịch vụ hoặc bộ phận chuyên trách ứng cứu sự cố khi phát hiện các hành vi phá hoại hoặc sự cố an toàn thông tin mạng.

Điều 16. Nguyên tắc bảo vệ thông tin cá nhân trên mạng

1. Cá nhân tự bảo vệ thông tin cá nhân của mình và tuân thủ quy định của pháp luật về cung cấp thông tin cá nhân khi sử dụng dịch vụ trên mạng.

2. Cơ quan, tổ chức, cá nhân xử lý thông tin cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng đối với thông tin do mình xử lý.

3. Tổ chức, cá nhân xử lý thông tin cá nhân phải xây dựng và công bố công khai biện pháp xử lý, bảo vệ thông tin cá nhân của tổ chức, cá nhân mình.

4. Việc bảo vệ thông tin cá nhân thực hiện theo quy định của Luật này và quy định khác của pháp luật có liên quan.

5. Việc xử lý thông tin cá nhân phục vụ mục đích bảo đảm quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội hoặc không nhằm mục đích thương mại được thực hiện theo quy định khác của pháp luật có liên quan.

Điều 17. Thu thập và sử dụng thông tin cá nhân

1. Tổ chức, cá nhân xử lý thông tin cá nhân có trách nhiệm sau đây:

a) Tiến hành thu thập thông tin cá nhân sau khi có sự đồng ý của chủ thể thông tin cá nhân về phạm vi, mục đích của việc thu thập và sử dụng thông tin đó;

b) Chỉ sử dụng thông tin cá nhân đã thu thập vào mục đích khác mục đích ban đầu sau khi có sự đồng ý của chủ thể thông tin cá nhân;

c) Không được cung cấp, chia sẻ, phát tán thông tin cá nhân mà mình đã thu thập, tiếp cận, kiểm soát cho bên thứ ba, trừ trường hợp có sự đồng ý của chủ thể thông tin cá nhân đó hoặc theo yêu cầu của cơ quan nhà nước có thẩm quyền.

2. Cơ quan nhà nước chịu trách nhiệm bảo mật, lưu trữ thông tin cá nhân do mình thu thập.

3. Chủ thể thông tin cá nhân có quyền yêu cầu tổ chức, cá nhân xử lý thông tin cá nhân cung cấp thông tin cá nhân của mình mà tổ chức, cá nhân đó đã thu thập, lưu trữ.

Điều 52. Trách nhiệm quản lý nhà nước về an toàn thông tin mạng

1. Chính phủ thống nhất quản lý nhà nước về an toàn thông tin mạng.

2. Bộ Thông tin và Truyền thông chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an toàn thông tin mạng, có nhiệm vụ, quyền hạn sau đây:

a) Ban hành hoặc xây dựng, trình cấp có thẩm quyền ban hành văn bản quy phạm pháp luật, chiến lược, quy hoạch, kế hoạch, tiêu chuẩn quốc gia, quy chuẩn kỹ thuật quốc gia về an toàn thông tin mạng;

b) Thẩm định về an toàn thông tin mạng trong hồ sơ thiết kế hệ thống thông tin;

c) Quản lý công tác giám sát an toàn hệ thống thông tin trên toàn quốc, trừ hệ thống thông tin quy định tại điểm c khoản 3 và điểm b khoản 5 Điều này;

d) Quản lý công tác đánh giá về an toàn thông tin mạng;

đ) Cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng, Giấy phép nhập khẩu sản phẩm an toàn thông tin, trừ sản phẩm, dịch vụ mật mã dân sự;

e) Nghiên cứu, ứng dụng khoa học và công nghệ về an toàn thông tin mạng; đào tạo, bồi dưỡng, phát triển nguồn nhân lực;

g) Quản lý và thực hiện hợp tác quốc tế về an toàn thông tin mạng;

h) Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về an toàn thông tin mạng;

i) Chủ trì, phối hợp với bộ, ngành, Ủy ban nhân dân cấp tỉnh và doanh nghiệp có liên quan trong việc bảo đảm an toàn thông tin mạng;

k) Tổ chức tuyên truyền, phổ biến pháp luật về an toàn thông tin mạng;

l) Định kỳ hằng năm báo cáo Chính phủ về hoạt động an toàn thông tin mạng.

3. Bộ Quốc phòng có nhiệm vụ, quyền hạn sau đây:

a) Ban hành hoặc xây dựng, trình cấp có thẩm quyền ban hành văn bản quy phạm pháp luật, chiến lược, quy hoạch, kế hoạch, tiêu chuẩn quốc gia, quy chuẩn kỹ thuật quốc gia về an toàn thông tin mạng thuộc lĩnh vực do Bộ Quốc phòng quản lý;

b) Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật trong hoạt động bảo đảm an toàn thông tin mạng thuộc lĩnh vực do Bộ Quốc phòng quản lý;

c) Thực hiện quản lý công tác giám sát an toàn hệ thống thông tin thuộc Bộ Quốc phòng.

4. Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng thực hiện quản lý nhà nước về mật mã dân sự, có nhiệm vụ sau đây:

a) Xây dựng, trình cấp có thẩm quyền ban hành văn bản quy phạm pháp luật về quản lý mật mã dân sự;

b) Chủ trì, phối hợp với bộ, ngành có liên quan xây dựng, trình cơ quan nhà nước có thẩm quyền ban hành tiêu chuẩn quốc gia, quy chuẩn kỹ thuật quốc gia đối với sản phẩm, dịch vụ mật mã dân sự;

c) Quản lý hoạt động kinh doanh, sử dụng mật mã dân sự; quản lý chất lượng sản phẩm, dịch vụ mật mã dân sự; quản lý công tác đánh giá, công bố hợp chuẩn, hợp quy đối với sản phẩm, dịch vụ mật mã dân sự;

d) Xây dựng, trình cấp có thẩm quyền ban hành Danh mục sản phẩm, dịch vụ mật mã dân sự và Danh mục sản phẩm mật mã dân sự xuất khẩu, nhập khẩu theo giấy phép;

đ) Cấp Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự, Giấy phép xuất khẩu, nhập khẩu sản phẩm mật mã dân sự;

e) Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật trong hoạt động kinh doanh, sử dụng mật mã dân sự;

g) Hợp tác quốc tế về mật mã dân sự.

5. Bộ Công an có nhiệm vụ, quyền hạn sau đây:

a) Chủ trì, phối hợp với bộ, ngành có liên quan xây dựng và trình cấp có thẩm quyền ban hành hoặc ban hành theo thẩm quyền và hướng dẫn thực hiện văn bản quy phạm pháp luật về bảo vệ bí mật nhà nước, phòng, chống tội phạm mạng, lợi dụng mạng để xâm phạm an ninh quốc gia, trật tự, an toàn xã hội;

b) Thực hiện quản lý công tác giám sát an toàn hệ thống thông tin thuộc Bộ Công an;

c) Tổ chức, chỉ đạo, triển khai công tác phòng, chống tội phạm, tổ chức điều tra tội phạm mạng và hành vi vi phạm pháp luật khác trong lĩnh vực an toàn thông tin mạng;

d) Phối hợp với Bộ Thông tin và Truyền thông, bộ, ngành có liên quan kiểm tra, thanh tra về an toàn thông tin mạng, xử lý vi phạm pháp luật về an toàn thông tin mạng theo thẩm quyền.

6. Bộ Nội vụ có trách nhiệm tổ chức đào tạo, bồi dưỡng kiến thức, nghiệp vụ an toàn thông tin mạng cho cán bộ, công chức, viên chức.

7. Bộ Giáo dục và Đào tạo có trách nhiệm tổ chức đào tạo, phổ biến kiến thức về an toàn thông tin mạng trong cơ sở giáo dục đại học.

8. Bộ Lao động - Thương binh và Xã hội có trách nhiệm tổ chức đào tạo, bồi dưỡng, phổ biến kiến thức về an toàn thông tin mạng trong cơ sở giáo dục nghề nghiệp.

9. Bộ Tài chính có trách nhiệm hướng dẫn, bố trí kinh phí thực hiện nhiệm vụ bảo đảm an toàn thông tin mạng theo quy định của pháp luật.

10. Bộ, cơ quan ngang bộ trong phạm vi nhiệm vụ, quyền hạn của mình có trách nhiệm quản lý an toàn thông tin mạng của ngành mình và phối hợp với Bộ Thông tin và Truyền thông thực hiện quản lý nhà nước về an toàn thông tin mạng.

11. Ủy ban nhân dân cấp tỉnh trong phạm vi nhiệm vụ, quyền hạn của mình thực hiện quản lý nhà nước về an toàn thông tin mạng ở địa phương.