QUỐC HỘI

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Luật số: 86/2015/QH13

LUẬT
AN TOÀN THÔNG TIN MẠNG

Căn cứ Hiến pháp nước Cộng hòa xã hội chủ nghĩa Việt Nam;

Quốc hội ban hành Luật an toàn thông tin mạng.

Chương I
NHỮNG QUY ĐỊNH CHUNG

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 2. Đối tượng áp dụng

Luật này áp dụng đối với cơ quan, tổ chức, cá nhân Việt Nam, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động an toàn thông tin mạng tại Việt Nam.

Điều 3. Giải thích từ ngữ

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

1. *An toàn thông tin mạng* là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

2. *Mạng* là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

3. *Hệ thống thông tin* là tập hợp phần cứng, phần mềm và cơ sở 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 mạng.

4. *Hệ thống thông tin quan trọng quốc gia* là hệ thống thông tin mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia.

5. *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.

6. *Xâm phạm an toàn thông tin mạng* là hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, phá hoại trái phép thông tin, hệ thống thông tin.

7. *Sự cố an toàn thông tin mạng* là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

8. *Rủi ro an toàn thông tin mạng* là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng.

9. *Đánh giá rủi ro an toàn thông tin mạng* là việc phát hiện, phân tích, ước lượng mức độ tổn hại, mối đe dọa đối với thông tin, hệ thống thông tin.

10. *Quản lý rủi ro an toàn thông tin mạng* là việc đưa ra các biện pháp nhằm giảm thiểu rủi ro an toàn thông tin mạng.

11. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay 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.

12. *Hệ thống lọc phần mềm độc hại* là tập hợp phần cứng, phần mềm được kết nối vào mạng để phát hiện, ngăn chặn, lọc và thống kê phần mềm độc hại.

13. *Địa chỉ điện tử* là địa chỉ được sử dụng để gửi, nhận thông tin trên mạng bao gồm địa chỉ thư điện tử, số điện thoại, địa chỉ Internet và hình thức tương tự khác.

14. *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 mạng.

15. *Thông tin cá nhân* là thông tin gắn với việc xác định danh tính của một người cụ thể.

16. *Chủ thể thông tin cá nhân* là người được xác định từ thông tin cá nhân đó.

17. *Xử lý thông tin cá nhân* là việc thực hiện một hoặc một số thao tác thu thập, biên tập, sử dụng, lưu trữ, cung cấp, chia sẻ, phát tán thông tin cá nhân trên mạng nhằm mục đích thương mại.

18. *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.

19. *Sản phẩm an toàn thông tin mạng* là phần cứng, phần mềm có chức năng bảo vệ thông tin, hệ thống thông tin.

20. *Dịch vụ an toàn thông tin mạng* là dịch vụ bảo vệ thông tin, hệ thống thông tin.

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 6. Hợp tác quốc tế về an toàn thông tin mạng

1. Hợp tác quốc tế về an toàn thông tin mạng phải tuân thủ các nguyên tắc sau đây:

a) Tôn trọng độc lập, chủ quyền và toàn vẹn lãnh thổ quốc gia, không can thiệp vào công việc nội bộ của nhau, bình đẳng và các bên cùng có lợi;

b) Phù hợp với quy định của pháp luật Việt Nam, điều ước quốc tế mà Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên.

2. Nội dung hợp tác quốc tế về an toàn thông tin mạng gồm:

a) Hợp tác quốc tế trong đào tạo, nghiên cứu và ứng dụng khoa học, kỹ thuật, công nghệ về an toàn thông tin mạng;

b) Hợp tác quốc tế trong phòng, chống hành vi vi phạm pháp luật về an toàn thông tin mạng; điều tra, xử lý sự cố an toàn thông tin mạng, ngăn chặn hoạt động lợi dụng mạng để khủng bố;

c) Hoạt động hợp tác quốc tế khác về an toàn thông tin mạng.

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.

Chương II
BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Mục 1
BẢO VỆ THÔNG TIN MẠNG

Điều 9. Phân loại thông tin

1. Cơ quan, tổ chức sở hữu thông tin phân loại thông tin theo thuộc tính bí mật để có biện pháp bảo vệ phù hợp.

2. Thông tin thuộc phạm vi bí mật nhà nước được phân loại và bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước.

Cơ quan, tổ chức sử dụng thông tin đã phân loại và chưa phân loại trong hoạt động thuộc lĩnh vực của mình phải có trách nhiệm xây dựng quy định, thủ tục để xử lý thông tin; xác định nội dung và phương pháp ghi truy nhập được phép vào thông tin đã được phân loại.

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

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

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

3. 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 Thông tin và Truyền thông chủ trì, phối hợp với Bộ Quốc phòng, Bộ Công an và Bộ, ngành có liên quan tổ chức phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại gây ảnh hưởng đến quốc phòng, an ninh quốc gia.