**TÀI LIỆU MỘT SỐ**

**VẤN ĐỀ CƠ BẢN VỀ**

**LUẬT AN NINH MẠNG**

**TÀI LIỆU GIỚI THIỆU, TUYÊN TRUYỀN LUẬT AN NINH MẠNG**

[1. Hoạt động chống phá, phản đối Luật An ninh mạng đang diễn ra như thế nào? 3](#_Toc516827736)

[2. Tại sao phải ban hành Luật An ninh mạng? 5](#_Toc516827737)

[3. Luật An ninh mạng có được xây dựng công phu, kỹ lưỡng không? 7](#_Toc516827738)

[4. Nội dung cơ bản của Luật An ninh mạng là gì? 8](#_Toc516827739)

[5. Phạm vi điều chỉnh của Luật An ninh mạng như thế nào? 10](#_Toc516827740)

[6. Luật An ninh mạng nghiêm cấm những hành vi nào? 11](#_Toc516827741)

[7. Cá nhân có trách nhiệm và được hưởng quyền lợi gì theo quy định của Luật An ninh mạng? 13](#_Toc516827742)

[8. Doanh nghiệp có trách nhiệm và quyền lợi gì theo quy định của Luật An ninh mạng? 15](#_Toc516827743)

[9. Luật An ninh mạng quy định bảo vệ thông tin cá nhân như thế nào? 17](#_Toc516827744)

[10. Luật An ninh mạng có kiểm soát toàn bộ thông tin cá nhân của công dân hay không? 17](#_Toc516827745)

[11. Các thông tin nào trên không gian mạng bị coi là vi phạm pháp luật và bị xử lý? 18](#_Toc516827746)

[12. Thông tin vi phạm pháp luật trên không gian mạng đến đánh giá, quyết định như thế nào? 19](#_Toc516827747)

[13. Thông tin vi phạm pháp luật trên không gian mạng được xử lý theo quy định nào? 19](#_Toc516827748)

[14. Lực lượng chuyên trách bảo vệ an ninh mạng có lạm quyền trong xử lý thông tin vi phạm pháp luật trên không gian mạng hay không? 20](#_Toc516827749)

[15. Luật An ninh mạng quy định như thế nào về lưu trữ dữ liệu người sử dụng trong nước? 20](#_Toc516827750)

[16. Doanh nghiệp nào thuộc diện điều chỉnh của quy định lưu trữ dữ liệu trong nước? 21](#_Toc516827751)

[17. Dữ liệu nào phải lưu trữ ở Việt Nam? 21](#_Toc516827752)

[18. Đã có quốc gia nào trên thế giới quy định lưu trữ dữ liệu trong nước chưa? 21](#_Toc516827753)

[19. Quy định trên có vi phạm các cam kết quốc tế mà Việt Nam tham gia hay không? 22](#_Toc516827754)

[20. Có phải chỉ Việt Nam mới quy định các doanh nghiệp nước ngoài cung cấp dịch vụ trên không gian mạng phải cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng? 23](#_Toc516827755)

[21. Trước Việt Nam, Facebook, Google đã đặt văn phòng đại diện ở đâu chưa? 23](#_Toc516827756)

[22. Quy định lưu trữ dữ liệu có cản trở Facebook, Google hoạt động không? 23](#_Toc516827757)

[23. Toàn bộ hệ thống thông tin trong nước có phải tiến hành thẩm định an ninh mạng theo quy định tại Điều 11 Luật An ninh mạng không? 24](#_Toc516827758)

[24. Luật An ninh mạng có gây cản trở hoạt động của doanh nghiệp, tạo giấy phép con hay không? 24](#_Toc516827759)

[25. Luật An ninh mạng quy định phòng, chống tấn công mạng như thế nào? 24](#_Toc516827760)

[26. Hệ thống thông tin quan trọng về an ninh quốc gia được bảo vệ như thế nào trong Luật An ninh mạng? 25](#_Toc516827761)

[27. Đào tạo nguồn nhân lực an ninh mạng chất lượng cao được quy định như thế nào trong Luật An ninh mạng? 26](#_Toc516827762)

[28. Chính sách của nước ta về an ninh mạng như thế nào? 26](#_Toc516827763)

# 1.Tại sao phải ban hành Luật An ninh mạng?

**TRẢ LỜI:**

Với sự phát triển như vũ bão của khoa học công nghệ, không gian mạng trở thành một bộ phận cấu thành không thể thiếu và đóng vai trò quan trọng trong xây dựng xã hội thông tin và phát triển kinh tế tri thức. Sự phát triển bùng nổ của công nghệ mang tính đột phá như trí tuệ nhân tạo, Internet của vạn vật, máy tính lượng tử, điện toán đám mây, dữ liệu lớn, dữ liệu nhanh… đã làm không gian mạng thay đổi sâu sắc cả về chất và lượng, được dự báo sẽ mang lại những lợi ích chưa từng có cho xã hội loài người nhưng cũng làm xuất hiện những nguy cơ tiềm ẩn vô cùng lớn. Nhiều quốc gia đã nhận thức rõ về những mối đe dọa đối với an ninh mạng, coi đây là thách thức mới, mối đe dọa mới có tầm quan trọng và nguy hiểm cao nên đã cụ thể hóa thành các văn bản chính sách, văn bản pháp luật như luật hoặc văn bản dưới luật tại hơn 80 quốc gia, tổ chức, liên minh quốc tế như Mỹ, Anh, Đức, Hà Lan, Pháp, Canada, Hàn Quốc, NATO... nhằm tạo ra các thiết chế, cơ sở pháp lý chống lại các nguy cơ đe dọa đến an ninh quốc gia từ không gian mạng; thành lập các lực lượng chuyên trách về an ninh mạng, tình báo mạng, chiến tranh mạng, phòng chống khủng bố mạng và tội phạm mạng. Chỉ trong vòng 06 năm trở lại đây, đã có 23 quốc gia trên thế giới ban hành trên 40 văn bản luật về an ninh mạng.

Ở nước ta, ứng dụng và phát triển mạnh mẽ công nghệ thông tin trong các lĩnh vực của đời sống đã góp phần to lớn đẩy nhanh quá trình công nghiệp hóa, hiện đại hóa đất nước, phát triển kinh tế, văn hóa, xã hội, nâng cao chất lượng y tế, giáo dục, phát huy sức sáng tạo và quyền làm chủ của nhân dân, giữ vững an ninh, quốc phòng. Tuy nhiên, vẫn còn những tồn tại, hạn chế về an ninh mạng cần khắc phục như:

(1) Tiềm lực quốc gia về an ninh mạng của nước ta chưa đủ mạnh, chưa huy động, khai thác được sức mạnh tổng hợp để đối phó với các mối đe dọa trên không gian mạng.

(2) Không gian mạng và một số loại hình dịch vụ, ứng dụng đang bị các thế lực thù địch, phản động sử dụng thực hiện âm mưu tiến hành “cách mạng màu”, “cách mạng đường phố”, “diễn biến hòa bình” nhằm xóa bỏ chế độ chính trị ở nước ta. Tình trạng đăng tải thông tin sai sự thật, làm nhục, vu khống tổ chức, cá nhân tràn lan trên không gian mạng nhưng chưa có biện pháp quản lý hữu hiệu, dẫn tới nhiều hậu quả đáng tiếc về nhân mạng, tinh thần, thậm chí ảnh hưởng tới chủ quyền, lợi ích, an ninh quốc gia, trật tự an toàn xã hội.

(3) Ngày càng xuất hiện nhiều cuộc tấn công mạng với quy mô lớn, cường độ cao, gia tăng về tính chất nghiêm trọng, mức độ nguy hiểm đe dọa trực tiếp đến an ninh quốc gia và trật tự an toàn xã hội. Khủng bố mạng nổi lên như một thách thức đe dọa nghiêm trọng tới an ninh quốc gia. Hoạt động phạm tội trên không gian mạng ngày càng gia tăng về số vụ, thủ đoạn tinh vi gây thiệt hại nghiêm trọng về kinh tế, ảnh hưởng đến tư tưởng, văn hóa, xã hội.

(4) Hệ thống thông tin quan trọng về an ninh quốc gia chưa được xác định và bảo vệ bằng các biện pháp tương xứng. Do chưa xác định nội hàm sự cố an ninh mạng nên khi xảy ra các sự cố gây nguy hại, ảnh hưởng tới chủ quyền, lợi ích, an ninh quốc gia, trật tự an toàn xã hội, việc triển khai hoạt động ứng phó, xử lý, khắc phục hậu quả của cơ quan chức năng có liên quan rất lúng túng, chưa có quy trình thống nhất, cơ quan có trách nhiệm bảo vệ an ninh mạng chưa thể chủ động triển khai các biện pháp, phương án phù hợp.

(5) Tình hình lộ, lọt bí mật nhà nước qua không gian mạng rất đáng lo ngại, nhiều văn bản thuộc bí mật nhà nước bị đăng tải trên không gian mạng. Một trong những nguyên nhân quan trọng dẫn tới tình trạng trên là do nhận thức của các cơ quan, doanh nghiệp và cá nhân về bảo vệ bí mật nhà nước trên không gian mạng còn hạn chế, ý thức trách nhiệm của nhiều cán bộ, nhân viên trong bảo mật thông tin trên không gian mạng còn chưa cao, chế tài xử phạt chưa đủ răn đe.

(6) Sự phụ thuộc vào thiết bị công nghệ thông tin có nguồn gốc nước ngoài. Không gian mạng đang ứng dụng sâu rộng vào mọi lĩnh vực của đời sống xã hội, tuy nhiên sự phụ thuộc vào trang thiết bị công nghệ thông tin xuất xứ từ nước ngoài, là mối đe dọa tiềm tàng đối với an ninh mạng nếu xảy ra xung đột. Để tránh bị tin tặc tấn công, thu thập thông tin, hoạt động tình báo, một số sản phẩm, dịch vụ mạng cần đáp ứng các tiêu chuẩn, quy chuẩn nhất định, nhất là khi các sản phẩm, dịch vụ này được sử dụng trong hệ thống thông tin quan trọng và an ninh quốc gia, địa điểm cơ yếu, bảo mật, chứa đựng bí mật nhà nước.

(7) Hệ thống văn bảnquy phạm pháp luật về an ninh mạng chưa được xây dựng, các văn bản hiện hành chưa đáp ứng được yêu cầu phòng ngừa, đấu tranh, xử lý các hành vi sử dụng không gian mạng vi phạm pháp luật.

Thực trạng trên đã đặt đất nước ta trước những nguy cơ sau:

Một là, Sự phát triển của mạng xã hội góp phần quan trọng phát triển kinh tế - xã hội, song cũng tạo môi trường thuận lợi cho các hoạt động tác động, chuyển hóa chính trị, khủng bố ở nhiều quốc gia và vùng lãnh thổ.

Hai là, Sự phát triển của trí tuệ nhân tạo đã và đang tạo ra những thành tựu khoa học công nghệ vượt trội, đóng vai trò ngày càng quan trọng trong nhiều lĩnh vực của đời sống xã hội nhưng cũng được dự báo sẽ gây nên “thảm họa” nếu không được kiểm soát chặt chẽ.

Ba là, Các thiết bị kết nối internet ngày càng phổ biến không chỉ mang lại những lợi ích to lớn cho cuộc sống con người, phát triển kinh tế - xã hội, bảo đảm quốc phòng - an ninh mà còn có thể bị sử dụng để tiến hành các cuộc tấn công mạng quy mô lớn.

Bốn là, Các cuộc tấn công mạng có chủ đích (Advanced Peristent Threat - APT) không chỉ có thể phá hoại các mục tiêu, công trình quan trọng về an ninh quốc gia mà còn chiếm đoạt thông tin, tài liệu bí mật, chiếm đoạt để sử dụng các hệ thống dữ liệu lớn, dữ liệu nhanh phục vụ các ý đồ chính trị và hoạt động phạm tội.

Thực trạng, nguy cơ trên đã đặt ra yêu cầu bức thiết phải xây dựng và ban hành văn bản luật về an ninh mạng để phòng ngừa, đấu tranh, xử lý các hành vi sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

# 2. Nội dung cơ bản của Luật An ninh mạng là gì?

**TRẢ LỜI:**

Luật An ninh mạng gồm 7 chương, 43 điều, quy định những nội dung cơ bản về bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh mạng; triển khai hoạt động bảo vệ an ninh mạng và quy định trách nhiệm của cơ quan, tổ chức, cá nhân.

Luật An ninh mạng được chuẩn bị công phu, kỹ lưỡng, với sự tham gia đóng góp ý kiến của các bộ, ngành chức năng, hơn 30 doanh nghiệp viễn thông, công nghệ thông tin lớn trong nước như VNPT, FPT, BKAV; nhiều chuyên gia, tập đoàn kinh tế, viễn thông trong và ngoài nước, trong đó có Facabook, Google, Apple, Amazon, Hội đồng kinh doanh Hoa Kỳ - ASEAN, Hiệp hội điện toán đám mây Châu Á; các cơ quan đại diện nước ngoài như Mỹ, Canada, Úc, Nhật Bản… và ý kiến rộng rãi của quần chúng nhân dân.

Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia là một trong những nội dung đặc biệt quan trọng của Luật An ninh mạng. Quy định đầy đủ các biện pháp, hoạt động bảo vệ tương xứng với mức độ quan trọng của hệ thống thông tin này, trong đó nêu ra tiêu chí xác định, lĩnh vực liên quan, quy định các biện pháp như thẩm định an ninh mạng, đánh giá điều kiện, kiểm tra, giám sát an và ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.

Để bảo vệ tối đa quyền và lợi ích hợp pháp của tổ chức, cá nhân, Luật An ninh mạng đã dành 01 chương quy định đầy đủ các biện pháp phòng ngừa, đấu tranh, xử lý nhằm loại bỏ các nguy cơ đe dọa, phát hiện và xử lý hành vi vi phạm pháp luật, bao gồm: phòng ngừa, xử lý thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế; phòng, chống gián điệp mạng, bảo vệ thông tin bí mật nhà nước, bí mật công tác, thông tin cá nhân trên không gian mạng; phòng ngừa, xử lý hành vi sử dung không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh, trật tự; phòng, chống tấn công mạng; Phòng, chống khủng bố mạng; phòng, chống chiến tranh mạng; phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng; đấu tranh bảo vệ an ninh mạng. Đây là hành lang pháp lý vững chắc để người dân có thể yên tâm buôn bán, kinh doanh hay hoạt động trên không gian mạng.

Chương IV của Luật An ninh mạng tập trung quy định về triển khai hoạt động bảo vệ an ninh mạng một cách đồng bộ, thống nhất từ Trung tương tới địa phương, trọng tâm là các cơ quan nhà nước và tổ chức chính trị, quy định rõ các nội dung triển khai, hoạt động kiểm tra an ninh mạng đối với hệ thống thông tin của các cơ quan, tổ chức này. Cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế cũng là một trong những đối tượng được bảo vệ trọng điểm. Với các quy định chặt chẽ, sự tham gia đồng bộ của cơ quan nhà nước, doanh nghiệp và tổ chức, cá nhân, việc sử dụng thông tin để vu khống, làm nhục, xâm phạm danh dự, nhân phẩm, uy tín của người khác sẽ được xử lý nghiêm minh. Các hoạt động nghiên cứu, phát triển an ninh mạng, phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng nhằm bảo vệ an ninh mạng, nâng cao năng lực tự chủ về an ninh mạng và bảo vệ trẻ em trên không gian mạng cũng được quy định chi tiết trong Chương này.

Hiện nay, dữ liệu của nước ta trên không gian mạng đã và đang bị sử dụng tràn lan, với mục đích lợi nhuận mà Nhà nước chưa có đủ hành lang pháp lý để quản lý, thậm chí là bị sử dụng vào các âm mưu chính trị hoặc vi phạm pháp luật. Để quản lý chặt chẽ, bảo vệ nghiêm ngặt dữ liệu của nước ta trên không gian mạng, Luật An ninh mạng đã quy định doanh nghiệp trong và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu về thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra phải lưu trữ dữ liệu này tại Việt Nam trong thời gian theo quy định của Chính phủ.

Nguồn nhân lực bảo vệ an ninh mạng là một trong những yếu tố quyết định sự thành bại của công tác bảo vệ an ninh mạng. Chương V Luật An ninh mạng đã quy định đầy đủ các nội dung bảo đảm triển khai hoạt động bảo vệ an ninh mạn*g*, xác định lực lượng chuyên trách bảo vệ an ninh mạng, ưu tiên đào tạo nguồn nhân lực an ninh mạng chất lượng cao, chú trọng giáo dục, bồi dưỡng, phổ biến kiến thức về an ninh mạng.

Trách nhiệm của cơ quan, tổ chức, cá nhân cũng được quy định rõ trong Luật An ninh mạng, tập trung vào trách nhiệm của lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Bộ Công an, Bộ Quốc phòng. Theo chức năng, nhiệm vụ được giao, các bộ, ngành chức năng có trách nhiệm thực hiện đồng bộ các biện pháp được phân công để hướng tới một không gian mạng ít nguy cơ, hạn chế tối đa các hành vi vi phạm pháp luật trên không gian mạng.

Mặc dù nhận được chuẩn bị kỹ lưỡng, được đa số Đại biểu Quốc hội tán thành, nhưng do đây là đạo luật có quy định về phòng ngừa, đấu tranh, xử lý trực tiếp các hoạt động xâm phạm an ninh quốc gia trên không gian mạng nên vẫn còn có những ý kiến băn khoăn về nội dung Luật. Một số đối tượng chống đối đã có hoạt động tuyên truyền, kích động biểu tình, chống phá Luật An ninh mạng hòng hướng lái dư luận theo hướng bất lợi, với các luận điệu như “chống lại loài người”, “bịt miệng dân chủ”, “đàn áp bất đồng chính kiến”, “tạo rào cản kinh doanh”, “tăng chi phí cho doanh nghiệp”, “thêm giấy phép con”, “lạm quyền”, “cấm sử dụng Facebook, Google”. Xin khẳng định rằng, đây là những thông tin bại đặt, xuyên tạc, với mục đích cản trở hoặc gây tâm lý hoang mang, nghi ngờ trong quần chúng nhân dân đối với chính sách của Đảng, Nhà nước về an ninh mạng. Luật An ninh mạng không có những quy định nêu trên, không tạo rào cản, không tăng thủ tục hành chính, không cấp giấy phép con và không cản trở hoạt động bình thường, đúng luật của các tổ chức, cá nhân.

# 3. Luật An ninh mạng nghiêm cấm những hành vi nào?

**TRẢ LỜI:**

Luật An ninh mạng chỉ nghiêm cấm thực hiện các hành vi vi phạm pháp luật đã được pháp luật quy định, cụ thể:

(1) Các hành vi chống nhà nước CHXHCN Việt Nam, bao gồm sử dụng không gian mạng tổ chức, hoạt động, cấu 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, ví dụ như thông tin kích động biểu tình trái pháp luật, kích động gây rối an ninh, trật tự…

(2) Các hành vi 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;

(3) Các hành vi phát tán thông tin gây hại cho tổ chức, cá nhân, gồm: thông tin sai sự thật gây hoang mang trong nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác;

(4) Các hành vi xâm phạm trật tự an toàn xã hội như sử dụng không gian mạng để hoạt động mại dâm, tệ nạn xã hội, mua bán người; đăng tải thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe cộng đồng, xúi giục, lôi kéo, kích động người khác phạm tội. (Những hành vi này đã được quy định rải rác, cụ thể trong 29 Điều của Bộ luật Hình sự năm 2015, sửa đổi năm 2017- có danh sách chi tiết kèm theo).

(5) Các hành vi tấn công mạng, gián điệp mạng, khủng bố mạng và liên quan như sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoạt động của mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; phát tán chương trình tin học gây hại cho hoạt động của mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử.

(6) Các hành vi lợi dụng quy định này của lực lượng chuyên trách để thực hiện hành vi vi phạm pháp luật (giải quyết lo ngại về lạm quyền).

Như vậy:

- Không có quy định nào cấm Facebook, Google hoặc các nhà cung cấp dịch vụ nước ngoài hoạt động tại Việt Nam.

- Không có quy định nào ngăn cản quyền tự do ngôn luận, quyền bày tỏ quan điểm của công dân.

- Không có quy định nào cấm công dân sử dụng các dịch vụ mạng xã hội như Facebook, Google; không cấm công dântham gia hoạt động trên không gian mạng hoặc truy cập, sử dụng thông tin trên không gian mạng.

- Không có quy định nào cấm công dân khởi nghiệp, sáng tạo hay trao đổi, triển khai ý tưởng sáng tạo của mình trên không gian mạng.

Việc quy định hành vi bị nghiêm cấm như trên bảo đảm được:

*(1) Đảm bảo thống nhất trong hệ thống pháp luật****.*** Điều 8 - Các hành vi bị nghiêm cấm cụ thể hóa các hành vi cấm, hành vi vi phạm pháp luật đã được quy định trong các luật hiện hành, như: Bộ luật hình sự (29 điều); Luật Bình đăng giới (Điều 10); Luật tín ngưỡng tôn giáo (Điều 5)…

*(2)Tác dụng phòng ngừa*: Điều 8 và một số điều khác trong Luật xác định rõ những hành vi bị cấm làm ranh giới cho các hoạt động trên không gian mạng. Người dân nhận diện hành vi trái pháp luật trên không gian mạng để không vi phạm, cũng như tham gia đấu tranh, tố giác và bài trừ các hành vi này.

*(3) Góp phầnxây dựng không gian mạng an toàn, lành mạnh,* trở thành động lực quan trọng trong phát triển kinh tế - xã hội và bảo vệ an ninh quốc gia của đất nước. Điều này đặc biệt quan trọng trong bối cảnh Việt Nam đang thúc đẩy nền kinh tế số và sẵn sàng bước vào cuộc cách mạng công nghệ lần thứ 4.

*(4) Đóng góp vào các nỗ lực chung xây dựng không gian mạng toàn cầu an toàn, lành mạnh****.*** Việt Nam cũng như nhiều quốc gia trên thế giới đang phải đối mặt với vấn nạn tin giả (fake news), phát ngôn thù địch (hate speech), nhiều quốc gia như Đức, Thái Lan… đang có những bước đi rất mạnh mẽ để chống tin giả, phát ngôn thù địch trên không gian mạng. Mỹ và các nước phương Tây đang đẩy mạnh cuộc chiến chống tư tưởng hồi giáo cực đoan do IS và các tổ chức khủng bố tiến hành.

# 4. Luật An ninh mạng có kiểm soát toàn bộ thông tin cá nhân của công dân hay không?

**TRẢ LỜI:**

Trước các hoạt động vi phạm pháp luật trên không gian mạng đang diễn ra nghiêm trọng, phức tạp, yêu cầu bảo đảm cơ sở, điều kiện để điều tra, xử lý nhanh chóng, hiệu quả của lực lượng bảo vệ pháp luật là cần thiết, cấp bách, trong đó có trách nhiệm của các doanh nghiệp cung cấp dịch vụ trong và ngoài nước. Thông tin của cá nhân có hoạt động vi phạm pháp luật là một trong những loại dữ liệu quan trọng để lực lượng bảo vệ pháp luật điều tra, xử lý hành vi vi phạm pháp luật.

Điểm a, khoản 2 Điều 26 dự thảo Luật An ninh mạng quy định: “*Doanh nghiệp trong và ngoài nước khi cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Namcó trách nhiệm cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi có yêu cầu bằng văn bản để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng*”.

Như vậy, lực lượng chuyên trách bảo vệ an ninh mạng chỉ được phép tiếp cận thông tin cá nhân của người sử dụng có hoạt động vi phạm pháp luật, với trình tự, thủ tục nghiêm ngặt (bằng văn bản), được các cấp có thẩm quyền phê duyệt. Hiện nay, có nhiều thông tin trên không gian mạng cho rằng, Luật An ninh mạng yêu cầu doanh nghiệp phải cung cấp toàn bộ thông tin người dùng như thông tin cá nhân, thông tin riêng tư cho cơ quan chức năng là không chính xác.

Luật An ninh mạng đã quy định rõ ràng, chỉ trong trường hợp phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng, lực lượng chuyên trách bảo vệ an ninh mạng mới được quyền yêu cầu cung cấp thông tin người dùng.

Các quy định trong Bộ luật Tố tụng Hình sự và các văn bản có liên quan đã quy định rõ về việc quản lý, sử dụng thông tin được cung cấp để phục vụ điều tra, xử lý các hành vi vi phạm pháp luật.

# 5. Các thông tin nào trên không gian mạng bị coi là vi phạm pháp luật và bị xử lý?

**TRẢ LỜI:**

Điều 8. Các hành vi bị nghiêm cấm và Điều 15 Luật An ninh mạng đã quy định cụ thể 05 nhóm thông tin trên không gian mạng bị coi là vi phạm pháp luật theo quy định của Bộ luật Hình sự (sửa đổi 2017), gồm:

*Nhóm 1*: Thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam.

*Nhóm 2*: Thông tin trên không gian mạng có nội dung kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng

*Nhóm 3*: Thông tin trên không gian mạng có nội dung làm nhục, vu khống

*Nhóm 4*: Thông tin trên không gian mạng có nội dung xâm phạm trật tự quản lý kinh tế

*Nhóm 5*: Thông tin trên không gian mạng có nội dung sai sự thật gây hoang mang trong nhân dân, gây thiệt hại cho các hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác

Như vậy, đây đều là những thông tin có thể gây nguy hại tới an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân, được quy định trong Bộ luật Hình sự, cần phải xử lý trên không gian mạng.

# 6. Thông tin vi phạm pháp luật trên không gian mạng được xử lý theo quy định nào?

**TRẢ LỜI:**

Đạo đức xã hội luôn lên án những lời nói xấu, nói dối, nói sai sự thật.

Bộ luật Hình sự điều chỉnh các hành vi xâm phạm an ninh quốc gia, trật tự an toàn xã hội, xúc phạm nghiêm trọng danh dự, uy tín, nhân phẩm của tổ chức, cá nhân (Tội làm nhục, Tội vu khống).

Bộ luật Dân sự quy định về mức bồi thường thiệt hại đối với các hành vi xúc phạm danh dự, nhân phẩm, uy tín của pháp nhân hoặc chủ thể khác theo mức độ thiệt hại.

Tùy theo mức độ vi phạm và chứng cứ thu thập được theo quy định của pháp luật, cơ quan chức năng sẽ đề xuất xử lý theo quy định của Bộ luật Hình sự hoặc Bộ luật Dân sự.

# 7. Luật An ninh mạng quy định như thế nào về lưu trữ dữ liệu người sử dụng trong nước?

**TRẢ LỜI:**

Khoản 3 Điều 26 Luật An ninh mạng quy định:

“3. Doanh nghiệp trong và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu về thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra phải lưu trữ dữ liệu này tại Việt Nam trong thời gian theo quy định của Chính phủ.

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

# 8. Đã có quốc gia nào trên thế giới quy định lưu trữ dữ liệu trong nước chưa?

Theo thống kê sơ bộ, hiện đã có 18 quốc gia trên thế giới quy định phải lưu trữ dữ liệu ở trong nước, như Mỹ, Canada, Liên bang Nga, Pháp, Đức, Trung Quốc, Úc, Indonesia, Hi Lạp, Bulgaria, Đan Mạch, Phần Lan, Thụy Điển, Thổ Nhĩ Kỳ, Venezuela, Colombia, Argentina, Brazil. Tùy vào tình hình thực tế, các quốc gia có thể yêu cầu lưu trữ các loại dữ liệu không giống nhau.

Nhiều quốc gia trên thế giới đã áp dụng các biện pháp quyết liệt hơn như truy tố trong phỉ báng hoàng gia (Thái Lan), phạt tiền tới 60 triệu USD (Đức), yêu cầu thành lập trung tâm giải quyết tin tức xấu độc (Châu Âu), đặt trung tâm lưu trữ dữ liệu (Trung Quốc áp dụng với Apple), yêu cầu đặt máy chủ nếu không sẽ dừng hoạt động Facebook (Nga).

Tại Châu Á, nhiều quốc gia đã áp dụng chính sách quản lý chặt chẽ dữ liệu quan trọng quốc gia, trong đó có Indonesia, mới đây là Philipinnes (xác định cấp độ các loại dữ liệu quan trọng và có chính sách quản lý tương ứng với từng loại cấp độ quản lý).

Ngày 30/3/2018, vì lý do an ninh quốc gia, Bộ Ngoại giao Mỹ công bố lấy ý kiến về chính sách siết chặt kiểm soát nhập cư của Tổng thống Donald Trump, yêu cầu người nhập cảnh phải cung cấp thông tin về tài khoản mạng xã hội trong vòng 5 năm gần nhất. Đáng chú ý, không chỉ các mạng xã hội của Mỹ như Facebook, Twitter, Youtube, Flickr, Instagram, Google+, Linkedin, Pinterest, Tumbir…, mà còn yêu cầu cung cấp thông tin về tài khoản mạng xã hội của nước ngoài như Sina Weibo, QQ, Douban (Trung Quốc), VK (Nga)....

Có thể thấy, Mỹ, Anh và nhiều quốc gia khác rất quan tâm tới dữ liệu cá nhân, quyền riêng tư trên mạng xã hội bao gồm cả hai khía cạnh là thu thập và bảo vệ. Dữ liệu người dùng được coi như tài sản quốc gia, giá trị mang lại từ những dữ liệu này là không chỉ trên lĩnh vực kinh tế, chính trị và còn là an ninh quốc gia.

Như vậy, nước ta không phải quốc gia đầu tiên quy định việc lưu trữ dữ liệu và cũng không phải duy nhất là quốc gia yêu cầu lưu trữ dữ liệu trong nước.

# 9. Có phải chỉ Việt Nam mới quy định các doanh nghiệp nước ngoài cung cấp dịch vụ trên không gian mạng phải cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng?

Tất cả các quốc gia trên thế giới đều coi an ninh quốc gia là điều kiện tiên quyết hàng đầu. Do đó, các doanh nghiệp cung cấp dịch vụ trên không gian mạng đã và đang phải phối hợp với các cơ quan chức năng của các quốc gia trên thế giới trong bảo vệ an ninh quốc gia, phòng chống tội phạm.

Khoản 2 Điều 26 đã quy định rõ các trường hợp phải cung cấp thông tin cho lực lượng chuyên trách bảo vệ an ninh mạng, cụ thể:

(1) Khi lực lượng chuyên trách bảo vệ an ninh mạng có yêu cầu bằng văn bản; và

(2) để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng.

Đây là hai điều kiện đồng thời, tức là khi có hành vi vi phạm pháp luật về an ninh mạng xảy ra, khi lực lượng chuyên trách bảo vệ an ninh mạng sẽ có văn bản yêu cầu các doanh nghiệp nêu trên cung cấp thông tin về hành vi vi phạm pháp luật đó. Cần đặc biệt lưu ý rằng, những thông tin cung cấp là thông tin liên quan tới hành vi vi phạm pháp luật.

# 10. Luật An ninh mạng có gây cản trở hoạt động của doanh nghiệp, tạo giấy phép con hay không?

Trong 7 quy định liên quan tới trách nhiệm của các doanh nghiệp cung cấp dịch vụ trên không gian mạng trong Luật An ninh mạng, không có quy định nào liên quan tới hoạt động kinh doanh của doanh nghiệp, cũng không có quy định nào yêu cầu các doanh nghiệp cung cấp dịch vụ trên không gian mạng phải có giấy phép con mới được phép hoạt động.

Ngoại trừ việc phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng xử lý các hành vi vi phạm pháp luật trên không gian mạng và một số trách nhiệm được quy định cụ thể trong Điều 41 liên quan tới cảnh báo, khắc phục, xử lý các hành vi vi phạm pháp luật, các doanh nghiệp không phải chấp hành nghĩa vụ nào khác đối với hoạt động kinh doanh của mình. Không có quy định nào về an ninh mạng trong Luật An ninh mạng quy định về hoạt động thành lập doanh nghiệp, khởi nghiệp, đầu tư, mua bán, kinh doanh của doanh nghiệp.