

**QUẬN ỦY QUẬN 10
BAN TUYÊN GIÁO**

*

Số 68-CV/BTGQU

*Sao gửi tài liệu “Một số nội dung
tuyên truyền về Luật An ninh mạng”*

ĐẢNG CỘNG SẢN VIỆT NAM
Quận 10, ngày 18 tháng 6 năm 2018

Kính gửi: - Cấp ủy 41 cơ sở Đảng.

Thực hiện Công văn số 1902-CV/BTGTU ngày 15 tháng 6 năm 2018 của Ban Tuyên giáo Thành ủy về việc gửi tài liệu “Một số nội dung tuyên truyền về Luật An ninh mạng”, Ban Tuyên giáo Quận ủy sao gửi tài liệu đến cấp ủy 41 cơ sở Đảng.

Đề nghị cấp ủy 41 cơ sở Đảng sử dụng làm tài liệu triển khai đến đảng viên trong sinh hoạt chi bộ.

Nơi nhận:

- Như trên,
- Lưu Ban Tuyên giáo Quận ủy.

**K/T TRƯỞNG BAN
PHÓ TRƯỞNG BAN**



Nguyễn Thị Yến Hương

MỘT SỐ NỘI DUNG CẦN TUYÊN TRUYỀN VỀ LUẬT AN NINH MẠNG

1. Sự cần thiết phải ban hành Luật An ninh mạng

- Không gian mạng là lĩnh vực mới, tác động sâu rộng vào mọi mặt đời sống xã hội. Các hành vi trên không gian mạng có thể xâm hại tới mọi người, mọi lĩnh vực như: độc lập, chủ quyền, an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

- Không gian mạng trở thành nơi “trú ẩn an toàn” của tội phạm mạng. Từ khi mạng internet xuất hiện, đã tạo ra nhiều lợi ích cho con người. Tuy nhiên, cũng mang lại những thách thức to lớn. Không gian mạng trở thành nơi “trú ẩn an toàn” của tội phạm, đặc biệt là tội phạm có tổ chức diễn biến phức tạp, tấn công mạng, khủng bố mạng, gián điệp mạng, chiến tranh mạng, sự cố an ninh mạng...

- Việt Nam nằm trong nhóm quốc gia bị tấn công mạng nhiều nhất trên thế giới, tội phạm phát triển nhanh, tình trạng nhiễu loạn thông tin trên không gian mạng, thông tin xuyên tạc, bôi nhọ, vu khống, xúc phạm nhân phẩm, vi phạm thuần phong mỹ tục diễn ra tràn lan..., cơ sở hạ tầng không gian mạng còn nhiều lỗ hổng. Việt Nam xếp ở vị trí thứ 4 trong Top 10 quốc gia bị kiểm soát bởi mạng máy tính bị nhiễm mã độc. Theo báo cáo của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam trong năm 2017, các hệ thống thông tin tại Việt Nam đã phải hứng chịu khoảng 15.000 cuộc tấn công mạng, gồm khoảng 3.000 cuộc tấn công lừa đảo, 6.500 cuộc tấn công cài phần mềm độc hại và 4.500 cuộc tấn công thay đổi giao diện. Trong đó, số cuộc tấn công vào hệ thống thông tin của các cơ quan nhà nước có tên miền “.gov.vn” cũng lên tới hàng trăm. Thiệt hại lên tới 12.300 tỷ đồng (540 triệu USD), vượt xa mốc 10.400 tỷ đồng của năm 2016 và đã đạt kỷ lục trong nhiều năm trở lại đây. Trong 5 tháng đầu năm 2018 đã ghi nhận 4.035 sự cố tấn công mạng vào Việt Nam, riêng tháng 2 và 3 có tới hơn 1.500 vụ tấn công mạng; bên cạnh đó với khoảng 637.400 máy tính bị kiểm soát nằm trong mạng máy tính bị nhiễm mã độc.

- Hậu quả của việc mất an ninh mạng để lại nhiều hậu quả phức tạp, ví dụ như: website cảng hàng không bị tin tặc tấn công, khiến việc làm thủ tục an ninh hàng không gặp trở ngại, nhiều hành khách bị chậm chuyến bay; một số tờ báo điện tử bị tin tặc tấn công khiến người đọc không thể truy cập được; tài khoản ngân hàng của khách hàng bị đột nhập và rút hết tiền; một số cá nhân sử dụng mạng xã hội để đăng, phát thông tin sai trái, bịa đặt, ảnh hưởng nghiêm trọng đến danh dự, nhân phẩm của cá nhân, thậm chí có trường hợp ảnh hưởng đến uy tín của cơ quan, tổ chức....

- Để có hệ thống phòng chống tấn công mạng hiệu quả, ngoài thực hiện các giải pháp kỹ thuật, thì cần có hành lang pháp lý cụ thể. Hiện nay, tình trạng mất an ninh mạng, lỗ hổng mất an toàn ngày càng gia tăng, khoảng hơn 300%/năm khiến nguy cơ mất an toàn thông tin mạng đang gia tăng nhanh chóng khi bước vào cách mạng công nghiệp 4.0. Theo các chuyên gia an ninh mạng, Việt Nam chưa đủ sức đối phó với tấn công mạng hiện đại vì các biện pháp triển khai thường độc lập với nhau; thiếu hành lang pháp lý rõ ràng, và trách nhiệm liên kết của các cơ quan chức năng Việt Nam với nhau. Điều đó nói lên rằng, chỉ có thể phòng chống tấn công mạng hiệu quả, ngoài biện pháp kỹ thuật, con người thì phải có hệ thống pháp luật cụ thể, rõ ràng, đủ điều kiện triển khai các biện pháp pháp lý và hợp tác quốc tế, khi đã có nhiều quốc gia trên thế giới ban hành Luật An ninh mạng. Do đó, việc xây dựng và ban hành Luật An ninh mạng xuất phát từ yêu cầu cấp thiết của tình hình an ninh mạng trong nước, ***bảo đảm an ninh mạng cũng đồng nghĩa với bảo đảm đời sống thực tiễn của tất cả chúng ta.***

2. Luật An ninh mạng bảo đảm an toàn, lành mạnh, hạn chế tối đa các yếu tố, nguy cơ xâm hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân

- Theo các chuyên gia công nghệ thông tin, tài khoản cá nhân sẽ được bảo vệ tốt hơn khi Luật An ninh mạng được ban hành. Các tổ chức, cá nhân hoạt động trên môi trường không gian mạng sẽ được bảo đảm an toàn, lành mạnh, hạn chế tối đa các yếu tố, nguy cơ xâm hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân như: bị đánh cắp thông tin cá nhân, lừa đảo, chiếm đoạt tài sản, bị vu khống, làm nhục, công kích bôi nhọ...

Việc quy định rõ các biện pháp bảo vệ an ninh mạng bảo đảm tuân thủ nghiêm túc quy định của Hiến pháp và hệ thống pháp luật hiện hành. Đồng thời, làm căn cứ pháp lý để các lực lượng chuyên trách, lực lượng bảo vệ an ninh mạng áp dụng khi triển khai công tác bảo vệ an ninh mạng, phòng ngừa, xử lý hành vi vi phạm pháp luật. Các hành vi bị nghiêm cấm trong dự thảo luật được quy định rõ ràng, theo từng nhóm, lĩnh vực cụ thể, bao gồm: tung tin, tuyên truyền, báo thông tin sai sự thật, bôi nhọ, xúc phạm danh dự nhân phẩm, làm nhục, vu khống gây thiệt hại đến quyền và lợi ích hợp pháp của tổ chức, cá nhân, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, gây mất ổn định về an ninh, trật tự...

- Luật An ninh mạng - tăng cường bảo vệ an ninh quốc gia trên không gian mạng. Bảo vệ dữ liệu người dùng Việt Nam là một trong những quy định trọng tâm của luật được nêu tại khoản 3 điều 26, 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.

Các doanh nghiệp này cũng phải đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam. Đây không phải là quy định mới, bởi trước đó, năm 2013, Nghị định 72/2013/NĐ-CP đã quy định tại khoản 2 điều 24, khoản 8 điều 25 yêu cầu một số doanh nghiệp nước ngoài phải có ít nhất 1 hệ thống máy chủ đặt tại Việt Nam.

Tuy nhiên, không phải tất cả các doanh nghiệp này đều phải thực hiện quy định trên, mà chỉ áp dụng đối với các doanh nghiệp có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu người dùng Việt Nam, bao gồm 3 loại dữ liệu cụ thể được nêu trong luật.

3. Luật An ninh mạng không cản trở Việt Nam thực hiện các cam kết quốc tế

- **Việt Nam không vi phạm các cam kết quốc tế**, qua rà soát các văn bản cam kết gia nhập tổ chức thương mại thế giới (WTO), Hiệp định chung về thuế quan và thương mại (GATT 1994), Hiệp định chung về thương mại dịch vụ (GATS), Hiệp định về các khía cạnh liên quan đến thương mại của quyền sở hữu trí tuệ (TRIPS); đồng thời, rà soát Hiệp định Đối tác toàn diện và tiến bộ xuyên Thái Bình Dương (CPTPP), các văn kiện này đều có quy định về ngoại lệ an ninh, cho phép tôn trọng và bảo vệ an ninh quốc gia ở mức cao nhất. Như vậy, có thể khẳng định, ta không vi phạm các cam kết quốc tế.

- **Về lưu trữ dữ liệu quan trọng quốc gia trong nước**, đây là thông lệ quốc tế đã có, chúng ta không phải là quốc gia đầu tiên áp dụng quy định này. Theo thống kê, 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. **Quy định nêu trên là có trọng tâm, trọng điểm, về dữ liệu, quy định này không yêu cầu lưu trữ toàn bộ dữ liệu có liên quan tới Việt Nam trên không gian mạng**, không yêu cầu lưu trữ dữ liệu nền tảng (platform), mà chỉ yêu cầu lưu trữ đối với một số loại dữ liệu cụ thể, liên quan tới bí mật cá nhân trong trường hợp cần thiết và các dữ liệu liên quan tới an ninh quốc gia, vì đây là tài sản của công dân, tài sản của quốc gia cần được quản lý, bảo vệ.

- **Trong thực tiễn, việc không quản lý được dữ liệu người dùng và dữ liệu quan trọng quốc gia đã và đang ảnh hưởng tới lợi ích, an ninh quốc gia**. Về an ninh quốc gia và phòng, chống tội phạm, hiện nay, các thế lực thù địch, phản động và tội phạm đang gia tăng việc sử dụng không gian mạng để xâm phạm an ninh quốc gia, trật tự an toàn xã hội, trong khi cơ quan

chức năng gặp rất nhiều khó khăn trong điều tra, xác minh, truy tìm, xử lý các trường hợp vi phạm này vì toàn bộ dữ liệu đều được đặt ở nước ngoài.

- **Phù hợp với pháp luật trong nước, thông lệ quốc tế, không cản trở hoạt động của doanh nghiệp.** Việc quy định “Lưu trữ tại Việt Nam đối với thông tin cá nhân của người sử dụng tại Việt Nam và các dữ liệu quan trọng liên quan đến an ninh quốc gia; đặt trụ sở hoặc văn phòng đại diện tại Việt Nam” được quy định tại Điều 26 là khả thi, phù hợp với pháp luật trong nước, thông lệ quốc tế, không trái với các điều ước mà chúng ta tham gia, cũng không cản trở hoạt động của doanh nghiệp. Theo thống kê có ít nhất 18 Quốc gia trong WTO có quy định về việc lưu trữ dữ liệu người sử dụng tại Quốc gia sở tại là: Mỹ, Canada, Liên bang Nga, Pháp, Đức, Trung Quốc, Australia, Indonesia, Hy Lạp, Bulgaria, Đan Mạch, Phần Lan, Thụy Điển, Thổ Nhĩ Kỳ, Venezuela, Colombia, Argentina, Brazil...

- Hiện Google đã đặt khoảng 70 văn phòng đại diện, Facebook khoảng 80 văn phòng đại diện tại các quốc gia trên thế giới. Hiện nay, Google và Facebook đang lưu trữ dữ liệu của cơ quan, tổ chức, cá nhân Việt Nam tại trung tâm lưu trữ đặt tại Hongkong và Singapore. Nếu quy định của Luật có hiệu lực, các doanh nghiệp này phải dịch chuyển đám mây (máy chủ ảo) về Việt Nam để mở trung tâm dữ liệu tại Việt Nam là hoàn toàn khả thi. Tuy có gia tăng chi phí cho doanh nghiệp nhưng là quy định cần thiết phải đáp ứng về yêu cầu an ninh mạng của nước ta. Mặt khác, trong hoạt động của doanh nghiệp cũng sẽ thuận lợi hơn, nếu gặp sự cố gián đoạn sẽ được xử lý nhanh hơn, cơ quan chức năng sẽ quản lý tốt hơn hoạt động kinh doanh của các doanh nghiệp này; và khi có hành vi xâm phạm an ninh mạng, việc phối hợp xử lý thông tin và hành vi vi phạm sẽ hiệu quả hơn. Quy định về việc đặt máy chủ và lưu trữ dữ liệu tại Việt Nam đã được quy định trong Nghị định số 72/2013/NĐ-CP của Chính phủ trước đây.

4. Yêu cầu đặt ra

Có thể khẳng định rằng, trong tình hình hiện nay, việc ban hành Luật An ninh mạng là hết sức cần thiết, tạo môi trường lành mạnh, bình đẳng cho tất cả các tổ chức, cá nhân cùng tham gia hoạt động và Luật An ninh mạng ra đời đáp ứng yêu cầu thực tiễn đặt ra trong quá trình phát triển đất nước, tập trung bảo vệ lợi ích hợp pháp của cá nhân, tổ chức trên không gian mạng. Đặc biệt, tạo hành lang pháp lý trong công tác an ninh mạng liên quan đến bảo vệ an ninh quốc gia, đảm bảo trật tự an toàn xã hội. Thời gian qua, việc thông qua Luật An ninh mạng được sự quan tâm của người dân và doanh nghiệp, các nhà đầu tư là rất lớn và hoàn toàn chính đáng.

Tuy nhiên, trong những ngày gần đây, các thế lực thù địch luôn tìm mọi cách chống phá Nhà nước ta, nên tìm mọi cách để xuyên tạc sai sự thật,

bằng mọi thủ đoạn đã lôi kéo, kích động người dân hiểu sai lệch bản chất việc ban hành và nội dung Luật An ninh mạng. Để tránh bị các thế lực thù địch lợi dụng lòng yêu nước của người dân, lôi kéo gây ảnh hưởng đến trật tự an toàn xã hội, người dân Thành phố hãy:

- Hết sức bình tĩnh, tin tưởng vào Đảng, Nhà nước.
- Không nghe theo lời kẻ xấu có những hành động vi phạm pháp luật (mất trật tự, vi phạm an toàn giao thông, gây thương tích cho người khác, hủy hoại tài sản của Nhà nước và doanh nghiệp...).
- Yên tâm làm việc bình thường. Phát hiện và chống mọi kẻ xấu xúi giục thực hiện hành vi vi phạm pháp luật, kịp thời thông báo cho các cơ quan chức năng xử lý.
- Cần chia sẻ những thông tin chính thống, những bài báo chính thống để Nhân dân được rõ. Không đăng tải, tán phát hình ảnh, phim cảnh tụ tập đông người, gây rối.
- Cùng tuyên truyền vận động bạn bè, người thân hiểu và nghiêm chỉnh chấp hành pháp luật, không tham gia các hoạt động của kẻ xấu.

Luật An ninh mạng Không cấm phát ngôn trên mạng, nhưng bạn phải chịu trách nhiệm về phát ngôn của mình. Khi bạn bị tấn công trên mạng, bạn sẽ được Luật An ninh mạng bảo vệ.

Mọi người dân đều được quyền bày tỏ chính kiến của mình nhưng không vi phạm pháp luật.

NGƯỜI YÊU NƯỚC LÀ NGƯỜI KHÔNG VI PHẠM PHÁP LUẬT!