

NHÌN LẠI MỘT NĂM THỰC HIỆN PHÁP LUẬT VỀ AN NINH MẠNG

★ PGS, TS NGUYỄN THỊ NGỌC HOA

Học viện Báo chí và Tuyên truyền

★ ThS BÙI THỊ LONG

Học viện Chính trị quốc gia Hồ Chí Minh

● **Tóm tắt:** Thời gian vừa qua, hành lang pháp lý về an ninh mạng của Việt Nam đã được hoàn thiện một bước quan trọng. Tuy nhiên, việc thi hành pháp luật về an ninh mạng còn hạn chế, hợp tác giữa các cơ quan, tổ chức, doanh nghiệp trong và ngoài nước về an ninh mạng còn yếu và thiếu chuyên nghiệp. Để góp phần nâng cao hiệu quả thực hiện pháp luật về an ninh mạng ở Việt Nam trong thời gian tới, bài viết trình bày khái quát thực trạng thực hiện Luật An ninh mạng ở Việt Nam và một số giải pháp nâng cao hiệu quả công tác này.

● **Từ khóa:** an ninh mạng, Luật An ninh mạng.

1. Thực trạng thực hiện Luật An ninh mạng ở Việt Nam

Luật An ninh mạng được Kỳ họp thứ 5 Quốc hội khóa XIV thông qua 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. Các quy định của Luật An ninh mạng năm 2018 tập trung hướng đến phòng ngừa, phát hiện, đấu tranh, xử lý các hành vi vi phạm pháp luật trên không gian mạng, xâm phạm tới các khách thể phải được bảo vệ là an ninh quốc gia, trật tự an toàn xã hội.

Từ khi được ban hành, thực hiện, Luật An ninh mạng đã cho thấy tính hiệu quả của các thiết chế pháp luật đối với các hoạt động trên không gian mạng. Thực tiễn một năm qua đã phản bác một số thông tin bịa đặt như Luật An ninh mạng ngăn cản, xâm phạm quyền tự do ngôn luận. Bằng chứng cho thấy Luật An ninh mạng không ngăn cản, xâm phạm quyền tự do ngôn luận của công dân. Các hoạt động liên lạc, trao đổi, đăng tải, chia sẻ thông tin, mua bán, kinh doanh, thương mại vẫn diễn ra bình thường trên không gian mạng, không hề bị ngăn cản, cấm đoán miễn là những hoạt động đó không vi phạm pháp luật của Việt Nam. Công dân có thể làm bất cứ điều gì trên không gian mạng mà pháp luật Việt Nam không cấm.

Luật An ninh mạng bảo vệ cho các hoạt động tự do ngôn luận, quyền và lợi ích hợp pháp của tổ chức cá nhân khi mua bán, kinh doanh, trao đổi, thương mại trên không gian mạng. Bất kỳ thông tin thiếu kiểm chứng, sai sự thật, gây tác động xấu đến trật tự an toàn xã hội sẽ bị xử lý kiên quyết, kịp thời⁽¹⁾. Điển hình như việc xử lý các đối tượng tung tin sai lệch về dịch Covid 2019 đã được các địa phương xử lý quyết liệt, nghiêm túc. Các cơ quan chức năng không chỉ truy tìm, xử lý các đối tượng tung tin giả mà còn yêu cầu các trang mạng xã hội gỡ bỏ các tin thất thiệt, đăng tải những thông tin chính thức từ các cơ quan có thẩm quyền. Chấm dứt tình trạng nhiễu loạn thông tin, tâm lý hoang mang lo ngại của người dân trong những ngày đầu bùng dịch, ảnh hưởng đến công tác phòng chống dịch.

Trong thực tế đã có nhiều kẻ xấu tung tin Luật An ninh mạng ngăn cấm người sử dụng internet truy cập Facebook, Google, Youtube. Tuy nhiên, từ khi áp dụng Luật, người dân sử dụng internet vẫn dễ dàng truy cập vào tất cả các trang mạng ở trong và ngoài nước. Luật An ninh mạng quy định các biện pháp bảo vệ về an ninh mạng cho người dân khi tham gia hoạt động trên các trang mạng xã hội như Facebook, Google... Nhưng nếu cá nhân, tổ chức nào sử dụng không gian mạng để thực hiện hành vi vi phạm pháp luật đều bị xử lý nghiêm theo quy định của pháp luật.

Trong khi Luật không có quy định nào về kiểm soát, quản lý, hạn chế hay gây cản trở hoạt động kinh doanh của doanh nghiệp, cũng như hoạt động khởi nghiệp. Tuy nhiên nhiều kẻ xấu đã tung tin Luật An ninh mạng gây cản trở các doanh nghiệp viễn thông, internet và các doanh nghiệp khởi nghiệp Việt Nam. Thời gian qua, Luật An ninh mạng đã chứng minh không có doanh nghiệp cung cấp dịch vụ trên mạng nào

bị dừng hoạt động kinh doanh. Mọi hoạt động kinh doanh miễn là không vi phạm pháp luật vẫn diễn ra bình thường trên môi trường mạng. Luật chỉ quy định trách nhiệm phối hợp của doanh nghiệp trong bảo vệ an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng; hướng dẫn các doanh nghiệp, tổ chức, cá nhân áp dụng các biện pháp để tự bảo vệ mình trước những mối đe dọa từ không gian mạng.

Do đó, mỗi chủ thể dùng không gian mạng cần nhận thức một cách sáng suốt trước những thông tin đăng tải, có ý thức thực hiện pháp luật vì sự bình yên phát triển của đất nước; nhận thức rõ việc thực hiện pháp luật về an ninh mạng góp phần bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch trong tình hình mới theo đúng tinh thần Nghị quyết 35-NQ/TW của Bộ Chính trị.

Thực trạng thực hiện pháp luật về an ninh mạng ở Việt Nam hiện nay thể hiện trên 4 mặt sau đây:

Thứ nhất, tuân thủ pháp luật về an ninh mạng: Thực hiện chủ trương, chính sách về an ninh mạng của Đảng và Nhà nước, Việt Nam đã ban hành Luật An ninh mạng năm 2018. Tình hình kiểm soát an ninh mạng ngày càng đi vào nền nếp. Điều đó cho thấy quyết tâm thực hiện đã có nhưng với công cụ pháp lý chính thức trong tay, mọi thứ trở nên thuận lợi và dễ dàng hơn. Tuy nhiên, cùng với những thành tựu bước đầu, an ninh không gian mạng đang đứng trước nhiều nguy cơ với những hành vi vi phạm pháp luật của các tác nhân ngày càng tinh vi. Theo báo cáo thường niên về tình hình an ninh của Bộ Công an, năm 2018, hoạt động lừa đảo chiếm đoạt tài sản trên mạng xã hội (Facebook, Zalo, Viber, WhatsApp...) diễn biến phức tạp, nổi lên là tình trạng lừa đảo chiếm đoạt tài sản

bằng hình thức nhắn tin thông báo trúng thưởng qua mạng xã hội; làm quen với người bị hại, tạo lòng tin, hứa gửi tiền, quà tặng có giá trị, sau đó giả mạo nhân viên hải quan yêu cầu nạn nhân chuyển tiền làm các thủ tục thông quan để chiếm đoạt. Hoạt động kinh doanh theo mô hình đa cấp qua mạng internet vẫn diễn biến phức tạp với nhiều phương thức, thủ đoạn mới, tinh vi như: Lập website để tổ chức huy động vốn trả lãi suất cao nhằm chiếm đoạt tài sản; lợi dụng hoạt động từ thiện để lừa đảo chiếm đoạt tài sản; lập và tạo ra nhiều sàn giao dịch các loại tiền điện tử hoạt động theo mô hình đa cấp như: Onecoin, Bitcoin, ILcoin, Gemcoin... để thu hút các nhà đầu tư nhằm chiếm đoạt tài sản hoặc kinh doanh tiền điện tử trái phép để rửa tiền, ship hàng, trả tiền cá độ bóng đá. Điển hình là vụ Nguyễn Hữu Tiến và đồng phạm thành lập website Otcmax.vn quảng cáo kêu gọi đầu tư dự án với lợi nhuận cao 1,8%/ngày và đầu tư tiền ảo VNCoins với lợi nhuận 2,5%/ngày, đã chiếm đoạt hơn 200 tỷ đồng của 6.000 người; vụ Hợp tác xã đào tiền ảo Sky Mining với thủ đoạn quảng cáo là công ty đào tiền ảo "lớn nhất Việt Nam" kêu gọi nhà đầu tư mua máy đào tiền ảo với hứa hẹn sau 12 tháng sẽ trả lại vốn và lãi đến 300% mức đầu tư, đã chiếm đoạt trên 300 tỷ đồng của nhà đầu tư. Bên cạnh đó, tình trạng đánh bạc, cá độ bóng đá trên mạng internet diễn ra rất phức tạp, số tiền đánh bạc lên đến hàng nghìn tỷ đồng. Các đối tượng nhà cái ở nước ngoài thường móc nối với các đối tượng trong nước hình thành mạng lưới tổ chức đánh bạc lớn cho cả người Việt Nam và người nước ngoài⁽²⁾. Vì mục đích lợi nhuận, nhiều tổ chức, cá nhân kinh doanh trên mạng đã không tuân thủ các quy định pháp luật về an ninh mạng. Nạn hàng quảng cáo online một đàng, nhưng khi giao hàng không

đúng chất lượng, không đúng thời gian như đã cam kết có xu hướng gia tăng.

Thứ hai, thi hành pháp luật về an ninh mạng: Xác định thi hành Luật An ninh mạng là một trong những nhiệm vụ trọng tâm, quyết định thành công của công tác thi hành pháp luật về an ninh mạng, ngày 1-2-2019, Thủ tướng Chính phủ đã ban hành Quyết định số 12/QĐ-TTg ban hành Kế hoạch triển khai thi hành Luật An ninh mạng, trong đó chỉ đạo tổ chức các Hội nghị quán triệt, phổ biến tới các bộ, ngành chức năng, Ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương, các đối tượng tác động của Luật An ninh mạng để người dân biết, hiểu và thực hiện nghiêm túc. Các cơ quan, tổ chức, cá nhân được giao nhiệm vụ thi hành pháp luật về an ninh mạng đã triển khai, tổ chức thực hiện các nhiệm vụ được giao đảm bảo đúng quy định, bảo đảm pháp luật về an ninh mạng được thực thi. Ngoài việc tiếp cận không gian mạng như một miền lãnh thổ mới cần được bảo vệ, việc tiếp cận không gian mạng theo phương diện kỹ thuật, theo đặc điểm hữu hình thì không gian mạng được coi như một hệ thống máy tính cần được bảo vệ. Theo nghĩa này, thi hành pháp luật về an ninh mạng được hiểu là bắt buộc áp dụng các biện pháp đảm bảo an toàn cho các thành phần mạng đã xác định gồm thiết bị, cơ sở dữ liệu, cơ sở hạ tầng. Bắt buộc các tài nguyên vật chất của mạng phải được sử dụng đúng quy định.

Thứ ba, sử dụng pháp luật về an ninh mạng: Pháp luật về an ninh mạng quy định các chủ thể pháp luật có quyền sử dụng các quyền chủ thể để bảo vệ quyền và lợi ích chính đáng của mình trong lĩnh vực an ninh mạng. Các cơ quan, tổ chức, cá nhân tích cực và chủ động trong việc sử dụng pháp luật để thực hiện và bảo vệ quyền và lợi ích hợp pháp là do các chủ

thể có thẩm quyền đã bảo đảm thực hiện các quy định pháp luật về an ninh mạng. Theo đó, các Điều 5, 6, 8, 9 Chương I Luật An ninh mạng quy định tổ chức, cá nhân có thẩm quyền sử dụng pháp luật về an ninh mạng trong việc áp dụng các biện pháp bảo vệ an ninh mạng như: thẩm định an ninh mạng; đánh giá điều kiện an ninh mạng; kiểm tra an ninh mạng; giám sát an ninh mạng; ứng phó, khắc phục sự cố an ninh mạng; đấu tranh bảo vệ an ninh mạng; sử dụng mật mã để bảo vệ thông tin mạng; 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; yêu cầu xóa bỏ, truy cập xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật 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; 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; 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; khởi tố, điều tra, truy tố, xét xử theo quy định của Bộ luật Tố tụng hình sự; biện pháp khác theo quy định của pháp luật về an ninh quốc gia, pháp luật về xử lý vi phạm hành chính...

Chương II Luật An ninh mạng còn quy định các hoạt động bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia như: Bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia, bao gồm: hệ thống thông tin quan trọng về an ninh quốc gia; bảo vệ an ninh mạng

đối với hệ thống thông tin quan trọng về an ninh quốc gia; thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; kiểm tra, đánh giá an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; giám sát, cảnh báo, ứng phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia...

Thứ tư, áp dụng pháp luật về an ninh mạng: Trách nhiệm bảo vệ an ninh mạng do nhiều cơ quan, tổ chức đảm nhiệm, trong đó được quy định rõ đầu mối quản lý nhà nước về an ninh mạng trong Luật An ninh mạng. Hoạt động giám sát, kiểm tra, xử lý vi phạm pháp luật của cơ quan nhà nước chức năng bảo vệ an ninh mạng là một hình thức áp dụng pháp luật quan trọng. Bộ Công an đã có nhiều hoạt động tích cực trong công tác phát hiện, điều tra, xử lý vi phạm pháp luật về an ninh mạng. Với tinh thần kiên quyết giảm thiểu những nguy cơ, thách thức từ an ninh mạng, bảo đảm 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, năm 2019, Bộ Công an đã tăng cường các biện pháp đấu tranh làm rõ phương thức, thủ đoạn mới của tội phạm sử dụng công nghệ cao trong hoạt động thanh toán thẻ, thanh toán điện tử; triệt phá nhiều đường dây tội phạm cờ bạc, cá độ bóng đá qua mạng internet như: Vụ bắt 10 đối tượng trong đường dây đánh bạc, tổ chức đánh bạc qua mạng internet với số tiền khoảng 500 tỷ đồng tại Hà Nội; vụ bắt 29 đối tượng đánh bạc qua internet với số tiền trên 1.000 tỷ đồng tại Hưng Yên; vụ bắt 13 đối tượng đánh bạc qua internet với số tiền 12 tỷ đồng, xác định có khoảng 100 tài khoản ở 33 tỉnh, thành trong cả nước tham gia đánh bạc tại Nghệ An; tội phạm người nước ngoài sử dụng

công nghệ cao tại Việt Nam. Điều tra, bắt giữ nhiều đối tượng lập nhiều trang web, facebook, zalo ảo, lừa đảo hàng tỷ đồng. Phát hiện 352 vụ, 503 đối tượng phạm tội, vi phạm pháp luật trong lĩnh vực viễn thông, tin học (tăng 17,73% số vụ so với cùng kỳ 2018). Đã khởi tố 164 vụ, 304 bị can (tăng 17,99% số vụ và tăng 6,29% bị can so với cùng kỳ năm 2018)⁽³⁾. Đầu tháng 2 vừa qua, lực lượng Công an tỉnh Quảng Nam vừa triệt phá thành công đường dây đánh bạc qua mạng internet với hình thức cá độ bóng đá và lô đề với số tiền hơn 40 tỷ đồng⁽⁴⁾.

Trong các hình thức của áp dụng pháp luật của các cơ quan nhà nước về an ninh mạng, hoạt động xét xử của tòa án đối với các vụ án vi phạm pháp luật an ninh mạng có vai trò và sức lan tỏa đặc biệt quan trọng, vì chỉ có Tòa án mới có chức năng xét xử. Trước khi thụ lý hồ sơ, Tòa án có thể áp dụng các biện pháp khẩn cấp tạm thời để bảo vệ lợi ích của các đương sự. Trong quá trình xét xử, tòa án tuân thủ chặt chẽ những quy định về trình tự, thủ tục chặt chẽ của Luật Tố tụng hình sự. Các chế tài áp dụng với các đối tượng vi phạm có tính răn đe và giáo dục. Tuy nhiên, thực tế xét xử của ngành tòa án thời gian qua cho thấy, các vụ án hình sự ở lĩnh vực này không nhiều.

Một số hạn chế trong việc thực hiện pháp luật về an ninh mạng trên đây bắt nguồn từ nhiều quy định pháp luật về an ninh mạng còn bất cập. Do đó, nhiều chủ thể còn lúng túng khi áp dụng vào thực tiễn cuộc sống. Ý thức tuân thủ pháp luật về an ninh mạng của đa số các tổ chức, cá nhân chưa cao; nguồn nhân lực chuyên trách bảo vệ an ninh mạng còn hạn chế về trình độ, năng lực, chưa đáp ứng yêu cầu trong tình hình mới. Chưa làm chủ được các thiết bị hạ tầng, còn phải nhập sản phẩm công nghệ từ nước ngoài, phần lớn từ Trung Quốc.

2. Một số giải pháp nâng cao hiệu quả thực hiện Luật An ninh mạng ở Việt Nam trong thời gian tới

Để phát huy tác động tích cực của Luật An ninh mạng năm 2018, khắc phục những hạn chế, bất cập trong việc thực hiện pháp luật về an ninh mạng, góp phần nâng cao hiệu quả thực hiện pháp luật về an ninh mạng, trong thời gian tới cần thực hiện đồng bộ các giải pháp sau đây:

Thứ nhất, quán triệt sự lãnh đạo của Đảng, sự quản lý thống nhất của Nhà nước; huy động sức mạnh tổng hợp của hệ thống chính trị và toàn dân; phát huy vai trò nòng cốt của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an được Chính phủ giao là đầu mối quản lý nhà nước về an ninh mạng.

Tăng cường sự lãnh đạo của Đảng trong xây dựng, hoàn thiện pháp luật về an ninh mạng làm cơ sở cho thực hiện pháp luật về an ninh mạng. Pháp luật về an ninh mạng đã góp phần xây dựng nhận thức thống nhất cho các chủ thể, điều chỉnh hành vi thực hiện pháp luật theo hướng ngày càng tích cực hơn. Do đó, cần nhanh chóng hoàn thiện hệ thống pháp luật về an ninh mạng.

Cần nghiên cứu loại bỏ những quy định gây ra cách hiểu trùng lặp giữa Luật An toàn thông tin mạng năm 2015 và Luật An ninh mạng năm 2018. Bổ sung những quy định còn thiếu, đáp ứng yêu cầu điều chỉnh các quan hệ xã hội mới phát sinh liên tục trong bối cảnh cuộc Cách mạng công nghiệp 4.0. Ngoài ra, cần khắc phục hiện tượng chưa thống nhất giữa các điều khoản trong các văn bản pháp luật.

Thứ hai, tiếp tục rà soát, xây dựng và hoàn thiện các quy định pháp luật về phòng chống tấn công mạng và vận hành hệ thống an ninh mạng phù hợp các chuẩn mực quốc tế; hoàn thiện thể chế pháp lý về thực hiện pháp luật nói chung và

pháp luật về an ninh mạng nói riêng nhằm đáp ứng yêu cầu bảo vệ an ninh không gian mạng quốc gia.

Đẩy mạnh công tác tuyên truyền, phổ biến pháp luật về an ninh mạng. Các cơ quan chức năng sớm nghiên cứu, đổi mới phương pháp, hình thức và nội dung hoạt động để người dân hiểu rõ, hiểu đúng pháp luật về an ninh mạng. Tuân thủ pháp luật về an ninh mạng; bảo đảm lợi ích của Nhà nước, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khi hoạt động trên môi trường mạng.

Thứ ba, bổ sung các chế tài trong pháp luật về an ninh mạng theo hướng quy định phải đủ sức răn đe, ngăn chặn vi phạm; quy định rõ cơ chế phối hợp giữa các cơ quan quản lý nhà nước về an ninh mạng, bảo đảm tất cả các hành vi vi phạm pháp luật về an ninh mạng phải được xử lý kịp thời, nghiêm minh. Các chế tài áp dụng phải đủ sức răn đe, giáo dục nhằm phòng ngừa, ngăn chặn các hành vi vi phạm.

Thứ tư, tăng cường hợp tác quốc tế, thúc đẩy chuyển giao công nghệ. Thực hiện pháp luật về an ninh mạng ở Việt Nam là hoạt động mới. Văn bản pháp lý đầu tiên điều chỉnh các quan hệ xã hội trong lĩnh vực an ninh mạng được Nhà nước ban hành vào năm 1997, đó là Nghị định số 21/NĐ-CP ngày 5-3-1997 của Thủ tướng Chính phủ về việc ban hành Quy chế tạm thời về quản lý, thiết lập, sử dụng mạng internet ở Việt Nam, đồng thời ra Quyết định thành lập Ban điều phối quốc gia mạng internet. Đây là Nghị định quan trọng xác định trách nhiệm quản lý nhà nước, cung cấp và sử dụng dịch vụ mạng internet. Trong khi đó, nhiều quốc gia trên thế giới có bề dày về bảo vệ an ninh mạng. Hoạt động thực hiện pháp luật về an ninh mạng ở các quốc gia này thực sự có nhiều kinh nghiệm để Việt Nam có thể tham khảo, vận dụng như Mỹ, Nga, Singapore,...

Thúc đẩy hợp tác quốc tế nhằm chuyển giao những kinh nghiệm phù hợp với thực tiễn Việt Nam, qua đó nâng cao ý thức tuân thủ pháp luật của các chủ thể khi tham gia hoạt động trên không gian mạng. Đồng thời, kiên quyết áp dụng các biện pháp mạnh để xử lý các hành vi vi phạm pháp luật trên không gian mạng, tận dụng lợi thế của các phương tiện truyền thông trong bối cảnh Công nghệ 4.0 để công khai kịp thời các vụ việc xâm phạm pháp luật an ninh mạng đã được xử lý.

Thứ năm, các cơ quan, tổ chức, doanh nghiệp nhà nước cần triển khai các giải pháp bảo đảm an toàn, an ninh mạng tổng thể nhằm khắc phục các tồn tại, hạn chế nêu trên, góp phần cải thiện hơn nữa xếp hạng của Việt Nam trong GCI. Quán triệt nguyên tắc Bộ trưởng, Thủ trưởng cơ quan ngang bộ, cơ quan thuộc Chính phủ, Chủ tịch Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương, Chủ tịch, Tổng giám đốc Tập đoàn, Tổng công ty nhà nước, Ngân hàng thương mại Nhà nước, Ngân hàng Phát triển Việt Nam, Ngân hàng Chính sách xã hội, Ngân hàng Hợp tác xã Việt Nam và các tổ chức tín dụng, tài chính Nhà nước khác chịu trách nhiệm trước Thủ tướng Chính phủ nếu để xảy ra mất an toàn, an ninh mạng, lộ lọt bí mật nhà nước tại cơ quan, đơn vị mình quản lý. Chỉ định, kiện toàn đầu mối đơn vị chuyên trách về an toàn thông tin mạng để làm tốt công tác tham mưu, tổ chức thực thi và kiểm tra, đôn đốc thực hiện các quy định của pháp luật về bảo đảm an toàn, an ninh mạng. Phối hợp chặt chẽ với cơ quan chuyên trách về an toàn, an ninh mạng của Bộ Thông tin và Truyền thông, Bộ Công an, Bộ Quốc phòng trong giám sát, chia sẻ thông tin, kiểm tra, đánh giá an toàn, an ninh mạng.

Đối với công tác giám sát, ứng cứu sự cố an toàn thông tin mạng, bảo vệ hệ thống thông tin

thuộc quyền quản lý: Tự thực hiện giám sát, ứng cứu sự cố an toàn thông tin mạng, bảo vệ hệ thống thông tin thuộc quyền quản lý hoặc lựa chọn tổ chức, doanh nghiệp có đủ năng lực để thực hiện; thông báo thông tin đầu mối thực hiện giám sát, ứng cứu sự cố an toàn thông tin mạng về Bộ Thông tin và Truyền thông và khi có sự thay đổi về thông tin đầu mối; kết nối, chia sẻ thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia trực thuộc Cục An toàn thông tin, Bộ Thông tin và Truyền thông.

Đối với công tác kiểm tra, đánh giá an toàn thông tin mạng cho hệ thống thông tin thuộc quyền quản lý cần lựa chọn tổ chức, doanh nghiệp độc lập với tổ chức, doanh nghiệp giám sát, bảo vệ để định kỳ kiểm tra, đánh giá an toàn thông tin mạng đối với hệ thống thông tin cấp độ 3 trở lên thuộc quyền quản lý hoặc kiểm tra, đánh giá đột xuất khi có yêu cầu theo quy định của pháp luật. Đối với các hệ thống thông tin cấp độ 3 và cấp độ 4, định kỳ hàng năm thực hiện kiểm tra, đánh giá và báo cáo Bộ Thông tin và Truyền thông, báo cáo Thủ tướng Chính phủ. Đối với hệ thống thông tin quan trọng quốc gia (cấp độ 5), định kỳ 06 tháng một lần thực hiện kiểm tra, đánh giá và báo cáo Bộ Thông tin và Truyền thông để tổng hợp, báo cáo Thủ tướng Chính phủ.

Ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ của doanh nghiệp trong nước đáp ứng yêu cầu về an toàn, an ninh mạng theo quy định của pháp luật đối với các hệ thống thông tin cấp độ 3 trở lên, các hệ thống thông tin phục vụ Chính phủ điện tử. Bảo đảm tỷ lệ kinh phí chi cho các sản phẩm, dịch vụ an toàn thông tin mạng đạt tối thiểu 10% trong tổng kinh phí triển khai kế hoạch ứng dụng công nghệ thông tin hàng năm, giai đoạn 5 năm và các dự án công nghệ thông tin (trong trường hợp chủ đầu

tư chưa có hệ thống kỹ thuật hoặc thuê dịch vụ bảo đảm an toàn thông tin mạng chuyên biệt đáp ứng được các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ). Sử dụng và quản lý khóa bí mật (USB token) của chữ ký số, dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ, chứng thư số, các giải pháp mã hóa của Ban Cơ yếu Chính phủ theo đúng quy định. Tiếp tục hoàn thiện cơ chế chính sách, hành lang pháp lý về an toàn thông tin mạng, an ninh mạng, tội phạm mạng, bảo vệ trẻ em trên môi trường mạng; chiến lược, quy hoạch, kế hoạch phát triển an toàn thông tin mạng; phát triển nguồn nhân lực an toàn, an ninh mạng; tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin mạng. Kịp thời cung cấp thông tin, số liệu về pháp lý, kỹ thuật, tổ chức, nâng cao năng lực và hợp tác trong lĩnh vực an toàn, an ninh mạng phục vụ việc đánh giá, xếp hạng chỉ số GCI của ITU⁽³⁾ □

(1) <https://vietnamnet.vn/>: "Virus Corona: Ngô Thanh Vân, Cát Phượng và Đàm Vĩnh Hưng bị phạt 30 triệu".

(2) Bộ Công an (2018), *Báo cáo thường niên về công tác phòng, chống tội phạm và vi phạm pháp luật năm 2018*, Hà Nội.

(3) Bộ Công an (2019), *Báo cáo thường niên về công tác phòng, chống tội phạm và vi phạm pháp luật năm 2019*, Hà Nội.

(4) <http://bocongan.gov.vn/>: "Công an Quảng Nam triệt phá đường dây đánh bạc qua mạng hơn 40 tỷ đồng".

(5) Thủ tướng Chính phủ (2019), *Chỉ thị số 14/CT-TTg ngày 7-6-2019 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*.