CHUYÊN ĐỀ: MỘT SỐ QUY ĐỊNH CỦA PHÁP LUẬT VỀ QUẢN LÝ, KHAI THÁC, SỬ DỤNG THÔNG TIN TRÊN INTERNET, MẠNG XÃ HỘI

Biên soạn: Thầy Nam Hà

1. Cơ sở pháp lý

1.1. Văn bản qui phạm pháp luật

- Luật An ninh mạng được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam khóa XIV, kỳ họp thứ 5 thông qua ngày 12/6/2018, có hiệu lực thi hành kể từ ngày 01/01/2019.

Luật An ninh mạng 2018 có 7 chương với 43 điều quy định về hoạt động bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội trên không gian mạng; phòng ngừa, xử lý hành vi xâm phạm an ninh mạng; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan, góp phần vào việc 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 tổ chức, cá nhân.

- Nghị định số 15/2020/NĐ-CP ngày 03/02/2020 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử.

1.2. Văn bản hành chính

- ***Bộ Quy tắc ứng xử*** trên mạng xã hội ban hành theo Quyết định số 874/QĐ-BTTT ngày 17/6/2021 của Bộ Thông tin và Truyền thông;

- ***Bộ quy tắc ứng xử*** của cán bộ, đảng viên, công chức, viên chức, người lao động, đoàn viên, hội viên tại các cơ quan, đơn vị, doanh nghiệp trực thuộc Đảng bộ Khối khi sử dụng internet, mạng xã hội, ban hành theo Quyết định số 599-QĐ/ĐUK ngày 28/6/2021 của Đảng ủy Khối cơ sở Bộ Công thương tại TP.HCM.

- Dự thảo Bộ qui tắc ứng xử trên mạng xã hội của HUFI năm 2021, đang được tổ chức lấy kiến góp ý của cán bộ, viên chức, người lao động, người học của HUFI (dự kiến sẽ ban hành trong năm 2021).

1.3. Giải thích thuật ngữ pháp lý liên quan

An ninh mạng là sự 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.

Bảo vệ an ninh mạng là phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng.

Không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian.

Không gian mạng quốc gia là không gian mạng do Chính phủ xác lập, quản lý và kiểm soát.

Tội phạm mạng là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện tội phạm được quy định tại Bộ luật Hình sự.

Tấn công mạng là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để phá hoại, gây gián đoạn hoạt động của mạng viễn thông, mạng

Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử.

Khủng bố mạng là việc sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện hành vi khủng bố, tài trợ khủng bố.

Gián điệp mạng là hành vi cố ý vượt qua cảnh báo, mã truy cập, mật mã, tường lửa, sử dụng quyền quản trị của người khác hoặc bằng phương thức khác để chiếm đoạt, thu thập trái phép thông tin, tài nguyên thông tin trên mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của cơ quan, tổ chức, cá nhân.

Nguy cơ đe dọa an ninh mạng là tình trạng không gian mạng xuất hiện dấu hiệu đe dọa xâm phạm an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

Sự cố an ninh mạng là sự việc bất ngờ xảy ra 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.

Tình huống nguy hiểm về an ninh mạng là sự việc xảy ra trên không gian mạng khi có hành vi xâm phạm nghiêm trọng an ninh quốc gia, gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2. Khái niệm, đặc điểm, vai trò và những hạn chế của mạng xã hội

2.1. Khái niệm mạng xã hội

Mạng xã hội (Social network) là một nền tảng trực tuyến, là nơi mà mọi người có thể xây dựng các mối quan hệ ảo với những người có chung tính cách, sở thích, nghề nghiệp… hoặc với cả những người có mối quan hệ ngoài đời thực. Mạng xã hội hiện nay có nhiều dạng thức và tính năng khác nhau, và có thể truy cập dễ dàng từ nhiều phương tiện, thiết bị như điện thoại di động, máy tính…

2.2. Đặc điểm của mạng xã hội

– Mạng xã hội là ứng dụng trên nền tảng Internet.

- Để thiết lập, cung cấp dịch vụ mạng xã hội trên nền tảng Internet tại Việt Nam, các doanh nghiệp cung cấp phải xin giấy phép thiết lập mạng xã hội trên Internet của Bộ thông tin và Truyền thông.

– Người dùng trên mạng xã hội phải tạo ra hồ sơ cá nhân theo yêu cầu và có tài khoản riêng.

– Mạng xã hội tạo ra các liên kết thông qua các tài khoản ảo do người dùng tạo ra.

– Nội dung trên mạng xã hội đều do chính người dùng tạo ra, chia sẻ.

+ Mạng xã hội tạo điều kiện cho sự phát triển của cộng đồng xã hội trên mạng bằng cách kết nối tài khoản của người dùng với tài khoản của các cá nhân, tổ chức khác.

Đặc điểm cơ bản của mạng xã hội đó chính là có sự tham gia trực tuyến của các cá nhân hay các chủ thể khác; mạng xã hội sẽ có các trang web mở, người tham gia tự xây dựng nội dung trong đó và các thành viên trong nhóm đó sẽ biết được các thông tin mà người dùng viết.

Hiện nay có rất nhiều các mạng xã hội, một số các loại mạng xã hội tiêu biểu hay được sử dụng ở nước ta phải đến ở đây là: Facebook, Zalo, Viber, YouTube, Tiktok,… Việc sử dụng mạng xã hội mang lại nhiều lợi ích nhưng cũng tồn tại rất nhiều bất cập.

2.3. Vai trò của mạng xã hội

Góc độ quản lý nhà nước, mạng xã hội là hệ thống thông tin cung cấp cho cộng đồng người sử dụng mạng các dịch vụ lưu trữ, cung cấp, sử dụng, tìm kiếm, chia sẻ và trao đổi thông tin với nhau, bao gồm dịch vụ tạo trang thông tin điện tử cá nhân, diễn đàn, trò chuyện trực tuyến, chia sẻ âm thanh, hình ảnh, video và các hình thức dịch vụ tương tự khác.

Góc độ văn hóa - xã hội, mạng xã hội là tập hợp các mối quan hệ giữa các cá nhân, nhóm cá nhân, tổ chức trên môi trường Internet. Chính vì thế, mạng xã hội có thể coi là một loại hình cộng đồng song mang tính chất ảo, trong đó bao gồm nhiều cộng đồng trực tuyến khác nhau nhằm thỏa mãn các nhu cầu về vật chất và tinh thần của con người. Một số cộng đồng như Facebook, YouTube, Zalo, Tiktok,… thu hút một số lượng lớn người tham gia, ngày càng đóng vai trò quan trọng trong đời sống xã hội.

Mạng xã hội góp phần tích cực vào sự phát triển nhận thức, tư duy và kỹ năng sống của con người.

Mạng xã hội đang ngày càng trở thành nơi cung cấp tin tức, kiến thức về tất cả các lĩnh vực của đời sống xã hội. Chỉ với một vài thao tác đơn giản, người dùng sẽ luôn nhận được những thông tin cập nhật kịp thời về lĩnh vực, vấn đề mà mình quan tâm theo dõi. Qua đó giúp họ có thể nắm bắt được các xu thế của đời sống phục vụ cho công việc và cuộc sống của mình. Bên cạnh đó, trên mạng xã hội có nhiều trang dạy kỹ năng sống như ngoại ngữ, nấu ăn, sửa chữa, giao tiếp, tâm lý, thể thao… giúp người dùng có những kỹ năng cơ bản cần thiết trong cuộc sống hiện đại mà không cần đến lớp hay đóng học phí.

Mạng xã hội góp phần tích cực vào sự phát triển của văn hóa cộng đồng.

Văn hóa mạng xã hội là một bộ phận của văn hóa cộng đồng và có ảnh hưởng ngày càng lớn đến văn hóa xã hội. Nhờ áp dụng tiến bộ của khoa học kỹ thuật, mạng xã hội cho phép người dùng có thể kết nối, tương tác với bạn bè, gia đình, cộng đồng ngày một thuận tiện hơn. Người dùng có thể dễ dàng chia sẽ tình cảm, niềm vui, nỗi buồn… với cộng đồng. Sự tham gia của cá nhân vào các công việc chung của cộng đồng cũng được thúc đẩy. Thực tế từ khi mạng xã hội phát triển, việc "dân biết, dân bàn, dân làm, dân kiểm tra" được thực hiện sinh động hơn. Công tác xã hội như cứu trợ thiên tai, xóa đói giảm nghèo… có nhiều khởi sắc. Nội lực của cộng đồng được phát huy hiệu quả hơn trong công cuộc phát triển kinh tế- xã hội. Các hình thức kinh doanh online trên mạng xã hội của cá nhân và doanh nghiệp ngày càng phát triển, mang tính chuyên nghiệp.

Mạng xã hội góp phần thúc đẩy quá trình hội nhập quốc tế trên lĩnh vực văn hóa của Việt Nam.

Các mạng xã hội xuyên quốc gia như Facebook, Youtube… đã tạo ra những cơ hội, khả năng tiếp xúc, giao lưu văn hóa, thúc đẩy xích lại gần nhau, hiểu biết lẫn nhau giữa dân tộc ta với các dân tộc khác trên thế giới. Thông qua mạng xã hội, thế giới biết đến Việt Nam hơn như một dân tộc yêu chuộng hòa bình, tôn trọng công lý, năng động với một kho tàng các giá trị văn hóa phong phú, đầy bản sắc.

2.4. Những mặt hạn chế của mạng xã hội

Bên cạnh mặt tích cực, mạng xã hội cũng tồn tại không ít những yếu tố tiêu cực, ảnh hưởng trực tiếp đến môi trường xã hội, lợi ích cộng đồng và an ninh trật tự, điển hình là:

Mạng xã hội đã và đang trở thành công cụ hàng đầu để các thế lực thù địch lợi dụng tiến hành phá hoại tư tưởng.

Trong những năm qua, các thế lực thù địch, phản động đã lập ra và sử dụng hàng ngàn trang mạng xã hội vào các hoạt động tuyên truyền phá hoại tư tưởng. Chúng tập trung xuyên tạc, nói xấu chủ nghĩa Mác- Lênin, tư tưởng Hồ Chí Minh và vai trò lãnh đạo của Đảng Cộng sản Việt Nam. Hiện nay, nhiều trang mạng xã hội của bọn phản động trong và ngoài nước như "Dân làm báo", "Quan làm báo"… thường xuyên đăng tải những bài viết với lời lẽ chống Đảng, chống chế độ một cách điên cuồng, mù quáng. Chúng tuyên truyền xuyên tạc chủ trương, chính sách của Đảng, Nhà nước, lợi dụng chiêu bài phản biện xã hội, đấu tranh chống tiêu cực, tham nhũng, bảo vệ môi trường… để đăng tải những bài viết có thông tin sai lệch, chưa được kiểm chứng, suy diễn xuyên tạc, từ đó kết luận các chủ trương, chính sách đó là sai lầm và đòi xóa bỏ. Lợi dụng những sơ hở, thiếu sót trong triển khai các chính sách phát triển kinh tế- xã hội của chính quyền các cấp, các vụ phức tạp như Đồng Tâm (Hà Nội), ô nhiễm môi trường biển do Formosa gây ra ở các tỉnh miền Trung, việc thảo luận dự luật đơn vị hành chính - kinh tế đặc biệt… để kích động dư luận, hình thành tâm lý phản kháng, tư tưởng bất mãn, chống đối, tiến tới kêu gọi biểu tình, bạo loạn lật đổ chế độ.

Mạng xã hội làm gia tăng nguy cơ lộ thông tin thuộc bí mật nhà nước.

Trong số 72 triệu người Việt Nam sử dụng mạng xã hội, có không ít người là cán bộ, đảng viên, làm việc trong các cơ quan, đơn vị có liên quan đến bí mật nhà nước. Nhiều người có thói quen thích chia sẻ thông tin về cuộc sống, công việc, hoạt động của cơ quan, đơn vị lên mạng xã hội hoặc sử dụng mạng xã hội làm công cụ liên lạc, trao đổi. Trong khi đó, hiểu biết về công tác bảo vệ bí mật nhà nước của một số cán bộ, đảng viên chưa cao, trách nhiệm ý thức bảo mật chưa tốt, làm gia tăng nguy cơ lộ lọt bí mật nhà nước. Lợi dụng các vụ lộ lọt bí mật nhà nước trên internet, nhiều đối tượng đã đăng tải lại các tài liệu mật trên mạng xã hội, tạo diễn đàn xuyên tạc, nói xấu chính quyền.

Mạng xã hội tác động tiêu cực đối với sự phát triển văn hóa.

Xã hội phát triển làm gia tăng nguy cơ xói mòn bản sắc văn hóa dân tộc. Khi mạng xã hội phát triển thì dòng chảy của những cuộc bá quyền, xâm lăng văn hóa trở nên mạnh mẽ hơn về cường độ, mở rộng về quy mô, tác động đến hầu hết các cá nhân, nhất là số người trẻ. Xuất hiện các trào lưu tuyên truyền, cổ vũ lối sống, các giá trị phương Tây, như tôn thờ tự do cá nhân, lối sống thực dụng, văn hóa đồi trụy, bạo lực… đi ngược lại truyền thống văn hóa dân tộc. Tình trạng nhiễu loạn thông tin, thật giả lẫn lộn trên mạng xã hội đang ở mức báo động, ảnh hưởng đến các giá trị văn hóa tốt đẹp của cộng đồng. Hoạt động tung tin đồn, giật gân câu "like" trên mạng xã hội ngày càng gia tăng, gây hoang mang trong dư luận. Một số vụ việc trên mạng xã hội (như BOT giao thông) thu hút số lượng rất lớn người quan tâm, theo dõi, hình thành tâm lý đám đông, áp lực dư luận, có thể tạo ra các giá trị lệch lạc hay khuynh hướng phức tạp trong văn hóa ứng xử.

Mạng xã hội đang trở thành công cụ, môi trường "màu mỡ" để tội phạm mạng lợi dụng hoạt động.

Với đặc tính ảo, mạng xã hội thường xuyên được các đối tượng phạm tội về hình sự, kinh tế, ma túy lợi dụng để hoạt động với các thủ đoạn như tạo tài khoản ảo để kết bạn, làm quen sau đó lừa đảo chiếm đoạt tiền, tài sản; tiến hành đánh cắp mật khẩu, chiếm giữ

quyền kiểm soát tài khoản trái phép để thu thập các thông tin cá nhân, nhất là những thông tin bí mật về tài chính, từ đó tìm cách đánh cắp, trục lợi. Một số đối tượng còn sử dụng mạng xã hội làm công cụ liên lạc trong quá trình mua bán, vận chuyển các loại hàng cấm, ma túy, vũ khí, vật liệu nổ và các hoạt động phạm tội khác.

Những năm gần đây, mạng xã hội đã có bước phát triển mạnh mẽ, tác động lớn đến đời sống xã hội ở hầu hết các quốc gia trên thế giới, trong đó có Việt Nam mạng xã hội đã trở thành một thuật ngữ phổ biến với những tính năng đa dạng cho phép người dùng kết nối, chia sẻ, tiếp nhận thông tin một cách nhanh chóng, hiệu quả. Không thể phủ nhận vai trò tích cực của mạng xã hội, song cũng phải nhận thấy, các thế lực thù địch và bọn tội phạm đã và đang biến nó thành công cụ đắc lực cho các hoạt động phá hoại tư tưởng, "diễn biến hòa bình" và các hoạt động phạm tội khác.

3. Sự cần thiết phải bảo vệ ninh mạng và ban hành Luật An ninh mạng

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, hệ thống dữ liệu lớn, hệ thống 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 6 năm trở lại đây, đã có 23 quốc gia trên thế giới ban hành trên 40 văn bản luật về bảo vệ 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 công nghệ thông tin đang bị các thế lực thù địch, phản động sử dụng để 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 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 từ 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 bản quy phạm pháp luật về an ninh mạng chưa được xây dụng, 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:

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.

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 thế 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 dụng 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.

3. Phạm vi điều chỉnh của Luật An ninh mạng

Đây là vấn đề được rất nhiều người quan tâm đặc biệt là cộng đồng mạng và giới trẻ. Điều 1 Luật An ninh mạng 2018 qui định rõ phạm vi điều chỉnh của Luật: "*Luật này quy định về hoạt động bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội trên không gian mạng; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan"*. An ninh mạng là sự 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.

Có thể nói, việc bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân khi sử dụng không gian mạng là vấn đề rất quan trọng nhưng chưa đặt ra từ khi mạng Internet được sử dụng ở Việt Nam. Vì vậy, trong một thời gian dài, đã có nhiều hoạt động sử dụng không gian mạng để kích động, chia rẽ, thậm chí xúc phạm nhân phẩm, xúc phạm tôn giáo, dân tộc. Đây là vấn đề rất mới, thể hiện quan điểm của các nhà lập pháp trong khía cạnh bảo vệ quyền, lợi ích hợp pháp của tổ chức, cá nhân gắn liền với an ninh quốc gia.

4. Mục đích của việc ban hành Luật An ninh mạng

Hoàn thiện cơ sở pháp lý ổn định về an ninh mạng theo hướng áp dụng các quy định pháp luật một cách đồng bộ khả thi trong thực tiễn thi hành. Phát huy các nguồn lực của đất nước để bảo đảm an ninh mạng, phát triển lĩnh vực an ninh mạng đáp ứng yêu cầu phát triển kinh tế xã hội, quốc phòng, an ninh, góp phần nâng cao chất lượng cuộc sống của nhân dân và bảo đảm quốc phòng, an ninh.

Bảo vệ chủ quyền, lợi ích, an ninh quốc gia, quyền và lợi ích hợp pháp của tổ chức, cá nhân tham gia hoạt động trên không gian mạng, xây dựng môi trường không gian mạng lành mạnh. Triển khai công tác an ninh mạng trên phạm vi toàn quốc, đẩy mạnh công tác giám sát, dự báo, ứng phó và diễn tập ứng phó sự cố an ninh mạng, bảo vệ hệ thống thông tin quan trọng về an, ninh quốc gia; đảm bảo hiệu quả công tác quản lý nhà nước trong lĩnh vực này.

Nâng cao năng lực tự chủ về an ninh mạng, hoàn thiện chính sách nghiên cứu, phát triển chiến lược, chia sẻ thông tin về an ninh mạng. Mở rộng hợp tác quốc tế về an ninh mạng trên cơ sở tôn trọng độc lập, chủ quyền, bình đẳng, cùng có lợi, phù hợp với pháp luật trong nước và điều ước quốc tế mà nước ta tham gia ký kết.

5. Vai trò của Luật An ninh mạng

Thứ nhất, là cơ sở pháp lý quan trọng để bảo vệ an ninh quốc gia; xử lý đối với các hành vi vi phạm pháp luật, như:

- Chống Nhà nước Cộng hòa xã hội chủ nghĩa 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 lôi kéo tụ tập đông người, gây rối an ninh trật tự, chống người thi hành công vu, cản trở hoạt động của cơ quan tô chức, gây mất ổn định về an ninh trật tự…

- 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;

- 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;

- 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).

- 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...

Thứ hai, nhằm bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia. Hệ thống thông tin quan trọng về an ninh quốc gia được quy định trong luật An ninh mạng là hệ thống thông tin khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ xâm phạm nghiêm trọng an ninh mạng. Với tiêu chí như trên, hệ thống thông tin quan trọng về an ninh quốc gia được xác định trong các lĩnh vực quan trọng đặc biệt đối với quốc gia như quân sự, an ninh, ngoại giao, cơ yếu; trong lĩnh vực đặc thù như lưu trữ, xử lý thông tin thuộc bí mật nhà nước; phục vụ hoạt động của các công trình quan trọng liên quan tới an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia hoặc những hệ thống thông tin quan trọng trong các lĩnh vực năng lượng, tài chính, ngân hàng, viễn thông, giao thông vận tải, tài nguyên và môi trường, hóa chất, y tế, văn hóa, báo chí. Chính phủ sẽ quy định cụ thể những hệ thống thông tin nào trong các lĩnh vực nêu trên thuộc Danh mục 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 được giao cho lực lượng chuyên trách bảo vệ an ninh mạng, trực tiếp là lực lượng An ninh mạng thuộc Bộ Công an, lực lượng Tác chiến Không gian mạng thuộc Bộ Quốc phòng Để bảo đảm phù hợp với hệ thống pháp luật trong nước, Luật An ninh mạng cũng giao Chính phủ quy định cụ thể việc phối hợp giữa Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông, Ban Cơ yếu Chính phủ, các bộ, ngành chức năng trong việc thẩm định, đánh giá, kiểm tra, giám sát, ứng phó, khắc phục sự cố đối với hệ thống thông tin quan trọng về an ninh quốc gia.

Thứ ba, nhằm phòng, chống tấn công mạng. Luật An ninh mạng là văn bản Luật đầu tiên quy định khái niệm của hoạt động "tấn công mạng". Theo đó "Tấn công mạng là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện từ để phá hoại, gây gián đoạn hoạt động của mạng viễn thống, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện từ." Đồng thời, quy định các nhóm hành vi cụ thể liên quan tới tấn công mạng tại Điều 17, 18, 19, 20 và Điều 2l; quy định cụ thể các nhóm giải pháp cụ thế để phòng, chống tấn công mạng, quy định trách nhiệm cụ thể của cơ quan chức năng, chủ quản hệ thống thông tin. Như vậy:

- Hệ thống thông tin của cơ quan, tổ chức, cá nhân được bảo vệ trước hoạt động tấn công mạng theo quy định của Luật An ninh mạng.

- Các hệ thống thông tin quan trọng về an ninh quốc gia được bảo vệ tương xứng với tầm quan trọng đối với an ninh quốc gia, trật tự an toàn xã hội.

- Quyền và lợi ích hợp pháp của tổ chức, cá nhân được bảo vệ trước các hành vi tấn công mạng.

- Luật An ninh mạng cũng quy định cụ thể cơ chế phối hợp phòng, chống tấn công mạng của các bộ, ngành chức năng, xác định trách nhiệm cụ thể của Bộ Công Thương.

6. Nội dung cơ bản của Luật An ninh mạng

Luật An ninh mạng 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.

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 ninh 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 (Chương III) quy định đầy đủ các biện pháp phòng ngừa, đấu tranh, xử lý nhằm loại bỏ các nguy cơ đe dọa, phát hiện và xửlý 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 dụng không gian mạng, công nghệ thông tin, phương tiện điện từ 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 ương 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 dư, 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 giá trị 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 mạng, 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, ủy ban nhân dân cấp tỉnh 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.

7. Các hành vi bị nghiêm cấm theo Luật An ninh mạng

Điều 8 Luật An ninh mạng 2018 quy định về các hành vi mà người sử dụng mạng xã hội bị cấm thực hiện trên không gian mạng:

1. Hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội bao gồm:

a) Đăng tải, phát tán thông tin trên không gian mạng có nội dung bị cấm theo Luật An ninh mạng (quy định tại các khoản 1, 2, 3, 4, 5 Điều 16; khoản 1 Điều 17 của Luật An ninh mạng);

b) Chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua mạng Internet; trộm cắp cước viễn thông quốc tế trên nền Internet; vi phạm bản quyền và sở hữu trí tuệ trên không gian mạng;

c) Giả mạo trang thông tin điện tử của cơ quan, tổ chức, cá nhân; làm giả, lưu hành, trộm cắp, mua bán, thu thập, trao đổi trái phép thông tin thẻ tín dụng, tài khoản ngân hàng của người khác; phát hành, cung cấp, sử dụng trái phép các phương tiện thanh toán;

d) Tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật;

đ) Hướng dẫn người khác thực hiện hành vi vi phạm pháp luật;

e) Hành vi khác sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội.

2. 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.

3. 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.

4. Thông tin 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 tổ chức, cá nhân khác.

5. 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;

6. Xúi giục, lôi kéo, kích động người khác phạm tội.

7. Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin quan trọng về an ninh quốc gia.

9. 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 máy tính, mạng viễn thông; phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử; xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác.

10. Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng.

11. Lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc để trục lợi.

8. Những thông tin bị nghiêm cấm tuyên truyền trên mạng

Điều 16 Luật An ninh mạng quy định các thông tin bị nghiêm cấm tuyên truyền trên mạng như sau:

Các thông tin tuyên truyền chống phá Nhà nước, kích động gây bạo loạn, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế gồm: Thông tin trên không gian mạng có nội dung tuyên xuyên tạc, phỉ báng chính quyền nhân dân; Thông tin chiến tranh tâm lý, kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước; Thông tin xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc.

Thông tin trên không gian mạng có nội dung kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng bao gồm: Kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân; Kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự.

Thông tin trên không gian mạng có nội dung làm nhục, vu khống bao gồm: Xúc phạm nghiêm trọng danh dự, uy tín, nhân phẩm của người khác; Thông tin bịa đặt, sai sự thật xâm phạm danh dự, uy tín, nhân phẩm hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của tổ chức, cá nhân khác.

Thông tin trên không gian mạng có nội dung xâm phạm trật tự quản lý kinh tế bao gồm: Thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá khác; Thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp, chứng khoán.

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 tổ chức, cá nhân khác.

9. Quy định trách nhiệm bảo vệ an ninh mạng

Điều 26 Luật An ninh mạng quy định về bảo đảm an ninh thông tin trên không gian mạng. Theo đó, các trang thông tin điện tử, cổng thông tin điện tử hoặc chuyên trang trên mạng xã hội của cơ quan, tổ chức, cá nhân không được cung cấp, đăng tải, truyền đưa thông tin có nội dung tuyên truyền chống Nhà nước CHXHCN 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.

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 Nam có trách nhiệm xác thực thông tin khi người dùng đăng ký tài khoản số; Bảo mật thông tin, tài khoản của người dùng; 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.

Chậm nhất là 24 giờ kể từ thời điểm có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an hoặc cơ quan có thẩm quyền của Bộ Thông tin và Truyền thông, các doanh nghiệp phải ngăn chặn việc chia sẻ thông tin, xoá bỏ các thông tin có nội dung vi phạm.

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 phải đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam. 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 tại Việt Nam.

10. Quy định về xử lý hành vi vi phạm Luật An ninh mạng

Người nào có hành vi vi phạm quy định của Luật An ninh mạng 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.

10.1. Xử phạt vi phạm hành chính *(qui định tại Nghị định số 15/2020/NĐ-CP ngày 03/02/2020 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử).*

10.1.1. Xử phạt vi phạm hành chính đối với hành vi vi phạm về an toàn thông tin mạng

10.1.1.1. Vi phạm quy định về cung cấp, sử dụng trái phép thông tin trên mạng (Điều 80 Nghị định 15/2020/NĐ-CP)

1. Phạt tiền từ 10.000.000 đồng đến 20.000.000 đồng đối hành vi bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của tổ chức, cá nhân khác trên môi trường mạng.

2. Phạt tiền từ 30.000.000 đồng đến 50.000.000 đồng đối với một trong các hành vi sau:

a) Truy cập trái phép vào mạng hoặc thiết bị số của người khác để chiếm quyền điều khiển thiết bị số hoặc thay đổi, xóa bỏ thông tin lưu trữ trên thiết bị số hoặc thay đổi tham số cài đặt thiết bị số hoặc thu thập thông tin của người khác;

b) Xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của tổ chức, cá nhân khác trên môi trường mạng;

c) Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin;

d) Ngăn chặn việc truy nhập đến thông tin của tổ chức, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép;

đ) Làm mất an toàn, bí mật thông tin của tổ chức, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

3. Hình thức xử phạt bổ sung:

Trục xuất khỏi lãnh thổ nước Cộng hòa xã hội chủ nghĩa Việt Nam đối với người nước ngoài có hành vi vi phạm quy định tại các khoản 1 và 2 Điều này.

10.1.1.2. Vi phạm quy định về sử dụng mạng nhằm chiếm đoạt tài sản (Điều 81 Nghị định 15/2020/NĐ-CP)

1. Phạt tiền từ 30.000.000 đồng đến 50.000.000 đồng đối với hành vi lợi dụng các phương tiện giao tiếp trực tuyến trên mạng Internet, mạng viễn thông nhằm chiếm đoạt tài sản của tổ chức, cá nhân có trị giá dưới 2.000.000 đồng.

2. Phạt tiền từ 70.000.000 đồng đến 100.000.000 đồng đối với một trong các hành vi sau:

a) Truy cập bất hợp pháp vào tài khoản của tổ chức, cá nhân nhằm chiếm đoạt tài sản có trị giá dưới 2.000.000 đồng;

b) Thiết lập hệ thống, cung cấp dịch vụ chuyển cuộc gọi quốc tế thành cuộc gọi trong nước phục vụ cho mục đích lừa đảo, chiếm đoạt tài sản có trị giá dưới 2.000.000 đồng;

c) Trộm cắp hoặc sử dụng trái phép thông tin về tài khoản, thẻ ngân hàng của tổ chức, cá nhân để chiếm đoạt, gây thiệt hại tài sản hoặc để thanh toán hàng hóa, dịch vụ có trị giá dưới 2.000.000 đồng.

3. Hình thức xử phạt bổ sung:

Tịch thu tang vật, phương tiện vi phạm hành chính đối với hành vi vi phạm quy định tại khoản 2 Điều này.

4. Biện pháp khắc phục hậu quả:

Buộc nộp lại số lợi bất hợp pháp có được do thực hiện hành vi vi phạm quy định tại các khoản 1 và 2 Điều này.

10.1.1.3. Vi phạm quy định về quản lý gửi thông tin trên mạng (Điều 82 Nghị định 15/2020/NĐ-CP)

1. Phạt tiền từ 10.000.000 đồng đến 20.000.000 đồng đối với một trong các hành vi sau:

a) 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;

b) Không có phương thức để người tiếp nhận thông tin từ chối việc tiếp nhận thông tin.

2. Phạt tiền từ 20.000.000 đồng đến 30.000.000 đồng đối với một trong các hành vi sau:

a) Giả mạo nguồn gốc gửi thông tin trên mạng;

b) Không cung cấp điều kiện kỹ thuật và nghiệp vụ cần thiết khi có yêu cầu của cơ quan nhà nước có thẩm quyền.

3. Phạt tiền từ 30.000.000 đồng đến 50.000.000 đồng đối với hành vi không áp dụng biện pháp ngăn chặn hoặc không xử lý khi nhận được thông báo của tổ chức, cá nhân về việc gửi thông tin vi phạm quy định của pháp luật.

10.1.1.4. Vi phạm quy định về thu thập, sử dụng thông tin cá nhân (Điều 84 Nghị định 15/2020/NĐ-CP)

1. Phạt tiền từ 10.000.000 đồng đến 20.000.000 đồng đối với một trong các hành vi sau:

a) Thu thập thông tin cá nhân khi chưa 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) Cung cấp thông tin cá nhân cho bên thứ ba khi chủ thể thông tin cá nhân đã yêu cầu ngừng cung cấp.

2. Phạt tiền từ 20.000.000 đồng đến 30.000.000 đồng đối với một trong các hành vi sau:

a) Sử dụng không đúng mục đích thông tin cá nhân đã thỏa thuận khi thu thập hoặc khi chưa có sự đồng ý của chủ thể thông tin cá nhân;

b) Cung cấp hoặc chia sẻ hoặc phát tán thông tin cá nhân đã thu thập, tiếp cận, kiểm soát cho bên thứ ba khi chưa có sự đồng ý của chủ thông tin cá nhân;

c) Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác.

3. Biện pháp khắc phục hậu quả:

Buộc hủy bỏ thông tin cá nhân do thực hiện hành vi vi phạm quy định tại điểm b khoản 1, các điểm b và c khoản 2 Điều này.

10.1.1.5. Vi phạm quy định về cập nhật, sửa đổi và hủy bỏ thông tin cá nhân (Điều 85 Nghị định 15/2020/NĐ-CP)

1. Phạt tiền từ 10.000.000 đồng đến 20.000.000 đồng đối với hành vi không thông báo cho chủ thể thông tin cá nhân sau khi hủy bỏ thông tin cá nhân đã lưu trữ hoặc chưa thực hiện được biện pháp phù hợp để bảo vệ thông tin cá nhân do yếu tố kỹ thuật.

2. Phạt tiền từ 20.000.000 đồng đến 30.000.000 đồng đối với một trong các hành vi sau:

a) Không cập nhật, sửa đổi, hủy bỏ thông tin cá nhân đã lưu trữ theo yêu cầu của chủ thể thông tin cá nhân hoặc không cung cấp cho chủ thể thông tin cá nhân quyền tiếp cận để tự cập nhật, sửa đổi, hủy bỏ thông tin cá nhân của họ;

b) Không hủy bỏ thông tin cá nhân đã được lưu trữ khi đã hoàn thành mục đích sử dụng hoặc hết thời hạn lưu trữ.

3. Phạt tiền từ 30.000.000 đồng đến 50.000.000 đồng đối với hành vi không áp dụng biện pháp quản lý hoặc biện pháp kỹ thuật theo quy định để bảo vệ thông tin cá nhân.

10.1.1.6. Vi phạm quy định về bảo đảm an toàn thông tin cá nhân trên mạng (Điều 86 Nghị định 15/2020/NĐ-CP)

1. Phạt tiền từ 10.000.000 đồng đến 20.000.000 đồng đối với hành vi tuân thủ không đầy đủ các tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn thông tin mạng.

2. Phạt tiền từ 20.000.000 đồng đến 30.000.000 đồng đối với hành vi không tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn thông tin mạng.

3. Phạt tiền từ 30.000.000 đồng đến 50.000.000 đồng đối với hành vi không áp dụng ngay biện pháp khắc phục, ngăn chặn khi có nguy cơ xảy ra sự cố an toàn thông tin mạng.

4. Phạt tiền từ 50.000.000 đồng đến 70.000.000 đồng đối với hành vi không áp dụng ngay biện pháp khắc phục, ngăn chặn trong khi xảy ra sự cố an toàn thông tin mạng.

10.1.2. Xử phạt vi phạm hành chính đối với hành vi vi phạm về chống thư rác, tin nhắn rác và cung cấp dịch vụ nội dung

10.1.2.1. Vi phạm qui định liên quan tới thư điện tử, tin nhắn cung cấp thông tin về sản phẩm, dịch vụ (Điều 94 Nghị định 15/2020/NĐ-CP)

1. Phạt tiền từ 1.000.000 đồng đến 2.000.000 đồng đối với hành vi cung cấp số điện thoại liên hệ trong các biển quảng cáo, rao vặt được treo, đặt, dán, vẽ các sản phẩm quảng cáo trên cột điện, trụ điện, cột tín hiệu giao thông, bờ tường, cây xanh, nơi công cộng.

2. Phạt tiền từ 5.000.000 đồng đến 10.000.000 đồng đối với một trong các hành vi:

a) Gửi thư điện tử quảng cáo, tin nhắn quảng cáo đến người nhận nhưng chưa được sự đồng ý của người nhận;

b) Gắn nhãn thư điện tử quảng cáo, tin nhắn quảng cáo không đúng hoặc không đầy đủ theo quy định.

3. Phạt tiền từ 10.000.000 đồng đến 20.000.000 đồng đối với một trong các hành vi sau:

a) Không gắn nhãn thư điện tử quảng cáo, tin nhắn quảng cáo theo quy định;

b) Không lưu lại thông tin đăng ký nhận quảng cáo, thông tin yêu cầu từ chối và thông tin xác nhận yêu cầu từ chối thư điện tử quảng cáo, tin nhắn quảng cáo;

c) Gửi tin nhắn quảng cáo, thư điện tử quảng cáo, tin nhắn qua mạng Internet khi chưa được cấp mã số quản lý hoặc có mã số quản lý không đúng mã số quản lý được Bộ Thông tin và Truyền thông cấp.

4. Phạt tiền từ 20.000.000 đồng đến 30.000.000 đồng đối với một trong các hành vi sau:

a) Không cung cấp miễn phí cho người sử dụng cơ chế tiếp nhận và xử lý các thông báo về thư rác;

b) Không có biện pháp để tránh mất mát và ngăn chặn sai thư điện tử của người sử dụng dịch vụ;

c) Không phối hợp với các nhà cung cấp dịch vụ Internet trong nước và quốc tế, nhà cung cấp dịch vụ tin nhắn trong và ngoài nước để hạn chế, ngăn chặn thư rác;

d) Không gửi ngay hoặc gửi thông tin xác nhận đã nhận được yêu cầu từ chối thư điện tử, tin nhắn không bảo đảm các yêu cầu theo quy định;

đ) Không có biện pháp giới hạn số lượng, tốc độ và tần suất nhắn tin;

e) Không giới hạn tần suất nhắn tin từ mỗi nguồn gửi hoặc không ngăn chặn các tin nhắn có nguy cơ gây mất an toàn, an ninh thông tin theo quy định;

g) Gửi thư điện tử quảng cáo hoặc tin nhắn quảng cáo nhưng không gửi bản sao nội dung tới hệ thống kỹ thuật của Bộ Thông tin và Truyền thông;

h) Che giấu tên, địa chỉ điện tử của mình khi gửi thư điện tử, tin nhắn;

i) Không chấm dứt việc gửi đến người nhận thư điện tử quảng cáo hoặc tin nhắn quảng cáo ngay sau khi nhận được yêu cầu từ chối của người nhận;

k) Không phối hợp với các doanh nghiệp viễn thông được cấp phép thiết lập mạng viễn thông di động trong và ngoài nước ngăn chặn tin nhắn rác;

l) Không thực hiện biện pháp ngăn chặn tin nhắn rác theo yêu cầu của cơ quan nhà nước có thẩm quyền;

m) Không ngăn chặn tin nhắn rác giả mạo nguồn gửi trước khi gửi tới người sử dụng dịch vụ;

n) Không ngừng cung cấp dịch vụ nội dung qua tin nhắn khi khách hàng yêu cầu;

o) Thực hiện không đầy đủ các yêu cầu điều phối, ngăn chặn, xử lý tin nhắn rác.

5. Phạt tiền từ 30.000.000 đồng đến 40.000.000 đồng đối với một trong các hành vi sau:

a) Không tuân thủ các yêu cầu điều phối, ngăn chặn, xử lý tin nhắn rác;

b) Không thực hiện yêu cầu xử lý các thông báo, phản ánh tin nhắn rác của Bộ Thông tin và Truyền thông;

c) Không thực hiện các biện pháp nhằm hạn chế thư điện tử rác theo yêu cầu của cơ quan nhà nước có thẩm quyền;

d) Không cung cấp thông tin và ngăn chặn các nguồn phát tán thư điện tử rác hoặc phần mềm độc hại theo yêu cầu của cơ quan nhà nước có thẩm quyền;

đ) Không thực hiện các biện pháp đánh giá tình trạng tin nhắn rác trên mạng viễn thông di động của nhà cung cấp dịch vụ tin nhắn theo hướng dẫn của Bộ Thông tin và Truyền thông.

6. Phạt tiền từ 60.000.000 đồng đến 80.000.000 đồng đối với một trong các hành vi sau:

a) Không có đầy đủ các hình thức từ chối nhận thư điện tử quảng cáo hoặc từ chối nhận tin nhắn quảng cáo;

b) Gửi hoặc phát tán thư điện tử rác, tin nhắn rác, phần mềm độc hại;

c) Tạo hàng loạt cuộc gọi nhỡ nhằm dụ dỗ người sử dụng gọi điện thoại, nhắn tin đến các số cung cấp dịch vụ nội dung để trục lợi hoặc để cung cấp thông tin, quảng cáo;

d) Khai thác, sử dụng các số dịch vụ, số thuê bao viễn thông không đúng mục đích;

đ) Số dịch vụ gọi tự do, số dịch vụ gọi giá cao được mở chiều gọi đi hoặc để gửi tin nhắn hoặc nhận tin nhắn.

7. Phạt tiền từ 80.000.000 đồng đến 100.000.000 đồng đối với hành vi quảng cáo bằng thư điện tử hoặc quảng cáo bằng tin nhắn hoặc cung cấp dịch vụ nhắn tin qua mạng Internet nhưng không có hệ thống tiếp nhận, xử lý yêu cầu từ chối của người nhận.

8. Phạt tiền từ 180.000.000 đồng đến 200.000.000 đồng đối với hành vi không ngăn chặn, thu hồi số thuê bao được dùng để phát tán tin nhắn rác.

9. Hình thức xử phạt bổ sung:

a) Đình chỉ hoạt động cung cấp dịch vụ từ 01 tháng đến 03 tháng đối với hành vi vi phạm quy định tại các điểm c, d, e và h khoản 4, các khoản 6 và 7 Điều này;

b) Tước quyền sử dụng mã số quản lý, tên định danh từ 01 tháng đến 03 tháng đối với hành vi vi phạm quy định tại các điểm a và b khoản 3, các điểm d, g, h, i và o khoản 4, các điểm a và b khoản 6 Điều này.

10. Biện pháp khắc phục hậu quả:

a) Buộc hoàn trả hoặc buộc nộp lại số lợi bất hợp pháp có được do thực hiện hành vi vi phạm quy định tại các điểm d và đ khoản 6 Điều này;

b) Buộc thu hồi đầu số, kho số viễn thông do thực hiện hành vi vi phạm tại điểm h khoản 4, các điểm b và c khoản 5 và khoản 6 Điều này.

10.1.2.2. Vi phạm qui định về cung cấp dịch vụ thư điện tử, tin nhắn quảng cáo, dịch vụ nội dung qua tin nhắn (Điều 95 Nghị định 15/2020/NĐ-CP)

1. Phạt tiền từ 10.000.000 đồng đến 20.000.000 đồng đối với một trong các hành vi sau:

a) Không có trang thông tin điện tử sử dụng tên miền quốc gia Việt Nam ".vn" khi cung cấp dịch vụ gửi thư điện tử quảng cáo hoặc dịch vụ nhắn tin qua mạng Internet hoặc dịch vụ nội dung qua tin nhắn;

b) Cung cấp không đầy đủ hoặc không rõ ràng thông tin về các dịch vụ trên trang thông tin điện tử trước khi cung cấp dịch vụ gồm có: tên dịch vụ, mã lệnh tương ứng, mô tả dịch vụ, cách thức sử dụng, giá cước dịch vụ tương ứng, hướng dẫn hủy dịch vụ, số điện thoại hỗ trợ khách hàng, cam kết đồng ý sử dụng dịch vụ.

2. Phạt tiền từ 20.000.000 đồng đến 30.000.000 đồng đối với một trong các hành vi sau:

a) Cung cấp dịch vụ quảng cáo bằng thư điện tử hoặc dịch vụ quảng cáo bằng tin nhắn hoặc dịch vụ nội dung qua tin nhắn hoặc dịch vụ nhắn tin qua mạng Internet khi chưa được cấp mã số quản lý;

b) Khi quảng cáo, cung cấp thông tin về dịch vụ nội dung qua tin nhắn, nhắn tin trúng thưởng, chương trình bình chọn, quyên góp, ủng hộ qua tin nhắn trên báo in, báo hình, báo điện tử, trang thông tin điện tử, Internet, tin nhắn, thư điện tử, nhưng không cung cấp thông tin về giá, giá cước và loại thiết bị phù hợp để sử dụng bằng tiếng Việt Nam một cách dễ đọc; hoặc giá cước hiển thị không cùng kiểu với mã lệnh, không ngay sát mã lệnh hoặc có kích thước nhỏ hơn 2/3 kích thước của mã lệnh;

c) Không cung cấp thông tin về giá cước trước khi tính cước khi người sử dụng gọi điện tới tổng đài dịch vụ gọi giá cao, dịch vụ giải đáp thông tin;

d) Không hướng dẫn thuê bao gửi thông báo tin nhắn rác và phản hồi các thông báo về tin nhắn rác tiếp nhận được;

đ) Lưu trữ dữ liệu cung cấp dịch vụ nội dung qua tin nhắn không đầy đủ theo quy định.

3. Phạt tiền từ 50.000.000 đồng đến 70.000.000 đồng đối với một trong các hành vi:

a) Cung cấp thông tin về sản phẩm, dịch vụ bằng thư điện tử mà máy chủ gửi thư điện tử không đặt tại Việt Nam;

b) Cung cấp dịch vụ nhắn tin qua mạng Internet có máy chủ dịch vụ gửi tin nhắn không đặt tại Việt Nam;

c) Cung cấp thông tin về sản phẩm, dịch vụ bằng tin nhắn không sử dụng số gửi tin nhắn được cấp theo quy định;

d) Cung cấp dịch vụ quảng cáo bằng thư điện tử, quảng cáo bằng tin nhắn không có hệ thống tiếp nhận, xử lý yêu cầu từ chối nhận thư điện tử quảng cáo, tin nhắn quảng cáo;

đ) Không cung cấp miễn phí chức năng tiếp nhận thông báo về tin nhắn rác hoặc thư điện tử rác từ người sử dụng;

e) Không triển khai hệ thống ngăn chặn tin nhắn rác có khả năng ngăn chặn tin nhắn rác theo nguồn gửi hoặc từ khóa trong nội dung tin nhắn gửi;

g) Không cung cấp dịch vụ gửi nhận tin nhắn, dịch vụ gửi nhận tin nhắn sử dụng tên định danh cho các nhà cung cấp dịch vụ đã được cấp mã số quản lý;

h) Không cho phép doanh nghiệp đã được cấp mã số quản lý kết nối kỹ thuật với hệ thống của mình, để cung cấp dịch vụ;

i) Không lưu trữ dữ liệu cung cấp dịch vụ nội dung qua tin nhắn đầy đủ theo quy định;

k) Không cung cấp thông tin về giá cước khi người sử dụng gọi điện tới tổng đài dịch vụ gọi giá cao, dịch vụ giải đáp thông tin.

4. Phạt tiền từ 140.000.000 đồng đến 170.000.000 đồng đối với hành vi thu cước dịch vụ đối với các tin nhắn lỗi hoặc tin nhắn không được cung cấp dịch vụ hoặc tin nhắn đã được cung cấp dịch vụ nhưng có nội dung khác với mã lệnh mà doanh nghiệp công bố hoặc tin nhắn do người dùng bị lừa đảo.

5. Hình thức xử phạt bổ sung:

a) Đình chỉ hoạt động cung cấp dịch vụ từ 01 tháng đến 03 tháng đối với hành vi vi phạm quy định tại điểm h khoản 3, khoản 4 Điều này;

b) Tước quyền sử dụng mã số quản lý từ 01 tháng đến 03 tháng đối với hành vi vi phạm quy định tại điểm a khoản 1, điểm đ khoản 2, các khoản 3 và 4 Điều này.

6. Biện pháp khắc phục hậu quả:

a) Buộc hoàn trả hoặc buộc nộp lại số lợi bất hợp pháp có được do thực hiện hành vi vi phạm quy định tại điểm c khoản 2, điểm k khoản 3 và khoản 4 Điều này;

b) Buộc thu hồi mã số quản lý, tên định danh do thực hiện hành vi vi phạm quy định tại các điểm a khoản 1, điểm đ khoản 2, các điểm a, b, c và d khoản 3 và khoản 4 Điều này.

10.1.2.3. Vi phạm các quy định về trách nhiệm sử dụng dịch vụ mạng xã hội (Điều 101 Nghị định 15/2020/NĐ-CP)

1. Phạt tiền từ 10.000.000 đồng đến 20.000.000 đồng đối với hành vi lợi dụng mạng xã hội để thực hiện một trong các hành vi sau:

a) Cung cấp, chia sẻ thông tin giả mạo, thông tin sai sự thật, xuyên tạc, vu khống, xúc phạm uy tín của cơ quan, tổ chức, danh dự, nhân phẩm của cá nhân;

b) Cung cấp, chia sẻ thông tin cổ súy các hủ tục, mê tín, dị đoan, dâm ô, đồi trụy, không phù hợp với thuần phong, mỹ tục của dân tộc;

c) Cung cấp, chia sẻ thông tin miêu tả tỉ mỉ hành động chém, giết, tai nạn, kinh dị, rùng rợn;

d) Cung cấp, chia sẻ thông tin bịa đặt, gây hoang mang trong Nhân dân, kích động bạo lực, tội ác, tệ nạn xã hội, đánh bạc hoặc phục vụ đánh bạc;

đ) Cung cấp, chia sẻ các tác phẩm báo chí, văn học, nghệ thuật, xuất bản phẩm mà không được sự đồng ý của chủ thể quyền sở hữu trí tuệ hoặc chưa được phép lưu hành hoặc đã có quyết định cấm lưu hành hoặc tịch thu;

e) Quảng cáo, tuyên truyền, chia sẻ thông tin về hàng hóa, dịch vụ bị cấm;

g) Cung cấp, chia sẻ hình ảnh bản đồ Việt Nam nhưng không thể hiện hoặc thể hiện không đúng chủ quyền quốc gia;

h) Cung cấp, chia sẻ đường dẫn đến thông tin trên mạng có nội dung bị cấm.

2. Phạt tiền từ 20.000.000 đồng đến 30.000.000 đồng đối với hành vi tiết lộ thông tin thuộc danh mục bí mật nhà nước, bí mật đời tư của cá nhân và bí mật khác mà chưa đến mức truy cứu trách nhiệm hình sự.

3. Biện pháp khắc phục hậu quả:

Buộc gỡ bỏ thông tin sai sự thật hoặc gây nhầm lẫn hoặc thông tin vi phạm pháp luật do thực hiện hành vi vi phạm quy định tại các khoản 1 và 2 Điều này.

10.1.2.3. Vi phạm quy định về người chơi (Điều 106 Nghị định 15/2020/NĐ-CP)

1. Phạt cảnh cáo đối với hành vi đăng ký không đúng thông tin cá nhân khi chơi các trò chơi điện tử G1.

2. Phạt tiền từ 600.000 đồng đến 1.000.000 đồng đối với hành vi không chấp hành quy định về quản lý giờ chơi tại điểm cung cấp dịch vụ trò chơi điện tử công cộng.

3. Phạt tiền từ 2.000.000 đồng đến 3.000.000 đồng đối với một trong các hành vi sau:

a) Lợi dụng trò chơi điện tử để thực hiện hành vi vi phạm pháp luật, gây mất trật tự, an toàn xã hội và an ninh quốc gia;

b) Mua, bán vật phẩm ảo hoặc đơn vị ảo hoặc điểm thưởng.

10.2. Truy cứu trách nhiệm hình sự (Bộ luật hình sự 2015, sửa đổi bổ sung 2017 qui định về tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông)

10.2.1. Tội sản xuất, mua bán, trao đổi hoặc tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật (truy cứu trách nhiệm hình sự đối với người từ đủ 16 tuổi) (Điều 285 Bộ luật hình sự 2015)

1. Người nào sản xuất, mua bán, trao đổi hoặc tặng cho công cụ, thiết bị, phần mềm có tính năng tấn công mạng máy tính, mạng viễn thông, phương tiện điện tử để sử dụng vào mục đích trái pháp luật, thì bị phạt tiền từ 20.000.000 đồng đến 100.000.000 đồng, phạt cải tạo không giam giữ đến 02 năm hoặc phạt tù từ 03 tháng đến 02 năm.

2. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tiền từ 100.000.000 đồng đến 500.000.000 đồng hoặc phạt tù từ 01 năm đến 05 năm:

a) Có tổ chức;

b) Phạm tội 02 lần trở lên;

c) Có tính chất chuyên nghiệp;

d) Thu lợi bất chính từ 50.000.000 đồng đến dưới 500.000.000 đồng;

đ) Gây thiệt hại về tài sản từ 100.000.000 đồng đến dưới 1.000.000.000 đồng;

e) Tái phạm nguy hiểm.

3. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tiền từ 500.000.000 đồng đến 1.000.000.000 đồng hoặc phạt tù từ 03 năm đến 07 năm:

a) Thu lợi bất chính 500.000.000 đồng trở lên;

b) Gây thiệt hại về tài sản 1.000.000.000 đồng trở lên.

4. Người phạm tội còn có thể bị phạt tiền từ 5.000.000 đồng đến 100.000.000 đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ 01 năm đến 05 năm hoặc tịch thu một phần hoặc toàn bộ tài sản.

10.2.2. Tội phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử (truy cứu trách nhiệm hình sự đối với người từ đủ 14 tuổi) (Điều 286 Bộ luật hình sự 2015)

1. Người nào cố ý phát tán chương trình tin học gây hại cho mạng máy tính, mạng viễn thông, phương tiện điện tử thuộc một trong các trường hợp sau đây, thì bị phạt tiền từ 50.000.000 đồng đến 200.000.000 đồng, phạt cải tạo không giam giữ đến 03 năm hoặc phạt tù từ 06 tháng đến 03 năm:

a) Thu lợi bất chính từ 50.000.000 đồng đến dưới 200.000.000 đồng;

b) Gây thiệt hại từ 50.000.000 đồng đến dưới 300.000.000 đồng;

c) Làm lây nhiễm từ 50 phương tiện điện tử đến dưới 200 phương tiện điện tử hoặc hệ thống thông tin có từ 50 người sử dụng đến dưới 200 người sử dụng;

d) Đã bị xử phạt vi phạm hành chính về hành vi này hoặc đã bị kết án về tội này, chưa được xóa án tích mà còn vi phạm.

2. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tiền từ 200.000.000 đồng đến 500.000.000 đồng hoặc phạt tù từ 03 năm đến 07 năm:

a) Có tổ chức;

b) Thu lợi bất chính từ 200.000.000 đồng đến dưới 500.000.000 đồng;

c) Gây thiệt hại từ 300.000.000 đồng đến dưới 1.000.000.000 đồng;

d) Làm lây nhiễm từ 200 phương tiện điện tử đến dưới 500 phương tiện điện tử hoặc hệ thống thông tin có từ 200 người sử dụng đến dưới 500 người sử dụng;

đ) Tái phạm nguy hiểm.

3. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ 07 năm đến 12 năm:

a) Đối với hệ thống dữ liệu thuộc bí mật nhà nước; hệ thống thông tin phục vụ quốc phòng, an ninh;

b) Đối với cơ sở hạ tầng thông tin quốc gia; hệ thống thông tin điều hành lưới điện quốc gia; hệ thống thông tin tài chính, ngân hàng; hệ thống thông tin điều khiển giao thông;

c) Thu lợi bất chính 500.000.000 đồng trở lên;

d) Gây thiệt hại 1.000.000.000 đồng trở lên;

đ) Làm lây nhiễm 500 phương tiện điện tử trở lên hoặc hệ thống thông tin có từ 500 người sử dụng trở lên.

4. Người phạm tội còn có thể bị phạt tiền từ 30.000.000 đồng đến 200.000.000 đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ 01 năm đến 05 năm.

10.2.3. Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử (truy cứu trách nhiệm hình sự đối với người từ đủ 14 tuổi) (Điều 287 Bộ luật hình sự 2015)

1. Người nào tự ý xóa, làm tổn hại hoặc thay đổi phần mềm, dữ liệu điện tử hoặc ngăn chặn trái phép việc truyền tải dữ liệu của mạng máy tính, mạng viễn thông, phương tiện điện tử hoặc có hành vi khác cản trở hoặc gây rối loạn hoạt động của mạng máy tính,

mạng viễn thông, phương tiện điện tử thuộc một trong các trường hợp sau đây, nếu không thuộc trường hợp quy định tại Điều 286 và Điều 289 của Bộ luật này, thì bị phạt tiền từ 30.000.000 đồng đến 200.000.000 đồng hoặc phạt tù từ 06 tháng đến 03 năm:

a) Thu lợi bất chính từ 50.000.000 đồng đến dưới 200.000.000 đồng;

b) Gây thiệt hại từ 100.000.000 đồng đến dưới 500.000.000 đồng;

c) Làm tê liệt, gián đoạn, ngưng trệ hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử từ 30 phút đến dưới 24 giờ hoặc từ 03 lần đến dưới 10 lần trong thời gian 24 giờ;

d) Làm đình trệ hoạt động của cơ quan, tổ chức từ 24 giờ đến dưới 72 giờ;

đ) Đã bị xử phạt vi phạm hành chính về hành vi này hoặc đã bị kết án về tội này, chưa được xóa án tích mà còn vi phạm.

2. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tiền từ 200.000.000 đồng đến 1.000.000.000 đồng hoặc phạt tù từ 03 năm đến 07 năm:

a) Có tổ chức;

b) Lợi dụng quyền quản trị mạng máy tính, mạng viễn thông;

c) Tái phạm nguy hiểm;

d) Thu lợi bất chính từ 200.000.000 đồng đến dưới 1.000.000.000 đồng;

đ) Gây thiệt hại từ 500.000.000 đồng đến dưới 1.500.000.000 đồng;

e) Làm tê liệt, gián đoạn, ngưng trệ hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử từ 24 giờ đến dưới 168 giờ hoặc từ 10 lần đến dưới 50 lần trong thời gian 24 giờ;

g) Làm đình trệ hoạt động của cơ quan, tổ chức từ 72 giờ đến dưới 168 giờ.

3. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ 07 năm đến 12 năm:

a) Đối với hệ thống dữ liệu thuộc bí mật nhà nước; hệ thống thông tin phục vụ quốc phòng, an ninh;

b) Đối với cơ sở hạ tầng thông tin quốc gia; hệ thống thông tin điều hành lưới điện quốc gia; hệ thống thông tin tài chính295, ngân hàng; hệ thống thông tin điều khiển giao thông;

c) Thu lợi bất chính 1.000.000.000 đồng trở lên;

d) Gây thiệt hại 1.500.000.000 đồng trở lên;

đ) Làm tê liệt, gián đoạn, ngưng trệ hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử 168 giờ trở lên hoặc 50 lần trở lên trong thời gian 24 giờ,

e) Làm đình trệ hoạt động của cơ quan, tổ chức 168 giờ trở lên.

4. Người phạm tội còn có thể bị phạt tiền từ 30.000.000 đồng đến 200.000.000 đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ 01 năm đến 05 năm.

10.2.4. Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông (truy cứu trách nhiệm hình sự đối với người từ đủ 16 tuổi) (Điều 288 Bộ luật hình sự 2015)

1. Người nào thực hiện một trong các hành vi sau đây, thu lợi bất chính từ 50.000.000 đồng đến dưới 200.000.000 đồng hoặc gây thiệt hại từ 100.000.000 đồng đến dưới 500.000.000 đồng hoặc gây dư luận xấu làm giảm uy tín của Cơ quan, tổ chức, cá

nhân, thì bị phạt tiền từ 30.000.000 đồng đến 200.000.000 đồng, phạt cải tạo không giam giữ đến 03 năm hoặc bị phạt tù từ 06 tháng đến 03 năm:

a) Đưa lên mạng máy tính, mạng viễn thông những thông tin trái với quy định của pháp luật, nếu không thuộc một trong các trường hợp quy định tại các điều 117, 155, 156 và 326 của Bộ luật này;

b) Mua bán, trao đổi, tặng cho, sửa chữa, thay đổi hoặc công khai hóa thông tin riêng hợp pháp của cơ quan, tổ chức, cá nhân trên mạng máy tính, mạng viễn thông mà không được phép của chủ sở hữu thông tin đó;

c) Hành vi khác sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông.

2. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tiền từ 200.000.000 đồng đến 1.000.000.000 đồng hoặc phạt tù từ 02 năm đến 07 năm:

a) Có tổ chức;

b) Lợi dụng quyền quản trị mạng máy tính, mạng viễn thông;

c) Thu lợi bất chính 200.000.000 đồng trở lên;

d) Gây thiệt hại 500.000.000 đồng trở lên;

đ) Xâm phạm bí mật cá nhân dẫn đến người bị xâm phạm tự sát;

e) Gây ảnh hưởng xấu đến an ninh, trật tự, an toàn xã hội hoặc quan hệ đối ngoại của Việt Nam;

g) Dẫn đến biểu tình.

3. Người phạm tội còn có thể bị phạt tiền từ 20.000.000 đồng đến 200.000.000 đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ 01 năm đến 05 năm.

10.2.5. Tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác (truy cứu trách nhiệm hình sự đối với người từ đủ 14 tuổi) (Điều 289 Bộ luật hình sự 2015)

1. Người nào cố ý vượt qua cảnh báo, mã truy cập, tường lửa, sử dụng quyền quản trị của người khác hoặc bằng phương thức khác xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác chiếm quyền điều khiển; can thiệp vào chức năng hoạt động của phương tiện điện tử; lấy cắp, thay đổi, hủy hoại, làm giả dữ liệu hoặc sử dụng trái phép các dịch vụ, thì bị phạt tiền từ 50.000.000 đồng đến 300.000.000 đồng hoặc phạt tù từ 01 năm đến 05 năm.

2. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tiền từ 300.000.000 đồng đến 1.000.000.000 đồng hoặc bị phạt tù từ 03 năm đến 07 năm:

a) Có tổ chức;

b) Lợi dụng chức vụ, quyền hạn;

c) Thu lợi bất chính từ 200.000.000 đồng đến dưới 500.000.000 đồng;

d) Gây thiệt hại từ 300.000.000 đồng đến dưới 1.000.000.000 đồng;

đ) Đối với trạm trung chuyển internet quốc gia, hệ thống cơ Sở dữ liệu tên miền và hệ thống máy chủ tên miền quốc gia;

e) Tái phạm nguy hiểm.

3. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ 07 năm đến 12 năm:

a) Đối với hệ thống dữ liệu thuộc bí mật nhà nước; hệ thống thông tin phục vụ quốc phòng, an ninh;

b) Đối với cơ sở hạ tầng thông tin quốc gia; hệ thống thông tin điều hành lưới điện quốc gia; hệ thống thông tin tài chính, ngân hàng; hệ thống thông tin điều khiển giao thông;

c) Thu lợi bất chính 500.000.000 đồng trở lên;

d) Gây thiệt hại 1.000.000.000 đồng trở lên.

4. Người phạm tội còn có thể bị phạt tiền từ 5.000.000 đồng đến 50.000.000 đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ 01 năm đến 05 năm.

10.2.6. Tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản (truy cứu trách nhiệm hình sự đối với người từ đủ 14 tuổi) (Điều 290 Bộ luật hình sự 2015)

1. Người nào sử dụng mạng máy tính, mạng viễn thông hoặc phương tiện điện tử thực hiện một trong những hành vi sau đây, nếu không thuộc một trong các trường hợp quy định tại Điều 173 và Điều 174 của Bộ luật này, thì bị phạt cải tạo không giam giữ đến 03 năm hoặc phạt tù từ 06 tháng đến 03 năm:

a) Sử dụng thông tin về tài khoản, thẻ ngân hàng của Cơ quan, tổ chức, cá nhân để chiếm đoạt tài sản của chủ tài khoản, chủ thẻ hoặc thanh toán hàng hóa, dịch vụ;

b) Làm, tàng trữ, mua bán, sử dụng, lưu hành thẻ ngân hàng giả nhằm chiếm đoạt tài sản của chủ tài khoản, chủ thẻ hoặc thanh toán hàng hóa, dịch vụ;

c) Truy cập bất hợp pháp vào tài khoản của cơ quan, tổ chức, cá nhân nhằm chiếm đoạt tài sản;

d) Lừa đảo trong thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp hoặc giao dịch chứng khoán qua mạng nhằm chiếm đoạt tài sản;

đ) Thiết lập, cung cấp trái phép dịch vụ viễn thông, internet nhằm chiếm đoạt tài sản.

2. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ 02 năm đến 07 năm:

a) Có tổ chức;

b) Phạm tội 02 lần trở lên;

c) Có tính chất chuyên nghiệp;

d) Số lượng thẻ giả từ 50 thẻ đến dưới 200 thẻ;

đ) Chiếm đoạt tài sản trị giá từ 50.000.000 đồng đến dưới 200.000.000 đồng;

e) Gây thiệt hại từ 50.000.000 đồng đến dưới 300.000.000 đồng;

g) Tái phạm nguy hiểm.

3. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ 07 năm đến 15 năm:

a) Chiếm đoạt tài sản trị giá từ 200.000.000 đồng đến dưới 500.000.000 đồng;

b) Gây thiệt hại từ 300.000.000 đồng đến dưới 500.000.000 đồng;

c) Số lượng thẻ giả từ 200 thẻ đến dưới 500 thẻ.

4. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ 12 năm đến 20 năm:

a) Chiếm đoạt tài sản trị giá 500.000.000 đồng trở lên;

b) Gây thiệt hại 500.000.000 đồng trở lên;

c) Số lượng thẻ giả 500 thẻ trở lên.

5. Người phạm tội còn có thể bị phạt tiền từ 20.000.000 đồng đến 100.000.000 đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ 01 năm đến 05 năm hoặc tịch thu một phần hoặc toàn bộ tài sản.

10.2.7. Tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng (truy cứu trách nhiệm hình sự đối với người từ đủ 16 tuổi) (Điều 291 Bộ luật hình sự 2015)

1. Người nào thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng của người khác với số lượng từ 20 tài khoản đến dưới 50 tài khoản hoặc thu lợi bất chính từ 20.000.000 đồng đến dưới 50.000.000 đồng, thì bị phạt tiền từ 20.000.000 đồng đến 100.000.000 đồng hoặc phạt cải tạo không giam giữ đến 03 năm.

2. Phạm tội thuộc một trong những trường hợp sau đây, thì bị phạt tiền từ 100.000.000 đồng đến 200.000.000 đồng hoặc phạt tù từ 03 tháng đến 02 năm:

a) Thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng của người khác với số lượng từ 50 tài khoản đến dưới 200 tài khoản;

b) Có tổ chức;

c) Có tính chất chuyên nghiệp;

d) Thu lợi bất chính từ 50.000.000 đồng đến dưới 200.000.000 đồng;

đ) Tái phạm nguy hiểm.

3. Phạm tội thuộc một trong những trường hợp sau đây, thì bị phạt tiền từ 200.000.000 đồng đến 500.000.000 đồng hoặc phạt tù từ 02 năm đến 07 năm:

a) Thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng của người khác với số lượng 200 tài khoản trở lên;

b) Thu lợi bất chính 200.000.000 đồng trở lên.

4. Người phạm tội còn có thể bị phạt tiền từ 10.000.000 đồng đến 50.000.000 đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ 01 năm đến 05 năm hoặc tịch thu một phần hoặc toàn bộ tài sản.

10.2.8. Tội sử dụng trái phép tần số vô tuyến điện dành riêng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu hộ, cứu nạn, quốc phòng, an ninh (truy cứu trách nhiệm hình sự đối với người từ đủ 16 tuổi) (Điều 293 Bộ luật hình sự 2015)

1. Người nào sử dụng trái phép tần số vô tuyến điện dành riêng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu hộ, cứu nạn, quốc phòng, an ninh vào mục đích khác gây thiệt hại từ 200.000.000 đồng đến dưới 500.000.000 đồng hoặc đã bị xử phạt vi phạm hành chính về hành vi này hoặc đã bị kết án về tội này, chưa được xóa án tích mà còn vi phạm, thì bị phạt tiền từ 50.000.000 đồng đến 100.000.000 đồng hoặc phạt cải tạo không giam giữ đến 03 năm.

2. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ 01 năm đến 05 năm:

a) Có tổ chức;

b) Gây thiệt hại 500.000.000 đồng trở lên;

c) Tái phạm nguy hiểm.

10.2.9. Tội cố ý gây nhiễu có hại (truy cứu trách nhiệm hình sự đối với người từ đủ 16 tuổi) (Điều 294 Bộ luật hình sự 2015)

1. Người nào cố ý gây nhiễu có hại, cản trở hoạt động bình thường của hệ thống thông tin vô tuyến điện gây thiệt hại từ 200.000.000 đồng đến dưới 500.000.000 đồng hoặc đã bị xử phạt vi phạm hành chính về hành vi này hoặc đã bị kết án về tội này, chưa được xóa án tích mà còn vi phạm, thì bị phạt tiền từ 50.000.000 đồng đến 100.000.000 đồng hoặc phạt cải tạo không giam giữ đến 03 năm.

2. Phạm tội thuộc một trong các trường hợp sau, thì bị phạt tù từ 01 năm đến 05 năm:

a) Có tổ chức;

b) Gây thiệt hại 500.000.000 đồng trở lên;

c) Tái phạm nguy hiểm.

11. Những hành vi vi phạm Luật An ninh mạng thường gặp trong thực tiễn

(1) Kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự;

(2) Xúc phạm nghiêm trọng danh dự, uy tín, nhân phẩm của người khác;

(3) Thông tin bịa đặt, sai sự thật xâm phạm danh dự, uy tín, nhân phẩm hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác;

(4) Thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá khác;

(5) Thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp, chứng khoán;

(6) Thông tin trên không gian mạng có nội dung bịa đặt, 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;

(7) Chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân;

(8) Đưa lên không gian mạng những thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trái quy định của pháp luật;

(9) Cố ý nghe, ghi âm, ghi hình trái phép các cuộc đàm thoại;

(10) Đăng tải, phát tán thông tin trên không gian mạng có nội dung bị cấm theo quy định tại các khoản 1, 2, 3, 4 và 5 Điều 16 và hành vi quy định tại khoản 1 Điều 17 của Luật An ninh mạng;

(11) Chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua mạng Internet; trộm cắp cước viễn thông quốc tế trên nền Internet; vi phạm bản quyền và sở hữu trí tuệ trên không gian mạng;

(12) Tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật;

(13) Hướng dẫn người khác thực hiện hành vi vi phạm pháp luật;

(14) Phát tán chương trình tin học gây hại cho mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử.

12. Nhận diện những thủ đoạn lừa đảo của tội phạm mạng

12.1. Kết bạn, làm quen trên mạng xã hội để lừa đảo

Các đối tượng thường là người nước ngoài sử dụng mạng xã hội như Facebook, Zalo... để kết bạn, làm quen với người bị hại để tạo sự tin tưởng. Sau một thời gian, đối tượng thông báo gửi quà là tiền mặt hoặc tài sản có giá trị rất lớn qua đường hàng không. Sau đó, có đối tượng người Việt Nam giả danh nhân viên sân bay, hải quan yêu cầu người bị hại nộp tiền để nhận được quà. Các đối tượng giả danh tạo ra rất nhiều lý do chưa nhận được quà để người bị hại chuyển tiền làm nhiều lần vào tài khoản ngân hàng do đối tượng cung cấp để chiếm đoạt. Khi người bị hại không còn khả năng tiếp tục chuyển tiền, các đối tượng bỏ số điện thoại, xóa tài khoản Facebook, Zalo...

12.2. Giả danh cán bộ công an, viện kiểm sát, tòa án

Các đối tượng dùng phần mềm công nghệ cao (Voice over IP) có chức năng giả mạo số điện thoại CQNN, tự xưng là cán bộ Công an / Viện kiểm sát / Tòa án báo người bị hại có liên đến một vụ án hình sự đang điều tra, làm họ hoang mang, lo sợ để cung cấp thông tin cá nhân và tài khoản. Sau đó, đối tượng yêu cầu người bị hại chuyển tiền vào các tài khoản chỉ định, cung cấp mã OTP / hướng dẫn bị hại tải ứng dụng giả mạo có tên "Bộ Công an" và truy cập để cung cấp thông tin cá nhân, thông tin tài khoản ngân hàng với vỏ bọc xác minh, điều tra. Sau đó, đối tượng chiếm quyền sử dụng tài khoản của bị hại và chuyển khoản và chiếm đoạt tiền của bị hại.

12.3. Giả danh người thân nhờ chuyển tiền rồi chiếm đoạt

Đối tượng lập tài khoản mạng xã hội như Facebook, Zalo... hoặc chiếm quyền quản trị tài khoản mạng xã hội (hack) của người khác rồi nhắn tin cho người thân, bạn bè trong danh sách liên lạc của chủ tài khoản giả vay, mượn tiền, hoặc nhờ chuyển tiền số lượng lớn vào tài khoản ngân hàng của đối tượng, hoặc gửi thông báo lệnh chuyển tiền giả, kèm đường link trang web giả mạo ngân hàng, yêu cầu bị hại truy cập, kiểm tra. Kết hợp với mã OTP của ngân hàng lừa lấy được từ bị hại, sau đó kiểm soát tài khoản Internet banking, chiếm đoạt toàn bộ số tiền có trong tài khoản ngân hàng của bị hại.

12.4. Nhắn tin trúng thưởng

Đối tượng sử dụng Messenger gửi tin nhắn cho người bị hại thông báo trúng thưởng tài sản giá trị lớn (Honda SH, điện thoại, đồng hồ) hoặc tiền (phiếu quà tặng, phiếu mua hàng…). Sau đó, yêu cầu người bị hại nạp tiền qua thẻ điện thoại / chuyển tiền qua tài khoản ngân hàng để làm thủ tục nhận thưởng. Việc chuyển khoản/nạp thẻ phải được thực hiện trong vòng 60 đến 90 phút, nếu không giải thưởng sẽ chuyển cho người khác.

Bên cạnh đó, trên trang web để hoàn tất thủ tục hồ sơ nhận thưởng thông tin về đơn vị tổ chức được dựng lên chi tiết, bao gồm cả tên tuổi địa chỉ những người đã trúng trước đó, căn cước công dân của nhân viên hỗ trợ nhận thưởng khiến người bị hại mất cảnh giác và chuyển tiền theo yêu cầu của đối tượng.

12.5. Kinh doanh đa cấp qua các sàn giao dịch tiền ảo, sàn ngoại hối, hoặc đầu tư đào tiền kỹ thuật số

Các đối tượng lập website đầu tư tài chính, các ứng dụng, rồi lôi kéo nhiều người tham gia như: Gọi điện thoại tư vấn, gửi tin nhắn, đăng tin quảng bá, mời chào qua Zalo, Facebook..., tổ chức các buổi hội thảo, đưa người tự xưng là chuyên gia tài chính đến chia sẻ kinh nghiệm.

Các sàn đều được quảng cáo có nguồn gốc từ nước ngoài, liên kết với nền tảng giao dịch điện tử hàng đầu thế giới, cam kết người chơi sẽ được hưởng mức lãi suất cao, an toàn, có thể rút vốn bất kỳ lúc nào, không cần đầu tư trí tuệ, thời gian. Sau một thời gian, sàn giao dịch thông báo dừng hoạt động để bảo trì hoặc lỗi không truy cập được, khách hàng không đăng nhập được để rút tiền, mất hết tiền.

12.6. Đầu tư kinh doanh, chơi hoa lan đột biến gen

Các đối tượng lợi dụng việc đầu tư kinh doanh, chơi hoa lan đột biến gen đang trở thành trào lưu được nhiều tầng lớp, thành phần trong xã hội tham gia và tâm lý hám lợi của một bộ phận người dân. Các đối tượng thường cấu kết thành nhóm, thuê nhà, đựng giàn, làm vườn trồng lan rồi thông qua các trang MXH như Facebook, Zalo, Youtube, Tiktok để lập ra các hội, nhóm như: Hội chơi lan quý, lan đột biến... Công khai, quảng bá, giới thiệu, quay clip trực tuyến các sản phẩm hoa lan đột biến gen và tổ chức trao đổi, mua bán trực tiếp hoặc đấu giá trực tuyến. Đối với giao dịch trực tiếp, các đối tượng hẹn người mua đến địa chỉ nhà thuê để giao dịch, sau khi giao dịch thành công, nhận được tiền, các đối tượng khóa tài khoản, chặn liên lạc và bỏ đi khỏi địa điểm nhà thuê.

12.7. Giả mạo hòm thư điện tử

Đối tượng lập các hộp thư điện tử tương tự hộp thư điện tử của các tổ chức, cá nhân kinh doanh, sản xuất có thực hiện các giao dịch bằng thư điện tử, mạo danh đối tác để đề nghị các tổ chức, cá nhân chuyển tiền thanh toán hợp đồng vào tài khoản ngân hàng của đối tượng và chiếm đoạt.

12.8. Chuyển khoản nhầm tiền để lừa đảo ép vay nặng lãi

Các đối tượng lừa đảo sẽ cố ý chuyển nhầm một khoản tiền đến tài khoản của người bị hại. Sau đó đối tượng lừa đảo sẽ giả danh là người thu hồi nợ của một công ty tài chính liên hệ yêu cầu người dùng trả lại số tiền như một khoản vay cùng với khoản lãi cắt cổ. Vì vậy, các bạn cần chú ý, khi bỗng dưng nhận được một khoản tiền "chuyển nhầm" vào tài khoản, thì không nên sử dụng số tiền đó. Nếu là tiền chuyển nhầm thật thì sẽ có đại diện ngân hàng liên hệ làm việc, nếu phát hiện là chuyển tiền nhầm là thủ đoạn lừa đảo thì báo ngay cho công an.

12.9. Lừa đảo chiếm đoạt tài sản thông qua hoạt động thương mại điện tử

Các đối tượng mở các trang cá nhân bán hàng online, order hàng, sau đó quảng cáo, rao bán các mặt hàng, yêu cầu bị hại chuyển khoản đặt cọc. Sau khi nhận cọc hay được chuyển khoản trước để đặt mua hàng, đối tượng không giao hàng hoặc giao hàng giả, hàng kém chất lượng, chúng thường khóa trang mạng của mình hoặc xóa hẳn để xóa dấu vết, bỏ số điện thoại và chiếm đoạt tài sản của bị hại.

12.10. Giả danh cán bộ ngân hàng, nhân viên công ty điện lực

Đối tượng giả danh cán bộ ngân hàng yêu cầu cung cấp mật khẩu, mã PIN hoặc thông tin thẻ để xử lý sự cố liên quan đến các giao dịch ngân hàng của người bị hại để chiếm đoạt tài sản.

Tại TP.HCM công an còn ghi nhận trường hợp đối tượnggiả danh là nhân viên Điện lực Việt Nam thông báo đến khách hàng sẽ tạm thời cắt điện vì lý do phát hiện sử dụng điện bất thường hoặc khách hàng còn nợ tiền điện để yêu cầu người bị hại cung cấp thông tin cá nhân, số tài khoản nhằm chiếm đoạt tài sản.

13. Kết luận

Là sinh viên của HUFI, chúng ta cần phải làm gì?

Thứ nhất, phải tích cực tìm hiểu kiến thức pháp luật về an toàn thông tin, an ninh mạng, các qui tắc ứng xử đúng đắn trên mạng xã hội. Chỉ sử dụng mạng xã hội cho mục đích học tập, nghiên cứu khoa học sinh viên, kết nối trao đổi thông tin với thầy cô, gia đình, người thân và bạn bè. Tỉnh táo nhận diện mục tiêu của các nhóm chat trên mạng xã hội, tránh bị rủ rê, lôi kéo vào các nhóm chat sử dụng mạng xã hội vào các mục đích tiêu cực, trái đạo đức xã hội, vi phạm pháp luật. Tự đề ra cho bản thân các nguyên tắc sử dụng mạng xã hội, nhằm phát huy mặt tích cực và hạn chế tối đa mặt tiêu cực của mạng xã hội đối với bản thân, gia đình và xã hội.

Thứ hai, nâng cao cảnh giác với các thủ đoạn lừa đảo qua mạng, luôn có ý thức bảo mật thông tin cá nhân. Cùng với sự phát triển của công nghệ viễn thông, những đối tượng xấu luôn nghĩ ra các cách thức, thủ đoạn phạm tội mới để thực hiện hành vi lừa đảo. Vì vậy, chúng ta phải hết sức cảnh giác khi giao lưu, kết bạn trên môi trường mạng, không cả tin bất kỳ thông tin gì, cá nhân nào khi thông tin đó chưa được kiểm chứng, xác thực, cá nhân đó ta chưa biết rõ là ai.

Đại tá Trương Sơn Lâm, Phó Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an, cũng là chuyên gia về an ninh mạng khuyên rằng, hiện nay số lượng người sử dụng các mạng xã hội như: Facebook, Zalo, Instagram... ở nước ta rất lớn. Đây là điều kiện thuận lợi để các đối tượng xấu lợi dụng thực hiện hành vi lừa đảo, chiếm đoạt tài sản. Để tránh trở thành nạn nhân của các hành vi lừa đảo trực tuyến, cá nhân sử dụng mạng xã hội cần luôn tỉnh táo, cảnh giác. Khi có người nhắn tin hỏi vay tiền, nhờ nạp tiền điện thoại... thì phải gọi điện trực tiếp kiểm tra, xác minh. Không tin vào những chiêu trò nhận thưởng qua mạng với yêu cầu nạp tiền qua thẻ điện thoại hoặc chuyển tiền qua tài khoản ngân hàng để làm thủ tục nhận thưởng. Tuyệt đối không truy cập các đường link, liên kết trong tin nhắn, Email lạ hoặc không rõ nguồn gốc. Giữ bí mật thông tin cá nhân, không cung cấp thông tin cá nhân, số điện thoại, địa chỉ nhà ở, thông tin về tài khoản ngân hàng, tài khoản các dịch vụ trên Internet... cho bất kỳ người lạ nào gọi đến. Trong mọi trường hợp, không cho mượn, cho thuê các giấy tờ cá nhân như: Căn cước công dân, giấy chứng minh nhân dân, sổ hộ khẩu hoặc thẻ ngân hàng, không bán, cho mượn, cho thuê tài khoản ngân hàng, không nhận chuyển khoản ngân hàng hay nhận tiền chuyển khoản của ngân hàng cho người không quen biết... Trường hợp có nghi ngờ về hoạt động lừa đảo chiếm đoạt tài sản cần bình tĩnh, kịp thời thông báo cho cơ quan công an nơi gần nhất để được hướng dẫn giải quyết và giúp đỡ.

TÀI LIỆU THAM KHẢO

[1] Luật An ninh mạng được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam khóa XIV, kỳ họp thứ 5 thông qua ngày 12/6/2018, có hiệu lực thi hành kể từ ngày 01/01/2019.

[2] Bộ luật Hình sự số 100/2015/QH13 được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam khóa XIII, kỳ họp thứ 10 thông qua ngày 27/11/2015, sửa đổi, bổ sung ngày 20/6/2017, có hiệu lực thi hành kể từ ngày 01/01/2018.

[3] Nghị định số 15/2020/NĐ-CP ngày 03/02/2020 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử.

[4] Quyết định số 874/QĐ-BTTT ngày 17/6/2021 của Bộ Thông tin và Truyền thông ban hành Bộ Quy tắc ứng xử trên mạng xã hội.

[5] Dự thảo Bộ qui tắc ứng xử trên mạng xã hội của HUFI năm 2021.

[6] Chỉ thị số 21/CT-TTg ngày 25/5/2020 của Thủ tướng Chính phủ về tăng cường phòng ngừa, xử lý hoạt động lừa đảo chiếm đoạt tài sản.

[7] Cổng thông tin điện tử của Bộ Công an (https://congan.com.vn).