**Những điểm cần lưu ý trong Luật An ninh mạng**

            **Luật An ninh mạng số 24/2018/QH14 được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam khóa XIV, kỳ họp thứ 5 thông qua ngày 12 tháng 6 năm 2018 và chính thức có hiệu lực thi hành từ ngày 01 tháng 01 năm 2019.** **Luật gồm 7 chương, 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; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan, gồm:**

            - Chương I: Những quy định chung, từ Điều 1 đến Điều 9

           - Chương II: Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, từ Điều 10 đến Điều 15

            - Chương III: Phòng ngừa, xử lý hành vi xâm phạm an ninh mạng, từ Điều 16 đến Điều 22

            - Chương IV: Hoạt động bảo vệ an ninh mạng, từ Điều 23 đến Điều 29

            - Chương V: Bảo đảm hoạt động bảo vệ an ninh mạng, từ Điều 30 đến Điều 35

            - Chương VI: Trách nhiệm của cơ quan, tổ chức, cá nhân, từ Điều 36 đến Điều 42

            - Chương VII: Điều khoản thi hành, tại Điều 43

****

**Các biện pháp bảo vệ an ninh mạng**

            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 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. (Quy định tại Khoản 1, 2 Điều 2 của Luật)

            Biện pháp bảo vệ an ninh mạng (quy định tại Điều 5) bao gồm: 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; 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 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; 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;
Các hành vi gây hậu quả nghiêm trọng có thể bị khởi tố, điều tra, truy tố, xét xử theo quy định của Bộ luật Tố tụng hình sự...

            Lực lượng bảo vệ an ninh mạng gồm: Lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Bộ Công an, Bộ Quốc phòng; Lực lượng bảo vệ an ninh mạng được bố trí tại Bộ, ngành, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia; Tổ chức, cá nhân được huy động tham gia bảo vệ an ninh mạng.

**6 nhóm hành vi bị cấm (**Theo quy định của Điều 8, có 6 nhóm hành vi bị nghiêm cấm) gồm:

(1) Sử dụng không gian mạng để thực hiện hành vi sau đây:

            a. Tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân; 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; Xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc.

            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.

            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 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.

            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 tổ chức, cá nhân;

            Cố ý xóa, làm hư hỏng, thất lạc, thay đổi 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 được truyền đưa, lưu trữ trên không gian mạng;

            Cố ý thay đổi, hủy bỏ hoặc làm vô hiệu hóa các biện pháp kỹ thuật được xây dựng, áp dụng để bảo vệ 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;

            Đưa lên không gian mạng những thông tin thuộc bí mật cá nhân, bí mật gia đình, đời sống riêng tư trái quy định của pháp luật;

            Cố ý nghe, ghi âm trái phép các cuộc đàm thoại;

            Hành vi khác cố ý xâm phạm 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

            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;

            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 các phương tiện thanh toán trái phép;
            Tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật;

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

            Hành vi khác sử dụng không gian mạng vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội.

            b. 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;

            c. 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;

            d. 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;

            đ. 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;
            e) Xúi giục, lôi kéo, kích động người khác phạm tội.

(2)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.

(3) 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.

(4)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.

(5)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.

(6) Hành vi khác vi phạm quy định của Luật này.

**Một số rủi ro và các biện pháp đảm bảo an toàn khi sử dụng mạng xã hội**

Không ai có thể phủ nhận những giá trị mà mạng xã hội mang lại trong việc kết nối cộng đồng, chia sẻ thông tin. Tuy nhiên đi cùng với đó là những nguy cơ tiềm ẩn, đòi hỏi mỗi người tham gia mạng xã hội phải trang bị cho mình những kiến thức cơ bản nhất để đảm bảo an toàn khi sử dụng mạng xã hội.

**Phát triển bùng nổ kéo theo nhiều nguy cơ tiềm ẩn**

Tại Việt Nam, theo thống kê của Facebook vào tháng 8/2021 có khoảng hơn 90 triệu người dùng có tài khoản mạng xã hội Facebook và con số này không ngừng tăng lên kể từ năm 2012 đến nay. Đồng thời cũng dễ dàng nhận thấy số người sử dụng Internet nói chung và số người sử dụng Facebook liên tục tăng trưởng về số người dùng trên toàn cầu và tại Việt Nam cũng vậy.

**Số tài khoản người dùng Facebook tại Việt Nam sẽ tiếp tục tăng lên.**

Cần nhấn mạnh rằng đã có hơn 90 triệu tài khoản người dùng Facebook tại Việt Nam và dự đoán sẽ tiếp tục tăng lên khoảng 75-80 triệu tài khoản Facebook tại Việt Nam đến hết năm 2021 và những năm sau đó. Theo một thống kê khác mới công bố gần đây của hãng We Are Social thì Việt Nam hiện tại đã  có 90 triệu người dùng Facebook, đứng thứ 7 trên toàn thế giới về số lượng người sử dụng Facebook.

***Ngoài ra, số lượng người dùng Zalo, Youtube cũng đang không ngừng tăng lên.***

Với số lượng người dùng lớn như vậy, mạng xã hội đang tác động lên mọi mặt đời sống, trở thành kênh truyền thông hiệu quả. Tuy nhiên, kéo theo đó là nhiều nguy cơ với người sử dụng.

Đầu tiên là việc đảm bảo an toàn với các thông tin cá nhân. Mạng xã hội thông thường được các nhà cung cấp dịch vụ đảm bảo về bảo mật thông tin, tuy nhiên, thực tế cho thấy các nhà cung cấp cũng bị tấn công mạng đánh cắp thông tin, hoặc người dùng bất cẩn gây ra những nguy cơ lộ lọt thông tin, gây ảnh hưởng tới hình ảnh, uy tín bản thân.

Nhiều tin tặc cũng lợi dụng mạng xã hội để khai thác thông tin cá nhân: email, điện thoại, tên người nhà… hay nguy hiểm hơn là chiếm đoạt tài khoản rồi sử dụng nó vào các mục đích xấu.

Một vấn đề khác đối với các mạng xã hội xuyên biên giới như Facebook, Google, Youtube là hầu hết các nền tảng mạng xã hội đều thu thập dữ liệu người dùng. Facebook là ví dụ điển hình cho việc biến dữ liệu người dùng thành thứ "hái ra tiền". Ngay từ bước đăng ký, Facebook đã yêu cầu người dùng cung cấp email, số điện thoại, tên, tuổi, địa chỉ...

Trong quá trình hoạt động, nền tảng này còn thu thập vị trí, ghi nhớ các hành động, thói quen và nội dung tìm kiếm của người dùng. Những thông tin này sau đó được dùng để phân tích nhằm phục vụ cho quảng cáo hướng đối tượng.

Google cũng có cách làm tương tự Facebook nhưng ở quy mô còn khủng khiếp hơn. Với hàng loạt các công cụ như Google Search, YouTube, Google Maps, Gmail,... gã khổng lồ tìm kiếm, nắm trong tay lượng dữ liệu khổng lồ từ hàng tỷ thiết bị.

Trước những thực tế đó, nhiều chính phủ trên thế giới đã có các biện pháp mạnh tay với các mạng xã hội này. Điển hình là Trung Quốc, Triều Tiên gần như ngăn cấm hoàn toàn sự hiện diện của các nền tảng nước ngoài.

**Một số biện pháp để đảm bảo ATTT khi sử dụng mạng xã hội**

Cấm hoàn toàn một mạng xã hội được xem là giải pháp hơi cực đoan. Đó là lý do phần lớn các quốc gia trên thế giới không chọn cách này. Bởi vậy, các chính phủ có những chính sách để buộc các mạng xã hội phải tuân thủ. Quan trọng hơn nữa là nâng cao ý thức của người sử dụng khi tham gia các mạng xã hội. Trong đó, một số kỹ năng sau đặc biệt quan trọng khi sử dụng mạng xã hội nói chung và mạng Facebook nói riêng:

- Hạn chế đưa thông tin cá nhân quan trọng lên mạng xã hội: Điển hình là thông tin ngày tháng năm sinh của trẻ nhỏ. Nếu đưa lên, nên để ở chế độ riêng tư, để người lạ không xem được. Cũng nên hạn chế đăng (hoặc tag) ảnh chính diện của trẻ nhỏ, người thân trong gia đình.

- Xác minh bạn bè: Chỉ nên kết bạn với những người thân, quen biết ở ngoài đời. Xác minh với bạn bè, người thân trước khi kết bạn trên mạng xã hội. Nên thiết lập chế độ để giới hạn những ai/ứng dụng nào được phép xem thông tin của bạn.

- Thiết lập an toàn cho tài khoản Facebook: Đầu tiên là mọi người dùng đều nên cài đặt chế độ cảnh báo đăng nhập. Với tính năng này, bạn sẽ nhận được một thông báo mỗi khi một ai đó (hoặc bạn vào các thời điểm) đăng nhập vào tài khoản Facebook từ một máy tính hoặc thiết bị không rõ. Thông báo này sẽ hiển thị rõ thông tin về thời gian, địa điểm và thiết bị mà tài khoản Facebook của bạn vừa đăng nhập. Qua đó giúp bạn kiểm tra được ngay nếu có ai đó chiếm tài khoản của bạn.

- Thiết lập quyền riêng tư: Trong phần Quyền riêng tư, giới hạn người xem cho các bài viết trong tương lai tại phần "Ai có thể thấy các bài đăng sau này của bạn?". Kiểm tra các hoạt động của tài khoản Facebook tại mục "Sử dụng nhật ký hoạt động". Ẩn các bài viết cá nhân tại dòng thời gian hoặc thiết lập chế độ chỉ cho phép bạn bè đọc.

- Kiểm tra lại phần hiển thị của các thông tin cá nhân: Click vào Dòng thời gian và gắn thẻ, chọn "Xem với tư cách là" để thấy được những thông tin cá nhân của mình hiển thị với Bạn bè, người lạ trên Facebook như thế nào. Truy cập Bảo mật rồi chọn "Địa điểm bạn đã đăng nhập" để xem xét các truy cập đối với tài khoản Facebook của mình. Khi xuất hiện các truy cập bất thường, click vào "kết thúc hoạt động" để ngăn chặn.

- Cuối cùng, nên sử dụng mật khẩu mạnh khi tham gia mạng xã hội: Tuyệt đối không đặt mật khẩu đơn giản, dễ đoán hay dùng chung mật khẩu cho nhiều tài khoản mạng xã hội. Thực hiện đổi mật khẩu định kỳ cũng là biện pháp để đảm bảo an toàn. Mật khẩu mạnh có chứa kí tự hoa, thường, đặc biệt, các số và các dấu chấm câu và sử dụng một mật khẩu cho mỗi trang web.

**Hết**