KPMG 30+ YEARS IN VIETNAM & CAMBODIA

Bản tin cập nhật về Pháp luật

Tháng 03 năm 2024

ẢNH HƯỞNG CỦA CÁC CUỘC TẤN CÔNG MẠNG ĐẾN VIỆC BẢO VỆ DỮ LIỆU CÁ NHÂN TẠI VIỆT NAM

Trong năm 2023, Việt Nam có khoảng 13.900 cuộc tấn công mạng nhắm vào các hệ thống trên cả nước đã được báo cáo, và hơn 83.000 máy tính và máy chủ đã trở thành nạn nhân của các cuộc tấn công liên quan đến mã độc ransomware – loại mã độc chuyên mã hoá dữ liệu để tống tiền[1]. Phần lớn các cuộc tấn công mạng này nhắm vào các doanh nghiệp cung cấp dịch vụ trực tuyến hoặc hoạt động kinh doanh trên môi trường số trong các lĩnh vực tài chính, thương mại điện tử, viễn thông và công nghệ, ví dụ như các công ty chứng khoán, ngân hàng và các công ty công nghệ thông tin.

Các cuộc tấn công mạng gây ra những rủi ro đáng kể cho cá nhân và tổ chức. Người dùng có thể bị các đối tượng xấu xâm phạm, truy cập trái phép vào các tài khoản ngân hàng, tài khoản chứng khoán, hoặc bị sử dụng dữ liệu cá nhân của mình cho các mục đích bất hợp pháp. Mặt khác, các doanh nghiệp sẽ đối diện với việc gián đoạn hoạt động kinh doanh, thiệt hại về uy tín và có thể phải chịu các trách nhiệm pháp lý nếu như doanh nghiệp bỏ qua việc thực thi các biện pháp an ninh mạng đầy đủ để ngăn chặn các cuộc tấn công như vậy. Thêm vào đó, các doanh nghiệp bị tấn công có khả năng phải trải qua sự kiểm tra của cơ quan có thẩm quyền chuyên trách để đánh giá việc tuân thủ các quy định pháp luật về bảo vệ dữ liệu cá nhân.

Để giảm thiểu những rủi ro pháp lý có thể phát sinh từ việc không tuân thủ pháp luật, các doanh nghiệp cần dần làm quen và tuân thủ nghiêm ngặt các quy định hiện hành liên quan.

1. Pháp luật về Bảo vệ dữ liệu cá nhân tại Việt Nam đối với các cuộc tấn công mạng

a. *Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân*

Từ góc độ bảo vệ dữ liệu cá nhân, Nghị định số 13/2023/ND-CP về bảo vệ dữ liệu cá nhân ("Nghị định 13") không quy định rõ các biện pháp cụ thể để bảo vệ dữ liệu cá nhân. Điều 26 của nghị định chỉ nêu ra hai loại biện pháp bảo vệ chính mà các bên liên quan đến hoạt động xử lý dữ liệu cá nhân phải thực hiện, bao gồm: (i) Biện pháp quản lý và (ii) Biện pháp kỹ thuật. Bên cạnh đó, Điều 23 yêu cầu các tổ chức kiểm soát dữ liệu cá nhân phải thông báo chậm nhất 72 giờ kể từ khi xảy ra bất kỳ hành vi vi phạm quy định bảo vệ dữ liệu cá nhân nào, như rò rỉ dữ liệu hoặc các cuộc tấn công mạng.

Để đảm bảo sự tuân thủ và thúc đẩy trách nhiệm của các tổ chức trong việc bảo vệ dữ liệu cá nhân, nghị định xử phạt hành chính điều chỉnh cụ thể các hành vi vi phạm đang được xây dựng và sẽ ban hành trong thời gian tới. Mục tiêu của nghị định sẽ thiết lập một cơ sở chế tài cụ thể đối với những tổ chức không tuân thủ và thực hiện các quy định về bảo vệ dữ liệu cá nhân. Tuy nhiên, trong thời điểm các quy định về bảo vệ dữ liệu cá nhân vẫn còn chưa rõ ràng và đầy đủ, các doanh nghiệp cần tìm hiểu kỹ lưỡng và dẫn chiếu đến các quy định pháp luật về an toàn thông tin mạng và pháp luật chuyên ngành để đảm bảo sự tuân thủ và hạn chế tối đa các rủi ro pháp lý.

b. *Pháp luật về An toàn thông tin mạng*

Năm 2015, Việt Nam đã xây dựng khung pháp lý toàn diện đối với việc bảo đảm an toàn thông tin mạng và phòng tránh các mối đe dọa tấn công mạng. Luật An toàn thông tin mạng cung cấp các nguyên tắc căn bản để bảo vệ hệ thống thông tin trong nước, bao gồm cả mạng và máy chủ. Đối với các hệ thống thông tin cung cấp dịch vụ trực tuyến hoặc phục vụ cho hoạt động của cơ quan, tổ chức nhà nước, Nghị định số 85/2016/NĐ-CP ("Nghị định 85") và Thông tư số 12/2022/NHNN ("Thông tư 12") đã được ban hành để điều chỉnh chi tiết về các tiêu chuẩn và các biện pháp bảo mật.

Các văn bản pháp luật này quy định một loạt các khía cạnh bảo đảm an toàn từ quản lý đến kỹ thuật, tập trung vào việc xây dựng và duy trì các chính sách bảo mật thông tin, thành lập các đơn vị chuyên trách về bảo mật và tầm quan trọng của việc đảm bảo an toàn thông tin cho nguồn nhân lực.

[1] Theo Báo cáo tổng kết An ninh mạng Việt Nam năm 2023 của Công ty Công nghệ An ninh mạng Quốc gia Việt Nam (NCS) [https://ncsgroup.vn/tong-ket-an-ninh-mang-viet-nam-nam-2023-va-du-bao-2024/]

Về mặt kỹ thuật, các quy định hướng dẫn yêu cầu việc thiết lập các mạng an toàn, triển khai các phương pháp quản lý từ xa và thực hiện kiểm soát việc truy cập một cách toàn diện, nhằm ngăn chặn sự xâm nhập và bảo vệ khỏi các phần mềm độc hại. Các quy định hướng dẫn cũng đề xuất việc sử dụng các giao thức bảo mật nghiêm ngặt hơn để đáp ứng nhu cầu bảo mật cấp cao, bao gồm việc tối ưu hóa hạ tầng mạng, bảo vệ dữ liệu và phát triển kế hoạch khôi phục khẩn cấp, nhằm bảo đảm tính liên tục và toàn vẹn của dữ liệu.

Các đối tượng không tuân thủ hoặc tuân thủ không đầy đủ các tiêu chuẩn như trên có thể bị xử phạt vi phạm hành chính từ 10.000.000 đồng đến 30.000.000 triệu đồng, và mức phạt có thể tăng lên từ 30 triệu đồng đến 70 triệu đồng nếu không thực hiện các biện pháp ứng phó kịp thời đối với các sự cố bảo mật.

Trong bối cảnh Việt Nam đang ngày càng tập trung vào việc bảo vệ dữ liệu cá nhân, dự kiến các chế tài đối với hành vi vi phạm quy định bảo vệ dữ liệu do không tuân thủ các biện pháp bảo mật sẽ được tăng cường theo các quy định mới được ghi nhận trong Nghị định 13.

c. Pháp luật chuyên ngành

Ngoài các quy định tổng quát về bảo đảm an toàn thông tin mạng, Việt Nam đã thiết lập các quy định riêng biệt về đảm bảo an toàn thông tin mạng để đáp ứng được các nhu cầu đặc biệt của từng ngành.

Ví dụ, trong lĩnh vực chứng khoán, quy định tại Điều 20 của Thông tư 121/2020/TT-BTC yêu cầu các công ty chứng khoán cung cấp dịch vụ giao dịch trực tuyến phải đảm bảo rằng các giao dịch diễn ra một cách liên tục và hiệu quả, bảo đảm sự an toàn, toàn vẹn và bảo mật của hệ thống dữ liệu, duy trì các hệ thống dự phòng và ứng phó đột xuất, có sự tách biệt với các hệ thống thông tin điện tử khác, và thiết lập các quy trình vận hành, quản lý và sử dụng hệ thống giao dịch trực tuyến. Quy định này tập trung vào cam kết về an toàn thông tin mạng trong quá trình cung cấp dịch vụ chứng khoán trực tuyến, và đối với hành vi vi phạm các nghĩa vụ trên có thể bị áp đặt mức phạt tiền từ 100 triệu đồng đến 150 triệu đồng.

Trong lĩnh vực ngân hàng, Thông tư 09/2020/TT-NHNN đã xây dựng khung pháp lý quy định chi tiết về các biện pháp quản lý và biện pháp kỹ thuật nhằm bảo vệ tài sản công nghệ thông tin, bao gồm tài sản thông tin, tài sản vật lý và tài sản phần mềm. Các biện pháp quản lý yêu cầu việc lập danh mục toàn bộ tài sản công nghệ thông tin liên quan đến hệ thống thông tin, thực hiện việc làm mới danh mục hàng năm và áp dụng các biện pháp bảo vệ phù hợp theo từng cấp độ hệ thống thông tin. Các biện pháp kỹ thuật bao gồm biên pháp mã hóa dữ liệu, xây dựng quy trình, kịch bản phòng tránh thiệt hại, chính sách quản lý thiết bị di động và vật mang tin (ví dụ như vô hiệu hóa thiết bị hoặc xóa dữ liệu từ xa) và quản lý tài sản phần mềm, bao gồm việc cập nhật định kỳ các bản vá lỗi về an ninh bảo mật.

Để tránh xung đột lợi ích và bảo đảm sự giám sát có hiệu quả, Thông tư cũng nhấn mạnh tầm quan trọng của sự tham gia trực tiếp của người đại diện theo pháp luật trong việc bảo đảm an toàn thông tin, ứng phó với sự cố và phân chia rõ ràng vai trò của nhân viên chuyên trách.

2. Lưu ý cho các doanh nghiệp:

Trong bối cảnh Nghị định 13 vẫn chưa có những quy định cụ thể về những biện pháp mà các doanh nghiệp cần phải thực hiện để bảo vệ dữ liệu cá nhân và phòng tránh các các cuộc tấn công mạng thì các quy định tại Luật ATTTM, Nghị định 85, Thông tư 12 cùng với các chế tài xử phạt vi phạm hành chính trong lĩnh vực an toàn thông tin mạng tại Nghị định 15/2020/NĐ-CP vẫn tiếp tục đóng vai trò là cơ sở quan trọng để điều chỉnh các hành vi không tuân thủ các biện pháp bảo đảm an toàn thông tin của các doanh nghiệp vận hành hệ thống thông tin.

Vì vậy, để giảm thiểu rủi ro pháp lý cho doanh nghiệp trong trường hợp rò rỉ dữ liệu, việc tuân thủ các tiêu chuẩn kỹ thuật về an ninh mạng và đáp ứng đầy đủ nghĩa vụ theo Luật An toàn thông tin mạng và các quy định ngành liên quan là vô cùng quan trọng.

KPMG có thể hỗ trợ các doanh nghiệp như thế nào

KPMG hỗ trợ toàn diện các tổ chức để đáp ứng các yêu cầu pháp lý chung. Chúng tôi giúp doanh nghiệp hiểu và tuân thủ các nghĩa vụ theo quy định, chẳng hạn như luật bảo vệ dữ liệu, khung an ninh mạng và các quy định riêng của từng ngành. Đội ngũ của chúng tôi luôn cập nhật những yêu cầu pháp lý mới nhất, đảm bảo khách hàng nắm rõ thông tin và sẵn sàng đáp ứng các nghĩa vụ tuân thủ.

Dịch vụ của chúng tôi bao gồm: xây dựng chương trình tuân thủ, đánh giá rủi ro và đào tạo về thực tiễn tuân thủ hiệu quả. Bên cạnh đó, chúng tôi tư vấn về quy định bảo mật dữ liệu, chẳng hạn như Quy định Bảo vệ Dữ liệu Chung (GDPR) và Nghị định 13, hỗ trợ doanh nghiệp xây dựng và thực hiện các chính sách, quy trình phù hợp để bảo vệ dữ liệu khách hàng.

Cùng với các chuyên gia Tư vấn CNTT, chúng tôi cung cấp giải pháp trọn gói giúp doanh nghiệp vượt qua môi trường pháp lý luôn thay đổi.

Tìm hiểu thêm về:

- Dịch vụ pháp lý - Quy định Bảo vệ Dữ liệu Cá nhân

Liên hệ với chúng tôi

Hà Nội

Tầng 46, Tòa tháp Keangnam Landmark 72,
E6 Phạm Hùng, Mễ Trì, Nam Từ Liêm

T +84 (24) 3946 1600

Tp. Hồ Chí Minh

Tầng 10, Tòa nhà Sun Wah,
115 Nguyễn Huệ, Bến Nghé, Quận 1

T +84 (28) 3821 9266

Đà Nẵng

Lô D3, Tầng 5, Tòa nhà Indochina Riverside Towers,
74 Bạch Đằng, Hải Châu I, Hải Châu

T +84 (236) 351 9051

Quét mã QR để truy cập website: kpmg.com.vn

Email: info@kpmg.com.vn