Ngày 18 tháng 11 năm 2021

Ý KIẾN ĐÓNG GÓP CỦA BSA VỀ DỰ THẢO NGHỊ ĐỊNH QUY ĐỊNH VỀ XỬ PHẠT VI PHẠM HÀNH CHÍNH TRONG LĨNH VỰC AN NINH MẠNG

Gửi đến Bộ Công an qua phương thức điện tử

BSA | Liên Minh Phần Mềm (**BSA**)[1] trân trọng cảm ơn Bộ Công an (**Bộ CA**) vì đã cho chúng tôi cơ hội đóng góp ý kiến đối với những đề xuất thay đổi đối với Dự thảo Nghị định quy định về xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng (**Dự thảo Nghị định**).

BSA là tổ chức hàng đầu hỗ trợ ngành công nghiệp phần mềm toàn cầu trước chính phủ và trên thị trường quốc tế. Chúng tôi có rất nhiều kinh nghiệm tham gia cùng các chính phủ trên toàn thế giới để thúc đẩy xây dựng các hệ thống pháp lý hiệu quả, có khả năng vận hành liên kết quốc tế, giúp nâng cao tiêu chuẩn về an ninh mạng, bảo vệ thông tin cá nhân trong khi vẫn hỗ trợ hoạt động sử dụng các công nghệ dựa trên dữ liệu một cách có trách nhiệm.

Các thành viên của BSA đều là những công ty tiên phong về các cải tiến dựa trên dữ liệu, chuyên phát triển nhiều giải pháp tiên tiến trong lĩnh vực trí tuệ nhân tạo, học máy (machine learning), và phân tích dựa trên dữ liệu đám mây (cloud-based analytics). Các thành viên của chúng tôi nhận thức được rằng niềm tin của người dùng sẽ có được thông qua các hành động có trách nhiệm đối với dữ liệu cá nhân của họ và cung cấp các công nghệ bảo mật cần thiết giúp bảo vệ khỏi các mối đe dọa trên không gian mạng.

BSA và các thành viên của chúng tôi đặc biệt quan tâm đến Luật An ninh mạng của Việt Nam (**Luật ANM**) và các dự thảo nghị định có liên quan, và đã đóng góp ý kiến đối với Luật ANM và các dự thảo nghị định thông qua nhiều quá trình lấy ý kiến do Bộ CA tiến hành.[2] Chúng tôi xin ghi nhận nỗ lực liên tục của Chính phủ Việt Nam trong việc phát triển một khung pháp lý cho lĩnh vực an ninh mạng và an ninh thông tin. Chúng tôi cũng công nhận nhiệm vụ quan trọng của Bộ CA trong việc đảm bảo Việt Nam được chuẩn bị đầy đủ để có thể phòng ngừa và quản lý các hình thức vi phạm và mối đe dọa khác nhau trên không gian mạng.

Chúng tôi hiểu rằng Dự thảo Nghị định là văn bản dưới luật của Luật ANM và có mục đích tổng hợp nhiều hình thức xử phạt hành chính đối với các vi phạm theo Dự thảo Nghị định về An ninh mạng (**Nghị**

---

[1] BSA | Liên minh Phần mềm (www.bsa.org) là tổ chức hàng đầu hỗ trợ ngành công nghiệp phần mềm toàn cầu. Thành viên của tổ chức là những công ty sáng tạo nhất thế giới, chuyên xây dựng các giải pháp phần mềm giúp các doanh nghiệp ở mọi quy mô, trong mọi thành phần của nền kinh tế hiện đại hóa và tăng trưởng. Có trụ sở chính tại Washington, DC và hoạt động tại hơn 30 quốc gia, BSA là tổ chức tiên phong trong các chương trình về tuân thủ khuyến khích sử dụng phần mềm hợp pháp và ủng hộ các chính sách công nhằm đẩy mạnh đổi mới công nghệ và thúc đẩy tăng trưởng trong nền kinh tế kỹ thuật số. Theo dõi BSA tại @BSAnews.

Các thành viên của BSA bao gồm: Adobe, Altium, Atlassian, Autodesk, AVEVA, Amazon Web Services, Bentley Systems, Box, Cisco, Dassault Systems, DocuSign, IBM, Informatica, Intel, Mastercam, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell Automation, Salesforce, ServiceNow, Siemens PLM Software, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, Workday, và Zoom.

[2] https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-draft-vietnam-personal-data-protection-decree
https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-draft-decree-implementing-law-on-cybersecurity

định An ninh mạng) và Nghị định BVDLCN. Tuy nhiên, chúng tôi lo ngại rằng pham vi thực thi quá rộng các quy định của Luật ANM và các dự thảo nghị định liên quan, cụ thể là Nghị định An ninh mạng và Nghị định BVDLCN, sẽ không giúp đạt được mục đích này và có thể gây cản trở hoạt động sáng tạo và đầu tư vào Việt Nam. Chúng tôi xin đưa ra các ý kiến đóng góp sau với mong muốn sẽ giúp ích cho Bộ CA trong quá trình hoàn thiện Nghị định An ninh mạng và Nghị định BVDLCN và cân nhắc về tác động của các văn bản này đối với Dự thảo Nghị định quy định về xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng.

Đánh giá Chung

Trước hết, chúng tôi xin nhấn mạnh rằng cả Nghị định An ninh mạng và BVDLCN đều chưa được hoàn thiện, mặc dù Dự thảo Nghị định là văn bản tổng hợp nhiều hình thức xử phạt hành chính đối với các vi phạm quy định trong hai nghị định nêu trên. Chúng tôi ghi nhận sự minh bạch và việc Bộ CA đón nhận ý kiến của nhiều bên liên quan thông qua quá trình lấy ý kiến góp ý này. Tuy nhiên, doanh nghiệp khó có thể đóng góp các ý kiến đầy đủ cho Dự thảo Nghị định khi chưa có hiểu biết rõ ràng về các nghĩa vụ trong hai Nghị định kia. Về vấn đề này, chúng tôi khuyến nghị Bộ CA đẩy nhanh quá trình làm việc với doanh nghiệp về dự thảo các Nghị định ANM và BVDLCN và cung cấp cho chúng tôi toàn văn dự thảo hai Nghị định này để chúng tôi xem xét đóng góp thêm ý kiến.

BSA nhận thấy đối tượng có thể bị xử phạt (của Dự thảo Nghị định) rất rộng, bao gồm "*doanh nghiệp nước ngoài hoặc chi nhánh, văn phòng đại diện, địa điểm kinh doanh của doanh nghiệp nước ngoài cung cấp dịch vụ viễn thông, Internet, dịch vụ cung cấp nội dung trên không gian mạng, công nghệ thông tin, an ninh mạng, an toàn thông tin mạng*", bao gồm cả các nhà cung cấp dịch vụ trong nước và nước ngoài. Việc xử phạt chỉ có thể hiệu quả và có kết quả nếu có các nghĩa vụ của các chủ thể khác nhau được quy định rõ ràng và điều chỉnh sao cho phù hợp với vai trò và trách nhiệm của mỗi chủ thể. Chúng tôi sẽ mô tả chi tiết hơn các vai trò và trách nhiệm này trong phần tiếp theo.

Dự thảo Nghị định quy định nhiều mức phạt tiền từ 10 đến 100 triệu VNĐ (tương đương với 440 đến 4,400 đô la Mỹ). Dự thảo Nghị định cũng quy định rằng, tùy thuộc vào mức độ, hậu quả và tính chất của hành vi vi phạm, mức phạt có thể lên đến 5% doanh thu hàng năm của tổ chức vi phạm tại Việt Nam. Mức phạt nên tương xứng với những tổn hại đã bị gây ra cho cá nhân; và cần phải xem xét đầy đủ cả các yếu tố tăng nặng và giảm nhẹ khi quyết định mức phạt. Dự thảo Nghị định hiện nay mới chỉ xem xét các yếu tố tăng nặng (như số lượng cá nhân bị ảnh hưởng và liệu hành vi vi phạm đó có phải tái phạm hay không) khi quyết định có cần tăng thêm mức phạt hay không. Tuy nhiên, các biện pháp do các tổ chức thực hiện để khắc phục tình hình cũng nên được xem xét. Những yếu tố giảm nhẹ đó bao gồm: (a) tổ chức đó đã cố gắng giải quyết vấn đề với (những) cá nhân bị ảnh hưởng kịp thời và tích cực đến mức độ nào; (b) tổ chức đó đã thực hiện các bước hợp lý để phòng ngừa và giảm thiểu thiệt hại gây ra do hành vi vi phạm hay chưa; và (c) tổ chức đó đã bồi thường cho (những) cá nhân bị ảnh hưởng hay chưa. **Vì vậy, BSA khuyến nghị Bộ CA xem xét lại cấu trúc xử phạt để có thể xem xét cả những yếu tố giảm nhẹ nêu trên khi quyết định mức độ và giá trị xử phạt.**

Ý kiến và Khuyến nghị Cụ thể

Trong phần này, chúng tôi đưa ra các ý kiến và khuyến nghị đối với các quy định tại Mục 2, "Vi phạm Quy định về Bảo vệ Dữ liệu Cá nhân" (Điều 14 – 30), Mục 3 "Vi phạm Quy định về Phòng, Chống Tấn công Mạng" (Điều 31 – 33), và Mục 4, "Vi phạm Quy định về Triển khai Hoạt động Bảo vệ An ninh Mạng" (Điều 34 – 39).

Hình thức Xử phạt "Bên Xử lý Dữ liệu Cá nhân và Bên thứ ba"

Mục 2 của Dự thảo Nghị định dẫn chiếu tới "*Bên Kiểm soát Dữ liệu Cá nhân*", "*Bên Kiểm soát và Xử lý Dữ liệu Cá nhân*", "*Bên Xử lý Dữ liệu Cá nhân*", và "*Bên thứ ba*". Điều này cho thấy dường như Nghị định BVDLCN hiện nay đã công nghận khái niệm bên kiểm soát dữ liệu, bên kiểm soát dữ liệu đồng thời là bên xử lý dữ liệu, bên xử lý dữ liệu, và bên thứ ba. Mặc dù chúng tôi không rõ các khái niệm này sẽ được định nghĩa như thế nào trong Nghị định BVDLCN, BSA vẫn khuyến khích Bộ CA **xây dựng các khái niệm "bên kiểm soát dữ liệu cá nhân" và "bên xử lý dữ liệu cá nhân" tương thích với các luật khác và trách nhiệm của các chủ thể này phải phù hợp với vai trò của họ**. Chúng tôi cũng khuyến nghị rằng **vai trò và trách nhiệm của "Bên Xử lý Dữ liệu Cá nhân" tương ứng với "Bên thứ ba" nên được quy định rõ ràng trong Nghị định BVDLCN**.

BSA cũng nhận thấy rằng nhiều hình thức xử phạt theo Mục 2 là dành cho "*Bên Xử lý Dữ liệu Cá nhân*" và "*Bên Kiểm soát và Xử lý Dữ liệu Cá nhân*" đối với các nghĩa vụ trực tiếp với khách hàng. Các hình thức xử phạt này được quy định trong các Điều 15-1(đ), 15-1(e), 15-1(i), 17, và 22-23. Đây là một sửa đổi hợp lý, bởi các nghĩa vụ như có được sự đồng ý của chủ thể dữ liệu đối với việc xử lý dữ liệu và yêu cầu tôn trọng các yêu cầu thực hiện quyền của chủ thể dữ liệu đúng là nên được đặt lên các bên kiểm soát dữ liệu có mối quan hệ trực tiếp với chủ thể dữ liệu. Tuy nhiên, chúng tôi nhận thấy **các quy định tại các Điều 15-1(g), 15-1(h), 19-1(b) vẫn xử phạt "Bên Xử lý Dữ liệu Cá nhân" và "Bên thứ ba" cho các nghĩa vụ mà đúng ra phải thuộc về bên kiểm soát dữ liệu. Vì vậy, chúng tôi vẫn khuyến khích Bộ CA loại trừ "Bên Xử lý Dữ liệu Cá nhân" và "Bên thứ ba" khỏi các nghĩa vụ đó**.

Hình thức Xử phạt đối với Vi phạm Quy định về Chuyển Dữ liệu Xuyên Biên giới

Điều 26-1(a) quy định rằng một mức phạt sẽ được áp dụng nếu dữ liệu cá nhân của công dân Việt Nam được chuyển mà chưa đáp ứng đồng thời ba điều kiện tại khoản 2 Điều 16 Nghị định Bảo vệ Dữ liệu Cá nhân. Mặc dù Nghị định BVDLCN chưa được hoàn thiện và chúng tôi không rõ ba điều kiện đó là gì, chúng tôi nhận thấy Điều 26-1(b) và (c) có dẫn chiếu đến "đánh giá tác động" và thỏa thuận có hiệu lực pháp lý ràng buộc. Thêm vào đó, Dự thảo Nghị định cũng yêu cầu tổ chức chuyển dữ liệu phải thông báo cho Cơ quan bảo vệ dữ liệu cá nhân về việc chuyển dữ liệu, và lưu trữ hồ sơ đánh giá tác động và/hoặc các thỏa thuận có hiệu lực pháp lý ràng buộc để phục vụ hoạt động kiểm tra, đánh giá.

Nhìn chung, chúng tôi vô cùng lo ngại về quy định hạn chế việc chuyển dữ liệu cá nhân xuyên biên giới. Việc yêu cầu các tổ chức phải đáp ứng nhiều điều kiện như được mô tả ở trên trước khi được phép chuyển dữ liệu cá nhân sẽ gây ảnh hưởng xấu đến khả năng kinh doanh tại Việt Nam của các công ty toàn cầu và gây tổn hại đến khả năng cung cấp dịch vụ toàn cầu của các công ty Việt Nam. Các nghĩa vụ thông báo và lưu trữ làm tăng chi phí tuân thủ cho các doanh nghiệp mà không tạo ra giá trị nào cho chủ thể dữ liệu, và có thể không may tạo ra nhiều mối lo ngại mới về riêng tư và bảo mật khi họ bị bắt buộc phải lưu trữ và truy cập vào các dữ liệu mà thông thường họ không cần lưu trữ và truy cập vào. **Chúng tôi khuyến nghị Bộ CA sửa lại các quy định trong dự thảo Nghị định BVDLCN liên quan đến hoạt động chuyển dữ liệu cá nhân qua biên giới nhằm tạo thêm sự linh hoạt**.

Hình thức Xử phạt liên quan đến Phòng ngừa và Xử lý Tình huống Nguy hiểm về An ninh Mạng

Điều 33-1 yêu cầu các tổ chức phải phối hợp triển khai các giải pháp kỹ thuật, nghiệp vụ để phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng và ngăn chặn, gỡ bỏ thông tin có nội dung kích động trên không gian mạng có nguy cơ xảy ra bạo loạn, phá rối an ninh, khủng bố. Chúng tôi nhận thấy phiên bản tháng 7 năm 2018 của Nghị định An ninh mạng không bao gồm định nghĩa hay giải thích cụ thể cho khái niệm "tình huống nguy hiểm về an ninh mạng", và cũng không đưa ra cơ chế yêu cầu gỡ bỏ nội dung vi phạm. Vì vậy, chúng tôi khuyến nghị Bộ CA đưa ra quy định rõ ràng về thế nào là "tình huống nguy hiểm về an ninh mạng" và xây dựng cơ chế rõ ràng với các kênh liên lạc chính thức và hình thức của yêu cầu gỡ bỏ nội dung vi phạm trong Nghị định An ninh mạng.

Như chúng tôi đã nhấn mạnh ở trên, việc điều chỉnh các nghĩa vụ và trách nhiệm sao cho phù hợp với vai trò và trách nhiệm của mỗi chủ thể là vô cùng quan trọng. Vì các nhà cung cấp dịch vụ cho doanh nghiệp thường không thể truy cập vào dữ liệu của các khách hàng doanh nghiệp của họ do các nghĩa vụ trong hợp đồng, BSA cũng **khuyến nghị rằng các nhà cung cấp dịch vụ cho doanh nghiệp được loại trừ khỏi nghĩa vụ liên quan đến gỡ bỏ nội dung vi phạm pháp luật**. Yêu cầu gỡ bỏ nội dung vi phạm pháp luật và phối hợp với cơ quan chức năng liên quan đến các nội dung vi phạm pháp luật nên được đặt cho các chủ thể có trách nhiệm tạo ra và đăng tải các nội dung đó (tức là các khách hàng của dịch vụ dành cho doanh nghiệp), chứ không nên dành cho một bên trung gian lưu trữ hoặc truyền tải nội dung đó thay mặt cho khách hàng doanh nghiệp, như nhà cung cấp dịch vụ điện toán đám mây hay nhà cung cấp dịch vụ trung tâm dữ liệu. Khách hàng doanh nghiệp đó sẽ có địa vị pháp lý và kỹ thuật đầy đủ nhất để xử lý các yêu cầu có tính chất như vậy. Trong hầu hết các trường hợp, nhà cung cấp dịch vụ cho doanh nghiệp sẽ chuyển lại các yêu cầu đó cho khách hàng của mình. Vì vậy, chúng tôi khuyến nghị quy định các nghĩa vụ liên quan trong Nghị định An ninh mạng chỉ nên được áp dụng một cách phù hợp cho các doanh nghiệp tiếp xúc trực tiếp với người tiêu dùng và đang cung cấp các thông tin mà công chúng nói chung có thể tiếp cận được.

Hình thức Xử phạt liên quan đến Bảo vệ An ninh Mạng đối với Hệ thống Thông tin

Điều 34 và 35 đưa ra các hình thức xử phạt cho các hệ thống thông tin đối với các vi phạm liên quan đến bảo vệ an ninh mạng. Điều 34 được áp dụng cụ thể cho "các hệ thống thông tin quan trọng về an ninh quốc gia", trong khi Điều 35 áp dụng cho tất cả các loại hệ thống thông tin. BSA rất mừng vì Bộ CA đã có cách tiếp cận khác khi các hệ thống thông tin không "quan trọng về an ninh quốc gia" sẽ được loại trừ khỏi các yêu cầu như đánh giá, kiểm tra, và thẩm định an ninh mạng, bên cạnh các yêu cầu khác. Tuy nhiên, chúng tôi vẫn khuyến nghị Bộ CA:

a) Thu hẹp định nghĩa và phạm vi "*hệ thống thông tin quan trọng về an ninh quốc gia*"

b) Đưa ra quy định chi tiết hơn về thủ tục rà soát và kiểm tra

c) Bổ sung chi tiết về thủ tục thanh tra / thẩm định an ninh mạng (bao gồm việc giám sát và quyền khiếu nại thủ tục đó)

Hình thức Xử phạt liên quan đến Địa phương hóa Dữ liệu

Điều 37-2 quy định rằng một mức phạt sẽ được áp dụng nếu một tổ chức không lưu trữ dữ liệu hoặc thành lập chi nhánh hoặc văn phòng đại diện tại Việt Nam theo khoản 3 Điều 26 Luật ANM. Các văn bản ý kiến trước liên quan đến Nghị định An ninh mạng đã nhấn mạnh nhu cầu phải có quy định rõ ràng về giới hạn đối với yêu cầu địa phương hóa dữ liệu và có văn phòng tại địa phương.

Việc áp dụng quá rộng chính sách về địa phương hóa dữ liệu và văn phòng đại diện tại địa phương sẽ làm ảnh hưởng xấu đến khả năng cạnh tranh về kinh tế của Việt Nam do các doanh nghiệp hoạt động trong tất cả các lĩnh vực và ở mọi quy mô tại Việt Nam phụ thuộc vào và hưởng lợi từ dòng lưu chuyển liên tục dữ liệu vào trong và ra ngoài nước. Người tiêu dùng sẽ không tránh khỏi phải chịu chi phí cho việc địa phương hóa khi các doanh nghiệp tăng giá. Việc yêu cầu các doanh nghiệp địa phương phải sử dụng trung tâm dữ liệu địa phương sẽ làm tăng các chi phí mà các doanh nghiệp vừa và nhỏ sẽ không chi trả được. Cuối cùng, các yêu cầu địa phương hóa này sẽ làm ảnh hưởng xấu đến an ninh mạng khi bắt buộc các công ty phải sử dụng máy chủ tại địa phương ít bảo mật hơn và phải trả thêm chi phí (cho việc địa phương hóa), trong khi khoản tiền này có thể được chi vào việc cải thiện bảo mật hệ thống mạng.

Khi Việt Nam tiếp tục thực thi Luật ANM, các yêu cầu về địa phương hóa cần phải được giới hạn chỉ dành cho các dữ liệu an ninh quốc gia nhạy cảm, nếu thấy cần thiết. Điều này sẽ giúp xử lý và địa phương hóa những dữ liệu thực sự trọng yếu và giúp các công ty quốc tế quan tâm đến việc đầu tư và mở rộng hoạt động đầu tư vào Việt Nam hiểu rõ và chắc chắn hơn.

Thêm vào đó, phạm vi áp dụng của yêu cầu địa phương hóa dữ liệu cũng cần được thu hẹp để loại trừ các tổ chức không phân phối thông tin đến công chúng, bao gồm, nhưng không giới hạn ở, các nhà cung cấp phần mềm doanh nghiệp và dịch vụ điện toán đám mây. Chúng tôi lưu ý rằng Điều 26.1.c của dự thảo Nghị định An ninh mạng (phiên bản tháng 7 năm 2019) yêu cầu các doanh nghiệp "*biết rõ rằng dịch vụ mà doanh nghiệp liên quan cung cấp đang được sử dụng để thực hiện các hành vi vi phạm pháp luật Việt Nam...*" phải lưu trữ dữ liệu của mình tại Việt Nam.Tuy nhiên, các nhà cung cấp dịch vụ cho doanh nghiệp, họ thường không thấy hoặc không biết về nội dung mà các khách hàng doanh nghiệp của họ đăng tải trên các dịch vụ của họ, và các nội dung đó có phải các dữ liệu vi phạm quy định của pháp luật Việt Nam hay không. Vì vậy, **chúng tôi khuyến nghị không áp dụng các nghĩa vụ liên quan theo dự thảo Nghị định An ninh mạng về địa phương hóa dữ liệu cho các doanh nghiệp xử lý dữ liệu đại diện cho các khách hàng doanh nghiệp.**

Kết luận

Chúng tôi xin một lần nữa cảm ơn Bộ CA vì đã cho chúng tôi cơ hội được đóng góp ý kiến đối với Dự thảo Nghị định và sự quan tâm xem xét của Bộ CA đối với các ý kiến nêu trên của chúng tôi. Nếu Quý Bộ có bất cứ câu hỏi hay vấn đề nào cần làm rõ về bất cứ phần nào của văn bản ý kiến này, vui lòng liên hệ với người ký tên dưới đây tại eunicel@bsa.org. Chúng tôi xin chân thành cảm ơn sự xem xét của Quý Bộ.

Trân trọng,

Eunice Lim

Eunice Lim
Quản lý Cấp cao, Chính sách – Khu vực Châu Á, Thái Bình Dương
BSA | Liên Minh Phần Mềm