Ngày 13 tháng 12 năm 2018

Kính gửi: **Bộ Công An**
Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao

Xin chuyển tới: **Thiếu tướng Nguyễn Minh Chính**
Cục trưởng

GÓP Ý CỦA BSA ĐỐI VỚI DỰ THẢO NGHỊ ĐỊNH QUY ĐỊNH CHI TIẾT MỘT SỐ ĐIỀU CỦA LUẬT AN NINH MẠNG

A. Lời giới thiệu

BSA | Liên minh Phần mềm (**BSA**)[1] xin cảm ơn Bộ Công An (**BCA**) đã tạo cơ hội cho chúng tôi đóng góp ý kiến cho Dự thảo Nghị định quy định chi tiết một số điều của Luật An ninh mạng (viết tắt lần lượt là "**Dự thảo Nghị định**" và "**Luật ANM**"). Chúng tôi xin đưa ra một số góp ý như dưới đây với hy vọng sẽ giúp ích cho BCA và Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao trong quá trình hoàn thiện Dự thảo Nghị định và cân nhắc những sửa đổi, bổ sung Luật ANM trong tương lai.

Các thành viên của chúng có mối quan tâm đặc biệt đối với Luật ANM của Việt Nam và các dự thảo nghị định liên quan. Trước đây, BSA đã nhiều lần tham gia đóng góp ý kiến và trình các văn bản sau đây (xem đính kèm):

(i) Phụ lục A: Bản góp ý chung của các Hiệp hội về hướng dẫn thi hành Luật An ninh mạng của Việt Nam (ngày 3 tháng 9 năm 2018)
(ii) Phụ lục B: Bản góp ý chung của các doanh nghiệp trong ngành về bản dự thảo Luật An ninh mạng được sửa đổi ngày 24 tháng 5 (ngày 28 tháng 5 năm 2018);
(iii) Phụ lục C: Bản góp ý chung của các doanh nghiệp trong ngành về dự thảo Luật An ninh mạng (ngày 26 tháng 2 năm 2018); và
(iv) Phụ lục D: Bản góp ý chung của các doanh nghiệp trong ngành về dự thảo Luật An ninh mạng (ngày 8 tháng 8 năm 2017).

[1] BSA | Liên minh Phần mềm (www.bsa.org) là tổ chức hàng đầu hỗ trợ ngành công nghiệp phần mềm thế giới trước các chính phủ và thị trường quốc tế. Các thành viên của BSA nằm trong số những công ty cải tiến nhất trên thế giới, kiến tạo những giải pháp phần mềm tạo động lực cho nền kinh tế và cải thiện cuộc sống hiện đại. Với trụ sở tại Washington, DC, và các cơ sở hoạt động tại hơn 60 quốc gia, BSA tiên phong dẫn đầu các chương trình về tuân thủ, qua đó thúc đẩy việc sử dụng phần mềm hợp pháp và ủng hộ những chính sách công giúp phát triển cải tiến công nghệ và tạo ra sự tăng trưởng trong nền kinh tế số.

Các thành viên của BSA bao gồm: Adobe, Akamai, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, Box, CA Technologies, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, SAS Institute, Siemens PLM Software, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, và Workday.

Chúng tôi ghi nhận và thật sự trân trọng những nỗ lực quan trọng mà BCA và *Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao* đã và đang thực hiện nhằm đảm bảo rằng Việt Nam có khả năng sẵn sàng ngăn chặn và kiểm soát các nguy cơ về an ninh mạng. Tuy nhiên, việc thi hành Luật ANM trên phạm vi quá rộng - đặc biệt đối với yêu cầu lưu trữ dữ liệu tại Việt Nam, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam và quyền truy cập thông tin của cơ quan thực thi pháp luật - vẫn là những biện pháp thiếu hiệu quả để đạt được mục tiêu này và sẽ có tác động bất lợi với sự đổi mới và các khoản đầu tư.

Như đã nêu trong bản ý kiến trước đây của chúng tôi vào ngày 28/05/2018, điều quan trọng đối với Chính phủ Việt Nam là một cách tiếp cận linh hoạt, có khả năng hỗ trợ nhiều lĩnh vực kinh doanh, cũng như việc công nhận và tích hợp các cơ chế chuyển dữ liệu hiện có trong khu vực. Một khuôn khổ pháp lý mang tính dự báo tốt và đủ linh hoạt để cho phép sử dụng các sản phẩm và dịch vụ công nghệ tân tiến về lâu dài sẽ mang đến những kết quả tốt nhất về bảo vệ an ninh. Chúng tôi xin đưa ra những khuyến nghị sau đây nhằm giúp thực hiện được những mục tiêu đó.

Các điều khoản về lưu trữ dữ liệu tại Việt Nam không phù hợp với tinh thần của các cam kết của Việt Nam trong khuôn khổ Hiệp định Đối tác Toàn diện và Tiến bộ xuyên Thái Bình Dương (**CPTPP**), trong đó các bên đã thỏa thuận cấm yêu cầu lưu trữ dữ liệu một cách bắt buộc. Những quy định này cũng gây ra lo ngại liên quan đến cam kết của Việt Nam theo Hiệp định chung về Thương mại Dịch vụ (**GATS**), trong đó cho phép thương mại dịch vụ xuyên biên giới trong nhiều lĩnh vực mà không có hạn chế hay giới hạn. Những cam kết đó bao trùm nhiều ngành dịch vụ có liên quan mật thiết hoặc bao gồm dịch vụ trao đổi dữ liệu xuyên biên giới, mà hệ lụy là những giới hạn mà Việt Nam đưa ra sẽ vi phạm và làm suy giảm giá trị của các cam kết của mình theo Hiệp định GATS. Những quy định đó cũng gây ra lo ngại liên quan đến cam kết của Việt Nam trong nghĩa vụ đối xử quốc gia với dịch vụ nước ngoài và nhà cung cấp dịch vụ nước ngoài.

Cuối cùng, với tư cách một nền kinh tế thành viên APEC, Việt Nam không nên bỏ qua khả năng tham gia vào Hệ thống Quy tắc Bảo mật Xuyên biên giới của APEC (**CBPR**) trong tương lai. Như Bộ trưởng các nền kinh tế thành viên đã ghi nhận vào năm 1998, "*Một hệ thống pháp lý ngăn chặn hoặc cản trở không cần thiết dòng chảy thông tin sẽ có tác động tiêu cực tới doanh nghiệp, nền kinh tế và từng cá nhân trên thế giới.*"

Khi dòng chảy dữ liệu sẽ bị gián đoạn do yêu cầu dữ liệu phải được lưu trữ tại một nơi nhất định, an ninh mạng sẽ bị suy giảm nghiêm trọng. Bảo mật dữ liệu về bản chất không phụ thuộc vào vị trí địa lý của dữ liệu đó hoặc địa điểm đặt cơ sở hạ tầng hỗ trợ chúng. Các doanh nghiệp sẽ cân nhắc rất nhiều yếu tố khi quyết định đặt cơ sở hạ tầng kỹ thuật số, chẳng hạn như tối ưu hóa tốc độ và khả năng truy cập Internet, phát triển khả năng sao lưu và lưu trữ, và sử dụng giải pháp bảo mật tân tiến nhất Dự thảo Nghị định giới hạn khả năng quyết định của doanh nghiệp với các yếu tố trên. Do tính chất phức tạp và nhạy cảm của vấn đề, chúng tôi đặc biệt khuyến khích BCA không nên vội vàng thi hành tất cả các khía cạnh của Luật ANM, đặc biệt là những quy định liên quan đến lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam, mà nên xem xét kỹ lưỡng mọi vấn đề được đặt ra, bao gồm những tác động và hậu quả không mong muốn của Dự thảo Nghị định.

Trong góp ý này, chúng tôi sẽ nhấn mạnh một số quy định của Dự thảo Nghị định gây ra nhiều lo ngại đối với các thành viên của chúng tôi. Về vấn đề này, chúng tôi rất mong BCA xem xét, làm rõ thêm một số nội dung của Dự thảo Nghị định bởi việc thi hành Luật ANM sẽ ảnh hưởng rất lớn tới sự phát triển của nền công nghiệp số của Việt Nam. Nhìn chung, góp ý của chúng tôi tập trung vào một số điểm sau:

(i) Yêu cầu lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam theo Chương V của Dự thảo Nghị định nên được giới hạn trong phạm vi rõ ràng và cụ thể, trong đó bao gồm các thủ tục hành chính và cơ chế khiếu nại thích hợp;

(ii) Hệ thống thông tin mà <u>không phải</u> là "hệ thống thông tin quan trọng về an ninh quốc gia" nên được loại bỏ khỏi những yêu cầu theo quy định tại Điều 19 của Dự thảo Nghị định và cần phải có các thủ tục hành chính và cơ chế khiếu nại đối với việc "kiểm tra đột xuất"; và

(iii) Cần bao gồm trình tự thẩm định, đánh giá cụ thể cũng như ngoại lệ đối với các điều kiện bảo đảm an ninh mạng đối với trang thiết bị, phần cứng, phần mềm là thành phần hệ thống thông tin quan trọng về an ninh quốc gia theo quy định tại Điều 14 của Dự thảo Nghị định.

B. Góp ý và Khuyến nghị

1. Yêu cầu lưu trữ dữ liệu và đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam theo Chương V của Dự thảo Nghị định nên được giới hạn trong phạm vi rõ ràng và cụ thể, trong đó bao gồm các thủ tục hành chính và cơ chế khiếu nại thích hợp

Điều 25 của Dự thảo Nghị định quy định rằng, các doanh nghiệp trong và ngoài nước có đầy đủ các điều kiện sau đây phải lưu trữ dữ liệu và đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam:

(i) Là doanh nghiệp cung cấp một trong các dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng có hoạt động kinh doanh tại Việt Nam sau đây: Dịch vụ viễn thông; Dịch vụ lưu trữ, chia sẻ dữ liệu trên không gian mạng; Cung cấp tên miền quốc gia hoặc quốc tế cho người sử dụng dịch vụ tại Việt Nam; Thương mại điện tử; Thanh toán trực tuyến; Trung gian thanh toán; Dịch vụ kết nối vận chuyển qua không gian mạng; Mạng xã hội và truyền thông xã hội; Trò chơi điện tử trên mạng; Thư điện tử;

(ii) Có hoạt động thu thập, khai thác, phân tích, xử lý các loại dữ liệu quy định tại Điều 24 Nghị định này;

(iii) Để cho người sử dụng dịch vụ thực hiện hành vi được quy định tại Khoản 1, 2 Điều 8 Luật An ninh mạng; và

(iv) Vi phạm quy định tại Khoản 4 Điều 8, điểm a hoặc điểm b khoản 2 Điều 26 Luật An ninh mạng.

Bộ trưởng BCA sẽ có toàn quyền yêu cầu các doanh nghiệp cụ thể có các điều kiện trên lưu trữ dữ liệu tại Việt Nam và thành lập chi nhánh/văn phòng đại diện tại Việt Nam.

Định nghĩa này có phạm vi rộng và có khả năng bao trùm hầu như toàn bộ các dịch vụ trực tuyến hiện đang có mặt tại Việt Nam thông qua mạng Internet. Khung pháp lý cho việc thi hành yêu cầu lưu trữ dữ liệu và đặt chi nhánh/văn phòng tại Việt Nam theo Chương V của Dự thảo Nghị định có thể được làm rõ và hoàn thiện hơn như sau:

1.1. Điều 24, 25 và 26 của Dự thảo Nghị định chỉ nên được áp dụng trong trường hợp vi phạm quy định tại khoản 1 hoặc khoản Điều 8, và khoản 4 Điều 8, điểm a hoặc điểm b khoản 2 Điều 26 Luật ANM

Dựa trên bản dự thảo hiện tại, vẫn chưa rõ liệu Điều 25 chỉ áp dụng cho các doanh nghiệp có đủ cả bốn (4) điều kiện trên (Khoản 1 Điều 25) **và** đã được Bộ Công an yêu cầu (Khoản 2 Điều 25) thì mới phải tuân thủ các quy định về lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam.

BSA khuyến nghị việc thi hành yêu cầu lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam được giới hạn trong phạm vi hẹp - và chỉ nên áp dụng trong trường hợp cần thiết để đạt được mục tiêu của Luật ANM. Về vấn đề này, BCA nên sửa đổi Dự thảo Nghị định theo hướng **giới hạn phạm vi điều chỉnh của khoản 1 Điều 25 chỉ đối với những doanh nghiệp bị kết luận là có vi phạm Luật ANM, cụ thể là các điều sau: (a) Khoản 1 hoặc khoản 2 Điều 8; và (b) khoản 4 Điều 8, điểm a khoản 2 Điều 26 hoặc điểm b khoản 2 Điều 26**, như đã được đề cập trong Dự thảo Nghị định hiện tại là những mối quan tâm chủ yếu của BCA. BSA cũng khuyến nghị **xóa bỏ điểm a và điểm b khoản 1 Điều 25 để làm sáng tỏ hơn phạm vi điều chỉnh.**

Bên cạnh đó, chúng tôi khuyến nghị BCA ***làm rõ thêm rằng chỉ những doanh nghiệp sở hữu và kiểm soát dữ liệu được quy định tại Điều 24 mới có thể thực hiện những hành vi vi phạm***

các điều khoản trên, và do đó Điều 25 không nên được áp dụng cho các doanh nghiệp không sở hữu hoặc kiểm soát dữ liệu được quy định tại Điều 24. Chẳng hạn đối với cơ sở hạ tầng công nghệ thông tin tự phục vụ, khách hàng của các nhà cung cấp dịch vụ đám mây thường sở hữu và kiểm soát dữ liệu; họ có quyền lựa chọn dữ liệu nào để lưu trữ, lưu trữ ở đâu và thường chịu toàn bộ trách nhiệm trong việc thực hiện các biện pháp kỹ thuật và tổ chức thích hợp để bảo vệ dữ liệu cá nhân khỏi việc bị phá hoại tình cờ hoặc bất hợp pháp, hoặc bị mất, thay đổi, tiết lộ hoặc truy cập không phép. Trong những trường hợp này, các nhà cung cấp dịch vụ đám mây không có khả năng kiểm soát hoặc không thể biết được liệu khách hàng đang tải loại dữ liệu gì lên dịch vụ của họ, bao gồm nội dung có thể vi phạm pháp luật Việt Nam của dữ liệu.

Thi hành chính sách lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng tại Việt Nam trên phạm vi rộng sẽ ảnh hưởng tiêu cực tới sức cạnh tranh của nền kinh tế Việt Nam, bởi các doanh nghiệp thuộc mọi lĩnh vực và quy mô ở Việt Nam đều phụ thuộc và hưởng lợi từ dòng chảy dữ liệu tự do vào và ra khỏi quốc gia. Người tiêu dùng sẽ không tránh khỏi việc gián tiếp chịu các chi phí cho việc lưu trữ dữ liệu khi giá cả leo thang. Khi yêu cầu các doanh nghiệp tại Việt Nam phải sử dụng các trung tâm dữ liệu trong nước, điều đó sẽ làm tăng chi phí - một áp lực đối với các doanh nghiệp vừa và nhỏ. Về lâu dài, những yêu cầu này cũng có khả năng làm suy giảm an ninh mạng khi các công ty buộc phải sử dụng nguồn quỹ đáng lẽ được dành cho hoạt động tăng cường bảo mật kết nối mạng.

1.2. Yêu cầu lưu trữ dữ liệu và đặt chi nhánh/văn phòng tại Việt Nam chỉ nên được thi hành với tư cách là biện pháp cuối cùng và cần đi kèm thủ tục pháp lý và cơ chế khiếu nại

Chúng tôi khuyến nghị BCA làm rõ rằng ***chỉ khi nào các doanh nghiệp bị xác định là vi phạm các điều trên thì BCA mới xem xét yêu cầu doanh nghiệp có hoạt động vi phạm phải thực hiện lưu trữ dữ liệu và đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam***. Trong trường hợp đó, việc áp dụng yêu cầu lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam nên được coi là giải pháp cuối cùng, và cần có các thủ tục pháp lý và cơ chế khiếu nại nhằm tạo ra phương thức xem xét và giải quyết khiếu nại. Về những nội dung trên, chúng tôi đưa ra những khuyến nghị như sau:

(i) **Doanh nghiệp sẽ không bị buộc phải lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam nếu họ có thể tuân thủ yêu cầu truy cập dữ liệu hợp pháp.** Chúng tôi khuyến nghị BCA làm rõ rằng các doanh nghiệp hiện đã cung cấp dữ liệu cho BCA hoặc trao quyền truy cập dữ liệu theo yêu cầu căn cứ theo quy định của pháp luật, sẽ không bị buộc phải lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam.

(ii) **Các thủ tục pháp lý và quyết định của tòa án nên được đảm bảo đầy đủ trước khi thực hiện yêu cầu lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam.** Phạm vi dữ liệu sẽ được lưu trữ tại Việt Nam cũng như tính chất và hoạt động bắt buộc đối với chi nhánh hoặc văn phòng đại diện tại Việt Nam cần được xác định và giới hạn cụ thể bởi các thể chế giám sát và đánh giá tư pháp độc lập. Các doanh nghiệp nên được thông báo trước, được tạo cơ hội thực hiện các biện pháp khắc phục, và được quyền phản đối các quyết định và được quyền khiếu nại các quyết định bất lợi tại tòa án, trước khi các yêu cầu lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam chính thức được áp dụng . Hơn nữa, các yêu cầu đó chỉ nên được áp dụng với các doanh nghiệp vi phạm có quyền kiểm soát những loại dữ liệu theo quy định, thay vì với các bên cung cấp thứ ba hoặc các bên xử lý dữ liệu của họ. Việc áp dụng trực tiếp quyết định của tòa án với các bên cung cấp thứ ba và bên xử lý dữ liệu có thể khiến họ khó xử khi buộc phải vi phạm các thỏa thuận hợp đồng mà họ có với khách hàng hoặc các nghĩa vụ pháp lý của họ tại các quốc gia, vùng lãnh thổ khác.

(iii) **Quyền khiếu nại nên được đảm bảo đối với tất cả các quyết định của tòa án.** Quyền khiếu nại tương ứng nên được đảm bảo trong mọi trường hợp có các yêu cầu bắt buộc liên quan tới lưu trữ dữ liệu và đặt chi nhánh/văn phòng tại Việt Nam. Những hành vi bắt buộc phải thực hiện có thể quá chi tiết và tạo gánh nặng cho các doanh nghiệp hoặc không khả thi về mặt kỹ thuật, hoặc có thể không liên quan trực tiếp đến vi phạm. Do đó cung cấp một phương thức khiếu nại trong các tình huống như vậy là điều vô cùng cần thiết.

1.3. Giới hạn phạm vi dữ liệu cần phải lưu trữ tại Việt Nam theo quy định tại Điều 24

Điều 24 hiện tại áp đặt yêu cầu lưu trữ tại Việt Nam lên một phạm vi dữ liệu rất rộng. Chúng tôi hiểu rằng BCA quan tâm đến vấn đề chủ quyền dữ liệu và đảm bảo rằng dữ liệu luôn sẵn có và có thể truy cập được tại Việt Nam để duy trì an ninh quốc gia. Tuy nhiên, việc đòi hỏi phải lưu trữ tại Việt Nam một phạm vi dữ liệu cá nhân người dùng rất rộng là không cân xứng với mối quan tâm này, và là không cần thiết và nặng nề cho các nhà cung cấp dịch vụ.

Khi phạm vi dữ liệu cần phải đáp ứng yêu cầu càng rộng, gánh nặng và chi phí mà các nhà cung cấp dịch vụ sẽ càng lớn. Trong khi đó, một số loại dữ liệu cá nhân, dữ liệu được tạo ra bởi người sử dụng dịch vụ tại Việt Nam và dữ liệu liên quan đến mối quan hệ của người sử dụng dịch vụ tại Việt Nam không cần thiết phải lưu trữ trong nước mới có thể tiếp cận được. Thay vào đó, phát triển một thỏa thuận chung/khuôn khổ hoặc nguyên tắc ứng xử với các doanh nghiệp quốc tế có thể là một lựa chọn tốt hơn cho BCA và môi trường kinh doanh.

Hơn nữa, yêu cầu lưu trữ dữ liệu tại Việt Nam sẽ có tác động tiêu cực tới những nỗ lực bảo vệ an ninh mạng. Nguy cơ tấn công an ninh mạng và đột nhập dữ liệu được lưu trữ tại Việt Nam có thể sẽ tăng cao, bởi thông tin được lưu trữ tập trung là một mục tiêu hấp dẫn đối với những phần tử xấu. Chúng hiểu rằng khi xâm nhập hệ thống dữ liệu trong nước sẽ có thể thu lại được những bộ dữ liệu hoàn chỉnh. Ngược lại, sử dụng hệ thống đám mây để phân bổ việc lưu trữ dữ liệu ra toàn cầu sẽ tăng cường khả năng phân hóa các bộ dữ liệu, qua đó tránh được khả năng một hành vi xâm nhập tại một địa điểm có thể trao quyền truy cập toàn bộ một bộ dữ liệu.

Nếu BCA vẫn cần đặt ra yêu cầu lưu trữ dữ liệu bởi một nhà cung cấp dịch vụ không cấp quyền truy cập hoặc cung cấp dữ liệu cho Bộ, chúng tôi khuyến nghị BCA triển khai yêu cầu lưu trữ dữ liệu tại Việt Nam trong phạm vi hẹp và chỉ khi thực sự cần thiết như sau:

(i) ***Dữ liệu cần phải lưu trữ tại Việt Nam nên được giới hạn trong phạm vi thông tin thực sự cần thiết đối với mục tiêu của BCA.*** Đây có thể bao gồm dữ liệu liên quan tới quá trình điều tra hoặc vi phạm Khoản 1, 2 hoặc 4 Điều 8, điểm a hoặc điểm b khoản 2 Điều 26 Luật An ninh mạng. Yêu cầu lưu trữ dữ liệu tại Việt Nam không nên đồng nghĩa với việc yêu cầu *tất cả dữ liệu* được liệt kê theo quy định tại Điều 24 phải được lưu trữ tại Việt Nam mà không có lý do rõ ràng.

(ii) ***Những bộ dữ liệu nếu bị xâm nhập sẽ có tác động đáng kể tới cá nhân nên được loại bỏ khỏi Điều 24.*** Do yêu cầu lưu trữ dữ liệu tại Việt Nam sẽ làm gia tăng nguy cơ an ninh mạng, BCA cũng nên xem xét loại bỏ những bộ dữ liệu có thể có tác động đáng kể tới cá nhân nếu xảy ra một tấn công mạng hoặc xâm nhập dữ liệu ra khỏi phạm vi yêu cầu lưu trữ tại Việt Nam. Ví dụ, các thông tin như số thẻ căn cước công dân, số thẻ tín dụng, tình trạng sức khỏe, hồ sơ y tế và sinh trắc học cần được loại trừ khỏi Điều 24, bởi việc xâm nhập dữ liệu có liên quan đến các loại dữ liệu này có thể gây hại đáng kể cho cá nhân;

(iii) ***Chỉ nên lưu trữ một bản sao dữ liệu liên quan tại Việt Nam.*** BCA cần làm rõ trong Dự thảo Nghị định rằng bản sao dữ liệu quy định tại Điều 24 cũng có thể được lưu trữ ngoài lãnh thổ Việt Nam, để các công ty có thể dựa vào thông tin này để phân tích và liên hệ, và đặc biệt để truy cập kịp thời nguồn thông tin có nguy cơ và khả năng tổng hợp dữ liệu thu thập được thành nguồn thông tin hữu ích cho các sản phẩm và dịch vụ an ninh;

(iv) ***Yêu cầu lưu trữ dữ liệu tại Việt Nam cần phải cụ thể và được áp dụng theo trình tự pháp luật.*** Điều này sẽ đảm bảo rằng trình tự sự việc được ghi lại và có sự giải thích về phạm vi, mục đích, hoàn cảnh và thời gian;

(v) ***Các doanh nghiệp không nên bị yêu cầu phải thu thập thêm dữ liệu.*** Ngoài ra, cần phải công nhận một thực tế rằng không phải công ty nào cũng thu thập dữ liệu cá nhân giống nhau. Bởi vậy, BCA nên làm rõ rằng các doanh nghiệp sẽ không bị yêu cầu phải thu thập dữ liệu cá nhân không cần thiết hoặc các dữ liệu khác không phục vụ cho các nhu cầu của mô hình kinh doanh của mình; và

(vi) ***Các bên xử lý dữ liệu (data processor) và bên cung cấp không nên có trách nhiệm thu thập, lưu giữ và lưu trữ bản sao thông tin người sử dụng dịch vụ.*** Dự thảo Nghị định không định nghĩa khái niệm "người sử dụng dịch vụ tại Việt Nam" cũng như tiêu chí xác định thế nào là "người sử dụng dịch vụ tại Việt Nam". Khái niệm "người sử dụng dịch vụ" nên được làm rõ là "người sử dụng dịch vụ" của bên quản lý dữ liệu (data controller), từ đó làm rõ rằng thương nhân hoặc nhà cung cấp dịch vụ của người quản lý dữ liệu không có nghĩa vụ phải thu thập, lưu giữ và lưu trữ bản sao thông tin của "người sử dụng dịch vụ" của bên quản lý dữ liệu ở Việt Nam.

1.4. Phạm vi điều chỉnh của khái niệm "nhà cung cấp dịch vụ" theo quy định tại khoản 1 Điều 25 nên được thu hẹp và làm rõ

Khoản 3 Điều 26 của Luật ANM quy định doanh nghiệp trong nước và ngoài nước *"cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam"* ("**Nhà cung cấp dịch vụ trên không gian mạng**") sẽ phải tuân thủ yêu cầu lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam. Khoản 1 Điều 2[2] và điểm a khoản 1 Điều 25 của Dự thảo Nghị định quy định chung rằng Nhà cung cấp dịch vụ trên không gian mạng là các doanh nghiệp hoạt động thương mại nhằm cung cấp một trong các dịch vụ sau tại Việt Nam::

1. Dịch vụ viễn thông;
2. Dịch vụ lưu trữ, chia sẻ dữ liệu trên không gian mạng;
3. Dịch vụ cung cấp tên miền quốc gia hoặc quốc tế cho người sử dụng dịch vụ tại Việt Nam;
4. Thương mại điện tử;
5. Thanh toán trực tuyến;
6. Trung gian thanh toán;
7. Dịch vụ kết nối vận chuyển qua không gian mạng;
8. Mạng xã hội và truyền thông xã hội;
9. Trò chơi điện tử trên mạng;
10. Thư điện tử.

Theo khoản 1 Điều 25, phạm vi các doanh nghiệp thỏa mãn điều kiện là "Nhà cung cấp dịch vụ trên không gian mạng" vẫn còn rất rộng và thiếu rõ ràng. Điều 25 chưa ghi nhận mối quan hệ của doanh nghiệp với bên cung cấp và bên xử lý dữ liệu, cũng như hiệu lực của Điều 25 đối với từng bên. Bên cung cấp và bên xử lý dữ liệu có nhiệm vụ xử lý dữ liệu và thông tin thay mặt cho các doanh nghiệp khác (tức bên quản lý dữ liệu) hầu như không nắm được thông tin về dữ liệu của khách hàng của mình. Do đó, họ có thể không biết liệu người quản lý dữ liệu có lưu trữ dữ liệu được điều chỉnh đối với dịch vụ hay không, mà điều đó sẽ dẫn tới việc áp dụng Luật ANM và Dự thảo Nghị định. Chẳng hạn, nhà cung cấp dịch vụ đám mây có thể không biết liệu người dùng dữ liệu có lưu trữ dữ liệu cá nhân trên nền tảng đám mây hay không. Do đó, ***chúng tôi khuyến nghị BCA loại bỏ khỏi phạm vi điều chỉnh các doanh nghiệp xử lý dữ liệu và thông tin thay mặt cho các doanh nghiệp khác (tức bên quản lý dữ liệu).***

Thêm vào đó, các dịch vụ được liệt kê phía trên, khi đặt trong mối tương quan với các luật khác (ví dụ Luật Viễn thông), lại trở nên trùng lặp và dễ nhầm lẫn. Chúng tôi cho rằng các dịch vụ sau cần phải được cụ thể hóa:

(i) Không rõ dịch vụ nào sẽ được coi là "Lưu trữ và chia sẻ dữ liệu trên không gian mạng".
(ii) Không rõ dịch vụ nào sẽ được coi là "thương mại điện tử" theo Dự thảo Nghị định, và liệu thuật ngữ này có dẫn chiếu tới các quy định khác có liên quan hay không (chẳng hạn Nghị định số 52/2013/NĐ-CP và/hoặc Nghị định số 09/2018/NĐ-CP).

Khi thiếu định nghĩa cụ thể, một số dịch vụ được nêu trên có thể trùng lặp với nhau, chẳng hạn dịch vụ viễn thông và thư điện tử. Chúng tôi xin lưu ý rằng dịch vụ thư điện tử là một dịch vụ viễn

[2] Khoản 1 Điều 2 của Dự thảo Nghị định có một lỗi soạn thảo là viện dẫn nhầm tới Điều 24. Danh sách các doanh nghiệp cung cấp dịch vụ thực chất được quy định tại Điều 25.

thông giá trị gia tăng. Trên cơ sở này, chúng tôi khuyến nghị BCA rút ngắn danh sách doanh nghiệp đủ điều kiện là "Nhà cung cấp dịch vụ trên không gian mạng". ***Cụ thể, chúng tôi cũng khuyến nghị BCA xóa bỏ Danh mục số 2 và số 10 (tức dịch vụ lưu trữ, chia sẻ dữ liệu trên không gian mạng; và dịch vụ thư điện tử) để tránh gây nhầm lẫn và trùng lặp.***

Chúng tôi cũng khuyến nghị BCA cần định nghĩa rõ danh mục dịch vụ tại khoản 1 Điều 25 của Dự thảo Nghị định. Cách tốt nhất là các dịch vụ này nên phù hợp với các định nghĩa và danh mục đã được cung cấp trong các quy định hiện hành. Ví dụ, dịch vụ viễn thông và dịch vụ viễn thông giá trị gia tăng đã được quy định tại Luật Viễn thông và Thông tư số 05/2012/TT-BTTT.

1.5. Thời gian lưu trữ dữ liệu theo quy định tại Điều 26

Điều 26 quy định về thời gian lưu giữ, nhưng không rõ liệu thời gian này chỉ áp dụng cho các doanh nghiệp phải tuân thủ các yêu cầu lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam, hay áp dụng cho *tất cả* các doanh nghiệp nói chung. Lý do là bởi thời gian lưu trữ "nhật ký hệ thống" theo quy định tại Điều 26 không rơi vào bất kỳ danh mục dữ liệu nào phải được lưu trữ tại Việt Nam theo quy định tại Điều 24. Chúng tôi cũng lưu ý rằng Điều 26 quy định "thời gian lưu trữ dữ liệu" thay vì "thời gian lưu giữ dữ liệu ở Việt Nam".

Hơn nữa, Điều 24 và Điều 26 không nêu rõ liệu yêu cầu này có nghĩa là phải lưu trữ các dữ liệu đó duy nhất tại Việt Nam hay chỉ cần lưu trữ một bản sao các dữ liệu đó tại Việt Nam.

Chúng tôi khuyến nghị BCA nên loại bỏ thời gian lưu trữ liên quan đến "nhật ký hệ thống" ở Điều 26 và trong Chương 5 vì "nhật ký hệ thống" không phải là một loại dữ liệu nằm trong danh sách những dữ liệu phải được lưu trữ tại Việt Nam theo quy định tại Điều 24. Tiêu đề của Điều 26 nên được thay đổi thành "thời gian lưu trữ dữ liệu ở Việt Nam đối với dữ liệu phải được lưu trữ tại Việt Nam".

Chúng tôi cũng khuyến nghị BCA nên làm rõ rằng yêu cầu lưu trữ dữ liệu không đồng nghĩa với việc phải lưu trữ những dữ liệu đó duy nhất tại Việt Nam (tức chỉ cần lưu trữ một bản sao của các dữ liệu ở Việt Nam mà thôi).

1.6. Thời hạn chuyển tiếp theo quy định tại Điều 29

Điều 29 quy định rằng các doanh nghiệp quy định tại Điều 25 sẽ có một (1) năm để tuân thủ các yêu cầu về lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam kể từ ngày BCA có yêu cầu. Một (1) năm là không đủ để doanh nghiệp tuân thủ yêu cầu của BCA về việc lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam, bởi trên thực tế phải mất rất nhiều thời gian để có thể xác lập hiện diện tại Việt Nam.

Do đó, chúng tôi khuyến nghị BCA xem xét một trong các phương án sau:

(i) Kéo dài thời hạn chuyển tiếp lên ba (3) năm và bổ sung quy định ngoại lệ cho các doanh nghiệp tùy từng hoàn cảnh cụ thể; hoặc

(ii) Nới lỏng quy định đối với các doanh nghiệp có yêu cầu phải lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam bằng cách cho phép họ nộp hồ sơ cam kết sẽ tuân thủ các yêu cầu trong trường hợp không đáp ứng được thời hạn một (1) năm.

2. Hệ thống thông tin không phải là "hệ thống thông tin quan trọng về an ninh quốc gia" nên được loại trừ rõ ràng khỏi các yêu cầu của Điều 19 của Dự thảo Nghị định và cần có thủ tục pháp lý và cơ chế khiếu nại thích hợp đối với việc"kiểm tra an ninh mạng đột xuất"

Khoản 2 Điều 19 của Dự thảo Nghị định quy định trình tự và thủ tục kiểm tra an ninh mạng không báo trước, bao gồm trường hợp tiến hành kiểm tra hệ thống thông tin không "quan trọng về an ninh quốc gia" (theo khoản 1 Điều 24 Luật ANM). Dù khoản 1 Điều 24 quy định rằng chỉ có thể tiến

hành kiểm tra nếu như có hành vi *"vi phạm pháp luật về an ninh mạng xâm phạm an ninh quốc gia, hoặc gây tổn hại nghiêm trọng đến trật tự, an toàn xã hội*", cả Dự thảo Nghị định và Luật ANM đều không quy định rõ các trường hợp việc kiểm tra này sẽ được thực hiện.

Với nội dung như hiện được soạn thảo, những quy định này gây ra nhiều lo lắng vì chúng có thể được diễn giải quá rộng và trao quá nhiều quyền lực cho cơ quan nhà nước để truy cập thông tin mà không cần trình bày lý do hoặc quyết định thích hợp. Điều 24 của Luật ANM và Điều 19 của Dự thảo Nghị định không hạn chế hoặc quy định phạm vi thông tin mà lực lượng chuyên trách bảo vệ an ninh mạng có thể truy cập trong quá trình kiểm tra. Nếu chỉ dựa vào riêng điều khoản này, có thể hiểu rằng lực lượng chuyên trách được quyền truy cập mọi thông tin trên bất kỳ hệ thống nào của các cơ quan, tổ chức ở Việt Nam (trong quá trình kiểm tra theo trường hợp trên). Hơn nữa, thông tin được kiểm tra nhiều khả năng sẽ bao gồm cả dữ liệu cá nhân hoặc bí mật thương mại được bảo hộ theo pháp luật liên quan của Việt Nam, chẳng hạn như Bộ luật Dân sự và Luật Sở hữu trí tuệ. Do đó, quyền truy cập bất hợp lý của một cơ quan vào bí mật cá nhân hoặc bí mật doanh nghiệp trong hệ thống thông tin sẽ có thể bị coi là xâm phạm quyền riêng tư của công dân.

Dựa trên những phân tích trên, chúng tôi đưa ra những khuyến nghị sau:

(i) **Giới hạn các trường hợp mà lực lượng chuyên trách bảo vệ an ninh mạng thực hiện kiểm tra trong phạm vi các trường hợp liên quan đến "hệ thống thông tin quan trọng về an ninh quốc gia" và dẫn đến tình trạng "xâm phạm an ninh quốc gia hoặc gây tổn hại nghiêm trọng trật tự, an toàn xã hội".** Các trường hợp như vậy cần được định nghĩa rõ ràng. Ngoài ra, phạm vi thông tin mà lực lượng chuyên trách bảo vệ an ninh mạng có thể truy cập trong quá trình kiểm tra phải được giới hạn trong phạm vi thông tin liên quan tới mục đích của việc kiểm tra;

(ii) **Một số danh mục thông tin có thể được miễn kiểm tra.** Danh mục này bao gồm như thông tin ưu tiên hoặc thông tin xâm phạm các quyền khác, chẳng hạn như thông tin cá nhân, hoặc thông tin không phù hợp với việc bảo hộ quyền sở hữu trí tuệ hoặc bí mật thương mại;

(iii) **Tạo ra một cơ chế khiếu nại để từ chối yêu cầu "kiểm tra đột xuất". BCA nên tạo một quy trình để cho phép các doanh nghiệp khiếu nại yêu cầu kiểm tra.** Các quyết định của tòa án phải được đảm bảo trong mọi trường hợp có yêu cầu buộc "kiểm tra đột xuất". Tất cả các biện pháp cưỡng chế đều phải được thực hiện theo quy định của pháp luật để đảm bảo rằng trình tự sự việc được ghi lại và có sự giải thích về phạm vi, mục đích, hoàn cảnh và thời gian. Quyền khiếu nại tương ứng cũng cần được đảm bảo. Nếu không có các biện pháp bảo đảm quy trình và cơ chế khiếu nại các biện pháp cưỡng chế, chẳng hạn như yêu cầu kiểm tra hệ thống máy tính hoặc tắt các máy tính đang hoạt động có thể là quá mức cần thiết và gây cản trở cho doanh nghiệp hoặc không khả thi về mặt kỹ thuật. Do đó, cung cấp một cơ chế khiếu nại những trường hợp như vậy là rất cần thiết. Trong trường hợp có yêu cầu "kiểm tra đột xuất" rơi vào ngoại lệ đối với quyết định của tòa án, những trường hợp ngoại lệ này phải được quy định cụ thể và hệ thống pháp luật Việt Nam cần quy định một văn bản tương ứng chẳng hạn như một lệnh bảo đảm hoặc "tài liệu khẩn cấp tạm thời" nhằm xác định rõ các yêu cầu kiểm tra; và

(iv) **Cần tránh việc áp dụng trực tiếp quyết định của tòa án cho các bên cung cấp thứ ba hoặc bên xử lý dữ liệu.** Khi việc kiểm tra bao gồm cả doanh nghiệp vận hành "hệ thống thông tin quan trọng về an ninh quốc gia" và bên cung cấp thứ ba, cần tránh việc áp dụng trực tiếp quyết định của tòa án cho các bên cung cấp thứ ba vì việc này sẽ đặt họ vào thế bí khi phải vi phạm các thỏa thuận hợp đồng mà họ có với doanh nghiệp vận hành "hệ thống thông tin quan trọng về an ninh quốc gia" (chẳng hạn nghĩa vụ bảo mật và bảo vệ dữ liệu) hoặc các nghĩa vụ pháp lý của họ tại các quốc gia, vùng lãnh thổ khác.

3. *Cần bao gồm trình tự thẩm định, đánh giá cụ thể cũng như ngoại lệ đối với các điều kiện bảo đảm an ninh mạng đối với trang thiết bị, phần cứng, phần mềm là thành phần hệ thống thông tin quan trọng về an ninh quốc gia ("Hệ thống Quan trọng") theo quy định tại Điều 14 của Dự thảo Nghị định*

Căn cứ Điều 14 của Dự thảo Nghị định, trang thiết bị, phần cứng và phần mềm là thành phần Hệ thống Quan trọng phải được kiểm tra an ninh mạng để phát hiện điểm yếu, lỗ hổng bảo mật, mã độc, bảo đảm sự tương thích với các thành phần khác trong hệ thống thông tin quan trọng về an ninh quốc gia. Ngoài ra, các sản phẩm được lực lượng chuyên trách bảo vệ an ninh mạng cảnh báo nguy cơ gây mất an ninh mạng sẽ không được sử dụng, hoặc phải có biện pháp xử lý, khắc phục điểm yếu, lỗ hổng bảo mật và mã độc trước khi đưa vào sử dụng.

Dự thảo Nghị định không quy định chi tiết về bất kỳ thủ tục thẩm định hay đánh giá hoặc bất kỳ tiêu chí khách quan nào để xác định liệu một sản phẩm hoặc dịch vụ cụ thể có phù hợp để sử dụng trong các Hệ thống Quan trọng hay không. Thủ tục đánh giá/thẩm định không rõ ràng có thể dẫn đến các thủ tục không minh bạch và tạo ra sự phân biệt đối xử giữa các nhà cung cấp nước ngoài và các nhà cung cấp trong nước. Hơn nữa, yêu cầu kiểm tra các thành phần và thiết bị của công ty có thể dẫn đến việc ép buộc truy cập thông tin ưu tiên hoặc thông tin xâm phạm các quyền khác, chẳng hạn như thông tin cá nhân, hoặc không phù hợp với việc bảo hộ quyền sở hữu trí tuệ hoặc bí mật thương mại. Do đó, chúng tôi xin đưa ra những khuyến nghị sau:

(i) BCA nên đưa ra ***một quy trình đánh giá hoặc thẩm định cụ thể*** cũng như các tiêu chí khách quan để xác định liệu một sản phẩm hoặc dịch vụ cụ thể có phù hợp để sử dụng trong Hệ thống Quan trọng hay không;

(ii) BCA nên bao gồm ***sự miễn trừ cụ thể đối với thông tin có thể được miễn kiểm tra*****,** bao gồm những thông tin không phù hợp với việc bảo hộ quyền sở hữu trí tuệ hoặc bí mật thương mại cũng như thông tin ưu tiên hoặc thông tin có thể xâm phạm các quyền khác; và

(iii) BCA cũng nên xem xét việc ***áp dụng các hệ thống chứng nhận được quốc tế công nhận như ISO/IEC 27034 hoặc Tiêu chí chung*** để xem xét và đánh giá các sản phẩm đã được sử dụng trong các hệ thống quan trọng thay vì đưa ra một cách tiếp cận khác.

C. Kết luận và Các bước tiếp theo

Chúng tôi xin một lần nữa cảm ơn BCA vì đã tạo cơ hội cho chúng tôi góp ý cho Dự thảo Nghị định. Chúng tôi trân trọng sự xem xét mà BCA dành cho những ý kiến nêu trên của chúng tôi.

BSA đại diện cho ngành công nghiệp phần mềm toàn cầu. Các thành viên của chúng tôi đang đi đầu trong quá trình đổi mới trong đó lấy dữ liệu làm động lực, phát triển những thành tựu tiên tiến trong trí tuệ nhân tạo, học máy và phân tích dựa trên điện toán đám mây. Các thành viên của chúng tôi có được lòng tin của người dùng bằng cách cung cấp các công nghệ bảo mật cần thiết nhằm chống lại các mối nguy hại trên môi trường mạng. Bằng cách làm việc sát sao với các chính phủ trên thế giới trong vấn đề phát triển chính sách và lập pháp về an ninh mạng, BSA đã thấy được tiềm năng của luật và các quy định về an ninh mạng trong việc ngăn chặn và quản lý các mối đe dọa trên môi trường mạng và đồng thời bảo vệ quyền riêng tư và tự do của công dân.

Dựa trên kinh nghiệm này, BSA đã phát triển Chính sách khung về An ninh mạng Quốc tế (**Chính sách khung**), trong đó đưa ra một mô hình được khuyến nghị đối với một chính sách an ninh mạng quốc gia toàn diện.[3] BSA khuyến khích Chính phủ Việt Nam và BCA tham khảo các thực tiễn quốc tế tốt nhất, như Chính sách khung về An ninh mạng của Viện Tiêu chuẩn và Công nghệ Quốc gia[4] và các nội dung tương tự trong Chính sách khung của BSA trong quá trình phát triển, thi hành và vận hành các quy tắc và yêu cầu liên quan đến an ninh mạng.

---

[3] *Chính sách khung về An ninh mạng Quốc tế của BSA* tại: https://bsacybersecurity.bsa.org/wp-content/uploads/2018/04/BSA_cybersecurity-policy.pdf. Để biết thêm thông tin chi tiết, tham khảo https://bsacybersecurity.bsa.org/.

[4] *Chính sách khung nhằm tăng cường cơ sở hạ tầng an ninh mạng thiết yếu, Phiên bản 1.1* cung cấp những hướng dẫn tập trung vào kết quả, dự trên phân tích rủi ro nhằm tăng cường cơ sở hạ tầng kết nối an ninh mạng thiết yếu. Tham khảo https://www.nist.gov/cyberframework.

Nếu có bất kỳ câu hỏi hoặc nội dung nào trong văn bản này cần được làm rõ, xin vui lòng liên hệ với chúng tôi. Chúng tôi xin chân thành cảm ơn ông và Bộ Công an đã dành thời gian quan tâm.

Trân trọng,

Tiến sỹ Jared Ragland
Giám đốc Cao cấp về Chính sách tại
Châu Á - Thái Bình Dương
BSA │ Liên minh phần mềm

PHỤ LỤC

(Đính kèm bản tiếng Anh)