CHƯƠNG 1 KỸ THUẬT SỐ

TỔNG QUAN

Kỹ thuật số là công cụ xuyên suốt của nền kinh tế và tác động đến tất cả các lĩnh vực và ngành nghề. Quá trình số hóa giúp tăng tốc và nâng cấp các quy trình và lĩnh vực kinh doanh truyền thống, đồng thời cũng đóng vai trò thiết yếu trong việc duy trì tính cạnh tranh trong bối cảnh nền kinh tế luôn thay đổi nhanh chóng.

Tuy nhiên những gì tồn tại trong thế giới vật chất hóa vẫn cần được phi vật chất hóa, và sự thay đổi thực sự sẽ diễn ra khi xuất hiện các giải pháp điện tử thay thế hợp pháp cho chữ ký sống, nhận dạng cá nhân, giấy phép kinh doanh, v.v., mà không cần nộp bản cứng vì lý do tuân thủ. Việc này cho phép các thủ tục hành chính hoặc kinh doanh có thể được thực hiện từ xa.

Việt Nam nên hướng tới xây dựng một môi trường thích hợp cho các công ty nhằm tận dụng công nghệ số để phát triển mạnh mẽ. Đặc biệt trong bối cảnh đại dịch COVID-19 toàn cầu, các doanh nghiệp và Chính phủ cần áp dụng các công nghệ và tiêu chuẩn mới để có thể cạnh tranh trên thị trường thế giới.

EVFTA là một cột mốc quan trọng đối với Việt Nam trong quá trình hội nhập toàn cầu. Vậy nhưng một trong những thách thức lớn nhất hiện nay là cuộc khủng hoảng do đại dịch COVID-19 đã và đang tạo ra những rào cản cho hoạt động giao thương. Tiểu ban Kỹ thuật số khuyến nghị ưu tiên các dự án giúp cải thiện tình hình, thu hút sự tham gia đối thoại của các chuyên gia quốc tế nhằm điều chỉnh cho phù hợp với các tiêu chuẩn toàn cầu.

Kể từ khi EVFTA có hiệu lực từ ngày 1 tháng 8 năm 2020, bây giờ chính là lúc chúng ta cần thực hiện các giải pháp nâng cao nền kinh tế số. Đồng thời, Việt Nam cũng đang thực hiện Quá trình Chuyển đổi số nhằm đạt được mục tiêu đề ra vào năm 2025-2030. Với mục tiêu tối đa hóa lợi ích của EVFTA và các hiệp định thương mại khác, Việt Nam sẽ cần tăng cường tạo thuận lợi cho thương mại xuyên biên giới.

Chúng tôi tin rằng những chủ đề sau đây có thể mang lại lợi ích ở cả cấp độ trong nước và quốc tế:

- Công nhận các giải pháp chữ ký điện tử để áp dụng cho các thỏa thuận xuyên biên giới
- Triển khai nền tảng và công cụ nhằm nâng cao truy xuất nguồn gốc, xuất xứ hàng hóa và tính minh bạch
- Tự do trao đổi dữ liệu xuyên biên giới
- Áp dụng các tiêu chuẩn bảo mật công nghệ được quốc tế công nhận

Chính phủ điện tử là một bước tiến lớn theo hướng phát triển này và Tiểu ban Kỹ thuật số rất quan tâm theo dõi những tiến triển sắp tới. Từ góc độ này, vấn đề chữ ký điện tử có tầm đặc biệt quan trọng, vì đây là một phương thức tối ưu giúp các doanh nghiệp tiếp tục hoạt động trong những hoàn cảnh khó có thể ký trực tiếp.

Chúng tôi luôn sẵn sàng hỗ trợ phát triển Chính phủ điện tử với tư cách là cầu nối trung gian giữa Việt Nam và EU.

I. AN NINH MẠNG

Cơ quan Chính phủ liên quan: Bộ Thông tin và Truyền thông (Bộ TT&TT), Bộ Công an (BCA), Văn phòng Chính phủ (VPCP)

Mô tả vấn đề

Luật an toàn thông tin mạng[1] đã thiết lập các tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin mạng, và Luật An ninh Mạng[2] (Luật ANM) đưa ra các quy định quản lý việc sử dụng các dịch vụ kỹ thuật số, bảo vệ và đảm bảo chủ quyền dữ liệu trong không gian mạng quốc gia, vì vậy việc thực thi hai quy định trên càng trở nên giá trị và cần thiết trong bối cảnh hiện tại. Những quy định trên bảo vệ bằng các biện pháp rộng nhất đối với "các chủ thể" trên lãnh thổ Việt Nam (ví dụ: người dùng sử dụng các dịch vụ trực tuyến, truy cập và truyền dữ liệu) và cuối cùng là thiết lập khuôn khổ và quy định yêu cầu các công ty nước ngoài tại thị trường Việt Nam phải tuân thủ. Luật ANM giúp Việt Nam bảo đảm cho nền kinh tế, tạo cơ sở đáng tin cậy cho các quan hệ đối tác kinh doanh trong và ngoài Việt Nam vì các nhà đầu tư sẽ tin tưởng vào khả năng tương thích của các hệ thống trong nước với các quy định quốc tế.

Cả quy định của Liên minh châu Âu và của Việt Nam đều buộc doanh nghiệp phải bảo mật hệ thống ở mức độ kỹ thuật để ngăn chặn bất kỳ sự cố rò rỉ thông tin nào do tấn công mạng. Tuy nhiên, vẫn có sự khác biệt về quy trình xử lý dữ liệu và quyền riêng tư hợp pháp như được đề cập dưới đây.

Theo những phân tích của chúng tôi về phạm vi và ứng dụng của Luật ANM, đồng thời với tư cách là đại diện của cộng đồng doanh nghiệp châu Âu, chúng tôi nhận định ba thách thức sau có thể xuất hiện:

- Làm thế nào để các tiêu chuẩn và ứng dụng của Việt Nam trở nên dễ hiểu đối với tất cả các đối tượng phải tuân thủ bộ quy tắc và quy trình này (đưa ra các tiêu chuẩn tương tự như quy định GDPR của châu Âu[3]).
- Giải quyết các mâu thuẫn có thể phát sinh đối với các công ty tuân theo quy định GDPR của châu Âu - và ngược lại, đối với các công ty Việt Nam kinh doanh với "chủ thể dữ liệu" châu Âu và do đó cần tuân thủ quy định GDPR.
- Nghiên cứu một chính sách dữ liệu đáp ứng chương trình nghị sự của Chính phủ Việt Nam về bảo mật dữ liệu, đồng thời giải quyết các mối quan tâm của cộng đồng doanh nghiệp. Tác động kinh tế của chính sách trên cần được xét đến.

1. Hài hòa hóa quy định trong nước và GDPR

Đảm bảo tự do trao đổi dữ liệu xuyên biên giới là nền tảng cho nền kinh tế kỹ thuật số và đóng vai trò then chốt trong tăng trưởng và đổi mới theo định hướng dữ liệu. Việc thành lập Tổ chức điều phối để giải quyết các trường hợp mâu thuẫn với sự đồng thuận của Ủy ban Bảo vệ Dữ liệu Cá nhân, hoặc bất kỳ tổ chức nào có liên quan về phía Việt Nam, Ban Bảo vệ Dữ liệu Châu Âu và Ủy ban Châu Âu sẽ đóng vai trò hỗ trợ quá trình này. Chứng nhận này công nhận việc tuân thủ Bộ quy tắc ứng xử (code of conduct), trong đó công ty cam kết rằng họ tuân thủ các tiêu chuẩn EU-GDPR để kinh doanh với các đối tác thuộc Liên minh châu Âu.

Phạm vi công việc của Tổ chức điều phối có thể bao gồm việc xử lý các vấn đề phát sinh hoặc khó khăn giữa các chủ thể Việt Nam và châu Âu. Ví dụ bất kỳ yêu cầu nào liên quan đến những xung đột

1 Luật số 86/2015/QH13 ngày 19 tháng 11 năm 2015 của Quốc hội về an toàn thông tin mạng.
2 Luật số 24/2018/QH14 ngày 12 tháng 6 năm 2018 của Quốc hội về An ninh mạng.
3 Quy định Chung về Bảo vệ Dữ liệu ngày 14 tháng 04 năm 2016 của Liên minh châu Âu (GDPR).

của các quy định của Việt Nam và EU-GDPR sẽ được xử lý bởi Điều phối viên.[4] Quyền truy cập đặc biệt vào dữ liệu được bảo vệ bởi GDPR có thể được cấp theo quy định tại Điều 49 của EU-GDPR (Điều khoản loại trừ) và theo Thỏa thuận tư pháp (Điều 48 EU-GDPR) của phía Liên minh Châu Âu. Tổ chức điều phối có thể là một tổ chức mới được thành lập với thành viên của Ủy ban Bảo vệ Dữ liệu Cá nhân từ phía Việt Nam và các thành viên được đề cử từ EU hoặc có thể thuộc một tổ chức của bên thứ ba, ví dụ như ở cấp ASEAN.

Vì GDPR được thông qua sau khi EVFTA kết thúc đàm phán, nên EVFTA không bao gồm các thỏa thuận liên quan về GDPR. Do đó, chúng tôi đề xuất thành lập một tổ công tác dưới Ủy ban Thương mại để giải quyết vấn đề này cũng như các vấn đề khác về thương mại điện tử và kỹ thuật số. Thành viên của tổ công tác này có thể bao gồm chuyên gia thuộc Ủy ban châu Âu, hoặc một nhóm công tác được hỗ trợ bởi EuroCham dưới Hội đồng Doanh nghiệp Liên minh châu Âu-Việt Nam. Chúng tôi cũng khuyến nghị thực hiện EVFTA để cho phép thảo luận và đạt được đồng thuận ở hai cấp độ: cấp độ thứ nhất là đàm phán giữa EU và Việt Nam, và cấp độ thứ hai là thông qua việc đánh giá các trường hợp thực tiễn.

Nhìn chung, chúng tôi khuyến nghị việc thực thi quy định của Việt Nam sẽ phù hợp với tinh thần và các cam kết của Hiệp định EVFTA nhằm đảm bảo sự ổn định của nền kinh tế quốc gia cũng như thương mại song phương. Về tính minh bạch trong quá trình thực thi, các cơ quan chức năng của Việt Nam cần truyền tải thông tin một cách công khai và rõ ràng, đặc biệt là đối với một chủ đề quan trọng liên quan đến công chúng và quyền riêng tư của công dân.

Việc đưa ra quá nhiều hạn chế có thể cản trở sự phát triển kinh tế của Việt Nam và từ đó khiến nền kinh tế trở nên kém hấp dẫn đối với nhà đầu tư, đặc biệt là vấn đề địa phương hóa dữ liệu nghiêm ngặt và các hướng dẫn tuân thủ chưa được rõ ràng.

2. Tác động đến nền kinh tế Việt Nam

Các yêu cầu lưu trữ dữ liệu tại Việt Nam sẽ gây xáo trộn và tốn kém cho tất cả các công ty Việt Nam sử dụng dịch vụ thanh toán, phương tiện truyền thông mạng xã hội, thanh toán điện tử, công nghệ thông minh, điện toán đám mây và quảng cáo toàn cầu khi phải lưu trữ dữ liệu tại Việt Nam, khi các dịch vụ từ các nhà cung cấp quốc tế cũng không được lưu trữ tại Việt Nam. Doanh nghiệp ở Việt Nam đang tận dụng CNTT-TT và các dịch vụ khác để hỗ trợ tốt hơn cho hoạt động kinh doanh và tham gia vào thương mại quốc tế.

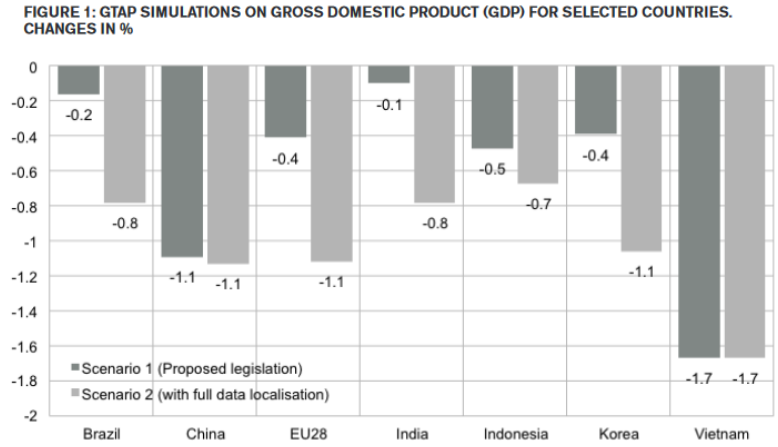
Ngoài ra, Việt Nam sẽ trở thành quốc gia duy nhất ở ASEAN có luật về cư trú dữ liệu trong nước mở rộng cho khu vực tư nhân[5]. Để duy trì khả năng cạnh tranh của Việt Nam trong khu vực và phù hợp với các thông lệ tốt nhất, Chính phủ nên áp dụng hệ thống phân loại dữ liệu, theo đó chỉ dữ liệu an ninh quốc gia thuộc khu vực công mới phải được lưu trữ ở Việt Nam. Trung Quốc thường được xem là quốc gia có chính sách lưu trữ dữ liệu trong nước thành công, nhưng phân tích này không giải thích được sự khác biệt trong nền kinh tế của Trung Quốc và Việt Nam. Trung Quốc có một thị trường trong nước khổng lồ của tầng lớp trung lưu và các tập đoàn nội địa hàng đầu quốc gia có thể cung cấp tất cả các dịch vụ kỹ thuật số trong nước. Ở giai đoạn phát triển hiện tại, Việt Nam dựa vào các dịch vụ kỹ thuật số do các công ty có quy mô toàn cầu cung cấp để thúc đẩy cuộc Cách mạng Công nghiệp lần thứ 4. Như vậy, Việt Nam sẽ được cung cấp những dịch vụ tốt hơn bằng cách hoạch định các chính sách kinh tế số theo mô hình của các quốc gia có cơ cấu kinh tế và trình độ phát triển tương tự Việt Nam.

4 Ví dụ, Điều 21 về phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng.

5 Indonesia, mốc so sánh trước đây, đã cho phép lưu trữ và xử lý phần lớn dữ liệu của khu vực tư nhân ở nước ngoài kể từ tháng 10 năm 2019.

Việt Nam có thể tăng 1% GDP trên mỗi 20% chi tiêu cho CNTT-TT, với Internet di động chiếm 6,2% GDP và 3,2% tổng số việc làm từ năm 2015 đến năm 2020. Chính phủ đã đặt mục tiêu chi tiêu hàng năm cho thương mại điện tử đạt 350 triệu USD, với doanh thu B2C tăng lên 10 tỷ USD và chiếm 5% tổng chi tiêu bán lẻ.

Biểu đồ 5: Ước tính của GTAP về tổng sản phẩm quốc nội của một số quốc gia



Đây là lý do tại sao một nghiên cứu trước đây của Trung tâm Kinh tế Chính trị Quốc tế Châu Âu cho thấy các chính sách bắt buộc lưu trữ dữ liệu tại Việt Nam sẽ làm giảm 1,7% tăng trưởng GDP của Việt Nam.

3. Tác động đến các Doanh nghiệp

Doanh nghiệp Việt Nam cạnh tranh trên quy mô toàn cầu, do đó cần có các nguồn lực công nghệ tiên tiến và bảo mật hàng đầu trong ngành để đảm bảo duy trì khả năng cạnh tranh với các công ty trong khu vực. Về bản chất, việc bắt buộc lưu trữ dữ liệu trong nước sẽ hạn chế khả năng của doanh nghiệp trong việc tiếp cận các công cụ cần thiết để giảm chi phí cho CNTT, đổi mới và nhanh chóng mở rộng quy mô.

Một báo cáo của Leviathan Security Group cho thấy các biện pháp lưu trữ dữ liệu trong nước làm tăng chi phí lưu trữ dữ liệu lên 30-60%. Điều này là bởi vì Internet cho phép lưu trữ và xử lý dữ liệu tập trung, mang lại hiệu quả kinh tế theo quy mô và tính nhất quán của mạng internet toàn cầu, từ đó giúp giảm chi phí.

Nhiều doanh nghiệp và công ty khởi nghiệp của Việt Nam đã và đang khai thác các dịch vụ CNTT-TT của nước ngoài để (1) nâng cao tính bảo mật, (2) đảm bảo kiểm soát chất lượng và (3) tiếp cận các dịch vụ sáng tạo nhất về phân tích dữ liệu, học máy và “Internet Vạn vật” (IoT). Nếu điều này không được tiếp tục, các công ty sẽ không thể phục vụ khách hàng hiệu quả. Các công ty có thể sẽ bị ảnh hưởng tiêu cực bởi yêu cầu lưu trữ dữ liệu trong nước gồm có:

- Các hãng hàng không của nhà nước và tư nhân
- Mạng truyền hình quốc gia
- Các công ty con về chăm sóc sức khỏe, CNTT-TT, lắp ráp xe hơi, thương mại điện tử của một số tập đoàn lớn tại Việt Nam;
- Các nhà sản xuất thiết bị chiếu sáng và điện
- Nhiều công ty khởi nghiệp, từ thanh toán đến trò chơi, ứng dụng truyền thông và xã hội

- Các doanh nghiệp nhà nước, doanh nghiệp tư nhân và được niêm yết của Việt Nam trong lĩnh vực tài chính, bán lẻ, bất động sản và truyền thông xã hội đang sử dụng các dịch vụ kế toán, hiệu suất và bảo mật dựa trên nền tảng điện toán đám mây
- Nhiều ngân hàng và công ty tài chính tiêu dùng đã được số hóa hoàn toàn hoặc đang trong giai đoạn số hóa các quy trình và dịch vụ của họ
- Các tập đoàn và tổ chức tài chính lớn nhất thuộc sở hữu của nhà nước và tư nhân sử dụng các dịch vụ ngân hàng toàn cầu của các tổ chức tài chính quốc tế.

Việc phân biệt giữa doanh nghiệp "trong nước" và "nước ngoài" có thể dẫn đến nhầm lẫn và gián đoạn đáng kể. Ví dụ, định nghĩa "doanh nghiệp trong nước" không nói rõ là có bao gồm công ty có vốn đầu tư trực tiếp nước ngoài (FDI) được đăng ký theo Luật Đầu tư của Việt Nam và được thành lập tại Việt Nam hay không (cả công ty 100% vốn nước ngoài và công ty có vốn nước ngoài chiếm đa số). Nếu có, tất cả các nhà cung cấp dịch vụ kỹ thuật số đó tại Việt Nam sẽ phải lưu trữ dữ liệu người dùng tại Việt Nam. Điều này hoàn toàn không phù hợp với mô hình kinh doanh của hầu hết các công ty đa quốc gia cung cấp dịch vụ kỹ thuật số. Ngay cả khi các công ty đa quốc gia sử dụng một số dịch vụ lưu trữ dữ liệu tại Việt Nam để giảm độ trễ cho khách hàng, thì đối với nhiều công ty trong số này, phần lớn quá trình xử lý dữ liệu và phân tích nâng cao đều diễn ra ở nước ngoài để đảm bảo đạt được hiệu quả chi phí và nắm được thông tin chuyên sâu về cải tiến dịch vụ thông qua tổng hợp dữ liệu. Vì vậy, vẫn chưa rõ làm thế nào để một công ty đa quốc gia cung cấp dịch vụ kỹ thuật số có thể tiếp tục hoạt động tại Việt Nam nếu yêu cầu lưu trữ dữ liệu này được thực hiện.

4. Tác động đến bảo mật

Chính phủ Việt Nam đặt ưu tiên trong việc bảo đảm an ninh quốc gia và bảo vệ công dân của mình. Tuy nhiên, các quy định lưu trữ dữ liệu trong nước sẽ không giúp cải thiện đáng kể về mức độ bảo mật. Bảo mật không liên quan đến vị trí thực tế của dữ liệu. Internet có quy mô toàn cầu, vì vậy bất kỳ hệ thống nào được kết nối với Internet, dù trực tiếp hay gián tiếp, đều dễ bị tấn công (nhất là các cuộc tấn công xuyên biên giới và xâm phạm dữ liệu).

Bảo mật về cơ bản là về (1) tính an toàn của cơ sở hạ tầng vật lý nơi dữ liệu được lưu trữ và (2) ai là người sở hữu và kiểm soát dữ liệu (và do đó có thể hỗ trợ việc thực thi pháp luật). Các công ty Việt Nam nên được phép lưu trữ và xử lý dữ liệu của mình tại các trung tâm dữ liệu an toàn nhất, được kiểm toán bởi các bên thứ ba độc lập theo các tiêu chuẩn quốc tế về bảo mật và quyền riêng tư. Chỉ các nhà cung cấp dịch vụ toàn cầu mới có thể cung cấp mức độ bảo mật cao nhất này.

Tiểu ban Kỹ thuật số tin rằng có thể đạt được mục tiêu cơ sở của Chính phủ về truy cập bảo mật/thực thi pháp luật mà không phải đặt ra các yêu cầu lưu trữ dữ liệu lên đối với các doanh nghiệp trong nước. Khi sử dụng các dịch vụ dữ liệu quốc tế, các doanh nghiệp trong nước có quyền kiểm soát thực tế đối với dữ liệu của mình cho dù dữ liệu được lưu trữ ở bất cứ nơi đâu và có thể truy xuất dữ liệu đó và/hoặc cung cấp quyền truy cập vào dữ liệu đó cho các cơ quan thực thi pháp luật của Việt Nam thực hiện thẩm quyền của mình. Điều này sẽ không bị cản trở bởi việc lưu trữ dữ liệu ở nước ngoài.

Lợi ích/quan ngại tiềm tàng đối với Việt Nam

Như đã phân tích, việc các quy định của Việt Nam có thể xung đột với các quy định của hệ thống pháp luật khác có thể gây khó khăn cho doanh nghiệp. Ví dụ, một doanh nghiệp Việt Nam thu thập và xử lý dữ liệu cá nhân của các chủ thể dữ liệu ở một quốc gia khác đang áp dụng các quy định nghiêm ngặt về bảo vệ dữ liệu (ví dụ: Quy định Chung về Bảo vệ Dữ liệu của Liên minh châu Âu–

EU GDPR) có thể rơi vào vị thế bất lợi khi các quốc gia này xử lý dữ liệu cá nhân của các chủ thể dữ liệu từ quốc gia khác. Việc tuân thủ các quy định của Việt Nam có thể được xem là không tương thích với các yêu cầu của Liên minh châu Âu được quy định trong GDPR.[6] Trong trường hợp cả luật Việt Nam và các luật khác được áp dụng để giải quyết một mâu thuẫn trong kinh doanh, các doanh nghiệp có thể lúng túng về luật áp dụng cho trường hợp của họ và gặp rủi ro không tuân thủ với quy định của một bên khi tuân thủ quy định của bên kia, cũng như rủi ro bị phạt số tiền lớn. Đây có thể là lý do để một công ty quyết định không phát triển kinh doanh tại Việt Nam. Vì vậy, việc bảo đảm tính thống nhất giữa quy định của Việt Nam và châu Âu theo Điều 45 của GDPR, phù hợp với quy định của Liên minh châu Âu trên cơ sở một quyết định đầy đủ. Đây sẽ là mục tiêu dài hạn mà Việt Nam cần đạt được với mốc thời gian và hành động cụ thể.

Khuyến nghị

Chúng tôi khuyến nghị như sau[7]:

- Bảo đảm tính thống nhất giữa quy định của Việt Nam và châu Âu theo Điều 45 của GDPR, phù hợp với quy định của Liên minh châu Âu trên cơ sở một quyết định đầy đủ, bao gồm mốc thời gian và hành động cụ thể.
- Thành lập Tổ chức điều phối để giải quyết các trường hợp mâu thuẫn với sự đồng thuận của Ủy ban Bảo vệ Dữ liệu Cá nhân, hoặc bất kỳ tổ chức nào có liên quan về phía Việt Nam, Ban Bảo vệ Dữ liệu Châu Âu và Ủy ban Châu Âu.
- Thiết lập một Cổng thông tin điện tử mà các công ty nước ngoài cũng có thể truy cập được bao gồm các hướng dẫn áp dụng, tài liệu đào tạo cho nhân viên, biểu mẫu cho các hồ sơ, tổ chức hỗ trợ tư vấn cơ bản, một diễn đàn và cung cấp danh sách các nhà tư vấn có thể hỗ trợ thực hiện các quy định của Việt Nam.
- Thiết lập một nhóm làm việc để hài hòa hóa quy định của EVFTA và các quy định của Việt Nam, giải quyết các xung đột pháp luật hiện tại.
- Phân loại xử lý dữ liệu và xây dựng hệ thống phân loại dữ liệu, theo đó chỉ những thông tin dữ liệu thuộc loại tối mật mới cần được yêu cầu lưu trữ ở trong nước, và những dữ liệu khác không thuộc bí mật quốc gia có thể được lưu trữ ở nước ngoài để giảm tác động kinh tế đối với nền kinh tế địa phương, đặc biệt là các công ty khởi nghiệp và các công ty có quy mô vừa và nhỏ là những đối tượng dễ bị tổn thương.
- Dỡ bỏ quy định yêu cầu doanh nghiệp trong nước phải lưu trữ dữ liệu trong nước nhằm cho phép xử lý dữ liệu xuyên biên giới với dữ liệu được lưu trữ ở nước ngoài, từ đó giúp các công ty Việt Nam giảm thiểu các chi phí cho hệ thống CNTT và đa quốc gia để duy trì mô hình kinh doanh của họ.
- Đảm bảo không có xung đột giữa các quy định của Luật An toàn thông tin mạng 2015 và Luật An ninh mạng 2018, và các Nghị định trong tương lai về bảo vệ dữ liệu cá nhân và an ninh mạng đang được soạn thảo.

6 Ví dụ, một đơn vị xử lý dữ liệu Việt Nam có thể bị yêu cầu chia sẻ dữ liệu cá nhân trong hệ thống của mình theo điều 21 Luật ANM. Trong khi đó, nếu dữ liệu này được bảo vệ bởi GDPR thông qua Điều khoản Hợp đồng Tiêu chuẩn thì sẽ có xung đột pháp luật.

7 Những khuyến nghị nêu trên được dựa trên những quy định tại Luật An toàn thông tin mạng (số 86/2015/QH13), trong đó bao gồm những quy định về nhiều nội dung liên quan tới an ninh mạng cho Chính phủ điện tử, cho Cloud và bảo đảm dữ liệu cá nhân.

II. CHÍNH PHỦ ĐIỆN TỬ

Cơ quan Chính phủ liên quan: Văn phòng Chính phủ (VPCP), Bộ Thông tin và Truyền thông (Bộ TT&TT)

Mô tả vấn đề

Chúng tôi hoan nghênh những tiến bộ ấn tượng của Chính phủ Việt Nam trong chương trình Chính phủ số vào năm 2020. Trong chặng đường xây dựng Chính phủ số, các Chính phủ số hàng đầu trên thế giới dựa vào tính linh hoạt, đổi mới và quy mô của điện toán đám mây để các công chức có những thông tin cần thiết để cung cấp các dịch vụ công được tốt nhất. Những người cung cấp dịch vụ trên tuyến đầu của các Chính phủ hiện đại phải đối mặt với những thử thách về mặt ngân sách. Không được phép lãng phí về hành chính, các Chính phủ ngày càng cần tiếp cận nhanh chóng với các công nghệ giúp đơn giản hóa các quy trình, giảm mạnh chi phí hành chính và cho phép đổi mới để tạo ra các dịch vụ công hiệu quả và nhanh chóng.

Để đạt được những tiến bộ hơn nữa, việc công nhận các chứng thư chữ ký điện tử được cấp cho các cá nhân là rất quan trọng. Nền tảng của thế giới số hóa là cung cấp các giải pháp điện tử thay thế cho chữ ký sống và nhận dạng Cá nhân. Việc điều chỉnh các quy chuẩn của Việt Nam cho phù hợp với các tiêu chuẩn trong Quy định về Định danh điện tử và các dịch vụ tin cậy[8] (eIDAS) sẽ là bước đầu tiên, thúc đẩy các quy định về tiêu chuẩn Chữ ký điện tử và cùng hướng tới một tiêu chuẩn toàn cầu.

Ngoài ra, các Chính phủ ban hành một báo cáo thường niên kèm theo một chỉ thị hành động - bao gồm thời gian cụ thể- tạo khuôn khổ cho việc triển khai công nghệ đám mây công cộng, làm rõ vai trò và trách nhiệm của các tổ chức chính phủ và Nhà cung cấp dịch vụ điện toán đám mây (CSPs) và đồng thời, thiết lập một cơ chế thuê dịch vụ được thiết kế với mục đích thu được toàn vẹn các lợi ích của công nghệ đám mây.

Các Chính phủ sử dụng các hệ thống tiêu chuẩn đã được quốc tế công nhận cho điện toán đám mây để đánh giá các CSPs (thay vì tạo các tiêu chuẩn chứng nhận riêng của từng nước) và tận dụng mô hình chia sẻ trách nhiệm trong bảo mật đám mây. Khi các khách hàng Chính phủ tận dụng chứng chỉ của bên thứ ba, họ sẽ không phải tuân theo các quy trình trùng lặp, thủ tục nặng nề hoặc các quy trình phê duyệt có thể không bắt buộc đối với môi trường đám mây. Việc sử dụng các hệ thống tiêu chuẩn được quốc tệ công nhận chung như vậy giúp các Chính phủ xây dựng một quy trình tuân thủ hiệu quả và nhanh chóng hơn.

Các Chính phủ phân loại dữ liệu dựa trên mức độ nhạy cảm và sau đó quản lý dữ liệu theo cách thức phù hợp với mức độ đó. Việc phân loại dữ liệu giúp các tổ chức đảm bảo các dữ liệu nhạy cảm hoặc quan trọng được bảo vệ ở mức độ thích hợp. Bất kể dữ liệu được xử lý hoặc lưu trữ trong các hệ thống máy chủ tại chỗ truyền thống hay trên đám mây, việc phân loại dữ liệu là cần thiết để duy trì tính bảo mật (và thậm chí là tính toàn vẹn và khả dụng) của dữ liệu dựa trên mức độ rủi ro. Các tổ chức tiêu chuẩn có uy tín như Tổ chức Tiêu chuẩn hóa Quốc tế (ISO) và Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) thuộc Bộ Thương mại Hoa Kỳ, đã đề xuất các phương án phân loại dữ liệu để có thể quản lý và bảo mật thông tin hiệu quả hơn theo mức độ rủi ro và tầm quan trọng của dữ liệu, khuyến cáo không nên sử dụng các phương thức xử lý cào bằng đối với tất cả dữ liệu.

Các Chính phủ thiết lập và/hoặc áp dụng các Chính sách bổ sung liên quan đến bảo mật, xử lý dữ liệu và quyền riêng tư nhằm hỗ trợ quá trình chuyển đổi thành công sang điện toán đám mây. Các Chính phủ giữ toàn quyền kiểm soát và sở hữu đối với dữ liệu, đồng thời có khả năng chọn (các) vị

8 Quy định về Định danh điện tử và các dịch vụ tin cậy ngày 23 tháng 07 năm 2014 của Liên minh châu Âu (eIDAS).

trí địa lý để lưu trữ dữ liệu. Các nhà cung cấp dịch vụ điện toán đám mây cũng cần cung cấp các biện pháp kiểm soát truy cập và nhận dạng để các cơ quan chính phủ chủ động hạn chế quyền truy cập vào cơ sở hạ tầng và dữ liệu. Trên đây là một số các khái niệm cơ bản quan trọng liên quan đến quyền sở hữu và quản lý dữ liệu trong mô hình trách nhiệm chung trên điện toán đám mây và tiếp sau đây là ba khái niệm khác[9]:

1. Các Chính phủ có thể tải về hoặc xóa dữ liệu của mình bất cứ khi nào.
2. Các Chính phủ có thể "xóa mã hóa" dữ liệu của họ bằng cách xóa các khóa mã hóa tổng cần thiết cho việc giải mã các khóa dữ liệu – công cụ đóng vai trò giải mã dữ liệu.
3. Các Chính phủ cần xem xét tính nhạy cảm của dữ liệu để quyết định có thực hiện mã hóa dữ liệu hay không và nếu có thì bằng phương thức nào khi dữ liệu đang được truyền đi và ở trạng thái nghỉ.
4. Các Chính phủ cần đảm bảo rằng các CSPs cung cấp tài liệu hướng dẫn chi tiết cách thức sử dụng dịch vụ điện toán đám mây, đáp ứng các yêu cầu cụ thể về tuân thủ và bảo vệ dữ liệu/quyền riêng tư theo các tiêu chuẩn quốc tế

Các yêu cầu về nơi lưu trữ dữ liệu trong nước không giúp cải thiện tình trạng bảo mật tổng thể của một tổ chức. Các Chính phủ cần đánh giá phương thức phân loại dữ liệu của mình và tập trung quyết định dữ liệu nào cần phải ở trong nước hoặc một khu vực nhất định và tại sao. Bằng cách này, các Chính phủ có thể nhận thấy các dữ liệu, ở dạng chính thức hay bí mật, có thể được lưu trữ và/hoặc sao chép ở nơi khác nếu không có yêu cầu cụ thể về địa lý hoặc pháp lý.

Khi công nghệ ngày càng phát triển và thay đổi các chiều hướng và điểm yếu đe dọa khách hàng, các Chính phủ buộc phải xem xét lại mô hình quản lý dữ liệu, chiến lược quyền riêng tư và khả năng chấp nhận rủi ro. Ba thực tế cơ bản sau đây đã phá vỡ mô hình quản lý dữ liệu máy chủ tại trò theo cách thức truyền thống trước đây:

1. Hầu hết các Mối đe doạ đều được Tiến hành Từ xa. Vị trí vật lý của dữ liệu hầu như không ảnh hưởng đến các mối đe dọa được lanh truyền trên mạng Internet.
2. Quy trình Thủ công Tiềm ẩn Sai sót do Con người gây ra. Sai sót do con người gây ra là một trong những nguyên nhân chính của hầu hết các lỗi an ninh mạng.
3. Các Mối đe doạ nghiêm trọng và phổ biết nhất xuất phát từ Nội bộ trong tổ chức. Phần lớn các vụ xâm phạm dữ liệu đã xảy ra do lỗi vô ý hoặc hành vi cố ý vi phạm của các tài khoản được cấp quyền truy cập.

Các vụ việc vi phạm không cần quá trình truy cập vật lý vào máy chủ mà thay vào đó lợi dụng tình trạng thiếu các biện pháp kiểm soát an ninh hiệu quả. Cơ chế tốt nhất để bảo vệ, phát hiện, xử lý và phục hồi là sử dụng các biện pháp bảo mật đột phá mà các nhà cung cấp dịch vụ điện toán đám mây cung cấp thông qua quá trình hiện đại hóa và tự động hóa.

Lợi ích/quan ngại tiềm tàng đối với Việt Nam

Trong những năm gần đây, các Chính phủ điện tử trên nền tảng điện toán đám mây trên thế giới đã bắt đầu áp dụng các chính sách khuyến khích các cơ quan thuộc chính phủ sử dụng dịch vụ điện toán đám mây công cộng. Nguyên nhân xuất phát từ thực tế các chính phủ đã nhận ra vai trò của điện toán đám mây trong việc tạo ra các dịch vụ công tốt hơn và tạo điều kiện cho quá trình cộng tác

9 Tài liệu tham khảo: European Regulation on Data Protection: https://gdpr.eu/, European Mechanism of Standard Contractual Clauses: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en, Singaporean Regulation on Data Protection : https://sso.agc.gov.sg/Act/PDPA2012, Singaporean Model Contractual Clause : https://www.aeilegal.com/tldr/asean%20data%20mgmt, UK Government Security Classifications: Government-Security-Classifications-Supplier-Briefing-Oct-2013.pdf (publishing.service.gov.uk), US National Security Classifications: The President Executive Order 13526 | National Archives, Phillippines' Cloud First Policy: DICT Releases Amended Cloud First Policy for Gov't Transition to "New Normal" | DICT.

và chia sẻ dữ liệu giữa các cơ quan thuộc chính phủ. Việc nâng cấp cơ sở hạ tầng có thể mang lại lợi ích cho các chính phủ và công dân của họ bằng cách khuyến khích sự đổi mới, tạo điều kiện cho quá trình hợp tác qua lại giữa các cơ quan và đẩy nhanh thời gian người dân tiếp cận được các dịch vụ công.

Khuyến nghị

Chúng tôi khuyến nghị như sau:

> Phát triển và áp dụng các chính sách đám mây thông minh để đẩy nhanh quá trình chuyển đổi số của họ. Chính phủ Việt Nam có thể xem xét một loạt các chính sách tối ưu nhằm hỗ trợ quá trình chuyển đổi sang một môi trường số hóa an toàn như sau:
>
> - Công nhận các chứng thư chữ ký điện tử được cấp cho các cá nhân
> - Thúc đẩy các chính sách ưu tiên dành cho nền tảng đám mây công cộng (Cloud First policy)
> - Công nhận, tuân thủ và bảo mật trên điện toán đám mây
> - Phân loại dữ liệu
> - Quyền riêng tư và Kiểm soát Dữ liệu
> - Lưu trữ dữ liệu trong nước
> - Thực hiện đánh giá rủi ro và các mối đe dọa (truy cập từ xa, các quy trình thủ công có nguy cơ do lỗi của con người và các mối đe dọa từ nội bộ)

LỜI CẢM ƠN

Tiểu ban Kỹ thuật số thuộc EuroCham.