Tạp chí Quản lý và Kinh tế quốc tế

Trang chủ: http://tapchi.ftu.edu.vn

BẢO VỆ DỮ LIỆU CÁ NHÂN XUYÊN BIÊN GIỚI: THỰC TIỄN VÀ KIẾN NGHỊ HOÀN THIỆN PHÁP LUẬT VIỆT NAM

Nguyễn Lan Phương[1]

Viện Nghiên cứu Chính sách và Phát triển Truyền thông, Hội Truyền thông số Việt Nam

Nguyễn Quang Đồng

Viện Nghiên cứu Chính sách và Phát triển Truyền thông, Hội Truyền thông số Việt Nam

Ngày nhận: 01/04/2022; **Ngày hoàn thành biên tập:** 30/08/2022; **Ngày duyệt đăng:** 06/09/2022

Tóm tắt: Dữ liệu cá nhân xuyên biên giới đã trở thành một vấn đề chính trị-pháp lý có ý nghĩa quan trọng trong xã hội số. Chính sách và pháp luật về bảo vệ loại dữ liệu này vừa phải đáp ứng mục tiêu an toàn thông tin, an ninh quốc gia vừa phải đảm bảo nhu cầu giao thương để phát triển kinh tế-xã hội, không nhu cầu nào triệt tiêu nhu cầu nào. Dựa trên phương pháp tổng hợp và so sánh, nhóm tác giả nghiên cứu thực trạng xây dựng pháp luật về bảo vệ dữ liệu cá nhân xuyên biên giới của các quốc gia, khu vực khác nhau trên thế giới gồm Liên minh Châu Âu (EU), Trung Quốc, Singapore và Việt Nam. Trên cơ sở đó, nhóm tác giả khuyến nghị hoàn thiện pháp luật về bảo vệ dữ liệu cá nhân xuyên biên giới của Việt Nam dựa trên trách nhiệm giải trình thay vì cách tiếp cận cấp phép như Dự thảo Nghị định quy định về bảo vệ dữ liệu cá nhân (bản công bố ngày 09/02/2021).

Từ khóa: Bảo vệ dữ liệu cá nhân, Bảo vệ dữ liệu cá nhân xuyên biên giới, Quyền riêng tư, Thương mại và kinh doanh quốc tế

CROSS-BORDER PERSONAL DATA PROTECTION: CURRENT SITUATION AND LEGAL RECOMMENDATIONS FOR VIETNAM

Abstract: Cross-border personal data have become a political-legal issue of great significance in digital society. Policies and laws on data protection need to meet on the one hand the goal of information security which is a part of national security, and the other hand the trading activities for socio-economic development. Applying the comparative method, we study the approaches of legislation and regulations in cross-border personal data protection in different countries/ regions around the world including the European Union (EU), China, Singapore and Vietnam. As a

[1] Tác giả liên hệ, Email: phuongnl@ips.org.vn

result, we recommend that the accountability approach is appropriate for Vietnam in cross-border personal data protection legislation instead of licensing like the Draft Decree on personal data protection (published on February 9, 2021).

Keywords: Personal Data Protection, Cross-Border Personal Data Protection, Privacy Rights, International Trade And Business

1. Đặt vấn đề

Ngày nay, khi các thông tin được số hóa dưới dạng dữ liệu thì dữ liệu cá nhân (DLCN) xuyên biên giới trở thành vấn đề chính trị - pháp lý có ý nghĩa quan trọng. Nó hoàn toàn có thể trở thành một vấn đề pháp lý về thương mại theo một cách khá đơn giản như một công ty đa quốc gia mở chi nhánh địa phương tại Việt Nam, nơi yêu cầu công ty nước ngoài duy trì một máy chủ lưu trữ trên lãnh thổ Việt Nam với dữ liệu của khách hàng Việt Nam. Hay phức tạp hơn là yêu cầu sửa đổi pháp luật trong nước để phù hợp với hiệp định thương mại tự do. Hiệp định Thương mại Tự do Hoa Kỳ-Hàn Quốc, tại chương 13 (Tài chính)-phụ lục 13-B, hai bên cam kết rằng "Bên này sẽ cho phép một tổ chức tài chính của Bên kia chuyển thông tin dưới dạng điện tử hoặc hình thức khác vào và ra lãnh thổ của mình để xử lý dữ liệu mà nơi xử lý đó là bắt buộc trong quá trình kinh doanh thông thường của tổ chức" (Office of the United States of Trade Representative, 2022). Mặc dù Hoa Kỳ đã cho phép các tổ chức dịch vụ tài chính thực hiện điều này từ trước nhưng Hàn Quốc yêu cầu tổ chức nêu trên phải đặt máy chủ dữ liệu ở Hàn Quốc và cấm chuyển dữ liệu ra bên ngoài lãnh thổ để xử lý. Tuy nhiên với thiện chí thực hiện cam kết quốc tế, năm 2020, Quốc hội Hàn Quốc đã thông qua Bản sửa đổi của Luật Bảo vệ thông tin cá nhân (Personal Information Protection Act), Luật Thông tin tín dụng (Credit Information Act) và Luật về Mạng (Network Act) vào tháng 01/2020 (có hiệu lực vào tháng 08/2020) cho phép chủ thể xử lý DLCN bao gồm cả tổ chức dịch vụ tài chính được chuyển dữ liệu ra bên ngoài lãnh thổ Hàn Quốc và kèm theo một số điều kiện nhất định (Romanosky & Acquisti, 2009; Garrie & cộng sự, 2010).

Có thể nói, vấn đề DLCN xuyên biên giới ảnh hưởng đến toàn bộ quá trình thực hiện các giao dịch kinh doanh quốc tế, nhất là các giao dịch trên môi trường số xuyên quốc gia hiện nay. Thực tế này cho phép các quốc gia thu nhận được các lợi ích kinh tế nhưng cũng phải đối mặt với nguy cơ bị xâm phạm dữ liệu. Do đó, bảo vệ DLCN xuyên biên giới đòi hỏi phải đáp ứng yêu cầu an toàn thông tin nhưng không nên triệt tiêu nhu cầu giao thương để phát triển kinh tế - xã hội. Với Việt Nam, một quốc gia nằm trong nhóm mười quốc gia có lượng trao đổi dữ liệu xuyên biên giới hàng đầu (Nikkei Asia, 2022), việc hoàn thiện những quy định pháp luật phù hợp điều chỉnh về bảo vệ DLCN xuyên biên giới là yêu cầu cấp thiết. Vậy Việt Nam cần hoàn thiện những quy định pháp luật về bảo vệ DLCN xuyên biên giới như thế nào? Việt Nam có thể học hỏi được kinh nghiệm gì từ một số quốc gia đi trước? Để tìm được câu trả lời cho những câu hỏi trên, bằng

những phương pháp nghiên cứu luật học truyền thống, bài viết sẽ tập trung làm rõ bối cảnh hợp tác kinh tế và những vấn đề pháp lý liên quan đến DLCN xuyên biên giới mà mỗi quốc gia cần lưu ý; kinh nghiệm của một số quốc gia về xây dựng khung pháp luật điều chỉnh việc bảo vệ DLCN xuyên biên giới; thực trạng khung pháp luật Việt Nam về bảo vệ DLCN xuyên biên giới; từ đó, đưa ra một số khuyến nghị đối với Việt Nam.

2. Bối cảnh hợp tác kinh tế và những vấn đề pháp lý của quốc gia về dữ liệu cá nhân xuyên biên giới

2.1 Bối cảnh hợp tác kinh tế liên quan đến dữ liệu cá nhân xuyên biên giới

Trong khuôn khổ Tổ chức Thương mại Thế giới (WTO), các cuộc thảo luận xoay quanh vấn đề DLCN xuyên biên giới đang diễn ra với tiến độ khá chậm, thì các hiệp định thương mại khu vực đề cập ngày càng nhiều về vấn đề dữ liệu xuyên biên giới. Cho đến nay, theo thống kê từ Tổ chức Hợp tác và Phát triển Kinh tế (OECD) có khoảng 25 thỏa thuận thương mại tự do (FTA) có chứa các điều khoản về dữ liệu xuyên biên giới như Hiệp định Đối tác Toàn diện và Tiến bộ xuyên Thái Bình Dương (CPTPP), FTA Hoa Kỳ-Mexico-Canada (USMCA), FTA Hoa Kỳ-Hàn Quốc, Hiệp định Kinh tế số Australia-Singapore… Các hiệp định thương mại này đều đặt ra nguyên tắc tự do chuyển dữ liệu xuyên biên giới, cho phép các bên duy trì các biện pháp đạt được các mục tiêu chính sách công nhưng phải đảm bảo các biện pháp minh bạch, không phân biệt đối xử, không hạn chế thương mại một cách không cần thiết. Các hiệp định cũng quy định rằng địa phương hóa dữ liệu (data localization) không được đặt ra như một điều kiện kinh doanh, đồng thời yêu cầu các bên thông qua một khuôn khổ để bảo vệ DLCN và thúc đẩy sự tương thích giữa cơ chế bảo vệ quyền riêng tư giữa các quốc gia.

Riêng với Việt Nam, một trong những quốc gia có nền kinh tế "mở" bậc nhất trên thế giới theo đánh giá của OECD, từ sau khi gia nhập WTO, Việt Nam liên tục ký kết các hiệp định thương mại tự do song phương, đa phương khác nhau, nổi bật gần đây như Hiệp định Đối tác Toàn diện và Tiến bộ xuyên Thái Bình Dương (CPTPP), Hiệp định Đối tác Kinh tế Toàn diện Khu vực (RCEP) và hướng tới hiệp định thương mại thế hệ mới-hiệp định kinh tế số (Digital Economic Agreement) với Singapore.

Có thể thấy rằng khi kinh tế số càng phát triển, xu hướng là hợp tác kinh tế gắn liền với hợp tác về dữ liệu. Cơ chế song phương, đa phương về thương mại tự do đi liền với đảm bảo dữ liệu xuyên biên giới là một dòng chảy tự do và an toàn.

2.2 Thực trạng chuyển dữ liệu cá nhân xuyên biên giới trên phạm vi quốc tế và tại Việt Nam

DLCN xuyên biên giới là một bộ phận của khối dữ liệu kinh doanh quốc tế. Vì vậy, thực trạng chuyển DLCN xuyên biên giới được phản ánh thông qua thực trạng chuyển dữ liệu qua biên giới nói chung.

Năm 2019, Nikkei Asia công bố thống kê về tình hình trao đổi dữ liệu qua biên giới trên thế giới (Nikkei Asia, 2022). Số liệu của Nikkei Asia được thu thập từ những nghiên cứu của Liên minh Viễn thông quốc tế (International Telecommunication Union - ITU) và TeleGeography - doanh nghiệp về phân tích và đánh giá dữ liệu có trụ sở ở Hoa Kỳ. Kết quả thống kế của Nikkei Asia cho thấy hai điểm đáng chú ý và ba xu hướng chính. Hai điểm đáng chú ý là châu Á trở thành châu lục năng động hàng đầu trên thế giới và Việt Nam được coi là quốc gia mới nổi về trao đổi dữ liệu xuyên biên giới. Ba xu hướng chính là:

Một là hoạt động trao đổi dữ liệu xuyên biên giới thể hiện ở lưu lượng dữ liệu tập trung nhiều hơn ở khu vực Châu Á - nơi có nhiều nền kinh tế đang phát triển thay vì khu vực phát triển Âu - Mỹ. Trong danh sách năm quốc gia đứng đầu về dòng dữ liệu được trao đổi xuyên biên giới năm 2019, có ba nước tại Châu Á (bao gồm: Trung Quốc, Ấn Độ, Singapore) và hai nước ở Châu Âu và Châu Mỹ (là Vương quốc Anh, Hoa Kỳ) thay vì chỉ có một quốc gia Châu Á (Nhật Bản) và 4 quốc gia Âu - Mỹ (Vương quốc Anh, Đức, Pháp, Hoa Kỳ) vào năm 2001. Đáng lưu ý là năm 2019 Trung Quốc thay thế Hoa Kỳ đứng vị trí thứ nhất về lượng dữ liệu xuyên biên giới (111 triệu Mbps). Lưu lượng này gấp 1,85 lần của Hoa Kỳ (được xếp thứ hai với 60 triệu Mbps) cũng như gấp 2,2 lần của Vương quốc Anh (được xếp ở vị trí thứ ba với 51,22 triệu Mbps). Với lưu lượng trao đổi gần 8 triệu Mbps, Việt Nam ở vị trí thứ bảy trong xếp hạng này.

Hai là sự phát triển không ngừng của trao đổi dữ liệu xuyên biên giới tập trung ở các quốc gia Châu Á. Trong giai đoạn 2001-2019, Việt Nam là quốc gia có mức độ tăng trưởng cao nhất với 230000 lần, gấp khoảng 30 lần so với quốc gia đứng đầu về lưu lượng luân chuyển dữ liệu là Trung Quốc với 7500 lần. Đứng thứ hai về tốc độ phát triển trao đổi dữ liệu xuyên biên giới là Ấn Độ với 22000 lần, xếp thứ ba là Singapore với 3000 lần.

Ba là điểm đến của dữ liệu xuyên biên giới tập trung ở khu vực Ấn Độ Dương - Thái Bình Dương thể hiện ở tỷ trọng dữ liệu được chuyển đến từng quốc gia. Tỷ trọng dữ liệu được chuyển từ một số quốc gia như Hoa Kỳ, Ấn Độ, Trung Quốc đến hai quốc gia ASEAN (Việt Nam và Singapore, do Nikkei xếp chung) trong năm 2019 đã gia tăng đáng kể so với 18 năm trước đó. Đồng thời, nếu vào năm 2001, Trung Quốc chủ yếu chuyển dữ liệu đến các nước phát triển thì đến năm 2019, Việt Nam và Singapore đã trở thành điểm đến có tỷ trọng dữ liệu từ quốc gia này lớn hơn so với phần được trao đổi với Nhật Bản hay Hoa Kỳ.

2.3 Những vấn đề pháp lý về dữ liệu cá nhân xuyên biên giới

Chuyển DLCN xuyên biên giới đặt ra nhiều thách thức cho từng quốc gia trong giai đoạn chuyển đổi số. Vì vậy, mỗi nước cần xem xét và ban hành những quy định phù hợp, đặc biệt tập trung vào bốn vấn đề quan trọng dưới đây.

Một là an toàn dữ liệu. Chuyển DLCN xuyên biên giới gia tăng tạo áp lực cho chính phủ các nước về kiểm soát và đảm bảo tính bảo mật của dữ liệu khi chúng không ở trong lãnh thổ quốc gia đó. Trong trường hợp hành vi xâm phạm và địa điểm xảy ra vi phạm nằm ngoài lãnh thổ quốc gia, cơ quan tài phán nào sẽ xét xử, pháp luật nào được áp dụng, nạn nhân được bù đắp như thế nào vẫn còn là câu hỏi. Ví dụ, vụ việc Cambrige Analytica (Meta, 2018), Facebook làm lộ dữ liệu của người dùng trong đó có hơn 400.000 người dùng ở Việt Nam. Dù giám đốc điều hành của hãng này là Mark Zuckerberg đã phải thực hiện điều trần ở Quốc hội Hoa Kỳ nhưng hãng này không có bất cứ hoạt động bồi thường nào cho nạn nhân ở Việt Nam.

Hai là bảo vệ quyền riêng tư. Chuyển DLCN xuyên biên giới yêu cầu phải bảo vệ được quyền riêng tư của cá nhân, chủ thể của dữ liệu được trao đổi, khi chúng được sử dụng ở một lãnh thổ khác. Vấn đề này được đặc biệt quan tâm khi mà quy định điều chỉnh việc bảo vệ quyền riêng tư trên lãnh thổ mà ở đó dữ liệu được sử dụng lại không phù hợp hoặc khác biệt, mâu thuẫn với quy định của quốc gia mà chúng được tạo ra và chuyển đi. Ví dụ, khu vực Liên minh Châu Âu (EU) đã ban hành đạo luật áp dụng trực tiếp trong EU về bảo vệ DLCN trong khi những đối tác thương mại của EU như Việt Nam hay Ấn Độ vẫn chưa quy định về quyền đối với DLCN, tiêu chuẩn an toàn của DLCN xuyên biên giới.

Ba là thực thi pháp luật quốc gia đối với chủ thể ở ngoài lãnh thổ quốc gia. DLCN xuyên biên giới đặt ra câu hỏi về khả năng thực thi pháp luật đối với chủ thể trong giao dịch mà chủ thể đó không tồn tại trong phạm vi lãnh thổ của quốc gia đó. Cơ quan nhà nước có thẩm quyền thanh tra, xử lý vi phạm, giải quyết các yêu cầu, tranh chấp về DLCN gặp khó khăn khi thực thi nhiệm vụ của mình trong trường hợp chủ thể nhận dữ liệu, chủ thể thu thập và lưu trữ dữ liệu không có hiện diện thương mại ở Việt Nam.

Bốn là cạnh tranh không lành mạnh. Các quốc gia có thể dựng nên những rào cản về mặt kỹ thuật (technical barriers) để ngăn cản khả năng tiếp cận thị trường trong nước của ngành công nghiệp dữ liệu nước ngoài, từ đó, tạo nên những điều kiện cạnh tranh bất bình đẳng, có lợi cho ngành công nghiệp trong nước. Chẳng hạn, hiện nay, một số nước thiết lập quy định về địa phương hóa dữ liệu để buộc doanh nghiệp có liên quan phải đặt các trung tâm dữ liệu trên lãnh thổ nước đó. Quy định của Trung Quốc hay Ấn Độ về vấn đề này thường được cho là nhằm mục đích thúc đẩy sự phát triển công nghệ thông tin ở trong nước hoặc nhằm đảm bảo an ninh, quốc phòng.

3. Kinh nghiệm quốc tế về thiết lập khung pháp luật điều chỉnh việc bảo vệ dữ liệu cá nhân xuyên biên giới

3.1 Một số cách tiếp cận khi thiết lập khung pháp luật

Nghiên cứu của Casalini & Gonzalez (2019) cho thấy trên thế giới có năm cách tiếp cận đối với việc thiết lập khung pháp luật về bảo vệ DLCN xuyên biên giới.

Thứ nhất, không điều chỉnh về trao đổi DLCN xuyên biên giới (no regulations). Cách tiếp cận này thường thể hiện ở dạng không có văn bản pháp lý nào về bảo vệ DLCN hoặc có văn bản pháp lý về bảo vệ DLCN nhưng không quy định về vấn đề này. Việc không có văn bản pháp lý và không quy định có thể được diễn giải theo nguyên tắc "không cấm", nghĩa là trao đổi DLCN xuyên biên giới có thể được thực hiện không có giới hạn. Tuy nhiên, điều này có thể tác động bất lợi đến việc quốc gia đó: i) trở thành thành viên của một điều ước quốc tế hoặc một thiết chế đa phương, khu vực có liên quan và ii) xử lý tình trạng xâm phạm DLCN xảy ra do chủ thể nước ngoài nhận DLCN.

Thứ hai, tập trung điều chỉnh trách nhiệm giải trình của chủ thể thực hiện việc trao đổi DLCN xuyên biên giới (ex-post accountability). Cách tiếp cận này thường thể hiện ở dạng quy định cho phép chủ thể trao đổi DLCN thực hiện giao dịch đó dựa trên các bước đánh giá an toàn thích hợp và phải chịu trách nhiệm giải trình nếu có hành vi xâm phạm xảy ra. Pháp luật không đưa ra trước các điều kiện về an toàn hoặc cấp phép. Cách tiếp cận này thường được biết đến rộng rãi với cách gọi "hậu kiểm" ở Việt Nam.

Thứ ba, thiết lập trước các điều kiện về an toàn đối với hành vi trao đổi DLCN qua biên giới (flows conditional on safeguards). Cách tiếp cận này thể hiện ở dạng có quy định các điều kiện pháp lý mà chủ thể chuyển DLCN phải tuân thủ hoặc chấp hành như: danh sách quốc gia an toàn, điều khoản mẫu, chính sách bảo vệ DLCN được thẩm định và đánh giá bởi cơ quan nhà nước có thẩm quyền…

Thứ tư, cấp phép cho từng giao dịch trao đổi DLCN qua biên giới (flows conditional on ad-hoc authorisation). Cách tiếp cận này thể hiện ở quy định chủ thể chuyển DLCN xuyên biên giới phải thực hiện thủ tục cấp phép tại cơ quan nhà nước có thẩm quyền trước khi chuyển DLCN xuyên biên giới cho từng giao dịch cụ thể.

Thứ năm, cấm trao đổi DLCN xuyên biên giới. Cách tiếp cận cứng rắn này thể hiện ở yêu cầu bắt buộc về lưu trữ, xử lý DLCN tại quốc gia mà dữ liệu được thu thập mà không được chuyển dữ liệu đó ra khỏi lãnh thổ.

3.2 Một số cách tiếp cận về yêu cầu địa phương hóa dữ liệu

Hiện nay chưa có định nghĩa thống nhất về địa phương hóa dữ liệu. Khái niệm này có thể được hiểu là chỉ bắt buộc lưu trữ DLCN tại quốc gia mà dữ liệu được thu thập hoặc phải lưu trữ và xử lý DLCN tại quốc gia đó. Hiện tại, có thể thấy tồn tại bốn cách tiếp cận đối với vấn đề này. *Thứ nhất,* không yêu cầu về địa phương hóa dữ liệu nghĩa là không có quy định về lưu trữ dữ liệu tại địa phương mà DLCN được thu thập hoặc chỉ có yêu cầu về lưu trữ dữ liệu tại địa phương trong một số lĩnh vực nhạy cảm như tài chính, chăm sóc sức khỏe. *Thứ hai,* yêu cầu DLCN phải được lưu trữ một bản sao tại địa phương mà dữ liệu đó được thu thập trước khi chúng được chuyển để xử lý hay lưu trữ ở nước ngoài. Yêu cầu này không nhằm hạn chế trao đổi dữ liệu xuyên biên giới nhưng làm tăng chi phí tuân thủ. Nó có tác dụng chính là đảm bảo khả năng truy

cập của cơ quan nhà nước có thẩm quyền của quốc gia mà dữ liệu được thu thập. *Thứ ba,* yêu cầu lưu trữ dữ liệu tại địa phương mà chúng được thu thập với ngoại lệ là cho phép xử lý dữ liệu đó tại nước ngoài. Yêu cầu này không được coi là một rào cản đối với trao đổi dữ liệu xuyên biên giới nhưng làm tăng chi phí tuân thủ. *Thứ tư,* quy định lưu trữ dữ liệu tại địa phương mà DLCN được thu thập kèm với các điều kiện khác trước khi chuyển dữ liệu ra nước ngoài hoặc xử lý dữ liệu ở nước ngoài. Quy định hạn chế chòng chảy dữ liệu xuyên quốc gia, làm tăng chi phí tuân thủ.

Như vậy, ở hai phần trên, một số cách tiếp cận đã được trình bày và phân tích để cho thấy sự đa dạng trong cách thức mà một quốc gia có thể lựa chọn để thiết lập khung pháp lý liên quan đến DLCN xuyên biên giới cũng như về yêu cầu địa phương hóa dữ liệu. Phần tiếp theo sẽ phân tích rõ hơn việc sử dụng những cách tiếp này bởi một số quốc gia trên thế giới.

3.3 Kinh nghiệm của một số quốc gia, khu vực

3.3.1 Kinh nghiệm của Singapore

Tại Singapore, văn bản quy định bảo vệ DLCN xuyên biên giới là Personal Data Protection Act/PDPA (Luật Bảo vệ DLCN năm 2012, sửa đổi, bổ sung năm 2020) (Singapore Statutes Online, 2020; Greenleaf, 2012). Luật này có đối tượng áp dụng là cá nhân, doanh nghiệp, hiệp hội thực hiện thu thập, sử dụng DLCN ở Singapore, không áp dụng cho cơ quan nhà nước, nhân viên công ty, cá nhân thực hiện hành vi vì mục đích cá nhân, gia đình của người đó (mở tài khoản chung giữa các thành viên, cha mẹ mua bảo hiểm nhân thọ cho con cái).

Khung pháp luật của Singapore về vấn đề này được xây dựng dựa trên các tiếp cận trách nhiệm giải trình như sau: chủ thể PDPA phải tiến hành các bước đảm bảo chủ thể nhận DLCN phải bảo vệ DLCN theo tiêu chuẩn tương đương với quy định trong PDPA (Nguyễn, 2019).

Cụ thể, điều kiện để thực hiện trao đổi DLCN xuyên biên giới yêu cầu chủ thể PDPA phải tiến hành các bước thích hợp (appropriate steps) để đảm bảo rằng bên nhận DLCN cung cấp tiêu chuẩn bảo vệ tương đương với mức độ được thiết lập trong PDPA. Chủ thể PDPA thực hiện các bước kiểm tra thích hợp để đảm bảo ràng bên nhận DLCN bị ràng buộc bởi những nghĩa vụ pháp lý (legally enforcement obligations) hoặc những chứng nhận cụ thể (specified certifications) mà cung cấp tiêu chuẩn bảo vệ DLCN tương đương với quy định thuộc PDPA. Trong đó, những nghĩa vụ pháp lý được ấn định cho tổ chức nhận DLCN có thể theo văn bản pháp lý, hợp đồng (khuyến khích sử dụng hợp đồng mẫu trong ASEAN), chính sách nội bộ về bảo vệ dữ liệu đó (binding corporate rules) hoặc bất kì công cụ pháp lý nào khác.

Ngoài ra, có năm ngoại lệ cho phép chủ thể PDPA thực hiện chuyển DLCN ra nước ngoài mà không phải đáp ứng điều kiện trên. *Thứ nhất,* chủ thể DLCN đồng ý về việc chuyển DLCN qua biên giới sau khi được thông báo DLCN của mình được

bảo vệ ở nơi được chuyển đến. *Thứ hai,* chủ thể DLCN được cho là đồng ý về việc chuyển DLCN nếu việc này nhằm thực hiện hợp đồng giữa chủ thể này với tổ chức chuyển DLCN. *Thứ ba,* chuyển DLCN là cần thiết vì lợi ích của cá nhân hoặc lợi ích quốc gia và chủ thể chuyển DLCN đảm bảo rằng DLCN không bị xâm phạm bởi bên nhận DLCN. *Thứ tư,* DLCN là loại dữ liệu quá cảnh (data in transit); *Thứ năm,* DLCN có sẵn và có thể được công khai (publicly available) ở Singapore.

3.3.2 Kinh nghiệm của Liên minh Châu Âu

Tại Liên minh Châu Âu (EU), văn bản quy định về bảo vệ DLCN xuyên biên giới là Regulation (EU) 2016/679 of the European Parliament and of the Council - General Data Protection Regulation/GDPR (Quy định số 2016/679 về bảo vệ DLCN) (The European Parliament and the Council, 2016; Allen & cộng sự, 2019; Ciriani, 2015). Quy định này áp dụng với ba dạng chủ thể gồm: chủ thể (cá nhân, pháp nhân, tổ chức) EU thực hiện hành vi kiểm soát, xử lí DLCN; chủ thể ngoài EU thực hiện hành vi kiểm soát, xử lí dữ liệu của cá nhân ở EU; chủ thể không ở EU nhưng là cơ quan ngoại giao của quốc gia thành viên EU ở nước ngoài, tàu bay, tàu biển hoạt động ngoài EU nhưng có quốc tịch của quốc gia thành viên EU.

Khung pháp luật có liên quan của EU được xây dựng dựa trên cách tiếp cận sử dụng điều kiện an toàn "cho trước" khi trao đổi DLCN xuyên biên giới, đảm bảo quy định bảo vệ dữ liệu được thực hiện dù dữ liệu được chuyển đến đâu.

Cụ thể, điều kiện để thực hiện việc trao đổi này được áp dụng theo thứ tự ưu tiên. *Thứ nhất,* chủ thể GDPR chuyển DLCN đến nơi nằm trong Quyết định của Ủy ban Châu Âu về quốc gia thứ ba có khả năng bảo vệ tương thích với EU (hiện nay đã có 12 quốc gia thuộc nhóm này, là: Andorra, Argentina, Canada (những tổ chức thương mại), Quần đảo Faroe, Guernsey, Israel, Đảo Man, Nhật Bản, Jersey, New Zealand, Thụy Sỹ và Uruguay, Anh Quốc (European Commission, 2017). *Thứ hai*, chủ thể GDPR cung cấp biện pháp bảo vệ cá nhân thích hợp (Appropriate Safeguards) gồm: (i) Đối với cơ quan, tổ chức công là thỏa thuận song phương hoặc đa phương có tính chất ràng buộc phát lý về bảo vệ DLCN đảm bảo tuân thủ GDPR; (ii) Đối với công ty đa quốc gia được thành lập ở EU phải ban hành chính sách bảo vệ DLCN được gọi là Quy định kinh doanh ràng buộc (Binding Corporate Rules) được phê chuẩn bởi Cơ quan giám sát về DLCN của quốc gia thành viên; (iii) Chủ thể GDPR ký kết hợp đồng với chủ thể nhận dữ liệu có sử dụng điều khoản bảo vệ mẫu DLCN (Standard Data Protection Clause) được thông qua bởi Ủy ban châu Âu; (iv) Chủ thể GDPR xây dựng và sử dụng bộ quy tắc ứng xử hoặc thủ tục chứng nhận được phê chuẩn bởi Cơ quan giám sát về DLCN của quốc gia thành viên kèm với nghĩa vụ và ràng buộc từ chủ thể nhận dữ liệu ở nước ngoài (Trần, 2021).

Ngoài ra, có năm ngoại lệ cho phép các chủ thể có liên quan chuyển dữ liệu ra khỏi lãnh thổ các nước thành viên EU mà không phải đáp ứng các điều kiện an toàn như trên gồm: có sự đồng ý minh thị từ chủ thể DLCN sau khi được cung cấp toàn

bộ thông tin cần thiết về rủi ro có thể xảy ra khi thực hiện trao đổi DLCN xuyên biên giới; vì lợi ích cộng đồng; để thiết lập, thực hiện, bảo vệ quyền yêu cầu theo luật; bảo vệ lợi ích quan trọng của chủ thể DLCN hoặc của những người khác, khi chủ thể DLCN không có khả năng về mặt thể chất hoặc pháp lý để đưa ra sự đồng ý; và trao đổi DLCN nhằm cung cấp thông tin/tham vấn cộng đồng hoặc người có quyền lợi hợp pháp liên quan với những điều kiện trong từng trường hợp cụ thể.

3.3.3 Kinh nghiệm của Trung Quốc

Tại Trung Quốc, các văn bản quy định về bảo vệ DLCN xuyên biên giới ở Trung Quốc gồm Cyber Security Law/CSL 2016 (Luật An ninh mạng năm 2016), Data Security Law/DSL 2021 (Luật An ninh dữ liệu năm 2021) và Personal Information Protection Law/PIPL 2021 (Luật Bảo vệ thông tin cá nhân) (The National People's Congress of the People's Republic of China, 2021). Trong đó, CSL 2016 đóng vai trò nền tảng cho các yêu cầu về bảo vệ DLCN xuyên biên giới và địa phương hóa dữ liệu. DSL 2021 quy định các tiêu chuẩn cụ thể đối với việc chuyển dữ liệu quan trọng ra khỏi lãnh thổ Trung Quốc và các quy tắc phê duyệt đối với việc cung cấp dữ liệu do các cơ quan tư pháp và thực thi pháp luật của nước ngoài yêu cầu. PIPL 2021 là luật chuyên ngành về bảo vệ thông tin cá nhân và đưa ra các yêu cầu cụ thể đối với chủ thể xử lý thông tin cá nhân khi họ chuyển thông tin cá nhân ra khỏi lãnh thổ Trung Quốc (Pernot-Leplay, 2020).

PIPL (The National People's Congress of the People's Republic of China, 2021) có phạm vi áp dụng bao trùm lên việc xử lý DLCN trong lãnh thổ Trung Quốc. Ngoài ra, Luật này cũng điều chỉnh các hoạt động xử lý thông tin cá nhân được thực hiện bên ngoài lãnh thổ Trung Quốc trong ba trường hợp: cung cấp các sản phẩm hoặc dịch vụ cho cá nhân ở Trung Quốc; phân tích và đánh giá các hoạt động của cá nhân ở Trung Quốc; và các trường hợp khác do pháp luật quy định.

Khung pháp luật về bảo vệ DLCN xuyên biên giới ở Trung Quốc được thiết lập trên cơ sở kết hợp cách tiếp cận trách nhiệm giải trình của chủ thể chuyển DLCN với cách tiếp cận điều kiện an toàn "cho trước" và cấp phép từng trường hợp cụ thể. Chủ thể PIPL phải thực hiện các biện pháp cần thiết để đảm bảo hoạt động xử lý DLCN do bên nhận nước ngoài thực hiện đáp ứng tiêu chuẩn bảo vệ thông tin cá nhân theo quy định của PIPL. Đồng thời chủ thể PIPL phải sử dụng hợp đồng mẫu do CAC công bố, chứng nhận bảo mật dữ liệu và vượt qua đánh giá an toàn thông tin của CAC trước khi thực hiện trao đổi dữ liệu xuyên biên giới.

Cụ thể, Điều 38 PIPL quy định chủ thể PIPL chỉ được chuyển thông tin cá nhân ra khỏi lãnh thổ Trung Quốc khi: (i) Được sự đồng ý của chủ thể thông tin cá nhân; (ii) Thực hiện thông báo cho họ về thông tin của chủ thể nhận ở nước ngoài, phương tiện xử lý dữ liệu, cách thức và thủ tục mà họ có thể thực thi quyền; (iii) Đáp ứng đầy đủ bốn điều kiện (đánh giá an toàn thông tin của CAC; chứng nhận bảo mật dữ liệu của một cơ quan chuyên môn được CAC công nhận; ký kết thỏa thuận với chủ

thể nhận DLCN ở nước ngoài với các điều khoản về quyền và nghĩa vụ của các bên dựa trên hợp đồng mẫu do CAC ban hành; và các điều kiện khác do pháp luật quy định, hoặc trong các quy tắc do CAC ban hành). Điều 40 PIPL quy định chủ thể vận hành cơ sở hạ tầng thông tin quan trọng và chủ thể xử lý thông tin cá nhân mà theo đó số lượng thông tin cá nhân được xử lý đạt đến ngưỡng do CAC quy định, sẽ lưu trữ thông tin cá nhân được thu thập và tạo ra tại Trung Quốc trong lãnh thổ Trung Quốc. Trong trường hợp cần chuyển thông tin cá nhân ra nước ngoài, chủ thể đó phải vượt qua đánh giá an toàn thông tin do CAC thực hiện, trừ trường hợp các luật, quy định hoặc quy tắc khác do CAC quy định miễn đánh giá an toàn thông tin thì quy định đó sẽ được thực hiện. Ngoài ra, trong trường hợp các hiệp ước và hiệp định quốc tế mà Trung Quốc đã ký kết hoặc tham gia có quy định về yêu cầu chuyển thông tin cá nhân ra khỏi lãnh thổ, thì những yêu cầu đó sẽ được tuân thủ.

Về yêu cầu địa phương hóa dữ liệu, nguyên tắc là lưu trữ dữ liệu gốc tại lãnh thổ Trung Quốc áp dụng với nhà khai thác cơ sở hạ tầng quan trọng (Critical Information Infrastructure Operator/CIIO), trường hợp ngoại lệ chuyển dữ liệu ra nước ngoài thì chủ thể thực hiện hành vi đó phải vượt qua đánh giá an toàn thông tin của CAC (và chỉ nên chuyển bản sao dữ liệu). Điều 37 CSL quy định "các nhà khai thác cơ sở hạ tầng thông tin quan trọng thu thập hoặc xử lý DLCN hoặc dữ liệu quan trọng khi hoạt động trên lãnh thổ của Trung Quốc, sẽ lưu trữ dữ liệu đó trong lãnh thổ Trung Quốc. Trong trường hợp do yêu cầu kinh doanh thực sự cần thiết phải chuyển thông tin đó ra khỏi lãnh thổ, họ sẽ tuân theo các biện pháp do Cục an ninh mạng và thông tin của Nhà nước và các cơ quan liên quan của Quốc vụ viện cùng xây dựng để tiến hành đánh giá an ninh; nếu có các quy định pháp luật khác thì thực hiện theo các quy định đó" (Cyberspace Administration of China, 2016). Một số ngành, lĩnh vực cụ thể ở Trung Quốc có yêu cầu riêng về địa phương hóa dữ liệu theo đặc thù của ngành đó như ngành tài chính, điều tra tín dụng (Yang, 2020) yêu cầu thông tin cá nhân được thu thập ở Trung Quốc sẽ được lưu trữ, xử lý hoặc phân tích tại Trung Quốc, ngoại trừ khi pháp luật có quy định khác. Riêng đối với dữ liệu được xếp vào nhóm bí mật nhà nước, bản đồ của Trung Quốc, sức khỏe dân số và thông tin di truyền của công dân Trung Quốc chỉ được lưu trữ tại lãnh thổ Trung Quốc (Zhang, 2020).

4. Thực trạng khung pháp luật của Việt Nam liên quan đến bảo vệ dữ liệu cá nhân xuyên biên giới

4.1 Cách tiếp cận và xu hướng thay đổi cách tiếp cận của Việt Nam

Có thể thấy Việt Nam chưa ban hành văn bản quy phạm pháp luật nào về bảo vệ DLCN nói chung, quy định về bảo vệ DLCN xuyên biên giới nói riêng (Lê, 2009; Nguyễn, 2017; Ngô, 2019; Nguyễn, 2021). Dự thảo Nghị định về Bảo vệ DLCN (Dự thảo nghị định) do Bộ Công an chủ trì đang ở giai đoạn thẩm định. Nhìn từ dự thảo, có thể thấy sự thay đổi trong cách tiếp cận của Việt Nam về vấn đề này, từ cách tiếp cận không quy định sang cách tiếp cận cấp phép. Dự thảo nghị định nêu rõ điều

kiện bắt buộc để chuyển DLCN qua biên giới là chủ thể chuyển DLCN phải gửi hồ sơ đăng kí chuyển dữ liệu đó tới Ủy ban bảo vệ DLCN và phải được sự chấp thuận của cơ quan này. Tuy nhiên, Dự thảo chưa làm rõ việc cấp phép này chỉ cần thực hiện một lần hay phải thực hiện nhiều lần cho mỗi vụ việc cụ thể.

Về yêu cầu địa phương hóa dữ liệu, cách tiếp cận cũng có có sự thay đổi từ yêu cầu cho từng lĩnh vực cụ thể thành quy định chung và nêu rõ các điều kiện phải đáp ứng trước khi dữ liệu được chuyển ra khỏi Việt Nam.

Trước năm 2018, Việt Nam không quy định chung về lưu trữ DLCN tại Việt Nam mà chỉ quy định theo lĩnh vực cụ thể là trò chơi điện tử, mạng xã hội tại Điều 25 khoản 8 và Điều 32 khoản 2 Nghị định số 72/2013/NĐ-CP của Chính phủ ngày 15/7/2013 về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng.

Năm 2018, với Luật An ninh mạng, Việt Nam đưa ra yêu cầu chung về địa phương hóa dữ liệu dành cho chủ thể là doanh nghiệp. Quy định này yêu cầu doanh nghiệp thực hiện hành vi thu thập DLCN của người dùng tại Việt Nam phải lưu trữ dữ liệu này tại Việt Nam (Điều 26 khoản 3).

Sau đó, theo Dự thảo nghị định, yêu cầu địa phương hóa dữ liệu được mở rộng về đối tượng áp dụng, gồm doanh nghiệp và cá nhân, tổ chức trong và ngoài nước tiến hành thu thập DLCN của người dùng tại Việt Nam. Thêm vào đó, đây trở thành một điều kiện bắt buộc trước khi chuyển DLCN qua biên giới.

4.2 Tác động của cách xây dựng quy định bảo vệ dữ liệu cá nhân xuyên biên giới và yêu cầu hoàn thiện pháp luật bảo vệ dữ liệu cá nhân xuyên biên giới tại Việt Nam

Xem xét sự thay đổi trong cách tiếp cận của Việt Nam về vấn đề này, có thể nhận thấy cách thức quản lý hoạt động trao đổi DLCN xuyên biên giới có thể tạo ra một số tác động như sau:

Thứ nhất, yêu cầu địa phương hóa dữ liệu được thiết lập theo hướng đặt điều kiện lưu trữ một bản gốc tại Việt Nam cùng các điều kiện khác trước khi được chuyển ra khỏi Việt Nam chỉ đảm bảo quyền truy cập của cơ quan quản lý nhà nước vào cơ sở dữ liệu trong trường hợp thực hiện nghĩa vụ theo luật định mà không thể tránh khỏi các hành vi xâm hại dữ liệu từ bên ngoài cũng như không hoàn toàn đảm bảo quyền riêng tư. Thêm vào đó, yêu cầu này buộc chủ thể trong và ngoài nước phải sử dụng dịch vụ lưu trữ của nhà cung cấp có trung tâm dữ liệu vật lí tại Việt Nam và thường là nhà cung cấp của Việt Nam, dẫn đến có khả năng đáp ứng mục đích khuyến khích ngành công nghiệp viễn thông, công nghệ thông tin trong nước nhưng làm giảm khả năng thu hút đầu tư và cạnh tranh lành mạnh trong môi trường hội nhập quốc tế, đồng thời cũng không phù hợp với nghĩa vụ quốc tế trong các hiệp định mà Việt Nam là thành viên. Chẳng hạn, Điều 14.13 CPTPP đòi hỏi mỗi quốc gia thành viên không được coi yêu cầu địa phương hóa dữ liệu là một điều kiện kinh

doanh, không áp dụng yêu cầu này hơn mức cần thiết, không sử dụng yêu cầu này để cản trở hoạt động thương mại.

Thứ hai, khung pháp luật về trao đổi DLCN qua biên giới được xây dựng theo hướng cấp phép làm phát sinh thêm thủ tục hành chính không thực sự cần thiết trong mọi trường hợp. Ví dụ, yêu cầu bên chuyển DLCN của công dân Việt Nam phải đăng kí chuyển DLCN với Ủy ban bảo vệ DLCN và được trả kết quả trong vòng 20 ngày, áp dụng với mọi loại dữ liệu trong khi DLCN cơ bản có mức độ đe dọa rủi ro thấp hơn so với DLCN nhạy cảm.

5. Khuyến nghị xây dựng quy định pháp luật bảo vệ dữ liệu cá nhân xuyên biên giới tại Việt Nam

Với địa vị là một trong mười quốc gia có lưu lượng trao đổi dữ liệu xuyên biên giới lớn nhất thế giới và trong bối cảnh kết nối kinh tế ngày càng sâu rộng, Việt Nam cần có khung pháp luật về bảo vệ DLCN xuyên biên giới linh hoạt hơn để tận dụng lợi thế của mình.

Thứ nhất, Việt Nam nên xem xét sử dụng cách tiếp cận trách nhiệm giải trình đối với chủ thể chuyển DLCN ra khỏi lãnh thổ Việt Nam thông qua học tập kinh nghiệm lập pháp của Singapore và áp dụng biện pháp cấp phép trong trường hợp đặc biệt (ví dụ, đối với dữ liệu dân số sức khỏe, tài chính của công dân). Ưu điểm của cách tiếp cận này giải quyết được ba vấn đề pháp lý (đã được đề cập ở mục 2.3) là an toàn dữ liệu, bảo vệ quyền riêng tư của người dùng và thực thi pháp luật quốc gia. Nó đồng thời cũng cho phép loại bỏ rào cản về dữ liệu đối với hoạt động thương mại. Ưu điểm của cách tiếp cận này đối với Việt Nam là: đòi hỏi chủ thể chuyển dữ liệu phải thực hiện các bước đánh giá hợp lý về mức độ an toàn và rủi ro trước khi chuyển DLCN qua biên giới; và cho phép họ có khả năng lựa chọn các biện pháp bảo vệ DLCN xuyên biên giới phù hợp với đặc điểm của họ.

Các biện pháp này chủ yếu đánh giá khả năng bảo vệ DLCN của chủ thể nhận DLCN thông qua nghĩa vụ mà họ phải tuân thủ. Nghĩa vụ này có thể được quy định trong văn bản quy phạm pháp luật của quốc gia của họ, hợp đồng giữa họ với chủ thể chuyển DLCN (có thể khuyến khích sử dụng hợp đồng mẫu do cơ quan có thẩm quyền của Việt Nam ban hành), một số cơ chế chứng nhận quốc tế hoặc chính sách bảo mật nội bộ có tính chất bắt buộc.

Thứ hai, về yêu cầu địa phương hóa dữ liệu, Việt Nam không nên quy định lưu trữ dữ liệu tại Việt Nam thông qua học tập kinh nghiệm lập pháp của Singapore. Quy định này là không tạo ra rào cản với dữ liệu xuyên biên giới đồng nghĩa giảm rào cản hợp tác kinh tế. Ngược lại nếu Việt Nam áp dụng quy định chung về địa phương hóa dữ liệu như một điều kiện trong hoạt động kinh doanh theo kinh nghiệm của Trung Quốc thì không phù hợp đặc điểm riêng của đất nước (vị trí địa lý, quy mô dân số và tình hình hợp tác kinh tế).

Thứ ba, cần thúc đẩy các hoạt động hợp tác quốc tế về bảo vệ DLCN xuyên biên giới thông qua việc tham gia các thiết chế đa phương hoặc khu vực về chuyển DLCN xuyên biên giới. Điều này góp phần giải quyết ba vấn đề pháp lý đáng lo ngại do dữ liệu xuyên biên giới tạo ra (đã được đề cập ở mục 2.3) là an toàn dữ liệu, bảo vệ quyền riêng tư của người dùng và thực thi pháp luật quốc gia. Các thiết chế mà Việt Nam cần tham gia như APEC Cross-Border Privacy Rule, các hiệp định hợp tác kinh tế số chứa đựng các quy định về bảo vệ dữ liệu xuyên biên giới. Tuy nhiên, để có thể tham gia vào các khuôn khổ đa phương về bảo vệ DLCN xuyên biên giới, Việt Nam cần phải có quy định pháp luật bảo vệ DLCN trong nước ở mức độ hoàn chỉnh được thể hiện rõ ràng nhất ở một đạo luật về bảo vệ DLCN. Thêm nữa, các quy định bảo vệ DLCN là quy định về quyền, giới hạn quyền của công dân, do đó phải nằm trong luật do cơ quan dân cử là Quốc hội thông qua.

6. Kết luận

Với tầm nhìn trở thành một quốc gia phát triển vào năm 2045, tận dụng cơ hội kinh tế do dữ liệu xuyên biên giới có thể nói là một bước đi tắt đón đầu khôn ngoan với một nước đang phát triển có thu nhập trung bình như Việt Nam. Do đó, trong quá trình thiết lập khung pháp luật về bảo vệ DLCN xuyên biên giới ở Việt Nam, giờ đây mới ở giai đoạn đầu nhưng việc xác định một cách tiếp cận pháp lý phù hợp lại chính là điểm mấu chốt để tạo ra hành lang pháp lý phát triển kinh tế trong sự bảo đảm bảo vệ quyền riêng tư của cá nhân trên môi trường số. Đồng thời, khi ban hành các quy định về bảo vệ DLCN xuyên biên giới, Việt Nam cần đặt vấn đề này trong tổng thể vấn đề về bảo vệ DLCN, trong tổng thể hệ thống pháp luật quốc gia, pháp luật quốc tế để ban hành chính sách pháp luật đồng bộ và tương thích, và đặt trên một nền tảng triết lý khoa học với những đánh giá kỹ thuật đầy đủ dựa trên hoàn cảnh của đất nước.

Tài liệu tham khảo

Allen, D.W.E., Berg, A., Berg, C., Markey-Towler, B. & Potts, J. (2019), "Some economic consequences of the GDPR", *Economics Bulletin*, Vol. 39 No. 2, pp. 785-797.

Casalini, F. & Gonzalez, J.L. (2019), "Trade and Cross-Border Data Flows", OECD Trade Policy Papers, No. 220, OECD Publishing, Paris..

Ciriani, S. (2015), "The economic impact of the european reform of data protection", *Communications & Strategies*, No. 97, pp. 41-58.

Cyberspace Administration of China (2016), "Cybersecurity law of the people's republic of China", http://www.cac.gov.cn/2016-11/07/c_1119867116_2.htm, truy cập ngày 16/02/2022.

European Commission (2017) "Adequacy Decisions: How the EU determines of a non-EU country has an adequate level of data protection", https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, truy cập ngày 15/02/2022.

Federal Register of Legislation (2021), "Privacy act 1988", https://www.legislation.gov.au/Details/C2021C00139, truy cập ngày 16/02/2022.

Garrie, D., Duffy-Lewis, T.H.M., Gillespie, R. & Wong, R. (2010), "Data protection: the challenges facing social networking", *Brigham International Law and Management Review*, Vol. 6, pp. 127-152.

Greenleaf, G. (2012), "Singapore's personal data protection act 2012: scope and principles (with so Many Exemptions, it is only a "Known Unknown"), Privacy Laws & Business International Report, No. 120, pp. 1, 5-7.

Lê, H. (2009), "Bảo vệ dữ liệu cá nhân trong thương mại điện tử", *Tạp chí Công nghiệp*, Số 3, tr. 7-8.

Meta (2018), "An update on our plans to restrict data access on Facebook", https://about.fb.com/news/2018/04/restricting-data-access/, truy cập ngày 25/02/2022.

Ministry of Foreign Affairs Singapore (2022), "Joint Press Statement Between the Socialist Republic of Vietnam and the Republic of Singapore on Strengthening Strategic Partnership and Recovery Cooperation", https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2022/02/20220225-Vietnam, ngày truy cập 25/02/2022.

Ngô, V.B.D. (2019), "Bảo vệ thông tin người tiêu dùng", *Tạp chí Nghiên cứu Lập pháp*, Số 12, tr. 19-28.

Nguyễn, Đ.B. (2021), "Bảo vệ dữ liệu cá nhân người dùng mạng xã hội trong bối cảnh hội nhập quốc tế", *Tạp chí Phát triển Khoa học & Công nghệ: Khoa học - Kinh tế - Luật và Khoa học quản lý*, Số 3, tr. 1764-1771.

Nguyễn, T.K.N. (2019), "Pháp luật của một số quốc gia Đông Nam Á về bảo vệ dữ liệu cá nhân và các gợi ý cho Việt Nam", *Tạp chí Nghiên cứu Lập pháp*, Số 7, tr. 53-64.

Nguyễn, T.T.V. (2017), "Bảo vệ dữ liệu cá nhân trong bối cảnh cách mạng công nghiệp 4.0", *Tạp chí Dân chủ & Pháp luật*, Số 10, tr. 3-7.

Nikkei Asia (2022), "Divided Internet - China and U.S switch places as data powerhouse", https://vdata.nikkei.com/en/newsgraphics/splinternet/, truy cập ngày 20/02/2022.

Office of Australian Information Commissioner (2019), "Chapter 8: Australian Privacy Principle 8 - Cross-border disclosure of personal information", version 1.2, https://www.oaic.gov.au/__data/assets/pdf_file/0006/1230/app-guidelines-chapter-8-v1.2.pdf, truy cập ngày 21/02/2022.

Office of the United States of Trade Representative (2022), "Korea - US Free trade agreement (KORUS FTA): chapter thirdteen: financial services", https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file35_12712.pdf, truy cập ngày 15/05/2022.

Pernot-Leplay, E. (2020), "China's approach on data privacy law: a third way between the U.S. and the E.U.?", *Penn State Journal of Law & International Affairs*, Vol. 8 No. 1, pp. 50-117.

Romanosky, S. & Acquisti, A. (2009), "Privacy costs and personal data protection: economic and legal perspectives", *Berkeley Technology Law Journal*, Vol. 24 No. 3, pp. 1062-1101.

Singapore Statutes Online (2020), "Personal data protection act 2012: 2020 revised edition", https://sso.agc.gov.sg/Act/PDPA2012#pr26-, truy cập ngày 18/02/2022.

The European Parliement and the Council (2016), "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Derective 95/46/EC (General Data Protection Regulation)", Official Journal of the European Union, L119/1.

The National People's Congress of the People's Republic of China (2021), "Personal information protection law", http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml, truy cập ngày 17/02/2022.

Trần, T.T.P. (2021), "Quy định chung của Liên minh Châu Âu về bảo vệ dữ liệu cá nhân và một số khuyến nghị đến Quốc hội, Chính phủ và doanh nghiệp Việt Nam", *Tạp chí Nghiên cứu Lập pháp*, Số 23, tr. 41-49.

Yang, S. (2020), "China: data localisation", *Global Data Review*, https://globaldatareview.com/insight/handbook/2021/article/china-data-localisation, truy cập ngày 17/02/2022.

Zhang, D. (2020), "China: Data localisation requirements", *Data Guidance*, https://www.dataguidance.com/opinion/china-data-localisation-requirements, truy cập ngày 09/02/2022.