HƯỚNG TIẾP CẬN VÀ HOÀN THIỆN PHÁP LUẬT BẢO VỆ DỮ LIỆU CÁ NHÂN TẠI VIỆT NAM TRƯỚC TÁC ĐỘNG LẬP PHÁP CỦA THẾ GIỚI VÀ KHU VỰC

BẠCH THỊ NHÃ NAM *

Tóm tắt: *Trong thời đại kinh tế số, dữ liệu cá nhân ngày càng trở nên quý giá và nhu cầu bảo vệ dữ liệu cá nhân trở nên cấp thiết đối với tất cả các quốc gia và vùng lãnh thổ, trong đó có Việt Nam. Nhiều quốc gia đã và đang trong quá trình xây dựng luật về bảo vệ dữ liệu cá nhân. Bài viết khái quát các mô hình tiếp cận và xây dựng pháp luật bảo vệ dữ liệu cá nhân của các khu vực pháp lí tiêu biểu trên thế giới và trong khu vực, từ đó chỉ ra các quan điểm tiếp cận điển hình, các giá trị chung, cốt lõi về dữ liệu cá nhân, cơ chế pháp lí bảo vệ dữ liệu cá nhân đã được công nhận cũng như chỉ ra các giá trị khác biệt tuỳ thuộc vào đặc điểm riêng của mỗi nền tài phán. Qua đó, bài viết đề xuất một số gợi ý ban đầu cho Việt Nam trong quá trình nghiên cứu, xây dựng, hoàn thiện pháp luật bảo vệ dữ liệu cá nhân.*

Từ khoá: Kinh tế số; dữ liệu cá nhân; bảo vệ dữ liệu

Nhận bài: 02/6/2021 Hoàn thành biên tập: 26/8/2022 Duyệt đăng: 26/8/2022

DIRECTIONS TO ACCESS AND REFINE THE LAW ON PERSONAL DATA PROTECTION IN VIETNAM FROM THE GLOBAL AND REGIONAL LEGAL IMPACT

Abstract: *In the era of digital economy, personal data becomes more and more precious, and the need to protect personal data becomes urgent for all countries and territories, including Vietnam. Many countries have been in the process of developing legislation on the protection of personal data. This article provides an overview of common approaches in the world and in the region, and pointing out typical legislative models, the common and core values of personal data, the recognized legal mechanism for the protection of personal data, as well as indicating different values due to the unique characteristics of each jurisdiction. Thereby, the article proposes some initial suggestions for Vietnam in the process of researching, developing and refining the law on personal data protection.*

Keywords: Digital economy; personal data; data protection

Received: Jun 2nd, 2021; Editing completed: Aug 26th, 2022; Accepted for publication: Aug 26th, 2022

1. Hai mô hình tiếp cận điển hình trong việc xây dựng quyền bảo vệ dữ liệu cá nhân trên thế giới

Trong bối cảnh nền kinh tế số diễn ra sôi động và ngày càng có nhiều hoạt động kinh tế, xã hội diễn ra trực tuyến, nhiều khu vực pháp lí khác nhau đã công nhận tầm quan trọng của quyền riêng tư và quyền bảo vệ dữ liệu. Số lượng các quốc gia ban hành đạo luật bảo vệ dữ liệu cá nhân không ngừng tăng lên. Tính đến tháng 4/2020, có 128/194 quốc gia trên thế giới đã ban hành quy định pháp luật bảo vệ dữ liệu và quyền riêng tư[1].

*** Thạc sĩ, Trường Đại học Kinh tế - Luật**
E-mail: nambtn@uel.edu.vn

[1] UNCTAD, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide, truy cập 20/8/2022.

Bảo vệ dữ liệu là bảo vệ bất kì thông tin nào liên quan đến một thể nhân đã được xác định hoặc có thể nhận dạng được, bao gồm tên, ngày tháng năm sinh, ảnh, cảnh quay video, địa chỉ email và số điện thoại. Các thông tin khác như địa chỉ IP và nội dung liên lạc liên quan đến hoặc được cung cấp bởi người dùng cuối của các dịch vụ truyền thông cũng được coi là dữ liệu cá nhân. Bảo vệ dữ liệu cá nhân có mục đích là đảm bảo việc xử lí hợp lí (thu thập, sử dụng, lưu trữ) dữ liệu cá nhân của cả khu vực công (cơ quan công quyền) và khu vực tư (công ti, tổ chức tư nhân hoạt động vì mục tiêu lợi nhuận).

Trước hết, cần phải đề cập khu vực Liên minh châu Âu (EU), các quốc gia ở khu vực này tiếp cận quyền bảo vệ dữ liệu theo mô hình bảo vệ toàn diện. Xuất phát từ quan niệm về quyền năng cơ bản của con người tại châu Âu, nhân phẩm (human dignity) được công nhận là quyền cơ bản tuyệt đối của con người. Trong khái niệm về nhân phẩm, quyền riêng tư hoặc quyền có cuộc sống riêng tư, được tự chủ, kiểm soát thông tin về bản thân đóng một vai trò quan trọng, theo đó quyền riêng tư không chỉ là quyền cá nhân mà còn là giá trị xã hội[2].

Quyền riêng tư và quyền bảo vệ dữ liệu mặc dù có mối liên hệ mật thiết với nhau nhưng đây là hai quyền riêng biệt. Khái niệm quyền bảo vệ dữ liệu bắt nguồn từ quyền riêng tư và cả hai đều là công cụ để bảo vệ và thúc đẩy các giá trị và quyền cơ bản của con người, là cơ sở để thực hiện các quyền tự do khác chẳng hạn như quyền tự do ngôn luận hoặc quyền hội họp. Vì đời sống riêng tư của cá nhân được đặt ở vị trí ưu tiên và cần được bảo vệ để đảm bảo cá nhân có quyền toàn vẹn đối với đời sống chính mình[3], do đó, bảo vệ dữ liệu được xem là một quyền cơ bản của cá nhân, không chỉ được bảo vệ bởi pháp luật quốc gia mà còn được bảo vệ bởi pháp luật của EU.

Xét về yếu tố lịch sử, người châu Âu có lịch sử lâu dài về các cuộc xâm phạm quyền riêng tư, ví dụ như trong Chiến tranh thế giới lần thứ hai, Đức Quốc xã đã sử dụng dữ liệu cá nhân nhạy cảm từ sổ đăng kí dân số địa phương để xác định vị trí và truy quét người Do Thái dẫn đến các cuộc thảm sát kinh hoàng, hay sau đó, ở Đông Đức, hoạt động của cảnh sát mật và cơ quan tình báo Stasi đã mở rộng việc tiến hành giám sát và trấn áp những người bất đồng chính kiến trong mọi khía cạnh của đời sống dân sự[4]. Những yếu tố lịch sử này đã tác động lớn đến ý thức bảo vệ đời sống riêng tư cũng như dữ liệu cá nhân của người châu Âu, đặc biệt trong thời kì phát triển sôi động của nền kinh tế số, trước những vụ bê bối đánh cắp dữ liệu của các công ti công nghệ hay những vụ tin tặc đánh cắp thông tin cá nhân và dữ liệu tài chính của hàng trăm nghìn người tiêu dùng trong khu vực.

---

[2] Thông tin công bố trên trang web chính thức của Cơ quan giám sát bảo vệ dữ liệu EU tại: https://edps.europa.eu/data-protection_en, truy cập 20/8/2022.

[3] Bạch Thị Nhã Nam, "Quyền được lãng quên từ thực tiễn phán quyết trong phạm vi Liên minh châu Âu", *Tạp chí Nghiên cứu lập pháp*, số 24/2020, tr. 38 - 47.

[4] Robert E.G. Beens, "The Privacy Mindset of The EU Vs. The US", 2020, https://www.forbes.com/ sites/ forbestechcouncil/2020/07/29/the-privacy-mindset-of-the-eu-vs-the-us/?sh=7b0088d67d01, truy cập 20/8/2022.

Tỉ lệ các quốc gia ban hành pháp luật về bảo vệ dữ liệu cá nhân châu Âu đến nay đạt 96%[5]. Sự hiểu biết của cộng đồng EU về quyền riêng tư bắt đầu được định hình vào những năm 1970 thông qua các phán quyết của Toà án nhân quyền châu Âu, Chỉ thị bảo vệ dữ liệu năm 1995 (Chỉ thị số 95/46/EC), Hiệp ước về hoạt động của EU, Hiến chương về các quyền cơ bản, cũng như các phán quyết của các toà án quốc gia trong EU về quyền riêng tư hay quyền bảo vệ dữ liệu cá nhân[6].

Đạo luật bảo vệ dữ liệu của EU được xem là tiêu biểu và hoàn thiện nhất hiện nay, chính là Quy định chung về bảo vệ dữ liệu (GDPR) có hiệu lực tháng 5/2018[7]. GDPR đã đưa ra các quyền mới đối với dữ liệu của cá nhân, chẳng hạn như quyền được lãng quên và quyền được di chuyển dữ liệu. GDPR đã góp phần nâng cao nhận thức bảo vệ dữ liệu đối với công chúng và tác động lớn tới chương trình nghị sự lập pháp của nhiều quốc gia trên toàn thế giới.

Ngoài tiêu chuẩn chung được tuân thủ trong các cam kết khu vực, các quốc gia thuộc EU và thuộc châu Âu thường ban hành đạo luật quốc gia về bảo vệ dữ liệu cá nhân để quy định tập trung, toàn diện, cụ thể và chi tiết các vấn đề có liên quan theo hướng đồng nhất hoá pháp luật trong khu vực; mở rộng tối đa phạm vi thông tin cá nhân được pháp luật điều chỉnh.

Quy tắc bảo vệ dữ liệu của EU bao gồm các quy tắc được áp dụng độc lập trong những hoàn cảnh riêng biệt, điều này thể hiện quyền bảo vệ dữ liệu không phải là một quyền tuyệt đối. Những nguyên tắc quan trọng được đề cập như tiêu chuẩn dữ liệu cá nhân, dữ liệu nhạy cảm, cơ quan giám sát độc lập, nguyên tắc giới hạn mục đích, các quy định về trao đổi dữ liệu giữa các cơ quan, giới hạn thời gian cho lưu trữ dữ liệu, xem xét hiệu quả các yêu cầu tư pháp và các khả năng tiếp cận dữ liệu, giám sát độc lập, nguyên tắc tương xứng khi hạn chế quyền bảo vệ dữ liệu, yêu cầu thông báo sau khi xảy ra vi phạm dữ liệu, quyền truy cập, sửa và xoá cũng như các quy định về quyết định tự động, bảo mật của chủ thể dữ liệu. Quyền của các chủ thể và nguyên tắc pháp lí có thể bị hạn chế nhưng những hạn chế này dựa trên nguyên tắc tương xứng, thiết lập tỉ lệ so sánh, chẳng hạn như so sánh giữa lợi ích bảo vệ thông tin cá nhân và lợi ích của cộng đồng đối với việc tiếp cận thông tin hoặc đối với yêu cầu tư pháp và yêu cầu điều tra tội phạm.

Vào ngày 19/02/2020, Uỷ ban châu Âu đã phát hành sách trắng giới thiệu *"Chiến lược châu Âu về dữ liệu"* [8]. Sách trắng này phác thảo các mục tiêu chính sách trong tương lai của Uỷ ban châu Âu trong lĩnh vực quyền riêng tư, bảo vệ dữ liệu, trí tuệ nhân tạo và các lĩnh vực khác trong thời đại kĩ

[5] UNCTAD, tlđd.

[6] Báo cáo nghiên cứu của Văn phòng Liên minh châu Âu (2010), "A comparison between US and EU data protection legislation for law enforcement purposes", tr. 67, https://op.europa.eu/en/publication-detail/-/publication/bf448177-771e-11e5-86db-01aa75ed71a1, truy cập 20/8/2022.

[7] Tra cứu toàn văn GDPR tại: https://gdpr-info.eu/, truy cập 20/8/2022.

[8] Thông tin sách trắng "Chiến lược châu Âu về dữ liệu" tra cứu tại: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy, truy cập 20/8/2022.

thuật số, điều này càng thể hiện xu hướng mạnh mẽ của EU trong việc hoàn thiện pháp luật và bảo vệ quyền lợi của chủ thể dữ liệu.

Trái ngược với mô hình tiếp cận của EU, Hoa Kỳ theo đuổi hướng tiếp cận tối giản đối với quyền bảo vệ dữ liệu cá nhân. Quyền bảo vệ dữ liệu cá nhân chỉ được xem là quyền thứ cấp so với các ưu tiên khác trong Hiến pháp Hoa Kỳ cũng như các lợi ích công cộng khác. Xuất phát từ Tu chính án thứ nhất bảo vệ quyền tự do ngôn luận, Tu chính án thứ tư bảo vệ quyền tìm kiếm và thu giữ[9], cũng như Đạo luật bảo vệ quyền riêng tư[10], Hoa Kỳ xem xét việc bảo vệ thông tin cá nhân là một khía cạnh của quyền riêng tư nhưng ở mức độ hài hoà hơn giữa bảo vệ quyền cá nhân của chủ thể dữ liệu và các lợi ích khác.

Thay vì xây dựng khuôn khổ pháp lí bảo vệ toàn diện đối với dữ liệu cá nhân như EU, Hoa Kỳ đã tiếp cận quyền riêng tư và bảo mật bằng cách điều chỉnh tối giản, phân tán quyền này trong một số lĩnh vực, xác định ưu tiên bảo vệ theo đối tượng và loại thông tin nhạy cảm (*ví dụ: tài chính, chăm sóc y tế, điện tử viễn thông, giáo dục*). Cụ thể, Hoa Kỳ ban hành Luật Quyền riêng tư năm 1974 nhằm hạn chế quyền đối với các dữ liệu do các cơ quan Chính phủ Hoa Kỳ nắm giữ; Luật Bảo vệ quyền riêng tư của tài xế năm 1994 (DPPA); Luật Riêng tư đối với giao tiếp điện tử năm 1986 (ECPA), Luật Bảo vệ quyền riêng tư của trẻ em trên nền tảng trực tuyến năm 2000 (COPPA), Luật về Trách nhiệm giải trình và trách nhiệm bảo hiểm y tế năm 1996 (HIPPA), bảo mật tất cả các dữ liệu liên quan đến chăm sóc sức khoẻ của bệnh nhân; Luật Bảo vệ quyền riêng tư video (VPPA), Luật Gramm-Leach-Bliley - là đạo luật quan trọng trong lĩnh vực tài chính và ngân hàng vào những năm 90 của thế kỉ XX đáp ứng các yêu cầu bảo mật và quyền riêng tư đối với dữ liệu quan trọng... Ngoài ra, Uỷ ban Thương mại liên bang (FTC) là cơ quan có thẩm quyền bảo vệ dữ liệu và bảo mật thông tin người tiêu dùng dựa trên Đạo luật FTC năm 1914. FTC cấm các công ti tham gia vào "các hành vi thương mại không công bằng hoặc lừa đảo" nhằm bảo vệ người tiêu dùng, FTC sẽ đưa ra lệnh phạt đối với các công ti không tuân thủ cam kết bảo mật hoặc không bảo vệ đầy đủ đối với thông tin cá nhân bên cạnh hành vi quảng cáo sai sự thật hoặc gây hiểu lầm đối với người tiêu dùng[11].

Ngoài ra, Hoa Kỳ nhấn mạnh và trao thẩm quyền lập pháp cho các các tiểu bang đối với quyền riêng tư và dữ liệu cá nhân. Tiêu biểu là tiểu bang California, Đạo luật về quyền riêng tư của người tiêu dùng California (CCPA) được ban hành vào năm 2018, có hiệu lực vào 01/01/2020 gần như đã giải quyết được vấn đề bảo mật dữ liệu người tiêu dùng ít nhất là ở California[12] và có tác động lớn tới việc ban hành đạo luật về

[9] Xem xét các Tu chính án của Hiến pháp Hoa Kỳ tại: https://constitutioncenter.org, truy cập 20/8/2022.

[10] Đạo luật này loại bỏ sự bảo vệ đối với những người không phải là công dân Hoa Kỳ.

[11] Tim Hickman, Detlev Gabel, Data Protection Laws and Regulations 2022, https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa. Ví dụ đối với mạng xã hội Facebook, FTC đã nộp đơn khiếu nại vào năm 2012 chống lại Facebook và Facebook đã đồng ý nộp số tiền phạt 5 tỉ đô la Mỹ.

[12] Xem toàn văn đạo luật CCPA tại: https://oag.ca.gov/privacy/ccpa, truy cập 20/8/2022.

bảo mật dữ liệu người tiêu dùng ở các tiểu bang khác[13].

Có nhiều lí do để giải thích cho cách tiếp cận tối giản của Hoa Kỳ đối với quyền bảo vệ dữ liệu cá nhân. *Trước hết,* mô hình tiếp cận tối giản và theo xu hướng bảo vệ ở cấp độ từ thấp đến cao đối với dữ liệu cá nhân phù hợp với cấu trúc nhà nước liên bang ở Hoa Kỳ, dần dần quá trình lập pháp ở các tiểu bang sẽ thúc đẩy nhận thức cộng đồng cũng như nỗ lực công nhận tiêu chuẩn pháp lí về bảo vệ dữ liệu ở khắp các tiểu bang, trong khi đó, chính quyền liên bang chỉ thiết lập các can thiệp hạn chế ở những lĩnh vực dữ liệu thiết yếu (thông tin y tế, tài chính...) hay đối tượng nhạy cảm cần được bảo vệ (trẻ em) trên toàn phạm vi liên bang.

Tiếp đến, việc không tích cực thiết lập sự bảo vệ tuyệt đối và toàn diện đối với dữ liệu cá nhân của Hoa Kỳ chịu sự chi phối và tác động mạnh mẽ bởi các công ti công nghệ và dữ liệu hàng đầu thế giới hình thành và phát triển hùng mạnh ở quốc gia này. Các công ti đã vận động hành lang ngăn cản nhà lập pháp ban hành các chính sách kiểm soát và quản lí dữ liệu cá nhân nghiêm ngặt. Thêm vào đó, các công ti này cũng tác động vào quan niệm của người tiêu dùng về vai trò kém quan trọng của quyền riêng tư. Một khảo sát thú vị đối với những người dùng internet ở Hoa Kỳ được công bố vào cuối năm 2019 cho thấy mức độ lo ngại về quyền riêng tư trên nền tảng trực tuyến có tỉ lệ chênh lệch ít ỏi với việc người dùng internet sẵn sàng chấp nhận đánh đổi những rủi ro nhất định về quyền riêng tư trên nền tảng trực tuyến để làm cho cuộc sống của họ tiện lợi hơn (74% so với 69%)[14]. Thói quen này của người tiêu dùng khiến nhu cầu bảo vệ đời sống riêng tư không phải là ưu tiên hàng đầu ở xứ sở công nghệ.

Ngoài ra, tại Hoa Kỳ, các lợi ích công cộng như an ninh cộng đồng, an ninh quốc gia và các quyền ưu tiên theo Hiến pháp như quyền tự do ngôn luận được đề cao bảo vệ hơn quyền riêng tư dữ liệu. Bên cạnh đó, nhằm phục vụ các cuộc điều tra tội phạm thông thường, một phần quan trọng là việc thu thập dữ liệu của khu vực công diễn ra trong khuôn khổ yêu cầu an ninh quốc gia trên cơ sở các điều khoản có trong Đạo luật Patriot và Fisa[15]. Trong thực tiễn xét xử, tư duy của các thẩm phán Hoa Kỳ có xu hướng coi trọng quyền tự do ngôn luận, ví dụ điển hình như án lệ Cox Broadcasting Corporation v. Cohn (1975)[16] của Toà án tối cao Hoa Kỳ. Trong vụ án này, con gái 17 tuổi của người khởi kiện Martin Cohn bị cưỡng bức và giết hại, hãng truyền hình địa phương sau khi thu thập thông tin đã công bố danh tính của con gái ông trong bản tin, hành vi này đã vi phạm pháp luật tiểu bang Georgia. Khi đó, Toà án tối cao Hoa Kỳ không đồng tình với

[13] Hiện có 6 tiểu bang Hoa Kỳ đã ban hành Đạo luật quyền riêng tư dữ liệu bao gồm: California, New York, Maryland, Masachusetts, Hawaii, North Dakota, trong khi một số tiểu bang khác ban hành Dự thảo luật và xem xét phê chuẩn.

[14] Statista, thông tin thống kê truy cập tại: https://www.statista.com/statistics/1023952/global-opinion-concern-internet-privacy-risk-convenience/, truy cập 20/8/2022.

[15] Báo cáo nghiên cứu của Văn phòng Liên minh châu Âu, tlđd, tr. 59.

[16] Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 1975, https://www.lexisnexis.com/community/casebrief/p/casebrief-cox-broad-corp-v-cohn, truy cập 20/8/2022.

quy định pháp luật của tiểu bang Georgia và cho rằng báo chí là nguồn quan trọng để công dân có thể theo dõi và đánh giá trình tự tư pháp của cơ quan công quyền, các thông tin về quy trình điều tra và xét xử tội phạm (dù có công bố thông tin cá nhân) thì việc công khai thông tin này vẫn có ý nghĩa quan trọng đối với lợi ích công cộng. Do đó, kiểm soát và giới hạn báo chí theo quy định pháp luật bang Georgia là một sự xâm phạm nguy hiểm đối với tự do báo chí và tự do ngôn luận - những quyền được bảo vệ trong Tu chính án thứ nhất.

Tóm lại, các phân tích trên cho thấy hai xu hướng lập pháp điển hình về quyền bảo vệ dữ liệu cá nhân hoàn toàn khác biệt giữa EU và Hoa Kỳ, do mô hình tiếp cđến xây dựng pháp luật bảo vệ dữ liệu cá nhân khác nhau dẫn đến các quy tắc pháp lí cụ thể quy định khác biệt. Ví dụ như thuật ngữ pháp lí thông tin cá nhân ở Hoa Kỳ có nội hàm hẹp hơn so với khái niệm dữ liệu cá nhân ở EU hay các tiêu chuẩn về mức độ bảo vệ dữ liệu cá nhân; nguyên tắc xử lí, kiểm soát dữ liệu và các hạn chế, ngoại lệ trong mối tương quan giữa lợi ích cá nhân và lợi ích cộng đồng, an ninh quốc gia hoàn toàn khác nhau.

Nếu EU hướng đến xây dựng khung pháp lí hoàn thiện nhất để bảo vệ quyền dữ liệu cá nhân như một quyền cơ bản trong một Đạo luật riêng biệt, cụ thể thì Hoa Kỳ hiện thiếu một khung pháp lí bảo vệ dữ liệu cá nhân trên phạm vi toàn liên bang và đặc biệt Hoa Kỳ bỏ qua mối lo ngại vi phạm dữ liệu cá nhân đối với chủ thể dữ liệu không phải là công dân Hoa Kỳ. Điểm khác biệt thứ hai là việc xử lí dữ liệu cá nhân ở các khu vực công và khu vực tư tại EU được thực hiện hạn chế trên cơ sở cân nhắc theo tiêu chuẩn tỉ lệ lợi ích, sự giải trình hợp pháp của cơ quan công quyền. Trong khi đó, Hoa Kỳ không hạn chế việc chia sẻ dữ liệu cá nhân giữa các cơ quan an ninh và tình báo quốc gia, điều này được xem như là một quy tắc pháp lí thay vì là ngoại lệ như tại EU chỉ được áp dụng hạn chế trong một số trường hợp.

Hoa Kỳ và EU là hai khu vực pháp lí lớn và có sức ảnh hưởng tới quá trình lập pháp đối với các quốc gia trên thế giới. Nghiên cứu hai mô hình này và tìm kiếm các giá trị phổ quát trong việc bảo vệ dữ liệu cá nhân nhằm tìm kiếm hướng tiếp cận lập pháp thích hợp cho quốc gia mình là việc cần làm trong quá trình xây dựng và hoàn thiện pháp luật bảo vệ dữ liệu ở các nền tài phán và khu vực pháp lí khác trên thế giới.

2. Đặc trưng của khu vực châu Á - Thái Bình Dương trong việc xây dựng pháp luật về quyền bảo vệ dữ liệu cá nhân

Châu Á - Thái Bình Dương là khu vực có tỉ lệ lập pháp về quyền bảo vệ dữ liệu thấp nhất trên thế giới (ở ngưỡng 55% - 57%)[17] khi so sánh với các khu vực khác.

Tại khu vực châu Á - Thái Bình Dương, trong số 60 quốc gia thì có 34 quốc gia đã ban hành pháp luật về bảo vệ dữ liệu[18], trong đó nhiều quốc gia đã xem xét sửa đổi khung pháp lí theo hướng tăng cường bảo vệ dữ liệu cá nhân như Nhật Bản, Kazakhstan, Hàn Quốc, New Zealand và Singapore sau lần đầu tiên ban hành. Từ năm 2010 đến năm 2020, 13 quốc gia tại khu vực châu Á - Thái

[17] UNCTAD, tlđd.
[18] UNCTAD, tlđd.

Bình Dương đã ban hành mới pháp luật bảo vệ dữ liệu và 07 quốc gia đã tiến hành sửa đổi pháp luật bảo vệ dữ liệu để phù hợp với bối cảnh mới[19].

Vào năm 2020, Nhật Bản đã sửa đổi Đạo luật Bảo vệ thông tin cá nhân (APPI) và ban hành Đạo luật sửa đổi vào ngày 05/6/2020, có hiệu lực vào 01/4/2022[20]. Uỷ ban Bảo vệ thông tin cá nhân (PPC) là cơ quan chính thức độc lập chịu trách nhiệm bảo vệ quyền quyền riêng tư của các cá nhân và giám sát việc sử dụng và lưu trữ dữ liệu cá nhân người tiêu dùng của các doanh nghiệp. PPC cũng chịu trách nhiệm về hợp tác quốc tế giữa Nhật Bản và các khu vực tài phán khác trong lĩnh vực luật bảo vệ dữ liệu.

Hàn Quốc đã sửa đổi ba luật chính về dữ liệu cá nhân: Đạo luật Bảo vệ thông tin cá nhân (PIPA); Đạo luật về Thúc đẩy sử dụng mạng thông tin, truyền thông và bảo vệ thông tin (Đạo luật về mạng); Đạo luật Sử dụng, bảo vệ thông tin tín dụng (Đạo luật Thông tin tín dụng)[21].

Trung Quốc - quốc gia láng giềng Việt Nam, có số lượng người dùng internet dẫn đầu thế giới, sau khi quốc gia này đã đưa ra những nguyên tắc pháp lí cơ bản về bảo vệ quyền riêng tư và quyền bảo vệ thông tin cá nhân trong Bộ luật Dân sự đầu tiên của nước này vào năm 2020[22]. Bước tiến lập pháp quan trọng là việc Trung Quốc đã ban hành Luật Bảo vệ thông tin cá nhân (PIPL) và Luật An toàn dữ liệu vào tháng 8/2021, hai đạo luật này sẽ có hiệu lực từ ngày 01/11/2021, cùng với Luật An ninh mạng năm 2017. Nhìn chung, Trung Quốc đã hoàn thiện khung pháp lí về bảo vệ dữ liệu cá nhân, đặc biệt là bảo vệ dữ liệu cá nhân trên không gian mạng.

Những vấn đề pháp lí mới được đề cập trong PIPL như: số tiền phạt cao áp dụng đối với các hành vi vi phạm, khả năng áp dụng pháp luật bảo vệ dữ liệu ngoài lãnh thổ Trung Quốc, các quy tắc mới quản lí việc chuyển dữ liệu xuyên biên giới, củng cố các quyền mới mà các chủ thể dữ liệu cư trú tại Trung Quốc, bất kể quốc tịch của họ, chẳng hạn như quyền xoá dữ liệu và quyền cá nhân hủy bỏ sự đồng ý đối với việc thu thập dữ liệu. Đối với các công ti xử lí khối lượng lớn thông tin cá nhân cũng sẽ được yêu cầu chỉ định một nhân viên bảo vệ dữ liệu chịu trách nhiệm xử lí dữ liệu cá nhân liên quan đến Trung Quốc. Việc xử lí thông tin cá nhân nhạy cảm xuyên biên giới sẽ phải tuân theo một ngưỡng tiêu chuẩn của PIPL, nếu công ti hành xử vượt mức tiêu chuẩn này, công ti buộc phải bản địa hoá các hoạt động xử lí dữ liệu của mình tại Trung Quốc.

Tại khu vực Đông Nam Á, trong lĩnh vực kĩ thuật số, đây là khu vực Internet phát triển nhanh nhất thế giới với gần bốn triệu người dùng mới đến từ nền tảng trực tuyến mỗi tháng trong suốt 5 năm qua, có hơn 700

[19] Các quốc gia bao gồm Úc, Trung Quốc, Hồng Kông, Ấn Độ, Indonesia, Nhật Bản, Kazakhstan, Kyrgyzstan, Macao, Malaysia, Nepal, New Zealand, Philippines, Singapore, Hàn Quốc, Đài Loan, Thái Lan, Turkmenistan và Uzbekistan.

[20] Thông tin công bố tại https://www.ppc.go.jp/en/news/archives/2020/20200618/, truy cập 20/8/2022.

[21] Theo Asia Business Law Journal, https://law.asia/data-privacy-framework-asia/, truy cập 20/8/2022.

[22] Toàn văn Bộ luật Dân sự Trung Quốc, http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf, truy cập 20/8/2022.

triệu kết nối di động đang hoạt động ở Đông Nam Á, chi tiêu trực tuyến dự kiến sẽ đạt 200 tỉ đô la Mỹ vào năm 2025[23].

Theo UNTACD, tính đến 4/2020, hầu hết các quốc gia trong khu vực đều có quy định pháp luật quyền bảo vệ dữ liệu cá nhân trừ ba quốc gia: Campuchia, Papua New Guinea chưa ban hành pháp luật về bảo vệ dữ liệu cá nhân và Myanmar đang xây dựng dự thảo luật[24].

Philippines là quốc gia xây dựng pháp luật về quyền riêng tư nghiêm ngặt nhất trong khu vực. Đạo luật Bảo mật dữ liệu của Philippines ban hành năm 2012, được mô phỏng theo Chỉ thị bảo vệ dữ liệu của EU. Philippines cũng đã thành lập thêm Uỷ ban quyền riêng tư quốc gia (NPC) vào năm 2016 để quản lí và thực hiện các điều khoản của đạo luật.

Tại Malaysia, Đạo luật Bảo vệ dữ liệu cá nhân (PDPA) có hiệu lực từ năm 2014, tuy nhiên luật này bộc lộ khuyết điểm là thiếu tính cưỡng chế thi hành khi có các hành vi vi phạm xảy ra. Do đó, quốc gia này đang xem xét sửa đổi PDPA sau khi đề xuất tham vấn cộng đồng vào năm 2020, về cơ bản sẽ mở rộng việc áp dụng pháp luật bảo vệ dữ liệu trên cơ sở tham chiếu quy định của EU.

Singapore đã ban hành Đạo luật Bảo vệ Dữ liệu Cá nhân 2012 ("PDPA") vào 15/10/2012 và thành lập Ủy ban Bảo vệ Dữ liệu Cá nhân. Vào 2/11/2020, Quốc hội Singapore đã thông qua Đạo luật bảo vệ dữ liệu cá nhân (Bản sửa đổi).Uỷ ban Bảo vệ dữ liệu cá nhân (PDPC) tại Singapore là cơ quan chịu trách nhiệm quản lí và thực thi PDPA. PDPA trao quyền cho các cá nhân bảo vệ dữ liệu của họ và quản lí cách các doanh nghiệp có thể sử dụng dữ liệu cá nhân được thu thập từ người tiêu dùng phù hợp với các mục đích hợp pháp[25].

Nhìn chung, khung cảnh lập pháp về quyền bảo vệ dữ liệu cá nhân ở khu vực châu Á - Thái Bình Dương hay khu vực Đông Nam Á đang diễn ra hết sức sôi động và thay đổi mạnh mẽ trong suốt thập kỉ qua. Trái ngược với khu vực EU thể hiện tính khái quát hoá và tính đồng nhất trong việc xây dựng khuôn khổ pháp lí đối với quyền bảo vệ dữ liệu, khu vực châu Á - Thái Bình Dương hay Đông Nam Á có đặc điểm là hệ thống pháp luật đa dạng và có nhiều khác biệt về lịch sử, văn hoá, trình độ phát triển kinh tế. Vậy nên các quốc gia trong khu vực châu Á - Thái Bình Dương không thể đồng nhất pháp luật bảo vệ dữ liệu và các đạo luật này đều có những quy định cụ thể khác biệt với các yếu tố tiêu biểu được nhận diện sau đây:

- Mô hình tiếp cận: hầu hết quốc gia ở khu vực châu Á - Thái Bình Dương lựa chọn cách tiếp cận dung hoà giữa hai mô hình EU và Hoa Kỳ như Nhật Bản, Hàn Quốc, Singapore, Thái Lan, Trung Quốc... Các quốc gia theo mô hình này thường ban hành một đạo luật riêng về bảo vệ thông tin cá nhân để quy định tập trung, toàn diện các

[23] Deloitte, "Data and privacy protection in ASEAN, What does it mean for businesses in the region?", 2021, https://www2.deloitte.com/id/en/pages/risk/articles/data-privacy-in-asean.html, truy cập 20/8/2022.

[24] UNCTAD, tlđd.

[25] Varin Khera, *Data Protection and Cybersecurity Laws In The Asia-Pacific Region,* https://itsec. group/blog-post-cybersecurity-regulations-asia-pacific.html, 2021, truy cập 20/8/2022.

vấn đề có liên quan đến bảo vệ dữ liệu. Trong đó, các đạo luật đều thừa nhận các giá trị cốt lõi phổ quát liên quan đến quyền bảo vệ dữ liệu cá nhân như khái niệm dữ liệu cá nhân, nguyên tắc xử lí dữ liệu cá nhân, cơ quan độc lập bảo vệ dữ liệu... dưới sự ảnh hưởng của GDPR, bên cạnh ghi nhận những nội dung khác biệt tuỳ thuộc điều kiện của quốc gia, ví dụ như phạm vi dữ liệu cá nhân, cơ chế bảo vệ dữ liệu, mức độ quản lí dữ liệu hợp lí, hài hoà hơn không quá thắt chặt, cũng không quá tối giản.

Cũng có số ít quốc gia lựa chọn theo một mô hình nhất định, ví dụ Philippines chịu sự ảnh hưởng mạnh mẽ của mô hình EU.

- Phạm vi áp dụng: Có sự quy định khác biệt giữa các đạo luật bảo vệ dữ liệu cá nhân trong khu vực châu Á - Thái Bình Dương, phần lớn các quốc gia đều quy định phạm vi áp dụng trong lãnh thổ của quốc gia. Tuy nhiên, có 05 quốc gia quy định áp dụng ngoài phạm vi lãnh thổ, cách quy định này tương tự hoặc vượt quá so với nội dung trong GDPR của EU bao gồm: Úc, Nhật Bản, New Zealand, Philippines và Thái Lan. *Ví dụ:* Đạo luật APPI của Nhật Bản quy định phạm vi áp dụng ngoài lãnh thổ Nhật Bản. Khi một chủ thể xử lí dữ liệu ở nước ngoài đã lấy được dữ liệu cá nhân của một cá nhân cư trú ở Nhật Bản qua việc cung cấp hàng hoá hoặc dịch vụ và thực hiện xử lí thông tin cá nhân đó hoặc bất kì thông tin ẩn danh nào được tạo ra từ đó, chủ thể xử lí dữ liệu dù ở nước ngoài nhưng buộc phải tuân theo quy định của Đạo luật APPI khi tiến hành xử lí dữ liệu ở nước ngoài[26].

- Hoạt động xuyên biên giới: Tương tự, 3/4 quốc gia trong khu vực áp đặt các hạn chế đối với việc chuyển dữ liệu cá nhân xuyên biên giới. Các quốc gia đều quy định hạn chế chuyển dữ liệu xuyên biên giới, nhưng cơ sở cơ sở pháp lí để thực hiện chuyển dữ liệu thì được các quốc gia quy định khác nhau. *Ví dụ*: yêu cầu quốc gia tiếp nhận dữ liệu đáp ứng việc bảo vệ dữ liệu đầy đủ, điều kiện chuyển dữ liệu trên cơ sở đồng ý (hoặc cơ sở pháp lí khác)... Trong khi đó, Hồng Kông, Indonesia, Nepal và Đài Loan không hạn chế việc chuyển dữ liệu cá nhân qua biên giới.

- Thông báo vi phạm: Các đạo luật yêu cầu thông báo đến các cá nhân và/hoặc cơ quan bảo vệ dữ liệu "ngay lập tức" hoặc "không chậm trễ", trong khi những đạo luật khác yêu cầu thông báo trong vòng 72 giờ (Philippines, Singapore và Thái Lan) hoặc trong vòng 14 ngày khi có sự vi phạm về xử lí dữ liệu.

- Căn cứ pháp lí để xử lí dữ liệu cá nhân: 2/3 quốc gia (12 quốc gia) không cho phép xử lí dữ liệu không dựa trên cơ sở lợi ích hợp pháp. Cơ sở lợi ích hợp pháp được quy định có nhiều khác biệt giữa các quốc gia.

- Quyền cá nhân của chủ thể dữ liệu: quyền truy cập dữ liệu và quyền chỉnh sửa dữ liệu của cá nhân được quy định ở tất cả các quốc gia ngoại trừ Nepal. Có 09 quốc gia quy định quyền xoá dữ liệu nhưng chỉ có bốn quốc gia cung cấp quyền di chuyển dữ liệu: Trung Quốc, Philippines, Singapore và Thái Lan. Khung thời gian để trả lời yêu cầu

[26] Phần 14 của Đạo luật APPI của Nhật Bản, https://www.dataguidance.com/notes/japan-data-protection-overview, truy cập 20/8/2022.

đối với các quyền cá nhân của chủ thể dữ liệu cũng rất khác nhau: 04 quốc gia yêu cầu phản hồi trong vòng 30 ngày; hai quốc gia yêu cầu phản hồi trong vòng 20 - 21 ngày; 02 quốc gia quy định phản hồi trong vòng 10 - 15 ngày; 03 quốc gia quy định phản hồi trong vòng 01 - 07 ngày; 07 quốc gia không xác định khoảng thời gian cụ thể.

- Nhân viên cơ quan bảo vệ dữ liệu: 08 quốc gia yêu cầu thiết lập quy trình bổ nhiệm nhân viên cơ quan bảo vệ dữ liệu: Trung Quốc, Nhật Bản, Kazakhstan, Hàn Quốc, New Zealand, Philippines, Singapore và Thái Lan nhằm đảm bảo nguyên tắc hoạt động độc lập, khách quan của cơ quan giám sát, bảo vệ dữ liệu quốc gia.

- Yêu cầu bản địa hoá: Có 04 loại biến thể của việc bản địa hoá dữ liệu: 1) bản địa hoá có điều kiện đòi hỏi yêu cầu lưu trữ trong những lĩnh vực cụ thể như y tế, thanh toán trực tuyến...; 2) yêu cầu lưu trữ tại bản địa vô điều kiện (đối với tất cả dữ liệu cá nhân); 3) yêu cầu sao chép vô điều kiện (đối với tất cả dữ liệu cá nhân) tại bản địa; 4) cho phép di chuyển và truy cập dữ liệu vô điều kiện trong khuôn khổ các hiệp định song phương/đa phương[27]. Theo đó, một số quốc gia áp đặt các yêu cầu về bản địa hoá dữ liệu, *ví dụ:* Kazakhstan, Trung Quốc đều yêu cầu các công ti lưu trữ dữ liệu tại quốc gia mình một cách vô điều kiện, bao gồm thông tin cá nhân và dữ liệu quan trọng được thu thập và sản xuất trong quá trình hoạt động kinh doanh của các công ti.

Luật An ninh mạng của Việt Nam quy định bên xử lí dữ liệu phải lưu trữ dữ liệu tại Việt Nam vô điều kiện nếu doanh nghiệp (nội địa hoặc nước ngoài) đó cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lí dữ liệu về thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra.

Luật Thông tin và giao dịch điện tử của Indonesia quy định lưu trữ vô điều kiện các dữ liệu trong lĩnh vực dịch vụ công, trong khi đó Úc quy định lưu trữ vô điều kiện các dữ liệu sức khỏe cá nhân nhạy cảm trong Đạo luật Lưu trữ thông tin sức khoẻ[28].

- Đăng kí hoạt động liên quan đến dữ liệu: Xu hướng trên thế giới là giảm thiểu các yêu cầu đăng kí, tuy nhiên có 04 quốc gia trong khu vực yêu cầu các tổ chức phải đăng kí hoạt động xử lí dữ liệu với cơ quan bảo vệ dữ liệu: Kazakhstan; Malaysia, Philippines, và Uzbekistan.

- Đánh giá tác động đối với việc bảo vệ dữ liệu: hầu hết đạo luật trong khu vực không yêu cầu các tổ chức thực hiện các hoạt động xử lí dữ liệu thực hiện đánh giá tác động bảo vệ dữ liệu, trừ các quốc gia yêu cầu bắt buộc thực hiện: Singapore, Hàn Quốc và Philippines.

- Tăng cường tính cưỡng chế thi hành: khi các vụ vi phạm dữ liệu lớn xảy ra trên thế giới và trong khu vực có xu hướng gia

[27] Anirudh Burman, Upasana Sharma, Research Paper, "How Would Data Localization Benefit India?", Carnegie Endowment for International Peace, 2021, https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291, truy cập 20/8/2022.

[28] Anirudh Burman, Upasana Sharma, tlđd.

tăng trong vài năm qua, các cơ quan bảo vệ dữ liệu (DPA) ở Hàn Quốc, Nhật Bản đã tập trung vào việc tăng cường các hoạt động bảo mật trong khu vực tư nhân. DPA ở Hàn Quốc, Nhật Bản và Úc thực hiện thanh tra và khởi kiện các tổ chức không tuân thủ các biện pháp bảo mật thích hợp, dẫn đến bên vi phạm phải nộp các khoản phạt và/hoặc yêu cầu bên vi phạm thực hiện các biện pháp khắc phục, sửa chữa dữ liệu.

Tóm lại, pháp luật bảo vệ dữ liệu trong khu vực châu Á - Thái Bình Dương có các yếu tố cốt lõi được tìm thấy trong hầu hết mọi đạo luật bảo vệ dữ liệu trên thế giới nhưng các quốc gia sẽ đưa ra các quy định khác biệt để đảm bảo việc tuân thủ và tính khả thi của pháp luật trên thực tiễn.

3. Những vấn đề pháp lí đặt ra đối với việc hoàn thiện pháp luật bảo vệ dữ liệu cá nhân ở Việt Nam

Từ việc quan sát quá trình các quốc gia trên thế giới và khu vực ban hành pháp luật bảo vệ dữ liệu cho thấy mỗi một quốc gia đều phải cân nhắc đặc trưng riêng của quốc gia mình trên phương diện tính khả thi, tính hiệu quả kinh tế, khác biệt văn hoá, lịch sử, điều kiện kinh tế, khả năng hoàn thiện pháp luật bảo vệ dữ liệu thích ứng với nền kinh tế số, bên cạnh việc tôn trọng những giá trị cốt lõi và nguyên tắc pháp lí cơ bản trong việc bảo vệ dữ liệu, quyền riêng tư của cá nhân.

Đối với Việt Nam, trong quá trình xây dựng pháp luật bảo vệ dữ liệu, Việt Nam cần cân nhắc những nội dung quan trọng sau đây:

Thứ nhất, Việt Nam cần xác định mô hình tiếp cận đối với việc xây dựng pháp luật về quyền bảo vệ dữ liệu cá nhân dựa trên việc quan sát quá trình lập pháp của các quốc gia trên thế giới, các quốc gia trong khu vực và đánh giá mức độ đáp ứng của khung pháp luật hiện tại với nhu cầu của xã hội Việt Nam với các điều kiện chính trị, kinh tế, xã hội, văn hoá riêng biệt. Điển hình, trên thế giới có hai mô hình tiếp cận khác biệt về quyền bảo vệ dữ liệu cá nhân. Hầu hết các quốc gia trong khu vực đều lựa chọn cách tiếp cận hỗn hợp để dễ dàng thúc đẩy việc công nhận quyền chủ thể dữ liệu trong điều kiện riêng biệt của quốc gia mình.

Việt Nam đang đối diện với sự phát triển nhanh chóng của nền kinh tế số với sự thống trị của các công ti dữ liệu toàn cầu trên nền tảng công nghệ còn kém phát triển. Trong quá trình đó, Việt Nam đã ghi nhận việc bảo vệ quyền riêng tư và quyền bảo vệ dữ liệu cá nhân trong Hiến pháp và các văn bản pháp luật chuyên ngành[29]. Tuy nhiên, các quy định này nằm rải rác, phân tán với mức độ bảo vệ khác nhau, có sự khác biệt, thiếu nhất quán. Tham khảo Trung Quốc, trước khi ban hành luật bảo vệ thông tin cá nhân, Trung Quốc hay những quốc gia khác cũng quy định phân tán trong các văn bản luật chuyên ngành[30].

[29] Luật Giao dịch điện tử năm 2005, Luật Điện ảnh năm 2006, Luật Công nghệ thông tin năm 2006, Luật Viễn thông năm 2009, Luật Các tổ chức tín dụng năm 2010, Luật Bưu chính năm 2010, Luật Bảo vệ quyền lợi người tiêu dùng năm 2010, Luật Xuất bản năm 2012, Luật Báo chí năm 2016...

[30] Trước khi có Dự luật Bảo vệ thông tin cá nhân, những văn bản pháp luật quy định bảo vệ quyền riêng tư, quyền bảo vệ dữ liệu bao gồm: Quyết định của Ủy ban Thường vụ Quốc hội Trung Quốc về việc tăng cường công tác bảo vệ thông tin mạng; Luật An ninh mạng; Luật Bảo vệ quyền và lợi ích của người tiêu dùng.

Do đó, việc thống nhất hoá và hướng đến xây dựng văn bản pháp luật chuyên biệt, toàn diện về bảo vệ dữ liệu tại Việt Nam là xu hướng cần được thúc đẩy. Đây là cách tiếp cận phù hợp với Việt Nam, vừa giải quyết kẻ hở pháp lí hiện tại, vừa khắc phục việc quy định rải rác, không thống nhất như hiện nay. Việc ban hành một luật riêng là xu hướng phổ quát của tất cả các quốc gia trong khu vực châu Á - Thái Bình Dương và gần đây nhất là Trung Quốc, bên cạnh hai đạo luật là Luật An toàn dữ liệu và Luật An ninh mạng.

Ở Việt Nam, Chính phủ đã ban hành Nghị quyết số 27/NQ-CP thông qua hồ sơ xây dựng Nghị định bảo vệ dữ liệu cá nhân vào 8/3/2022, theo đó, Chính phủ quyết nghị thông qua nội dung dự thảo Nghị định bảo vệ dữ liệu cá nhân, đồng thời giao Bộ trưởng Bộ Công an thừa ủy quyền Chính phủ báo cáo, xin ý kiến Ủy ban Thường vụ Quốc hội về dự thảo Nghị định, và yêu cầu Bộ Công an chủ trì, phối hợp với Bộ Tư pháp nghiên cứu, đề xuất xây dựng Luật Bảo vệ dữ liệu cá nhân.[31] Đây là hướng đi tích cực và đúng đắn trong việc nhận thức tầm quan trọng của việc hoàn thiện khung pháp lí về bảo vệ dữ liệu tại Việt Nam.

Thứ hai, việc xây dựng các quy định pháp luật bảo vệ dữ liệu cá nhân tại Việt Nam cần đảm bảo sự cân bằng giữa bảo vệ lợi ích cá nhân và lợi ích công cộng, lợi ích quốc gia.

Trong việc đấu tranh ngăn ngừa tội phạm và các hành vi trục lợi của các tổ chức, công ti, cá nhân, quốc gia nào cũng phải giải quyết bài toán khó là dung hoà sự tôn trọng tự do cá nhân với sự cần thiết duy trì trật tự xã hội. Nếu việc thiết lập quy định quá tôn trọng tự do cá nhân thì sự bảo vệ xã hội sẽ sơ khoáng và ngược lại, nếu pháp luật đề cao quyền lợi xã hội thì các quyền lợi cá nhân dễ bị xem nhẹ.

Quyền bảo vệ dữ liệu cá nhân không phải là một quyền tuyệt đối mà có các trường hợp hạn chế cho phép kiểm soát và xử lí dữ liệu cá nhân trên cơ sở hợp pháp, chính đáng. Trong mối quan hệ tương quan với các quyền lợi khác, nhiều trường hợp xảy ra xung đột quyền lợi, cụ thể: quyền bảo vệ dữ liệu cá nhân có thể xung đột với quyền tiếp cận thông tin, quyền bảo vệ dữ liệu cá nhân có thể xung đột với quyền tự do ngôn luận. Một cách cơ bản, quyền của một người yêu cầu người khác không sử dụng và không chia sẻ thông tin của họ hay bình luận về họ, vô hình chung sẽ hạn chế tự do ngôn luận của người khác trên các hình thức truyền thông, kể cả mạng xã hội và tác động vào quyền tự do của báo chí được đăng tải và bình luận về thông tin.

Theo như Nghị định bảo vệ dữ liệu cá nhân hiện nay, quyền của cá nhân được quy định khá rộng, bao gồm: quyền cho phép hay không cho phép người khác xử lí dữ liệu (thu thập, lưu trữ, sử dụng dữ liệu cá nhân); nhận thông báo nếu có người khác xử lí dữ liệu cá nhân của mình (có thể là chính quyền, doanh nghiệp...); yêu cầu chấm dứt việc xử lí dữ liệu, khiếu nại về hành vi vi phạm; đòi bồi thường nếu có vi phạm; được bảo vệ khỏi việc bị tiết lộ dữ liệu cá nhân nhạy cảm hoặc dữ liệu cơ bản nhưng gây tổn hại cho chủ thể. Cần nhìn nhận quyền của chủ thể dữ liệu là tập hợp rất nhiều nhóm quyền và các

[31] Theo tin đưa trên website chính thức của Bộ Thông tin và Truyền thông, https://www.mic.gov.vn/pages/tintuc/printpage.aspx?tintucID=152957, truy cập 20/8/2022.

ngoại lệ sẽ chỉ được phép vượt qua một số nhóm quyền trong số đó chứ không phải toàn bộ các quyền của chủ thể dữ liệu.

Các ngoại lệ pháp lí (legal exemptions) trong pháp luật bảo vệ dữ liệu cá nhân trên thế giới được quy định rõ ràng, hạn chế tronché ột danh sách các trường hợp cụ thể. GDPR đặt ra một số ngoại lệ về xử lí thông tin cá nhân cho hoạt động báo chí, xử lí và tiết lộ dữ liệu cá nhân theo yêu cầu của nhà nước và cơ quan cảnh sát. Trên cơ sở này, pháp luật của quốc gia trong khu vực EU cũng ban hành các quy định pháp luật liên quan để can thiệp vào dữ liệu cá nhân.

Hiện nay, Dự thảo Nghị định bảo vệ dữ liệu của Việt Nam đã quy định các trường hợp dữ liệu cá nhân có thể bị tiết lộ tại Điều 6 hay dữ liệu cá nhân có thể bị xử lí mà không cần chủ thể dữ liệu đồng ý tại Điều 10.[32] Theo đó, dữ liệu cá nhân dù có nhạy cảm hay không cũng có thể bị tiết lộ, bị công bố, bị thông báo trên truyền thông, miễn là có quy định của pháp luật hoặc được cho là cần thiết vì lợi ích, an ninh quốc gia, trật tự an toàn xã hội; vì mục đích quốc phòng, an ninh, đạo đức xã hội hoặc theo quy định của các luật khác như Luật Báo chí... Tương tự, dữ liệu cá nhân sẽ được xử lí (khai thác, trích xuất, tổng hợp...) dù không cần có sự đồng ý của chủ sở hữu của dữ liệu, vì lợi ích an ninh quốc gia và trật tự xã hội; trong trường hợp khẩn cấp hay khi phục vụ điều tra, hay trường hợp khẩn cấp về tự do của chủ thể; tính mạng, sức khoẻ của chủ thể lẫn cộng đồng; phục vụ điều tra, xử lí hành vi vi phạm pháp luật, nghiên cứu khoa học, thống kê (sau khi đã khử thông tin nhận dạng cá nhân) hoặc theo quy định của pháp luật và các điều ước quốc tế.

Xem xét hướng dẫn thực hiện GDPR, và luật bảo vệ dữ liệu của Văn phòng Uỷ viên thông tin Vương quốc Anh (Information Commissioner's Office - ICO), ICO quy định có 07 trường hợp mà chính quyền cũng như chủ thể kiểm soát và xử lí thông tin có thể can thiệp dữ liệu cá nhân bao gồm các lĩnh vực:

- Tội phạm, các vấn đề pháp lí và bảo vệ công cộng;
- Quản lí, thẩm quyền của nghị viện và cơ quan tư pháp;
- Báo chí, nghiên cứu và lưu trữ thông tin công cộng;
- Y tế, công tác xã hội, giáo dục và vấn đề lạm dụng trẻ em;
- Tài chính và thuế vụ nói chung;
- Các tham chiếu và các bài thi;
- Yêu cầu truy cập thông tin có liên quan đến các cá nhân khác.

Trong đó, chủ thể dữ liệu hoàn toàn có thể biết được khi nào các cơ quan chức năng và bên cung cấp dịch vụ sẽ can thiệp vào những loại thông tin gì và quy trình can thiệp ra sao. Từ đó, họ sẽ có quyết định cung cấp và xử lí thông tin phù hợp khi bắt đầu sử dụng một dịch vụ nhất định. Trong trường hợp điều tra hay truy tố tội phạm, cơ quan nhà nước có quyền yêu cầu nhà cung cấp dịch vụ cung cấp thông tin, dựa trên cơ sở rằng quyền tự do cá nhân và quyền được thông báo về việc tiết lộ thông tin của cá nhân đã không còn hiệu lực. Bên cung cấp dịch vụ cũng có quyền từ chối dựa trên các quy định

[32] Dựa theo Dự thảo lần 2 được đăng tải trên: https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Du-thao-Nghi-dinh-quy-dinh-ve-bao-ve-du-lieu-ca-nhan-465185.aspx, truy cập 20/8/2022.

liên quan đến trình tự tư pháp trong trường hợp bên cung cấp dịch vụ cho rằng phía cơ quan nhà nước không thể cung cấp lí do thuyết phục cho việc trích xuất dữ liệu. Một ví dụ điển hình là các công ti cung cấp dịch vụ liên lạc, các mạng xã hội sẽ thiết lập chức năng cho người dùng chủ động xoá thông tin định kì (như các dòng chat, ảnh chat) hoặc các dữ liệu mà người dùng đã chủ động xoá bỏ trên hệ thống dữ liệu cloud... không được phép khôi phục, lưu trữ hay cung cấp cho bên thứ ba dưới bất kì hình thức nào.

Nhìn chung, hệ thống pháp luật bảo vệ dữ liệu của nhiều quốc gia hướng tới xây dựng một danh sách các ngoại lệ mang tính giới hạn, toàn diện (exhaustive list) thay vì hướng tới việc mở rộng thẩm quyền nhằm can thiệp tối đa đối với dữ liệu cá nhân. Do đó, trong quá trình hoàn thiện pháp luật điều chỉnh lĩnh vực bảo vệ dữ liệu, để tránh khả năng chồng chéo quy định, xung đột thẩm quyền trong lĩnh vực bảo vệ dữ liệu, Việt Nam cần cân nhắc điều chỉnh kĩ thuật lập pháp cũng như cách tiếp cận đối với các trường hợp được phép xử lí dữ liệu cá nhân hợp pháp, đặc biệt là các tình huống không đòi hỏi sự đồng ý của cá nhân. Danh mục hạn chế thẩm quyền dành cho chính quyền hay tổ chức kiểm soát, xử lí dữ liệu hay việc phân biệt chi tiết các nhóm quyền cá nhân của các đạo luật bảo vệ dữ liệu của các quốc gia trên thế giới sẽ cung cấp các gợi mở lập pháp có giá trị tham khảo cao cho Việt Nam.

Việt Nam sẽ phải cân nhắc các lợi ích, giá trị mà Việt Nam muốn ưu tiên bảo vệ, đảm bảo phù hợp với truyền thống văn hoá, quan niệm về quyền riêng tư, quyền bảo vệ dữ liệu trong xã hội.

Thứ ba, để đảm bảo giám sát tuân thủ việc bảo vệ dữ liệu cá nhân từ các công ti và tổ chức tư nhân, Việt Nam cần xây dựng cơ quan giám sát việc tuân thủ quy định bảo vệ dữ liệu cá nhân từ các công ti và tổ chức tư nhân.

Hiện nay theo Dự thảo Nghị định bảo vệ dữ liệu cá nhân cũng như trong các văn bản cùng lĩnh vực điều chỉnh về thông tin cá nhân đã ban hành các cơ chế để ngăn ngừa hành vi vi phạm bao gồm: *cơ chế tự bảo vệ của chủ thể dữ liệu; cơ chế yêu cầu chủ thể xâm phạm bồi thường thiệt hại; cơ chế xử phạt hành chính và cơ chế truy cứu trách nhiệm hình sự*. Tuy nhiên, điểm yếu của Dự thảo Nghị định hiện nay là chưa giải thích rõ thế nào là "tiết lộ dữ liệu" và có tiết lộ cho ai ngoài trường hợp tiết lộ cho công chúng (Điều 6). Mặt khác, trong trường hợp có vi phạm, chủ thể dữ liệu cần thực hiện các bước cụ thể như thế nào để xử lí kịp thời, ngăn chặn các hành vi xâm phạm dữ liệu bất hợp pháp. Với tính chất thông tin trên nền tảng trực tuyến có thể lan truyền với tốc độ nhanh chóng, các thiết chế can thiệp và ngăn chặn hành vi vi phạm phải được quy định để dễ dàng cho người dùng mạng internet đưa ra các yêu cầu bảo vệ hay thông báo sự vi phạm, khiếu nại sự vi phạm đến cơ quan có thẩm quyền giám sát, xử lí.

Ngoài ra, trong quá trình thành lập một cơ quan giám sát và bảo vệ dữ liệu cá nhân, Việt Nam nên tham khảo các mô hình cơ quan bảo vệ dữ liệu của các quốc gia trên thế giới, đặc biệt nghiên cứu cách thức nâng cao tính độc lập của cơ quan này, đảm bảo tính khách quan trong việc xem xét, giải quyết các khiếu nại vi phạm phù hợp quy định pháp luật.

Đối với mô hình GDPR, các cơ quan giám sát bảo vệ dữ liệu cá nhân cấp quốc gia ("national supervisory authority" hay "data protection authority" - DPAs) sẽ do nhà nước đó tự chọn mô hình và phương pháp hoạt động để thành lập, song quốc gia phải tuân thủ các nguyên tắc cơ bản của GDPR. Pháp luật EU cho phép cá nhân thực hiện các quyền bảo vệ dữ liệu cụ thể và bắt buộc các tổ chức (khu vực công hoặc tư nhân) xử lí dữ liệu của họ phải tôn trọng các quyền này dưới sự giám sát và giải quyết khiếu nại vi phạm của DPA.

Để việc thực thi luật bảo vệ dữ liệu có hiệu quả, các DPA được trao quyền điều tra, phát hiện và trừng phạt các hành vi vi phạm cũng như có trách nhiệm nâng cao nhận thức về các quyền và nghĩa vụ bảo vệ dữ liệu. Ở EU, tính hiệu quả này được củng cố bởi yêu cầu các DPA phải độc lập với chính phủ hoặc các bên khác, nghĩa là quyền ra quyết định của DPA độc lập với mọi ảnh hưởng trực tiếp hoặc gián tiếp từ bên ngoài. Yêu cầu tính độc lập DPA tại Điều 16.2 của Hiệp ước về hoạt động của EU (TFEU), Điều 8.3 của Hiến chương về các quyền cơ bản của EU, Chương VI của GDPR đã đưa ra các quy định chi tiết về việc thành lập và hoạt động của cơ quan giám sát độc lập, bao gồm quy định về các nguồn lực cần thiết để thực hiện hiệu quả các nhiệm vụ và quyền hạn của họ. Toà án Công lí EU luôn nhấn mạnh rằng sự kiểm soát, giám sát của một cơ quan độc lập là một yếu tố thiết yếu đảm bảo quyền bảo vệ dữ liệu và đã đặt ra các tiêu chí xem xét tính độc lập của DPA.

Ở Nhật Bản, Uỷ ban Bảo vệ thông tin cá nhân (PPC) được công nhận là nơi xử lí các khiếu nại về việc chủ thể xử lí dữ liệu vi phạm Đạo luật Bảo vệ thông tin cá nhân (sửa đổi). PPC của Nhật Bản bao gồm chủ tịch và tám thành viên, do Thủ tướng Chính phủ bổ nhiệm với sự đồng ý của Nghị viện Nhật Bản - cơ quan lập pháp lưỡng viện của Nhật Bản. Nhiệm kì của Chủ tịch và các thành viên là 5 năm, chủ tịch và các thành viên thực hiện quyền hạn của họ một cách độc lập và PPC có trách nhiệm báo cáo cho Nghị viện Nhật Bản.

Như vậy, tuỳ theo mô hình và cấu trúc quyền lực Nhà nước, mỗi quốc gia có cách thức xây dựng cơ quan giám sát và bảo vệ dữ liệu cá nhân khác nhau nhưng đảm bảo tuân thủ nguyên tắc hoạt động độc lập để việc giải quyết khiếu nại và giám sát khách quan. Ở Việt Nam, cơ quan DPA có thể được thiết lập thuộc bộ máy nhà nước, mang quyền lực công để đảm bảo thẩm quyền giải quyết các khiếu nại. Tuy nhiên, Việt Nam cần chú trọng việc bổ nhiệm các thành viên, trao quyền hạn độc lập để họ không bị chi phối trong việc thực hiện quyền hạn và hoàn toàn khách quan trong việc đưa ra các quyết định giải quyết khiếu nại. Điều này giúp đảm bảo tính hiệu quả và công bằng giữa các cá nhân và các tổ chức, công ti xử lí dữ liệu cá nhân ở khu vực tư lẫn việc hướng đến cả khu vực công trong việc xử lí dữ liệu cá nhân ở Việt Nam trong tương lai./.

TÀI LIỆU THAM KHẢO

1. Anirudh Burman, Upasana Sharma, Research Paper, "How Would Data Localization Benefit India?", Carnegie Endowment for International Peace, 2021, https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291

(Xem tiếp trang 102)