Working Paper 2022.1.5.02
- Vol 1, No 5

BẢO VỆ DỮ LIỆU CÁ NHÂN TRÊN NỀN TẢNG TRỰC TUYẾN TẠI NHẬT BẢN – KHUYẾN NGHỊ VỚI VIỆT NAM

Chu Thị Minh Anh[1]
Sinh viên K56 Tiếng Nhật thương mại – Khoa Tiếng Nhật
Trường Đại học Ngoại thương, Hà Nội, Việt Nam

Phạm Hạnh Vân
Sinh viên K57 Tiếng Nhật thương mại – Khoa Tiếng Nhật
Trường Đại học Ngoại thương, Hà Nội, Việt Nam

Đào Xuân Thủy
Giảng viên Khoa Luật
Trường Đại học Ngoại thương, Hà Nội, Việt Nam

Tóm tắt

Từ lâu, nhân quyền luôn là chủ đề thu hút sự chú ý của tất cả mọi người trên thế giới. Bên cạnh đó, trong thời buổi các mạng xã hội lên ngôi, các vấn đề liên quan đến không gian mạng và bảo vệ dữ liệu đã tạo ra mối quan tâm lớn cho các học giả tại nhiều quốc gia trên thế giới. Nhiều quốc gia trên thế giới đã ưu tiên ban hành các đạo luật về bảo vệ thông tin cá nhân nhằm đảm bảo quyền lợi của mỗi cá nhân cũng như chính quốc gia của họ. Tại Việt Nam, vấn đề này hiện đang nhận được sự quan tâm lớn, tuy nhiên vẫn chưa có một bộ luật chính thức nào về bảo vệ thông tin cá nhân được ban hành cũng như được tuyên truyền rộng rãi. Trong phạm vi nghiên cứu, bài viết này sẽ đưa ra phân tích về một số các Đạo luật về bảo vệ thông tin cá nhân cũng như các biện pháp bảo vệ dữ liệu cá nhân tại Nhật Bản, qua đó nhận xét, rút ra bài học kinh nghiệm và đưa một số kiến nghị để áp dụng tại Việt Nam.

Từ khóa: Bảo vệ dữ liệu cá nhân, quyền riêng tư, Đạo luật bảo vệ thông tin cá nhân của Nhật Bản (APPI).

PROTECTION OF PERSONAL DATA ON ONLINE PLATFORM IN JAPAN – RECOMMENDATION TO VIETNAM

Abstract

Human rights has always been the topic that draws the attention of people all around the world. Besides, in the thriving era of SNS, issues that related to cyberspace and data protection have been a great concern for scholars and many countries around the world. Many countries around the world have been prioritizing the enactment of laws on the protection of personal information in

[1] Tác giả liên hệ, email: minhanh7898@gmail.com

order to ensure the rights of each individual as well as national security. In Vietnam, this issue is currently receiving great attention, but there is still no official law on protection of personal information that has been regulated or widely propagated. Within the scope of the research, this article will provide some analysis of the Personal Information Protection Acts as well as personal data protection measures that have been taken in Japan, thereby giving opinion and conclusions, as well as supplemental recommendations to apply in the case of Vietnam.

Keywords: Personal data protection, privacy right, Act for Protection of Personal Information (APPI).

Mở đầu

Khi nói đến Nhật Bản, người ta thường nghĩ ngay tới một quốc gia có nền văn hóa Á Đông lâu đời song song với sự hiện đại đi đầu đối với những đổi mới của nhân loại. Đối với quá trình lập pháp cũng như xuyên suốt lịch sử pháp luật, hệ thống pháp luật Nhật Bản cũng có sự kết hợp hài hòa giữa truyền thống, đạo đức và những ảnh hưởng tiến bộ của pháp luật phương Tây, tạo ra bước tiền đề vững chắc cho quá trình hội nhập và phát triển. Trong một xã hội phát triển, mỗi cá nhân đều tự ý thức được các quyền cơ bản của họ và quyền riêng tư hiện nay đã trở thành mối quan tâm hàng đầu. Tuy nhiên, sự hiểu biết về khái niệm và tầm quan trọng của quyền riêng tư không thật sự phổ quát và có sự đồng nhất. Điều này có thể được lý giải do sự khác biệt về văn hóa, kinh tế và xã hội theo từng vùng lãnh thổ. Đối với người Nhật Bản, trước đây, họ thường nhìn nhận khái niệm quyền riêng tư một cách chủ quan và ít coi trọng quyền này hơn các quốc gia phương Tây. Đối với người Nhật, quyền riêng tư là một ý tưởng đến từ các nước phương Tây, một số người cảm thấy rằng ý thức về quyền riêng tư có thể mang tính chủ quan vì nó có nghĩa là bất cứ ai cũng có thể tự ý từ chối sự can thiệp của người khác. Mặt khác, để thích ứng với sự phát triển của một xã hội thông tin, Đạo luật về bảo vệ dữ liệu cá nhân được ban hành tại Nhật Bản vào tháng 4 năm 2005. Đạo luật này đã giúp nhiều người ở Nhật Bản hiểu giá trị của việc bảo vệ dữ liệu cá nhân và tầm quan trọng của nó. Đồng thời, các tổ chức kinh doanh cũng như Chính phủ cũng quản lý đúng cách dữ liệu cá nhân mà họ có thể thu thập và lưu trữ trong cơ sở dữ liệu.

Thêm nữa, Nhật Bản cũng là quốc gia đầu tiên cải cách nền kinh tế thông qua chính sách mở cửa toàn bộ nền kinh tế với các nước phương Tây. Nhờ đó mà quốc gia này đã trở thành quốc gia có trình độ hiện đại hóa cao nhất châu Á. Cho tới nay Nhật Bản vẫn được coi là một trong số các cường quốc có thể sánh ngang với các quốc gia ở châu Âu. Chính vì thế, Việt Nam có thể học hỏi được rất bài học trong cả trong kinh tế, văn hóa, giáo dục và cả luật pháp của đất nước Nhật Bản.

Trong thời điểm vừa qua, dịch bệnh Covid-19 đã tác động lớn đến nền kinh tế thị trường trên toàn thế giới. Vì thế, mọi hoạt động không thể diễn ra trực tiếp mà phải thông qua mạng máy tính, Internet để duy trì các hoạt động như làm việc, học tập, kinh doanh buôn bán. Điều này đã tạo ra sự thay đổi lớn về nhận thức và tiếp nhận thông tin từ nền tảng trực tuyến của mọi người. Một vấn đề quan trọng không thể bỏ qua là việc bảo vệ dữ liệu cá nhân trên nền tảng này. Chính vì vậy, bài nghiên cứu này sẽ cung cấp một cái nhìn tổng quan về bảo vệ dữ liệu cá nhân trên nền tảng trực tuyến, từ đó nâng cao nhận thức về an toàn cá nhân trên không gian mạng cũng như có thêm những đóng góp để xây dựng pháp luật ngày càng chặt chẽ hơn tại Việt Nam.

1. Khái quát về dữ liệu cá nhân và bảo vệ dữ liệu cá nhân

1.1. Khái niệm dữ liệu cá nhân

Trong thời đại công nghệ số lên ngôi, với sự ra đời của nhiều thiết bị máy móc, điện tử, vi tính và đặc biệt là không gian mạng đã tạo nên cuộc cách mạng về dữ liệu số. Trong bối cảnh đó, nhiều mối lo ngại đến vấn đề bảo mật dữ liệu cá nhân cũng như dữ liệu được trao đổi giữa các quốc gia.

Theo quy định của Đạo luật bảo vệ thông tin cá nhân của Nhật Bản (APPI), Dữ liệu cá nhân được định nghĩa là thông tin cá nhân nằm trong một cơ sở dữ liệu thông tin cá nhân. Một cơ sở dữ liệu thông tin cá nhân là tập hợp thông tin, bao gồm:

a. Tập hợp thông tin được sắp xếp một cách có hệ thống theo cách cho phép thông tin cá nhân cụ thể được lấy ra bằng máy tính.

b. Bất kỳ việc thu thập thông tin nào khác được quy định trong Nghị định của Chính phủ được sắp xếp một cách có hệ thống theo một cách cho phép cụ thể để thông tin cá nhân dễ dàng được tìm kiếm.

Trong đó, thông tin cá nhân là thông tin về một cá nhân sống thuộc bất kỳ các mục sau đây:

a. Thông tin có chứa tên, ngày sinh hoặc các mô tả khác, theo đó một cá nhân cụ thể có thể được xác định (bao gồm thông tin cho phép dễ dàng tham khảo cho phép nhận dạng cá nhân);

b. Thông tin chứa mã nhận dạng cá nhân, là mã, bao gồm các ký tự, ký tự số và dấu, có thể được sử dụng để xác định cá nhân cụ thể và được quy định trong Nghị định của Chính phủ quy định về việc thực hiện Luật sửa đổi, bổ sung ban hành tháng 12 năm 2016 (Ví dụ: định danh sinh trắc học như dữ liệu vân tay, dữ liệu nhận dạng, hộ chiếu hoặc số giấy phép lái xe) (Lê, 2020).

1.2. Các biện pháp bảo vệ dữ liệu cá nhân

Các biện pháp bảo vệ dữ liệu cá nhân là những biện pháp phòng ngừa, phát hiện, ngăn chặn, xử lý các hành vi xâm phạm quy định của pháp luật về dữ liệu cá nhân. Các biện pháp này tại mỗi quốc gia được bảo vệ ở những mức độ khác nhau tùy vào những quy định cụ thể. Trong phạm vi bài viết, tác giả trình bày các biện pháp bảo vệ dữ liệu cá nhân tuân theo Quy định bảo vệ dữ liệu chung của EU (GDPR). Đây là các biện pháp được áp dụng phổ biến tại nhiều các quốc gia trên thế giới với rất nhiều ưu điểm nổi bật.

Chính sách về bảo vệ dữ liệu cá nhân tuân theo GDPR chỉ được áp dụng cho việc xử lý dữ liệu cá nhân tuân theo Quy định Bảo vệ dữ liệu chung 2016/679 của Liên Minh Châu Âu.

Xử lý "dữ liệu cá nhân" trong chính sách này có nghĩa là xử lý dữ liệu cá nhân của chủ thể dữ liệu nằm trong Khu vực Kinh tế Châu Âu (EEA) (Softbank, 2021).

a. Thu thập và xử lý dữ liệu cá nhân

Quá trình thu thập và xử lý dữ liệu cá nhân của chủ thể dữ liệu dựa trên bất kỳ cơ sở pháp lý được quy định trong Điều 6 và 7 trong GDPR. Ngoài ra, đối với xử lý dữ liệu cá nhân cần được xem xét đặc biệt theo các tiêu chuẩn đặc biệt sẽ được quy định trong Điều 9 và Điều 10 GDPR. Khi các công ty muốn thu thập và xử lý dữ liệu cá nhân, họ sẽ phải thông báo cho chủ thể dữ liệu về mục đích thu thập và xử lý dữ liệu cá nhân bằng một thông báo, hợp đồng hoặc các phương tiện thích hợp khác khi được sự đồng ý. Chủ thể dữ liệu có quyền rút lại sự đồng ý của mình bất cứ lúc nào nếu họ không đồng ý với việc thu thập và xử lý dữ liệu cá nhân.

b. Chia sẻ dữ liệu cá nhân

Với sự đồng ý trước của chủ thể dữ liệu, dữ liệu cá nhân sẽ được chuyển, lưu trữ và xử lý thêm bởi các chủ thể để cung cấp sản phẩm và dịch vụ hoặc hỗ trợ tiếp thị cho chủ thể dữ liệu.

Theo yêu cầu của các tổ chức công và cơ quan chính phủ trong và ngoài nước, công ty nắm giữ dữ liệu cá nhân có thể được yêu cầu tiết lộ dữ liệu cá nhân để phục vụ cho luật pháp, các thủ tục pháp lý, thủ tục tố tụng và nơi cư trú của chủ thể dữ liệu. Việc tiết lộ dữ liệu cá nhân là cần thiết hoặc thích hợp vì lý do an ninh quốc gia, thực thi pháp luật hoặc các vấn đề xã hội quan trọng khác. Công ty nắm giữ cũng có thể tiết lộ dữ liệu cá nhân của chủ thể nhằm bảo vệ quyền lợi của chính mình cũng như tìm kiếm các biện pháp khắc phục có sẵn, thực thi các quy tắc nội bộ điều tra gian lận hoặc bảo vệ doanh nghiệp và người dùng của công ty.

Trong trường hợp chia sẻ và tiết lộ dữ liệu cá nhân như được mô tả ở trên, có thể sẽ cần phải chuyển dữ liệu cá nhân đến một quốc gia khác ngoài EEA. Mỗi lần thực hiện việc chuyển giao như vậy, dữ liệu chuyển giao sẽ được bảo vệ ở mức độ thích hợp. Đặc biệt, việc này sẽ được thực thi bằng cách ký kết các điều khoản hợp đồng tiêu chuẩn như được xác định trong các quyết định của Ủy ban Châu Âu 2001/497/EC, 2002/16/EC, 2004/915/EC và 2010/87/EU.

c. Các hồ sơ liên quan đến việc xử lý dữ liệu cá nhân

Khi xử lý dữ liệu cá nhân, các hồ sơ liên quan đến việc xử lý dữ liệu cá nhân theo các nghĩa vụ được quy định tại Điều 30 trong GDPT sẽ được ghi lại tất cả những thông tin cần thiết để tuân thủ theo như GDPR để hợp tác với cơ quan giám sát theo điều 31 trong GDPR.

d. Các biện pháp an ninh

Trong quá trình xử lý dữ liệu cá nhân, công ty nắm giữ dữ liệu cá nhân sẽ thực hiện các biện pháp kỹ thuật và tổ chức để đảm bảo an ninh phù hợp (Như việc xử lý trái phép/bất hợp pháp, bảo vệ chống mất mát và phá hủy, gây thiệt hại ngẫu nhiên,…) (Theo Điều 25 và khoản 1 Điều 32 của GDPR).

e. Thông báo về vi phạm dữ liệu cá nhân cho cơ quan giám sát có thẩm quyền

Trong trường hợp phát hiện những hành vi vi phạm bảo mật dẫn đến việc vô tình hoặc cố ý thực hiện hành vi bất hợp pháp như phá hủy, gây mất mát, có sự thay đổi, tiết lộ hoặc truy cập trái phép dữ liệu cá nhân để chuyển giao, lưu trữ hoặc các hoạt động xử lý dữ liệu cá nhân khác, công ty nắm giữ dữ liệu cá nhân sẽ có những hệ thống và biện pháp tại chỗ để đánh giá. Tùy thuộc vào kết quả đánh giá, cơ quan giám sát sẽ được thông báo và liên hệ với đối tượng dữ liệu bị ảnh hưởng (Theo Điều 33 và 34 của GDPR).

2. Quy định về bảo vệ dữ liệu cá nhân tại Nhật Bản

2.1. Đạo luật bảo vệ thông tin cá nhân của Nhật Bản (APPI)

Tại Nhật Bản, việc bảo vệ các vấn đề về quyền riêng tư cá nhân của công dân được điều chỉnh bởi Đạo luật về Bảo vệ Thông tin Cá nhân (APPI).

APPI cung cấp nguồn luật và tiêu chuẩn về quyền riêng tư cũng như vấn đề bảo vệ dữ liệu. Trong đó bao gồm định nghĩa về thông tin cá nhân, cơ sở dữ liệu thông tin cá nhân, việc người điều hành kinh doanh xử lý thông tin cá nhân, dữ liệu cá nhân, thông tin được xử lý ẩn danh, thông tin được xử lý bằng bút danh, thông tin cá nhân nhạy cảm.

Kể từ khi được phê duyệt vào tháng 5 năm 2003, APPI đã trải qua 2 đợt sửa đổi, gần đây nhất là sửa đổi 2020 đã đưa có những cải biến thích hợp để thống nhất một số quy định chung với

GDGR của Châu Âu về bảo vệ quyền riêng tư cá nhân trong đó bao gồm cả những nghĩa vụ của doanh nghiệp đối với việc thu thập, sử dụng và bảo mật thông tin, dữ liệu người dùng. Dưới đây là một số nội dung cơ bản của APPI.

● ***Thông tin cá nhân và dữ liệu thông tin cá nhân***

APPI đưa ra một số định nghĩa liên quan đến quyền riêng tư và vấn đề bảo vệ dữ liệu. Trong đó, phạm vi "Thông tin cá nhân" bao gồm (Lê, 2020):

(a) Thông tin về một cá nhân đang sống và có thể nhận dạng người đó bằng tên, ngày sinh, các mô tả khác;

(b) Thông tin về một người còn sống có chứa mã nhận dạng cá nhân, nghĩa là bất kỳ ký tự, chữ cái, số, ký hiệu hoặc các mã khác.

Các mã nhận dạng cá nhân thuộc một trong hai trường hợp sau:

(1) Thông tin giúp xác định một cá nhân cụ thể, dưới dạng một ký tự, chữ cái, số, ký hiệu hoặc các mã khác chứa thông tin về toàn bộ hoặc một phần đặc điểm của cá nhân cụ thể để cung cấp cho hệ thống dữ liệu máy tính, bao gồm dữ liệu DNA, dữ liệu nhận dạng khuôn mặt, dữ liệu giọng nói, dữ liệu mẫu dáng đi, dữ liệu lòng bàn tay/ ngón tay/ dấu vân tay, mô hình tĩnh mạch;

(2) Những ký tự, chữ cái, số, ký hiệu hoặc các mã khác được gán liên quan đến việc sử dụng dịch vụ, mua bán hàng hóa cung cấp cho một cá nhân, hoặc được cấp, ghi lại bằng điện từ trong thẻ, những tài liệu khác được cấp cho một cá nhân nhằm xác định một người dùng hoặc người mua cụ thể, ví dụ như số hộ chiếu, số lương hưu, giấy phép lái xe và số bảo hiểm y tế.

"Cơ sở dữ liệu thông tin cá nhân" là tập hợp thông tin bao gồm:

(a) Tập hợp thông tin được sắp xếp một cách có hệ thống theo cách mà thông tin cá nhân cụ thể có thể được truy xuất bằng máy tính; hoặc

(b) bất kỳ việc thu thập thông tin nào khác được quy định trong Nghị định của Chính phủ được sắp xếp một cách có hệ thống theo một cách cho phép cụ thể để thông tin cá nhân dễ dàng được tìm kiếm.

Ban đầu, APPI không có định nghĩa về "Thông tin nhạy cảm", tuy nhiên các sửa đổi 2017 đã cung cấp định nghĩa rõ ràng hơn về loại thông tin này, bao gồm những thông tin liên quan đến các vấn đề như chủng tộc, tín ngưỡng, địa vị xã hội, hồ sơ phạm tội trong quá khứ hoặc bất kỳ thông tin nào khác có thể trở thành đối tượng của sự phân biệt đối xử trong xã hội. Ngoài ra, các điều khoản trong Đạo luật cũ đã không yêu cầu cụ thể nào về sự cho phép của chủ thể dữ liệu, nhưng APPI sửa đổi thì yêu cầu rõ ràng một nhà quản lý doanh nghiệp xử lý dữ liệu cần có được sự cho phép trước khi thu thập các loại thông tin nhạy cảm, ngoại trừ một vài trường hợp (Ishiara, 2021).

● ***Nghĩa vụ đối với người xử lý dữ liệu***

Theo điều 15 APPI, một doanh nghiệp xử lý thông tin cá nhân khi xử lý thông tin, dữ liệu cá nhân có nghĩa vụ phải giải thích một cách cụ thể mục đích sử dụng dữ liệu đó. Luật cũng quy định rõ doanh nghiệp hạn chế cung cấp dữ liệu cho bên thứ 3 và phải thông báo công khai các vấn đề liên quan đến dữ liệu cá nhân được lưu trữ.

Nếu một nhà quản lý doanh nghiệp xử lý thông tin cá nhân được một cá nhân yêu cầu sửa, thêm hoặc xóa những dữ liệu cá nhân đang lưu trữ có khả năng nhận dạng danh tính của họ trên cơ sở dữ liệu đó là không chính xác, người quản lý doanh nghiệp phải tiến hành điều tra ngay lập

tức trong phạm vi cần thiết để đạt được mục đích sử dụng và trên cơ sở kết quả thu được, tiến hành chỉnh sửa, thêm hoặc xóa dữ liệu lưu trữ, trừ khi có thủ tục đặc biệt được quy định bởi luật hay quy định nào khác về việc sửa chữa, bổ sung hoặc xóa bỏ dữ liệu này (Điều 29 Đạo luật về bảo vệ thông tin cá nhân 2021).

Ngoài một vài ngoại lệ theo quy định trong APPI, doanh nghiệp cần có sự cho phép trước để chuyển thông tin cá nhân cho bên thứ ba. Tuy trước đó APPI không có quy định cụ thể nào về việc cung cấp liên quan đến việc chuyển giao dữ liệu quốc tế trong APPI trước đây. Để đối phó với sự toàn cầu hóa việc chuyển giao dữ liệu, APPI yêu cầu phải có sự cho phép của của cơ quan có thẩm quyền đối với việc lưu chuyển quốc tế các dữ liệu cá nhân, ngoại trừ các trường hợp sau đây (Điều 24 Đạo luật về bảo vệ thông tin cá nhân 2021):

a. Chuyển giao quốc tế dữ liệu cá nhân cho một bên thứ ba (ở nước ngoài) có hệ thống tuân theo các tiêu chuẩn, quy tắc đề ra bởi PPC (Có nghĩa đã thực hiện các biện pháp phù hợp tuân thủ theo quy định của APPI hoặc được công nhận là đối tượng được phép thu nhận dữ liệu cá nhân theo các tiêu chuẩn quốc tế về bảo mật thông tin cá nhân, chẳng hạn như chứng nhận bởi Quy tắc về quyền riêng tư xuyên biên giới của Liên minh Châu Á - Thái Bình Dương).

b. Theo quy định của Ủy ban PPC, việc chuyển giao dữ liệu cá nhân quốc tế cho bên thứ ba ở nước ngoài được coi như đã thiết lập hệ thống bảo vệ thông tin cá nhân với các tiêu chuẩn tương đương tại Nhật Bản liên quan đến sự bảo vệ các quyền và lợi ích của mỗi cá nhân.

Theo các quy tắc chung về xử lý dữ liệu cá nhân, người xử lý thông tin cần phải (Điều 18 Đạo luật về bảo vệ thông tin cá nhân 2021):

(i) chỉ ra mục đích của việc xử lý thông tin cá nhân (hay "mục đích sử dụng") một cách rõ ràng;

(ii) không được thay đổi mục đích sử dụng nằm ngoài phạm vi có mối quan hệ thay thế chính đáng với mục đích sử dụng ban đầu;

(iii) không được xử lý thông tin cá nhân nằm ngoài phạm vi cần thiết để đạt được các mục đích mà không có sự cho phép trước của chủ thể dữ liệu.

Người nắm giữ và xử lý dữ liệu sẽ không được chuyển thông tin cá nhân cho một bên thứ ba mà không có sự đồng ý trước của chủ thể dữ liệu.

Tuy nhiên, có một số ngoại lệ đối với quy định này, chẳng hạn như:

(i) việc tiết lộ căn cứ vào luật Nhật Bản;

(ii) việc tiết lộ là cần thiết để hợp tác với một tổ chức chính phủ Nhật Bản nhằm thực hiện các nghĩa vụ pháp lý của mình và để có được sự cho phép của một chủ thể dữ liệu có khả năng cản trở việc đó;

(iii) tiết lộ vì mục đích sức khỏe hoặc vệ sinh công cộng và rất khó để có được sự cho phép;

(iv) tiết lộ là một phần của sự hợp nhất hoặc việc thừa kế kinh doanh, tùy thuộc việc nó có được sử dụng cho các mục đích sử dụng giống nhau hay không;

(v) việc tiết lộ là cho một bên thứ ba xử lý;

(vi) việc tiết lộ là cho một bên khác sử dụng chung và chủ thể dữ liệu đã được thông báo;

(vii) người xử lý thông tin thông báo cho chủ thể dữ liệu về việc sẽ chuyển giao, cung cấp thông tin cho bên thứ ba và các chủ thể dữ liệu đó không phản đối (điều kiện này chính là trường hợp "miễn trừ các quyết định không tham gia").

Theo APPI , bên xử lý dữ liệu được yêu cầu thực hiện các biện pháp cần thiết và thích hợp nhằm đảm bảo an toàn thông tin cá nhân. Việc lựa chọn biện pháp thích hợp sẽ tùy thuộc vào bản chất, phạm vi, bối cảnh cũng như mục đích của việc sử dụng hoặc xử lý những dữ liệu cá nhân có liên quan cũng như các rủi ro đối với quyền và tự do của cá nhân.

Trong văn bản hướng dẫn của APPI là các nguyên tắc chung về Luật Bảo vệ thông tin cá nhân tháng 11/2017 đã cung cấp một số chỉ dẫn về nghĩa vụ bắt buộc đối với người xử lý dữ liệu như: (i) có chính sách bảo mật cơ bản; (ii) có các quy tắc nội bộ và sự sắp xếp các tài liệu nội bộ khác được đưa ra nhằm bảo vệ dữ liệu cá nhân; (iii) có cấu trúc tổ chức sắp đặt nhằm bảo vệ dữ liệu cá nhân (ví dụ như bổ nhiệm một cán bộ chuyên bảo vệ dữ liệu); (iv) giáo dục đầy đủ cho các cán bộ nhân viên của mình về các yêu cầu đối với việc bảo vệ dữ liệu; (v) có hệ thống an ninh vật lý thích hợp; và (vi) thực hiện các biện pháp thích hợp liên quan đến hệ thống công nghệ thông tin. Bởi bên xử lý dữ liệu được yêu cầu thực hiện các biện pháp cần thiết và thích hợp nhằm bảo mật thông tin cá nhân nên tất yếu sẽ phải tiến hành kiểm tra các biện pháp an ninh dữ liệu của họ một cách thường xuyên.

● ***Quyền của chủ thể dữ liệu***

Bên nắm giữ và xử lý dữ liệu được yêu cầu cung cấp cho chủ thể dữ liệu những thông tin sau (và phải trả lời yêu cầu của chủ thể dữ liệu về thông tin đó ngay lập tức): (i) tên của bên xử lý thông tin; (ii) mục đích sử dụng thông tin cá nhân của chủ thể dữ liệu; (iii) thủ tục nhằm yêu cầu quyền truy cập các thông tin cá nhân do người xử lý thông tin nắm giữ (gồm số tiền của bất kỳ khoản phí nào phải trả); và (iv) chi tiết bên cần liên hệ nếu muốn khiếu nại về việc xử lý thông tin cá nhân của họ. Người xử lý thông tin khi đã có được thông tin cá nhân cũng phải nhanh chóng thông báo cho chủ thể dữ liệu mục đích sử dụng thông tin cá nhân của mình, trừ trường hợp mục đích sử dụng đã được tiết lộ công khai. Trường hợp khi một người xử lý dữ liệu đã chuyển đổi mục đích sử dụng thì được yêu cầu phải thông báo đến các chủ thể dữ liệu mục đích thay đổi hoặc công bố công khai mục đích đó (Điều 29 Đạo luật về bảo vệ thông tin cá nhân 2021).

Chủ thể dữ liệu có thể yêu cầu một người xử lý thông tin ngừng sử dụng hoặc xóa thông tin cá nhân của họ nếu thông tin cá nhân đó đang được sử dụng ngoài phạm vi mục đích sử dụng có sự cho phép của họ hoặc đã được thu thập bằng cách gian lận (Điều 17 Đạo luật về bảo vệ thông tin cá nhân 2021).

2.2. Bảo vệ quyền riêng tư cá nhân trên nền tảng trực tuyến

Quyền riêng tư trên nền tảng trực tuyến thuộc một phần quyền riêng tư dữ liệu, liên quan đến việc lưu trữ, hiển thị và cung cấp cho bên thứ ba thông tin liên quan đến cá nhân thông qua các nền tảng trực tuyến (Wheeler, 2017). Hiện nay, dữ liệu thông tin của người dùng đều có thể được thu thập trên nhiều nền tảng mạng xã hội phổ biến như Facebook, Google, Apple hay hệ thống GPS. Sự phát triển của truyền thông kỹ thuật số đã tạo điều kiện để một lượng lớn dữ liệu thông tin có thể được tổng hợp và lưu trữ trên hệ thống cơ sở máy chủ. Những thông tin này sau đó sẽ được phân tích, đánh giá và diễn giải bởi những nhà khoa học dữ liệu để xây dựng cơ sở thông tin về xu hướng và nhân khẩu học của người dùng.

Có thể thấy rằng đối với người dùng trực tuyến, việc cung cấp và chia sẻ những thông tin cá nhân trên những nền tảng này tiềm ẩn những nguy cơ bị xâm phạm quyền riêng tư. Các công ty cung cấp mạng xã hội và các dịch vụ trên mạng có khả năng bán cho bên thứ ba hoặc sử dụng vì mục đích kinh doanh khác như lập hồ sơ nhân khẩu học chi tiết của người dùng dịch vụ đó, ngay cả khi không được người dùng trực tiếp bày tỏ hoặc chỉ định (Kosinski, Stillwell & Graepel, 2013). Các thông tin được lưu trữ trên các nền tảng này như thông tin hình ảnh, tin nhắn cũng có khả năng bị người dùng khác sử dụng khi chưa được phép của chủ thể dữ liệu, dẫn đến việc xúc phạm nhân phẩm hay lan truyền các tin đồn vu khống và để lại hậu quả dài hạn đối với chủ thể dữ liệu đó.

Năm 2019, mạng xã hội lớn nhất thế giới Facebook tuyên bố có ý định hợp nhất những nền tảng thuộc quyền sở hữu của mình như Whatsapp, Instagram, Facebook và Messenger nhằm nâng cao trải nghiệm của người dùng. Xoay quanh tuyên bố này tồn tại nhiều ý kiến trái chiều cho rằng điều này giúp ổn định đồng thời phát triển mạnh mẽ mảng kinh doanh quảng cáo của Facebook. Nguồn dữ liệu khổng lồ có được từ những nền tảng này có thể được kết nối nhằm tạo ra một "nhân dạng" người dùng duy nhất để cung cấp cho các công ty quảng cáo một cách riêng biệt (Williams, 2019).

Nghiên cứu về quyền riêng tư cũng đã chỉ ra rằng trên thực tế, hầu hết người dùng không nhận ra việc hạn chế quyền truy cập dữ liệu không giải quyết được đầy đủ các rủi ro do số lượng, chất lượng và tính lâu dài của những dữ liệu họ cung cấp (Debatin, Lovejoy, Horn & Hughes, 2009). Suy cho cùng, việc hạn chế hiển thị hồ sơ cho bạn bè trên các nền tảng mạng xã hội chỉ đơn giản là hạn chế nó trong phần nổi của tảng băng. Nếu người dùng tiếp tục cung cấp cho phần chìm của tảng băng các dữ liệu cá nhân của mình một cách tự nguyện, thì quyền riêng tư của họ sẽ luôn có nguy cơ bị xâm phạm.

Vào tháng 12 năm 2019, Cơ quan quản lý cạnh tranh của Nhật Bản (Japan Fair Trade Commission) đã đưa ra hướng dẫn thi hành Luật chống độc quyền và các quy định liên quan ("Hướng dẫn JFTCN"). Theo các hướng dẫn của JFTC, khi các nền tảng kỹ thuật số thu thập và sử dụng lịch sử duyệt web hoặc thông tin định vị mà không thông báo việc sử dụng thông tin đó theo cách có thể xác định danh tính một người cụ thể nào đó thì có thể bị coi là đang lạm dụng quyền thương lượng vượt trội hơn của mình.

Trong hoạt động marketing qua Email, ARTSEM (Đạo luật về các quy tắc trao đổi thư điện tử xác định, 2002) quy định rằng người bán hàng hoặc các doanh nghiệp có thể gửi Email tiếp thị trực tiếp cho các thuê bao cá nhân với điều kiện có sự đồng ý của người nhận thông tin đó, trừ các trường hợp : (i) người nhận thông báo cho người gửi địa chỉ Email của mình bằng văn bản; (ii) người nhận mối quan hệ kinh doanh với một người khác tham gia vào công việc bán hàng liên quan đến tiếp thị; hoặc (iii) người nhận là một tổ chức hoặc một cá nhân hoạt động kinh doanh cung cấp địa chỉ thư điện tử của mình trên Internet.

Ngoài ra, theo ASCT (Đạo luật về các giao dịch thương mại cụ thể, 1976), việc gửi Email cho mục đích tiếp thị trực tiếp mà không cần sự đồng ý liên quan đến một số loại giao dịch bán hàng là hợp pháp nếu như: (i) Email để tiếp thị trực tiếp được gửi cùng với những thông báo về các vấn đề quan trọng liên quan đến hợp đồng; hoặc (ii) Email nhằm mục tiếp thị trực tiếp như vậy được gửi cùng với các email từ các nhà cung cấp email miễn phí, chẳng hạn như Yahoo! hoặc Google.

Người gửi Email phải được nhận dạng qua việc cung cấp tên và địa chỉ của mình. Người gửi cũng cần cung cấp cho người nhận quyền từ chối nhận các email tiếp thị khác trong tương lai và cung cấp địa chỉ email hoặc URL để họ thực hiện quyền từ chối của mình.

Tại Việt Nam, vào ngày 09/02/2021, Bộ Công an đã hoàn thành dự thảo Nghị định quy định về bảo vệ dữ liệu cá nhân để lấy ý kiến đóng góp của các cơ quan, tổ chức, cá nhân. Dự thảo Nghị định gồm 06 chương 30 điều, áp dụng đối với cơ quan, tổ chức, cá nhân có liên quan tới dữ liệu cá nhân.

Trước khi nghị định được đóng góp và ban hành thì hầu hết người dùng trực tuyến đều phải tự trang bị cho mình kiến thức chung về việc tự bảo vệ dữ liệu cá nhân trên các nền tảng trực tuyến. Ví dụ như đã có nhiều bài báo, trang mạng có đưa ra khuyến cáo người dùng Internet không nên đưa thông tin cá nhân của mình lên mạng xã hội, hoặc chấp nhận các trình duyệt, cookie không rõ nguồn gốc... Tuy nhiên, phần đông người dùng không đủ kiến thức cũng như nhận thức về quyền riêng tư của mình đang bị xâm phạm, chính vì vậy họ cũng không biết mình đã mắc phải những chiếc bẫy tinh vi trên mạng xã hội và các phần mềm trực tuyến. Họ cũng không rõ thông tin của mình đã bị rò rỉ hay đánh cắp bởi những hackers hay những phần mềm độc hại. Chính vì thế mà trong nhiều năm qua, cư dân mạng tại Việt Nam đã phải trải qua nhiều vụ việc gây bức xúc có liên quan đến quyền riêng tư và tài khoản cá nhân. Điều này vừa là nguyên nhân cũng vừa là động lực cho các Bộ, ban, ngành tại Việt Nam nhanh chóng đốc thúc để đưa ra những chính sách về an toàn cá nhân cũng như bảo vệ dữ liệu cá nhân trên nền tảng trực tuyến để chủ động bảo vệ người dùng Internet trên toàn quốc.

3. Một số kiến nghị đối với việt nam về việc bảo vệ dữ liệu cá nhân trên nền tảng trực tuyến

3.1. Đặt ra quy định bắt buộc dành cho doanh nghiệp trong việc quản lý thông tin cá nhân

Tại Việt Nam, tình trạng mua bán dữ liệu cá nhân hiện nay xuất hiện tràn lan trên các mạng xã hội, dẫn đến việc kẻ xấu giả mạo cơ quan công an, kiểm sát, tòa án, ngân hàng, điện lực để lừa đảo nhân dân bằng nhiều hình thức khác nhau. Nhiều dịch vụ trên không gian mạng có hoạt động thu thập, khai thác, phân tích thông tin, dữ liệu cá nhân như mạng xã hội, thanh toán trực tuyến, thương mại điện tử, trò chơi trực tuyến,... nhưng không có cơ chế quản lý dữ liệu người dùng an toàn. Các cơ quan, tổ chức, doanh nghiệp chưa có các biện pháp bảo mật thông tin đồng bộ, hiệu quả; hệ thống lưu trữ và xử lý thông tin cá nhân còn tồn tại những lỗ hổng bảo mật dễ bị hacker khai thác, tấn công, gây thiệt hại lớn. Rồi hiện tượng lộ, lọt, đánh cắp, buôn bán thông tin cá nhân một cách công khai trên không gian mạng cũng thường xuyên diễn ra, như vụ việc vừa xảy ra gần đây là thông tin chứng minh nhân dân của gần 10.000 người Việt bị đem rao bán, thách thức các cơ quan thi hành pháp luật (Lê, 2021).

Do vậy, cần xây dựng luật riêng để quy định cho các doanh nghiệp trong nước, nhằm bảo vệ các thông tin cá nhân cũng như dữ liệu cá nhân, tránh những trường hợp xâm phạm một cách bất hợp pháp. Đối tượng áp dụng chủ yếu trong đạo luật này là các công ty, doanh nghiệp, cơ quan, tổ chức bởi đây là nguồn lưu trữ số lượng lớn thông tin cá nhân, pháp nhân của các khách hàng và doanh nghiệp khác.

Hiện nay, dự thảo quy định về dữ liệu cá nhân tại Việt Nam đã được đưa ra, tuy nhiên vẫn chưa có điều luật dành riêng cho các doanh nghiệp về quy định bảo mật dữ liệu cũng như các biện

pháp xử lý vi phạm quy định về xử lý dữ liệu cá nhân. Một khuyến nghị khác liên quan đến quá trình thực thực thi và chế tài xử lý các hành vi vi phạm quy định về việc bảo vệ dữ liệu cá nhân.

3.2. Truy xuất nguồn gốc thông tin cá nhân thu được

Dựa trên những sửa đổi của APPI về nâng cao mức độ bảo vệ thông tin cá nhân, theo đó có thể đưa một số những điều sau vào nghị định của Việt Nam để áp dụng:

Thứ nhất, đặt ra các nghĩa vụ đối với các nhà điều hành kinh doanh xử lý cá nhân để lập và lưu giữ hồ sơ chính xác trong một thời gian nhất định khi họ cung cấp cho bên thứ ba thông tin cá nhân.

Thứ hai, đặt ra nghĩa vụ đối với các nhà điều hành kinh doanh xử lý thông tin cá nhân để xác minh tên của các bên thứ ba và cách họ lấy thông tin cá nhân khi nhận được thông tin cá nhân từ các bên thứ ba đó.

Thứ ba, xác lập trách nhiệm hình sự đối với việc cung cấp hoặc đánh cắp thông tin cá nhân nhằm thu lợi bất hợp pháp.

3.3. Nâng cao mức phạt xử lý vi phạm đối với hành vi vi phạm quy định về xử lý dữ liệu cá nhân

Hiện nay, mức phạt hành chính nặng nhất đối với vi phạm quyền riêng tư là 70 triệu đồng (Nghị định 15/2020/NĐ-CP) và mức phạt hình sự nặng nhất là 200 triệu đồng; thậm chí trong trường hợp xâm phạm bí mật cá nhân dẫn đến người bị xâm phạm tự sát thì cũng chỉ bị phạt tối đa 1.000.000.000 đồng hoặc phạt tù từ 02 năm đến 07 năm (Điều 288, Bộ luật Hình sự 2015). So sánh với quy định chung về bảo vệ dữ liệu do Ủy ban châu Âu xây dựng (GDPR) áp dụng mức phạt lên tới 20 triệu Euro, tương đương 500 tỷ VNĐ thì có thể thấy, mức phạt trong luật pháp Việt Nam còn khá nhẹ, trong khi hậu quả từ hành vi xâm phạm quyền riêng tư có thể rất nghiêm trọng, gây tổn hại tới danh dự, nhân phẩm, an toàn và cả tính mạng của không chỉ một mà có thể là nhiều nạn nhân.

Ngoài ra, quy định hành vi vi phạm trong một số nghị định về xử phạt vi phạm hành chính còn có nhiều điểm chưa hợp lý. Chẳng hạn, Điều 51 Nghị định 167/2013/NĐ-CP về xử phạt vi phạm hành chính trong lĩnh vực an ninh, trật tự, an toàn xã hội; phòng, chống tệ nạn xã hội; phòng cháy và chữa cháy; phòng, chống bạo lực gia đình, hành vi tiết lộ hoặc phát tán tư liệu, tài liệu thuộc bí mật đời tư của thành viên gia đình chỉ bị xử phạt khi hành vi này phải gắn với mục đích "nhằm xúc phạm danh dự, nhân phẩm". Việc pháp luật yêu cầu phải chứng minh mục đích của cá nhân, tổ chức tiết lộ, phát tán bí mật đời tư của người khác là điều không hợp lý. cần bãi bỏ; chỉ cần cá nhân, tổ chức có hành vi xâm phạm đời tư của người khác là đã bị xử lý vi phạm. Bên cạnh những đòi hỏi phải gia tăng mức phạt trong xử lý bằng con đường hành chính hay hình sự, cần đảm bảo hiệu quả giải quyết vụ việc theo cơ chế luật - đó là khởi kiện dân sự.

Kết luận

Sau gần 3 tháng nỗ lực nghiên cứu về luật pháp của Nhật Bản, những quy định của GDPR cũng như APPI, nhóm chúng tôi đã đúc kết được nhiều kinh nghiệm về việc bảo vệ dữ liệu cá nhân, sự khác biệt giữa luật pháp của các quốc gia, từ đó đưa ra những khuyến nghị, bổ sung thêm để luật pháp tại Việt Nam ngày càng phát triển hơn và hoàn thiện hơn.

Có thể thấy, với sự bùng nổ của cách mạng 4.0 cùng yêu cầu thu thập, lưu trữ, truyền tải thông tin ngày một tăng cao giữa các cơ quan nhà nước, doanh nghiệp với người dùng, công tác hoàn thiện pháp luật về bảo vệ dữ liệu cần sự quan tâm đặc biệt từ các cơ quan chức năng. Các quốc gia trong và ngoài khu vực đã có đạo luật riêng về bảo vệ dữ liệu cá nhân với tính hiệu quả, ứng dụng cao. Điều này cũng đã thôi thúc pháp luật Việt Nam có những bước tiến mới, phù hợp với những tiêu chuẩn của quốc tế cũng như thúc đẩy sự phát triển, hội nhập của quốc gia. Qua tìm hiểu về bảo vệ dữ liệu cá nhân tại đất nước Nhật Bản, bài nghiên cứu đã đưa ra một số bài học và đóng góp cho pháp luật Việt Nam trong thời kỳ cách mạng 4.0.

Tuy nhiên, bài nghiên cứu vẫn còn một số hạn chế về thực tiễn và lý luận do vẫn tồn tại một số khác biệt giữa văn hóa và pháp luật của hai quốc gia. Trong quá trình nghiên cứu và đưa ra đánh giá, nhóm tác giả đã đưa ra đánh giá dựa theo các quy định của GDPR, APPI và dự thảo nghị định quy định về dữ liệu cá nhân mới được đưa ra tại Việt Nam để đưa ra những phân tích mang tính khách quan nhất. Qua đó, nhóm tác giả hy vọng có thể đem lại đóng góp hữu ích cho những nghiên cứu về vấn đề này trong tương lai.

Tài liệu tham khảo

Lê, X.T. (2020), "Bảo vệ dữ liệu cá nhân tại Nhật Bản thông qua Đạo luật về bảo vệ thông tin cá nhân và một số khuyến nghị đối với Việt Nam", *Tạp chí Nghiên cứu Lập pháp,* http://lapphap.vn/Pages/tintuc/tinchitiet.aspx?tintucid=210586, truy cập ngày 18/10/2021.

Softbank. (2021), "Chính sách bảo vệ dữ liệu cá nhân theo đạo luật GDPR", https://www.softbank.jp/corp/privacy/gdpr-personal/, truy cập ngày 18/10/2021.

Ishiara, T. (2021), "The Privacy, Data Protection and Cybersecurity Law Review: Japan", *The Law Reviews*, https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/japan (Accessed 18 October, 2021).

Wheeler, T. (2017), "How the Republicans Sold Your Privacy to Internet Providers", *The New York Times*, https://www.nytimes.com/2017/03/29/opinion/how-the-republicans-sold-your-privacy-to-internet-providers.html (Accessed 1 November, 2021).

Kosinski, M., Stillwell, D., & Graepel, T. (2013), "Private traits and attributes are predictable from digital records of human behavior", *Proceedings of the National Academy of Sciences.*

Williams, O. (2019), "Facebook's Plan to Fuse Its Messaging Apps Is Not About Your Privacy", *Medium*, https://onezero.medium.com/facebooks-plan-to-fuse-its-messaging-apps-is-not-about-your-privacy-91c237e50c17 (Accessed 1 November, 2021).