BẢO VỆ QUYỀN ĐỐI VỚI DỮ LIỆU CÁ NHÂN TRONG PHÁP LUẬT QUỐC TẾ, PHÁP LUẬT Ở MỘT SỐ QUỐC GIA VÀ GIÁ TRỊ THAM KHẢO CHO VIỆT NAM

Vũ Công Giao*
Lê Trần Như Tuyên**
* PGS.TS. Khoa Luật, Đại học Quốc gia Hà Nội.
* * ThS. Khoa Luật, Đại học Quốc gia Hà Nội.

Thông tin bài viết:
Từ khóa: Kỹ thuật số, quyền về sự riêng tư, quyền đối với dữ liệu cá nhân

Lịch sử bài viết:
Nhận bài : 17/12/2019
Biên tập : 12/01/2020
Duyệt bài : 14/01/2020

Tóm tắt:
Thế kỷ XXI ghi dấu một bước ngoặt lớn trong sự phát triển của nhân loại. Đây là thế kỷ của kỹ thuật số, nơi mà những tiến bộ về công nghệ thông tin, thiết bị kết nối với Internet và phân tích dữ liệu đang diễn ra với tốc độ chóng mặt, nhanh hơn bất kỳ thời điểm nào khác trong lịch sử loài người. Sự phát triển của kỹ thuật số đã mở ra một kỷ nguyên mới cho khoa học công nghệ, là yếu tố đóng vai trò cốt lõi thúc đẩy Cách mạng công nghiệp 4.0, với những tác động vô cùng sâu rộng tới xã hội, làm thay đổi lối sống của con người. Tuy nhiên, sự phát triển của kỹ thuật đồng thời gây ra những tác động cực kỳ phức tạp đối với việc bảo vệ quyền về sự riêng tư của con người, đặc biệt là quyền đối với dữ liệu cá nhân. Bài viết này phân tích sự tác động của kỹ thuật số đến quyền đối với dữ liệu cá nhân; đánh giá các quy định của pháp luật quốc tế và pháp luật ở một số quốc gia về việc bảo vệ quyền này trong bối cảnh mới và nêu ra một số giá trị mà Việt Nam có thể tham khảo.

Article Infomation:
Key words: Digital, right to privacy, right to personal data

Article History:
Received : 17 Dec. 2020
Edited : 12 Jan. 2020
Approved : 14 Jan. 2020

Abstract:
The 20th century marked a major turning point in the development of mankind. This is the century of digital, where advances in communication technologies, devices connected to the Internet and data analytics are occurring at a breakneck pace and much quicker than at any other time in history. The growth of digital has resulted in broad social impacts and widespread lifestyle changes, and it has opened up a new era of science and technology development, contributing to the promoting the 4.0 Eevolution. However, the digital also pose incredibly complex risks to the right to privacy, especially the right to the protection of personal data. This article analyzes the impact of digital on the right to the protection of personal data; assess the provisions on protecting this right of international law and the laws of some countries in the new context and point out some values that Vietnam should consult.

1. Quyền đối với dữ liệu cá nhân trong Cách mạng công nghiệp 4.0

Quyền đối với dữ liệu cá nhân (*the right to personal data,* hay quyền bảo vệ dữ liệu cá nhân/quyền về sự riêng tư với dữ liệu cá nhân) là một phần cốt yếu của quyền về sự riêng tư (*the right to privacy*) của con người. Quyền về sự riêng tư là một quyền con người cơ bản, có tầm quan trọng thiết yếu để bảo đảm sự tự chủ và bảo vệ phẩm giá của con người. Quyền này giúp mỗi cá nhân tạo lập và kiểm soát ranh giới chính đáng với những người khác, từ đó bảo vệ bản thân trước những sự can thiệp tùy tiện trong cuộc sống, đồng thời cho phép mỗi cá nhân xác định mình là ai và cách thức mà bản thân muốn tương tác với thế giới xung quanh. Đối với xã hội, bảo vệ quyền về sự riêng tư của mỗi thành viên cũng chính là tạo lập và bảo vệ nền tảng của đời sống cộng đồng. Một cộng đồng không thể tồn tại nếu các thành viên của nó không được bảo vệ khỏi những hình thức lạm dụng. Theo nghĩa đó, bảo vệ quyền về sự riêng tư của mỗi cá nhân góp phần bảo đảm tính dân chủ, văn minh và sự phát triển ổn định, hài hòa của xã hội. Vì thế, quyền về sự riêng tư ngày nay đã trở thành một trong những vấn đề nhân quyền quan trọng.

Dữ liệu là yếu tố đóng vai trò then chốt cho sự tiến bộ của thời đại ngày nay. Điều đó dựa trên sự phát triển của các công nghệ lưu trữ và các loại cảm biến mà nó cho phép thu thập một khối lượng dữ liệu lớn từ đời sống xã hội. Tuy nhiên, điều đó cũng đặt ra yêu cầu phải bảo đảm để mọi người có thể kiểm soát thông tin hay dữ liệu cá nhân của mình. Do đó, thuật ngữ dữ liệu cá nhân được ghi nhận và trở nên phổ biến trong khoa học pháp lý.

Theo Ủy ban châu Âu, dữ liệu cá nhân là bất kỳ thông tin nào có liên quan nhằm xác định hoặc nhận dạng một cá nhân. Bên cạnh đó, những phần thông tin rời rạc khác nhau nếu được thu thập có thể dẫn đến việc xác định một con người cụ thể cũng được coi là dữ liệu cá nhân[1]. Quyền đối với dữ liệu cá nhân bao gồm các khía cạnh[2]: i) Quyền được sở hữu những thông tin cá nhân, bao gồm khả năng yêu cầu chủ thể nắm giữ chỉnh sửa nhằm bảo đảm tính toàn vẹn, chính xác của thông tin cá nhân của mình; ii) Quyền cho phép bên thứ ba tiếp cận thông tin cá nhân của mình; iii) Quyền yêu cầu các chủ thể có liên quan phải bảo đảm tính bí mật của thông tin, ví dụ như vô danh hóa thông tin cá nhân,...; iv) Quyền yêu cầu chủ thể nắm giữ bồi thường khi có hành vi xâm phạm thông tin trái pháp luật, gây thiệt hại cho cá nhân.

Cùng với sự phát triển của Cách mạng công nghiệp 4.0, dữ liệu cá nhân ngày nay đã trở thành một loại hàng hoá, được các tổ chức, cá nhân tìm kiếm, sử dụng để khai thác cho mục đích thương mại, đồng thời được các nhà nước sử dụng với mục đích quản lý người dân. Trong bối cảnh công nghệ thông tin phát triển, ngày càng có nhiều chương trình, hệ thống, biện pháp thu thập thông tin, theo dõi, giám sát cá nhân trên diện rộng, ở cấp độ quốc gia, thậm chí trên quy mô toàn cầu. Vấn đề là có rất nhiều chương trình, hệ thống như vậy đang được chính các cơ quan nhà nước, các thực thể kinh tế, thương mại, công nghệ và một số thực thể khác xây dựng và vận hành tràn lan, xâm phạm nghiêm trọng đến quyền về sự riêng tư của các cá nhân. Một trong những vụ việc tiêu biểu gây chấn động liên quan đến việc thu thập và lưu

1 European Commission, "What is personal data?", https://ec.europa.eu/info/law/law-topic/data-protection/reform /what-personal-data_en.

2 PGS.TS.NGUT. Chu Hồng Thanh, "Nhận thức pháp lý về quyền riêng tư", trong PGS.TS. Nguyễn Thị Quế Anh, PGS.TS. Vũ Công Giao, TS. Ngô Minh Hương& TS. Lã Khánh Tùng (eds), Quyền về sự riêng tư, Nxb. Chính trị quốc gia sự thật, Hà Nội, 2018, tr..48.

trữ dữ liệu cá nhân trái phép đã được tiết lộ bởi Edward Snowden, một nhân viên hợp đồng tại Cơ quan Tình báo Trung ương Hoa Kỳ (CIA), trong đó Cơ quan An ninh quốc gia (NSA) của Hoa Kỳ đã tạo lập một cơ sở dữ liệu bí mật khổng lồ chứa thông tin về hàng triệu người sống ở mọi nơi từ việc thu thập thông tin qua công nghệ máy tính ngày nay. Rõ ràng công nghệ đã tạo ra cơ hội cho nhiều chủ thể, bao gồm các chính phủ và các công ty, dễ dàng thu thập dữ liệu và theo dõi, giám sát các cuộc đàm thoại, trao đổi, các giao dịch thương mại, các hoạt động và thói quen của mọi cá nhân. Sự riêng tư của cá nhân, thậm chí là quyền tự do của con người, sẽ không còn nữa khi các chủ thể khác có thể quan sát tất cả các hoạt động của họ, dự báo các hành động tương lai của họ và từ đó định hướng, kiểm soát cuộc sống của họ. Điều này có thể làm trầm trọng hơn sự mất cân bằng quyền lực giữa cá nhân và các thiết chế, cả thiết chế công và tư, trong xã hội hiện đại.

Tóm lại, quyền về dữ liệu cá nhân nói riêng, quyền về sự riêng tư nói chung là một quyền con người có ý nghĩa to lớn để các cá nhân có thể khẳng định phẩm giá, sự tự chủ và nhân trạng của mình. Công nghệ thông tin với khả năng thu thập, phân tích và phổ biến dữ liệu về các cá nhân ngày càng tinh vi đã đặt ra nhu cầu cấp bách về bảo vệ quyền với dữ liệu cá nhân nói riêng và quyền về sự riêng tư nói chung. Các tổ chức quốc tế và các quốc gia cần nhận thức được thách thức to lớn này trong sự phát triển của Cách mạng công nghệ 4.0 để có biện pháp giải quyết hiệu quả, cụ thể là ban hành những chính sách và văn bản pháp luật nhằm bảo vệ dữ liệu cá nhân trước sự vi phạm của bất kỳ chủ thể nào, kể cả các cơ quan công quyền và các thiết chế tư nhân.

2. Pháp luật quốc tế và một số quốc gia về bảo vệ quyền đối với dữ liệu cá nhân

2.1. Pháp luật quốc tế về bảo vệ quyền đối với dữ liệu cá nhân

Ở cấp độ toàn cầu, các quy định về bảo vệ quyền về sự riêng tư có thể được tìm thấy trong Tuyên ngôn Nhân quyền phổ quát năm 1948 (UDHR), trong đó có Điều 12 về bảo vệ quyền về sự riêng tư. Từ nội dung Điều 12 UDHR, có thể thấy nội hàm của các giá trị riêng tư cần được bảo vệ không chỉ là cuộc sống riêng tư của mỗi cá nhân, mà còn bao gồm cả những khía cạnh đời sống có sự gắn kết mật thiết với cá nhân, cụ thể như gia đình, nơi ở, thư tín và cả những giá trị định tính như danh dự, uy tín cá nhân...

Tiếp theo UDHR, nhiều công ước quốc tế về quyền con người cũng công nhận quyền về sự riêng tư như một quyền cơ bản, cụ thể như: Công ước quốc tế về các quyền dân sự và chính trị (ICCPR) (Điều 17); Công ước về quyền của người lao động nhập cư (Điều 14); Công ước về quyền trẻ em (Điều 16); Công ước về quyền của người khuyết tật (Điều 22) ...

Dù vậy, sự phát triển của công nghệ trong cuộc Cách mạng công nghiệp 4.0 mà đi kèm với nó là tiềm năng giám sát ngày càng tinh vi của các hệ thống máy tính đã đặt ra những yêu cầu mới với bảo vệ dữ liệu của cá nhân. Để đáp ứng yêu cầu này, có hai công cụ pháp lý quốc tế đã được phát triển, trong đó đặt ra một số quy tắc cụ thể chi phối việc thu thập và xử lý dữ liệu cá nhân, bao gồm: Công ước năm 1981 của Hội đồng châu Âu về bảo vệ cá nhân liên quan đến việc xử lý dữ liệu cá nhân tự động[3] và Hướng dẫn của Tổ chức Hợp tác và Phát triển Kinh tế (OSCD) điều chỉnh việc bảo vệ quyền về sự riêng tư và việc chuyển đổi dữ

3 Convention on the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention, ETS No. 108, Stasbourg, 1981.

liệu cá nhân xuyên biên giới[4]. Các văn kiện này mô tả thông tin cá nhân là dữ liệu được bảo vệ ở mọi bước, từ thu thập đến lưu trữ và phổ biến. Quyền của mọi người được truy cập và sửa đổi dữ liệu của mình cũng là một khía cạnh chính của các quy tắc này. Biểu hiện của sự bảo vệ dữ liệu trong hai văn kiện đã nêu cơ bản là tương đồng, chỉ khác nhau ở mức độ, theo đó tất cả đều yêu cầu đối với thông tin cá nhân thì: i) Chỉ có thể được thu thập một cách công bằng và hợp pháp; ii) Chỉ được sử dụng cho mục đích ban đầu được biết rõ; iii) Bảo đảm tính đầy đủ, phù hợp và không vượt quá mục đích; iv) Bảo đảm tính chính xác và cập nhật; và v) Phải được loại bỏ sau khi mục đích sử dụng đã hoàn thành. Hai văn kiện nêu trên đã có tác động sâu sắc đến việc xây dựng và áp dụng luật pháp về bảo vệ dữ liệu cá nhân trên toàn thế giới, không giới hạn ở các nước châu Âu và các quốc gia thành viên của OECD.

Tuy nhiên, có thể nói rằng, luật pháp quốc tế hiện nay vẫn còn tương đối tụt hậu so với sự phát triển như vũ bão của công nghệ. Điều này đã khiến cho việc bảo vệ quyền đối với dữ liệu cá nhân của con người trong thực tế còn rất khó khăn. Tính đến thời điểm hiện nay, vẫn chưa có điều ước quốc tế toàn cầu nào về bảo vệ quyền đối với dữ liệu cá nhân. Hai văn kiện về bảo vệ dữ liệu cá nhân đã nêu trên (Công ước của Hội đồng châu Âu năm 1981 và Hướng dẫn của OECD) về nguyên tắc chỉ có tác động trong khu vực châu Âu và với các nước thành viên của OECD. Không chỉ vậy, Bản hướng dẫn của OECD chỉ có tính chất khuyến nghị, không có hiệu lực pháp lý ràng buộc.

2.2. Pháp luật của châu Âu và Hoa Kỳ về bảo vệ quyền đối với dữ liệu cá nhân

Đứng trước yêu cầu bảo vệ quyền về sự riêng tư trước tốc độ phát triển chóng mặt của công nghệ thông tin, nhiều khu vực và quốc gia đã củng cố khung pháp luật về vấn đề này. Mặc dù vậy, mỗi khu vực và quốc gia có những cách thức bảo vệ dữ liệu riêng tư khác nhau. Một số khu vực và quốc gia đã xây dựng thành công một cơ chế bảo vệ dữ liệu riêng tư mạnh mẽ thông qua luật pháp, trong khi nhiều khu vực và quốc gia khác mới đang lên kế hoạch xây dựng pháp luật về vấn đề này.

2.2.1. Luật bảo vệ dữ liệu cá nhân ở châu Âu

Quyền về sự riêng tư là một phần của Công ước châu Âu về quyền con người năm 1950, trong đó tuyên bố, mọi người đều có quyền được tôn trọng riêng tư và cuộc sống gia đình, nhà ở và thư từ. Từ cơ sở đó, các nước trong Liên minh châu Âu (EU) đã tìm cách đảm bảo quyền này thông qua việc xây dựng một văn bản pháp luật chung, đặc biệt khi Internet xuất hiện. Vào năm 1995, EU đã thông qua Chỉ thị về bảo vệ dữ liệu châu Âu (95/46/EC), trong đó thiết lập các tiêu chuẩn bảo mật và riêng tư dữ liệu tối thiểu để các quốc gia thành viên thực thi bằng cách đưa vào pháp luật của nước mình. Tuy nhiên, Chỉ thị năm 1995 được soạn thảo vào giai đoạn khi Internet mới chỉ được sử dụng bởi 1% dân số thế giới. Vì vậy, khi Internet bùng nổ, xuất hiện yêu cầu phải có văn bản pháp luật mới để giải quyết các vấn đề nảy sinh về bảo vệ dữ liệu cá nhân từ việc sử dụng Internet và các thiết bị thông minh trên quy mô lớn. Đây là lý do dẫn đến sự ra đời của Quy định chung về bảo vệ dữ liệu (GDPR) do Ủy ban châu Âu xây dựng, với mục đích vạch ra kế hoạch cải cách bảo vệ dữ liệu cá nhân trên toàn Liên minh châu Âu.

Về bản chất, GDPR là một bộ quy tắc mới, được xây dựng nhằm cung cấp cho công dân EU quyền kiểm soát nhiều hơn đối với dữ liệu cá nhân của họ. Theo các điều khoản của GDPR, không chỉ các tổ chức

4 OECD, Guidelines governing the Protection of Privacy and Transborder Data Flows of Personal Data, Paris, 1981.

phải đảm bảo dữ liệu cá nhân được thu thập hợp pháp và trong các điều kiện nghiêm ngặt, mà tất cả những bên thu thập và quản lý dữ liệu có nghĩa vụ bảo vệ dữ liệu khỏi việc bị lạm dụng và khai thác, cũng như tôn trọng quyền của chủ sở hữu dữ liệu. Tiền phạt đối với hành vi trái với quy định của GDPR rất cao. Theo đó có hai cách thức phạt, có thể tối đa là 20 triệu Euro hoặc 4% doanh thu toàn cầu (tùy theo mức nào cao hơn), cộng với việc các chủ thể dữ liệu có quyền yêu cầu bồi thường thiệt hại.

GDPR cũng là một bước tiến pháp lý lớn về xác định dữ liệu cá nhân. Dữ liệu cá nhân và dữ liệu cá nhân nhạy cảm là hai khái niệm nền tảng của GDPR. Dữ liệu cá nhân được định nghĩa là "bất kỳ thông tin nào liên quan đến một thể nhân ('data subject') đã được nhận định danh tính, hoặc có thể được nhận định danh tính, dù trực tiếp hay gián tiếp, cụ thể là bằng cách chỉ ra một định danh như tên, số định danh, dữ liệu vị trí, định danh trên mạng, hay một hoặc nhiều yếu tố chỉ định danh tính của một cá nhân mang tính vật lý, sinh lý, di truyền, tâm lý, kinh tế, văn hoá, hoặc xã hội". Định nghĩa này khá tương đồng với định nghĩa được đưa ra trong Chỉ thị năm 1995 của EU, nhưng có sự mở rộng hơn, bao gồm cả "địa chỉ IP" hay "giả danh tính" (pseudonymisation).

Dữ liệu cá nhân nhạy cảm được quy định dưới dạng hạng mục dữ liệu cá nhân đặc biệt trong GDPR, được xem là: "Bất kỳ dữ liệu nào tiết lộ chủng tộc hoặc sắc tộc, tư tưởng chính trị, đức tin tôn giáo, quan niệm triết lý, thành viên công đoàn, và việc xử lý dữ liệu di truyền và sinh trắc nhằm mục đích định danh, hoặc dữ liệu liên quan đến sức khoẻ, tình trạng sinh dục, và xu hướng tính dục"[5]. Việc xử lý và phân tích các dữ liệu nhạy cảm hoàn toàn bị cấm bởi GDPR. Một số trường hợp ngoại lệ cho phép xử lý dữ liệu cá nhân nhạy cảm, bao gồm có sự đồng thuận từ chủ thể dữ liệu, để bảo vệ quyền lợi cá nhân, để phục vụ công tác y tế dự phòng và y tế nghiệp vụ, hoặc vì lợi ích công cộng. Xét trên những điều kiện đó, việc Facebook hoặc Google cùng các đối tác kinh doanh thu thập và xử lý các dữ liệu cá nhân nhạy cảm có khả năng vi phạm GDPR rất cao. Trong những tình huống vi phạm, GDPR cho phép các cá nhân có quyền nộp đơn khiếu nại đến Cơ quan Quản lý Dữ liệu đặt tại các quốc gia thành viên nơi cá nhân đang làm việc hoặc sinh sống, hoặc nơi việc vi phạm đã diễn ra. Các cá nhân sau khi được thẩm định quyền bị xâm hại sẽ được xử lý đền bù theo quyết định của Cơ quan Quản lý Dữ liệu, theo tinh thần của những quyết định đưa ra bởi Hội đồng Bảo vệ Dữ liệu châu Âu (EDPB). Tính đến tháng 5/2019, khoản tiền phạt lớn nhất áp dụng theo GDPR là 50 triệu Euro. Ví dụ, Cơ quan giám sát bảo vệ dữ liệu của Pháp (CNIL), đã quyết định án phạt cho Google vào tháng 1/2019 sau khi đi đến kết luận rằng gã khổng lồ công cụ tìm kiếm này đã phá vỡ các quy tắc của GDPR về tính minh bạch và cơ sở pháp lý hợp lệ khi xử lý dữ liệu của mọi người cho mục đích quảng cáo[6].

GDPR thiết lập 7 nguyên tắc cần tuân thủ khi xử lý dữ liệu: 1) Tính hợp pháp, công bằng và minh bạch: Việc xử lý dữ liệu phải hợp pháp, công bằng và minh bạch đối với chủ thể dữ liệu; 2) Giới hạn mục đích: Mục đích xử lý dữ liệu phải hợp pháp và được thể hiện rõ ràng cho chủ thể dữ liệu khi thu thập; 3) Giảm thiểu dữ liệu: Chỉ thu thập và xử lý dữ liệu khi thực sự cần thiết cho các mục đích đã định; 4) Độ chính xác: Phải bảo đảm dữ liệu cá nhân là chính xác và cập nhật; 5)

5 Khoản 1, Điều 9 Quy định chung về bảo vệ dữ liệu của Liên minh châu Âu.

6 Danny Palmer, "What is GDPR? Everything you need to know about the new general data protection regulations", 2019, https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/.

Giới hạn lưu trữ: Chỉ lưu trữ dữ liệu nhận dạng cá nhân trong thời gian cần thiết cho mục đích đã định; 6) Tính toàn vẹn và bảo mật: Việc xử lý dữ liệu phải được thực hiện trên cơ sở đảm bảo tính bảo mật, tính toàn vẹn và bảo mật thích hợp (ví dụ: bằng cách sử dụng mã hóa); 7) Trách nhiệm giải trình: Người kiểm soát dữ liệu có trách nhiệm chứng minh sự tuân thủ GDPR với tất cả các nguyên tắc này.

GDPR cũng quy định "quyền được lãng quên" - cụ thể là quyền xóa dữ liệu cho những người muốn xóa dữ liệu cá nhân của họ khi không còn căn cứ để lưu giữ dữ liệu đó. GDPR được áp dụng ở cấp độ trong nước với hiệu lực ngay lập tức, bắt đầu từ ngày nó có hiệu lực và việc áp dụng luật quốc gia sẽ không ảnh hưởng đến hiệu lực của nó. Tuy nhiên, GDPR cho phép các quốc gia thành viên sự linh hoạt đến một mức độ nhất định khi áp dụng một số quy định.

Trong thực tế, các nước thành viên EU đã sửa đổi luật bảo vệ dữ liệu của họ để tuân thủ các yêu cầu GDPR. Ví dụ, Pháp đã điều chỉnh luật pháp nước mình theo GDPR với việc ban hành Luật số 2018-493 (FDPA) ngày 20/6/2018 về bảo vệ dữ liệu cá nhân, trong đó thay thế logic của các thủ tục trước đó (thông báo hoặc ủy quyền trước bởi CNIL) dựa trên triết lý về trách nhiệm giải trình nâng cao của các bên liên quan trong GDPR. Nước Anh cũng đã thông qua Luật Bảo vệ dữ liệu quốc gia mới (DPA) có hiệu lực vào ngày 25/5/2018, trong đó cho phép tiếp tục áp dụng GDPR kể cả khi nước này rời Liên minh châu Âu. DPA chuyển đổi Chỉ thị thực thi pháp luật ((EU) 2016/680) thành luật pháp của Vương quốc Anh, tạo ra một chế độ bảo vệ dữ liệu dành riêng cho việc xử lý dữ liệu cá nhân của cơ quan thực thi pháp luật, trong đó Phần 4 của DPA cập nhật chế độ bảo vệ dữ liệu để xử lý an ninh quốc gia; các Phần 5 và 6 đưa ra phạm vi nhiệm vụ và quyền hạn của Ủy viên Thông tin, đồng thời quy định một số tội hình sự liên quan đến xử lý dữ liệu cá nhân.

2.2.2. Luật Bảo vệ dữ liệu cá nhân ở Hoa Kỳ

Cho đến nay, Hoa Kỳ chưa có bất kỳ đạo luật riêng nào ở cấp liên bang về bảo vệ dữ liệu cá nhân, song vấn đề này đã được nêu trong nhiều văn bản pháp luật ban hành theo từng ngành, từng đối tượng. Ví dụ: Luật Bảo vệ quyền về sự riêng tư trực tuyến của trẻ em (COPPA) - cung cấp cho phụ huynh quyền kiểm soát đối với những thông tin mà các trang web có thể thu thập từ con cái họ; Luật về Trách nhiệm giải trình và trách nhiệm bảo hiểm y tế (HIPPA) - đảm bảo tính bảo mật của bệnh nhân đối với tất cả các dữ liệu liên quan đến chăm sóc sức khỏe; Luật Bảo vệ quyền về sự riêng tư video - ngăn chặn việc tiết lộ sai thông tin của một cá nhân xuất phát từ việc cho thuê hoặc mua tài liệu nghe nhìn của họ... Theo cách tiếp cận của Hoa Kỳ, việc bảo vệ dữ liệu và quyền về sự riêng tư được dựa trên sự kết hợp giữa luật pháp, quy định và tự điều chỉnh, thay vì chỉ có sự can thiệp của nhà nước[7]. Pháp luật thường chỉ được áp dụng cho các tình huống trong đó các cá nhân không thể tự kiểm soát việc sử dụng dữ liệu cá nhân của họ.

Sau khi GDPR được thông qua, một số tiểu bang của Hoa Kỳ đã đề xuất luật bảo vệ dữ liệu của riêng họ, thiết lập một số quyền giống như GDPR. Luật về Sự riêng tư của người tiêu dùng của bang California (CCPA) được thông qua vào tháng 6/2018 sau vụ bê bối Cambridge Analytica[8], dự kiến sẽ trở thành luật về quyền về sự riêng tư dữ liệu toàn diện nhất ở Hoa Kỳ. Giống như GDPR, văn bản luật này thiết lập một số quyền nhất định cho người tiêu dùng, bao gồm "quyền

7 HG.org, "Data Protection Law", https://www.hg.org/data-protection.html.

được biết", "quyền được tiếp cận", "quyền từ chối" và "quyền xóa bỏ". Ngoài ra, CCPA mở rộng đáng kể định nghĩa về thông tin cá nhân, từ đó đòi hỏi các công ty phải có những thay đổi đáng kể trong cách thức hoạt động của mình. Văn bản luật này, không giống như bất kỳ luật bảo vệ dữ liệu nào được ban hành trước đây ở Hoa Kỳ , yêu cầu có một lựa chọn trên trang web của công ty để cho phép người tiêu dùng từ chối chia sẻ dữ liệu cho bên thứ ba. Văn bản luật này cũng cho phép quyền hành động riêng tư trong trường hợp vi phạm dữ liệu và cho phép Bộ trưởng Tư pháp California áp dụng các hình phạt hành chính lên tới 7.500 đô la cho mỗi lần vi phạm mà không có giới hạn tối đa.

Không chỉ California, 11 bang khác của Hoa Kỳ bao gồm Maryland, New Jersey và Washington… gần đây đã đưa ra dự thảo văn bản pháp luật tương tự. Những dự luật này có các phiên bản riêng về quyền từ chối và các yêu cầu công bố mà khác một chút so với GDPR và CCPA. Nếu được ban hành, các luật này sẽ dẫn đến tăng chi phí đáng kể cho các doanh nghiệp khi phải cố gắng hiểu và đưa ra một khung bảo mật tuân thủ các quy định của của luật.

Trên thực tế, mức độ phức tạp và không chắc chắn do những thay đổi về khung pháp lý đang khiến các doanh nghiệp kêu gọi Quốc hội Hoa Kỳ ban hành và thực thi luật bảo mật dữ liệu cá nhân áp dụng cho toàn quốc. Đáp ứng lời kêu gọi đó, Quốc hội Hoa Kỳ đã đưa ra một số dự luật về quyền về sự riêng tư dữ liệu để thực hiện tiêu chuẩn bảo mật dữ liệu liên bang tại Hoa Kỳ. Ví dụ, Luật Phổ biến Dữ liệu Hoa Kỳ (S. 142) sẽ áp đặt các yêu cầu về quyền về sự riêng tư đối với các nhà cung cấp dịch vụ Internet tương tự như các yêu cầu áp đặt cho các cơ quan Liên bang theo Luật về quyền về sự riêng tư năm 1974. Luật bảo vệ quyền về sự riêng tư và quyền lợi người tiêu dùng trên phương tiện truyền thông xã hội năm 2019 (S. 189), sẽ yêu cầu các chủ thể: 1) cung cấp cho người dùng một bản sao miễn phí dưới dạng điện tử những dữ liệu cá nhân mà nhà điều hành đã xử lý và 2) thông báo cho người dùng trong vòng 72 giờ sau khi biết rằng dữ liệu của người dùng đã bị truyền đi mà vi phạm nền tảng bảo mật[9].

Tóm lại, trước những tác động của cuộc Cách mạng công nghiệp 4.0, nhiều khu vực và quốc gia đã có những động thái tích cực và hiệu quả về mặt lập pháp để bảo vệ quyền về sự riêng tư dữ liệu của cá nhân. Đây là một xu hướng chung trên thế giới mà tất cả các nước, trong đó có Việt Nam.

3. Những giá trị tham khảo cho Việt Nam

3.1. Khái quát thực trạng pháp luật Việt Nam về bảo vệ quyền đối với dữ liệu cá nhân

Vấn đề bảo vệ các giá trị riêng tư cơ bản của một cá nhân đã được ghi nhận ngay từ khi nước Việt Nam Dân chủ Cộng hòa được thành lập, mà thể hiện nổi bật ở quy định về *quyền được bảo vệ nhà ở và thư tín* trong Điều thứ 11 của Hiến pháp năm năm 1946. Xuyên suốt trong các bản hiến pháp tiếp theo (1959, 1980, 1992) đều có quy định về bảo vệ quyền về sự riêng tư, dù cách diễn đạt và nội dung ít nhiều khác nhau. Hiến pháp năm 2013 tiếp tục ghi nhận quyền về sự riêng tư của cá nhân nhưng mở rộng, bám sát hơn nội dung quyền này trong luật nhân quyền quốc

8 Wikipedia, "Facebook–Cambridge Analytica data scandal", https://en.wikipedia.org/wiki/Facebook%E2%80%93 Cambridge_Analytica_data_scandal.

9 U.S. GAO, "Report: INTERNET PRIVACY: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility", 2019, GAO-19-52.

tế. Theo quy định tại Điều 21 Hiến pháp năm 2013, mọi người có quyền bất khả xâm phạm về đời sống riêng tư, trong đó bao gồm cả bí mật cá nhân, bí mật gia đình, bí mật thư tín, điện thoại, điện tín và các hình thức trao đổi thông tin riêng tư khác. Nhìn chung, khái niệm đời sống riêng tư trong Điều 21 Hiến pháp 2013 được hiểu theo nghĩa rộng, bao gồm tất cả những gì gắn với danh dự, uy tín của một cá nhân. Đây là cách quy định rộng và chi tiết hơn so với quy định về quyền này trong các bản Hiến pháp trước đó. Không chỉ vậy, Điều 22 Hiến pháp năm 2013 còn quy định quyền bất khả xâm phạm về chỗ ở, đồng thời nêu rõ "Không ai được tự ý vào chỗ ở của người khác nếu không được người đó đồng ý", "Việc khám xét chỗ ở do luật định". Những quy định này cũng chính là để bảo vệ quyền về sự riêng tư.

Việc bảo vệ quyền về sự riêng tư nói chung ở Việt Nam còn được cụ thể hoá trong nhiều đạo luật chuyên ngành khác nhau, phụ thuộc vào bản chất của từng vấn đề, ví dụ như Bộ luật Dân sự, Bộ luật Hình sự, Bộ luật Tố tụng hình sự, Bộ luật Tố tụng dân sự, Luật Bưu chính, Luật Viễn thông, Luật Xuất bản, Luật Phòng, chống HIV/AIDS...

Dù vậy, Việt Nam hiện nay chưa có một văn bản pháp luật thống nhất điều chỉnh các vấn đề liên quan và bảo vệ quyền về dữ liệu cá nhân. Thay vào đó, quyền này được bảo vệ bởi nhiều văn bản pháp luật khác nhau như Luật Giao dịch điện tử, Luật Công nghệ thông tin, Luật Bảo vệ quyền lợi Người tiêu dùng, Luật An toàn thông tin mạng, Luật An ninh mạng, Nghị định số 52/2013/ND-CP về thương mại điện tử và Nghị định số 72/2013/ND-CP về quản lý, cung cấp và sử dụng dịch vụ Internet và thông tin trên mạng....

Trong nỗ lực tăng cường khung pháp lý về quyền về sự riêng tư thông tin, Việt Nam đã ban hành Luật An toàn thông tin mạng năm 2015. Luật nêu ra định nghĩa thông tin cá nhân, các nguyên tắc bảo vệ quyền về sự riêng tư dữ liệu, quy định về thu thập, sử dụng, sửa đổi, xóa thông tin cá nhân cùng với trách nhiệm của chính phủ trong việc bảo vệ dữ liệu riêng tư. Tương tự như các văn bản pháp luật đã nêu trên, Luật An toàn thông tin mạng cũng yêu cầu cần có sự đồng ý của chủ sở hữu trước khi xử lý thông tin cá nhân (bao gồm thu thập, chỉnh sửa, sử dụng, lưu trữ, cung cấp, chia sẻ hoặc lan truyền), đồng thời quy định tổ chức, cá nhân xử lý thông tin cá nhân có trách nhiệm bảo mật thông tin và phải công bố chính sách sử dụng và bảo vệ thông tin được xử lý[10].

Luật An ninh mạng năm 2018 lần đầu tiên yêu cầu các doanh nghiệp cung cấp dịch vụ trên không gian mạng tại Việt Nam phải thông báo trực tiếp cho người dùng nếu dữ liệu của họ bị vi phạm, bị hư hỏng hoặc bị mất[11]. Quy định này tương đồng với các yêu cầu đặt ra trong GDPR của Liên minh châu Âu. Tuy nhiên, xét chung, Luật An ninh mạng 2018 không giống các luật tương tự ở châu Âu và Hoa Kỳ, mà có nhiều điểm tương đồng với Luật An ninh mạng của Trung Quốc, thể hiện ở việc chủ yếu nhằm tăng cường khả năng của nhà nước trong việc kiểm soát luồng thông tin và bảo vệ các cơ sở hạ tầng thông tin quan trọng.

Tóm lại, có thể thấy rằng, cùng với Hiến pháp, hệ thống pháp luật của Việt Nam hiện đã xác lập nền tảng pháp lý ban đầu để bảo vệ quyền về sự riêng tư, trong đó bao gồm quyền về dữ liệu cá nhân trên nhiều lĩnh vực. Tuy nhiên, trước ảnh hưởng sâu rộng của cuộc Cách mạng công nghiệp 4.0 hiện nay,

10 Điều 17, Luật An toàn thông tin mạng 2015.

11 Điểm c, khoản 1, Điều 41 Luật An ninh mạng năm 2018.

so với các quy định của pháp luật quốc tế và pháp luật ở nhiều quốc gia, pháp luật Việt Nam trong lĩnh vực này vẫn còn một số hạn chế, cụ thể như sau:

Thứ nhất, khung pháp lý vẫn còn thiếu các văn bản riêng và quy định cụ thể về quyền về sự riêng tư dữ liệu và bảo vệ thông tin cá nhân.

Thứ hai, một số quy định của pháp luật hiện hành về bảo vệ quyền đối với dữ liệu cá nhân còn thiếu rõ ràng, nặng về nguyên tắc, có thể dẫn đến hiểu và áp dụng sai.

Thứ ba, các quy định về chế tài với những hành vi vi phạm quyền với dữ liệu cá nhân còn chưa tương xứng, chưa đảm bảo tính răn đe. Mức phạt tiền nặng nhất đối với vi phạm quyền về sự riêng tư trong pháp luật hành chính của Việt Nam hiện là 70 triệu đồng (Điều 66 Nghị định số 174/2013/NĐ-CP), trong pháp luật hình sự là 200 triệu đồng (Điều 288 Bộ luật Hình sự 2015, sửa đổi, bổ sung năm 2017). Trong khi đó, như đã đề cập, GDPR áp dụng mức phạt lên tới 20 triệu Euro (tương đương 500 tỷ VNĐ). Từ sự so sánh này, có thể thấy mức phạt trong luật pháp Việt Nam còn quá nhẹ so với mức độ nguy hại và hậu quả của hành vi xâm phạm quyền này.

3.2. Những kinh nghiệm gợi mở cho việc hoàn thiện pháp luật bảo vệ quyền với dữ liệu cá nhân ở Việt Nam

Từ thực trạng pháp luật trong nước, đối chiếu với các quy định trong pháp luật của châu Âu và Hoa Kỳ, có thể gợi mở một số giải pháp nhằm hoàn thiện pháp luật về quyền được bảo vệ bí mật dữ liệu cá nhân ở nước ta như sau:

Thứ nhất, xây dựng một văn bản pháp luật riêng bảo vệ dữ liệu cá nhân. Như đã đề cập, trước bối cảnh Cách mạng công nghiệp 4.0, ở châu Âu đã có văn bản pháp luật chung của EU và nhiều nước trong khu vực đã ban hành văn bản pháp luật riêng bảo vệ quyền về sự riêng tư, đặc biệt là bảo vệ dữ liệu cá nhân. Hoa Kỳ cũng đang xây dựng những đạo luật liên bang riêng về vấn đề này. Trong khi đó, quy định về bảo vệ quyền về dữ liệu cá nhân ở Việt Nam hiện vẫn nằm rải rác ở nhiều văn bản pháp luật khác nhau, dẫn đến tình trạng vừa chồng chéo, vừa thiếu thống nhất và khó khăn cho việc áp dụng pháp luật. Vì thế, Nhà nước cần nghiên cứu xây dựng, ban hành một văn bản pháp luật riêng để bảo vệ dữ liệu cá nhân, trong đó quy định đầy đủ các khái niệm, nguyên tắc, thể chế và thiết chế bảo vệ dữ liệu riêng tư của con người. Luật bảo vệ dữ liệu cá nhân cũng cần quy định rõ những giới hạn của quyền, những điều kiện và hạn chế đặt ra với việc khai thác, sử dụng, phổ biến dữ liệu cá nhân, quy định về cơ quan chuyên trách theo dõi, giám sát, giải quyết các khiếu nại, tố cáo về quyền này trên thực tế.

Thứ hai, sửa đổi, bổ sung các quy định về bảo mật thông tin/dữ liệu trong các luật chuyên ngành như Luật Công nghệ thông tin, Luật An toàn thông tin mạng, Luật An ninh mạng... Như đã đề cập, các quy định về vấn đề này trong pháp luật của châu Âu và Hoa Kỳ rất cụ thể và chặt chẽ, trong khi các văn bản pháp luật của Việt Nam mới chỉ dừng lại ở mức quy định nguyên tắc chung nên hiệu quả áp dụng trong thực tế thấp. Vì vậy, việc sửa đổi, bổ sung các quy định về vấn đề này là rất cần thiết.

Thứ ba, sửa đổi, bổ sung các quy định về chế tài với những hành vi vi phạm. Như đã phân tích, chế tài xử phạt vi phạm quyền về sự riêng tư nói chung và dữ liệu riêng tư nói riêng tại Việt Nam hiện quá thấp so với chế tài ở châu Âu và các quốc gia khác, chưa tương xứng với mức độ nghiêm trọng của hành vi vi phạm, chưa đảm bảo tính răn đe. Vì vậy, Nhà nước cần sửa đổi các văn bản pháp luật có liên quan để quy định những hình thức chế tài nghiêm khắc hơn, đặc biệt là về hành chính và dân sự, với các cơ quan,

tổ chức, doanh nghiệp và cá nhân vi phạm quyền về dữ liệu riêng tư.

Thứ tư, bảo đảm nghĩa vụ tôn trọng, bảo vệ và thúc đẩy quyền về sự riêng tư. Như đã phân tích ở các phần trên, quyền về sự riêng tư là quyền con người cơ bản, có ý nghĩa rất quan trọng, được công nhận và bảo vệ bởi luật nhân quyền quốc tế và pháp luật của hầu hết quốc gia. Sự phát triển của công nghệ đã cải thiện đáng kể đời sống của con người, song cũng là một nguy cơ lớn với quyền về sự riêng tư, do công nghệ có thể trở thành công cụ để nhiều chủ thể, trong đó có nhà nước, giám sát và can thiệp và đời sống riêng tư của con người. Ở Việt Nam, quyền riêng tư được bảo vệ bởi Hiến pháp và nhiều luật chuyên ngành, song trong thực tế sự bảo vệ của Nhà nước với quyền này còn thiếu hiệu quả, những nỗ lực đã được thực hiện chưa tương xứng với tầm quan trọng của nó. Đặc biệt, Luật An ninh mạng hiện còn có những lỗ hổng tiềm ẩn khả năng cơ quan nhà nước tuỳ tiện can thiệp vào đời tư thông qua việc thu thập dữ liệu riêng tư của cá nhân. Vì vậy, trong thời gian tới, Nhà nước cần tiếp tục xây dựng, hoàn thiện hệ thống pháp luật để thúc đẩy và bảo vệ hiệu quả hơn quyền về sự riêng tư nói chung, quyền về dữ liệu cá nhân nói riêng theo đúng tinh thần của Hiến pháp năm 2013 và các điều ước quốc tế mà Việt Nam đã tham gia ■

Tài liệu tham khảo

1. Amber Pariona, "What Was the Digital Revolution?", 2017, https://www.worldatlas.com/ articles/what-was-the-digital-revolution.html.
2. European Commission, "What is personal data?", https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en.
3. Cẩm Thi, "Tràn lan tình trạng mua bán thông tin cá nhân", 2018, https://kiemsat.vn/tran-lan-tinh-trang-mua-ban-thong-tin-ca-nhan-50866.html.
4. Convention fn the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention, ETS No. 108, Stasbourg, 1981.
5. Chính phủ, Dự thảo Nghị định quy định chi tiết một số điều của Luật an ninh mạng, 31/10/2018.
6. Danny Palmer, "What is GDPR? Everything you need to know about the new general data protection regulations", 2019, https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/.
7. Global Internet liberty campaign, "Privacy and human rights - An International Survey of Privacy Laws and Practice", 2004, http://gilc.org/privacy/survey/intro.html.
8. HG.org, Data Protection Law, https://www.hg.org/data-protection.html.
9. Hoàng Thị Ngọc Lan, "Những thành tựu cơ bản của các cuộc cách mạng công nghiệp trong lịch sử thế giới", 2019, http://vtec.edu.vn/index.php?option=com_content&view= article&id=995:nh-ng-thanh-t-u-co-b-n-c-a-cac-cu-c-cach-m-ng-cong-nghi-p-trong-l-ch-s-th-gi-i&catid=93&Itemid=492.
10. John Rose, Christine Barton & Rob Souza, "The Trust Advantage: How to Win with Big Data", Boston Consulting Group, 2013, https://www.bcg.com/publications/2013/marketing-sales-trust-advantage-win-with-big-data.aspx.
11. OECD, Guidelines governing the Protection of Privacy and Transborder Data Flows of Personal Data, Paris, 1981.
12. Chu Hồng Thanh, "Nhận thức pháp lý về quyền riêng tư", trongQuyền về sự riêng tư, Nxb. Chính trị quốc gia sự thật, Hà Nội, 2018.
13. Richard Hodson, "Digital revolution: An explosion in information technology is remaking the world, leaving few aspects of society untouched", 2018, https://www.nature.com/articles/ d41586-018-07500-z.
14. RMIT University, "what is Industry 4.0?", https://www.rmit.edu.au/industry/develop-your-workforce/tailored-workforce-solutions/c4de/industry-40.
15. Simon Davies, "Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity", in Agre and Rotenberg (ed) "Technology and Privacy: the new landscape", MIT Press, 1997, p. 143.
16. U.S. GAO, "Report: INTERNET PRIVACY: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility", 2019, GAO-19-52.
17. Ủy ban Nhân quyền, Bình luận chung số 16 về quyền về sự riêng tư, 1988.