**Quản lý nhà nước về bảo vệ dữ liệu cá nhân – thực trạng và kiến nghị**

##### **Việt Nam có tốc độ phát triển và ứng dụng internet vô cùng mạnh mẽ, cùng với đó, mục tiêu xây dựng chính phủ số, nền kinh tế số đang được Chính phủ chú trọng đẩy mạnh. Trong bối cảnh đó, việc trao đổi, chia sẻ dữ liệu cá nhân ngày càng trở nên phổ biến. Tuy nhiên, tình trạng lộ, lọt, hoạt động đánh cắp, mua bán dữ liệu cá nhân hiện đang diễn ra phổ biến ở hầu hết các quốc gia trên thế giới, trong đó có Việt Nam. Chính vì vậy, việc tìm hiểu, nghiên cứu pháp luật về bảo vệ dữ liệu cá nhân của các quốc gia trên thế giới là rất cần thiết. Trong bài viết, tác giả phân tích bản chất, vai trò của dữ liệu cá nhân và bảo vệ dữ liệu cá nhân, thực trang quản lý nhà nước về bảo vệ dữ liệu cá nhân tại một số nước trên thế giới và tại Việt Nam, từ đó đưa ra một số kiến nghị nhằm hoàn thiện hoạt động này tại Việt Nam.**

##### **Dữ liệu cá nhân và bảo vệ dữ liệu cá nhân**

Theo Ủy ban châu Âu (EC), dữ liệu cá nhân là bất kỳ thông tin nào có liên quan đến việc xác định hoặc nhận dạng một người đang sống. Các phần thông tin khác nhau được thu thập cùng nhau có thể giúp nhận dạng một người cụ thể, cũng tạo thành dữ liệu cá nhân1. Dữ liệu cá nhân đã được hủy nhận dạng, mã hóa hoặc đặt bút danh nhưng có thể được sử dụng để nhận dạng lại một người thì vẫn được coi là dữ liệu cá nhân, còn dữ liệu cá nhân được ẩn danh theo cách mà cá nhân không thể hoặc không còn nhận dạng được nữa sẽ không được coi là dữ liệu cá nhân. Để dữ liệu được ẩn danh thực sự, việc ẩn danh phải không thể thay đổi được.

Một số thông tin được coi là dữ liệu cá nhân theo EC là: tên và họ; địa chỉ nhà; địa chỉ email, như: name.surname@company.com; số chứng minh nhân dân; dữ liệu vị trí; địa chỉ IP; ID cookie; dữ liệu do bệnh viện hoặc bác sĩ nắm giữ. Một số thông tin khác không được coi là dữ liệu cá nhân, ví dụ như số đăng ký kinh doanh của công ty; địa chỉ email, như: info@company.com; các dữ liệu ẩn danh.

Đạo luật bảo vệ dữ liệu cá nhân của Thái Lan cũng đưa ra cách hiểu tương tự về thuật ngữ dữ liệu cá nhân. Theo đó, “dữ liệu cá nhân” nghĩa là bất kỳ thông tin nào liên quan đến một người, cho phép nhận dạng người đó, dù trực tiếp hay gián tiếp, nhưng không bao gồm thông tin của những người đã qua đời.

Thuật ngữ dữ liệu cá nhân trong Đạo luật bảo vệ dữ liệu cá nhân của Singapore là một khái niệm rất rộng bao gồm “dữ liệu, dù đúng hay không, về một cá nhân có thể được xác định từ dữ liệu đó, hoặc từ dữ liệu đó và thông tin khác mà tổ chức có hoặc có khả năng truy cập”.

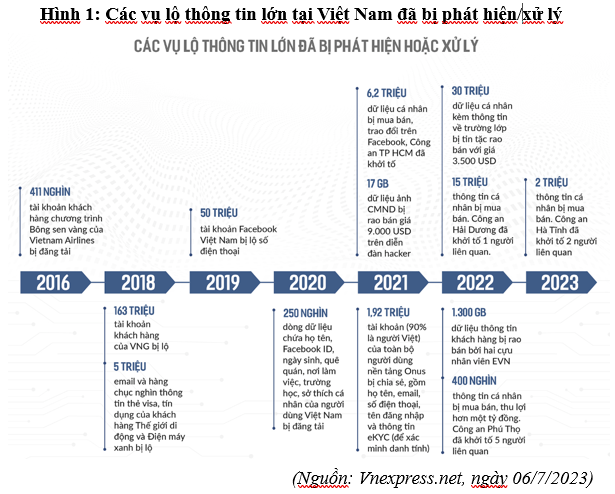
Theo Luật Bảo vệ dữ liệu chung của Brazil, dữ liệu cá nhân là một dữ liệu bất kỳ, ở dạng độc lập hay được tổng hợp với dữ liệu khác, có thể cho phép nhận dạng một người hoặc một chủ thể đến một hành vi nhất định. Trong thời đại dữ liệu lớn cho phép tương quan nhanh chóng giữa các cơ sở dữ liệu lớn, có cấu trúc và không có cấu trúc, hầu như mọi dữ liệu cuối cùng đều có thể được coi là dữ liệu cá nhân, do đó phải tuân theo luật pháp.

Trong luật của một số quốc gia, như: Đạo luật quyền riêng tư của New Zealand, Đạo luật bảo vệ thông tin cá nhân của Hàn Quốc, Luật Bảo vệ thông tin cá nhân của Trung Quốc thì không đề cập trực tiếp tới thuật ngữ “dữ liệu cá nhân” mà sử dụng thuật ngữ “thông tin cá nhân” với ý nghĩa tương tự.

Vậy có thể hiểu dữ liệu cá nhân là bất kỳ thông tin nào, dù đúng hoặc không đúng, tồn tại độc lập hoặc tổng hợp với dữ liệu khác, có liên quan đến việc xác định hoặc nhận dạng một người đang sống hoặc đã chết. Bảo vệ dữ liệu cá nhân là hoạt động phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi vi phạm liên quan đến dữ liệu cá nhân theo quy định của pháp luật.

##### **Tầm quan trọng của dữ liệu cá nhân**

Trong bối cảnh hiện nay, dữ liệu cá nhân là thực sự cần thiết đối với hầu hết các lĩnh vực, ngành nghề, đặc biệt là ngành quảng cáo marketing, ngân hàng, y tế… Từ đó, việc thu thập dữ liệu cá nhân trở lên phổ biến, tạo ra các kho lưu trữ dữ liệu khổng lồ và đặt ra bài toán phải có biện pháp bảo vệ phù hợp, nếu không sẽ bị các phần tử xấu lợi dụng. Những người bị lộ thông tin có thể sẽ bị gọi điện làm phiền, nhắn tin quảng cáo hay thậm chí bị đánh cắp danh tính với mục đích xấu, làm ảnh hưởng tới chủ sở hữu thông tin. Tình trạng này đã, đang diễn ra và ngày càng phức tạp hơn với những biến tướng khác nhau. Hậu quả trước tiên là sự phiền hà, khó chịu với người chủ sở hữu thông tin; nghiêm trọng hơn có thể dẫn tới các cuộc tấn công lừa đảo hay các vấn đề về an ninh thông tin, gây thiệt hại cả về vật chất và tinh thần, ảnh hưởng trực tiếp đến quyền và lợi ích hợp pháp của các cơ quan, tổ chức, doanh nghiệp và mỗi cá nhân.



**Một số phương thức thu thập, chiếm đoạt dữ liệu cá nhân:**

(1) Sử dụng mã độc, phần mềm gián điệp hoặc tấn công vào thiết bị của người sử dụng để chiếm đoạt thông tin cá nhân.

(2) Lợi dụng sự chủ quan, thiếu hiểu biết của người dùng, đề nghị họ tham gia vào các chương trình khuyến mãi, bốc thăm trúng thưởng, mua hàng online, mini game có thưởng… Họ sẽ phải cung cấp thông tin và sau đó bị chiếm đoạt các thông tin đó với mục đích xấu.

(3) Các doanh nghiệp chủ động thu thập thông tin cá nhân của khách hàng, tuy nhiên, các thông tin thu thập lại nhiều quá mức so với nhu cầu của hệ thống. Ví dụ, để sử dụng các ứng dụng trên điện thoại, nhà phát triển ứng dụng yêu cầu người dùng phải đồng ý cấp quyền truy cập camera, danh bạ, bộ sưu tập ảnh và video…, từ đó hình thành kho dữ liệu cá nhân phục vụ cho việc kinh doanh, buôn bán.

(4) Các doanh nghiệp thu thập dữ liệu cá nhân của khách hàng, sau đó cho phép các đối tác thứ ba tiếp cận các thông tin này nhưng lại không có các quy định chặt chẽ, để đối tác thứ ba chuyển giao, buôn bán cho các đối tác khác.

(5) Tấn công trực tiếp vào hệ thống lưu trữ thông tin khách hàng của doanh nghiệp, sau đó bán cho đối thủ của họ hoặc các bên liên quan khác.

##### **Quản lý nhà nước đối với bảo vệ dữ liệu cá nhân**

Các quốc gia trên thế giới

Vấn đề bảo vệ dữ liệu cá nhân đã được nhiều quốc gia rất coi trọng. Hiện nay, đã có hơn 80 quốc gia ban hành văn bản quy phạm pháp luật về bảo vệ dữ liệu cá nhân.

Đầu tiên phải kể đến là Quy định chung về bảo vệ dữ liệu ban hành ngày 14/4/2016 của Liên minh châu Âu (EU) (được gọi là GDPR), quy định cách xử lý và chuyển dữ liệu cá nhân ở EU. GDPR bảo vệ người dân EU khỏi việc thu thập hoặc xử lý dữ liệu bất hợp pháp, đồng thời đưa ra các yêu cầu về sự đồng ý cũng như các quyền nâng cao khác của người dùng. Các yêu cầu của GDPR áp dụng cho mọi quốc gia thành viên của EU nhằm mục đích tạo ra sự bảo vệ nhất quán đối với dữ liệu cá nhân và người tiêu dùng ở tất cả các quốc gia EU. Có thể nói, GDPR khá toàn diện khi áp dụng cho tất cả các lĩnh vực và công ty thuộc mọi quy mô, dù nằm trong hay nằm ngoài lãnh thổ châu Âu cũng phải chấp hành các quy định này. Nó đã truyền cảm hứng và là cơ sở cho sự ra đời của các luật về bảo vệ dữ liệu nói chung và dữ liệu cá nhân nói riêng trên toàn thế giới.

Tại Nhật Bản, từ năm 2003, Luật Bảo vệ thông tin cá nhân (APPI) đã được ban hành để quản lý các vấn đề về quyền riêng tư ở Nhật Bản. Đây là một trong những quy định bảo vệ dữ liệu đầu tiên ở châu Á. APPI đã được sửa đổi nhiều lần để phù hợp hơn với GDPR, lần sửa đổi gần nhất có hiệu lực từ ngày 01/04/2022 với sự mở rộng phạm vi quyền của chủ thể dữ liệu Nhật Bản, bắt buộc phải thông báo vi phạm dữ liệu và hạn chế phạm vi thông tin cá nhân có thể được gửi cho bên thứ ba2.

Ở Vương quốc Anh, việc bảo vệ dữ liệu được điều chỉnh bởi hai quy định chính là GDPR và Đạo luật bảo vệ dữ liệu (DPA) năm 2018 . Tại Anh, doanh nghiệp phải minh bạch về lý do thu thập dữ liệu cá nhân, cách họ dự định sử dụng dữ liệu đó và nhận được sự đồng ý rõ ràng từ người dùng. Tất cả các tổ chức ở Vương quốc Anh khi xử lý dữ liệu cá nhân phải tuân thủ hai luật bảo mật dữ liệu này nếu không sẽ phải đối mặt với mức phạt lên tới 17,5 triệu bảng Anh hoặc 4% doanh thu toàn cầu hàng năm, tùy theo mức nào lớn hơn3.

Tại Hoa Kỳ, cho đến hiện tại không có luật bảo mật dữ liệu nào được áp dụng ở cấp liên bang nhưng một số tiểu bang có luật bảo mật dữ liệu riêng. Ví dụ, như: Đạo luật về quyền riêng tư California (CPRA), Đạo luật bảo vệ dữ liệu của người tiêu dùng Virginia (CDPA), Đạo luật về quyền riêng tư Colorado (CPA), Đạo luật về quyền riêng tư của người tiêu dùng Utah (UCPA), Đạo luật về quyền riêng tư dữ liệu của Connecticut (CTDPA).

Tại Brazil, Luật bảo vệ dữ liệu chung (LGPD) là khung pháp lý để điều chỉnh việc thu thập và sử dụng dữ liệu cá nhân có hiệu lực vào ngày 16/08/2020. LGPD chịu ảnh hưởng của Quy định bảo vệ dữ liệu chung (GDPR) của Liên minh Châu Âu, yêu cầu các tổ chức ưu tiên quyền riêng tư dữ liệu trước tiên, đồng thời cân bằng điều này với mục tiêu doanh thu và tạo mối quan hệ với khách hàng. Nếu không tuân thủ, các công ty có thể phải chịu mức phạt lên tới hàng triệu Real Brazil.

Tại Trung Quốc, Luật Bảo vệ Thông tin Cá nhân (PIPL) có hiệu lực từ ngày 01/11/2021. Cùng với Luật An ninh mạng và Luật An ninh dữ liệu, PIPL là luật thứ ba của Trung Quốc nhằm bảo đảm cách tiếp cận tích hợp về an ninh mạng, bảo mật dữ liệu và quyền riêng tư dữ liệu. Như vậy PIPL có một số yếu tố rất giống với GDPR của EU.

Trong khu vực Đông Nam Á, tính đến tháng 9/2022 có 5 quốc gia có luật cụ thể về bảo vệ dữ liệu cá nhân bao gồm: Malaysia (thông qua năm 2010), Singapore (thông qua năm 2012), Philippines (thông qua năm 2012), Thái Lan (thông qua năm 2019), và Indonesia (thông qua năm 2022).

Được thảo luận từ năm 2016 nhưng đến cuối tháng 9/2022, Indonesia mới thông qua Luật Bảo vệ dữ liệu cá nhân. Luật này đưa ra các khung hình phạt nghiêm khắc đối với những chủ thể xử lý dữ liệu làm rò rỉ hoặc sử dụng sai mục đích thông tin cá nhân, tiền phạt lên đến 2% doanh thu hằng năm đối với doanh nghiệp và án tù lên đến 6 năm. Luật bao gồm giai đoạn “điều chỉnh” hai năm nhưng không nêu rõ phương thức xử lý vi phạm trong giai đoạn này. Theo những quy định mới, nạn nhân của việc sử dụng sai dữ liệu có quyền yêu cầu được bồi thường cho việc vi phạm dữ liệu cá nhân và có quyền rút lại sự đồng ý cho phép sử dụng dữ liệu.

Đạo luật Bảo vệ dữ liệu cá nhân (PDPA) của Thái Lan có hiệu lực vào ngày 01/6/2022, chịu ảnh hưởng lớn từ GDPR của EU. Luật này gồm những quy định mà các lĩnh vực công và tư phải tuân thủ khi thu thập, sử dụng dữ liệu cá nhân để bảo vệ sự riêng tư và an ninh. Tương tự như GDPR, PDPA có phạm vi ngoài lãnh thổ, tức là nó áp dụng cho tất cả các tổ chức thu thập, sử dụng hoặc tiết lộ dữ liệu cá nhân ở Thái Lan hoặc của cư dân Thái Lan, bất kể họ được thành lập hay công nhận theo luật pháp Thái Lan hay không và họ có phải là cư dân hay hiện diện kinh doanh ở Thái Lan hay không.

Trước đó, PDPA của Singapore được thông qua năm 2012 và có hiệu lực vào năm 2014. Lần được sửa đổi, gần đây nhất là vào năm 2021. Luật này có hiệu lực ngoài lãnh thổ, áp dụng cho mọi công ty xử lý dữ liệu của cư dân Singapore. Các tổ chức cần nhận được sự đồng ý để xử lý dữ liệu cá nhân, sự đồng ý có thể là khẳng định hoặc được coi là đồng ý. Dữ liệu cá nhân của người dùng có thể được chuyển ra nước ngoài nhưng quốc gia đó cần phải cung cấp tiêu chuẩn bảo vệ tương đương với tiêu chuẩn mà luật pháp Singapore quy định. Những yêu cầu này khiến PDPA của Singapore trở thành một trong những đạo luật bảo vệ dữ liệu nghiêm ngặt nhất ở Đông Nam Á.

Tại Việt Nam

Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân được Chính phủ Việt Nam thông qua vào ngày 17/04/2023 và chính thức có hiệu lực từ ngày 01/07/2023 (Nghị định 13). Theo thống kê, trước khi Nghị định 13 được ban hành, Việt Nam có tổng cộng 68 văn bản quy phạm pháp luật liên quan trực tiếp đến bảo vệ dữ liệu cá nhân bao gồm: Hiến pháp, 4 bộ luật (Bộ luật dân sự, Luật công nghệ thông tin, Luật Bảo vệ quyền lợi người tiêu dùng và Luật an toàn thông tin mạng), 39 luật, 1 pháp lệnh, 18 nghị định, 4 thông tư và thông tư liên tịch, 1 quyết định của bộ trưởng. Tuy nhiên, trong tất cả các văn bản này đều chưa sử dụng thuật ngữ “dữ liệu cá nhân” mà chủ yếu sử dụng thuật ngữ “thông tin cá nhân”. Hơn nữa, khái niệm và nội hàm của thuật ngữ “thông tin cá nhân” trong các văn bản này cũng chưa được thống nhất.

Nghị định 13 bao gồm 44 Điều được chia thành 4 chương. Đây là văn bản pháp lý có vai trò quan trọng trong việc bảo đảm quyền riêng tư và bảo vệ dữ liệu cá nhân của người dân Việt Nam. Nghị định có một số nội dung nổi bật như sau:

– Về phạm vi: Nghị định 13 có phạm vi ngoài lãnh thổ, tức là áp dụng đối mọi cá nhân, tổ chức trong nước hoặc nước ngoài có liên quan đến việc xử lý dữ liệu cá nhân tại Việt Nam, bao gồm cả việc xử lý dữ liệu cá nhân là công dân Việt Nam được thực hiện bên ngoài lãnh thổ Việt Nam.

– Về cách xác định dữ liệu cá nhân: theo Nghị định 13, dữ liệu cá nhân là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể. Dữ liệu cá nhân bao gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm.

Một số dữ liệu cá nhân cơ bản bao gồm: họ và tên; ngày, tháng, năm sinh/chết/mất tích; giới tính; nơi sinh, nơi đăng ký khai sinh, nơi thường trú, nơi tạm trú, nơi ở hiện tại, quê quán, địa chỉ liên hệ; quốc tịch; hình ảnh của cá nhân;…

Dữ liệu cá nhân nhạy cảm là dữ liệu cá nhân gắn liền với quyền riêng tư của cá nhân mà khi bị xâm phạm sẽ gây ảnh hưởng trực tiếp tới quyền và lợi ích hợp pháp của cá nhân gồm: quan điểm chính trị, quan điểm tôn giáo; tình trạng sức khỏe và đời tư được ghi trong hồ sơ bệnh án, không bao gồm thông tin về nhóm máu; thông tin liên quan đến nguồn gốc chủng tộc, nguồn gốc dân tộc;… Lưu ý rằng nội hàm của thuật ngữ dữ liệu cá nhân nhạy cảm theo Nghị định 13 là rộng hơn so với GDPR của EU, theo đó các thông tin tài chính như tổ chức tín dụng, ngân hàng… cũng được coi là dữ liệu nhạy cảm.

– Một số quy định chính của Nghị định 13: nghiêm cấm việc mua, bán dữ liệu cá nhân; dữ liệu cá nhân chỉ được xử lý đúng với mục đích đã đăng ký và tuyên bố. Các quy định này cũng làm cho Nghị định 13 chặt chẽ hơn so với GDPR khi GDPR không có bất kỳ lệnh cấm chung nào đối với việc bán hoặc chia sẻ dữ liệu cá nhân, và người kiểm soát dữ liệu có thể xử lý dữ liệu cá nhân cho “các mục đích tương đương”.

Về việc thông báo xử lý dữ liệu cá nhân cho chủ thể dữ liệu: sẽ được thực hiện một lần trước khi tiến hành và phải bao gồm các nội dung: (1) Mục đích xử lý; (2) Loại dữ liệu cá nhân được sử dụng (có liên quan tới mục đích xử lý); (3) Cách thức xử lý; (4) Thông tin về các tổ chức, cá nhân khác có liên quan tới mục đích xử lý; (5) Hậu quả, thiệt hại không mong muốn có khả năng xảy ra; (6) Thời gian bắt đầu, thời gian kết thúc xử lý dữ liệu.

Về việc xác định sự đồng ý của chủ thể dữ liệu: được thực hiện dựa trên nguyên tắc tự nguyện và biết rõ các nội dung trong thông báo xử lý dữ liệu cá nhân. Sự đồng ý này phải được thể hiện rõ ràng, cụ thể bằng văn bản, giọng nói hoặc một hành động khác thể hiện được điều này. Sự đồng ý phải được thể hiện ở một định dạng có thể được in, sao chép bằng văn bản. Sự im lặng hoặc không phản hồi của chủ thể dữ liệu không được coi là sự đồng ý.

Các quyền của chủ thể dữ liệu: bao gồm 11 quyền: quyền được biết; quyền đồng ý; quyền truy cập; quyền rút lại sự đồng ý; quyền xóa dữ liệu; quyền hạn chế xử lý dữ liệu; quyền cung cấp dữ liệu; quyền phản đối xử lý dữ liệu; quyền khiếu nại, tố cáo, khởi kiện; quyền yêu cầu bồi thường thiệt hại; quyền tự bảo vệ.

Việc thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân: bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân cần thông báo cho cơ quan chức năng (cụ thể là Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an) chậm nhất 72 giờ sau khi xảy ra hành vi vi phạm.

Việc chuyển dữ liệu cá nhân ra nước ngoài sẽ được tiến hành trong trường hợp bên chuyển dữ liệu ra nước ngoài lập hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài và gửi 1 bản chính bộ hồ sơ này tới cơ quan chức năng trong vòng 60 ngày kể từ ngày tiến hành xử lý dữ liệu cá nhân.

Về chế tài đối với các hành vi vi phạm: tùy theo mức độ vi phạm mà có thể bị xử lý kỷ luật, xử phạt vi phạm hành chính, xử lý hình sự theo quy định.

##### **Một số kiến nghị trong việc thực thi Nghị định 13**

Nghị định 13 được ban hành với nội dung khá toàn diện, đây là cơ sở trực tiếp và quan trọng trong việc bảo vệ dữ liệu cá nhân. Cùng với đó, việc triển khai Nghị định 13 cần được quan tâm, sát sao để việc ban hành thực sự có ý nghĩa. Để làm được điều đó, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao – Bộ Công an cần sớm có những hướng dẫn cụ thể về việc thi hành Nghị định 13, đặc biệt ở ba nhóm nội dung chính như sau:

Thứ nhất, việc thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân đã được quy định trong Điều 23 Nghị định 13. Tuy nhiên, nội dung của điều khoản này mới chỉ đề cập tới việc báo cáo vi phạm cho Bộ Công an, cụ thể là Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao chứ chưa đề cập tới việc phải thông báo vi phạm cho chủ thể dữ liệu. Trong khi đó, Điều 9 về Quyền của chủ thể dữ liệu đã chỉ ra rằng, chủ thể dữ liệu có quyền yêu cầu bồi thường thiệt hại khi có vi phạm liên quan tới dữ liệu cá nhân của mình. Vậy, Bộ Công an cần có hướng dẫn, bổ sung để bảo đảm quyền lợi cho chủ thể dữ liệu.

Thứ hai, về biện pháp bảo vệ dữ liệu cá nhân. Điều 26 trong Nghị định 13 đã nhấn mạnh rằng việc bảo vệ dữ liệu cá nhân cần được tiến hành ngay từ khi bắt đầu và trong suốt quá trình xử lý dữ liệu cá nhân. Ngoài các biện pháp theo chức năng quản lý của Nhà nước, có hai nhóm giải pháp bảo vệ do các cá nhân, tổ chức có liên quan thực hiện bao gồm các biện pháp quản lý và các biện pháp kỹ thuật. Tuy nhiên, các hướng dẫn về giải pháp quản lý, đặc biệt là giải pháp kỹ thuật nào bảo đảm tiêu chuẩn lại chưa được đề cập.

Thứ ba, về chế tài bảo đảm thi hành Nghị định 13. Theo đó, Điều 4 Nghị định 13 quy định về ba chế tài, tùy theo mức độ vi phạm và chủ thể thực hiện hành vi bao gồm xử lý kỷ luật, xử phạt vi phạm hành chính và xử lý hình sự. Tuy nhiên, hiện chưa có hành lang pháp lý để xử lý kỷ luật một tổ chức, cũng như chưa có quy định về xử phạt vi phạm hành chính và quy định xử lý hình sự trực tiếp đối với hành vi vi phạm về bảo vệ dữ liệu cá nhân theo Nghị định 13. Bộ Công an cần sớm hoàn thiện khung chế tài để Nghị định 13 bảo đảm tính răn đe.

##### **Kết luận**

Trong bối cảnh bùng nổ thương mại điện tử và kinh tế số, dữ liệu cá nhân ngày càng thể hiện vai trò quan trọng. Tuy nhiên, việc thu thập và xử lý dữ liệu cá nhân một cách đúng đắn và hợp pháp thì không phải lúc nào cũng được thực hiện, ảnh hưởng tới quyền riêng tư cũng như các quyền lợi hợp pháp của các cá nhân. Do đó, việc bảo vệ dữ liệu cá nhân là cần thiết và cần phải làm triệt để. Chính phủ Việt Nam đã ban hành nhiều văn bản luật và nghị định đề cập tới vấn đề này, trong đó Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân là trực tiếp và toàn diện nhất. Vấn đề tiếp theo là cần triển khai Nghị định 13 một cách quyết liệt, có trách nhiệm để bảo đảm an toàn dữ liệu cá nhân trong bối cảnh hiện nay.

**Chú thích**:

1. PGS.TS. Vũ Công Giao, ThS. Lê Trần Như Tuyên. 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. Tạp chí Nghiên cứu Lập pháp số 09 (409), tháng 5/2020.

2.  Pháp luật dân sự Nhật Bản về bảo vệ dữ liệu cá nhân trong hoạt động giao dịch thương mại điện tử và kinh nghiệm cho Việt Nam. https://danchuphapluat.vn, ngày 27/6/2023.

3. Data Protection Act 2018.

4. Quản trị không gian mạng các nước ASEAN năm 2022. https://antoanthongtin.vn, ngày 28/4/2023.

**Tài liệu tham khảo**:

1. Bộ luật Dân sự năm 2015.

2. Luật An toàn thông tin mạng năm 2015.

3. Luật Bảo vệ quyền lợi người tiêu dùng năm 2010.

4. Luật Công nghệ thông tin năm 2006.

###### 5. Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân.

###### **Tác giả: ThS. Vũ Thị Hải Lý,** Trường Đại học Thương mại

###### Nguồn: https://www.quanlynhanuoc.vn/2024/01/30/quan-ly-nha-nuoc-ve-bao-ve-du-lieu-ca-nhan-thuc-trang-va-kien-nghi/