PHÁP LUẬT MỘT SỐ QUỐC GIA VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN - MỘT SỐ BÀI HỌC KINH NGHIỆM VÀ GIẢI PHÁP HOÀN THIỆN PHÁP LUẬT VIỆT NAM

BÙI THỊ ÁNH LINH
Công ty TNHH Dịch vụ kỹ thuật công nghiệp PVChem

Nhận bài ngày 27/3/2025. Sửa chữa xong 31/3/2025. Duyệt đăng 05/4/2025.

Abstract

In the context of strong digital transformation taking place globally, personal data is becoming a particularly valuable asset class, but at the same time it also faces many risks of abuse and infringement. Many countries have enacted relatively complete legal frameworks to protect personal data, such as the European Union, the United States, and China. The article analyzes the experiences of some countries in developing and enforcing laws on personal data protection, thereby drawing lessons for Vietnam and proposing some solutions to improve the law, ensure effectiveness in personal data protection and promote sustainable digital economic development.

Keywords: *Protection, personal data, personal information, national law, experience.*

1. Đặt vấn đề

Cùng với sự phát triển bùng nổ của công nghệ số, đặc biệt là các nền tảng số, mạng xã hội, thương mại điện tử (TMĐT) và trí tuệ nhân tạo, dữ liệu cá nhân đang ngày càng trở thành trung tâm của mọi hoạt động trong đời sống kinh tế - xã hội. Bảo vệ dữ liệu cá nhân không chỉ liên quan đến quyền con người mà còn liên quan đến an ninh mạng, an ninh quốc gia và lợi ích phát triển bền vững của quốc gia trong thời đại số. Tuy nhiên, thực tiễn cho thấy dữ liệu cá nhân đang bị thu thập, khai thác, chia sẻ và thậm chí bị mua bán một cách phổ biến mà chưa có sự kiểm soát chặt chẽ. Người dân thường không biết dữ liệu của mình bị thu thập ra sao, sử dụng vào mục đích gì, lưu trữ trong bao lâu và ai có quyền tiếp cận. Trong khi đó, hành lang pháp lý để điều chỉnh hoạt động xử lý dữ liệu cá nhân ở Việt Nam vẫn còn nhiều khoảng trống.

Trên thế giới, nhiều quốc gia đã đi trước trong việc ban hành và thực hiện các quy định pháp luật nghiêm ngặt về bảo vệ dữ liệu cá nhân. Việc tìm hiểu, phân tích những điểm mạnh và hạn chế trong mô hình pháp luật của các quốc gia như Liên minh châu Âu, Hoa Kỳ hay Trung Quốc sẽ giúp Việt Nam có thêm cơ sở thực tiễn để tham khảo và lựa chọn những giải pháp phù hợp với điều kiện cụ thể trong nước. Từ đó, bài viết hướng đến việc đưa ra một số bài học kinh nghiệm và đề xuất giải pháp nhằm hoàn thiện pháp luật Việt Nam trong lĩnh vực quan trọng và mang tính thời sự này.

2. Nội dung nghiên cứu

2.1. Quy định pháp luật một số quốc gia về bảo vệ dữ liệu cá nhân

2.1.1. Liên minh châu Âu

Năm 2016, Liên minh châu Âu đã chính thức thông qua Quy định chung về bảo vệ dữ liệu (General Data Protection Regulation – viết tắt là GDPR) nhằm thay thế cho Chỉ thị 95/46/EC trước đó. Đây là một văn bản pháp lý chuyên biệt, gồm tổng cộng 99 điều khoản và kèm theo 173 phần trích dẫn giải thích. Những điều khoản và phần trích dẫn này đóng vai trò như kim chỉ nam, giúp các bên liên quan

Email: anhlinhbui1310@gmail.com

hiểu rõ nội dung và cách thực thi luật một cách thống nhất. 99 điều trong văn bản được chia thành 11 chương khác nhau, tạo nên một hệ thống quy phạm rõ ràng, nhằm đảm bảo rằng các tổ chức hoặc cá nhân giữ vai trò quản lý dữ liệu, xử lý dữ liệu, cũng như các cơ quan giám sát dữ liệu trong khối EU có thể tuân thủ đầy đủ các yêu cầu mà GDPR đặt ra. GDPR được xem là một trong những văn bản pháp lý điển hình của thế giới trong lĩnh vực bảo vệ dữ liệu cá nhân, bởi những quy định rất chặt chẽ và minh bạch về việc xác định hành vi vi phạm, quy định chế tài xử phạt, cũng như thiết lập một quy trình nghiêm ngặt để bảo vệ thông tin dữ liệu nhạy cảm của cá nhân.

a. Về chế tài, trách nhiệm pháp lý và mức phạt

Trong trường hợp hành vi vi phạm được xác định là nghiêm trọng, cơ quan có thẩm quyền ở các quốc gia thành viên Liên minh châu Âu có quyền áp dụng mức phạt tiền lên tới 20 triệu Euro (tương đương khoảng 22 triệu đô la Mỹ), hoặc 4% tổng doanh thu toàn cầu của tổ chức vi phạm – tùy theo mức nào cao hơn[1]. Mức phạt này được tính cho từng hành vi cụ thể, không áp dụng theo gói hay giới hạn cho toàn bộ vụ việc. Bên cạnh đó, cá nhân có thông tin cá nhân bị xử lý sai cách, không đúng quy định của GDPR có thể gửi đơn khiếu nại đến cơ quan quản lý có thẩm quyền để yêu cầu xử lý vụ việc. Ngoài ra, những người bị ảnh hưởng bởi hành vi vi phạm còn có quyền khởi kiện đối với các cá nhân hoặc tổ chức đóng vai trò kiểm soát hoặc xử lý dữ liệu, đây là những chủ thể có trách nhiệm pháp lý về hành vi vi phạm để yêu cầu bồi thường các thiệt hại thực tế đã phát sinh.

b. Về cơ quan giám sát độc lập.

Nội dung được đề cập tại Chương 6 của GDPR quy định rằng mỗi quốc gia thành viên thuộc Liên minh châu Âu đều có nghĩa vụ thành lập ít nhất một cơ quan giám sát nhằm bảo đảm việc thực hiện đúng quy định pháp luật về bảo vệ dữ liệu cá nhân. Cơ quan giám sát này có trách nhiệm giám sát hoạt động xử lý dữ liệu trong phạm vi quốc gia mình, đảm bảo rằng các quyền và tự do cá nhân của người dân được bảo vệ, đồng thời góp phần thúc đẩy sự lưu chuyển thông tin trong nội bộ khối EU theo hướng an toàn và thống nhất. Mặc dù các cơ quan giám sát ở mỗi nước có thể phối hợp với nhau để đảm bảo sự thống nhất trong việc áp dụng GDPR, nhưng mỗi cơ quan đều có quyền thực hiện chức năng giám sát và ra quyết định một cách độc lập, theo các nhiệm vụ và quyền hạn được quy định cụ thể trong Điều 57 và Điều 58 của văn bản này. Bên cạnh đó, GDPR cũng quy định cụ thể các yêu cầu đối với người đảm nhiệm vị trí trong cơ quan giám sát, điều kiện hoạt động, cũng như cơ chế thành lập cơ quan này theo nội dung tại Điều 53[2].

Ngoài ra, Điều 59 của GDPR cũng yêu cầu các cơ quan giám sát phải lập báo cáo hàng năm về toàn bộ hoạt động của mình. Những bản báo cáo này không chỉ phải được công bố công khai cho người dân biết mà còn phải gửi tới các cơ quan chính phủ, Ủy ban châu Âu và Ban Bảo vệ dữ liệu của Liên minh châu Âu nhằm phục vụ công tác kiểm tra, giám sát và đánh giá việc thực thi quy định pháp luật về bảo vệ dữ liệu trong toàn khối.

2.1.2. Hoa Kỳ

a. Quy định về chế tài, trách nhiệm pháp lý và mức xử phạt

Xét tổng thể, pháp luật của Hoa Kỳ về bảo vệ dữ liệu cá nhân bao quát khá đầy đủ các loại chế tài, từ biện pháp dân sự, hành chính cho tới hình sự, nhằm xử lý các hành vi xâm phạm hoặc vi phạm quy định trong các đạo luật liên quan. Ví dụ, Đạo luật về Quyền riêng tư của người tiêu dùng California (CCPA) quy định rằng người tiêu dùng có quyền khởi kiện trong trường hợp thông tin cá nhân của họ bị truy cập trái phép, bị đánh cắp hoặc bị tiết lộ mà nguyên nhân là do doanh nghiệp không thực hiện đầy đủ nghĩa vụ bảo mật dữ liệu. Ngoài ra, Văn phòng công tố bang California cũng có quyền xử phạt doanh nghiệp không tuân thủ quy định của CCPA với mức phạt từ 2.500 đến 7.500 đô la Mỹ cho mỗi hành vi vi phạm, căn cứ theo quy định tại Điều 1798.155 của Bộ luật Dân sự California. So

1) GDPR Điều 83.
2) GDPR Điều 53.

với hệ thống GDPR của châu Âu khi mức phạt được tính theo phần trăm doanh thu toàn cầu, có thể lên đến hàng chục triệu euro thì mức xử phạt theo CCPA được đánh giá là nhẹ hơn, và có phần kém hiệu quả hơn về mặt răn đe.

b. Quy định về cơ quan giám sát độc lập

Tại Hoa Kỳ hiện chưa có một văn bản luật liên bang mang tính toàn diện về bảo vệ dữ liệu cá nhân, và do đó cũng không tồn tại một cơ quan giám sát tập trung có trách nhiệm thống nhất về lĩnh vực này trên toàn quốc. Tuy vậy, pháp luật Hoa Kỳ lại phân chia trách nhiệm giám sát cho từng lĩnh vực cụ thể, với các cơ quan có thẩm quyền độc lập được giao nhiệm vụ thực thi pháp luật trong phạm vi ngành của mình. Chẳng hạn, Bộ Y tế và Dịch vụ Nhân sinh (HHS) được giao trách nhiệm giám sát việc thực hiện đạo luật HIPAA và có quyền điều tra, xử phạt đối với các hành vi vi phạm liên quan đến thông tin y tế cá nhân. Ủy ban Thương mại Liên bang (FTC) là cơ quan chịu trách nhiệm thi hành quy định bảo mật theo đạo luật GLBA, cũng như thực thi đạo luật bảo vệ quyền riêng tư của trẻ em trên môi trường trực tuyến (COPPA). Ngoài ra, Văn phòng công tố bang California là cơ quan có thẩm quyền xử lý các vi phạm theo quy định của CCPA. Dù không có một cơ quan trung ương thống nhất, nhưng các cơ quan nói trên đều có quyền độc lập trong việc tiến hành điều tra và áp dụng hình phạt phù hợp với phạm vi quản lý của mình.

Một điểm khác biệt đáng chú ý là các quy định pháp luật của Hoa Kỳ thường chỉ áp dụng cho một phạm vi hẹp các chủ thể, chủ yếu là những tổ chức hoặc cá nhân có hoạt động trong lãnh thổ nước này, và đối tượng được bảo vệ cũng chỉ giới hạn trong công dân hoặc người cư trú tại Hoa Kỳ. Trong khi đó, hệ thống pháp luật của Liên minh châu Âu lại áp dụng rộng rãi hơn, khi bảo vệ tất cả các cá nhân có thể nhận diện được, bất kể quốc tịch hay nơi cư trú của họ[3]. Cách định nghĩa về "dữ liệu cá nhân" trong các văn bản pháp luật của Hoa Kỳ cũng thường hẹp hơn so với định nghĩa tương ứng trong pháp luật châu Âu, điều này ảnh hưởng trực tiếp đến phạm vi và mức độ áp dụng các quy định bảo vệ [4].

Tuy có sự phân tán trong hệ thống cơ quan giám sát, nhưng thực tế cho thấy việc thực thi pháp luật tại Hoa Kỳ vẫn đạt được những kết quả đáng ghi nhận. Ví dụ, trong năm 2021, FTC đã tham gia giải quyết hai vụ việc liên quan đến việc vi phạm quyền riêng tư của trẻ em theo đạo luật COPPA, một vụ với một nền tảng cung cấp quảng cáo trực tuyến, vụ còn lại với một nhà phát triển phần mềm dành cho trẻ em. Hai bên vi phạm đã đồng ý nộp các khoản tiền phạt tương ứng là 2 triệu và 3 triệu đô la Mỹ để giải quyết tranh chấp. Trong cùng năm, do ảnh hưởng từ đại dịch Covid-19 và sự gia tăng nhu cầu sử dụng các dịch vụ y tế từ xa, Bộ Y tế và Dịch vụ Nhân sinh (HHS) – cơ quan giám sát thực thi HIPAA – đã phát hành một văn bản có tên gọi là "Thông báo về tùy ý thực thi", trong đó cho phép các nhà cung cấp dịch vụ y tế được linh hoạt sử dụng các nền tảng liên lạc video trực tuyến để chăm sóc bệnh nhân, miễn là họ hành động trên tinh thần thiện chí[5]. Quyết định này cho thấy khả năng thích ứng và vai trò điều tiết thực tiễn của các cơ quan quản lý theo từng lĩnh vực chuyên ngành trong bối cảnh xã hội có nhiều biến động.

2.1.3. Trung Quốc

Tại Trung Quốc, hệ thống pháp luật về bảo vệ dữ liệu cá nhân đã có những bước phát triển đáng kể, đặc biệt là với sự ra đời và có hiệu lực của Luật Bảo vệ thông tin cá nhân (PIPL) từ năm 2021, cùng với Luật An ninh mạng, Bộ luật Dân sự và Bộ luật Hình sự – các văn bản có liên quan đến điều chỉnh vấn đề bảo vệ dữ liệu cá nhân. PIPL được thiết kế gồm 8 chương với tổng cộng 74 điều, thiết lập một khuôn khổ pháp lý tương đối toàn diện nhằm bảo vệ thông tin cá nhân của công dân Trung Quốc.

a. Quy định về chế tài, trách nhiệm pháp lý, mức phạt

PIPL quy định rõ các biện pháp xử lý hành chính đối với các hành vi vi phạm quy định về bảo vệ dữ liệu. Mức phạt tối đa có thể lên tới 5% doanh thu hàng năm hoặc 50 triệu nhân dân tệ (tương đương

3) GDPR Điều 4(1).

khoảng 7,7 triệu USD), tùy theo mức nào cao hơn. Đây là một mức phạt mang tính răn đe rõ rệt, được đánh giá là có sự tham chiếu hợp lý với cơ chế xử phạt hành chính của GDPR.

b. Quy định về cơ quan giám sát độc lập

Khác với mô hình châu Âu, PIPL không thiết lập một cơ quan giám sát độc lập chuyên trách cho việc thực thi các quy định về quyền riêng tư dữ liệu. Thay vào đó, Cục Quản lý Không gian mạng Trung Quốc (CAC) giữ vai trò chủ đạo trong việc thực thi, bên cạnh đó còn có một số cơ quan quản lý khác phụ trách các lĩnh vực cụ thể – ví dụ, việc bảo vệ dữ liệu liên quan đến tín dụng được giao cho Ngân hàng Nhân dân Trung Quốc (PBOC). Cách phân bổ thẩm quyền này phần nào tương đồng với mô hình đa cơ quan tại Hoa Kỳ, và vẫn còn tồn tại những điểm chưa rõ ràng về ranh giới trách nhiệm giữa các cơ quan [6].

Kể từ khi PIPL có hiệu lực, hiệu quả thực thi của văn bản này đã bắt đầu được thể hiện rõ nét. Nhiều tổ chức quốc tế đã tiến hành đánh giá tác động của PIPL đối với hoạt động của họ khi có liên quan đến Trung Quốc. Các cơ quan chức năng Trung Quốc cũng đã tăng cường các hoạt động thực thi, đặc biệt là đối với hành vi thu thập dữ liệu trái phép và tình trạng rò rỉ thông tin cá nhân. Cùng với đó, việc quản lý dữ liệu cá nhân trên các nền tảng ứng dụng di động cũng được tăng cường. Kể từ năm 2020, CAC, Bộ Công nghiệp và Công nghệ Thông tin (MIIT), cùng với Cục Công an Trung Quốc (PSB), đã thực hiện các chiến dịch kiểm tra, giám sát nghiêm ngặt đối với các hành vi thu thập thông tin cá nhân quá mức, sử dụng trái phép chức năng đẩy thông báo, và hạn chế quyền thực hiện của chủ thể dữ liệu. Năm 2021, nhiều ứng dụng giáo dục và đào tạo trực tuyến, bao gồm cả Offcn – một công ty có tiếng trong lĩnh vực giáo dục nghề – đã bị xử lý vì vi phạm quyền riêng tư của người dùng. Các biện pháp thực thi nêu trên cho thấy cơ quan chức năng Trung Quốc hiện đang chú trọng đến các vấn đề như cơ chế đồng ý, bảo vệ dữ liệu trong lĩnh vực giáo dục và các ứng dụng công nghệ. Bộ Giáo dục Trung Quốc vào năm 2021 cũng đã ban hành một số văn bản hướng dẫn nhằm thúc đẩy hoạt động bảo vệ thông tin cá nhân trong bối cảnh gia tăng mạnh mẽ của các chương trình giáo dục trực tuyến.

2.2. Một số bài học kinh nghiệm đối với Việt Nam

Từ kinh nghiệm xây dựng và thực thi pháp luật bảo vệ dữ liệu cá nhân tại Liên minh châu Âu, Hoa Kỳ và Trung Quốc, Việt Nam có thể rút ra một số bài học kinh nghiệm, vừa mang tính tham khảo, vừa phù hợp với bối cảnh trong nước.

2.2.1. Liên minh châu Âu là hình mẫu điển hình về cách tiếp cận toàn diện, thống nhất và lấy cá nhân làm trung tâm trong bảo vệ dữ liệu. Với Quy định chung về bảo vệ dữ liệu (GDPR), EU đã thiết lập khung pháp lý nghiêm ngặt, quy định rõ các nguyên tắc xử lý dữ liệu, quyền của cá nhân, trách nhiệm của bên xử lý và đặc biệt là cơ chế thực thi hiệu quả với mức phạt rất cao. Việt Nam có thể học hỏi việc xây dựng một đạo luật có tính hệ thống, minh bạch và bảo vệ quyền lợi của cá nhân một cách rõ ràng, đồng thời chú trọng thiết lập cơ chế giám sát độc lập, giống như mô hình Cơ quan bảo vệ dữ liệu của các nước thành viên EU.

2.2.2. Mô hình của Hoa Kỳ thiên về điều chỉnh theo ngành hoặc lĩnh vực, đặt trọng tâm vào trách nhiệm giải trình của doanh nghiệp, bảo vệ người tiêu dùng và an ninh quốc gia. Mặc dù không có đạo luật liên bang thống nhất về bảo vệ dữ liệu cá nhân, nhưng nhiều đạo luật chuyên biệt như HIPAA, COPPA hay CCPA ở các bang lớn vẫn cho thấy sự linh hoạt và tính ứng dụng cao. Từ kinh nghiệm này, Việt Nam có thể cân nhắc kết hợp giữa luật khung và các văn bản hướng dẫn cụ thể theo lĩnh vực, để vừa đảm bảo tính linh hoạt vừa có sự điều chỉnh phù hợp với đặc thù từng ngành.

2.2.3. Trung Quốc với PIPL lại lựa chọn hướng tiếp cận kết hợp giữa mô hình châu Âu và Hoa Kỳ. Dù không có một cơ quan giám sát độc lập chuyên trách, nhưng Trung Quốc vẫn tổ chức bộ máy thực thi rộng khắp, lồng ghép bảo vệ dữ liệu vào các lĩnh vực khác như tài chính, giáo dục, công nghệ. PIPL quy định mức phạt nghiêm khắc, có tác dụng răn đe mạnh, đồng thời các cơ quan như CAC hay Bộ

Công an đã vào cuộc tích cực, đặc biệt trong giám sát các ứng dụng di động và nền tảng công nghệ. Việt Nam có thể tham khảo kinh nghiệm này trong việc phân cấp trách nhiệm quản lý dữ liệu cá nhân cho các cơ quan theo ngành, đồng thời chú trọng ứng dụng công nghệ vào giám sát và xử lý vi phạm.

2.2.4. Một điểm chung của cả ba mô hình là việc chú trọng đến nhận thức và vai trò của người dân. EU coi trọng quyền chủ thể dữ liệu và yêu cầu doanh nghiệp minh bạch tối đa. Hoa Kỳ khuyến khích sự tham gia của người tiêu dùng vào việc giám sát thông tin cá nhân của họ. Trung Quốc đã bắt đầu xử lý các vụ kiện dân sự liên quan đến quyền riêng tư, cho thấy người dân ngày càng quan tâm và chủ động bảo vệ thông tin cá nhân. Việt Nam cũng cần đặt trọng tâm vào việc nâng cao nhận thức của người dân, giúp họ hiểu rõ quyền và trách nhiệm trong môi trường số, tránh tình trạng thờ ơ hay phó mặc dữ liệu cá nhân cho các nền tảng công nghệ.

2.2.5. Trong bối cảnh toàn cầu hóa và chuyển đổi số mạnh mẽ, Việt Nam không thể đứng ngoài xu thế xây dựng một hệ thống pháp luật về bảo vệ dữ liệu cá nhân hiện đại, hội nhập và khả thi. Việc tham khảo kinh nghiệm của các quốc gia và khu vực nêu trên không nhằm sao chép máy móc, mà để chọn lọc những yếu tố phù hợp, từ đó tạo ra một mô hình pháp luật đặc thù, có khả năng áp dụng hiệu quả tại Việt Nam trong thời gian tới.

2.3. Một số giải pháp hoàn thiện pháp luật Việt Nam

2.3.1. Cần sớm ban hành một đạo luật chuyên biệt, có hiệu lực pháp lý cao, điều chỉnh một cách toàn diện các vấn đề liên quan đến dữ liệu cá nhân. Kinh nghiệm quốc tế cho thấy rằng, một văn bản dưới luật sẽ khó có thể bao quát được đầy đủ các vấn đề pháp lý phát sinh trong quá trình xử lý dữ liệu cá nhân. Hơn nữa, khi chưa có luật thì mức độ ràng buộc, tính ổn định và tính khả thi của các quy định vẫn còn bị hạn chế. Luật cần quy định rõ ràng các khái niệm pháp lý cơ bản, phân loại các loại dữ liệu cá nhân, xác định rõ nghĩa vụ của các bên liên quan, đồng thời đặt ra cơ chế giám sát, chế tài và xử lý vi phạm một cách cụ thể, chi tiết. Việc xây dựng đạo luật này cũng cần dựa trên quá trình đánh giá kỹ lưỡng các mô hình pháp luật quốc tế, lựa chọn những điểm phù hợp để nội luật hóa, đồng thời phản ánh được điều kiện kinh tế - xã hội, trình độ phát triển công nghệ và mức độ nhận thức của người dân Việt Nam.

2.3.2. Cần quy định rõ ràng về quyền của chủ thể dữ liệu. Hiện nay, trong nhiều trường hợp, người dân không thực sự hiểu rõ họ có quyền gì đối với dữ liệu cá nhân của mình, cũng như không biết phải làm gì khi quyền riêng tư của họ bị xâm phạm. Vì vậy, pháp luật cần xác lập một cách cụ thể các quyền của chủ thể dữ liệu như quyền được biết, quyền truy cập, quyền yêu cầu chỉnh sửa, xóa bỏ dữ liệu, quyền phản đối, quyền yêu cầu giới hạn xử lý, và đặc biệt là quyền được rút lại sự đồng ý. Đi kèm với việc ghi nhận quyền là trách nhiệm của các tổ chức, cá nhân thu thập và xử lý dữ liệu phải bảo đảm cho người dân có thể thực hiện các quyền này một cách dễ dàng, thuận tiện và minh bạch. Việc xây dựng các biểu mẫu, quy trình chuẩn để người dân thực hiện các quyền này cũng là điều cần thiết để tránh hình thức hoặc bị phức tạp hóa.

2.3.3. Việt Nam cần xây dựng một cơ quan giám sát độc lập có thẩm quyền rõ ràng trong việc bảo vệ dữ liệu cá nhân. Kinh nghiệm từ Liên minh châu Âu với Cơ quan giám sát độc lập được thành lập theo GDPR cho thấy mô hình này đã giúp nâng cao đáng kể mức độ tuân thủ pháp luật và bảo vệ quyền của người dân. Ở Việt Nam, hiện nay chức năng giám sát bảo vệ dữ liệu cá nhân chủ yếu vẫn nằm trong thẩm quyền của Bộ Công an. Tuy nhiên, cơ chế giám sát như vậy có thể chưa đáp ứng được yêu cầu về tính độc lập, minh bạch và hiệu quả trong dài hạn. Do đó, cần tính tới việc thành lập một cơ quan độc lập hoặc ít nhất là một cơ quan chuyên trách với đủ năng lực, thẩm quyền và nguồn lực để thực hiện vai trò giám sát việc tuân thủ pháp luật về bảo vệ dữ liệu cá nhân trong toàn xã hội.

2.3.4. Chế tài xử lý vi phạm cần được quy định nghiêm khắc hơn, đặc biệt là đối với các hành vi thu thập, sử dụng, chia sẻ dữ liệu cá nhân trái phép. Hiện nay, nhiều tổ chức, doanh nghiệp vẫn

vi phạm các quy định về thu thập và xử lý dữ liệu cá nhân mà không phải chịu hậu quả pháp lý nghiêm trọng. Pháp luật cần bổ sung các chế tài xử lý hành chính với mức phạt cao, cũng như quy định rõ ràng về trách nhiệm bồi thường dân sự trong trường hợp dữ liệu cá nhân bị xâm phạm gây thiệt hại. Đặc biệt, với các doanh nghiệp công nghệ lớn có khả năng xử lý dữ liệu với quy mô lớn, cần quy định mức phạt dựa trên tỷ lệ phần trăm doanh thu toàn cầu, tương tự như mô hình của GDPR để đảm bảo tính công bằng và hiệu quả. Ngoài ra, cũng cần thiết lập cơ chế xử lý hình sự đối với các hành vi có mức độ nguy hiểm cao, xâm phạm nghiêm trọng đến quyền riêng tư của cá nhân hoặc được thực hiện có tổ chức.

2.3.5. Cần chú trọng đến công tác phổ biến pháp luật và nâng cao nhận thức của cộng đồng về quyền bảo vệ dữ liệu cá nhân. Thực tế cho thấy, không ít người dân, đặc biệt ở khu vực nông thôn, vùng sâu, vùng xa vẫn chưa có khái niệm rõ ràng về dữ liệu cá nhân, thậm chí chưa từng nghe nói đến khái niệm này. Họ thường dễ dàng chia sẻ các thông tin cá nhân như số CMND, số tài khoản ngân hàng, mã OTP… cho người khác mà không lường hết được rủi ro. Điều này xuất phát từ việc pháp luật chưa được truyền thông đầy đủ, hiệu quả, bằng những hình thức phù hợp với từng nhóm đối tượng. Vì vậy, cần đa dạng hóa các hình thức truyền thông pháp luật, từ việc sử dụng mạng xã hội, truyền hình, radio, đến việc đưa nội dung về bảo vệ dữ liệu cá nhân vào chương trình giáo dục phổ thông và đại học. Đồng thời, cần có sự tham gia của các tổ chức xã hội, các hiệp hội nghề nghiệp và doanh nghiệp công nghệ trong việc nâng cao nhận thức chung về quyền riêng tư và bảo vệ dữ liệu cá nhân.

3. Kết luận

Hoàn thiện pháp luật về bảo vệ dữ liệu cá nhân ở Việt Nam là một yêu cầu cấp thiết, cần có cách tiếp cận tổng thể, bài bản, không chỉ về mặt nội dung pháp lý mà còn cả về tổ chức thực thi và nâng cao nhận thức xã hội. Đây là nền tảng quan trọng để bảo vệ quyền con người trong thời đại số và xây dựng một môi trường số an toàn, văn minh, đáng tin cậy.

Tài liệu tham khảo

[1] Liên minh châu Âu (2016), *Quy định chung về bảo vệ dữ liệu.*

[2] Hoa Kỳ (2018), *Đạo luật về Quyền riêng tư của người tiêu dùng California.*

[3] Trung Quốc (2021), *Luật Bảo vệ thông tin cá nhân.*

[4] Paul Schwartz & Daniel Solove, 2013, *Reconciling Personal Information in the United States and European Union (tạm dịch: Hòa giải thông tin cá nhân giữa Hoa Kỳ và Liên minh Châu Âu)*, nguồn: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2103&context=faculty_publications. , truy cập ngày 13/4/2025.

[5] F Paul Pittman, Abdul Hafiz, Andrew Hamm (2024), *Data Protection Laws and Regulations USA 2022 – 2023 (tạm dịch: Các luật và quy định về bảo vệ dữ liệu tại Mỹ 2022-2023)*, ICLG, nguồn: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa, truy cập ngày 13/4/2025.

[6] Bo Zhao, GP (Jeanne) Mifsud Bonnici (2016), *Protecting EU Citizens' Personal Data in China: a Reality or a Fantacy? (tạm dịch: Bảo vệ dữ liệu cá nhân của công dân EU tại Trung Quốc: một hiện thực hay một giấc mơ?)*, International Journal of Law and Information Technology, nguồn: https://academic.oup.com/ijlit/article-abstract/24/2/128/1750163?redirectedFrom=fulltext, truy cập ngày 13/4/2025.