

PHÁP LUẬT MỘT SỐ QUỐC GIA VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN - KHUYẾN NGHỊ CHO VIỆT NAM TRONG BỐI CẢNH CHUYỂN ĐỔI SỐ

ĐINH THI THANH THỦY*

Abstract: In the era of digital transformation, personal data has become a valuable resource, often referred to as “black gold” due to its significant value. Personal data is collected, analyzed, and stored for various purposes, including commercial activities, research, and labor management. Meanwhile, incidents of personal data breaches worldwide have been increasing rapidly, creating an urgent need to establish effective mechanisms for the control and protection of personal data.

This article analyzes the legal regulations on personal data protection in several representative jurisdictions, including the European Union (EU), the United States, and China. On that basis, it proposes several lessons and recommendations for improving Vietnam’s legal framework on personal data protection.

Keywords: *Personal Data Protection; Legal Framework; Digital Transformation.*

1. Đặt vấn đề

Trong bối cảnh dữ liệu và mối quan hệ dữ liệu đối với quyền cá nhân của con người ngày càng trở nên quan trọng, nhiều quốc gia trên thế giới đã ban hành nhiều văn bản pháp lý nhằm xác lập nguyên tắc xử lý dữ liệu một cách minh bạch, công bằng và có trách nhiệm, đồng thời có cơ chế bảo vệ, kiểm soát hệ thống và yêu cầu tuân thủ chặt chẽ đối với dữ liệu cá nhân (DLCN) của các chủ thể trong bối cảnh chuyển đổi số mạnh mẽ (Liên minh Châu Âu với Quy định chung về bảo vệ dữ liệu (GDPR) và Đạo luật AI (AI Act)).

Trong chiến lược Chuyển đổi số Quốc gia đến năm 2025, tầm nhìn 2030, Việt Nam đặt mục tiêu đưa kinh tế số chiếm 20% GDP vào năm 2025 và 30% vào năm 2030, trong đó dữ liệu là một trong ba trụ cột chính bên cạnh hạ tầng số và nhân lực số. Để hiện thực hoá mục tiêu này, Việt Nam đã ban hành các văn bản pháp luật như Luật An ninh mạng 2018, Luật An toàn thông tin mạng 2015, Luật Dữ liệu (hiệu lực 1/7/2025), Luật Bảo vệ dữ liệu cá nhân (hiệu lực 1/1/2026)... và các văn bản hướng dẫn thi hành. Tuy nhiên, trên thực tế, nhiều quy định hiện hành vẫn còn phân tán, chưa tạo thành một khung pháp lý đồng bộ và đầy đủ để bảo đảm, bảo vệ DLCN trước những thách thức mới của công nghệ chuyển đổi số hiện tại. Bài viết đặt vấn đề nghiên cứu, phân tích các quy định pháp luật của một số quốc gia điển hình về bảo vệ DLCN, từ đó rút ra những bài học phù hợp cho Việt Nam trong việc xây dựng và hoàn thiện khung pháp lý trong lĩnh vực này giúp đảm bảo quyền và lợi ích hợp pháp về dữ liệu của cá nhân, đồng thời tạo điều kiện thuận lợi cho đổi mới sáng tạo và phát triển bền vững trong kỷ nguyên số là cần thiết.

2. Pháp luật một số quốc gia về bảo vệ dữ liệu cá nhân trong bối cảnh chuyển đổi số

Dữ liệu cá nhân còn được gọi là thông tin cá nhân (personal information), thông tin nhận dạng cá nhân (personally identifying information - PII) hoặc thông tin cá nhân nhạy cảm (sensitive personal information - SPI), (<https://vi.wikipedia.org/wiki>). Tuyên ngôn Toàn cầu về Nhân quyền (UDHR) được Đại hội đồng Liên hợp quốc công bố ngày 10 tháng 12 năm 1948 khẳng định nghĩa vụ tôn trọng đời sống riêng tư, chỉ cho phép xử lý dữ liệu theo mục đích xác định, trên cơ sở đồng ý và bảo đảm an toàn cho cá nhân dữ liệu (Điều 12). Như vậy, dữ liệu của cá nhân thuộc sở hữu của cá nhân đó, là quyền riêng tư, quyền con người được luật pháp quốc tế thừa nhận và bảo vệ.

2.1. Luật về bảo vệ dữ liệu (GDPR - General Data Protection Regulation) của Liên minh châu Âu, chính thức có hiệu lực từ ngày 25/5/2018 ra đời với bốn mục tiêu chính: *Một là*, tạo ra một thị trường chung kỹ thuật số, nơi những doanh nghiệp có thể hoạt động tự do mà không bị cản trở bởi các quy định khác nhau về bảo vệ dữ liệu quốc gia thành viên. GDPR giúp đơn giản hoá các quy định về bảo vệ dữ liệu trong EU, tạo điều kiện cho doanh nghiệp hoạt động dễ dàng hơn; *Hai là*, trao nhiều

* Trường Đại học Thủy lợi; Email: thuydingh@tlu.edu.vn

quyền kiểm soát cho cá nhân đối với DLCN, chẳng hạn như quyền truy cập, sửa đổi, xoá và hạn chế việc sử dụng dữ liệu, giúp cá nhân kiểm soát tốt hơn dữ liệu và bảo vệ quyền riêng tư của họ; *Ba là*, yêu cầu các tổ chức thực hiện những biện pháp kỹ thuật và tổ chức phù hợp để bảo vệ DLCN khỏi bị truy cập trái phép, sử dụng sai mục đích hoặc tiết lộ, giúp tăng cường an ninh mạng và giảm thiểu nguy cơ rò rỉ dữ liệu; *Bốn là*, áp đặt các hình phạt nghiêm khắc đối với các vi phạm. Phạm vi áp dụng của GDPR không giới hạn ở lãnh thổ EU, mà bao gồm cả các tổ chức nằm ngoài EU nhưng có hoạt động xử lý DLCN của công dân EU với những nguyên tắc cơ bản về xử lý DLCN, bao gồm: (i) Nguyên tắc 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. (ii) Giới hạn mục đích đã xác định, rõ ràng và hợp pháp; (iii) Tối thiểu hoá dữ liệu, vừa đủ cần thiết để đạt mục tiêu xử lý; (iv) Dữ liệu phải chính xác và được cập nhật kịp thời; (v) Giới hạn thời gian lưu trữ dữ liệu đủ để hoàn thành mục đích thu thập ban đầu; (vi) Bảo mật và toàn vẹn dữ liệu tránh các rủi ro mất mát, phá hủy, hoặc truy cập bất hợp pháp; (vi) Trách nhiệm giải trình - Người kiểm soát dữ liệu có trách nhiệm chứng minh tuân thủ GDPR đối với tất cả các nguyên tắc này (Điều 5.1-2).

Cùng với đó, quyền kiểm soát dữ liệu của các cá nhân cũng được GDPR xác định gồm: (i) Quyền được biết với quy định người dùng phải được thông báo về việc thu thập dữ liệu (Điều 12-14); (ii) Quyền truy cập quy định việc người dùng có thể yêu cầu doanh nghiệp cung cấp thông tin về dữ liệu cá nhân của họ (Điều 15); (iii) Quyền chỉnh sửa quy định về việc sửa đổi dữ liệu cá nhân nếu có sai sót (Điều 16); (iv) Quyền xoá dữ liệu quy định việc cá nhân có thể yêu cầu doanh nghiệp xoá dữ liệu của họ vĩnh viễn (Điều 17); (v) Quyền phản đối quy định việc từ chối việc sử dụng dữ liệu của họ cho mục đích tiếp thị; (vi) Quyền di chuyển dữ liệu quy định về việc người dùng có thể yêu cầu chuyển dữ liệu sang một nền tảng khác; (vii) Các quyền liên quan đến việc ra quyết định tự động và lập hồ sơ cá nhân (Điều 18- Điều 22). GDPR cũng không chấp nhận bất kì việc chỉ định hoặc ủy thác các quyền này cho người khác. Về bản chất, GDPR xây dựng dựa trên các điều khoản trong Chỉ thị EU nhưng đã củng cố thêm một số quyền của chủ thể dữ liệu (quyền chuyển nhượng dữ liệu và quyền được lãng quên) và giới thiệu một số khái niệm mới (đánh giá tác động bảo vệ dữ liệu, quyền riêng tư và thông báo vi phạm dữ liệu) (G. González Fuster, & R. Gellert, 2012).

2.2. Đạo luật Dữ liệu (Data Act) của Liên minh Châu Âu (có hiệu lực từ 11/1/2024, áp dụng từ 12/9/2025) là khung pháp lý toàn diện nhằm thúc đẩy kinh tế dữ liệu, giải quyết những thách thức và khai thác những cơ hội do dữ liệu mang lại, nhấn mạnh quyền truy cập công bằng và quyền của người dùng, đồng thời đảm bảo bảo vệ dữ liệu cá nhân. Luật cho phép người dùng (cá nhân/doanh nghiệp) tiếp cận dữ liệu từ sản phẩm kết nối (IoT) và chia sẻ với bên thứ ba, đồng thời yêu cầu nhà cung cấp dịch vụ đám mây dễ dàng chuyển đổi. Theo đó, các quyền truy cập dữ liệu trong Luật Dữ liệu bao gồm: (i) Quyền truy cập dữ liệu phải được thiết kế và mặc định đảm bảo. Các sản phẩm kết nối/dịch vụ liên quan phải được thiết kế và sản xuất/cung cấp theo cách mà dữ liệu sản phẩm và dịch vụ liên quan có thể truy cập được theo mặc định. Việc truy cập phải dễ dàng, an toàn, toàn diện, có cấu trúc và được cung cấp ở định dạng thông dụng và có thể đọc được bằng máy. Người dùng phải được truy cập miễn phí; (ii) Truy cập trực tiếp. Khi cần thiết và khả thi về mặt kỹ thuật, dữ liệu phải được người dùng truy cập trực tiếp, nghĩa là không cần yêu cầu truy cập dữ liệu. Các nghĩa vụ minh bạch liên quan của người nắm giữ dữ liệu bao gồm: (i) Trước khi ký kết hợp đồng mua, thuê hoặc cho thuê sản phẩm kết nối, người bán, người cho thuê hoặc người cho thuê (có thể là nhà sản xuất) phải cung cấp thông tin cụ thể cho người dùng một cách rõ ràng và dễ hiểu; (ii) Thông tin tương tự phải được cung cấp cho người dùng các dịch vụ liên quan đến sản phẩm được kết nối. Nếu không thể truy cập trực tiếp, người nắm giữ dữ liệu phải cung cấp dữ liệu một cách dễ dàng cho người dùng. Người dùng cũng có thể yêu cầu người nắm giữ dữ liệu cung cấp dữ liệu cho bên thứ ba. Như vậy, các yêu cầu chính đối với người nắm giữ dữ liệu khi xử lý yêu cầu truy cập dữ liệu được đặt ra là: Chủ sở hữu dữ liệu không được phép gây khó khăn quá mức cho sự lựa chọn hoặc quyền lợi của người dùng; Chủ sở hữu dữ liệu không được lưu giữ bất kì thông tin nào về việc người dùng truy cập dữ liệu, được yêu cầu vượt quá mức cần thiết để thực hiện yêu cầu truy cập một cách hợp lệ và để đảm bảo an ninh và duy trì cơ sở hạ tầng dữ liệu. Ngoài ra, việc truy cập và sử dụng dữ liệu có thể bị hạn chế trong một số điều kiện nhất định, bao gồm cả vì mục đích an ninh và bảo vệ bí mật thương mại. Như vậy, GDPR của EU xem DLCN như

một sự mở rộng của quyền con người và mỗi cá nhân có quyền tự chủ hoàn toàn đối với thông tin cá nhân, DLCN mang tính không thể tách rời, tương tự như quyền riêng tư hay quyền tự do ngôn luận. Do đó, cá nhân không “sở hữu” dữ liệu như một tài sản có thể mua bán hoặc chuyển nhượng toàn bộ mà thay vào đó, chủ thể dữ liệu có quyền kiểm soát và giới hạn cách thức dữ liệu được sử dụng.

Như vậy, Data Act không ảnh hưởng đến các quyền và nghĩa vụ theo GDPR và không tạo ra bất kỳ cơ sở pháp lý mới nào cho việc xử lý DLCN, hay nói cách khác, GDPR được ưu tiên áp dụng khi dữ liệu được điều chỉnh bởi Đạo luật dữ liệu là “dữ liệu cá nhân”. Nhìn chung, việc tuân thủ GDPR và Đạo luật Dữ liệu sẽ gặp nhiều thách thức do cách diễn giải hạn chế của các cơ quan bảo vệ dữ liệu đối với GDPR và nguyên tắc giảm thiểu dữ liệu, yêu cầu không xử lý nhiều dữ liệu cá nhân hơn mức cần thiết. Do đó, các doanh nghiệp cần phải xây dựng một chính sách được cân nhắc kỹ lưỡng và xem xét các lựa chọn phù hợp, đặc biệt là việc ẩn danh hoá dữ liệu, vốn có thể là một quá trình phức tạp, tốn thời gian và nguồn lực.

2.3. Tại Mỹ đã ban hành Luật Bảo vệ Quyền riêng tư của Người tiêu dùng California (CCPA) là một đạo luật về bảo vệ dữ liệu được ban hành tại California vào năm 2018 và có hiệu lực từ ngày 1 tháng 1 năm 2020. CCPA nhằm mục đích tăng cường quyền riêng tư và bảo vệ người tiêu dùng cho cư dân California (California Consumer Privacy Act (CCPA). (2020). Đạo luật này trao cho người tiêu dùng California quyền được biết các doanh nghiệp thu thập những thông tin cá nhân nào về họ, dữ liệu được sử dụng như thế nào và được chia sẻ với ai. người tiêu dùng có một số quyền, bao gồm quyền truy cập thông tin cá nhân của họ, quyền yêu cầu xóa dữ liệu của họ, quyền từ chối việc bán thông tin cá nhân của họ và quyền không bị phân biệt đối xử khi thực hiện các quyền CCPA của họ. Các tổ chức thuộc phạm vi điều chỉnh của CCPA phải tuân thủ các quyền của người tiêu dùng này và thực hiện các biện pháp bảo mật thích hợp để bảo vệ dữ liệu cá nhân. CCPA áp dụng cho các doanh nghiệp vì lợi nhuận thu thập thông tin cá nhân của người tiêu dùng, hoạt động kinh doanh tại California và đáp ứng một số ngưỡng doanh thu hoặc xử lý dữ liệu nhất định. Mỹ thực hiện mô hình dữ liệu mở qua cổng Data.gov, cung cấp hơn 250.000 bộ dữ liệu công khai, từ dữ liệu khí hậu đến kinh tế, tạo điều kiện cho doanh nghiệp khai thác dữ liệu linh hoạt, nhưng thiếu sự kiểm soát tập trung có thể dẫn đến lạm dụng dữ liệu. Việt Nam có thể tham khảo mô hình này nhằm khuyến khích khu vực tư nhân trên cơ sở những điều kiện kinh tế xã hội phù hợp của đất nước.

Ở cấp liên bang, Mỹ đã xây dựng các luật điều chỉnh việc bảo vệ, thu thập và xử lý dữ liệu trong từng lĩnh vực mà không hình thành một đạo luật thống nhất, có thể kể đến như: Luật Bảo vệ quyền riêng tư trực tuyến của trẻ em dưới 13 tuổi (COPPA - 1998) năm 1998 là Luật Liên bang Hoa Kỳ (có hiệu lực từ năm 2000) yêu cầu các trang web/dịch vụ trực tuyến thương mại phải có sự đồng ý xác thực của phụ huynh trước khi thu thập, sử dụng dữ liệu cá nhân từ trẻ em dưới 13 tuổi trên các ứng dụng di động, định vị địa lý, ảnh và video, nhằm mục đích bảo vệ an toàn cho trẻ; Đạo luật HIPAA năm 1996 (Health Insurance Portability and Accountability Act) là tiêu chuẩn Hoa Kỳ bắt buộc nhằm bảo vệ sự riêng tư và bảo mật thông tin sức khỏe cá nhân (PHI). Luật này yêu cầu các nhà cung cấp dịch vụ y tế, bảo hiểm thiết lập các biện pháp an ninh kỹ thuật, vật lý và hành chính để ngăn chặn việc truy cập, chia sẻ trái phép dữ liệu y tế điện tử (ePHI). Hiện nay, để tạo ra một khuôn khổ toàn diện, thống nhất về quyền riêng tư tại Hoa Kỳ, thay thế cho các luật tiểu bang riêng lẻ hiện nay, dự luật liên bang về quyền riêng tư dữ liệu đầu tiên của Hoa Kỳ American Data Privacy Protection Act (ADPPA) được thông qua tại ủy ban với sự đồng thuận cao (năm 2022), hướng tới thiết lập các quy tắc thống nhất về cách các doanh nghiệp thu thập, sử dụng và bảo vệ dữ liệu cá nhân trên toàn quốc. ADPPA cung cấp cho người dùng quyền kiểm soát cao hơn đối với thông tin cá nhân của họ. Khi được thông qua, luật sẽ cho phép người dùng truy cập, chỉnh sửa, xóa và chuyển dữ liệu, cũng như từ chối việc bán hoặc sử dụng dữ liệu cho quảng cáo cá nhân hoá...

Có thể thấy rằng, việc ban hành nhiều đạo luật về quyền riêng tư và bảo vệ DLCN ở các bang khác nhau ở Mỹ khiến cho các doanh nghiệp gặp nhiều khó khăn trong thực thi và thiếu sự thống nhất, toàn diện trong triển khai áp dụng vấn đề này

2.4. Hiện tại ở Trung Quốc có ba đạo luật liên quan đến bảo vệ dữ liệu và thông tin: Luật An toàn không gian mạng (Cyber Security Law - CSL) được thực thi vào ngày 01/6/2017; Luật An toàn dữ liệu

(Data Security Law - DSL) có hiệu lực từ ngày 01/9/2021; Luật bảo vệ thông tin cá nhân (Personal Information Protection Law - PIPL) mới được thông qua và sẽ có hiệu lực vào ngày 01/11/2021. PIPL xác định các nguyên tắc chủ yếu trong bảo vệ quyền riêng tư DLCN là: Doanh nghiệp phải được sự đồng ý từ người dùng trước khi thu thập, xử lý dữ liệu cũng như khi bán dữ liệu, người dùng có quyền truy cập, chỉnh sửa, xóa dữ liệu cá nhân, đặc biệt đối với những dữ liệu quan trọng phải được lưu trữ trong lãnh thổ quốc gia, nếu muốn chuyển ra ngoài biên giới phải xin phép chính quyền. PIPL quy định mức phạt đối với các vi phạm khá nghiêm khắc với 5% doanh thu hàng năm hoặc gần 7 triệu USD. So với CSL, DSL định nghĩa dữ liệu rộng hơn và không giới hạn ở dữ liệu điện tử trong mạng công nghệ thông tin viễn thông, thuộc thẩm quyền của CSL. Ngoài ra, trọng tâm bảo vệ dữ liệu của DSL khác với PIPL, chủ yếu tập trung vào bảo vệ dữ liệu từ góc độ thông tin cá nhân, trong khi DSL tập trung vào việc bảo vệ dữ liệu nhằm bảo đảm an ninh quốc gia. Đặc biệt, một số điều khoản đáng chú ý của DSL đó là: (i) cơ quan quản lý Trung ương về an ninh chịu trách nhiệm ra quyết định chính, cân nhắc và điều phối nhiệm vụ bảo vệ dữ liệu của quốc gia; nghiên cứu, soạn thảo và hướng dẫn triển khai chiến lược bảo vệ dữ liệu quốc gia và các chỉ thị chính sách lớn có liên quan; lập kế hoạch, điều phối, thiết lập cơ chế phối hợp cho công tác bảo vệ dữ liệu quốc gia (Điều 5); (ii) Nhà nước thiết lập hệ thống phân loại và bảo vệ dữ liệu, thực hiện phân loại và bảo vệ dữ liệu theo mức độ quan trọng đối với sự phát triển kinh tế - xã hội của Nhà nước, cũng như cấp độ nguy hại đối với an ninh quốc gia, lợi ích xã hội hoặc lợi ích hợp pháp của cá nhân, tổ chức nếu dữ liệu bị giả mạo, hư hỏng, rò rỉ hoặc bị sử dụng bất hợp pháp (Điều 21); (iii) Nhà nước thiết lập một cơ chế tập trung, hiệu quả và có thẩm quyền để đánh giá, báo cáo, chia sẻ thông tin, giám sát và cảnh báo rủi ro về bảo vệ dữ liệu (Điều 22); (iv) Các đơn vị thực hiện hoạt động xử lý dữ liệu phải thiết lập và hoàn thiện hệ thống quản lý bảo vệ dữ liệu trong toàn bộ quy trình làm việc, tổ chức và thực hiện đào tạo về bảo vệ dữ liệu, áp dụng các biện pháp kỹ thuật tương ứng và các biện pháp cần thiết khác để bảo vệ an toàn dữ liệu theo quy định của pháp luật (Điều 27); (v) Việc chuyển ra nước ngoài các dữ liệu quan trọng do nhà điều hành cơ sở hạ tầng thông tin trọng yếu thu thập và tạo ra trong quá trình hoạt động trên lãnh thổ Trung Quốc sẽ phải tuân theo các yêu cầu Luật CSL của Trung Quốc; việc chuyển ra nước ngoài các dữ liệu quan trọng do các đơn vị xử lý dữ liệu khác thu thập và tạo ra trong quá trình hoạt động của họ trên lãnh thổ Trung Quốc sẽ phải tuân theo các quy tắc do Cơ quan quản lý không gian mạng quốc gia và các cơ quan liên quan của Quốc Vụ viện xây dựng (Điều 31, Luật Dữ liệu của Trung Quốc (2021)... Những quy định này có giá trị tham khảo cho Việt Nam trong việc tiếp tục hoàn thiện pháp luật về bảo vệ DLCN.

2.5. Singapore là trung tâm dữ liệu và công nghệ lớn, nơi đặt trụ sở của các công ty công nghệ lớn như Google, Facebook, Microsoft... phát triển với những giao dịch dữ liệu được cung cấp bởi AI, phân tích dữ liệu lớn (Big Data), blockchain... *Luật Bảo vệ Dữ liệu Cá nhân (PDPA - Personal Data Protection Act, 2012, sửa đổi 2020)* quy định doanh nghiệp phải xin phép trước khi thu thập và xử lý dữ liệu cá nhân, đồng thời người dùng có quyền truy cập, chỉnh sửa, xóa dữ liệu cá nhân, đặc biệt luật cho phép việc chuyển dữ liệu ra nước ngoài nếu đáp ứng được tiêu chuẩn bảo mật. Theo đó, khung pháp luật của Singapore khá linh hoạt trong việc điều chỉnh vấn đề dữ liệu xuyên biên giới. Cùng với đó, PDPA cũng quy định mức phạt nêu vi phạm lên tới 10% doanh thu toàn cầu hoặc 750 nghìn USD (Vũ Thị Hải Lý, 2024).

3. Đánh giá chung quy định pháp luật Việt Nam về bảo vệ dữ liệu cá nhân và một số bài học kinh nghiệm

Xuyên suốt trong tinh thần của các bản Hiến pháp của Việt Nam đều khẳng định quyền riêng tư của cá nhân là bất khả xâm phạm, đồng thời phát triển mở rộng phạm vi quyền riêng tư không chỉ về thân thể, nhà ở, thư tín mà còn bao gồm quyền bảo vệ bí mật cá nhân, trong đó có thông tin về đời sống riêng tư, bí mật cá nhân, bí mật gia đình (Điều 21, Hiến pháp sửa đổi năm 2025). Quy định này thể hiện cam kết của Nhà nước trong việc bảo vệ nhân quyền cơ bản, vừa là cơ sở pháp lý cho việc điều chỉnh thu thập và xử lý DLCN trong các quan hệ xã hội, bao gồm cả quan hệ lao động; Bộ luật Dân sự 2015 quy định nghĩa vụ bảo mật thông tin trong quan hệ hợp đồng, theo đó các bên không được tiết lộ hoặc sử dụng thông tin về đời sống riêng tư, bí mật cá nhân, bí mật gia đình mà mình biết được trong quá trình giao kết và thực hiện hợp đồng cho mục đích riêng hoặc mục đích trái pháp luật (khoản 4,

Điều 38 và khoản 2, Điều 387), do đó, hợp đồng lao động, xét về bản chất pháp lý, là một dạng hợp đồng dân sự đặc thù; do đó, quy định này có ý nghĩa trực tiếp trong việc ràng buộc doanh nghiệp phải bảo mật DLCN của NLĐ mà họ có được trong quá trình tuyển dụng và quản lý lao động. Bộ luật Lao động năm 2019 quy định về quyền riêng tư, được bảo vệ danh dự, uy tín, danh dự, nhân phẩm và bí mật đời tư tại nơi làm việc, người sử dụng lao động không được yêu cầu cung cấp thông tin không liên quan trực tiếp đến việc giao kết hợp đồng lao động (Điều 8, Điều 21, Điều 169), Luật An toàn thông tin mạng, Luật Công nghệ thông tin và một số các văn bản pháp luật khác có quy định liên quan đều đề cập đến quyền được bảo vệ về dữ liệu thông tin của cá nhân. Nghị định 13/2023/NĐ-CP được ban hành và có hiệu lực từ tháng 7/2023, được xem là bước ngoặt trong nỗ lực xây dựng khung pháp lý về bảo vệ DLCN tại Việt Nam, lần đầu đã xác lập rõ các quyền của chủ thể dữ liệu, bao gồm quyền được biết, quyền đồng ý, quyền truy cập, chỉnh sửa, xoá bỏ và phản đối việc xử lý dữ liệu cá nhân. Điều 2, Luật Bảo vệ DLCN năm 2025 quy định DLCN bao gồm DLCN cơ bản là các yếu tố nhân thân, lai lịch phổ biến, thường xuyên sử dụng trong các giao dịch, quan hệ xã hội thuộc danh mục do Chính phủ ban hành hoặc DLCN nhạy cảm gắn liền với quyền riêng tư của cá nhân, khi bị xâm phạm sẽ gây ảnh hưởng trực tiếp đến quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

Có thể thấy, quy định về bảo vệ DLCN trong pháp luật Việt Nam có góc độ tiếp cận khác so với pháp luật EU, Hoa Kỳ, Trung Quốc... về quyền của chủ thể dữ liệu, cơ chế thực thi, quản lý dữ liệu, quy định phân loại dữ liệu theo tính chất và quyền tài sản gắn liền, phân định quyền sở hữu dữ liệu giữa cá nhân, tổ chức và nhà nước, tùy theo nguồn gốc dữ liệu như: dữ liệu cá nhân, dữ liệu sản sinh từ hoạt động sản xuất, dữ liệu công... Trước ảnh hưởng sâu rộng của cuộc Cách mạng công nghiệp 4.0 hiện nay cho thấy, pháp luật Việt Nam về bảo vệ DLCN cần sớm hoàn thiện một số vấn đề như sau:

Một là, một số quy định của pháp luật hiện hành về bảo vệ quyền đối với DLCN thiếu rõ ràng, nặng về nguyên tắc, có thể dẫn đến hiểu và áp dụng sai; tiếp tục hoàn thiện khung pháp lý về quyền sở hữu dữ liệu và cơ chế kiểm soát, quản lý dữ liệu.

Hai là, cần thống nhất chế tài xử lý vi phạm về DLCN trong các Luật chuyên ngành (Luật Xử lý vi phạm hành chính, Luật Dân sự, Luật Hình sự...) đảm bảo tính răn đe, nghiêm khắc của pháp luật.

Ba là, hiện nay Việt Nam vẫn chưa quy định cơ chế cho việc chuyển dữ liệu ra nước ngoài hoặc nhập dữ liệu từ các quốc gia khác. Điều này khiến cho thị trường Việt Nam bị giới hạn và mất nhiều cơ hội để phát triển kinh tế trong bối cảnh mở rộng hợp tác quốc tế,

Một số bài học kinh nghiệm cho Việt Nam hiện nay

Thứ nhất, rà soát, sửa đổi quy định trong các văn bản pháp luật chuyên ngành về dữ liệu và bảo vệ dữ liệu như Bộ luật Dân sự, Luật Sở hữu trí tuệ, Luật Giao dịch điện tử... bổ sung thêm những quy định phù hợp về quyền sở hữu dữ liệu, thúc đẩy dữ liệu mở, xây dựng quy định phân loại dữ liệu theo tính chất và quyền tài sản gắn liền, phân định quyền sở hữu dữ liệu giữa cá nhân, tổ chức và nhà nước, tùy theo nguồn gốc dữ liệu như: dữ liệu cá nhân, dữ liệu sản sinh từ hoạt động sản xuất, dữ liệu công... Theo kinh nghiệm của pháp luật EU, Trung Quốc, cần coi dữ liệu cũng là tài sản, tài sản đặc biệt, tài sản phi vật thể. Việc xác định quyền sở hữu, quyền kiểm soát, quyền sử dụng và quyền định đoạt dữ liệu cũng tương tự như quyền tài sản, có cơ chế chia sẻ lợi ích cho người sở hữu hoặc tạo ra dữ liệu nếu dữ liệu cá nhân hoặc dữ liệu cộng đồng tạo ra giá trị kinh tế.

Thứ hai, hoàn thiện chế tài xử phạt các hành vi vi phạm dữ liệu đảm bảo tính răn đe, không tái phạm hành vi vi phạm. Ngoài hình thức phạt tiền, Việt Nam có thể cân nhắc các hình phạt bổ sung như đình chỉ hoạt động đối với các doanh nghiệp vi phạm nhiều lần, buộc doanh nghiệp khắc phục hậu quả và bồi thường cho người dùng bị ảnh hưởng, cấm doanh nghiệp vi phạm tham gia giao dịch dữ liệu trong thời gian nhất định

Thứ ba, Luật DSL của Trung Quốc với nhiều quy định có giá trị tham khảo cho Việt Nam, trong đó có quy định về cơ chế để kiểm soát chặt việc chuyển dữ liệu qua biên giới mà không được cơ quan nhà nước có thẩm quyền cho phép; sớm cần nhanh chóng xây dựng trung tâm dữ liệu quốc gia (National Big Data Center) do Nhà nước quản lý tập trung và yêu cầu tất cả các tổ chức, doanh nghiệp trong nước

có trách nhiệm kết nối máy chủ và chia sẻ dữ liệu với trung tâm này. Cần có sự quản lý tập trung, thống nhất dữ liệu của các tỉnh, thành, bộ, ban, ngành. Trên cơ sở đó, phải tiếp tục xây dựng, hoàn thiện khung an toàn dữ liệu quốc gia, trong đó có các hệ thống bảo vệ dữ liệu được phân lớp, hệ thống quản lý nguy cơ an toàn dữ liệu, hệ thống ứng cứu, đối phó với các nguy cơ an toàn dữ liệu, hệ thống đánh giá an toàn dữ liệu (một số nhiệm vụ cụ thể cũng đã được xác định trong Quyết định số 942/QĐ-TTg ngày 15/6/2021 của Thủ tướng Chính phủ về việc phê duyệt Chiến lược phát triển Chính phủ điện tử hướng tới Chính phủ số giai đoạn 2021 - 2025, định hướng đến năm 2030).

Thứ tư, cần tăng cường hợp tác quốc tế để thúc đẩy giao dịch dữ liệu xuyên biên giới, phối kết hợp cùng các quốc gia trong khu vực về bảo vệ dữ liệu, xây dựng cơ chế chia sẻ dữ liệu an toàn giữa các nước; thiết lập cơ chế chuyển dữ liệu xuyên biên giới nhưng vẫn đảm bảo an toàn, bảo mật như GDPR của Liên minh châu Âu và CCPA của Mỹ; đàm phán và kí kết hiệp định song phương về dữ liệu với các quốc gia có thị trường dữ liệu phát triển như Mỹ, EU, Trung Quốc... để tạo tiền đề thúc đẩy giao dịch dữ liệu quốc tế.

4. Kết luận

Trong bối cảnh chuyển đổi số, bảo vệ dữ liệu cá nhân là yêu cầu pháp lý cấp bách để bảo vệ quyền riêng tư của cá nhân. Trên cơ sở tham khảo pháp luật các quốc gia phát triển về bảo vệ DLCN, Việt Nam 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

Tiếng Việt

1. Đạo luật Trí tuệ nhân tạo của EU. Truy cập ngày 12/2/2026, <https://artificialintelligenceact.eu/>
2. Hiến pháp nước Cộng hòa xã hội chủ nghĩa Việt Nam năm 2013, sửa đổi bổ sung năm 2025.
3. Luật về bảo vệ dữ liệu (*GDPR - General Data Protection Regulation*) của Liên minh châu Âu. Truy cập ngày 11/1/2026, <https://gdpr-info.eu/>.
4. Luật Dữ liệu (*Data Act*) của Liên minh Châu Âu. Truy cập ngày 12/2/2026, <https://www.osborneclarke.com/insights/eu-data-act-part-1-what-does-it-regulate>.
5. Luật Dữ liệu của Trung Quốc (*Data Security Law*) (2021). National People's Congress, PRC. Truy cập ngày 12/1/2026, <http://www.npc.gov.cn>.
6. Luật An ninh mạng của Việt Nam năm 2018, Luật An toàn thông tin mạng của Việt Nam năm 2015, Luật Dữ liệu năm của Việt Nam năm 2024, Luật bảo vệ dữ liệu cá nhân của Việt Nam năm 2025.
7. Luật Bảo vệ Quyền riêng tư của Người tiêu dùng California (*CCPA*). Truy cập ngày 12/2/2026, <https://www.esri.com/vi-vn/privacy/ccpa>
8. Luật Bảo vệ Thông tin Cá nhân (*PIPL*), Luật An ninh mạng (*CSL*) và Luật An ninh Dữ liệu (*DSL*) của Trung quốc. Truy cập ngày 12/2/2026, <https://www.dlapiperdataprotection.com/index.html?c=CN>
9. Luật Bảo vệ Dữ liệu Cá nhân (*PDPA - Personal Data Protection Act*) của Singapore. Truy cập ngày 10/2/2026, <https://iclg.com/practice-areas/data-protection-laws-and-regulations/singapore>.
10. Vũ Thị Hải Lý (2024). *Quản lý nhà nước về bảo vệ dữ liệu cá nhân - thực trạng và kiến nghị*. Tạp chí Quản lý nhà nước. Truy cập ngày 12/2/2026, <https://www.quanlynhanuoc.vn/2024/01/30/quan-lynha-nuoc-ve-bao-ve-du-lieu-ca-nhan-thuc-trang-va-kien-nghi/>
11. Tuyên ngôn Toàn cầu về Nhân quyền (UDHR). Truy cập ngày 12/2/2026, <https://www.un.org/en/about-us/universal-declaration-of-human-rights>

Tiếng nước ngoài

12. Amber Pariona. (2017). "What Was the Digital Revolution?". Truy cập ngày 10/2/2026, <https://www.worldatlas.com/articles/what-was-the-digital-revolution.html>.
13. Daniel & Paul, M. (2020). *Principles of data protection under GDPR*. Journal of European Data Law, 12(3), 45-59.
14. Fuster & Gellert. (2012). *The fundamental right of data protection in the European Union: in search of an uncharted right*. International Review of Law, Computers & Technology, 26(1), p. 73- 82.
15. European Commission. (2018). *What is personal data?*. Truy cập ngày 8/1/2026, https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en