HOÀN THIỆN PHÁP LUẬT VỀ BẢO VỆ QUYỀN RIÊNG TƯ VÀ DỮ LIỆU CÁ NHÂN TRONG KỶ NGUYÊN TRÍ TUỆ NHÂN TẠO

ThS. NCS. NGUYỄN HẢI YẾN
Vụ Pháp luật hình sự - hành chính, Bộ Tư pháp.

Thông tin bài viết:

Từ khóa: Trí tuệ nhân tạo; quyền riêng tư; dữ liệu cá nhân.

Lịch sử bài viết:

Nhận bài : 07/11/2025
Hoàn thành phản biện: 19/11/2025
Duyệt đăng : 21/11/2025

Tóm tắt:

Trí tuệ nhân tạo góp phần cải thiện hiệu quả lợi ích kinh tế, nhưng đồng thời gây ra những rủi ro đối với quyền riêng tư và bảo vệ dữ liệu cá nhân. Khả năng thúc đẩy đổi mới sáng tạo công nghệ trong khi ưu tiên quyền của người dùng sẽ là thách thức rõ ràng khi Việt Nam củng cố vị thế của mình trong nền kinh tế kỹ thuật số toàn cầu. Dựa trên các kinh nghiệm quốc tế, tác giả bài viết đưa ra một số khuyến nghị nhằm hoàn thiện mô hình pháp lý của Việt Nam về quyền riêng tư và bảo vệ dữ liệu cá nhân.

Article Information:

Keyworks: Artificial intelligence; privacy right; personal data.

Article History:

Received : 07 Nov. 2025
Review completed : 19 Nov. 2025
Approved : 21 Nov. 2025

Abstract:

Artificial intelligence contributes to enhancing economic efficiency and benefits, yet simultaneously poses risks to privacy and personal data protection. The capacity to promote technological innovation while prioritizing user rights presents a distinct challenge as Vietnam strengthens its position in the global digital economy. Drawing upon international experiences, the author proposes some recommendations to perfect Vietnam's legal framework on privacy and personal data protection.

Trí tuệ nhân tạo (AI) là khoa học và kỹ thuật chế tạo ra các bộ máy thông minh, đặc biệt là các chương trình máy tính thông minh. Nó liên quan đến nhiệm vụ tương tự sử dụng máy tính để hiểu trí thông minh của con người, nhưng AI không nhất thiết phải giới hạn trong các hình thái có thể quan sát được về mặt sinh học[1]. Ở dạng đơn giản nhất, AI là một lĩnh vực kết hợp khoa học máy tính và các bộ dữ liệu vững chắc, nhằm cho phép giải quyết vấn đề. Nó cũng bao gồm các lĩnh vực con của học máy và học sâu, thường được đề cập cùng với AI[2].

Tại Việt Nam, Chương trình Chuyển đổi số quốc gia đến năm 2025 và định hình đến năm 2030 đã xác định hai mục tiêu chính. Đó là phát triển cùng một lúc Chính phủ số, kinh tế số và xã hội số, cũng như tạo ra các doanh nghiệp công nghệ số Việt Nam có khả năng hoạt động toàn cầu[3].

1. Nguy cơ từ trí tuệ nhân tạo đối với quyền riêng tư và bảo vệ dữ liệu cá nhân

Hoạt động của các hệ thống AI có thể tạo điều kiện và làm trầm trọng thêm sự xâm phạm quyền riêng tư và các hành vi can thiệp

[1] John McCarthy (2007), *What Is Artificial Intelligence?*, Stanford University, https://www-formal.stanford.edu/jmc/whatisai.pdf, truy cập ngày 7/12/2023.
[2] IBM, *What Is Artificial Intelligence (AI)?*, https://www.ibm.com/topics/artificial-intelligence, truy cập ngày 1/12/2023.
[3] Việt Anh - Hồng Vân (2023), *Phát triển và ứng dụng công nghệ trí tuệ nhân tạo: Đòn bẩy thúc đẩy chuyển đổi số quốc gia*, https://special.nhandan.vn/tri-tue-nhan-tao-viet-nam/index.html, truy cập ngày 12/12/2023.

khác đối với các quyền con người theo nhiều cách khác nhau. AI chỉ hoạt động được khi được cung cấp dữ liệu đầu vào và đây là công cụ phục vụ mục đích của con người, thực hiện các tác vụ và hiểu nhu cầu khách hàng. Trong kỷ nguyên kỹ thuật số ngày nay, các hệ thống AI thường dựa vào các bộ dữ liệu lớn trong đó bao gồm dữ liệu cá nhân. Điều này khuyến khích việc thu thập, lưu trữ và xử lý dữ liệu rộng khắp. Tuy nhiên, sự phụ thuộc này đặt ra những lo ngại về quyền riêng tư và bảo mật dữ liệu. Nhiều doanh nghiệp tối ưu hóa các dịch vụ thông qua thu thập càng nhiều dữ liệu càng tốt. Điển hình là các doanh nghiệp trực tuyến như các công ty mạng xã hội dựa vào việc thu thập và thương mại hóa khối lượng dữ liệu khổng lồ về người dùng Internet. Việc thu thập dữ liệu diễn ra mọi nơi ở những không gian riêng tư và công cộng. Các chuyên viên môi giới dữ liệu thu thập, kết hợp, phân tích và chia sẻ dữ liệu cá nhân với vô số đối tượng và các giao dịch dữ liệu này phần lớn được che giấu khỏi tầm nhìn của công chúng và chỉ bị hạn chế một cách sơ sài bởi các khuôn khổ pháp lý hiện hành. Kết quả là các bộ dữ liệu thông tin được thu thập có quy mô chưa từng có trước đây[4].

Dữ liệu cá nhân của mỗi người được thu thập liên tục thông qua tương tác của cá nhân trên không gian số. Dữ liệu này có thể đến từ các nguồn cố ý, như khi khách hàng cung cấp thông tin cá nhân của họ hoặc các nguồn vô tình, nơi AI thu thập dữ liệu mà các cá nhân không nhận ra, chẳng hạn như thông qua nhận dạng khuôn mặt. Do AI có thể vô tình thu thập dữ liệu cá nhân mà chúng ta không hề hay biết hoặc mong muốn, những dữ liệu này có thể bị sử dụng trái ý muốn và ngoài tầm kiểm soát quyền riêng tư của chúng ta[5]. Nhiều doanh nghiệp tư nhân xây dựng và triển khai các mô hình ngôn ngữ lớn (LLMs) và mô hình nền tảng đa phương tiện (MFMs) đã công khai nhiều chi tiết về dữ liệu được sử dụng hoặc nguồn gốc của dữ liệu đó để đào tạo. Điều này có thể đặt ra các vấn đề về việc mua dữ liệu và thu thập dữ liệu[6]. Những doanh nghiệp này cũng khó có khả năng có được sự cho phép sử dụng dữ liệu internet từ chủ thể dữ liệu[7]. Bên cạnh đó, việc nhận dạng lại dữ liệu ẩn danh là đặc biệt đáng lo ngại khi các mô hình ngôn ngữ lớn và mô hình nền tảng đa phương tiện thu thập lượng lớn dữ liệu để huấn luyện. Cách các thông tin được sử dụng kết hợp với các dạng dữ liệu cá nhân khác có thể dấy lên lo ngại bởi việc thu thập các mảnh dữ liệu cá nhân có vẻ nhỏ và vô hại (lịch sử duyệt web, thông tin sinh trắc...) có thể, tích tụ lại, cung cấp một hồ sơ chi tiết về một cá nhân[8].

Ngoài ra, một trong những thách thức chính là bản chất hay hiệu ứng black box - "hộp đen" của đa số các hệ thống AI khiến rất khó có thể hiểu rõ không chỉ cách thức ra quyết

[4] Human Rights Council (2021), *The right to privacy in the digital age*, Report of the United Nations High Commissioner for Human Rights, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/249/21/PDF/G2124921.pdf?, p. 4.

[5] Casey Aonso (2018), *Why You Keep Getting Ads For Things You've Talked About But Haven't Searched Up Online*, https://www.narcity.com/why-you-keep-getting-ads-for-things-youve-talked-about-but-havent-searched-up-online, truy cập ngày 8/12/2023.

[6] G. Bell (2023), *Rapid Response Information Report: Generative AI - language models (LLMs) and multimodal foundation models (MFMs)*, Australian Council of Learned Academies, https://www.chiefscientist.gov.au/sites/default/files/2023-5/Rapid%20Response%20Information%20Report%20-%20Generative%20AI.pdf, truy cập ngày 12/12/2023.

[7] G. Bell (2023), *Rapid Response Information Report: Generative AI - language models (LLMs) and multimodal foundation models (MFMs)*, tlđd.

[8] Australian Human Rights Commission (2021), *Human Rights and Technology Final Report 2021*, https://humanrights.gov.au/sites/default/files/document/publication/ahrc_rightstech_2021_final_report_10.pdf, truy cập ngày 22/12/2023.

định của chúng, mà còn sự phức tạp và tự chủ của chúng, khiến việc phân loại AI trong hầu hết các thể chế pháp lý thông thường (không chỉ chủ thể xử lý dữ liệu) trở nên cực kỳ khó khăn. Do đó, để có được câu trả lời hợp lý, rõ ràng và dễ hiểu về vấn đề xử lý dữ liệu cá nhân trong các hệ thống AI là không dễ dàng. Ngay cả bên điều khiển dữ liệu cũng khó có thể trả lời câu hỏi về tính minh bạch của AI vì nó dựa trên học máy - khi nào nó học, cách thức thuật toán hoạt động và đến mức độ phần trăm chính xác nào. Bên cạnh đó, điều chúng ta cần xem xét sâu sắc hơn không chỉ là cách hệ thống AI đang hoạt động mà còn là tính chất của dữ liệu nó đang xử lý, kết quả của chính hệ thống xử lý đó và cách những vấn đề này có thể ảnh hưởng đến chủ thể dữ liệu[9].

Nhìn gần hơn vào thực tiễn ứng dụng AI tại Việt Nam có thể chỉ ra một số lĩnh vực nhạy cảm có thể phát sinh vấn đề bảo vệ quyền riêng tư và dữ liệu cá nhân. Trong lĩnh vực y tế, đại dịch Covid-19 (cuộc khủng hoảng sức khỏe toàn cầu) là một ví dụ mạnh mẽ và dễ nhận thấy về tốc độ, quy mô và tác động của AI trong nhiều lĩnh vực khác nhau của cuộc sống. Các hệ thống truy vết tiếp xúc sử dụng nhiều loại dữ liệu và thông tin về các mạng cá nhân đã được sử dụng để theo dõi sự lây lan của dịch bệnh. Tương tự tại Việt Nam, trong giai đoạn đại dịch Covid-19, các ứng dụng AI đã được sử dụng để thu thập dữ liệu cá nhân như định vị, hệ thống giao thông vận tải, sức khỏe và dân số nhằm truy vết người tiếp xúc khi có ổ dịch hoặc ca nhiễm mới trong cộng đồng để điều tra lịch trình, lấy thông tin dịch tễ.

Trong lĩnh vực tài chính, để đưa mô hình dựa trên AI vào hoạt động thực tế trong một tổ chức tài chính đòi hỏi sự hợp tác chặt chẽ giữa các nhà khoa học dữ liệu, chuyên gia công nghệ thông tin (IT) và các bên kinh doanh liên quan[10]. Các tổ chức tài chính khi thiết lập quan hệ đối tác với các công ty công nghệ có năng lực AI sẽ phải đối mặt với một loạt các rủi ro khi ký hợp đồng hợp tác. Những rủi ro này có thể liên quan đến "siêu dữ liệu" (metadata)[11] mà AI có thể tạo ra từ dữ liệu ngân hàng - khách hàng, cũng như các vấn đề về quyền riêng tư nói chung. Cụ thể, liên quan đến việc bảo vệ dữ liệu cá nhân của khách hàng, khi việc đánh giá rủi ro (trước khi cung ứng dịch vụ tài chính) được giao cho một đơn vị bên ngoài thực hiện, trường hợp này đặt ra câu hỏi về việc bảo đảm dữ liệu của ngân hàng không được giữ lại sau khi hoàn thành quá trình phát triển mô hình đánh giá rủi ro[12]. Các tổ chức tài chính phải ưu tiên các biện pháp bảo mật vững chắc để bảo vệ dữ liệu người dùng khỏi việc bị xâm phạm và truy cập trái phép. Việc không bảo vệ dữ liệu đầy đủ có thể dẫn đến những hậu quả pháp lý và tài chính đáng kể, làm suy giảm lòng tin của khách hàng và ảnh hưởng xấu đến danh tiếng của công ty.

Gần đây, một số startup công nghệ trong và ngoài Việt Nam đã ứng dụng AI và dữ liệu lớn - Big data vào xếp hạng tín dụng thuật toán. Theo đó, họ sử dụng nguồn dữ liệu đa dạng như viễn thông, mạng xã hội, thương mại điện tử, giao dịch tài chính... để xây dựng các thẻ điểm tín dụng, từ đó đánh giá và phân loại

[9] Miriam Podskubova (2023), *GDPR Compliance in the Age of Artificial Intelligence*, https://www.linkedin.com/pulse/gdpr-compliance-age-artificial-intelligence-polyd, truy cập ngày 22/12/2023.

[10] Vspry Platform (2023), *Designing and Implementing AI-Based Credit Scoring*, https://www.vspry.com/ai-based-credit-scoring/, truy cập ngày 6/12/2023.

[11] Andrew Barber, Rory Copeland (2019), *With Great Power Comes Great Responsibility: Artificial Intelligence In Banking*, https://internationalbanker.com/banking/with-great-power-comes-great-responsibility-artificial-intelligence-in-banking/, truy cập ngày 8/12/2023.

[12] Hicham Sadok & Fadi Sakka & Mohammed El Hadi El Maknouzi (2022), *Artificial Intelligence And Bank Credit Analysis: A Review*, https://ideas.repec.org/a/taf/oaefxx/v10y2022i1p2023262.html, truy cập ngày 7/12/2023.

khách hàng. Việc ứng dụng công nghệ mới giúp quá trình cho vay được thông minh và hiệu quả hơn nhưng cũng đặt ra những lo ngại đáng kể về việc bảo vệ quyền riêng tư của cá nhân bởi sự phụ thuộc vào các dữ liệu phong phú và thường nhạy cảm trong các hệ thống chấm điểm tín dụng dựa trên AI làm tăng các rủi ro tiềm ẩn đối với người tiêu dùng[13].

Những ứng dụng này đã chứng minh phạm vi rộng lớn các tác động, nguy cơ mà hệ thống AI có thể có đối với quyền riêng tư, với AI sử dụng thông tin cá nhân và thường đưa ra quyết định có ảnh hưởng thực tế đến cuộc sống của con người. Việt Nam đứng thứ 107 trên 110 quốc gia về chỉ số riêng tư trên mạng[14]. Số ca lạm dụng dữ liệu cá nhân đã xảy ra ở Việt Nam trong những năm gần đây rất lớn, bao gồm đánh cắp danh tính, gian lận tài chính, quảng cáo xâm phạm và bóc lột những cá nhân dễ bị tổn thương. Một báo cáo cho thấy chỉ riêng năm 2022, hơn 17 triệu dữ liệu cá nhân bị thu thập và bán trái phép để lừa đảo và mỗi dữ liệu cá nhân đã được buôn bán 987 lần mỗi ngày[15]. Tuy nhiên, cùng với vấn đề quyền riêng tư là các tác động khác nhau đến việc hưởng các quyền khác, chẳng hạn như các quyền về sức khỏe, giáo dục, tự do đi lại, tự do hội họp ôn hòa và tự do ngôn luận[16]. Do đó, việc thu thập và xử lý dữ liệu cá nhân cần có một khung chính sách và pháp luật điều chỉnh chặt chẽ và thích ứng với sự phát triển không ngừng của công nghệ[17].

2. Khung pháp lý về quyền riêng tư và bảo vệ dữ liệu cá nhân

2.1. Quyền riêng tư và dữ liệu cá nhân theo tiêu chuẩn quốc tế

Quyền riêng tư là biểu hiện của nhân phẩm con người và liên quan đến việc bảo vệ quyền tự chủ và nhân thân con người. Điều 12 Tuyên ngôn phổ quát về nhân quyền quy định không ai có thể bị xâm phạm một cách độc đoán vào đời tư, gia đình, nhà ở, thư tín hay bị xúc phạm đến danh dự hoặc thanh danh. Ai cũng có quyền được luật pháp bảo vệ chống lại những xâm phạm ấy. Điều 17 Công ước quốc tế về Các quyền dân sự và chính trị quy định không ai bị can thiệp một cách tuỳ tiện hoặc bất hợp pháp vào đời sống riêng tư, gia đình, nhà ở, thư tín, hay bị xâm phạm bất hợp pháp đến danh dự và uy tín. Mọi người đều có quyền được pháp luật bảo vệ chống lại những can thiệp hoặc xâm phạm như vậy. Quyền riêng tư cũng được bảo vệ trong nhiều văn kiện quốc tế khác[18]. Cách mạng công nghiệp lần thứ tư với đặc trưng là phát triển công nghệ nhanh chóng. Những thay đổi này có lẽ đã củng cố tầm quan trọng trung tâm của quyền riêng tư - đặc biệt là đối với AI. Các khía cạnh của quyền riêng tư đặc biệt quan trọng trong bối cảnh sử dụng AI bao gồm quyền riêng tư thông tin, thông tin tồn tại hoặc có thể rút ra về một người và cuộc sống của người đó, các quyết định dựa

[13] Hiệp hội ngân hàng Việt Nam, *Ứng dụng trí tuệ nhân tạo trong xếp hạng tín dụng tại Việt Nam: Triển vọng và trở ngại*, https://vnba.org.vn/vi/ung-dung-tri-tue-nhan-tao-trong-xep-hang-tin-dung-tai-viet-nam-trien-vong-va-tro-ngai-5178.htm, truy cập ngày 10/12/2023.

[14] VPN (2023), *Internet Privacy Index (2023)*, https://bestvpn.org/privacy-index/, truy cập ngày 12/12/2023.

[15] Quốc Nam (2022), *Đường dây thu thập 17 triệu dữ liệu thông tin cá nhân rồi đem bán*, https://tuoitre.vn/duong-day-thu-thap-17-trieu-du-lieu-thong-tin-ca-nhan-roi-dem-ban-20221123195747524.htm, truy cập ngày 1/12/2023.

[16] Human Rights Council (2021), *The right to privacy in the digital age*, Report of the United Nations High Commissioner for Human Rights, tlđd, p. 2.

[17] Vân Anh (2023), *Quyền riêng tư trong thời đại trí tuệ nhân tạo*, https://genk.vn/quyen-rieng-tu-trong-thoi-dai-tri-tue-nhan-tao-20230709194901827.chn, truy cập ngày 6/12/2023.

[18] Xem: Điều 16 Công ước về Quyền trẻ em năm 1989; Điều 14 Công ước quốc tế về Bảo vệ quyền của tất cả những người lao động di trú và các thành viên gia đình họ năm 1990; Điều 22 Công ước về Quyền của người khuyết tật năm 2007; Điều 8 Công ước châu Âu về Bảo vệ nhân quyền và tự do cơ bản năm 1950.

trên những thông tin đó và tự do đưa ra quyết định về bản sắc của một người[19]. Hội đồng Nhân quyền Liên hợp quốc cũng cho rằng, quyền riêng tư ngày càng quan trọng đối với người dân thường trong thời đại công cụ kỹ thuật số có thể bị lợi dụng để giám sát, lập hồ sơ và kiểm soát họ theo những cách mới[20].

2.2. Quyền riêng tư và bảo vệ dữ liệu cá nhân theo pháp luật Việt Nam

Ở Việt Nam, quyền riêng tư và bí mật cá nhân là quyền hiến định. Hiến pháp năm 2013 đưa ra các nguyên tắc chung rằng mọi người có quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân và bí mật gia đình; có quyền bảo vệ danh dự, uy tín của mình. Thông tin về đời sống riêng tư, bí mật cá nhân, bí mật gia đình được pháp luật bảo đảm an toàn (Điều 21 Hiến pháp năm 2013). Liên quan đến bảo vệ dữ liệu cá nhân có thể thấy, pháp luật Việt Nam về bảo vệ dữ liệu cá nhân có nguồn gốc từ quyền riêng tư - một quyền con người cơ bản. Mỗi khía cạnh và mỗi ngành có thể có văn bản quy định riêng...

Điều 16 Luật An toàn thông tin mạng năm 2015 đã đưa ra các nguyên tắc bảo vệ thông tin cá nhân trên mạng. Cụ thể, Điều 18 cho phép chủ thể thông tin cá nhân có quyền yêu cầu tổ chức, cá nhân đang xử lý thông tin của mình cập nhật, sửa đổi, xóa bỏ hoặc ngừng cung cấp cho bên thứ ba. Khi nhận được yêu cầu, bên xử lý thông tin phải thực hiện và thông báo lại hoặc cấp quyền truy cập để chủ thể tự cập nhật, sửa đổi. Điều 19 yêu cầu tổ chức, cá nhân xử lý thông tin cá nhân phải áp dụng các biện pháp quản lý và kỹ thuật thích hợp để bảo vệ thông tin do mình thu thập, lưu trữ, đồng thời tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin. Họ cũng phải xóa bỏ thông tin cá nhân đã lưu khi hết mục đích sử dụng hoặc thời hạn lưu trữ, đồng thời thông báo cho chủ thể thông tin cá nhân. Bên cạnh đó, Luật này quy định việc thiết lập kênh thông tin trực tuyến để tiếp nhận và xử lý các phản ánh của người dân về vấn đề bảo vệ thông tin cá nhân.

Ngày 17/4/2023, Chính phủ đã chính thức ban hành Nghị định số 13/2023/NĐ-CP về Bảo vệ dữ liệu cá nhân (Nghị định 13). Nghị định 13 lần đầu tiên hệ thống hóa các quy định bảo vệ dữ liệu cá nhân trong một văn bản thống nhất. Sau đó, Quốc hội đã ban hành một loạt các đạo luật mới, kiến tạo một nền tảng pháp lý vững chắc và có hệ thống cho kỷ nguyên số, bao gồm Luật Dữ liệu năm 2024, Luật Bảo vệ dữ liệu cá nhân năm 2025, Luật Công nghiệp công nghệ số năm 2025 và hiện nay tiếp tục dự thảo Luật Trí tuệ nhân tạo.

Luật Dữ liệu số 60/2024/QH15, được Quốc hội thông qua ngày 30/11/2024 và có hiệu lực từ ngày 01/07/2025. Đạo luật này chính thức công nhận và thiết lập khung pháp lý cho khía cạnh kinh tế của dữ liệu. Điểm đột phá nhất của Luật Dữ liệu là việc lần đầu tiên khẳng định dữ liệu được coi là một loại tài sản và quyền của chủ sở hữu dữ liệu đối với dữ liệu là quyền tài sản theo quy định của pháp luật về dân sự[21]. Quy định này mở đường cho việc thương mại hóa dữ liệu một cách hợp pháp, tạo cơ sở cho sự phát triển của một thị trường dữ liệu sôi động. Luật đã định hình các quy tắc cho thị trường này bằng cách quy định về các Sản phẩm và Dịch vụ trung gian dữ liệu (kết nối, chia sẻ dữ liệu)[22] và Sàn giao dịch dữ liệu[23]. Đáng chú ý, để bảo đảm sự kiểm soát của nhà nước, dịch vụ sàn giao dịch dữ liệu

[19] Human Rights Council (2022), *The right to privacy in the digital age*, Report of the United Nations High Commissioner for Human Rights, tlđd.

[20] Human Rights Council (2022), *The right to privacy in the digital age*, Report of the United Nations High Commissioner for Human Rights, tlđd.

[21] Khoản 15 Điều 3 Luật Dữ liệu năm 2024.

[22] Điều 40 Luật Dữ liệu năm 2024.

[23] Điều 42 Luật Dữ liệu năm 2024.

chỉ được cung cấp bởi các đơn vị sự nghiệp công lập hoặc doanh nghiệp nhà nước đã được cấp phép[24]. Luật cũng phân định rõ các loại dữ liệu được phép giao dịch, trong đó nhấn mạnh rằng dữ liệu cá nhân chỉ có thể được đưa vào giao dịch khi có sự đồng ý của chủ thể dữ liệu hoặc khi pháp luật cho phép[25]. Bên cạnh việc thúc đẩy thị trường, Luật Dữ liệu cũng trao cho nhà nước quyền lực quan trọng trong việc yêu cầu các doanh nghiệp cung cấp dữ liệu trong các trường hợp khẩn cấp hoặc để bảo vệ an ninh quốc gia, thể hiện sự cân bằng giữa lợi ích kinh tế và an ninh công cộng[26].

Nếu Luật Dữ liệu tập trung vào giá trị kinh tế, thì Luật Bảo vệ dữ liệu cá nhân (BVDLCN) số 91/2025/QH15 được Quốc hội thông qua ngày 26/06/2025 lại đặt trọng tâm vào khía cạnh quyền con người. Đây là đạo luật chuyên ngành đầu tiên của Việt Nam ở cấp luật điều chỉnh toàn diện lĩnh vực này, thể hiện một bước tiến vượt bậc so với Nghị định số 13/2023/NĐ-CP trước đó. Việc nâng cấp từ một Nghị định lên thành một đạo luật không chỉ mang ý nghĩa về mặt hình thức mà còn củng cố mạnh mẽ hiệu lực pháp lý và tính ổn định của các quy định. Luật BVDLCN của Việt Nam được xây dựng với ảnh hưởng rõ nét từ Quy định chung về bảo vệ dữ liệu của Liên minh châu Âu (GDPR), vốn được xem là tiêu chuẩn toàn cầu trong lĩnh vực này. Tuy nhiên, bên cạnh việc kế thừa những nguyên tắc và cấu trúc cơ bản của GDPR, luật của Việt Nam cũng thể hiện sự điều chỉnh đáng kể nhằm phản ánh các ưu tiên chính sách và đặc thù pháp lý quốc gia, đặc biệt trong việc nhấn mạnh vai trò của an ninh, chủ quyền số và trật tự quản lý nhà nước.

Luật BVDLCN[27] và GDPR[28] đều dựa trên những nguyên tắc cốt lõi của bảo vệ dữ liệu như hợp pháp, minh bạch, giới hạn mục đích, giảm thiểu dữ liệu, tính chính xác, giới hạn lưu trữ, bảo mật và trách nhiệm giải trình. Cả hai đều bảo đảm quyền của chủ thể dữ liệu, bao gồm quyền được biết, truy cập, chỉnh sửa, xóa, hạn chế xử lý, phản đối và không bị quyết định hoàn toàn tự động. Quy định về dữ liệu nhạy cảm - bao gồm thông tin sinh trắc học, sức khỏe, tôn giáo, chính trị - cũng được đặt ở mức bảo vệ cao hơn. Một điểm đáng chú ý là cả hai văn bản đều mở rộng phạm vi áp dụng ngoài lãnh thổ, điều chỉnh cả các tổ chức nước ngoài nếu xử lý dữ liệu của công dân trong phạm vi quốc gia mình, qua đó thể hiện tinh thần bảo vệ chủ quyền số. Cả hai cũng yêu cầu tiến hành đánh giá tác động bảo vệ dữ liệu đối với các hoạt động có nguy cơ cao, cũng như đặt ra điều kiện nghiêm ngặt đối với việc chuyển dữ liệu xuyên biên giới - đòi hỏi quốc gia tiếp nhận phải có mức độ bảo vệ tương đương hoặc có biện pháp bảo vệ thích hợp.

Về điểm tiến bộ, Luật BVDLCN có mức phạt nghiêm khắc, lên đến 5% doanh thu hàng năm, cao hơn cả mức tối đa 4% trong GDPR. Một điểm khác biệt lớn nữa là Việt Nam cấm tuyệt đối việc mua bán dữ liệu cá nhân dưới mọi hình thức (Điều 7, 8), trong khi GDPR không đặt ra lệnh cấm tổng thể mà điều chỉnh thông qua các nguyên tắc hợp pháp, minh bạch và sự đồng ý. Ngoài ra, Luật BVDLCN cũng quy định rõ ràng về "khử nhận dạng dữ liệu" (khoản 11 Điều 2), trong khi GDPR chỉ đề cập khái niệm "pseudonymization" (Điều 4(4)) một cách khái quát. Luật của Việt Nam còn có điều khoản riêng (Điều 30) điều chỉnh hoạt động xử lý dữ liệu liên quan đến trí tuệ nhân tạo (AI) và Big Data, tương ứng với xu hướng mà EU thể hiện qua Đạo luật AI (EU AI Act, 2024). Luật cũng quy định chuyên biệt về dữ liệu sinh trắc học, yêu cầu minh bạch về thuật toán và kiểm tra định kỳ nhằm tránh sai lệch,

[24] Khoản 2 Điều 42 Luật Dữ liệu năm 2024.
[25] Điểm b khoản 3 Điều 42 Luật Dữ liệu năm 2024.
[26] Khoản 2 Điều 18 Luật Dữ liệu năm 2024.
[27] Điều 3 Luật BVDLCN năm 2025.
[28] Điều 5 GDPR.

phân biệt đối xử. Luật cũng yêu cầu cập nhật đánh giá tác động định kỳ 6 tháng, quy định chi tiết về bảo vệ dữ liệu trong các lĩnh vực cụ thể như tiếp thị, y tế, mạng xã hội… Đây là những điểm phù hợp thực tiễn và nâng cao khả năng bảo vệ dữ liệu cá nhân của người dùng. Tuy nhiên, Luật BVDLCN vẫn tồn tại một số hạn chế so với GDPR. GDPR quy định rõ ràng về các giới hạn đối với quyết định tự động (Điều 22) và tăng cường quyền của cá nhân để nhận được lời giải thích (explanation) về logic liên quan và kết quả của các quyết định đó trong khi đó Luật BVDLCN không có điều khoản tương đương Điều 22 của GDPR hoặc các quy định cụ thể yêu cầu tổ chức phải cấp cho cá nhân quyền được giải thích có ý nghĩa (meaningful explanation) về các quyết định hoàn toàn tự động ảnh hưởng đến quyền của họ.

Luật Công nghiệp công nghệ số số 71/2025/QH15, được Quốc hội thông qua ngày 14/06/2025. Đạo luật này vừa mang tính thúc đẩy, vừa mang tính quản lý đối với các ngành công nghệ cao, trong đó AI là một trọng tâm. Về mặt thúc đẩy, Luật đưa ra các chính sách ưu đãi vượt trội nhằm thu hút đầu tư và phát triển các lĩnh vực công nghệ mũi nhọn như AI và công nghiệp bán dẫn. Các ưu đãi này bao gồm miễn, giảm thuế thu nhập doanh nghiệp, thuế thu nhập cá nhân cho chuyên gia, hỗ trợ tài chính từ ngân sách, và ưu đãi về đất đai. Mục tiêu là tạo ra một môi trường kinh doanh thuận lợi, hình thành các doanh nghiệp công nghệ số lớn mạnh, có khả năng cạnh tranh trên thị trường toàn cầu. Tuy nhiên, song song với việc khuyến khích, Luật Công nghiệp công nghệ số cũng thiết lập những lằn ranh đỏ rõ ràng. Điều 12 của Luật quy định cụ thể các hành vi bị nghiêm cấm, trong đó có một điều khoản trực tiếp nhắm vào AI: Cấm sử dụng, cung cấp, triển khai hệ thống trí tuệ nhân tạo để xâm phạm lợi ích quốc gia, quốc phòng, an ninh, trật tự an toàn xã hội, quyền con người, quyền công dân và phá hoại thuần phong mỹ tục. Việc tích hợp quy định cấm này ngay trong một đạo luật mang tính thúc đẩy phát triển cho thấy ý chí của nhà làm luật trong việc quản lý rủi ro từ AI một cách chủ động, bảo đảm công nghệ phát triển trong một khuôn khổ có trách nhiệm. Ngày 15/9/2025, Bộ Khoa học và Công nghệ thông báo Việt Nam sẽ ban hành phiên bản cập nhật của Chiến lược AI Quốc gia (lần đầu ban hành năm 2021) và Luật AI đầu tiên vào cuối năm 2025[29].

Luật Công nghiệp công nghệ số năm 2025 cùng với Dự thảo Luật Trí tuệ nhân tạo đang được xây dựng đã đánh dấu bước ngoặt trong việc định hình khung pháp lý về AI tại Việt Nam, hướng tới một mô hình quản trị tương đồng với EU AI Act - đạo luật đầu tiên và toàn diện nhất trên thế giới về trí tuệ nhân tạo, có hiệu lực từ tháng 8 năm 2024. EU AI Act thiết lập một cách tiếp cận dựa trên rủi ro, chia các hệ thống AI thành bốn cấp độ: rủi ro không chấp nhận được (unacceptable risk) - bị cấm hoàn toàn; rủi ro cao (high risk) - chịu sự quản lý nghiêm ngặt; rủi ro hạn chế hoặc trung bình (limited risk) - yêu cầu minh bạch; và rủi ro tối thiểu (minimal risk) - không chịu quy định bắt buộc. Cách tiếp cận này cho phép Chính phủ điều chỉnh linh hoạt theo mức độ nguy cơ, vừa bảo đảm an toàn vừa khuyến khích đổi mới công nghệ. Dự thảo Luật Trí tuệ nhân tạo của Việt Nam thể hiện sự tương đồng rõ nét với triết lý và cấu trúc của EU AI Act. Trước hết, về cách tiếp cận quản lý, cả hai đều áp dụng mô hình phân loại rủi ro để xác định nghĩa vụ pháp lý tương ứng. Các hệ thống AI bị cấm trong dự thảo của Việt Nam có sự tương đồng với danh mục của EU, bao gồm các ứng dụng có khả năng gây tổn hại nghiêm trọng đến quyền con người và trật tự xã hội như AI thao túng hành vi con người, chấm điểm tín nhiệm xã hội (social scoring), hay giám sát sinh trắc học theo thời gian thực

[29] Thu Giang, *Sẽ có bản cập nhật Chiến lược AI quốc gia và Luật AI*, https://baochinhphu.vn/se-co-ban-cap-nhat-chien-luoc-ai-quoc-gia-va-luat-ai-102250915130224143.htm, truy cập ngày 25/10/2025.

trong không gian công cộng. Đối với các hệ thống AI rủi ro cao, cả hai khuôn khổ đều đặt ra các yêu cầu nghiêm ngặt trước khi được đưa ra thị trường, như thiết lập hệ thống quản lý rủi ro, bảo đảm chất lượng dữ liệu và tính toàn vẹn, có cơ chế giám sát của con người, bảo mật mạng, và minh bạch trong thuật toán. Trong lĩnh vực AI rủi ro trung bình hoặc hạn chế, các hệ thống tương tác trực tiếp với con người - như chatbot hoặc deepfake - đều phải minh bạch về bản chất của AI, bảo đảm người dùng nhận thức rõ họ đang giao tiếp hoặc tiếp xúc với sản phẩm do AI tạo ra.

Tuy nhiên, có sự khác biệt trong việc phân loại các hệ thống trí tuệ nhân tạo có rủi ro giữa Dự thảo Luật Trí tuệ nhân tạo và Luật Công nghiệp công nghệ số năm 2025. Luật Công nghiệp công nghệ số năm 2025 tập trung vào việc quản lý Hệ thống trí tuệ nhân tạo rủi ro cao (có khả năng gây tổn hại nghiêm trọng tới sức khỏe con người, quyền con người, lợi ích công cộng, an toàn xã hội) và Hệ thống trí tuệ nhân tạo tác động lớn (hệ thống đa mục đích, số lượng người dùng và dữ liệu lớn) (Điều 43). Dự thảo Luật Trí tuệ nhân tạo hiện phân loại hệ thống AI thành 4 mức độ rủi ro: Rủi ro không chấp nhận (bị cấm), Rủi ro cao, Rủi ro trung bình, và Rủi ro thấp.[30] Việc hai văn bản pháp luật, đều được ban hành hoặc dự thảo trong cùng năm 2025 và cùng đề cập đến lĩnh vực AI, sử dụng các thuật ngữ và sơ đồ phân loại khác nhau (4 cấp độ rủi ro trong Dự thảo Luật Trí tuệ nhân tạo so với 2 loại hệ thống quản lý chính trong Luật Công nghiệp công nghệ số năm 2025) có thể gây nhầm lẫn trong việc áp dụng quản lý rủi ro đối với các hệ thống AI.

3. Đề xuất hoàn thiện khuôn khổ pháp lý

Quyền riêng tư trong bối cảnh AI có những xem xét khác biệt so với quyền riêng tư nói chung. Một trong những thách thức của việc bảo vệ quyền riêng tư trong kỷ nguyên AI là việc làm sao để tạo ra các quy định phù hợp để bảo vệ quyền riêng tư mà không làm suy giảm sự tiến bộ của công nghệ AI. Theo đó, các cách thức để điều chỉnh AI và giảm thiểu rủi ro về quyền con người có thể bao gồm: thứ nhất, việc tạo ra khung pháp lý đặc thù cho AI; thứ hai, cải cách và mở rộng quy định hiện tại để bảo đảm rằng các quy định này điều chỉnh tất cả các ứng dụng của công nghệ; hoặc thứ ba, kết hợp giữa cả hai cách thức trên tức là vừa ban hành văn bản chuyên biệt vừa sửa đổi, bổ sung những văn bản hiện hành.

Việt Nam có thể cân nhắc cách tiếp cận kết hợp các cách thức với nhau trong việc hoàn thiện khung pháp luật về AI trong việc bảo vệ quyền riêng tư và dữ liệu cá nhân. Ngoài các quy định về quyền riêng tư và dữ liệu cá nhân, Việt Nam phải xem xét và có thể phải bổ sung một loạt các quy định để giải quyết những thách thức của AI trong các lĩnh vực một cách tôn trọng đến quyền lợi cá nhân. Với sự đa dạng của các hệ thống và cách ứng dụng AI, các quy định cần phải chi tiết đến mức để giải quyết các vấn đề cụ thể trong từng ngành và điều chỉnh các biện pháp phản ứng theo các rủi ro liên quan. Đối với những lĩnh vực có rủi ro cao đối với quyền con người, lĩnh vực thi hành pháp luật, an ninh quốc gia, việc làm, chăm sóc sức khỏe, giáo dục và tài chính, yêu cầu pháp lý cho việc sử dụng công nghệ AI nên được ưu tiên hơn. Các giải pháp cụ thể cho từng lĩnh vực đòi hỏi sự nghiên cứu chuyên sâu, trong phạm vi bài viết, dưới đây là một số đề xuất giải pháp áp dụng chung.

3.1. Một số vấn đề về Luật Bảo vệ dữ liệu cá nhân

Luật BVDLCN năm 2025 có điều khoản điều chỉnh việc bảo vệ dữ liệu cá nhân trong xử lý dữ liệu lớn (big data) và trí tuệ nhân tạo (AI) (Điều 30). Các hệ thống sử dụng AI phải được tích hợp các biện pháp bảo mật dữ liệu cá nhân phù hợp và phải thực hiện phân loại theo mức độ rủi ro để có biện pháp bảo vệ

[30] Dự thảo có thể xem tại: https://mst.gov.vn/van-ban-phap-luat/du-thao/2294.htm

thích hợp, tuy nhiên các quy định này không trao trực tiếp cho chủ thể dữ liệu quyền phản đối một quyết định cá nhân được đưa ra hoàn toàn tự động hoặc quyền được giải thích về logic quyết định tương tự như GDPR yêu cầu.

Điều 22 GDPR quy định rõ ràng và chi tiết về việc giới hạn các quyết định được đưa ra hoàn toàn dựa trên xử lý tự động, bao gồm lập hồ sơ (profiling), khi các quyết định này tạo ra hiệu ứng pháp lý hoặc ảnh hưởng đáng kể đến chủ thể dữ liệu. Chủ thể dữ liệu có quyền không phải tuân theo quyết định dựa hoàn toàn vào xử lý tự động, bao gồm lập hồ sơ, mà quyết định đó tạo ra hiệu ứng pháp lý hoặc ảnh hưởng đáng kể đến họ. Trong các trường hợp được phép đưa ra quyết định tự động (ví dụ: cần thiết cho việc ký kết hoặc thực hiện hợp đồng, hoặc dựa trên sự đồng ý rõ ràng của chủ thể dữ liệu), bên kiểm soát dữ liệu phải thực hiện các biện pháp bảo vệ thích hợp. Các biện pháp này bao gồm ít nhất là quyền được có sự can thiệp của con người, quyền bày tỏ quan điểm và quyền phản đối quyết định. GDPR đặc biệt nhấn mạnh yêu cầu cung cấp thông tin có ý nghĩa (meaningful information) về logic liên quan (the logic involved) và tầm quan trọng (significance) cũng như hậu quả dự kiến (envisaged consequences) của việc xử lý đó đối với chủ thể dữ liệu (Điều 13). Do vậy, trong thời gian tới cần tiếp tục nghiên cứu, bổ sung các quy định cụ thể về khả năng giải thích AI (AI Explainability), yêu cầu các hệ thống AI rủi ro cao phải có khả năng giải thích các quyết định của mình đối với dữ liệu cá nhân một cách dễ hiểu cho người dùng, đặc biệt khi các quyết định đó ảnh hưởng tiêu cực đến họ; đặt ra các giới hạn đối với loại dữ liệu có thể được suy luận, sử dụng và chia sẻ một cách hợp pháp; tăng cường quyền của cá nhân, bao gồm cả việc cấp cho họ quyền được giải thích có ý nghĩa và phản đối các quyết định hoàn toàn tự động ảnh hưởng đến quyền của họ. Điều này có nghĩa là các tổ chức phải xem xét tác động tiềm tàng của hệ thống AI của mình đối với các cá nhân và bảo đảm rằng không một quyết định nào được đưa ra mà ảnh hưởng đáng kể đến các cá nhân mà không có sự giám sát đầy đủ của con người.

3.2. Khung pháp lý đặc thù cho AI

Đề xuất về một khung pháp lý đặc thù cho AI đang được Nhà nước tích cực triển khai qua hai hướng song song. Thứ nhất, Luật Công nghiệp công nghệ số số 71/2025/QH15 đã được ban hành, trong đó dành riêng Chương IV để điều chỉnh các hoạt động liên quan đến AI, đưa ra các định hướng phát triển và các hành vi bị cấm. Thứ hai, và quan trọng hơn, Dự thảo Luật Trí tuệ nhân tạo chuyên biệt đang được xây dựng, với định hướng quản lý dựa trên cấp độ rủi ro tương tự EU AI Act. Đây là những bước đi đúng hướng, tuy nhiên, để bắt kịp tốc độ phát triển của công nghệ, Dự thảo Luật cần được các quy định chi tiết hơn cho các vấn đề mới nổi:

Tính minh bạch: Các tổ chức hưởng lợi từ lợi thế AI phải có khả năng giải thích cách hệ thống AI của họ đưa ra quyết định nói chung. Điều này có thể là thách thức đối với các mô hình học máy phức tạp. Ngoài nghĩa vụ mà Luật AI đưa ra, các tổ chức có thể áp dụng các kỹ thuật AI có thể giải thích được để làm cho hệ thống AI của họ trở nên minh bạch và dễ hiểu hơn. Họ cũng có thể cung cấp thông tin rõ ràng và dễ tiếp cận về việc sử dụng AI cũng như tác động của nó đối với các cá nhân[31]. Đối với AI tạo sinh (Generative AI), cần có các nghĩa vụ cụ thể tham khảo kinh nghiệm từ EU AI Act, bao gồm nghĩa vụ công khai tóm tắt dữ liệu có bản quyền được sử dụng để huấn luyện. Đồng thời, cần xác định trách nhiệm pháp lý đối với các "ảo giác" (hallucination) và thông tin sai lệch do mô hình tạo ra.

Thống nhất phân loại hệ thống AI: Dựa trên sự khác biệt giữa Dự thảo Luật Trí tuệ nhân tạo và Luật Công nghiệp công nghệ số

[31] The AI Act, https://artificialintelligenceact.com/.

năm 2025 trong việc phân loại mức độ rủi ro của hệ thống AI, cần thiết phải có sự hài hòa hóa và thống nhất khái niệm pháp lý để tránh chồng chéo, bảo đảm tính nhất quán và khả thi trong thực thi. Theo đó, cần thống nhất hệ thống phân loại rủi ro theo mô hình bốn cấp độ của Dự thảo Luật Trí tuệ nhân tạo (Rủi ro không chấp nhận - Rủi ro cao - Rủi ro trung bình - Rủi ro thấp), bởi đây là cách tiếp cận tương thích với EU AI Act, phản ánh đầy đủ phổ mức độ nguy cơ từ cấm tuyệt đối đến kiểm soát linh hoạt. Trong mô hình này, các nhóm "Hệ thống trí tuệ nhân tạo rủi ro cao" và "Hệ thống tác động lớn" theo Luật Công nghiệp công nghệ số năm 2025 có thể được tích hợp và diễn giải lại như nhóm AI rủi ro cao trong Dự thảo Luật Trí tuệ nhân tạo, nhưng cần có tiêu chí định lượng và định tính rõ ràng hơn, ví dụ: phạm vi ảnh hưởng đến sức khỏe, quyền con người, lợi ích công cộng hoặc quy mô dữ liệu, số lượng người dùng.

Phân định rõ ràng trách nhiệm đa cấp trong chuỗi cung ứng AI: Khi xây dựng luật về AI, các nhà làm luật Việt Nam cũng cần cân nhắc quy định vấn đề phân hóa trách nhiệm trong từng khâu phát triển và ứng dụng AI. Vấn đề này, Việt Nam có thể tham khảo quy định của Đạo luật AI và dữ liệu (AIDA) của Canada. Theo đó, trường hợp một hệ thống AI được phát triển bởi nhiều chủ thể, có nhiều bước phát triển, bao gồm cả hoạt động nghiên cứu và thương mại, thì việc xác định trách nhiệm sẽ được xác định như ví dụ sau[32]:

Trong giai đoạn 1: Một nhà nghiên cứu tại một trường đại học xuất bản một mô hình mới có thể được sử dụng để phát triển hệ thống AI. Bước này sẽ không có yêu cầu pháp lý hay trách nhiệm pháp lý nào theo AIDA, vì đây không phải là một hoạt động thương mại và chỉ riêng mô hình đó thì không phải là một hệ thống AI hoàn chỉnh.

Trong giai đoạn 2: Công ty A sử dụng mô hình này để phát triển một hệ thống có tác động cao bằng cách huấn luyện nó dựa trên dữ liệu mà họ kiểm soát, sau đó đưa nó ra thị trường để sử dụng - Công ty A cần phải tuân thủ các yêu cầu để phát triển và sử dụng hệ thống theo quy định (ví dụ: thử nghiệm, bảo đảm rằng tất cả các biện pháp cần thiết để vận hành an toàn và công bằng đều được áp dụng, cung cấp tài liệu cho các công ty mua hệ thống). Nếu Công ty A không thực hiện các nghĩa vụ này, họ có thể phải chịu các hình phạt. Nếu Công ty A cung cấp hệ thống để sử dụng khi biết rằng nó có thể gây tổn hại nghiêm trọng, công ty có thể bị truy tố hình sự.

Trong giai đoạn 3: Công ty B đưa hệ thống vào hoạt động vì mục đích thương mại - Công ty B cần phải tuân thủ các yêu cầu về quản lý hoạt động (ví dụ: bảo đảm rằng việc sử dụng này là phù hợp với những rủi ro và hạn chế được Công ty A ghi lại, giám sát hệ thống, xuất bản mô tả hệ thống). Nếu hệ điều hành gây hại, Công ty B chỉ phải chịu trách nhiệm nếu họ không đáp ứng các nghĩa vụ liên quan đến quản lý hoạt động. Nếu trong quá trình vận hành hệ thống, Công ty B bất cẩn hoặc coi thường sự an toàn của người khác, công ty có thể bị truy tố tội hình sự.

3.3. Bổ sung tội danh

Hiện nay, Bộ luật Hình sự hiện hành chưa có quy định tội danh riêng về hành vi xâm phạm dữ liệu cá nhân. Thay vào đó, vi phạm các quy định về thông tin cá nhân có thể bị xử phạt hình sự theo 02 tội danh "Tội xâm phạm bí mật hoặc an toàn thư tín, điện thoại, điện tín hoặc hình thức trao đổi thông tin riêng tư khác của người khác" (Điều 159); và "Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông" (Điều 288). Hầu hết các vụ việc buôn bán dữ liệu

[32] Government of Canada (2023), *The Artificial Intelligence and Data Act (AIDA) - Companion document*, https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document, truy cập ngày 10/12/2023.

cá nhân đang được hoàn thiện theo hướng chứng minh 02 tội danh này. Tuy nhiên, cả 2 tội danh này chưa quy định cụ thể, trực tiếp về các hành vi vi phạm pháp luật liên quan tới dữ liệu cá nhân nói chung và quy định việc vi phạm liên quan đến dữ liệu cá nhân trong ứng dụng AI nói riêng. Cần bổ sung vào Bộ luật Hình sự một tội danh mới như "Tội sử dụng trái phép hệ thống trí tuệ nhân tạo để xâm phạm dữ liệu cá nhân và quyền riêng tư", và điều chỉnh mức phạt tương xứng với Luật BVDLCN năm 2025.

Việt Nam có thể tham khảo kinh nghiệm của Canada trong việc xây dựng tội danh chuyên biệt cho hành vi xâm phạm quyền đối với dữ liệu cá nhân trong quá trình ứng dụng AI. Theo đó, Đạo luật AI và dữ liệu của Canada đã bổ sung ba tội hình sự mới trong đó có một tội danh liên quan đến việc xâm phạm dữ liệu cá nhân trong quá trình ứng dụng AI[33]. Những hành vi phạm tội có tính chất hình sự này nhằm mục đích cấm và trừng phạt các hoạt động liên quan đến AI được thực hiện bởi người nhận thức được tác hại mà AI đang gây ra hoặc có nguy cơ gây ra. Tội danh liên quan đến việc xâm phạm dữ liệu cá nhân trong quá trình ứng dụng AI như sau: cố ý sở hữu hoặc sử dụng thông tin cá nhân có được một cách bất hợp pháp nhằm thiết kế, phát triển, sử dụng hoặc cung cấp để sử dụng hệ thống AI. Hành vi này có thể bao gồm việc cố ý sử dụng thông tin cá nhân thu được do vi phạm dữ liệu để đào tạo hệ thống AI[34].

3.4. Tăng cường hợp tác và hài hòa hóa pháp luật quốc tế

Trong bối cảnh AI là một công nghệ không biên giới, Việt Nam cần tích cực tham gia các diễn đàn đa phương và thúc đẩy hài hòa hóa quy định trong ASEAN, ký kết các thỏa thuận song phương với các quốc gia có khung pháp luật tương đương để tạo điều kiện cho dòng chảy dữ liệu và đổi mới công nghệ. Điều này không chỉ giúp Việt Nam học hỏi kinh nghiệm mà còn tạo điều kiện thuận lợi cho các doanh nghiệp công nghệ trong nước xuất khẩu sản phẩm, dịch vụ AI ra thị trường toàn cầu. Bên cạnh đó, có thể tham khảo các mô hình quản trị linh hoạt hơn như các bộ quy tắc ứng xử tự nguyện của Singapore[35] và Nhật Bản[36] để bổ sung cho khung pháp lý bắt buộc, tạo ra một môi trường pháp lý đa dạng và thích ứng■

---

[33] Government of Canada (2023), *The Artificial Intelligence and Data Act (AIDA) - Companion document*.

[34] Hai tội danh còn lại là thứ hai, cố ý hoặc cẩu thả cung cấp hệ thống AI có khả năng gây tổn hại nghiêm trọng hoặc thiệt hại đáng kể cho tài sản, trường hợp việc sử dụng hệ thống đã thực sự gây ra tổn hại hoặc thiệt hại đó; thứ ba, cung cấp hệ thống AI để sử dụng với mục đích lừa gạt công chúng và gây ra tổn thất kinh tế đáng kể cho một cá nhân, trường hợp việc sử dụng hệ thống đã thực sự gây ra tổn thất đó.

[35] Singapore áp dụng hệ thống AI governance đa tầng, dựa trên khung hướng dẫn tự nguyện thay vì quy định bắt buộc. Trung tâm của mô hình này là Model AI Governance Framework (MAGF), được công bố lần đầu năm 2019 và cập nhật năm 2020, 2024 bởi Infocomm Media Development Authority (IMDA) và Personal Data Protection Commission (PDPC). Phương châm của Singapore được gọi là "Assurance-led Innovation" – khuyến khích đổi mới công nghệ dưới sự bảo chứng của niềm tin xã hội, thay vì khuôn khổ pháp lý cưỡng chế. Mô hình này đã giúp Singapore trở thành trung tâm điều tiết AI thân thiện với đổi mới nhất châu Á. Xem: Luke Soon, The Global AI Regulation Landscape: From Voluntary Frameworks to Global Assurance, https://genesishumanexperience.com/2025/09/18/singapores-ai-governance-roadmap-from-voluntary-frameworks-to-global-assurance/, truy cập ngày 25/10/2025.

[36] Nhật Bản áp dụng cách tiếp cận điều chỉnh mềm, đặt trọng tâm vào các hướng dẫn tự nguyện và nguyên tắc đạo đức thay vì chế tài ràng buộc. Nền tảng của mô hình này là AI Promotion Act 2025, được thông qua bởi Quốc hội Nhật Bản vào tháng 3 năm 2025 và có hiệu lực từ 01/7/2025. AI Promotion Act mang tính khuyến nghị, mời gọi các doanh nghiệp, cơ quan nhà nước, viện nghiên cứu và người dân "tự nguyện phối hợp" với chiến lược quốc gia về AI thay vì cưỡng chế. Chính phủ, thông qua AI Strategy Headquarters, điều phối các bộ, ngành và địa phương xây dựng bản kế hoạch tổng thể về phát triển AI quốc gia. Xem: Hiroki Habuka, *Japan's Agile AI Governance in Action: Fostering a Global Nexus Through Pluralistic Interoperability*, https://www.csis.org/analysis/japans-agile-ai-governance-action-fostering-global-nexus-through-pluralistic, truy cập ngày 25/10/2025.