

BẢO VỆ DỮ LIỆU CÁ NHÂN VÀ QUYỀN RIÊNG TƯ TRONG KỶ NGUYÊN TRÍ TUỆ NHÂN TẠO - NHÌN TỪ THẾ GIỚI VÀ KHUYẾN NGHỊ CHO VIỆT NAM*

■ TÀO NAM KHÁNH, BÙI ĐÔNG NGUYÊN PHƯƠNG & NGUYỄN CAO THẢO**

Tóm tắt: Bài viết phân tích chính sách bảo vệ dữ liệu cá nhân và quyền riêng tư liên quan đến trí tuệ nhân tạo (AI) ở một số quốc gia trên thế giới, từ đó, đưa ra một số khuyến nghị cho Việt Nam về vấn đề này.

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

Nhận bài: 07/3/2025

Hoàn thành biên tập: 25/3/2025

Duyệt đăng: 03/4/2025

PERSONAL DATA PROTECTION AND PRIVACY IN THE ERA OF ARTIFICIAL INTELLIGENCE - VIEWS FROM THE WORLD AND RECOMMENDATIONS FOR VIETNAM

Abstract: The article analyzes the policies on personal data protection and privacy related to artificial intelligence (AI) in some countries around the world, from which, it gives some recommendations for Vietnam on this issue.

Keywords: Artificial intelligence; AI; personal data; privacy.

Article received: 07/3/2025

Editing completed: 25/3/2025

Approved for publication: 03/4/2025

Đặt vấn đề

Ngày nay, trí tuệ nhân tạo (AI) không chỉ là một công nghệ mới nổi mà còn là một động lực thúc đẩy sự phát triển của xã hội, đã và đang mang lại những lợi ích to lớn cho nhân loại, từ cải thiện chất lượng dịch vụ y tế, giáo dục đến việc tạo ra những sản phẩm thông minh, tiện ích, hay có khả năng phân tích và khai thác dữ liệu với quy mô lớn, giúp doanh nghiệp và tổ chức đưa ra quyết định chính xác hơn. Nhiều quốc gia trên thế giới đã xác định công nghệ AI là đột phá chiến lược trong phát triển đất nước. Tuy nhiên, bên cạnh những lợi ích to lớn, AI cũng đặt ra nhiều thách thức mới về đạo đức, xã hội và pháp luật. Nếu không có cơ chế kiểm soát phù hợp, sự phát triển của AI có thể dẫn đến những hậu quả nghiêm trọng, đặc biệt, trong việc bảo vệ dữ liệu cá nhân và quyền riêng

tư. Việc sử dụng công nghệ AI thu thập, xử lý và phân tích dữ liệu quy mô lớn mà không có sự giám sát chặt chẽ có thể làm gia tăng nguy cơ lạm dụng thông tin, xâm phạm đời tư, thậm chí tạo ra sự phân biệt đối xử trong các quyết định tự động. Do đó, việc bảo vệ dữ liệu cá nhân và quyền riêng tư cần có một khuôn khổ pháp lý chặt chẽ để bảo đảm công nghệ AI phát triển theo hướng vừa thúc đẩy đổi mới sáng tạo, vừa bảo vệ quyền lợi chính đáng của con người.

1. Bảo vệ dữ liệu cá nhân và quyền riêng tư trong việc phát triển công nghệ trí tuệ nhân tạo ở một số quốc gia trên thế giới

Hiện nay, phần lớn các hoạt động phân tích dữ liệu liên quan đến quyền riêng tư, như thuật toán tìm kiếm, hệ thống gợi ý và mạng lưới quảng cáo kỹ thuật số, đều được vận hành bởi máy học và các quyết định

* Bài nghiên cứu là một phần kết quả của đề tài “Phát triển trí tuệ nhân tạo có trách nhiệm - Kinh nghiệm quốc tế và một số khuyến nghị cho Việt Nam” tham gia Cuộc thi sinh viên Nghiên cứu khoa học năm 2025 của Trường Đại học Luật Hà Nội.

** Trường Đại học Luật Hà Nội

từ thuật toán. Khi AI ngày càng phát triển, nó ngày càng khuếch đại khả năng sử dụng thông tin cá nhân gây xâm phạm đến quyền riêng tư của con người, theo đó, một số nước trên thế giới đã có những quy định về việc bảo vệ dữ liệu cá nhân và quyền riêng tư trong phát triển công nghệ AI.

Trung Quốc, một trong những cường quốc AI hàng đầu thế giới, đã nhanh chóng xây dựng các chính sách và quy định nhằm định hướng sự phát triển của công nghệ AI, nổi bật là việc ban hành Luật An ninh dữ liệu năm 2021 (DSL) quy định chi tiết việc các doanh nghiệp thu thập, xử lý và bảo vệ dữ liệu cá nhân.

Vào tháng 10/2021, Trung Quốc đề xuất các tiêu chuẩn bảo mật nghiêm ngặt đối với các nhà cung cấp dịch vụ AI, gồm việc quản lý dữ liệu, đánh giá an ninh dữ liệu, tuân thủ DSL, bảo vệ thông tin cá nhân cũng như việc lập danh sách đen các nguồn dữ liệu không được phép sử dụng để đào tạo mô hình AI. Tiếp theo, vào tháng 7/2023, Chính phủ Trung Quốc đã ban hành quy định mới về xây dựng các mô hình AI, yêu cầu các nhà cung cấp dịch vụ AI tuân thủ nghiêm ngặt các tiêu chuẩn đạo đức xã hội, bảo đảm không tạo ra nội dung có thể kích động, đe dọa an ninh quốc gia hoặc gây tổn hại đến lợi ích công cộng. Đồng thời, các thuật toán và dữ liệu đào tạo AI phải được thiết kế và lựa chọn theo chuẩn mực nghiêm ngặt, tạo tiền đề cho sự phát triển AI an toàn và có trách nhiệm.

Ở Hoa Kỳ, việc bảo vệ dữ liệu cá nhân và quyền riêng tư dựa trên sự kết hợp giữa luật pháp, quy định và tự điều chỉnh¹. Ngày 30/10/2023, Tổng thống Mỹ Joe Biden đã ban hành sắc lệnh nhằm giảm thiểu

những rủi ro mà công nghệ AI có thể gây ra, thiết lập các tiêu chuẩn mới về an toàn và bảo mật, bảo vệ quyền riêng tư của người dùng, thúc đẩy đổi mới và cạnh tranh trong lĩnh vực AI. Sắc lệnh yêu cầu: (i) các cơ quan chức năng của Chính phủ Mỹ thiết lập các tiêu chuẩn, công cụ và thử nghiệm để giúp bảo đảm các hệ thống AI an toàn, bảo mật và đáng tin cậy; (ii) các công ty khi phát triển các hệ thống AI mà có nguy cơ gây rủi ro cho an ninh và nền kinh tế quốc gia, sức khỏe hoặc an toàn cộng đồng, phải chia sẻ kết quả kiểm tra an toàn với Chính phủ Mỹ trước khi công bố rộng rãi². Ngoài ra, để giải quyết những khó khăn và phức tạp trên thực tế đối với việc bảo vệ dữ liệu cá nhân và quyền riêng tư, Quốc hội Hoa Kỳ đã đưa ra một số dự luật về quyền về sự riêng tư dữ liệu để thực hiện tiêu chuẩn bảo mật dữ liệu liên bang. Chẳng hạn, Luật Phổ biến Dữ liệu Hoa Kỳ (S. 142) áp đặt các yêu cầu về quyền về sự riêng tư đối với các nhà cung cấp dịch vụ Internet tương tự như các yêu cầu áp đặt cho các cơ quan liên bang theo Luật về quyền về sự riêng tư năm 1974. Luật bảo vệ quyền về sự riêng tư và quyền lợi người tiêu dùng trên phương tiện truyền thông xã hội năm 2019 (S. 189), sẽ yêu cầu các chủ thể: (i) cung cấp cho người dùng một bản sao miễn phí dưới dạng điện tử những dữ liệu cá nhân mà nhà điều hành đã xử lý; (ii) thông báo cho người dùng trong vòng 72 giờ sau khi biết dữ liệu của người dùng đã bị truyền đi mà vi phạm nền tảng bảo mật³. Bên cạnh đó, do lo ngại về quyền riêng tư liên quan đến công nghệ nhận diện khuôn mặt, các thành phố như Oakland, Berkeley và San Francisco ở bang California, cùng với Brookline, Cambridge, Northampton và Somerville ở bang Massachusetts,

1. Global Internet liberty campaign (2004), “*Privacy and human rights - An International Survey of Privacy Laws and Practice*”, <http://gilc.org/privacy/survey/intro.html>, truy cập ngày 01/11/2024.

2. Cameron F. Kerry (2020), “*Protecting privacy in an AI-driven world*”, <https://www/articles/protecting-privacy-in-an-ai-driven-world/>, truy cập ngày 21/9/2024.

3. 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 9 (409), tháng 5/2020.

đã ban hành lệnh cấm sử dụng công nghệ này⁴. Một số bang như California, New Hampshire và Oregon cũng đã thông qua các đạo luật cấm sử dụng công nghệ nhận diện khuôn mặt kết hợp với camera gắn trên người của lực lượng Cảnh sát.

Ngoài ra, quy định bảo vệ dữ liệu chung (GDPR) của Liên minh châu Âu (EU) đã thiết lập tiêu chuẩn cao về bảo vệ dữ liệu cá nhân và các quy định tương tự đang được xem xét và áp dụng trên khắp thế giới. Các chính sách này nhằm bảo đảm việc thu thập, xử lý và sử dụng dữ liệu trong các hệ thống AI được thực hiện minh bạch, công bằng, bảo vệ quyền riêng tư của người dùng. GDPR đã thiết lập 07 nguyên tắc cần tuân thủ khi xử lý dữ liệu: (i) tính hợp pháp, công bằng và minh bạch: việc xử lý dữ liệu phải hợp pháp, công bằng và minh bạch đối với chủ thể dữ liệu; (ii) giới hạn mục đích: mục đích xử lý dữ liệu phải hợp pháp và được thể hiện rõ ràng cho chủ thể dữ liệu khi thu thập; (iii) giảm thiểu dữ liệu: chỉ thu thập và xử lý dữ liệu khi thực sự cần thiết cho các mục đích đã định; (iv) độ chính xác: phải bảo đảm dữ liệu cá nhân là chính xác và cập nhật; (v) giới hạn lưu trữ: chỉ lưu trữ dữ liệu nhận dạng cá nhân trong thời gian cần thiết cho mục đích đã định; (vi) tính toàn vẹn và bảo mật: việc xử lý dữ liệu phải bảo đảm tính bảo mật, tính toàn vẹn và bảo mật thích hợp (ví dụ: bằng cách sử dụng mã hóa); (vii) trách nhiệm giải trình: người kiểm soát dữ liệu có trách nhiệm chứng minh sự tuân thủ GDPR với tất cả các nguyên tắc này. GDPR cũng quy định “quyền được lãng quên” - là quyền xóa dữ liệu cho những người muốn xóa dữ liệu cá nhân của họ khi không còn cần cứ để lưu giữ dữ liệu đó. GDPR được áp dụng ở cấp độ trong nước với hiệu lực ngay lập tức, bắt đầu từ ngày có hiệu lực và việc áp dụng luật quốc gia sẽ không ảnh hưởng đến hiệu lực của nó. Tuy nhiên, GDPR cho phép các quốc gia thành

viên áp dụng linh hoạt một số quy định trong phạm vi nhất định.

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

2. Thực trạng bảo vệ dữ liệu cá nhân và quyền riêng tư trong việc phát triển trí tuệ nhân tạo tại Việt Nam

Tại Việt Nam, pháp luật hiện hành về bảo vệ dữ liệu cá nhân quy định tản mát tại nhiều văn bản quy phạm pháp luật. Tại khoản 1 Điều 21 Hiến pháp năm 2013 quy định: “Mọi người có quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân và bí mật gia đình... Thông tin về đời sống riêng tư, bí mật cá nhân, bí mật gia đình được pháp luật bảo đảm an toàn”. Điều 17 Luật An toàn thông tin mạng năm 2015 (sửa đổi, bổ sung năm 2018) quy định việc thu thập và sử dụng thông tin cá nhân: (i) chỉ được thực hiện sau khi có sự đồng ý của chủ thể thông tin về phạm vi và mục đích thu thập, sử dụng thông tin; (ii) thông tin cá nhân

4. Sara Merken (October 16, 2019), “*Berkeley Bans Government Face Recognition Use, Joining Other Cities*”, Bloomberg Law; Nikolas DeCosta-Klipa (December 12, 2019), “*Brookline becomes 2nd Massachusetts community to ban facial recognition*”, Boston.com; Tori Bedford (January 13, 2020), “*Cambridge Votes To Ban Face Surveillance Technology*”, WGBH.

chỉ được sử dụng vào mục đích khác với mục đích ban đầu khi có sự chấp thuận từ chủ thể thông tin; (iii) việc cung cấp, chia sẻ, phát tán thông tin cá nhân cho bên thứ ba chỉ được thực hiện với sự đồng ý của chủ thể hoặc theo yêu cầu từ cơ quan nhà nước có thẩm quyền. Ngoài ra, Điều 159 và Điều 288 Bộ luật Hình sự năm 2015, sửa đổi, bổ sung năm 2017 (Bộ luật Hình sự năm 2015) hiện chưa quy định cụ thể các chế tài hình sự đối với hành vi xâm phạm “dữ liệu cá nhân” mà chỉ đề cập đến việc xâm phạm “thông tin cá nhân” với hình phạt tối đa là 07 năm tù giam. Đồng thời, chủ thể mà pháp luật nhắc đến là các cá nhân, tổ chức mà chưa gồm các đối tượng khác như AI nói chung.

Trong khi các nước trên thế giới đã ban hành một số bộ luật kiểm soát việc thu thập dữ liệu cá nhân, tại Việt Nam, hiện mới chỉ có Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân điều chỉnh vấn đề này⁵. Tuy nhiên, phạm vi điều chỉnh và đối tượng áp dụng được quy định tại Điều 1 Nghị định này giới hạn trong “cơ quan, tổ chức, cá nhân có liên quan”. Điều này dẫn đến một “khoảng trống” pháp lý đáng kể khi đối diện với các hệ thống AI, vốn có khả năng tự động tìm kiếm, thu thập và xử lý dữ liệu trên không gian mạng mà không cần sự can thiệp trực tiếp từ con người. Trên thực tế, đã có nhiều trường hợp chứng minh AI có thể xâm phạm quyền riêng tư và khai thác dữ liệu cá nhân mà không có sự cho phép từ chủ thể dữ liệu. Ví dụ, các mô hình học máy thường sử dụng dữ liệu lớn (big data) để cải thiện hiệu quả, nhưng nguồn gốc và tính hợp pháp của dữ liệu được thu thập thường không được kiểm soát chặt chẽ. Điều này đặt ra nguy cơ xâm phạm quyền lợi cá nhân, tạo điều kiện cho các hành vi vi phạm pháp luật, như 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 Bộ luật

Hình sự năm 2015), hay tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác (Điều 289 Bộ luật Hình sự năm 2015).

Gần đây, Việt Nam đã có dự thảo Luật Bảo vệ dữ liệu cá nhân, quy định những cá nhân, tổ chức phát triển AI có một số quyền và nghĩa vụ cụ thể, ví dụ: thông báo cho chủ thể dữ liệu về việc xử lý dữ liệu cá nhân tự động, giải thích ảnh hưởng thuận toán, trí tuệ nhân tạo và các hệ thống tự động đối với quyền và lợi ích hợp pháp của chủ thể dữ liệu⁶. Ngoài ra, dự thảo Luật cũng quy định nghiêm ngặt trách nhiệm của tổ chức, cá nhân cung cấp dịch vụ mạng xã hội, dịch vụ truyền thông được cung cấp trực tiếp đến người xem thông qua không gian mạng (OTT) (Điều 31) cũng như đặt ra những quy định về phòng, chống thu thập, chuyển giao trái phép, mua, bán dữ liệu cá nhân (Điều 33)... Tuy nhiên, nhìn chung, hệ thống pháp luật Việt Nam liên quan đến vấn đề này, bước đầu được hình thành và còn nhiều hạn chế. Các quy định mới chỉ đề cập ở mức độ khái quát, chưa đủ chi tiết để xử lý các vấn đề phức tạp mà AI đặt ra, các cơ chế bảo vệ trên thực tế chưa được thiết lập hiệu quả, dẫn đến tình trạng các hành vi thu thập và sử dụng dữ liệu không minh bạch, không có sự đồng ý của cá nhân vẫn xảy ra mà chưa bị xử lý triệt để.

3. Một số khuyến nghị trong việc phát triển trí tuệ nhân tạo tại Việt Nam để bảo vệ dữ liệu cá nhân và quyền riêng tư

Thứ nhất, quy định cụ thể về quyền và nghĩa vụ của nhà phát triển AI.

- Các cá nhân, tổ chức phát triển AI cần tiến hành đánh giá tác động của hệ thống AI đối với quyền riêng tư và dữ liệu cá nhân, thông qua đó, xác định cách thức hệ thống, quy trình hoặc công nghệ xử lý dữ liệu ảnh hưởng đến quyền riêng tư và dữ liệu cá nhân; bảo

5. Nguyễn Lan Phương (2023), “AI tác động thế nào đến quyền riêng tư của cá nhân?”, Viện Nghiên cứu Chính sách và Phát triển Truyền thông (IPS), <https://viettimes.vn/ai-tac-dong-the-nao-den-quyen-rieng-tu-cua-ca-nhan>, truy cập ngày 30/10/2024.

6. Khoản 2 Điều 24 Dự thảo Luật Bảo vệ dữ liệu cá nhân.

đảm các rủi ro cần phòng tránh hoặc giảm thiểu tối đa; minh bạch các hoạt động thu thập dữ liệu, gồm các loại dữ liệu được thu thập, cách sử dụng dữ liệu và người có quyền truy cập vào dữ liệu.

- Đánh giá dữ liệu một cách toàn diện và hệ thống, thiết lập quy trình quản lý bảo mật dữ liệu hiệu quả; bảo đảm tính chính xác của dữ liệu; ngăn ngừa các rủi ro như rò rỉ, mất mát và phát tán dữ liệu.

- Cần xin phép và tôn trọng quyết định của chủ thể dữ liệu về việc thu thập, sử dụng, tiếp cận, chuyển giao và xóa dữ liệu theo cách thức phù hợp và khả thi nhất. Bảo đảm mọi chủ thể dữ liệu đều được bảo vệ, chống lại lạm dụng dữ liệu thông qua các tính năng cài đặt sẵn trong hệ thống.

- Trong một số lĩnh vực nhạy cảm (y tế, lao động, giáo dục, tư pháp, hình sự, tài chính...), dữ liệu cá nhân chỉ được sử dụng trong các trường hợp cần thiết và chủ thể khai thác, sử dụng dữ liệu phải được trải qua quy trình kiểm tra về đạo đức⁷.

Thứ hai, tăng cường quyền kiểm soát của cá nhân đối với dữ liệu cá nhân.

Chủ thể dữ liệu cá nhân cần có quyền được biết dữ liệu cá nhân của họ đang được thu thập, xử lý và sử dụng như thế nào để cân nhắc, cân trọng việc cho phép thu thập, xử lý dữ liệu cá nhân. Ví dụ, trên thực tế, có rất nhiều đối tượng lợi dụng lỗ hổng bảo mật để chiếm đoạt tài sản của người sử dụng các ứng dụng ngân hàng điện tử, cụ thể, khi người mua hàng cần chuyển tiền thanh toán, những đối tượng này sẽ gửi cho người mua hàng mã QR có chứa mã độc để điền thông tin, dữ liệu cá nhân, từ đó, bị chiếm đoạt tất cả số tiền trong tài khoản. Vì vậy, các tổ chức thu thập dữ liệu cần phải cung cấp thông tin minh bạch về mục đích và phương thức xử lý dữ liệu ngay từ khi thu thập. Ngoài ra, cần có quy định về quyền yêu cầu xóa dữ liệu cá nhân khi cá nhân không còn muốn dữ liệu

của mình được lưu trữ hoặc sử dụng. Đây là quyền đã được quy định trong nhiều hệ thống pháp luật quốc tế, như quyền được lãng quên trong GDPR của EU. Việc áp dụng quyền kiểm soát này giúp cá nhân có khả năng bảo vệ quyền riêng tư trước nguy cơ bị theo dõi hoặc lạm dụng dữ liệu.

Thứ ba, hoàn thiện cơ chế thực thi và chế tài xử phạt.

Hiện nay, Dự thảo Luật Bảo vệ dữ liệu cá nhân đã quy định về các hành vi vi phạm và mức phạt tương ứng. Tuy nhiên, cần làm rõ về trách nhiệm của các tổ chức, doanh nghiệp trong việc xử lý dữ liệu cá nhân, đặc biệt, đối với những hệ thống AI có khả năng thu thập và phân tích dữ liệu ở quy mô lớn. Do đó, cần thành lập một cơ quan chuyên trách về bảo vệ dữ liệu cá nhân, tương tự như Cơ quan Bảo vệ Dữ liệu (Data Protection Authority) ở các nước châu Âu. Cơ quan này có nhiệm vụ giám sát việc thực thi luật, xử lý khiếu nại và đưa ra hướng dẫn cụ thể để bảo đảm tuân thủ pháp luật. Bên cạnh đó, cần nâng cao chế tài xử phạt đối với các vi phạm về bảo vệ dữ liệu cá nhân bởi các quy định còn “khá nhẹ”, chưa bảo đảm tính răn đe⁸, Luật cần quy định mức phạt nghiêm khắc hơn đối với các hành vi như thu thập dữ liệu trái phép, rò rỉ dữ liệu quy mô lớn hoặc sử dụng dữ liệu sai mục đích, tương tự như các mức phạt nặng trong GDPR.

Thứ tư, hoàn thiện các nguyên tắc bảo vệ dữ liệu cá nhân và quyền riêng tư.

- Cần áp dụng nguyên tắc “hạn chế mục đích” để bảo đảm dữ liệu cá nhân chỉ được thu thập cho các mục đích cụ thể, rõ ràng và hợp pháp. Việc xử lý dữ liệu sau đó không được mở rộng tùy tiện mà phải tuân theo mục đích ban đầu. Nguyên tắc này giúp ngăn chặn tình trạng lạm dụng dữ liệu và bảo đảm tính minh bạch trong quá trình xử lý dữ liệu cá nhân. Theo GDPR của EU, việc xử lý dữ liệu ngoài phạm vi mục

7. Trường Đại học Luật, Đại học Quốc gia Hà Nội - Bộ Khoa học và Công nghệ Việt Nam (2024), “Dự thảo một số hướng dẫn thực hiện bộ nguyên tắc về phát triển trí tuệ nhân tạo có trách nhiệm ở Việt Nam”, tr. 6 - 7.

8. Ka Mi (2022), “Còn những khoảng trống pháp luật về bảo vệ dữ liệu cá nhân”, <https://vietnamnet.vn/con-nhung-khoang-trong-phap-luat-ve-bao-ve-du-lieu-ca-nhan-i404631.html>, truy cập ngày 01/11/2024.

đích ban đầu phải được đánh giá lại và có cơ sở pháp lý phù hợp⁹.

- Nguyên tắc “tối thiểu hóa dữ liệu” cần được áp dụng để giới hạn lượng dữ liệu cá nhân thu thập ở mức cần thiết nhất cho mục đích xử lý. GDPR quy định chỉ những dữ liệu thực sự cần thiết mới được thu thập và xử lý nhằm giảm thiểu nguy cơ lạm dụng hoặc rò rỉ thông tin cá nhân.

- Áp dụng nguyên tắc “bảo vệ quyền riêng tư theo thiết kế” và “bảo vệ quyền riêng tư theo mặc định” để bảo đảm các hệ thống AI phải được xây dựng với các biện pháp bảo vệ dữ liệu ngay từ đầu. Theo GDPR, doanh nghiệp và tổ chức phải tích hợp các cơ chế bảo vệ dữ liệu vào sản phẩm và dịch vụ ngay từ đầu, thay vì chỉ bổ sung sau khi đã triển khai. Điều này giúp giảm thiểu rủi ro rò rỉ dữ liệu cá nhân và tăng cường bảo vệ quyền riêng tư¹⁰.

Kết luận

AI đang trở thành một phần không thể thiếu trong sự phát triển của xã hội hiện đại, mang lại nhiều lợi ích nhưng cũng đặt ra những thách thức không nhỏ về đạo đức, pháp lý và quyền riêng tư. Tại Việt Nam, dù đã có những bước tiến quan trọng trong việc xây dựng khung pháp lý và chiến lược phát triển AI, nhưng còn nhiều khoảng trống cần được hoàn thiện, đặc biệt, trong vấn đề bảo vệ dữ liệu cá nhân. Để AI phát triển theo hướng bền vững, các nhà phát triển, doanh nghiệp, cơ quan quản lý và người dùng cần có nhận thức đầy đủ và tuân thủ các nguyên tắc bảo mật dữ liệu. Việc xây dựng một hệ thống pháp lý chặt chẽ, kết hợp với các biện pháp công nghệ tiên tiến và nâng cao nhận thức cộng đồng sẽ giúp Việt Nam tận dụng tối đa lợi ích của AI, đồng thời, bảo vệ quyền lợi chính đáng của công dân trong kỷ nguyên số □

TÀI LIỆU THAM KHẢO

1. Ka Mi (2022), “Còn những khoảng trống pháp luật về bảo vệ dữ liệu cá nhân”, <https://vietnamnet.vn/con-nhung-khoang-trong-phap-luat-ve-bao-ve-du-lieu-ca-nhan-i404631.html>, truy cập ngày 01/11/2024.

2. Nguyễn Lan Phương (2023), “AI tác động thế nào đến quyền riêng tư của cá nhân?”, Viện Nghiên cứu Chính sách và Phát triển Truyền thông (IPS), <https://viettimes.vn/ai-tac-dong-the-nao-den-quyen-rieng-tu-cua-ca-nhan>, truy cập ngày 30/10/2024.

3. Trường Đại học Luật, Đại học Quốc gia Hà Nội - Bộ Khoa học và Công nghệ Việt Nam (2024), “Dự thảo một số hướng dẫn thực hiện bộ nguyên tắc về phát triển trí tuệ nhân tạo có trách nhiệm ở Việt Nam”.

4. Cameron F. Kerry (2020), “Protecting privacy in an AI-driven world”, <https://www/articles/protecting-privacy-in-an-ai-driven-world/>, truy cập ngày 21/9/2024.

5. Global Internet liberty campaign (2004), “Privacy and human rights - An International Survey of Privacy Laws and Practice”, <http://gilc.org/privacy/survey/intro.html>, truy cập ngày 01/11/2024.

6. Paul Mozur (2019), “One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority”, New York Times, <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence>, truy cập ngày 01/11/2024.

7. Sara Merken (October 16, 2019), “Berkeley Bans Government Face Recognition Use, Joining Other Cities”, Bloomberg Law.

8. Nikolas DeCosta-Klipa (December 12, 2019), “Brookline becomes 2nd Massachusetts community to ban facial recognition”, Boston.com.

9. Tori Bedford (January 13, 2020), “Cambridge Votes to Ban Face Surveillance Technology”, WGBH.

10. U.S. GAO (2019), “Report: INTERNET PRIVACY: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility”, GAO-19-52.

9. Xem thêm Điều 5 GDPR: Nguyên tắc liên quan đến việc xử lý dữ liệu cá nhân.

10. Xem thêm Điều 25 GDPR: Bảo vệ dữ liệu theo thiết kế và theo mặc định.