TẠP CHÍ KHOA HỌC
ĐẠI HỌC QUỐC TẾ SÀI GÒN
Saigon International University Journal of Science

Số 01 - Tháng 10/2025
Website: https://js.siu.edu.vn

NHỮNG THÁCH THỨC ĐỐI VỚI VIỆC BẢO VỆ DỮ LIỆU CÁ NHÂN TRONG BỐI CẢNH PHÁT TRIỂN TRÍ TUỆ NHÂN TẠO

Nguyễn Thị Hạnh*

Tóm tắt: Trí tuệ nhân tạo (AI) đã và đang tạo ra sự thay đổi lớn trong các lĩnh vực như y tế, giáo dục, tài chính, công nghiệp và nông nghiệp. Công nghệ này giúp tối ưu hóa quy trình, nâng cao năng suất và hiệu suất, đồng thời mở ra nhiều cơ hội cải thiện cuộc sống. Tuy nhiên, AI cũng tạo ra thêm nhiều thách thức về quyền riêng tư, bảo mật dữ liệu cá nhân như rò rỉ thông tin cá nhân, mua bán dữ liệu cá nhân. Bài viết sẽ đưa ra một số kiến nghị về bảo vệ dữ liệu cá nhân trong bối cảnh phát triển AI với mục tiêu then chốt để đảm bảo quyền lợi và an toàn của người dân, đồng thời thúc đẩy sự phát triển bền vững của công nghệ.

Từ khóa: trí tuệ nhân tạo, dữ liệu cá nhân, rò rỉ dữ liệu, riêng tư

1. SỰ PHÁT TRIỂN CỦA TRÍ TUỆ NHÂN TẠO TRONG MỘT SỐ LĨNH VỰC

Sự phát triển của AI là một trong những hiện tượng quan trọng nhất của thế kỷ 21, đã và đang tạo ra sự thay đổi mạnh mẽ trong xã hội và cuộc sống con người. AI đã nhanh chóng trở thành một trong những đỉnh cao của sự tiến bộ trong thế giới hiện đại.

AI là một lĩnh vực khoa học máy tính cố gắng xây dựng các máy tính có thể bắt chước các khả năng nhận thức của con người hoặc trí thông minh. Các hệ thống AI có thể được nhóm thành bốn loại: học máy, hệ thống dựa trên quy tắc, tính toán mềm và trí tuệ tính toán. Học máy sử dụng dữ liệu và thuật toán để tạo ra các máy thông minh; tính toán mềm sử dụng phép tính mờ để phát triển các máy thông minh; hệ thống dựa trên quy tắc sử dụng các quy tắc để xây dựng các máy thông minh và trí tuệ tính toán sử dụng các hiện tượng tự nhiên và sinh học để tạo ra các máy thông minh (Marwala & Mpedi, 2024).

AI hoạt động dựa trên cơ chế mô phỏng suy nghĩ, nhận thức của con người và đưa vào bộ não của các thiết bị, hệ thống. Từ đó hệ thống sẽ có được trí thông minh như con người, biết dựa vào từng tình huống mà có cách xử lý khác nhau. Một vài ứng dụng của AI như: y tá ảo, trợ lý ảo, tư vấn viên ảo, robot làm việc nhà, robot công nghiệp,… (Trường Đại học Hoa Sen, 2024). AI còn cải thiện cuộc sống hàng ngày của con người thông qua các tiện ích thông minh. Trợ lý ảo như Siri hoặc Google Assistant giúp con người giải quyết nhiều công việc hàng ngày từ việc lên lịch hẹn đến tra cứu thông tin. Các hệ thống học máy tùy chỉnh giúp tạo ra các giải pháp và quyết định phù hợp với từng cá nhân.

AI trải qua những tiến bộ nhanh chóng, ảnh hưởng đáng kể đến nhiều lĩnh vực của đời sống xã hội như chăm sóc sức khỏe, tài chính, giáo dục, giao thông,…

Hiện nay, AI đang dần trở thành một phần không thể thiếu trong cuộc sống hiện đại, AI đang len lỏi đến mọi khía cạnh của xã hội, mang lại vô số lợi ích nhưng cũng đặt ra nhiều mối lo ngại.

Trong lĩnh vực sản xuất và công nghiệp, AI góp phần quan trọng vào việc tăng cường năng suất lao động. Khả năng tự động hóa các quy trình sản xuất không chỉ giúp doanh nghiệp tiết kiệm thời gian, nguồn lực mà còn tạo điều kiện thuận lợi cho sự phát triển bền vững và cải thiện hiệu quả kinh doanh. AI có thể thực hiện các tác vụ lặp đi lặp lại một cách nhanh chóng và chính xác, giúp giảm thiểu lỗi phát sinh từ con người và tiết kiệm thời gian đáng kể. Trong lĩnh vực sản xuất, AI đã thúc

* TS., Vụ Pháp luật hình sự - hành chính, Bộ Tư pháp

đẩy tự động hóa, giúp giảm chi phí sản xuất và tạo ra sản phẩm với chất lượng cao hơn.

AI giúp tự động hóa nhiều quy trình, giảm thiểu lao động thủ công, tăng năng suất và chất lượng sản phẩm. Các robot và hệ thống tự động hóa được điều khiển bởi AI có thể thực hiện các công việc nguy hiểm, giúp bảo vệ an toàn cho con người. Điều này giúp các doanh nghiệp tiết kiệm chi phí và tăng cường cạnh tranh.

Các ứng dụng của AI trong sản xuất bao gồm kiểm soát chất lượng, bảo trì dự đoán, tối ưu hóa chuỗi cung ứng và robot. Các thuật toán tiên tiến đảm bảo chất lượng bằng cách phát hiện lỗi trong sản phẩm trong khi bảo trì dự đoán sẽ tối thiểu hóa thời gian ngừng hoạt động của các trang thiết bị. Các công ty có thể tối ưu chuỗi cung ứng, từ đó phân phối tài nguyên hiệu quả hơn. Các cơ sở sản xuất cũng có thể sử dụng robot để tăng năng suất và mức độ chính xác trong các quy trình.

Trong lĩnh vực y tế, AI có thể phân tích lượng dữ liệu lớn từ bệnh nhân để đưa ra chẩn đoán chính xác và nhanh chóng hơn. Các hệ thống AI có khả năng đọc và phân tích hình ảnh y học, từ đó giúp phát hiện sớm các bệnh nguy hiểm như ung thư; AI không chỉ giúp giảm thiểu thời gian chẩn đoán mà còn nâng cao hiệu quả điều trị. Hệ thống AI có khả năng dự đoán bệnh tật và đề xuất phương pháp điều trị hiệu quả cho từng bệnh nhân, giúp tiết kiệm chi phí cho người bệnh.

AI cũng được tích hợp vào các thiết bị đeo thông minh và các hệ thống giám sát y tế IoT (Internet of Things). Những công nghệ này sẽ liên tục thu thập dữ liệu quý giá liên quan bệnh nhân, như nhịp tim, huyết áp, nồng độ glucose, … để các nhân viên y tế có thể kiểm tra và theo dõi các tình trạng bệnh mãn tính hiệu quả hơn.

Ngoài ra, AI còn đóng góp lớn vào cải thiện sức khỏe tâm thần của người bệnh thông qua các hệ thống hỗ trợ cá nhân hóa. Các chatbot và chuyên gia trị liệu ảo được tạo ra nhờ các thuật toán xử lý ngôn ngữ tự nhiên và học máy có thể tương tác với người dùng trong các phiên trị liệu, giúp họ giải tỏa các triệu chứng căng thẳng, trầm cảm và các vấn đề sức khỏe tâm thần khác.

Trong lĩnh vực dịch vụ khách hàng, các trợ lý ảo và chatbot tích hợp trí tuệ nhân tạo đã giúp đơn giản hóa và cải thiện quy trình hỗ trợ bằng cách cung cấp câu trả lời tức thì (24/7) cho mọi truy vấn từ khách hàng.

Các hệ thống tổng đài tự động hiển nhiên đạt năng suất cao gấp nhiều lần con người, trong khi AI hỗ trợ phân tích cảm xúc khách hàng cho phép các doanh nghiệp hiểu rõ hơn về tình trạng của khách hàng, từ đó phản ứng phù hợp hơn. Các doanh nghiệp còn dùng AI để phân tích dữ liệu người tiêu dùng – bao gồm hành vi, sở thích và lịch sử mua sắm – rồi dùng dữ liệu đó để mang lại một trải nghiệm siêu cá nhân hóa. Thuật toán AI cũng có thể tự động đề xuất sản phẩm, giới thiệu các chương trình khuyến mãi cũng như đưa ra các nội dung liên quan sản phẩm mà khách hàng quan tâm.

AI còn có vai trò quan trọng trong việc đối phó với những thách thức toàn cầu như biến đổi khí hậu và nạn đói. Các hệ thống AI có khả năng phân tích dữ liệu về khí hậu và đề xuất các giải pháp để giảm thiểu tác động của con người lên môi trường. Hơn nữa, AI có thể giúp dự đoán và phát hiện các dịch bệnh và nạn đói, giúp các tổ chức và chính phủ thực hiện các biện pháp phòng ngừa và ứng phó kịp thời.

Trong lĩnh vực tài chính, các tổ chức tài chính hiện đang triển khai AI để phát hiện lừa đảo, thực hiện giao dịch, chấm điểm tín nhiệm và đánh giá rủi ro. Các thuật toán học máy có thể xác định các giao dịch nghi vấn trong thời gian thực, trong khi đó các hệ thống giao dịch thuật toán có tốc độ thực thi lệnh cực nhanh và chính xác. Với AI, các tổ chức tài chính có thể đánh giá rủi ro chính xác hơn, từ đó cải thiện các quyết định cho vay và thực hiện các chiến lược đầu tư.

AI còn cách mạng hóa lĩnh vực hoạch định tài chính và quản lý tài sản bằng cách tạo ra đội quân tư vấn viên robot siêu thông minh, chăm sóc được những tệp khách hàng đa dạng từ các nhà đầu tư mới cho đến các chuyên gia

dày dạn kinh nghiệm thương trường. Các nền tảng AI sử dụng thuật toán cao cấp để phân tích xu hướng thị trường, đánh giá khả năng chịu đựng rủi ro khách hàng và đề xuất các hình thức đầu tư cá nhân hóa.

Trong lĩnh vực vận tải, ô tô cá nhân và xe tải tự lái sẽ giảm thiểu sơ suất từ con người và cải thiện độ an toàn trong lưu thông, đồng thời các hệ thống quản lý giao thông thông minh có thể giúp hạn chế tắc nghẽn. Các thuật toán tối ưu hóa tuyến đường sẽ giúp tiết kiệm thời gian và nhiên liệu, trong khi drone có thể phục vụ giao hàng nhanh chóng và thân thiện với môi trường.

AI cũng tăng cường và cải thiện các hệ thống vận tải công cộng bằng cách dự đoán nhu cầu của hành khách và tối ưu hóa lịch trình.

Trong lĩnh vực nông nghiệp, trên đồng ruộng và trong lĩnh vực công nghệ nông nghiệp (AgTech), người nông dân và các nhà khoa học đang sử dụng AI để giám sát vụ mùa, dự báo thời điểm thu hoạch và diệt trừ sâu bệnh. Các hệ thống nông nghiệp chính xác cao sử dụng AI giúp người nông dân đưa ra những quyết định dựa trên dữ liệu thu được để tối ưu hóa hệ thống tưới tiêu, cải thiện khả năng bón phân và giảm rác thải. Nông dân cũng đang tích cực sử dụng các loại máy móc tự hành - có thể xem chúng như một cuộc cách mạng đối với nông nghiệp truyền thống. Máy cày tự lái - được trang bị các cảm biến tiên tiến, GPS và hệ thống điều khiển bằng AI - có thể thực hiện các tác vụ như cày, xới, gieo hạt và phun nước/thuốc với độ chính xác và hiệu quả cao.

Trong lĩnh vực bán lẻ, các công ty bán lẻ hiện đang sử dụng AI để quản lý kho hàng và tiếp thị nhắm mục tiêu đồng thời tạo ra các hệ thống đề xuất cá nhân hóa và chăm sóc khách hàng bằng chatbot. Các nhà bán lẻ cũng tích hợp công nghệ tìm kiếm thị giác vào các cửa hàng trực tuyến để khách hàng tìm sản phẩm bằng cách upload ảnh thay vì dựa trên các truy vấn từ khóa truyền thống. Các loại engine tìm kiếm thị giác bằng AI này có thể phân tích các đặc điểm của ảnh được upload và cung cấp một danh sách các sản phẩm tương tự để khách hàng ra quyết định mua sắm.

Trong lĩnh vực giáo dục, trong lớp học, hệ thống học thích ứng sẽ sắp xếp nội dung học tập phù hợp với nhu cầu của người học, trong khi thuật toán phát hiện "đạo văn" sẽ đảm bảo tính công bằng và trung thực cho các kỳ thi. Giáo viên thậm chí có thể sử dụng các hệ thống phân tích dữ liệu để dự báo hiệu suất học tập của người học, từ đó can thiệp sớm nếu phát hiện vấn đề.

AI cũng đóng một vai trò đáng kể trong việc phổ cập giáo dục, đặc biệt đối với những khu vực vùng sâu, vùng xa. Các công cụ dịch thuật AI và phiên dịch thời gian thực sẽ xóa bỏ mọi rào cản ngôn ngữ, cho phép người học toàn cầu tiếp cận nội dung giáo dục từ bất cứ đâu trên thế giới. Bên cạnh đó, các gia sư ảo tích hợp AI có thể cung cấp dịch vụ dạy kèm 1 – 1, bổ trợ kiến thức cho người học ngoài giờ học chính, đảm bảo đưa các chương trình giáo dục chất lượng đến một lượng lớn học viên hơn nữa (TENTEN, 2023).

2. NHỮNG THÁCH THỨC ĐỐI VỚI BẢO VỆ DỮ LIỆU CÁ NHÂN TRONG BỐI CẢNH PHÁT TRIỂN TRÍ TUỆ NHÂN TẠO

Quyền riêng tư dữ liệu, vấn đề bảo vệ dữ liệu cá nhân là một mối quan tâm đáng kể liên quan đến AI vì nó chủ yếu dựa vào thông tin cá nhân và nhạy cảm. Nếu không có quy định đầy đủ, các hệ thống AI có thể vi phạm quyền riêng tư của cá nhân, làm suy giảm quyền tự chủ và phẩm giá của con người, làm gia tăng sự chênh lệch liên quan đến việc khai thác dữ liệu,…

Việc sử dụng AI trong công nghệ thanh quản nhân tạo đặt ra những lo ngại đáng kể về quyền riêng tư và bảo mật dữ liệu do các thiết bị này có thể sử dụng các mẫu giọng nói cá nhân và dữ liệu người dùng có thể mang tính bảo mật.

Việc tích hợp AI vào hình ảnh y khoa đại diện cho một cuộc cách mạng đột phá trong

chẩn đoán y tế. AI đặc biệt là các hệ thống sử dụng học máy và học sâu đang ngày càng được sử dụng để cải thiện độ chính xác của các phương pháp hình ảnh y khoa, bao gồm X-quang, MRI và CT scan. Tuy nhiên quyền riêng tư và bảo mật dữ liệu là những mối lo ngại quan trọng đối với các hệ thống AI vì chúng yêu cầu truy cập vào các bộ sưu tập hình ảnh bệnh nhân rộng lớn, điều này đặt ra những lo ngại về bảo vệ dữ liệu y khoa nhạy cảm (Marwala & Mpedi, 2024).

Các quy trình do AI điều khiển như tuyển dụng, đánh giá, giám sát và phân tích năng suất của người lao động cũng đặt ra vấn đề bảo vệ quyền riêng tư của người lao động xung quanh việc sử dụng dữ liệu.

Việc sử dụng công nghệ thiết bị đeo trong nơi làm việc tạo nên mối lo ngại đáng kể có thể xâm phạm quyền riêng tư và bảo vệ dữ liệu.

Sự phát triển của công nghệ lưới điện thông minh do AI điều khiển cho phép phân bổ và quản lý năng lượng tái tạo hiệu quả hơn. Do các hệ thống AI trong năng lượng tái tạo thường phụ thuộc vào các tệp dữ liệu lớn, có thể bao gồm dữ liệu người dùng, việc đảm bảo quyền riêng tư và an ninh dữ liệu là bắt buộc về mặt pháp lý.

AI cho phép các phương tiện không người lái, máy bay không người lái và các nền tảng khác điều hướng một cách độc lập trong địa hình khó khăn mà không cần sự can thiệp của con người.

Sử dụng AI trong vũ khí với các loại vũ khí tự động gây chết người (phương tiện/máy bay không người lái, rô-bốt tự động chiến đấu trên mặt đất, súng tự động, thuyền tự động trên bề mặt, máy bay không người lái dưới nước tự động, công nghệ tự động đám đông, hệ thống tự động mạng) không chỉ là mối lo ngại về quyền dữ liệu mà còn có thể dẫn đến sự gia tăng nhanh chóng về cường độ của các xung đột khi các quyết định được đưa ra vượt quá thời gian phản ứng của con người. Việc tích hợp AI vào vũ khí tự động gây chết người gây ra mối lo ngại lớn về an ninh toàn cầu. Các cuộc tấn công mạng có thể dẫn đến vi phạm dữ liệu, liên quan đến lấy trộm trái phép thông tin quân sự nhạy cảm.

Đối với vấn đề bảo vệ quyền riêng tư và an ninh thông tin, an ninh dữ liệu cũng là một vấn đề bất cập. Các hệ thống AI thường thu thập và xử lý lượng lớn dữ liệu cá nhân, từ thông tin y tế đến thói quen mua sắm. Nếu không được quản lý và bảo mật tốt, dữ liệu này có thể bị lạm dụng hoặc rò rỉ, gây ra hậu quả nghiêm trọng cho cá nhân và xã hội. Với việc thu thập và phân tích dữ liệu ngày càng mạnh mẽ, có nguy cơ rò rỉ thông tin cá nhân và vi phạm quyền riêng tư của cá nhân.

Sự phát triển một số công nghệ mới đặt ra yêu cầu phải bảo vệ dữ liệu cá nhân, như: xử lý dữ liệu lớn, trí tuệ nhân tạo, điện toán đám mây, blockchain, vũ trụ ảo. Blockchain đặt ra một số rủi ro mới với dữ liệu cá nhân, như: dữ liệu cá nhân không thể thay đổi hay xóa; Blockchain công khai cho phép mọi người truy cập tất cả dữ liệu dẫn đến khả năng lộ thông tin nhạy cảm; cơ chế bán ẩn danh vẫn có thể bị truy vết thông qua việc suy luận hành vi người dùng; tính phi tập trung khiến việc thực thi các quy định bảo vệ dữ liệu cá nhân trở nên khó khăn.

AI vẫn đang tạo nên những chuyển biến vô cùng tích cực trong nhiều lĩnh vực khác nhau. Ưu điểm rõ ràng nhất của AI có thể xử lý khối lượng lớn công việc với dữ liệu lớn hơn, nhiều vấn đề hơn cũng như có thể đưa ra những phân tích và dự đoán chính xác hơn con người. Thông thường khi xử lý một lượng dữ liệu lớn, con người chúng ta khó có thể chính xác hoàn toàn, điều này có thể thực hiện được bởi công nghệ trí tuệ nhân tạo. Ngay cả những nhà khoa học cũng cảm thấy khó khăn khi giải quyết số lượng dữ liệu lớn, AI sử dụng học máy để có thể lấy những dữ liệu đó và nhanh chóng biến nó thành thông tin có thể thực hiện được.

Tuy nhiên, nguy cơ rò rỉ thông tin, dữ liệu cá nhân cũng rất cao. Việc sử dụng AI và dữ liệu lớn đòi hỏi sự thu thập và lưu trữ thông tin cá nhân của người dùng. Nếu không có các biện pháp bảo mật mạnh mẽ, thông tin cá nhân có thể bị rò rỉ và đe dọa an ninh

thông tin của người dùng (FPT AfterSchool, 2023).

AI tạo sinh có thể tạo ra những nội dung giả mạo độc hại, vô tình tiết lộ dữ liệu cá nhân trong khi huấn luyện AI, mất quyền kiểm soát của người dùng đối với việc sử dụng dữ liệu. Trong Vũ trụ ảo có lượng dữ liệu cá nhân khổng lồ, chi tiết và được thu thập trong quá trình trải nghiệm đa giác quan (bao gồm hành vi, cảm xúc, cuộc trò chuyện, thói quen), tổng hợp và tạo hồ sơ cá nhân chi tiết (bằng cách kết hợp với dữ liệu cá nhân hiện hữu), ranh giới mờ nhạt giữa danh tính trong môi trường thực ảo (Bộ Công an, 2024).

Do đó, việc xây dựng chính sách bảo mật dữ liệu mạnh mẽ và quản lý thông tin một cách cẩn thận trở nên cực kỳ quan trọng để bảo vệ quyền lợi của người dùng (Trường Đại học Hoa Sen, 2023).

Bảo vệ dữ liệu cá nhân trong bối cảnh Việt Nam thúc đẩy chuyển đổi số

Chuyển đổi số, phát triển kinh tế số, xây dựng xã hội số là xu thế của thời đại. Việt Nam đang đẩy mạnh quá trình này để làm chủ cuộc Cách mạng công nghiệp lần thứ tư. Việt Nam đang đẩy mạnh xây dựng Chính phủ điện tử, hướng tới chính phủ số, nền kinh tế số với sự tham gia ngày càng sâu rộng của các lĩnh vực y tế, thương mại điện tử, giáo dục, tài chính, ngân hàng, thuế,… Công nghệ thông tin, truyền thông, trí tuệ nhân tạo, internet vạn vật, điện toán đám mây, dữ liệu lớn, dữ liệu nhanh,… được ứng dụng sâu rộng tạo ra những giá trị xã hội to lớn.

Dữ liệu cá nhân là một trong những nguyên liệu chính để thực hiện chuyển đổi số, phát triển kinh tế số, xây dựng xã hội số. Dữ liệu cá nhân là vấn đề liên quan tới chặt chẽ tới quyền con người, quyền công dân, an toàn, an ninh mạng, an ninh thông tin, an ninh dữ liệu. Dữ liệu cá nhân của hơn 2/3 dân số nước ta đang được lưu trữ, đăng tải, chia sẻ và thu thập trên không gian mạng với nhiều hình thức và mức độ chi tiết khác nhau. Cơ sở hạ tầng không gian mạng phát triển nhanh và ngày càng hoàn thiện, tạo điều kiện thuận lợi cho các ngành, nghề, dịch vụ kinh doanh có liên quan tới dữ liệu cá nhân phát triển.

Thách thức trong bảo vệ dữ liệu cá nhân ở Việt Nam

Bối cảnh hiện nay ở Việt Nam cũng đặt ra nhiều thách thức về bảo vệ dữ liệu cá nhân. Cụ thể:

Tình trạng lộ dữ liệu cá nhân diễn ra phổ biến trên không gian mạng. Người sử dụng chưa có ý thức bảo vệ dữ liệu cá nhân, đăng tải công khai hoặc lộ trong quá trình chuyển giao, lưu trữ, trao đổi phục vụ hoạt động kinh doanh hoặc do biện pháp bảo vệ không tương xứng dẫn tới bị chiếm đoạt và đăng tải công khai. Tình trạng mua bán dữ liệu cá nhân hiện đang diễn ra phổ biến, công khai, với các dữ liệu thô và dữ liệu cá nhân đã qua xử lý, nhiều hành vi chưa được xử lý vì thiếu quy định của pháp luật. Các doanh nghiệp, công ty kinh doanh dịch vụ có thu thập dữ liệu cá nhân của khách hàng, cho phép các đối tác thứ ba tiếp cận thông tin dữ liệu cá nhân nhưng không có yêu cầu, quy định chặt chẽ, để đối tác thứ ba chuyển giao, buôn bán cho các đối tác khác. Các doanh nghiệp chủ động thu thập thông tin cá nhân của khách hàng, hình thành kho dữ liệu cá nhân, phân tích, xử lý các loại dữ liệu đó để tiến hành kinh doanh, buôn bán. Việc buôn bán dữ liệu cá nhân được tiến hành có hệ thống, có tổ chức, cam kết "bảo hành" và có khả năng cập nhật dữ liệu, trích xuất dữ liệu theo yêu cầu người mua. Nhiều dữ liệu bị rao bán công khai trong thời gian dài với số lượng lớn trên không gian mạng. Việc mua bán được tiến hành qua website, tài khoản, trang, nhóm trên mạng xã hội, diễn đàn tin tặc. Việc thanh toán được thực hiện thông qua tài khoản ngân hàng, nhiều giao dịch ghi rõ nội dung mua bán dữ liệu (Bộ Công an, 2024).

Nhiều tổ chức, doanh nghiệp thu thập thừa dữ liệu cá nhân so với ngành nghề, sản phẩm, dịch vụ kinh doanh; thiếu cơ sở pháp lý khi thu thập dữ liệu. Bên cạnh đó, đơn vị thu thập không xác định được dữ liệu cá nhân được sử dụng như thế nào, vào mục đích gì, chuyển

giao cho ai, tác động thế nào. Nhiều hoạt động thu thập, xử lý dữ liệu cá nhân mà chưa có sự đồng ý của chủ thể dữ liệu. Thậm chí, nhiều chủ thể dữ liệu không biết tại sao các công ty này lại có dữ liệu của mình.

Pháp luật Việt Nam về bảo vệ dữ liệu cá nhân

Để bảo vệ quyền riêng tư, Điều 21 Hiến pháp năm 2013 đã kế thừa các quy định của các bản Hiến pháp trước đây, 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 là quyền bất khả xâm phạm 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.

Hiện nay việc quản lý dữ liệu cá nhân được thực hiện theo Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân. Nghị định số 13/2023/NĐ-CP là văn bản pháp lý quan trọng đầu tiên quy định đầy đủ các biện pháp quản lý nhà nước cũng như biện pháp bảo vệ dữ liệu cá nhân cùng với các quyền, nghĩa vụ, trách nhiệm của các chủ thể có liên quan. Nhiều nội dung của Nghị định đã được kế thừa và phát triển để quy định trong Luật Bảo vệ dữ liệu cá nhân được Quốc hội thông qua năm 2025.

Nghị định này đưa ra định nghĩa khái niệm dữ liệu cá nhân là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể. Nghị định số 13/2003/NĐ-CP xác định nội hàm của bảo vệ dữ liệu cá nhân là hoạt động phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi vi phạm liên quan đến dữ liệu cá nhân theo quy định của pháp luật; đồng thời xác định xử lý dữ liệu cá nhân là một hoặc nhiều hoạt động tác động tới dữ liệu cá nhân, như: thu thập, ghi, phân tích, xác nhận, lưu trữ, chỉnh sửa, công khai, kết hợp, truy cập, truy xuất, thu hồi, mã hóa, giải mã, sao chép, chia sẻ, truyền đưa, cung cấp, chuyển giao, xóa, hủy dữ liệu cá nhân hoặc các hành động khác có liên quan.

Dữ liệu cá nhân bao gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm.

Dữ liệu cá nhân cơ bản bao gồm: Họ, chữ đệm và tên khai sinh, tên gọi khác (nếu có); ngày, tháng, năm sinh; ngày, tháng, năm chết hoặc mất tích; giới tính; nơi sinh, nơi đăng ký khai sinh, nơi thường trú, nơi tạm trú, nơi ở hiện tại, quê quán, địa chỉ liên hệ; quốc tịch; hình ảnh của cá nhân; số điện thoại, số chứng minh nhân dân, số định danh cá nhân, số hộ chiếu, số giấy phép lái xe, số biển số xe, số mã số thuế cá nhân, số bảo hiểm xã hội, số thẻ bảo hiểm y tế; tình trạng hôn nhân; thông tin về mối quan hệ gia đình (cha mẹ, con cái); thông tin về tài khoản số của cá nhân; dữ liệu cá nhân phản ánh hoạt động, lịch sử hoạt động trên không gian mạng;…

Dữ liệu cá nhân nhạy cảm là dữ liệu cá nhân gắn liền với quyền riêng tư của cá nhân mà khi bị xâm phạm sẽ gây ảnh hưởng trực tiếp tới quyền và lợi ích hợp pháp của cá nhân gồm: quan điểm chính trị, quan điểm tôn giáo; tình trạng sức khỏe và đời tư được ghi trong hồ sơ bệnh án, không bao gồm thông tin về nhóm máu; thông tin liên quan đến nguồn gốc chủng tộc, nguồn gốc dân tộc; thông tin về đặc điểm di truyền được thừa hưởng hoặc có được của cá nhân; thông tin về thuộc tính vật lý, đặc điểm sinh học riêng của cá nhân; thông tin về đời sống tình dục, xu hướng tình dục của cá nhân; dữ liệu về tội phạm, hành vi phạm tội được thu thập, lưu trữ bởi các cơ quan thực thi pháp luật; thông tin khách hàng của tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, tổ chức cung ứng dịch vụ trung gian thanh toán, các tổ chức được phép khác, gồm: thông tin định danh khách hàng theo quy định của pháp luật, thông tin về tài khoản, thông tin về tiền gửi, thông tin về tài sản gửi, thông tin về giao dịch, thông tin về tổ chức, cá nhân là bên bảo đảm tại tổ chức tín dụng, chi nhánh ngân hàng, tổ chức cung ứng dịch vụ trung gian thanh toán; dữ liệu về vị trí của cá nhân được xác định qua dịch vụ định vị; dữ liệu cá nhân khác được pháp luật quy định là đặc thù và cần có biện pháp bảo mật cần thiết.

Ngày 26/6/2025, Quốc hội thông qua Luật Bảo vệ dữ liệu cá nhân, có hiệu lực thi hành từ ngày 01/01/2026. Việc ban hành Luật Bảo vệ dữ liệu cá nhân nhằm thể chế hóa quan điểm chỉ đạo của Đảng về bảo vệ quyền con người, quyền công dân, quyền và lợi ích hợp pháp của cá nhân; hoàn thiện, thống nhất hệ thống pháp luật về bảo vệ dữ liệu cá nhân, tạo hành lang pháp lý cho công tác bảo vệ dữ liệu cá nhân, nâng cao năng lực bảo vệ dữ liệu cá nhân cho các tổ chức, cá nhân trong nước tiếp cận trình độ quốc tế, khu vực; đẩy mạnh sử dụng dữ liệu cá nhân đúng pháp luật phục vụ phát triển kinh tế, xã hội. Luật gồm 05 Chương, 39 Điều, quy định về các vấn đề: 1) phạm vi điều chỉnh, đối tượng áp dụng, nguyên tắc bảo vệ dữ liệu cá nhân, quyền và nghĩa vụ của chủ thể dữ liệu cá nhân, hành vi bị nghiêm cấm, xử lý vi phạm pháp luật về bảo vệ dữ liệu cá nhân; 2) bảo vệ dữ liệu cá nhân trong quá trình xử lý dữ liệu và bảo vệ dữ liệu cá nhân trong một số hoạt động, lĩnh vực cụ thể; 3) lực lượng, điều kiện bảo đảm bảo vệ dữ liệu cá nhân; 3) trách nhiệm của cơ quan, tổ chức, cá nhân về bảo vệ dữ liệu cá nhân.

Trước đó, ngày 30/11/2024 Quốc hội đã thông qua Luật Dữ liệu, Luật có hiệu lực từ ngày 01/7/2025, sẽ từng bước thiết lập thị trường dữ liệu, thúc đẩy chuyển đổi số quốc gia. Luật Dữ liệu vừa được thông qua có quy định lập Cơ sở dữ liệu tổng hợp quốc gia, nhằm phục vụ mục đích quốc phòng, an ninh, đối ngoại, cơ yếu, đấu tranh phòng, chống tội phạm, xử lý vi phạm pháp luật; phục vụ nhu cầu khai thác, sử dụng, ứng dụng dữ liệu của tổ chức, cá nhân. Cơ sở dữ liệu này sẽ được tích hợp thông tin từ kết quả thực hiện thủ tục hành chính, dịch vụ công; dữ liệu được chia sẻ, đồng bộ từ các cơ sở dữ liệu khác; dữ liệu được số hóa, cung cấp bởi cá nhân, tổ chức và nguồn khác theo quy định. Mô hình này phục vụ giải quyết thủ tục hành chính, dịch vụ công, đưa ra các chỉ tiêu, chỉ số phục vụ chỉ đạo điều hành của Chính phủ; phục vụ công tác thống kê, hoạch định chính sách, xây dựng quy hoạch, chiến lược phát triển kinh tế - xã hội. Trong Luật Dữ liệu vừa thông qua có nhiều quy định hoạt động xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu; sản phẩm, dịch vụ về dữ liệu; quản lý nhà nước về dữ liệu, trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan đến hoạt động về dữ liệu. Bên cạnh đó, Luật có quy định về việc chuyển, xử lý dữ liệu xuyên biên giới. Theo đó, cơ quan, tổ chức, cá nhân được tự do chuyển dữ liệu từ nước ngoài về Việt Nam, xử lý dữ liệu của nước ngoài tại Việt Nam, được Nhà nước bảo vệ các quyền và lợi ích hợp pháp theo quy định của pháp luật.

Tổ chức, cá nhân phải cung cấp dữ liệu cho cơ quan Nhà nước khi có yêu cầu của cơ quan có thẩm quyền mà không cần chủ thể dữ liệu đồng ý trong các trường hợp sau đây: Ứng phó với tình trạng khẩn cấp; Khi có nguy cơ đe dọa quốc phòng, an ninh nhưng chưa đến mức ban bố tình trạng khẩn cấp; Thảm họa; Phòng, chống bạo loạn, khủng bố. Bên cạnh đó, cơ quan Nhà nước nhận được dữ liệu có trách nhiệm sử dụng dữ liệu đúng mục đích. Cơ quan này cũng bảo đảm an ninh, an toàn dữ liệu, bảo vệ bí mật dữ liệu, lợi ích hợp pháp khác của chủ thể dữ liệu, tổ chức, cá nhân cung cấp dữ liệu theo quy định của pháp luật,...

3. KẾT LUẬN

Để pháp luật đáp ứng yêu cầu của cuộc Cách mạng công nghiệp 4.0 và sự phát triển của trí tuệ nhân tạo, cần hoàn thiện hệ thống pháp luật theo hướng vừa phải tuân thủ các nguyên lý nền tảng, vừa đủ thông thoáng nhằm thúc đẩy nghiên cứu và ứng dụng trí tuệ nhân tạo nhưng cũng cần đủ chặt chẽ, đảm bảo an toàn cho con người và xã hội; tiếp tục duy trì các nguyên tắc công bằng, minh bạch và công lý; cân bằng đúng đắn giữa tiến bộ công nghệ và bảo vệ quyền bảo vệ dữ liệu cá nhân, khai thác lợi ích và giảm thiểu rủi ro của AI.