VNU Journal of Science: Legal Studies

Journal homepage: https://js.vnu.edu.vn/LS

Original Article

Artificial Intelligence and the Challenge of Protecting Privacy in Legal Consultancy Services in Viet Nam

Tran Phu Tai*

Nguyen Chi Thanh Political School, 266 Dien Bien Phu, Thuan Hoa, Hue, Vietnam

Received 21st June 2025
Revised 28 September 2025; Accepted 14 April 2026

Abstract: Artificial Intelligence (AI) has been generating numerous opportunities for innovation in the field of legal consultancy, particularly through digital platforms and automated support systems. However, the deepening integration of AI into the processes of handling, analyzing, and storing legal information simultaneously poses significant challenges to the protection of privacy, a fundamental human right enshrined in international treaties and Vietnamese law. This article, adopting a human rights-based approach, analyzes the potential privacy risks associated with the use of AI in legal consultancy services. These risks include the collection, processing, and storage of sensitive personal data, lack of transparency in data handling, potential information leakage, and the absence of effective mechanisms for accountability and oversight. Through an examination of AI-based legal consultancy models implemented in several countries, and a comparison with the current practices in Vietnam, the article identifies existing legal gaps - particularly regarding the regulation of legal liability for system operators, the enforcement of ethical standards in technology deployment, and the protection of personal data in digital legal consultancy environments. The paper aims to contribute to the development of a modern legal framework that not only promotes innovation but also ensures the robust protection of fundamental human rights.

Keywords: Artificial Intelligence, Human Rights, Legal Consultancy, Personal Data.

* Corresponding author.
E-mail address:

https://doi.org/10.25073/2588-1167/vnuls.4790

Trí tuệ nhân tạo và thách thức bảo vệ quyền riêng tư trong dịch vụ tư vấn pháp luật tại Việt Nam

Trần Phú Tài*

Trường Chính trị Nguyễn Chí Thanh, 266 Điện Biên Phủ, Thuận Hóa, Huế, Việt Nam

Nhận ngày 21 tháng 6 năm 2025
Chỉnh sửa ngày 28 tháng 9 năm 2025; Chấp nhận đăng ngày 20 tháng 5 năm 2026

Tóm tắt: Trí tuệ nhân tạo đã và đang mở ra nhiều cơ hội đổi mới trong lĩnh vực tư vấn pháp luật, đặc biệt là thông qua các nền tảng số và hệ thống hỗ trợ tự động. Tuy nhiên, sự can thiệp ngày càng sâu rộng của trí tuệ nhân tạo vào quy trình xử lý, phân tích và lưu trữ thông tin pháp lý cũng đồng thời đặt ra những thách thức nghiêm trọng đối với việc bảo vệ quyền riêng tư - quyền con người cơ bản được ghi nhận trong các điều ước quốc tế và pháp luật Việt Nam. Trên cơ sở tiếp cận dựa trên quyền con người, bài viết sẽ tập trung phân tích những rủi ro tiềm ẩn về quyền riêng tư khi sử dụng trí tuệ nhân tạo trong dịch vụ tư vấn pháp luật, như việc thu thập, xử lý và lưu trữ dữ liệu cá nhân nhạy cảm, không minh bạch, nguy cơ rò rỉ thông tin, thiếu vắng cơ chế giải trình và kiểm soát hiệu quả. Trên cơ sở phân tích các mô hình tư vấn pháp luật sử dụng AI đang triển khai tại một số quốc gia và so sánh với thực tiễn tại Việt Nam, bài viết chỉ ra những khoảng trống pháp lý hiện hữu, đặc biệt là trong việc điều chỉnh trách nhiệm pháp lý của các chủ thể vận hành hệ thống, bảo đảm tiêu chuẩn đạo đức công nghệ và bảo vệ dữ liệu cá nhân. Bài viết còn hướng đến việc góp phần xây dựng một môi trường pháp lý hiện đại, vừa thúc đẩy đổi mới sáng tạo, vừa bảo đảm vững chắc các quyền cơ bản của con người.

Từ khóa: Trí tuệ nhân tạo, quyền con người, tư vấn pháp luật, dữ liệu cá nhân.

1. Mở đầu

Cuộc cách mạng công nghiệp lần thứ tư đã thúc đẩy sự phát triển mạnh mẽ của công nghệ, trong đó trí tuệ nhân tạo (AI) ngày càng giữ vai trò trung tâm, kể cả trong lĩnh vực tư vấn pháp luật vốn đòi hỏi cao về chuyên môn, đạo đức và bảo mật. Tại Việt Nam, chuyển đổi số được xác định là nhiệm vụ trọng tâm trong cải cách tư pháp, lập pháp và hành pháp. Các cơ quan tư pháp và công ty luật đã bắt đầu ứng dụng AI thông qua các nền tảng tư vấn pháp luật trực tuyến, dịch vụ số hóa, làm thay đổi cách tiếp cận vụ việc và cung cấp dịch vụ. Sự chuyển đổi này giúp tiết kiệm chi phí, nâng cao khả năng tiếp cận công lý và rút ngắn thời gian xử lý.

Tuy nhiên, ứng dụng AI trong dịch vụ tư vấn pháp luật cũng đặt ra câu hỏi nghiêm túc về quyền riêng tư của người dùng trong môi trường số. Đặc biệt, dữ liệu pháp lý vốn được bảo vệ nghiêm ngặt nay có nguy cơ bị AI thu thập, xử lý và chia sẻ khi thiếu sự kiểm soát và giám sát pháp lý phù hợp. Vấn đề này làm nảy sinh mối quan ngại sâu sắc liên quan đến khả năng bảo vệ quyền riêng tư – một quyền cơ bản đã được ghi nhận trong luật quốc tế về nhân quyền và Hiến pháp Việt Nam. Xuất phát từ yêu cầu đó, bài viết sử dụng các phương pháp nghiên cứu định tính,

* Tác giả liên hệ.
Địa chỉ email:

https://doi.org/10.25073/2588-1167/vnuls.4790

bao gồm phân tích - tổng hợp tài liệu, so sánh luật và nghiên cứu trường hợp (case study), nhằm đảm bảo cách tiếp cận có hệ thống, khách quan và toàn diện đối với vấn đề nghiên cứu. Trên cơ sở cách tiếp cận liên ngành giữa pháp luật và công nghệ, bài viết phan tích vòng đời dữ liệu AI (thu thập, xử lý, lưu trữ, chia sẻ) với các rủi ro pháp lý và biện pháp kỹ thuật tương ứng; đồng thời cập nhật và đánh giá các quy định mới của Luật Bảo vệ dữ liệu cá nhân năm 2025 và Luật Công nghiệp công nghệ số năm 2025.

Dưới góc độ quyền con người, bài viết tập trung làm rõ các vấn đề sau: i) AI đang làm thay đổi bản chất và quy trình của dịch vụ tư vấn pháp luật như thế nào? ii) Những rủi ro cụ thể nào về quyền riêng tư phát sinh trong quá trình ứng dụng AI vào hoạt động tư vấn pháp luật? iii) Liệu rằng khung pháp luật hiện hành ở Việt Nam và quốc tế đã đủ khả năng để bảo vệ quyền riêng tư trước sự phát triển của AI hay chưa? Trên cơ sở đó, bài viết đề xuất các định hướng hoàn thiện pháp luật nhằm tăng cường bảo vệ quyền riêng tư, đồng thời bảo đảm sự cân bằng giữa đổi mới công nghệ và bảo vệ các quyền cơ bản của con người trong bối cảnh chuyển đổi số hiện nay.

2. Nghiên cứu và thảo luận

2.1. Khái niệm và khung pháp lý về quyền riêng tư

Quyền riêng tư (right to privacy) xét về mặt học thuật, không chỉ được hiểu đơn thuần là quyền được sống tách biệt hay tránh khỏi sự can thiệp không chính đáng vào đời sống cá nhân, mà còn gắn liền với các chức năng thiết yếu trong đời sống con người như: bảo vệ tự do, thúc đẩy tính tự chủ, khẳng định bản sắc cá nhân, duy trì các mối quan hệ xã hội lành mạnh và góp phần vào việc xây dựng một xã hội tự do [1]. Theo định nghĩa kinh điển của Warren và Brandeis (1890), quyền riêng tư là "the right to be let alone" [2] - tức quyền được hưởng cuộc sống một cách riêng biệt, không bị xâm phạm. Quyền riêng tư là một trong những quyền con người cơ bản được ghi nhận rộng rãi trong hệ thống pháp luật quốc tế, từ các công ước toàn cầu đến các văn kiện khu vực và các chuẩn mực quốc gia, gồm Việt Nam. Điều 17 Công ước Quốc tế về các Quyền Dân sự và Chính trị năm 1966 (ICCPR) quy định: "Không ai bị can thiệp một cách tùy tiện hoặc bất hợp pháp vào đời sống riêng tư, gia đình, nhà ở, thư tín, hoặc bị xâm phạm bất hợp pháp đến danh dự và uy tín" [3]. Trong bối cảnh Việt Nam, sự riêng tư được tác giả trong sách do Nguyễn Thị Quế Anh và cộng sự đồng chủ biên (2018) cho rằng đó là "trao cho mỗi cá nhân một không gian để là chính mình mà không bị người khác phán xét một cách vô cớ, cho phép mỗi người suy nghĩ một cách tự do mà không bị kỳ thị hoặc phân biệt đối xử, cũng như khả năng kiểm soát ai được biết gì về bản thân mình" [4]. Điều này hàm ý rằng quyền riêng tư không chỉ là việc giữ bí mật thông tin cá nhân hay tránh bị người khác xâm phạm, mà còn là quyền để mỗi người được sống là chính mình, có một không gian riêng, nơi họ được suy nghĩ, cảm nhận và hành động theo cách riêng của mình mà không bị áp đặt hay can thiệp. Điều 21 Hiến pháp Việt Nam năm 2013 lần đầu tiên ghi nhận: "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" [5], thể hiện sự tiếp cận tiến bộ trong bảo vệ quyền riêng tư, quyền con người. Nội dung này đã được cụ thể hóa trong một số văn bản pháp luật quan trọng của Việt Nam, như Bộ luật Dân sự năm 2015 (Điều 38 Quyền về đời sống riêng tư, bí mật cá nhân, bí mật gia đình), Luật An toàn thông tin mạng năm 2015,… gần đây nhất là Luật Bảo vệ dữ liệu cá nhân năm 2025. Như vậy, hệ thống pháp luật Việt Nam hiện hành đã từng bước tiếp cận với các nguyên tắc quốc tế, nhất là trong bối cảnh Việt Nam đang đẩy mạnh chuyển đổi số quốc gia và phát triển Chính phủ điện tử.

Với những phân tích trên, có thể nhìn nhận một cách khái quát rằng: "Quyền riêng tư là quyền của cá nhân được bảo vệ khỏi sự can thiệp trái phép vào đời sống cá nhân, thông tin cá nhân, thân thể, mối quan hệ và các hoạt động riêng tư khác, đồng thời có quyền kiểm soát việc thu thập,

sử dụng và chia sẻ thông tin về bản thân mình". Quyền riêng tư bao gồm: sự riêng tư về thông tin cá nhân (Privacy of information); sự riêng tư về cơ thể (Bodily privacy); sự riêng tư về thông tin liên lạc (Privacy of communications); sự riêng tư về nơi cư trú (Territorial privacy) [6]. Đồng thời quyền này mang một số đặc điểm nổi bật như sau: (1) Tính cá nhân hóa: đây được xem là quyền tự thân, phát sinh ngay khi một cá nhân tồn tại với tư cách là một chủ thể có tư duy và nhân cách độc lập, gắn liền với nhân phẩm con người và không thể bị tước bỏ một cách tùy tiện. Quyền này phản ánh nhu cầu được "là chính mình" và kiểm soát thông tin về bản thân. (2) Tính hai chiều: một mặt quyền này đòi hỏi sự tôn trọng và không xâm phạm quyền riêng tư của người khác từ mọi chủ thể, cả Nhà nước và các tổ chức, cá nhân khác, tức có hiệu lực ngang nhau đối với cả khu vực công và tư; mặt khác, quyền này vừa mang tính chủ động kiểm soát, tức là cá nhân có quyền lựa chọn ai được biết điều gì, trong hoàn cảnh nào các thông tin của mình. (3) Quyền riêng tư không phải là quyền tuyệt đối và có thể bị hạn chế trong những trường hợp nhất định. Tuy nhiên, theo các chuẩn mực của luật nhân quyền quốc tế, mọi biện pháp can thiệp vào quyền riêng tư chỉ được chấp nhận khi đáp ứng đồng thời ba điều kiện: i) có cơ sở pháp lý rõ ràng, minh bạch và có thể dự liệu được (legality); ii) nhằm đạt được một mục tiêu chính đáng như bảo vệ an ninh quốc gia, trật tự công cộng, sức khỏe cộng đồng hoặc quyền và tự do của người khác (legitimacy); và iii) bảo đảm tính cần thiết và tương xứng giữa mức độ can thiệp với mục tiêu cần bảo vệ (necessity and proportionality) [3]. Với ba đặc điểm nêu trên cho thấy quyền riêng tư là một quyền có tính nền tảng, gắn liền với nhân phẩm con người và không thể bị xâm phạm một cách tùy tiện.

Trong quyền riêng tư này, các dữ liệu cá nhân nhạy cảm là những thông tin gắn liền với quyền riêng tư cá nhân, khi bị xâm phạm sẽ gây ảnh hưởng trực tiếp đến quyền, lợi ích hợp pháp của cá nhân và các bên liên quan. Ở chuẩn mực quốc tế, Quy định chung về bảo vệ dữ liệu (GDPR) của Liên minh Châu Âu (EU) cũng định nghĩa "dữ liệu đặc biệt" tương tự, bao gồm thông tin về chủng tộc, quan điểm chính trị, tín ngưỡng, sinh học/di truyền, sức khỏe, đời sống tình dục, v.v., và cấm xử lý các loại này trừ khi có điều kiện đặc biệt (đồng ý rõ ràng, quyền lợi pháp lý, y tế công cộng…) [7]. Theo pháp luật Việt Nam, dữ liệu cá nhân nhạy cảm bao gồm các loại thông tin như: dữ liệu tiết lộ nguồn gốc chủng tộc, nguồn gốc dân tộc; quan điểm chính trị, tôn giáo, tín ngưỡng; thông tin về đời sống riêng tư, bí mật cá nhân, bí mật gia đình; tình trạng sức khỏe; dữ liệu sinh trắc học, đặc điểm di truyền; đời sống tình dục hay xu hướng tình dục; dữ liệu tội phạm (của cơ quan điều tra); thông tin tài chính - tín dụng cá nhân; vị trí định vị cá nhân; cùng các dữ liệu khác đặc thù cần bảo mật [8, 9]. Trong lĩnh vực pháp lý nói chung và lĩnh vực tư vấn pháp luật nói riêng, dữ liệu khách hàng thường rất đa dạng và nhiều khi mang tính chất cực kỳ nhạy cảm [10]: từ các thông tin nhận dạng cá nhân (PII), thông tin vụ án, tình tiết, chiến lược kinh doanh, bí mật công nghiệp đến thông tin cá nhân như sức khỏe, tài chính, tư tưởng chính trị, tôn giáo,… Một minh chứng điển hình là vụ rò rỉ Hồ sơ Panama, trong đó các thông tin bí mật của khách hàng tại công ty luật Mossack Fonseca đã bị công bố rộng rãi, cho thấy dữ liệu do các công ty luật nắm giữ hoàn toàn có thể trở thành mục tiêu của các cuộc tấn công và bị đánh cắp [11]. Trong bối cảnh dữ liệu cá nhân bị xâm phạm, khách hàng có thể phải gánh chịu những thiệt hại nghiêm trọng về mặt cá nhân, như bị lừa đảo, phân biệt đối xử hoặc mất uy tín xã hội, đặc biệt, khách hàng sẽ đánh mất niềm tin vào luật sư cũng như toàn bộ hệ thống pháp lý. Vì vậy, rủi ro này không chỉ dừng lại ở mức xử phạt hành chính hay kỷ luật nghề nghiệp, mà còn có thể kéo theo những tổn thất kinh tế - xã hội đáng kể đối với cả khách hàng, luật sư và tổ chức cung cấp dịch vụ pháp lý. Do đó, việc phân loại chính xác và áp dụng các biện pháp bảo vệ nghiêm ngặt đối với dữ liệu cá nhân, đặc biệt là dữ liệu nhạy cảm, là yêu cầu bắt buộc nhằm bảo đảm quyền riêng tư và duy trì niềm tin vào các dịch vụ pháp lý.

2.2. Mối quan hệ giữa AI và quyền riêng tư trong dịch vụ tư vấn pháp luật

Trong bối cảnh AI đã và đang được ứng dụng vào rất nhiều các lĩnh vực khác nhau, trong đó có cả lĩnh vực tư vấn pháp luật đã tạo ra những thay đổi sâu sắc cả về bản chất lẫn cách thức thực hiện hoạt động tư vấn. Trước đây, hoạt động tư vấn pháp luật chủ yếu dựa vào kỹ năng suy luận, đạo đức nghề nghiệp và sự hiện diện trực tiếp thực hiện của con người (những luật sư, cộng tác viên, thực tập sinh, chuyên viên tư vấn pháp lý, trợ giúp viên pháp lý hoặc một số cá nhân người am hiểu pháp luật…), thì hiện nay, trên thế giới các nền tảng "legal tech" (công nghệ pháp lý) có ứng dụng AI đã và đang phát triển mạnh mẽ trong việc nghiên cứu pháp luật, dự đoán kết quả vụ án, soạn thảo văn bản pháp lý, tư vấn sơ bộ cho khách hàng,… Một ví dụ điển hình là hệ thống Luminance của Anh, sử dụng AI để tự động hóa quy trình rà soát hợp đồng, phân tích rủi ro pháp lý và tổng hợp thông tin trong các giao dịch sáp nhập - mua bán doanh nghiệp (M&A) tại Anh. Luminance được thiết kế theo nguyên tắc "privacy by design", tức hệ thống mặc định hạn chế việc thu thập dữ liệu cá nhân, cho phép người dùng kiểm soát quyền truy cập, và đảm bảo dữ liệu được mã hóa tuân theo tiêu chuẩn bảo mật ISO 27001. Người dùng được yêu cầu đồng ý rõ ràng trước khi dữ liệu được xử lý, có thể chỉnh sửa, xóa, chuyển dữ liệu, và luôn được thông báo về phạm vi sử dụng thông tin. Mọi hoạt động xử lý dữ liệu đều nằm trong phạm vi giám sát của Văn phòng Ủy viên Thông tin (ICO), cơ quan có thẩm quyền xử phạt nếu phát hiện vi phạm quyền riêng tư của người dùng [12]. Hay mô hình DoNotPay [13], một chatbot pháp lý ra đời tại Hoa Kỳ năm 2015, ban đầu nhằm hỗ trợ người dùng kháng lại biên bản phạt giao thông, sau đó đã phát triển thành một nền tảng hỗ trợ xử lý nhiều vấn đề pháp lý phổ biến như khiếu nại người tiêu dùng, yêu cầu hoàn tiền, hoặc hủy đăng ký dịch vụ. Hoặc một mô hình khác là ROSS Intelligence [14] là một trợ lý pháp lý để hỗ trợ luật sư tra cứu án lệ, văn bản pháp luật và đưa ra đề xuất sơ bộ, hệ thống này không tiếp xúc trực tiếp với khách hàng cá nhân mà chủ yếu phục vụ các hãng luật lớn tại Hoa Kỳ và Canada, nhưng sau đó đã ngừng hoạt động do tranh chấp bản quyền. Có thể thấy rằng, ứng dụng AI không chỉ là một xu hướng công nghệ mà là một cuộc cách mạng trong phương thức cung cấp và sử dụng dịch vụ pháp lý. Khi các hệ thống này ngày càng được tích hợp nhiều vào quá trình ra quyết định pháp lý, các vấn đề liên quan đến trách nhiệm pháp lý, tính minh bạch và hiệu lực pháp lý trở nên cấp thiết và đặt ra yêu cầu phải được làm rõ một cách kịp thời và toàn diện [15]. Việc ứng dụng AI trong tư vấn pháp luật làm thay đổi vai trò của luật sư, mô hình kinh doanh của hãng luật, và thậm chí là vai trò của Nhà nước trong đảm bảo công lý. Cùng với đó, quyền riêng tư không chỉ dừng lại ở việc bảo mật thông tin cá nhân, mà còn liên quan đến quyền kiểm soát dữ liệu của chính họ, quyền không bị theo dõi và quyền được biết thông tin của họ đang bị xử lý ra sao.

Hệ thống AI dành cho lĩnh vực tư vấn pháp luật thường tuân theo quy trình nhiều giai đoạn: từ thu thập dữ liệu pháp lý ban đầu, đến tiền xử lý và phân tích, rồi lưu trữ và cuối cùng là sử dụng kết quả phân tích để đưa ra khuyến nghị pháp lý. Việc thu thập dữ liệu pháp lý sẽ tự động hóa kết nối và tải về các văn bản pháp lý đa dạng (án lệ, luật, hợp đồng,…) từ nhiều nguồn khác nhau; sau đó dữ liệu này được làm sạch (loại bỏ ký tự thừa, chuẩn hóa ngôn ngữ), trích xuất đặc trưng (định danh thực thể, token hóa) để đưa vào bước huấn luyện mô hình học máy. Sau khi thu thập, dữ liệu được xử lý và phân tích bằng các mô hình học máy. Lớp xử lý của kiến trúc AI chịu trách nhiệm tiền xử lý dữ liệu, trích xuất đặc trưng và huấn luyện mô hình học máy trên tập dữ liệu đã được làm sạch. Ở giai đoạn này, AI có thể sử dụng cả kỹ thuật học có giám sát lẫn không giám sát để xây dựng các mô hình phân loại, định hướng tìm kiếm văn bản hoặc đề xuất tài liệu pháp lý phù hợp. Một lớp lưu trữ trung tâm (Data Layer) chuyên biệt lưu trữ toàn bộ dữ liệu pháp lý đã thu thập, đóng vai trò như kho trung tâm cho hệ thống. Tại đây, dữ liệu được tổ chức theo cấu trúc rõ ràng, giúp đảm bảo pháp lý và thuận tiện cho việc truy xuất. Đồng thời tuân thủ các tiêu chuẩn pháp lý và tạo điều kiện cho các hoạt động quản lý dữ liệu hiệu quả [16]. Theo Feenberg (1999), công nghệ mang theo các giá trị định hướng và không thể được coi là trung

lập, công nghệ tác động đến người dùng không chỉ ở mức phương tiện mà còn định hình cả hành vi, lựa chọn và thậm chí là tư duy của người sử dụng [17], từ đó ảnh hưởng trực tiếp đến quyền con người, bao gồm cả quyền riêng tư. Dưới góc độ tiếp cận về quyền con người, Mantelero (2016) cho rằng mọi công nghệ, bao gồm AI, phải được thiết kế ngay từ đầu để tôn trọng và bảo vệ các quyền con người, đặc biệt là quyền riêng tư [18]. Điều này đòi hỏi các hệ thống tư vấn pháp luật dựa trên AI cần phải đảm bảo khả năng kiểm soát dữ liệu cho người dùng, minh bạch thuật toán, và có cơ chế phản hồi/giải trình phù hợp.

Việc các dữ liệu pháp lý để huấn luyện AI thường bao gồm cả thông tin nhạy cảm và cá nhân đặt ra vấn đề là lượng dữ liệu cần dùng cho huấn luyện thường rất lớn, trong khi các quy định bảo vệ dữ liệu cá nhân lại khuyến cáo hạn chế thu thập và lưu giữ dữ liệu. Bởi việc sử dụng nhiều dữ liệu nhạy cảm cũng tiềm ẩn rủi ro lớn. Nghiên cứu của Carlini và cộng sự (2023) chỉ ra rằng các mô hình ngôn ngữ lớn (LLM) có xu hướng "ghi nhớ" và có thể tiết lộ dữ liệu huấn luyện [19]. Bên cạnh đó, nghiên cứu của Hu và cộng sự (2025) cho thấy việc tinh chỉnh mô hình ngôn ngữ theo phương thức liên kết (federated fine-tuning) vẫn tiềm ẩn nguy cơ rò rỉ dữ liệu nhạy cảm từ phía khách hàng, có đến 56,57% thông tin nhạy cảm của các cá nhân dễ dàng bị tấn công [20]. Báo cáo của Trung tâm chính sách thông tin (CIPL) chỉ rõ: "Đối với AI, đặc biệt là ở giai đoạn phát triển và đào tạo, điều cần thiết là một lượng dữ liệu đáng kể, và việc có quá ít dữ liệu có thể cản trở sự phát triển của thuật toán" [21]. Nói cách khác, nếu AI được huấn luyện trên dữ liệu hồ sơ khách hàng thực mà không bảo vệ kỹ, có nguy cơ mô hình sẽ vô tình "tiết lộ" lại các chi tiết riêng tư này trong khi trả lời các truy vấn của luật sư khác. Bên cạnh đó, các nguyên tắc tư pháp truyền thống như bí mật thông tin khách hàng càng gia tăng sức ép kiểm soát. Ví dụ, ABA cảnh báo rằng AI "tạo sinh" (generative AI) có thể tiết lộ thông tin của một khách hàng này cho khách hàng khác qua các câu hỏi không liên quan [22]. Do đó, luật sư phải cẩn trọng và thường ưu tiên chỉ sử dụng AI trên dữ liệu đã được che kín hoặc trong hệ thống an toàn. Nhưng một vấn đề khác lại được đặt ra trong việc huấn luyện AI, đó là: nếu dữ liệu thiếu đa dạng, hoặc không đầy đủ có thể dẫn đến việc các kết quả của AI sẽ bị thiên lệch, thiếu công bằng (về chủng tộc, giới tính,…). Việc này mâu thuẫn ngầm với việc "chỉ dùng dữ liệu tối thiểu cần thiết".

Trong bối cảnh chuyển đổi số diễn ra sâu rộng trên toàn cầu, hàng loạt mô hình AI tiên tiến như ChatGPT, Claude, Gemini, Grok,… đã được phát triển và ứng dụng vào nhiều lĩnh vực khác nhau của đời sống xã hội. Tại Việt Nam, lĩnh vực pháp luật cũng không nằm ngoài xu hướng này khi ngày càng xuất hiện nhiều mô hình ứng dụng AI, ban đầu chỉ là các chatbot pháp lý đơn giản ở giai đoạn sơ khai, được tích hợp vào các nền tảng pháp lý trực tuyến, như nền tảng "Thư viện pháp luật" nhằm hỗ trợ người dùng tra cứu văn bản, đặt câu hỏi thường gặp, hoặc kết nối với luật sư qua khung hội thoại. Thì đến nay một số nền tảng như: LEXcentra, Trợ lý ảo ngành Tòa án, AI Pháp luật của Bộ Tư pháp, nền tảng Thư Viện Pháp Luật và Trợ lý LuatVietnam.vn. đã được phát triển với việc ứng dụng kỹ thuật xử lý ngôn ngữ tự nhiên (NLP), học máy và mô hình LLM nhằm tự động hóa các tác vụ tra cứu, phân tích và giải đáp pháp lý. Qua đó, các nền tảng này đã hỗ trợ hiệu quả hơn cho cá nhân, doanh nghiệp và cơ quan công quyền trong tiếp cận và thực thi pháp luật. Cụ thể, nền tảng LEXcentra là nền tảng legal-AI thương mại cung cấp dịch vụ tra cứu văn bản quy phạm pháp luật, bản án và án lệ dựa trên tìm kiếm ngữ nghĩa, đồng thời tích hợp chức năng hỏi-đáp pháp luật và tóm tắt bản án tự động, với cơ sở dữ liệu lên tới hàng triệu văn bản [23]. Trong khi đó, Trợ lý LuatVietnam.vn là một trong những ứng dụng tiên phong trong khu vực tư nhân, cung cấp khả năng tra cứu văn bản quy phạm pháp luật đến từng điều khoản và giải đáp pháp lý tình huống cụ thể, nhờ vào cơ sở dữ liệu pháp luật lớn, cập nhật liên tục và tích hợp công nghệ AI tạo sinh [24]. Ngoài ra, AI Pháp luật được tích hợp vào Cổng Pháp luật quốc gia, là nền tảng do Bộ Tư pháp phát triển nhằm cung cấp thông tin pháp luật theo hình thức hỏi-đáp ngôn ngữ tự nhiên cho người dân và doanh

nghiệp trên hơn 30 lĩnh vực, hướng đến phổ biến, giáo dục pháp luật qua công nghệ [25]. Trong ngành tư pháp, Trợ lý ảo do hệ thống Tòa án nhân dân triển khai ứng dụng, đóng vai trò như công cụ nội bộ hỗ trợ thẩm phán và thư ký trong việc truy xuất án lệ, ẩn danh hóa bản án và lập lịch xử án; cho thấy tiềm năng rõ nét trong cải cách tư pháp và giảm tải hành chính [26]. Tuy nhiên, các hệ thống này chủ yếu hoạt động theo dạng cây quyết định (decision tree) [27] với dữ liệu được lập trình sẵn, thiếu khả năng học máy sâu (deep learning) [28] theo ngữ cảnh hoặc xử lý ngôn ngữ tự nhiên ở mức cao. Các công cụ hỗ trợ luật sư, thẩm phán truy xuất án lệ, tìm kiếm văn bản pháp luật có tích hợp yếu tố AI vẫn còn ở mức độ hạn chế. Các công cụ này chủ yếu vẫn đóng vai trò hỗ trợ sơ cấp trong các hoạt động pháp lý, phần lớn dừng lại ở mức số hóa cơ sở dữ liệu thay vì phát triển các mô hình phân tích ngữ nghĩa, gợi ý văn bản phù hợp theo tình huống, hay hỗ trợ soạn thảo pháp lý tự động. Như vậy, các mô hình trên một mặt góp phần nâng cao hiệu quả tiếp cận pháp luật, mặt khác đặt ra yêu cầu cấp thiết về khung pháp lý điều chỉnh việc sử dụng AI, đặc biệt liên quan đến bảo vệ dữ liệu cá nhân, trách nhiệm giải trình và tính minh bạch của hệ thống AI trong trả lời pháp lý. Trong tương lai gần, các nền tảng legal-AI này hoàn toàn có thể thể đảm nhận vai trò tư vấn độc lập trong hệ sinh thái dịch vụ pháp lý. Do vậy, việc chuẩn hóa cơ chế vận hành, kiểm định chất lượng đầu ra và kiểm soát rủi ro pháp lý của các nền tảng legal-AI sẽ là yếu tố then chốt để đảm bảo sự cân bằng giữa đổi mới công nghệ và bảo vệ quyền con người trong tư pháp số.

Trong khi đó, hạ tầng dữ liệu pháp lý tại Việt Nam vẫn tồn tại tình trạng phân mảnh và thiếu tính liên thông. Các văn bản quy phạm pháp luật, bản án, án lệ và các tài liệu nghiệp vụ được lưu trữ rải rác ở nhiều cơ quan khác nhau, chưa có một hệ thống tích hợp tập trung, đồng bộ. Bên cạnh đó, việc thiếu chuẩn hóa định dạng dữ liệu (ví dụ: thiếu quy ước thống nhất về cấu trúc văn bản, phân loại lĩnh vực, trạng thái hiệu lực) khiến cho quá trình truy xuất, phân tích và khai thác thông tin gặp nhiều khó khăn, đặc biệt đối với các hệ thống pháp lý ứng dụng AI. Ngoài ra, siêu dữ liệu (metadata), như thông tin về thời điểm áp dụng, phạm vi hiệu lực, đối tượng điều chỉnh, mối quan hệ giữa các văn bản (hướng dẫn, thay thế, sửa đổi…) vẫn chưa được gắn kết đầy đủ và có hệ thống. Tình trạng này không chỉ làm giảm hiệu quả của các công cụ tra cứu và hỗ trợ tư vấn pháp luật, mà còn là rào cản lớn trong việc xây dựng các nền tảng legal-tech thông minh, có khả năng xử lý ngữ nghĩa và cung cấp gợi ý pháp lý theo ngữ cảnh. Việc thiếu một tập hợp văn bản pháp lý chuẩn hóa, có thể đọc được bằng máy sẽ làm khó khăn trong việc huấn luyện AI pháp lý [29]. Sự phát triển của AI đặt ra một nghịch lý đáng chú ý: một mặt, AI cần "dữ liệu lớn" để được đào tạo và vận hành; mặt khác, hạ tầng dữ liệu yếu kém không đáp ứng được. Điều này buộc các chủ thể phát triển AI phải điều chỉnh giải pháp như tạo dữ liệu tổng hợp hoặc đẩy mạnh hợp tác chia sẻ dữ liệu. Tuy nhiên, việc xử lý dữ liệu lớn trong AI có thể xung đột với quyền riêng tư của cá nhân, từ đó tạo ra sự căng thẳng giữa yêu cầu đổi mới công nghệ và vấn đề bảo vệ quyền con người trong môi trường số. Pháp luật Việt Nam quy định cá nhân phải được thông báo về mục đích sử dụng dữ liệu và phải đồng ý nếu dữ liệu nhạy cảm được xử lý [9, Điều 4]. Nếu AI yêu cầu sử dụng các bộ dữ liệu cá nhân rất lớn (ví dụ để phân tích khuynh hướng xét xử hàng loạt vụ án), luật sư và các đương sự phải đảm bảo thông báo và bảo vệ quyền này. Và phương án dung hòa được áp dụng đó là sử dụng dữ liệu đã được ẩn danh hoặc tổng hợp cho mục đích nghiên cứu, trong khi các bản ghi cá nhân chỉ được lưu hành nội bộ và chịu sự quản lý nghiêm ngặt. Việc cân bằng giữa hiệu quả khai thác AI và yêu cầu tuân thủ nguyên tắc giảm thiểu dữ liệu sẽ tiếp tục là một thách thức quan trọng trong thời gian tới.

2.3. Thách thức pháp lý về bảo vệ quyền riêng tư trong dịch vụ tư vấn pháp luật có sử dụng AI

Việc ứng dụng AI trong lĩnh vực tư vấn pháp luật không còn là ý tưởng mang tính lý thuyết, mà đã được nhiều quốc gia trên thế giới đã thiết lập các chuẩn mực pháp lý tương đối hoàn chỉnh, đặc biệt là trong các hệ thống pháp lý theo thông

luật (common law), bởi với khối lượng án lệ và văn bản pháp lý lớn sẽ tạo điều kiện thuận lợi cho công nghệ học máy phát huy hiệu quả, đáng chú ý nhất là EU và Hoa Kỳ,…

Tại EU, quyền riêng tư được quy định tại Điều 8 của Công ước Châu Âu về Nhân quyền (ECHR) [30] và GDPR năm 2016 [31] được xem là khuôn khổ pháp lý toàn diện đầu tiên về quyền riêng tư và dữ liệu cá nhân, thiết lập các quyền rõ ràng cho chủ thể dữ liệu và yêu cầu minh bạch trong thu thập, xử lý, lưu trữ thông tin [32]. Khoản 2 Điều 1 GDPR xác định rõ mục tiêu cốt lõi của văn bản là bảo vệ các quyền và tự do cơ bản của cá nhân, đặc biệt là quyền đối với dữ liệu cá nhân. Các Điều từ 5 đến 9 GDPR tiếp tục cụ thể hóa các nguyên tắc pháp lý nền tảng để ngăn chặn sự can thiệp tùy tiện vào đời sống riêng tư thông qua việc thu thập, xử lý và sử dụng dữ liệu cá nhân.

Đồng thời, EU đang hoàn thiện Đạo luật AI (EU AI Act), nhằm phân loại các hệ thống AI theo 4 mức độ rủi ro: tối thiểu, hạn chế, cao và bị cấm [33]. Theo GDPR, các tổ chức phải thực hiện đánh giá tác động bảo vệ dữ liệu (DPIA) đối với hệ thống có rủi ro cao, bảo đảm quyền truy cập, chỉnh sửa, xóa dữ liệu của cá nhân và thiết lập cơ chế giải trình rõ ràng. Như hệ thống Luminance của Anh [12]. Mặc dù, các nền tảng này đã triển khai nhiều biện pháp bảo mật, tuân thủ pháp lý để bảo vệ dữ liệu và quyền riêng tư của người dùng, nhưng bất kỳ nền tảng công nghệ nào cũng sẽ vẫn tồn tại những nguy cơ tiềm ẩn về mất kiểm soát dữ liệu. Đặc biệt khi các dữ liệu này không rõ ràng về vị trí lưu trữ và nguy cơ bị truy cập trái phép từ các cơ quan nhà nước nơi đặt máy chủ [34]. Đối với vấn đề chuyển dữ liệu quốc tế, sau phán quyết Schrems II, nhiều cơ chế chuyển dữ liệu bị nghi ngờ về tính hợp pháp, đặc biệt khi luật quốc gia nơi nhận dữ liệu không đảm bảo mức độ bảo vệ tương đương với chuẩn mực EU [35]. Đồng thời, việc ẩn danh dữ liệu khi chia sẻ không đảm bảo loại bỏ hoàn toàn khả năng tái nhận dạng, đặc biệt khi dữ liệu được khai thác bởi các bên thứ ba [36].

Tại Hoa Kỳ, mặc dù Hoa Kỳ chưa có đạo luật liên bang tương đương với GDPR, nhiều bang đã ban hành quy định riêng về quyền riêng tư, tiêu biểu là Đạo luật Quyền riêng tư Người tiêu dùng California (CCPA). CCPA yêu cầu tổ chức minh bạch mục đích thu thập dữ liệu và trao cho người tiêu dùng các quyền như: biết thông tin, yêu cầu xóa dữ liệu, hạn chế chia sẻ, không bị phân biệt đối xử, và xác minh yêu cầu thực hiện quyền [37]. Bên cạnh đó, năm 2022, Nhà Trắng công bố Tuyên bố Quyền AI (AI Bill of Rights), một văn bản định hướng không mang tính pháp lý ràng buộc, nhằm khuyến nghị việc thiết kế và triển khai AI tôn trọng quyền con người, bao gồm bảo vệ dữ liệu, công bằng thuật toán, minh bạch và quyền từ chối tương tác với AI [38]. Dù không phải là đạo luật, nhưng tài liệu này được xem như một "khởi đầu cần thiết" cho việc hình thành nền tảng pháp lý toàn diện về quản lý hệ thống tự động và AI tại Hoa Kỳ. Mô hình DoNotPay của Hoa Kỳ [13], với giao diện đơn giản và khả năng hiểu ngôn ngữ tự nhiên (natural language processing), cho phép người dùng không chuyên tiếp cận dịch vụ pháp lý với chi phí thấp, thậm chí miễn phí. Tuy nhiên, để sử dụng, người dùng phải cung cấp nhiều thông tin cá nhân nhạy cảm như: họ tên, địa chỉ, ngày sinh, giấy phạt, hợp đồng, thông tin tài chính và cả tài khoản mạng xã hội. Như vậy, trong khi các hệ thống có chức năng tư vấn pháp lý phải chịu sự điều chỉnh của các quy định bảo mật dữ liệu chuyên ngành và đạo đức nghề luật, DoNotPay không chịu sự điều chỉnh bởi bất kỳ chuẩn mực pháp luật chuyên biệt nào, vì nó không được công nhận là tổ chức hành nghề luật [39]. Điều này dẫn đến lỗ hổng nghiêm trọng về trách nhiệm giải trình và bảo mật, làm gia tăng nguy cơ lạm dụng hoặc rò rỉ dữ liệu, đặc biệt khi nó được chia sẻ với bên thứ ba. Cùng với đó, vào năm 2023, Ủy ban Thương mại Liên bang Hoa Kỳ (FTC) [40] đã xử phạt nền tảng DoNotPay do quảng cáo sai lệch về chức năng và phạm vi dịch vụ, khiến người dùng có thể bị đánh lừa cung cấp thông tin mà không hiểu rõ cách hệ thống hoạt động hoặc ai kiểm soát dữ liệu. Đồng thời, không cung cấp cơ chế khiếu nại rõ ràng, không cho phép người dùng yêu cầu xóa hay chỉnh sửa dữ liệu, cũng như không xác định được chủ thể chịu trách nhiệm khi xảy ra sai sót. Điều này vi phạm nghiêm trọng nguyên tắc minh bạch và giải trình,

làm suy yếu quyền kiểm soát thông tin cá nhân. Dù tuyên bố tuân thủ các quy định bảo mật của Hoa Kỳ, nền tảng này lại yêu cầu cung cấp dữ liệu nhạy cảm thông qua các điều khoản sử dụng phức tạp, thiếu cơ chế "privacy by default" rõ ràng. Với bản chất là một hệ thống AI không được cấp phép hành nghề và thiếu giám sát chuyên môn, DoNotPay tiềm ẩn rủi ro lớn cho quyền riêng tư người dùng và đi ngược lại các nguyên tắc cơ bản của một hệ thống pháp lý tin cậy. Hay mô hình ROSS Intelligence [14], dù hệ thống không thu thập dữ liệu trực tiếp từ cá nhân người dùng, nhưng vẫn sử dụng các dữ liệu pháp lý, trong đó có những thông tin cá nhân, tình tiết vụ việc và các yếu tố pháp lý nhạy cảm để huấn luyện hệ thống AI một cách gián tiếp, tiềm ẩn nguy cơ xâm phạm quyền riêng tư. Đây là điều không thể xem nhẹ, đặc biệt nếu dữ liệu đó không được xử lý ẩn danh hoặc bảo mật đúng cách. Việc bảo vệ quyền riêng tư không thể chỉ dựa vào trách nhiệm đạo đức của luật sư, dù họ có nghĩa vụ giữ bí mật thông tin nghề nghiệp. Trong môi trường số, khi các hệ thống AI do bên thứ ba phát triển và vận hành, nhà phát triển công nghệ cũng phải chịu trách nhiệm pháp lý. Họ cần đảm bảo dữ liệu không bị lưu trữ, chia sẻ hoặc sử dụng sai mục đích, đồng thời xây dựng cơ chế kiểm soát rõ ràng, minh bạch.

Việt Nam đang ở giai đoạn đầu xây dựng khung pháp lý điều chỉnh hoạt động của AI trong các lĩnh vực. Ngày 01/3/2026, Luật Trí tuệ nhân tạo chính thức có hiệu lực với kỳ vọng là luật khung về AI, kiến tạo môi trường pháp lý thuận lợi để thúc đẩy đổi mới sáng tạo, nâng cao năng lực cạnh tranh quốc gia; đồng thời quản lý rủi ro, bảo vệ lợi ích quốc gia, quyền con người và chủ quyền số. Tuy vậy, lĩnh vực tư vấn pháp luật vẫn cần có các quy định cụ thể đối với đánh giá tác động quyền riêng tư hoặc minh bạch thuật toán khi sử dụng AI, do đây là lĩnh vực liên quan trực tiếp đến việc xử lý dữ liệu cá nhân, thông tin pháp lý nhạy cảm và quyền tiếp cận công lý.

Ngoài ra, thời gian qua, Quốc hội khóa XV đã ban hành Luật Công nghiệp công nghệ năm 2025 và Luật Bảo vệ dữ liệu cá nhân năm 2025 (đều có hiệu lực thi hành từ ngày 01/01/2026), bước đầu đã thiết lập một nền tảng pháp lý chuyên biệt, tiến bộ và đồng bộ nhằm điều chỉnh các vấn đề phát sinh trong bối cảnh dữ liệu và công nghệ số ngày càng phát triển mạnh mẽ. Cụ thể, Luật Bảo vệ dữ liệu cá nhân năm 2025 đã nâng cấp các quy định trước đó thành một đạo luật chuyên biệt, xác lập rõ các hành vi xử lý dữ liệu cá nhân, bao gồm thu thập, phân tích, tổng hợp, mã hóa, xóa, hủy và chuyển giao. Đáng chú ý, Luật này đã có các quy định về bảo vệ dữ liệu trong môi trường công nghệ cao (Điều 30); Nghĩa vụ đánh giá tác động xử lý dữ liệu (Điều 21); Chuyển dữ liệu cá nhân xuyên biên giới (Điều 20). Cùng với đó, Luật Công nghiệp công nghệ số năm 2025 đã cung cấp nền tảng pháp lý cho việc phát triển và ứng dụng AI, trong đó định nghĩa hệ thống AI: "là hệ thống dựa trên máy móc được thiết kế để hoạt động với các mức độ tự chủ khác nhau và có khả năng thích ứng sau khi triển khai nhằm đạt được những mục tiêu rõ ràng hoặc ngầm định…" (Khoản 9 Điều 3). Đặc biệt, Điều 41 của luật này đã nêu lên các nguyên tắc trong phát triển, cung cấp, triển khai sử dụng AI, về phục vụ con người; tính minh bạch và có thể giám sát; tuân thủ pháp luật về dữ liệu; và đảm bảo việc nhận diện AI. Có thể thấy rằng, những quy định trong hai đạo luật này không chỉ xác lập rõ các khái niệm, nguyên tắc và nghĩa vụ liên quan đến xử lý dữ liệu cá nhân và phát triển AI, mà còn tiệm cận các chuẩn mực quốc tế về quyền riêng tư, trách nhiệm giải trình, minh bạch và đạo đức công nghệ. Tuy nhiên, chính vì là khuôn khổ pháp lý mới, mang tính định hướng cao, nên vẫn còn không ít thách thức trong việc chuyển hóa các quy định từ luật thành cơ chế thực thi khả thi trong thực tiễn. Các yêu cầu như lập hồ sơ DPIA, bảo đảm khả năng giám sát của con người đối với hệ thống AI, hay kiểm soát hoạt động chuyển dữ liệu cá nhân xuyên biên giới tuy đã được quy định tương đối đầy đủ, nhưng vẫn cần có các hướng dẫn cụ thể về quy trình, tiêu chí kỹ thuật và chế tài thực hiện.

Mặc dù đến nay, vẫn chưa ghi nhận vụ rò rỉ nào trực tiếp trong lĩnh vực tư vấn pháp luật, nhưng thực tế tại Việt Nam cho thấy nguy cơ là rất rõ ràng. Trong năm 2023, Công an TP. Huế đã triệt phá đường dây mua bán gần 56 triệu dữ liệu cá nhân, bao gồm thông tin của hàng triệu

công dân, cán bộ và người lao động trên cả nước [41]. Trong năm 2024, có tới 66,24% người dùng xác nhận rằng thông tin của họ từng bị sử dụng trái phép [42]. Hay như vừa qua Trung tâm Thông tin tín dụng quốc gia (CIC) bị tấn công, xâm nhập nhằm đánh cắp dữ liệu cá nhân [43], cho thấy rằng, các lĩnh vực như tài chính, y tế, giáo dục và thương mại điện tử mặc dù có hệ thống bảo mật cực kỳ nghiêm ngặt, nhưng vẫn phải đối mặt với các sự cố rò rỉ thông tin, đe dọa nghiêm trọng quyền riêng tư và an ninh dữ liệu quốc gia. Còn đối với lĩnh vực tư vấn pháp luật, dù hiện chưa ghi nhận các hành vi tấn công, chiếm đoạt dữ liệu trực tiếp, nhưng nguy cơ tiềm ẩn là điều không thể loại trừ, nhất là khi công nghệ số và AI ngày càng phát triển và được tích hợp vào hoạt động pháp lý mà thiếu sự điều chỉnh kịp thời của pháp luật thì việc thực thi, giám sát và bảo đảm quyền riêng tư của người sử dụng dịch vụ tư vấn pháp luật trực tuyến đang đứng trước nhiều nguy cơ đáng lo ngại.

Trước hết, về tính minh bạch, giải trình và khoảng trống trách nhiệm pháp lý. Nếu như trong hoạt động tư vấn pháp luật truyền thống, luật sư bị ràng buộc chặt chẽ bởi nghĩa vụ bảo mật thông tin khách hàng theo Luật Luật sư năm 2006 (sửa đổi, bổ sung 2012) và các chuẩn mực đạo đức quốc tế, ngay cả khi quan hệ pháp lý đã chấm dứt. Đây là cơ sở pháp lý quan trọng nhằm bảo đảm quyền riêng tư và duy trì lòng tin của khách hàng. Nhưng khi hoạt động tư vấn được thực hiện qua hệ thống AI, các cơ chế này không còn phát huy hiệu lực, như vụ việc của DoNotPay. Thuật toán không phải là chủ thể pháp lý, không chịu trách nhiệm đạo đức hay pháp lý như con người. Điều này đã tạo ra khoảng trống pháp lý đáng kể, dẫn đến nguy cơ dữ liệu cá nhân bị thu thập, xử lý hoặc chia sẻ trái phép mà không có cơ chế kiểm soát hiệu quả.

Thứ hai, thách thức trong thu thập dữ liệu và nguyên tắc tối thiểu hóa. Nhiều nền tảng yêu cầu người dùng cung cấp thông tin cá nhân như họ tên, số điện thoại, địa chỉ email, thậm chí cả nội dung tranh chấp hoặc tình tiết vụ án, nhưng lại không công khai minh bạch về mục đích thu thập, thời gian lưu trữ hay đơn vị xử lý dữ liệu. Việc thu thập dữ liệu quá mức so với nhu cầu thực tế, cộng với thiếu minh bạch trong mục tiêu sử dụng, làm xói mòn nguyên tắc tự quyết thông tin cá nhân, vốn là nội dung cốt lõi của quyền riêng tư. Trong vụ việc DoNotPay [13], hệ thống này đã yêu cầu người dùng cung cấp nhiều thông tin cá nhân nhạy cảm thông qua các điều khoản phức tạp, nhưng lại thiếu cơ chế "privacy by default".

Thứ ba, về phân tích, xử lý dữ liệu và nguy cơ thiên lệch thuật toán. Phần lớn hệ thống thuật toán được sử dụng trong các chatbot pháp lý hiện theo dạng rule-based (lập trình tuyến tính), tức đáp ứng theo kịch bản và cây quyết định đã định nghĩa sẵn [44], nhưng khi xu hướng phát triển AI học máy (machine learning) phát triển mạnh, có thể dẫn tới hiện tượng "thiên lệch thuật toán" (algorithmic bias), đặc biệt nếu dữ liệu đầu vào bị hạn chế hoặc mang định kiến xã hội. Điều này có thể dẫn đến phân biệt đối xử trong việc tư vấn, nhất là với những nhóm dễ bị tổn thương như dân tộc thiểu số, người yếu thế hoặc nhóm tôn giáo...

Thứ tư, thách thức trong việc chia sẻ và lưu trữ dữ liệu với bên thứ ba và xuyên biên giới. Các ứng dụng pháp lý hiện nay cho phép lưu lại lịch sử tư vấn pháp luật mà không cung cấp cho người dùng cơ chế kiểm soát, chỉnh sửa hoặc xóa bỏ dữ liệu. Đáng lo ngại hơn, không ít hệ thống tư vấn pháp luật hiện nay đang sử dụng dịch vụ lưu trữ đám mây từ bên thứ ba (như Google Cloud hoặc AWS) để xử lý và lưu trữ dữ liệu, nhưng không thông báo rõ cho người dùng, điều này tiềm ẩn rủi ro lớn về rò rỉ thông tin khi dữ liệu được chuyển xuyên biên giới, khi dữ liệu rơi vào các khu vực pháp lý không bảo đảm mức độ bảo vệ tương đương. Mặc dù Việt Nam đã có cơ chế đánh giá tác động đối với việc chuyển dữ liệu cá nhân ra nước ngoài tại Nghị định 356/2025/NĐ-CP, và đã được luật hóa trong Luật Bảo vệ dữ liệu cá nhân năm 2025, nhưng cách tiếp cận của Việt Nam vẫn khác biệt so với cơ chế Transfer Impact Assessment (TIA) trong GDPR của châu Âu. Cơ chế TIA nhấn mạnh tính tự chủ và trách nhiệm giải trình của tổ chức dữ liệu, phù hợp với môi trường kinh doanh linh hoạt và xuyên biên giới, nhưng đòi hỏi năng lực pháp lý và kỹ thuật cao [45]. Trong khi đó, mô hình tiền kiểm dựa trên hồ sơ của Việt Nam, tạo

cơ sở cho quản lý dữ liệu hiệu quả hơn trong giai đoạn chuyển đổi số, song vẫn tồn tại khoảng trống về tiêu chuẩn đánh giá, thiếu minh bạch trong thực thi, và dễ dẫn đến gánh nặng thủ tục nếu không có hướng dẫn kỹ thuật chi tiết và hỗ trợ doanh nghiệp tuân thủ. Bên cạnh đó, Việt Nam hiện chưa có hướng dẫn chi tiết về mẫu đánh giá, tiêu chí xác định rủi ro, hay danh mục quốc gia được coi là an toàn, dẫn đến khó khăn trong triển khai thực tế và gia tăng gánh nặng tuân thủ cho doanh nghiệp.

Thứ năm, tính ẩn danh và nguy cơ tái định danh. Ở Việt Nam, Luật Bảo vệ dữ liệu cá nhân năm 2025 quy định rằng dữ liệu đã được khử định danh hoàn toàn, tức là không thể nhận diện cá nhân thì không còn bị điều chỉnh bởi luật. Khác với GDPR, luật Việt Nam không chấp nhận ẩn danh giả (pseudonymization) và nghiêm cấm mọi hành vi tái định danh dữ liệu (re-identification). Quy trình khử định danh phải được lập thành văn bản, kiểm tra định kỳ và đánh giá rủi ro theo các tiêu chuẩn quốc tế (như ISO/IEC 20889 hoặc khung NIST De-Identification) để chứng minh hiệu quả ẩn danh. Ngoài ra, cần giám sát các nguồn dữ liệu phụ trợ (như mã bưu chính, dữ liệu viễn thông,…) để ngăn chặn nguy cơ dữ liệu bị nhận diện lại sau khi đã khử định danh. Nghiên cứu của Sweeney (2002) đã chỉ ra rằng với vài thuộc tính "định danh ngầm" (ví dụ mã bưu chính, ngày sinh, giới tính) trong dữ liệu y tế đã ẩn danh, kẻ tấn công có thể kết hợp với nguồn dữ liệu khác để tái xác định cá nhân [46]. Tương tự, Rubinstein & Hartzog (2016) cũng đã nhận định rằng "tính ẩn danh hoàn hảo… đã thất bại" (Perfect anonymization of data sets that contain personal information has failed) và đề nghị chính sách nên tập trung vào giảm thiểu rủi ro tái định danh hơn là chỉ dựa vào việc dữ liệu có được ẩn danh tuyệt đối hay không [47]. Điều này nhấn mạnh rằng trong thực tế, ngay cả khi dữ liệu đã được xóa tên hoặc mã hóa, kẻ tấn công vẫn có thể tận dụng các phương pháp phân tích tiên tiến và dữ liệu phụ trợ (từ bên thứ ba) để khôi phục lại danh tính. Đặc biệt, với việc dữ liệu pháp lý được chia sẻ hoặc xử lý bởi các dịch vụ bên ngoài (cloud, nền tảng AI, bên thứ ba) sẽ làm tăng nguy cơ phá vỡ ẩn danh. Chẳng hạn, một tập dữ liệu ẩn danh về vụ kiện hoặc khách hàng có thể được kết nối với cơ sở dữ liệu viễn thông, mạng xã hội hay cơ sở công khai khác để truy tìm thông tin cá nhân.

Với việc một lượng lớn dữ liệu cá nhân nhạy cảm (hồ sơ khách hàng, phán quyết…) trong lĩnh vực tư vấn pháp luật được xử lý trong môi trường số, những sự cố rò rỉ dữ liệu từng xảy ra trên thế giới, cũng như ở Việt Nam cho thấy không thể xem nhẹ. Cho dù hệ thống có được thiết kế với tiêu chuẩn kỹ thuật cao đến đâu, thì nguy cơ rò rỉ hoặc bị khai thác trái phép thông tin cá nhân vẫn luôn hiện hữu, đặc biệt khi thiếu vắng cơ chế kiểm soát, giám sát và xử lý kịp thời [48]. Trong hoạt động tư vấn pháp luật, những sự cố như vậy không chỉ gây tổn hại nghiêm trọng đến danh dự và uy tín cá nhân mà còn ảnh hưởng trực tiếp đến quyền lợi pháp lý của người được tư vấn, đặc biệt nếu thông tin là bí mật kinh doanh, hay các thông tin bị khai thác nhằm chống lại họ trong các thủ tục tố tụng hoặc tranh chấp pháp lý sau này.

3. Một số giải pháp nhằm tăng cường bảo vệ quyền riêng tư trong dịch vụ tư vấn pháp luật có ứng dụng trí tuệ nhân tạo tại Việt Nam

Trên nền tảng tiếp cận quyền con người và xuất phát từ những thách thức pháp lý mới do sự phát triển và ứng dụng AI trong lĩnh vực tư vấn pháp luật đặt ra, việc xây dựng và hoàn thiện khung pháp luật cần được định hướng bởi các nguyên tắc nền tảng mang tính hệ chuẩn và phổ quát. Trong đó, theo khuyến nghị bởi các chuẩn mực quốc tế như: Nguyên tắc AI của OECD [49] và Khuyến nghị của UNESCO về Đạo đức của Trí tuệ nhân tạo [50] ba nguyên tắc cốt lõi thường được đề xuất trong thiết kế đạo đức AI gồm: (i) Nguyên tắc minh bạch (transparency) đòi hỏi các hệ thống tư vấn pháp lý sử dụng AI phải công bố rõ ràng quy trình thu thập, xử lý, lưu trữ dữ liệu cá nhân và cảnh báo đầy đủ về giới hạn pháp lý của nội dung tư vấn, giúp người dùng nhận diện bản chất phi nhân sự của hệ thống và từ đó đưa ra quyết định sử dụng một cách có hiểu biết; (ii) Nguyên tắc giải trình (accountability) đảm bảo rằng mọi chủ thể tham

gia phát triển và vận hành hệ thống đều phải chịu trách nhiệm pháp lý rõ ràng trước các hậu quả phát sinh, bao gồm cả trách nhiệm trong trường hợp không có lỗi cố ý, nhằm tránh hiện tượng "khoảng trống trách nhiệm" trong môi trường pháp lý số; (iii) Nguyên tắc bảo vệ quyền riêng tư mặc định (privacy by default) đặt ra yêu cầu thiết kế kỹ thuật hệ thống theo hướng tối thiểu hóa dữ liệu thu thập, tích hợp mặc định các biện pháp bảo vệ như ẩn danh hóa, giới hạn truy cập, và trao cho người dùng quyền tự kiểm soát thông tin của mình. Đây là ba nguyên tắc nền tảng cho một hệ thống AI đáng tin cậy, vừa thúc đẩy đổi mới sáng tạo, vừa đảm bảo không xâm hại đến các quyền cơ bản của con người, đặc biệt là quyền riêng tư, tự chủ, và quyền được bảo vệ khỏi các quyết định tự động thiếu minh bạch trong hoạt động tư vấn pháp luật. Ngoài ra, để đảm bảo quyền con người cần áp dụng thêm (iv) Nguyên tắc lồng ghép nhân quyền trong thiết kế (human rights by design) nhấn mạnh tầm quan trọng của việc thực hiện đánh giá tác động quyền con người (Human Rights Impact Assessment - HRIA) trong toàn bộ vòng đời phát triển và triển khai hệ thống [51], bảo đảm rằng công nghệ không trở thành công cụ xâm phạm mà phải là phương tiện hỗ trợ và củng cố các quyền cơ bản của con người.

Trên cơ sở bốn nguyên tắc định hướng nêu trên, việc xây dựng các giải pháp cụ thể nhằm bảo vệ quyền riêng tư trong môi trường pháp lý số là yêu cầu cấp thiết. Các nguyên tắc này không chỉ đóng vai trò như kim chỉ nam về đạo đức công nghệ, mà còn là nền tảng cấu trúc để thiết kế hệ thống giải pháp đồng bộ, phù hợp với điều kiện phát triển của Việt Nam và tham chiếu có chọn lọc kinh nghiệm quốc tế, nhằm khắc phục, hạn chế các thách thức pháp lý, kỹ thuật đã được phân tích trong Mục 2. Cụ thể:

3.1. Hoàn thiện khung pháp lý, cơ chế giải trình và chuẩn mực đạo đức chuyên ngành

Đây là các giải pháp ưu tiên, tập trung vào việc hoàn thiện khuôn khổ pháp luật; giải quyết khoảng trống trách nhiệm pháp lý và thiếu cơ chế giải trình.

Thứ nhất, cần cụ thể hóa và triển khai đồng bộ khung pháp lý mới. Theo đó, ưu tiên cụ thể hóa và triển khai các quy định của Luật Trí tuệ nhân tạo năm 2025, Luật Bảo vệ dữ liệu cá nhân năm 2025 và Luật Công nghiệp công nghệ số năm 2025 trong lĩnh vực tư vấn pháp luật có ứng dụng AI. Việc Quốc hội thông qua ba đạo luật này đã đánh dấu một bước tiến quan trọng trong việc thiết lập nền tảng pháp lý cho bảo vệ quyền riêng tư và điều tiết công nghệ mới nổi tại Việt Nam. Từ nay đến thời điểm luật có hiệu lực, việc sớm ban hành các văn bản hướng dẫn thi hành, đồng thời xây dựng năng lực thể chế và chuyên môn cho các chủ thể liên quan, đặc biệt là các đơn vị cung cấp dịch vụ pháp lý ứng dụng AI sẽ đóng vai trò then chốt.

Thứ hai, làm rõ trách nhiệm pháp lý và giải trình của hệ thống AI. Cần làm rõ trách nhiệm pháp lý của các chủ thể tham gia phát triển và vận hành hệ thống AI, đặc biệt trong các tình huống xảy ra thiệt hại hoặc rò rỉ dữ liệu nhưng chưa xác định được chủ thể chịu trách nhiệm (khoảng trống trách nhiệm). Việc này góp phần bảo đảm tính minh bạch, giải trình và bảo vệ quyền riêng tư một cách thực chất, phù hợp với yêu cầu của kỷ nguyên số.

Thứ ba, cần xây dựng bộ Quy tắc đạo đức ứng xử với công nghệ trong hành nghề luật sư. Bộ Quy tắc này sẽ góp phần bổ sung và cập nhật các quy tắc đạo đức nghề nghiệp truyền thống. Bộ quy tắc này nên quy định các chuẩn mực đạo đức chuyên biệt đối với việc ứng dụng AI trong hoạt động tư vấn pháp lý, bao gồm nghĩa vụ minh bạch về việc sử dụng AI, trách nhiệm giải trình đối với kết quả tư vấn, cũng như các biện pháp phòng ngừa rủi ro liên quan đến khai thác dữ liệu cá nhân trái phép hoặc phát sinh thiên lệch trong quá trình xử lý và cung cấp thông tin pháp lý cho khách hàng. Việc thiết lập bộ quy tắc như vậy không chỉ góp phần định hướng hành vi nghề nghiệp phù hợp với bối cảnh công nghệ mới, mà còn là cơ sở để nâng cao niềm tin của xã hội đối với các dịch vụ pháp lý ứng dụng AI, bảo đảm quyền lợi hợp pháp của người sử dụng dịch vụ trong môi trường số.

3.2. Áp dụng các biện pháp kỹ thuật và công cụ

quản lý rủi ro

Trước hết, cần học hỏi và áp dụng theo lộ trình công cụ HRIA/DPIA. Việc thiết lập yêu cầu HRIA và DPIA được xem là biện pháp tiến bộ nhằm phòng ngừa sớm các rủi ro xâm phạm quyền con người trong quá trình thiết kế và vận hành hệ thống AI, đặc biệt trong các lĩnh vực nhạy cảm như tư vấn pháp luật. Tuy nhiên, trong bối cảnh pháp lý và thể chế hiện nay của Việt Nam, việc áp dụng ngay các tiêu chuẩn HRIA và DPIA theo mô hình các nước phát triển, đặc biệt là EU với GDPR vẫn cần được cân nhắc kỹ lưỡng do còn hạn chế về khung pháp lý, năng lực thực thi và nhận thức xã hội. Do đó, việc học hỏi và áp dụng các nguyên tắc của HRIA và DPIA cần phù hợp với điều kiện thực tiễn và được triển khai theo lộ trình cụ thể. Theo đó, có thể ưu tiên áp dụng trước đối với các hệ thống AI có mức độ rủi ro cao, thông qua các chương trình thí điểm (sandbox) có sự hướng dẫn chuyên môn của cơ quan quản lý nhà nước. Đồng thời, cần ban hành các văn bản hướng dẫn kỹ thuật về đánh giá tác động quyền và dữ liệu, nhằm hỗ trợ các tổ chức, doanh nghiệp thực hiện đúng quy trình, nâng cao năng lực đánh giá và tăng cường tính khả thi trong thực tiễn áp dụng. Việc tiếp cận theo hướng từng bước, có trọng tâm và phù hợp với điều kiện nội tại sẽ tạo nền tảng pháp lý vững chắc, đồng thời đảm bảo sự hội nhập hiệu quả với các chuẩn mực quốc tế về bảo vệ quyền con người trong kỷ nguyên số.

Hai là, cụ thể hóa các nguyên tắc kỹ thuật và kiểm soát dữ liệu. Cần áp dụng nguyên tắc "Privacy by Default", tức là các nền tảng AI dùng trong tư vấn pháp luật phải tự động bảo vệ quyền riêng tư người dùng ngay từ khi khởi động, không cần cài đặt thêm. Nguyên tắc này là một trong ba nguyên tắc cốt lõi được đề xuất trong thiết kế đạo đức AI. Cụ thể, hệ thống phải được thiết kế để thu thập ít dữ liệu nhất có thể, ẩn danh hóa thông tin nhạy cảm, và hạn chế truy cập dữ liệu cá nhân chỉ trong trường hợp thật sự cần thiết. Mô hình Luminance (Anh) là ví dụ điển hình cho việc hệ thống được thiết kế theo nguyên tắc này, mặc định hạn chế thu thập dữ liệu cá nhân. Hay Demir (2025) đã đề xuất khung "LegalGuardian", theo đó mô hình nhận dạng thực thể (NER) và một LLM chạy cục bộ để tự động phát hiện và ẩn PII trong câu hỏi của luật sư (như tên đương sự, chi tiết vụ việc) trước khi gửi tới AI lớn trên đám mây. Khi LLM trả lời, dữ liệu được giải mã trở lại dạng gốc [52]. Cách làm này giúp bảo toàn bảo mật khách hàng: thông tin nhạy cảm không bao giờ rời hệ thống của luật sư, và AI vẫn có đủ ngữ cảnh để đưa ra gợi ý pháp lý chính xác.

Bên cạnh đó, cần bổ sung công cụ cho phép người dùng tự kiểm soát dữ liệu cá nhân trong toàn bộ quá trình tư vấn pháp lý, bao gồm các quyền như: xem, chỉnh sửa, xóa hoặc yêu cầu chuyển dữ liệu và cả sau khi kết thúc dịch vụ. Hiện nay, nhiều ứng dụng pháp lý tại Việt Nam chưa có cơ chế này. Việc thực hiện hai nội dung này sẽ giúp giảm rủi ro lộ lọt thông tin, tăng tính minh bạch và bảo vệ tốt hơn quyền riêng tư của người dân trong môi trường pháp lý số.

Ba là, ban hành hướng dẫn kỹ thuật về kiểm soát dữ liệu xuyên biên giới. Nhất là trong bối cảnh có nhiều nền tảng AI ra đời, và dữ liệu được lưu trữ trên các dịch vụ đám mây của bên thứ ba (như AWS, Google Cloud), tiềm ẩn nguy cơ cao về rò rỉ hoặc lạm dụng thông tin. Hướng dẫn này cần quy định cụ thể các yêu cầu kỹ thuật và quy trình đánh giá tác động của việc chuyển dữ liệu xuyên biên giới, có thể lấy mô hình đánh giá theo GDPR (TIA) làm tham chiếu. Mục tiêu là đảm bảo rằng quốc gia hoặc tổ chức nhận dữ liệu phải có hệ thống pháp luật bảo vệ dữ liệu cá nhân ở mức tương đương hoặc không thấp hơn so với chuẩn mực của Việt Nam; đồng thời yêu cầu tổ chức gửi dữ liệu phải thực hiện các biện pháp kỹ thuật, pháp lý bổ sung nếu phát hiện rủi ro. Đây là bước đi cần thiết để hạn chế việc dữ liệu pháp lý nhạy cảm của công dân Việt Nam bị khai thác ngoài tầm kiểm soát của pháp luật trong nước và nâng cao năng lực quản trị rủi ro dữ liệu trong môi trường AI.

3.3. Tăng cường giám sát, quản lý và hợp tác quốc tế

Các giải pháp này tăng cường vai trò của các cơ quan quản lý nhà nước và cơ chế giám sát đối

với các tổ chức cung cấp dịch vụ pháp lý, đặc biệt là các mô hình phi truyền thống.

Thứ nhất, cần phân quyền giám sát và mở rộng phạm vi quản lý. Trong đó, cần tăng cường cơ chế quản lý nhà nước và giám sát xã hội đối với các hệ thống tư vấn pháp lý có ứng dụng AI. Phân quyền rõ ràng cho các cơ quan quản lý chuyên ngành (Bộ Khoa học và Công nghệ, Bộ Tư pháp, Sở Tư pháp các tỉnh và Đoàn Luật sư Việt Nam) trong việc cấp phép, giám sát và xử lý vi phạm liên quan đến bảo mật dữ liệu và quyền riêng tư. Đây là bước đi quan trọng để bảo đảm tính kiểm soát, minh bạch và trách nhiệm trong hoạt động tư vấn pháp luật. Cơ chế này không chỉ giới hạn trong phạm vi các chủ thể truyền thống như luật sư hay trợ giúp viên pháp lý thuộc Trung tâm trợ giúp pháp lý Nhà nước, mà phải mở rộng sang các tổ chức, doanh nghiệp tư nhân cung cấp dịch vụ pháp lý thông qua nền tảng công nghệ (legal tech), nhất là các hệ thống có sử dụng AI.

Thứ hai, thiết lập cơ chế tiếp nhận và xử lý khiếu nại rõ ràng. Cần thiết lập cơ chế tiếp nhận, xác minh và xử lý khiếu nại của người dân khi dữ liệu và quyền riêng tư bị xâm phạm trong quá trình sử dụng các nền tảng tư vấn pháp luật. Ví dụ: người dùng có thể gửi khiếu nại qua ứng dụng/web/chatbot/điện thoại, nhận mã theo dõi tức thì, và được cam kết thời gian xử lý rõ ràng minh bạch (ví dụ: xác nhận trong 24 giờ, xác minh trong 7 ngày, xử lý trong 30 ngày). Quy trình gồm 4 bước gọn: tiếp nhận → xác minh → khắc phục/khôi phục quyền → phản hồi kết quả; mọi thao tác trong quá trình xử lý dữ liệu đều được ghi lại đầy đủ và mã hóa. Đồng thời, cơ chế khiếu nại cần có một bộ phận độc lập đứng ra tiếp nhận và giám sát quá trình xử lý. Nếu phát hiện có sai sót, cần có biện pháp khắc phục rõ ràng như: sửa hoặc xóa dữ liệu sai, ngừng sử dụng dữ liệu đó, thông báo cho bên thứ ba nếu dữ liệu đã chia sẻ, hoặc bồi thường cho người bị ảnh hưởng theo quy định của pháp luật.

Cách tiếp cận này đặc biệt phù hợp với các mô hình legal tech hiện đại, không chỉ giúp nâng cao trách nhiệm giải trình của đơn vị cung cấp dịch vụ mà còn bảo vệ hiệu quả quyền lợi hợp pháp và củng cố niềm tin của người dùng. Đây là một bước đi tất yếu nhằm đảm bảo tính công bằng trong thực thi pháp luật trong bối cảnh hệ sinh thái dịch vụ pháp lý đang chuyển dịch mạnh mẽ sang hình thức số hóa. Đồng thời, giải pháp này góp phần lấp đầy khoảng trống quản lý hiện hữu, trước sự phát triển nhanh chóng của các nền tảng pháp lý phi truyền thống, vốn tiềm ẩn không ít rủi ro xâm phạm quyền riêng tư nếu thiếu cơ chế kiểm soát chặt chẽ và minh bạch.

Thứ ba, đẩy mạnh hợp tác quốc tế và học hỏi các chuẩn mực quản trị AI. Việt Nam cần đẩy mạnh hợp tác quốc tế và học hỏi có chọn lọc các chuẩn mực quốc tế về quyền riêng tư và quản trị AI. Trong xu thế toàn cầu hóa, nơi dữ liệu cá nhân có thể được chuyển giao, lưu trữ và xử lý xuyên biên giới, việc tham gia các sáng kiến khu vực như Hội nghị Bộ trưởng Kỹ thuật số ASEAN sẽ tạo điều kiện thuận lợi để Việt Nam tiếp cận các chuẩn kỹ thuật và pháp lý chung, hướng tới bảo đảm quyền riêng tư trong môi trường số. Đồng thời, cần nghiên cứu tiếp thu có chọn lọc các chuẩn mực quốc tế như GDPR của EU, AI Bill of Rights của Hoa Kỳ, và OECD AI Principles, nhằm hình thành một khung pháp luật hiện đại, hài hòa với thông lệ quốc tế nhưng vẫn đảm bảo tính phù hợp với điều kiện phát triển về kinh tế, xã hội và pháp lý của Việt Nam.

Trong lĩnh vực tư vấn pháp luật, việc đẩy mạnh hợp tác quốc tế và pháp điển hóa các chuẩn mực quản trị AI cần tập trung nghiên cứu bốn trụ cột chính, nhằm đảm bảo sự phát triển công nghệ đi đôi với bảo vệ quyền con người và chuẩn mực nghề nghiệp, đó là: (i) Bộ quy tắc đạo đức công nghệ trong hành nghề luật; (ii) cơ chế đánh giá tác động xử lý dữ liệu (DPIA) và kiểm soát rủi ro pháp lý trước khi triển khai công nghệ; (iii) bảo đảm quyền riêng tư của khách hàng; và (iv) nâng cao năng lực số cho luật sư. Đây là nền tảng để Việt Nam xây dựng một môi trường pháp lý số an toàn, hiện đại và nhân bản, trong đó quyền riêng tư được bảo vệ như một nguyên tắc nền tảng trong mọi hoạt động ứng dụng AI trong dịch vụ pháp lý.

3.4. Phát triển năng lực và nâng cao nhận thức

Để bảo đảm hiệu quả thực thi pháp luật trong

lĩnh vực mới mẻ này, cần đặc biệt chú trọng phát triển năng lực chuyên môn và nâng cao nhận thức xã hội. Hiện nay, nhận thức về quyền kiểm soát thông tin cá nhân, cũng như các rủi ro tiềm ẩn liên quan đến việc sử dụng dữ liệu chưa được đặt đúng tầm, dẫn đến sự thờ ơ hoặc thiếu cảnh giác của người cung cấp và người sử dụng dịch vụ trước những nguy cơ xâm phạm quyền riêng tư trong môi trường pháp lý số.

Đầu tiên, cần phát triển năng lực chuyên môn và đào tạo chuyên sâu về công nghệ nhằm nâng cao năng lực số cho luật sư, cán bộ tư pháp và chuyên gia công nghệ là yêu cầu cấp thiết trong bối cảnh AI ngày càng được ứng dụng trong dịch vụ pháp lý. Cần tổ chức các chương trình đào tạo chuyên sâu, tập trung vào các nội dung chính, như: i) quản trị dữ liệu cá nhân theo đúng chuẩn mực pháp lý; ii) đạo đức số, đặc biệt là kỹ năng nhận diện và xử lý rủi ro thiên lệch thuật toán; và iii) kỹ năng làm việc với hệ thống AI, bao gồm khả năng kiểm định kết quả đầu ra, phát hiện sai lệch và đảm bảo tính công bằng,… Đi cùng với đó là đào tạo năng lực đánh giá rủi ro pháp lý và công nghệ cho các tổ chức hành nghề luật, nhằm bảo đảm các quy trình HRIA/DPIA không chỉ được thực hiện theo hình thức mà thực sự có giá trị phòng ngừa, kiểm soát và tăng cường trách nhiệm giải trình. Mục tiêu là duy trì vai trò trung tâm của con người trong quá trình tư vấn pháp luật, đảm bảo rằng AI chỉ đóng vai trò hỗ trợ, không thay thế tư duy pháp lý. Đây là bước quan trọng để xây dựng một hệ sinh thái pháp lý số vừa hiệu quả, vừa nhân văn.

Đồng thời, cần nâng cao nhận thức xã hội về quyền kiểm soát dữ liệu. Mà trọng tâm là triển khai các chiến dịch truyền thông và giáo dục cộng đồng một cách đồng bộ và thiết thực. Trước hết, cần xây dựng các chương trình truyền thông đại chúng trên truyền hình, mạng xã hội, và các nền tảng pháp lý trực tuyến nhằm phổ biến kiến thức về quyền kiểm soát thông tin cá nhân, các dấu hiệu nhận biết hành vi xâm phạm dữ liệu, và cách thức khiếu nại, yêu cầu bồi thường khi quyền riêng tư bị xâm phạm. Song song, cần đưa nội dung giáo dục về bảo vệ dữ liệu cá nhân vào chương trình đào tạo pháp luật cơ bản tại trường học và trung tâm phổ biến pháp luật, hướng tới hình thành "văn hóa dữ liệu" trong cộng đồng. Ngoài ra, có thể triển khai các ứng dụng hỗ trợ người dùng kiểm soát dữ liệu, như cổng thông tin điện tử cho phép tra cứu, chỉnh sửa hoặc rút lại thông tin cá nhân đã cung cấp cho các nền tảng pháp lý. Việc nâng cao nhận thức không chỉ giúp người dân thận trọng và chủ động hơn khi sử dụng dịch vụ số, mà còn tạo ra áp lực xã hội yêu cầu các tổ chức cung cấp dịch vụ phải minh bạch, tuân thủ các nguyên tắc bảo vệ dữ liệu và chịu trách nhiệm rõ ràng khi có vi phạm xảy ra. Đây là nền tảng quan trọng để xây dựng môi trường pháp lý số an toàn, lấy quyền con người làm trọng tâm.

Việc tiếp cận theo hướng từng bước, có trọng tâm và phù hợp với điều kiện nội tại, đặc biệt trong lĩnh vực tư vấn pháp luật, sẽ vừa tạo nền tảng pháp lý vững chắc, vừa tăng khả năng hội nhập với các chuẩn mực quốc tế về bảo vệ quyền con người và dữ liệu cá nhân trong kỷ nguyên số.

4. Kết luận

Sự phát triển mạnh mẽ của AI trong lĩnh vực tư vấn pháp luật là một xu hướng tất yếu, phản ánh quá trình chuyển đổi số sâu rộng đang diễn ra trên toàn cầu. AI không chỉ mở rộng khả năng tiếp cận dịch vụ pháp lý, giảm chi phí và nâng cao hiệu quả xử lý, mà còn đang từng bước thay đổi cấu trúc và phương thức vận hành của hoạt động hành nghề luật. Tuy nhiên, bên cạnh những lợi ích to lớn, việc tích hợp AI vào dịch vụ pháp lý cũng đặt ra những thách thức nghiêm trọng đối với quyền con người, đặc biệt là quyền riêng tư, một trong những quyền nền tảng nhất trong xã hội hiện đại. Bài viết đã chỉ ra rằng, quyền riêng tư không chỉ là một quyền pháp lý trừu tượng, mà còn là biểu hiện cụ thể của nhân phẩm và quyền kiểm soát thông tin cá nhân trong môi trường kỹ thuật số. Một khi AI ngày càng can thiệp sâu vào quá trình thu thập, xử lý và lưu trữ dữ liệu pháp lý, việc bảo vệ quyền riêng tư không thể chỉ dừng ở tuyên bố nguyên tắc, mà cần được cụ thể hóa bằng cơ chế pháp lý rõ ràng và thực thi hiệu quả từ minh bạch thuật toán, cơ chế giải trình, đến đánh giá tác động quyền con người và

dữ liệu cá nhân trước khi triển khai công nghệ.

Với định hướng xây dựng và hoàn thiện Nhà nước pháp quyền xã hội chủ nghĩa Việt Nam trong thời gian tới, việc bảo vệ quyền riêng tư phải được xem là một biểu hiện cụ thể của nguyên tắc thượng tôn pháp luật và cam kết bảo đảm, tôn trọng, bảo vệ quyền con người. Mọi tiến bộ công nghệ, bao gồm việc ứng dụng AI trong tư vấn pháp luật, đều phải phục vụ con người, vì con người và do con người quản lý. Việc xây dựng Luật về trí tuệ nhân tạo, ban hành bộ quy tắc đạo đức nghề nghiệp trong môi trường số, cùng với việc nội luật hóa có chọn lọc các chuẩn mực quốc tế như HRIA và DPIA sẽ góp phần hoàn thiện khuôn khổ pháp luật, bảo vệ các quyền cơ bản của cá nhân trong môi trường số, phù hợp với định hướng phát triển nhà nước pháp quyền và hội nhập quốc tế sâu rộng của Việt Nam. Mọi giải pháp công nghệ trong lĩnh vực tư vấn pháp luật chỉ có giá trị khi lấy con người, nhân phẩm và quyền lợi làm trung tâm và mọi sự tiến bộ kỹ thuật chỉ thực sự có ý nghĩa khi phục vụ việc bảo vệ và thúc đẩy các quyền cơ bản của con người trong một xã hội dân chủ, công bằng và bền vững.

Tài liệu tham khảo

[1] R. Gavison, Privacy and the limits of law, The Yale Law Journal, 89(3), 421–471, https://doi.org/10.2307/795891

[2] S. D. Warren, L. D. Brandeis, The Right to Privacy, Harvard Law Review, 4(5), 193–220, p. 193. https://doi.org/10.2307/1321160

[3] United Nations General Assembly, International Covenant on Civil and Political Rights, United Nations, Treaty Series No. 999, p. 171, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights, (accessed on: May 20th, 2025).

[4] T. Q. A. Nguyen, C. G. Vu, M. H. Ngo, K. T. La, The right to privacy [Quyền về sự riêng tư], National Political Publishing House-Truth [Nxb. Chính trị quốc gia Sự thật], Ha Noi, p. 13.

[5] National Assembly of Vietnam, Constitution of the Socialist Republic of Vietnam [Hiến pháp nước Cộng hòa Xã hội Chủ nghĩa Việt Nam], Hanoi, Vietnam.

[6] T. T. H. Hanh, Improving the legal framework for personal data protection in contemporary Vietnam [Hoàn thiện pháp luật về bảo vệ thông tin cá nhân ở Việt Nam hiện nay], Doctoral dissertation, Ho Chi Minh National Academy of Politics [Học viện Chính trị quốc gia Hồ Chí Minh], Hanoi, Vietnam, p. 34.

[7] European Union, General Data Protection Regulation, Official Journal of the European Union, L119, 1–88, https://eur-lex.europa.eu/eli/reg/2016/679/oj, (accessed on: May 20th, 2025).

[8] Government of Vietnam, Decree No. 13/2023/ND-CP dated 17 April 2023 on Personal Data Protection [Bảo vệ dữ liệu cá nhân], Hanoi.

[9] National Assembly of Vietnam, Law on Personal Data Protection [Luật Bảo vệ dữ liệu cá nhân] No. 91/2025/QH15, Hanoi.

[10] N. Babazadeh, Legal ethics and cybersecurity: Managing client confidentiality in the digital age, Journal of Law & Cyber Warfare, 7(1), 85–116, p. 88, https://www.jstor.org/stable/26777964

[11] E. Wald, Legal ethics' next frontier: Lawyers and cybersecurity, Chapman Law Review, 19, 501–528, U. Denver Legal Studies Research Paper No. 16-04, p. 501, https://ssrn.com/abstract=2724017.

[12] Luminance, Luminance Legal - Privacy Policy, https://www.luminance.com/legal.html, (accessed on: May 20th, 2025).

[13] L. Dye, Chatbot Law Site DoNotPay Settles With FTC, Above the Law, https://abovethelaw.com/2024/09/chatbot-law-site-donotpay-settles-with-ftc/, (accessed on: May 20th, 2025).

[14] R. Ambrogi, ROSS artificial intelligence outperforms Westlaw and LexisNexis, study finds, LawNext, https://www.lawnext.com/2017/01/ross-artificial-intelligence-outperforms-westlaw-lexisnexis-study-finds.html, (accessed on: May 20th, 2025).

[15] D. Szostek, M. Załucki (eds.), LegalTech: Information technology tools in the administration of justice, Nomos Verlagsgesellschaft, p. 22, https://doi.org/10.5771/9783748922834.

[16] M. Andrews, P. Bromiley, E. Chow, T. Gibson, A machine learning framework for legal document recommendations, Journal of Computer Science and Artificial Intelligence, 1(1), 17–23, pp. 18–19, https://doi.org/10.54097/0my1t737.

[17] A. Feenberg, Questioning Technology, Routledge, London and New York, p. 2.

[18] A. Mantelero, Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection, Computer Law & Security Review, 32(2), 238–255, p. 243, https://doi.org/10.1016/j.clsr.2016.01.014.

[19] N. Carlini, D. Ippolito, M. Jagielski, K. Lee, F. Tramèr, C. Zhang, Quantifying memorization across neural language models, Proceedings of the Eleventh International Conference on Learning Representations (ICLR), Kigali, Rwanda, May 1–5, 2023, p. 1, https://openreview.net/forum?id=TatRHT_1cK.

[20] Y. Hu, Z. Zhang, J. Zhang, L. Qu, Z. Xu, Simple yet effective: Extracting private data across clients in federated fine-tuning of large language models, arXiv preprint [cs.CL], p. 2, http://arxiv.org/abs/2506.06060.

[21] Centre for Information Policy Leadership (CIPL), Artificial Intelligence and Data Protection: Hard Issues and Practical Solutions, Second Report, p. 18, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_second_report_-_artificial_intelligence_and_data_protection_-_hard_issues_and_practical_solutions__27_february_2020_.pdf, (accessed on: May 20th, 2025).

[22] M. M. Demir, H. T. Otal, M. A. Canbaz, LegalGuardian: A privacy-preserving framework for secure integration of large language models in legal practice, arXiv preprint [cs.CL], p. 2, http://arxiv.org/abs/2501.10915.

[23] LEXcentra, Lexcentra.ai, https://lexcentra.ai/home, (accessed on: May 20th, 2025).

[24] LuatVietnam, AI Luật, https://ailuat.luatvietnam.vn/, (accessed on: May 20th, 2025).

[25] Cổng pháp luật quốc gia, AI pháp luật, https://ai.phapluat.gov.vn/, (accessed on: May 20th, 2025).

[26] N. Diệp, Tuyển bài trợ lý ảo AI: Bài 3 – Giải mã trợ lý ảo ngành Tòa án, Vjst.vn, https://vjst.vn/tuyen-bai-tro-ly-ao-ai-bai-3-giai-ma-tro-ly-ao-nganh-toa-an-66219.html, (accessed on: May 20th, 2025).

[27] K. D. Ashley, Artificial Intelligence and Legal Analytics, Cambridge University Press, p. 110.

[28] C. Janiesch, P. Zschech, K. Heinrich, Machine learning and deep learning, Electronic Markets, 31(3), 685–695, p. 687, https://doi.org/10.1007/s12525-021-00475-2, (accessed on: March 23rd, 2025).

[29] H. Lâm, Ứng dụng trí tuệ nhân tạo trong hệ thống pháp luật Việt Nam: Cơ hội, thách thức và định hướng phát triển, Tạp chí Tòa án Nhân dân điện tử, https://tapchitoaan.vn/ung-dung-tri-tue-nhan-tao-trong-he-thong-phap-luat-viet-nam-co-hoi-thach-thuc-va-dinh-huong-phat-trien13897.html, (accessed on: May 20th, 2025).

[30] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended), Rome, https://www.echr.coe.int/documents/convention_eng.pdf, (accessed on: May 20th, 2025).

[31] P. Voigt, A. Von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide, Springer International Publishing, p. 63.

[32] M. Kop, EU Artificial Intelligence Act: The European Approach to AI, Stanford-Vienna TTLF Working Paper, No. 2/2021, pp. 3–4, https://ssrn.com/abstract=3930959.

[33] P. M. Schwartz, Legal access to the global cloud, Columbia Law Review, 118, 1681, https://doi.org/10.2139/ssrn.3008392.

[34] M. Fenwick, P. Jurcys, M. C. Compagnucci, The Future of International Data Transfers: Managing New Legal Risk with a 'User-Held' Data Model, SSRN Working Paper, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4010356.

[35] C. C. Porter, De-identified data and third party data mining: The risk of re-identification of personal information, Shidler Journal of Law, Commerce & Technology, 5(1), 3, https://digitalcommons.law.uw.edu/wjlta/vol5/iss1/3.

[36] E. Illman, P. Temple, California Consumer Privacy Act: What Companies Need to Know, The Business Lawyer, 75(1), 1637–1646, pp. 1641–1644, https://www.jstor.org/stable/27171063.

[37] E. Park, The AI Bill of Rights: A Step in the Right Direction, Orange County Lawyer, 65(2), 2528, pp. 25–26, https://ssrn.com/abstract=4351423.

[38] K. McDonough, 'World's first robot lawyer' hit with lawsuit for practising without a licence, Legal Services Journal, https://lsj.com.au/articles/worlds-first-robot-lawyer-hit-with-lawsuit-for-practising-without-a-license/, (accessed on: May 20th, 2025).

[39] Federal Trade Commission, DoNotPay, Inc, https://www.ftc.gov/legal-library/browse/cases-proceedings/donotpay, (accessed on: May 20th, 2025).

[40] D. Bao, Strict legal sanctions needed to prevent leakage and trading of personal data and state secrets [Cần chế tài nghiêm khắc để ngăn chặn lộ, lọt, rao bán dữ liệu, bí mật nhà nước], Vietnam Law Newspaper [Báo Pháp luật Việt Nam], https://phapluatmedia.vn/can-che-tai-nghiem-khac-de-ngan-chan-lo-lot-rao-ban-du-lieu-bi-mat-nha-nuoc-27290.html, (accessed on: May 20th, 2025).

[41] D. Anh, More than 66% of Internet users' personal data were misused in 2024 [Dữ liệu cá nhân của hơn 66% người dùng Internet bị sử dụng trái phép trong năm 2024], Vietnamese Lawyer e-Journal [Tạp chí điện tử Luật sư Việt Nam], https://lsvn.vn/du-lieu-ca-nhan-cua-hon-66-nguoi-dung-internet-bi-su-dung-trai-phep-trong-nam-2024-a151492.html, (accessed on: May 20th, 2025).

[42] Báo Điện tử Chính phủ, CIC bị hacker tấn công, VNCERT khuyến cáo người dân nâng cao cảnh giác, https://baochinhphu.vn/cic-bi-hacker-tan-cong-vncert-khuyen-cao-nguoi-dan-nang-cao-canh-giac-102250911201710342.htm, (accessed on: May 20th, 2025).

[43] M. Queudot, É. Charton, M.-J. Meurs, Improving access to justice with legal chatbots, Stats, 3(3), 356–375, pp. 363–364, https://doi.org/10.3390/stats3030023.

[44] M. Corrales Compagnucci, M. Fenwick, M. Aboy, T. Minssen, Supplementary measures and appropriate safeguards for international transfers of health data after Schrems II, Perspectives in Law, Business and Innovation, 151–172, Springer Nature Singapore, 2024, https://doi.org/10.1007/978-981-99-6540-3_9.

[45] L. Sweeney, K-Anonymity: A model for protecting privacy, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10, 557–570, p. 2, https://doi.org/10.1142/S0218488502001648.

[46] I. Rubinstein, W. Hartzog, Anonymization and risk, Washington Law Review, 91, 703–760, NYU School of Law, Public Law Research Paper No. 15-36, p. 703, https://ssrn.com/abstract=2646185.

[47] D. Thien, Personal data and corporate documents of Vietnamese entities widely traded online [Thông tin cá nhân, tài liệu doanh nghiệp Việt bị rao bán rộng rãi trên mạng], Tuoi Tre Online, https://tuoitre.vn/thong-tin-ca-nhan-tai-lieu-doanh-nghiep-viet-bi-rao-ban-rong-rai-tren-mang-20250401211304 04.htm, (accessed on: May 20th, 2025).

[48] OECD, OECD principles on artificial intelligence, OECD.AI, https://oecd.ai/en/ai-principles, (accessed on: May 20th, 2025).

[49] UNESCO, Recommendation on the ethics of artificial intelligence, United Nations Educational, Scientific and Cultural Organization, https://unesdoc.unesco.org/ark:/48223/pf0000381137, (accessed on: May 20th, 2025).

[50] D. Kemp, F. Vanclay, Human rights and impact assessment: Clarifying the connections in practice, Impact Assessment and Project Appraisal, 31(2), 86–96, p. 90, https://doi.org/10.1080/14615517.2013.782978.