

KHUNG PHÁP LÝ VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN TRONG GIAO DỊCH TÀI SẢN SỐ TẠI VIỆT NAM - THỰC TRẠNG VÀ GIẢI PHÁP

NGUYỄN TRÍ CƯỜNG
Trưởng Đại học Kinh tế - Luật,
Đại học Quốc gia TP. Hồ Chí Minh

Nhận bài ngày 13/7/2026. Sửa chữa xong 10/8/2026. Duyệt đăng 14/8/2026.

Abstract

The recognition of digital assets under the 2025 Law on Digital Technology Industry lays the legal foundation for the development of a regulated digital asset market in Vietnam. However, digital asset transactions are commonly conducted through blockchain-based infrastructure, where transaction data are distributed, difficult to modify, and virtually impossible to erase once validated. In the context of Vietnam's increasing use of electronic identification, customer authentication, anti-money laundering mechanisms, and regulatory oversight of digital asset service providers, tensions have emerged between personal data protection requirements and the technological characteristics of digital asset transactions. This article examines the principal legal conflicts arising in this context and proposes directions for legal reform, including enhanced governance of off-chain data, clearer responsibilities for digital asset service providers, and the establishment of mechanisms for exercising data protection rights that are compatible with blockchain technology.

Keywords: Blockchain; digital assets; personal data; right to be forgotten.

1. Đặt vấn đề

Tài sản số không còn là hiện tượng nằm ngoài đời sống pháp lý. Sự phát triển của tiền mã hóa, token, tài sản số hóa, vật phẩm số, tài sản trong môi trường trò chơi điện tử và các sản phẩm dựa trên chuỗi khối đã làm thay đổi cách con người xác lập, lưu giữ, chuyển giao và chứng minh quyền tài sản. Trước đây, pháp luật dân sự chủ yếu tiếp cận tài sản thông qua vật, tiền, giấy tờ có giá và quyền tài sản. Với sự xuất hiện của tài sản số, ranh giới giữa tài sản, dữ liệu và phương tiện kỹ thuật ghi nhận quyền đã trở nên phức tạp hơn. Luật Công nghiệp công nghệ số năm 2025 lần đầu tiên thiết lập nền tảng pháp lý riêng cho công nghiệp công nghệ số, trong đó có nội dung về tài sản số, tạo cơ sở để Nhà nước từng bước quản lý hoạt động phát hành, lưu ký, trao đổi và cung cấp dịch vụ liên quan đến tài sản số¹.

Sự thay đổi này diễn ra đồng thời với quá trình hoàn thiện pháp luật về dữ liệu. Luật Dữ liệu năm 2024 quy định về xây dựng, phát triển, bảo vệ, quản trị, xử lý và sử dụng dữ liệu. Đồng thời đặt vấn đề nhận diện, quản trị rủi ro phát sinh trong xử lý dữ liệu, bao gồm rủi ro quyền riêng tư, an ninh mạng, nhận dạng và quản lý truy cập². Luật Bảo vệ dữ liệu cá nhân năm 2025 tiếp tục nâng cấp các quy định về quyền của chủ thể dữ liệu, nghĩa vụ của bên kiểm soát dữ liệu, bên xử lý dữ liệu, hoạt động chuyển dữ liệu xuyên biên giới, đánh giá tác động xử lý dữ liệu và trách nhiệm bảo vệ dữ liệu trong các lĩnh vực

1) Quốc hội (2025). Luật Công nghiệp công nghệ số số 71/2025/QH15, ban hành ngày 14/6/2025, có hiệu lực từ ngày 01/01/2026. Cổng thông tin văn bản quy phạm pháp luật Chính phủ. <https://vanban.chinhphu.vn/?classid=1&docid=214609&pageid=27160&typegroupid=3>. Truy cập ngày 26/6/2026.

2) Quốc hội (2024). Luật Dữ liệu số 60/2024/QH15, ban hành ngày 30/11/2024, có hiệu lực từ ngày 01/7/2025. Cổng thông tin văn bản quy phạm pháp luật Chính phủ. <https://vanban.chinhphu.vn/?classid=1&docid=212488&orggroupid=1&pageid=27160>. Truy cập ngày 26/6/2026.

Email: cuongnt@uel.edu.vn.

đặc thù³. Trước khi luật này có hiệu lực, Nghị định số 13/2023/NĐ-CP đã đặt nền móng cho cơ chế bảo vệ dữ liệu cá nhân tại Việt Nam, trong đó ghi nhận quyền của chủ thể dữ liệu đối với việc truy cập, chỉnh sửa, xóa dữ liệu, hạn chế xử lý, phản đối xử lý và yêu cầu bồi thường khi dữ liệu bị xử lý trái pháp luật⁴.

Vấn đề pháp lý phát sinh khi giao dịch tài sản số không còn là giao dịch tài sản. Để một giao dịch được thực hiện, hệ thống phải xử lý nhiều lớp dữ liệu: địa chỉ ví, khóa công khai, dữ liệu giao dịch, thời điểm giao dịch, giá trị chuyển giao, dấu vết kỹ thuật, thông tin thiết bị, thông tin định danh khách hàng, dữ liệu phòng chống rửa tiền và dữ liệu do sàn giao dịch hoặc đơn vị lưu ký thu thập. Khi các lớp dữ liệu này được liên kết, địa chỉ ví tưởng như không nêu tên vẫn có thể trở thành dữ liệu cá nhân.

Chuỗi khối được thiết kế để bảo đảm tính toàn vẹn, chống sửa đổi, phân tán và minh bạch. Chính các đặc tính này lại làm cho việc thực hiện quyền xóa dữ liệu hoặc quyền được lãng quên trở nên khó khăn. Trong bối cảnh Việt Nam, Nhà nước đang đồng thời thúc đẩy định danh điện tử, xác thực dữ liệu dân cư và chuyển đổi số quốc gia theo Quyết định số 06/QĐ-TTg⁵. Khi cơ chế định danh được kết nối với tài khoản giao dịch tài sản số, rủi ro đối khả năng toàn bộ lịch sử giao dịch trên chuỗi bị gắn với danh tính thực. Từ đây, vấn đề pháp lý không thể giải quyết bằng một mệnh đề đơn giản rằng “dữ liệu trên chuỗi không thể xóa nên miễn áp dụng quyền xóa dữ liệu”.

2. Nội dung nghiên cứu

2.1. Cơ sở pháp lý về bảo vệ dữ liệu cá nhân trong giao dịch tài sản số

Pháp luật Việt Nam chưa có luật riêng về giao dịch tài sản số theo nghĩa đầy đủ, nhưng khung điều chỉnh đã hình thành từ bốn nhóm quy phạm dân sự về tài sản, công nghiệp công nghệ số, dữ liệu cá nhân và phòng, chống rửa tiền. Bộ luật Dân sự năm 2015 xác định tài sản gồm vật, tiền, giấy tờ có giá và quyền tài sản; cấu trúc mở này cho phép pháp luật chuyên ngành ghi nhận các dạng tài sản mới khi có khả năng xác định, kiểm soát và chuyển giao (Bộ luật Dân sự, 2015, Điều 105)⁶.

Luật Dữ liệu năm 2024 tạo ra trục pháp lý về quản trị dữ liệu. Trong giao dịch tài sản số, dữ liệu không đơn thuần là thông tin phụ trợ. Dữ liệu có thể là căn cứ xác lập quyền, chứng minh giao dịch, truy vết dòng tài sản, định danh chủ thể và đánh giá rủi ro. Làm phát sinh mối quan hệ mới giữa quyền tài sản và quyền đối với dữ liệu. Nếu pháp luật chỉ tập trung vào bảo vệ quyền tài sản đối với đơn vị dữ liệu số hoặc tài sản mã hóa mà bỏ qua dữ liệu cá nhân gắn với giao dịch, khung quản lý sẽ bị lệch.

Luật Bảo vệ dữ liệu cá nhân năm 2025 và Nghị định số 13/2023/NĐ-CP đặt ra nguyên tắc cơ bản đối với mọi hoạt động xử lý dữ liệu cá nhân: xử lý đúng mục đích, đúng phạm vi, có căn cứ pháp lý, bảo đảm minh bạch, an toàn và tôn trọng quyền của chủ thể dữ liệu. Dữ liệu cá nhân trong giao dịch tài sản số bao gồm họ tên, số định danh cá nhân, số điện thoại, email hoặc thông tin sinh trắc học mà người dùng cung cấp khi mở tài khoản. Trong nhiều trường hợp, địa chỉ ví, mã giao dịch, thông tin thiết bị, địa chỉ IP, mẫu hành vi giao dịch và lịch sử nạp rút cũng có thể là dữ liệu cá nhân nếu được kết hợp với dữ liệu định danh khác. Cách tiếp cận này phù hợp với thực tiễn của Liên minh châu Âu, nơi dữ liệu giả danh vẫn có thể được xem là dữ liệu cá nhân nếu còn khả năng liên kết với một cá nhân xác định (European Data Protection Board, 2025).

Pháp luật phòng, chống rửa tiền làm phát sinh nghĩa vụ nhận biết khách hàng, lưu giữ hồ sơ, giám sát giao dịch và báo cáo giao dịch đáng ngờ. Luật Phòng, chống rửa tiền năm 2022 đã đặt ra nghĩa vụ

3) Quốc hội (2025). *Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15*, ban hành ngày 26/6/2025, có hiệu lực từ ngày 01/01/2026. Xem thêm: Bộ Công an (2026). *Luật Bảo vệ dữ liệu cá nhân chính thức có hiệu lực thi hành từ ngày 01/01/2026*. Bộ Công an. <https://bocongan.gov.vn/bai-viet/luat-bao-ve-du-lieu-ca-nhan-chinh-thuc-co-hieu-luc-thi-hanh-tu-ngay-01-01-2026-1767186124>. Truy cập ngày 26/6/2026.

4) Chính phủ, (2023). *Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân*, có hiệu lực từ ngày 01/7/2023. Cổng thông tin văn bản quy phạm pháp luật Chính phủ. <https://vanban.chinhphu.vn/?docid=207759&pageid=27160>. Truy cập ngày 26/6/2026.

5) Thủ tướng Chính phủ (2022). *Quyết định số 06/QĐ-TTg ngày 06/01/2022 phê duyệt Đề án phát triển ứng dụng dữ liệu về dân cư, định danh và xác thực điện tử phục vụ chuyển đổi số quốc gia giai đoạn 2022-2025, tầm nhìn đến năm 2030*. <https://vanban.chinhphu.vn/?docid=205022&pageid=27160>. Truy cập ngày 26/6/2026.

6) Quốc hội (2015). *Bộ luật Dân sự số 91/2015/QH13*. Cổng thông tin điện tử Chính phủ. <https://vanban.chinhphu.vn/?pageid=27160&docid=183188&classid=1&typegroupid=3>.

nhận biết khách hàng, cập nhật thông tin, lưu giữ hồ sơ, đánh giá rủi ro và báo cáo đối với các đối tượng báo cáo⁷. Đối với tài sản số, chuẩn mực quốc tế của Lực lượng đặc nhiệm tài chính quốc tế - Financial Action Task Force (FATF) yêu cầu các quốc gia đưa tài sản ảo và nhà cung cấp dịch vụ tài sản ảo vào khuôn khổ phòng, chống rửa tiền, trong đó có quy tắc yêu cầu truyền kèm thông tin người khởi tạo và người thụ hưởng trong giao dịch tài sản ảo (Financial Action Task Force, 2021). Nghĩa vụ này có mục tiêu chính đáng về phòng, chống rửa tiền và tài trợ khủng bố, nhưng đồng thời làm tăng quy mô dữ liệu định danh được thu thập, lưu trữ và trao đổi giữa các chủ thể trung gian.

2.2. Mâu thuẫn giữa quyền được lãng quên và công nghệ chuỗi khối

Quyền được lãng quên không nên được hiểu giản lược là quyền xóa mọi dấu vết đã tồn tại. Về bản chất, đó là quyền của cá nhân yêu cầu chấm dứt việc tiếp tục xử lý, công khai, lưu giữ hoặc liên kết dữ liệu cá nhân khi không còn căn cứ pháp lý chính đáng (European Union, 2016). Quyền này bảo vệ con người trước nguy cơ bị quá khứ dữ liệu chi phối vĩnh viễn, nhất là trong môi trường số nơi thông tin có thể được sao chép, tìm kiếm, kết nối ở quy mô lớn. Trong lĩnh vực tài sản số, quyền này có ý nghĩa đặc biệt vì lịch sử giao dịch có thể phản ánh năng lực tài chính, thói quen đầu tư, quan hệ kinh tế, mạng lưới đối tác và trong một số trường hợp còn phản ánh quan điểm, lối sống hoặc tình trạng cá nhân.

Chuỗi khối lại được thiết kế theo một logic khác. Một giao dịch sau khi được xác nhận sẽ trở thành một phần của sổ cái phân tán. Mỗi nút mạng lưu giữ bản sao dữ liệu, thuật toán đồng thuận bảo vệ tính toàn vẹn của chuỗi, và việc sửa đổi dữ liệu quá khứ đòi hỏi thay đổi đồng thời trên mạng lưới. Đối với chuỗi khối công khai, không có một “người quản trị trung tâm” có quyền đơn phương xóa dữ liệu theo yêu cầu của chủ thể dữ liệu (European Parliament Research Service, 2019). Chính vì vậy, các cơ quan bảo vệ dữ liệu của châu Âu đã nhiều lần khuyến nghị hạn chế tối đa việc đưa dữ liệu cá nhân lên chuỗi và ưu tiên mô hình lưu trữ ngoài chuỗi, chỉ đưa lên chuỗi các giá trị băm hoặc bằng chứng kỹ thuật không đủ để nhận diện cá nhân (Commission nationale de l’informatique et des libertés, 2018).

Ngoài ra, người dùng thường giao dịch bằng địa chỉ ví, không trực tiếp hiển thị họ tên. Tuy nhiên, nặc danh giả không đồng nghĩa với ẩn danh. Một địa chỉ ví có thể bị liên kết với cá nhân thông qua sàn giao dịch tập trung, thông tin KYC, địa chỉ IP, thiết bị, dữ liệu nạp rút tiền pháp định, dữ liệu ngân hàng hoặc dữ liệu từ cơ quan nhà nước. Khi liên kết này hình thành, toàn bộ lịch sử giao dịch công khai của địa chỉ ví có thể trở thành hồ sơ cá nhân có giá trị phân tích rất lớn. Đây là điểm khiến quyền riêng tư trong giao dịch tài sản số dễ bị tổn thương hơn so với giao dịch tài sản truyền thống. Một giao dịch ngân hàng thông thường được lưu giữ trong hệ thống có kiểm soát; còn giao dịch trên chuỗi khối công khai có thể được quan sát bởi bất kỳ ai, dù người quan sát chưa biết ngay danh tính thật của chủ ví.

2.3. Thực trạng rủi ro bảo vệ dữ liệu cá nhân trong giao dịch tài sản số tại Việt Nam

Sự không tương thích giữa tốc độ phát triển của thị trường và mức độ hoàn thiện của khuôn khổ quản lý. Người dùng Việt Nam đã tiếp cận tài sản số qua sàn giao dịch quốc tế, ví điện tử phi lưu ký, trò chơi blockchain, NFT và nhiều sản phẩm đầu tư số. Tuy nhiên, trước khi Luật Công nghiệp công nghệ số năm 2025 được ban hành, pháp luật chưa có cơ chế đầy đủ để xác định tư cách pháp lý của tài sản số, điều kiện cung cấp dịch vụ, trách nhiệm lưu ký, nghĩa vụ minh bạch thông tin, bảo vệ nhà đầu tư và bảo vệ dữ liệu cá nhân. Khoảng trống này khiến người dùng phải dựa nhiều vào điều khoản sử dụng do nền tảng soạn sẵn, trong khi khả năng thương lượng gần như không tồn tại.

Để mở tài khoản tại sàn giao dịch tập trung, người dùng thường phải cung cấp giấy tờ định danh, ảnh khuôn mặt, số điện thoại, email, địa chỉ cư trú, tài khoản ngân hàng và thông tin thiết bị. Khi các dữ liệu này được gắn với địa chỉ ví, lịch sử giao dịch trên chuỗi không còn là các ký hiệu rời rạc. Nó có thể trở thành bản đồ tài chính cá nhân. Nếu sàn giao dịch bị tấn công, bán dữ liệu, chia sẻ dữ liệu vượt quá mục đích hoặc chuyển dữ liệu xuyên biên giới không có kiểm soát, hậu quả đối với cá nhân rất khó

7) Quốc hội (2022). *Luật Phòng, chống rửa tiền số 14/2022/QH15*, ban hành ngày 15/11/2022, có hiệu lực từ ngày 01/3/2023. Cổng thông tin điện tử Chính phủ. <https://chinhphu.vn/?docid=207710&pageid=27160>. Truy cập ngày 26/6/2026.

khắc phục. Khác với mật khẩu, lịch sử giao dịch trên chuỗi không thể thay đổi; khác với số tài khoản ngân hàng, địa chỉ ví cũ vẫn tồn tại vĩnh viễn trong các công cụ tra cứu công khai.

Việt Nam đang chịu áp lực hoàn thiện khuôn khổ quản lý tài sản ảo, nhà cung cấp dịch vụ tài sản ảo và thực thi các khuyến nghị của FATF. Trong danh sách các nội dung cần khắc phục, FATF đã khuyến nghị Việt Nam có hành động để điều chỉnh tài sản ảo và nhà cung cấp dịch vụ tài sản ảo (Financial Action Task Force, 2026). Về mặt chính sách, yêu cầu này là cần thiết để ngăn chặn rửa tiền, tài trợ khủng bố, lừa đảo và chuyển tài sản bất hợp pháp. Tuy nhiên, ở phương diện bảo vệ dữ liệu cá nhân, càng mở rộng nghĩa vụ thu thập và trao đổi thông tin giao dịch thì càng phải có cơ chế giới hạn mục đích, giới hạn thời hạn lưu giữ, bảo mật, phân quyền truy cập và kiểm toán việc sử dụng dữ liệu. Nếu không, phòng, chống rửa tiền có thể trở thành lý do bao trùm để tích lũy dữ liệu quá mức.

Đề án 06 đặt mục tiêu phát triển ứng dụng dữ liệu dân cư, định danh và xác thực điện tử phục vụ chuyển đổi số quốc gia giai đoạn 2022-2025, tầm nhìn đến năm 2030⁸. Đây là nền tảng quan trọng cho chính phủ số, kinh tế số và xã hội số. Khi cơ chế định danh mạnh được sử dụng trong giao dịch tài sản số, cần tránh xu hướng đồng nhất hóa mọi dữ liệu giao dịch với hồ sơ định danh tập trung. Một hệ thống quản lý hợp lý phải xác thực được người dùng khi cần thiết, nhưng không biến mọi dấu vết giao dịch thành dữ liệu định danh có thể bị truy cập rộng rãi. Nhà nước có thể yêu cầu VASP biết khách hàng của mình, nhưng không nên để mọi chủ thể trong hệ sinh thái đều biết khách hàng đó là ai.

2.4. Giải pháp hoàn thiện pháp luật Việt Nam

Một là, cần xác lập nguyên tắc phân tầng dữ liệu trong giao dịch tài sản số. Văn bản hướng dẫn Luật Công nghiệp công nghệ số và Luật Bảo vệ dữ liệu cá nhân nên phân biệt rõ dữ liệu định danh trực tiếp, dữ liệu giả danh trên chuỗi, dữ liệu giao dịch thuần túy, dữ liệu phòng chống rửa tiền và dữ liệu đã được ẩn danh. Mỗi nhóm dữ liệu phải có chế độ xử lý khác nhau. Dữ liệu định danh trực tiếp phải chịu cơ chế bảo vệ nghiêm ngặt nhất; dữ liệu giả danh phải được bảo vệ khi có khả năng liên kết với cá nhân; dữ liệu đã ẩn danh chỉ được coi là ngoài phạm vi bảo vệ dữ liệu cá nhân khi không còn khả năng tái định danh bằng phương tiện hợp lý.

Hai là, cần quy định nguyên tắc không đưa dữ liệu định danh trực tiếp lên chuỗi. Đây phải là yêu cầu pháp lý bắt buộc đối với nhà cung cấp dịch vụ tài sản ảo (Virtual Asset Service Provider – VASP), tổ chức phát hành tài sản số, nền tảng lưu ký, nền tảng giao dịch và nhà phát triển ứng dụng có xử lý dữ liệu cá nhân. Thay vì ghi họ tên, số định danh, thông tin và tài liệu thu thập trong quá trình nhận biết khách hàng (Know Your Customer – KYC) hoặc dữ liệu nhạy cảm lên chuỗi, hệ thống chỉ nên ghi bằng chứng kỹ thuật ở mức tối thiểu, như mã tham chiếu, giá trị băm hoặc chứng thư xác nhận đã định danh. Dữ liệu gốc phải được lưu giữ ngoài chuỗi trong môi trường có kiểm soát, có thể sửa, xóa, hạn chế hoặc hủy khi hết căn cứ xử lý.

Ba là, cần thiết kế cơ chế thực hiện quyền xóa dữ liệu theo hướng phù hợp với chuỗi khối. Đối với dữ liệu ngoài chuỗi, VASP phải tiếp nhận và giải quyết yêu cầu xóa, hủy, hạn chế xử lý theo thời hạn luật định, trừ trường hợp có nghĩa vụ lưu giữ theo pháp luật. Đối với dữ liệu trên chuỗi, VASP không thể bị buộc xóa giao dịch đã xác nhận nếu họ không có khả năng kỹ thuật và pháp lý để làm việc đó; tuy nhiên, họ phải có nghĩa vụ cắt liên kết định danh, ngừng công khai hóa quan hệ giữa địa chỉ ví và cá nhân, ngừng chia sẻ dữ liệu với bên thứ ba khi không còn căn cứ, và áp dụng biện pháp làm giảm khả năng tái định danh. Đây là cách hiểu thực chất hơn về quyền được lãng quên trong môi trường bất biến.

Bốn là, cần giới hạn chặt chẽ ngoại lệ vì phòng, chống rửa tiền. Pháp luật có thể cho phép VASP lưu giữ dữ liệu KYC và dữ liệu giao dịch trong thời hạn cần thiết để tuân thủ nghĩa vụ phòng, chống rửa tiền, thuế, kế toán, thanh tra, điều tra hoặc giải quyết tranh chấp. Tuy nhiên, ngoại lệ này phải đi kèm ba điều kiện: mục đích lưu giữ cụ thể; thời hạn lưu giữ xác định; phạm vi truy cập được phân quyền và ghi nhận. Không nên cho phép nền tảng sử dụng dữ liệu được thu thập vì mục đích tuân thủ để quảng cáo, chấm điểm hành vi, bán dữ liệu, hoặc huấn luyện hệ thống phân tích thương mại nếu không có căn cứ pháp lý riêng.

8) Thủ tướng Chính phủ (2022). *Quyết định số 06/QĐ-TTg, ttdđ.*

Năm là, cần quy định nghĩa vụ đánh giá tác động bảo vệ dữ liệu đối với dịch vụ tài sản số. Mọi VASP trước khi cung cấp dịch vụ tại Việt Nam hoặc cho người dùng Việt Nam cần thực hiện đánh giá tác động xử lý dữ liệu, trong đó làm rõ loại dữ liệu thu thập, căn cứ xử lý, nơi lưu trữ, chủ thể được chia sẻ, thời hạn lưu giữ, rủi ro tái định danh, biện pháp mã hóa, cơ chế xóa dữ liệu ngoài chuỗi và phương án xử lý khi có yêu cầu của chủ thể dữ liệu. Đối với dịch vụ có chuyển dữ liệu xuyên biên giới, hồ sơ đánh giá phải bổ sung thông tin về quốc gia tiếp nhận, tiêu chuẩn bảo vệ tương đương và cơ chế xử lý khi xảy ra vi phạm.

Sáu là, cần gắn trách nhiệm bảo vệ dữ liệu với điều kiện cấp phép hoặc đăng ký hoạt động của VASP. Một nhà cung cấp dịch vụ tài sản số không nên được phép hoạt động chỉ vì đáp ứng yêu cầu về vốn, nhân sự, hệ thống kỹ thuật hoặc phòng, chống rửa tiền. Họ còn phải chứng minh năng lực bảo vệ dữ liệu cá nhân: có cán bộ phụ trách bảo vệ dữ liệu, quy trình tiếp nhận yêu cầu của chủ thể dữ liệu, hệ thống phân quyền truy cập, mã hóa dữ liệu, quản lý bên thứ ba, kế hoạch ứng phó sự cố và cơ chế thông báo vi phạm dữ liệu. Trường hợp không bảo đảm các yêu cầu này, cơ quan quản lý cần có quyền đình chỉ, hạn chế dịch vụ hoặc buộc khắc phục.

3. Kết luận

Giao dịch tài sản số đặt pháp luật Việt Nam trước một bài toán khó: phải bảo vệ quyền tài sản, bảo đảm an toàn thị trường, đáp ứng yêu cầu phòng chống rửa tiền, nhưng đồng thời không được hy sinh quyền riêng tư và quyền tự quyết thông tin của cá nhân. Chuỗi khối đem lại niềm tin bằng tính bất biến, nhưng tính bất biến ấy cũng có thể làm cho dữ liệu cá nhân bị lưu giữ và liên kết ngoài ý chí của chủ thể dữ liệu. Vì vậy, cách tiếp cận phù hợp không phải là phủ nhận quyền được lãng quên, cũng không phải là buộc hệ thống chuỗi khối thực hiện điều không thể. Giải pháp đúng hơn là thiết kế lại khung pháp lý theo hướng phân tầng dữ liệu, hạn chế dữ liệu cá nhân trên chuỗi, kiểm soát dữ liệu ngoài chuỗi, cụ thể hóa nghĩa vụ của VASP và đặt phòng, chống rửa tiền trong giới hạn của bảo vệ dữ liệu cá nhân.

Việt Nam đang có cơ hội hình thành khuôn khổ pháp lý cho tài sản số ngay trong giai đoạn đầu của thị trường. Nếu khung pháp lý chỉ chú trọng quản lý tài sản mà xem nhẹ dữ liệu cá nhân, thị trường có thể phát triển trên nền tảng rủi ro. Nếu khung pháp lý quá cứng nhắc, yêu cầu xóa mọi dữ liệu giao dịch trên chuỗi, quy định sẽ không thể thực thi. Do đó, hướng hoàn thiện cần dựa trên nguyên tắc khả thi, tương xứng và bảo vệ quyền con người trong môi trường số. Tài sản số chỉ có thể trở thành một bộ phận hợp pháp của nền kinh tế số khi quyền tài sản và quyền dữ liệu được bảo vệ trong cùng một khuôn khổ pháp lý thống nhất.

Tài liệu tham khảo

Commission nationale de l'informatique et des libertés (2018, October 29). *Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data*. <https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data>. Truy cập ngày 26/6/2026.

European Data Protection Board (2025, April 8). *Guidelines 02/2025 on processing of personal data through blockchain technologies*. https://www.edpb.europa.eu/news/news/2025/edpb-adopts-guidelines-processing-personal-data-through-blockchains-and-ready_en, truy cập ngày 26/6/2026.

European Parliament Research Service (2019, July). *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?*

European Union (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)*.

European Union (2023). *Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets*.

Financial Action Task Force (2021, October). *Updated guidance for a risk-based approach to virtual assets and virtual asset service providers*. <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html>. Truy cập ngày 26/6/2026.

Financial Action Task Force (2026, June 19). *Jurisdictions under increased monitoring*. <https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/increased-monitoring-february-2025.html>. Truy cập ngày 26/6/2026.