



VNU Journal of Science: Legal Studies

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



Original Article

Legal Frameworks for Personal Data Protection in Digital Finance: International Practices and Implications for Vietnam

Tran Xuan Nhat^{1,*}, Nguyen Tran Anh Dung²

¹*Ho Chi Minh University of Banking, 36 Ton That Dam, Sai Gon, Ho Chi Minh City, Vietnam*

²*University Phuong Dong, 171 Trung Kinh, Yen Hoa, Ha Noi, Vietnam*

Received 28th May 2026

Revised 15th July 2026; Accepted 25th September 2026

Abstract: Digital finance has accelerated the collection and monetization of personal data, as data constitutes both an object of privacy rights and a valuable economic asset. In addition to the benefits of service personalization and financial management, digital finance also poses risks related to data breaches, financial fraud, and algorithmic bias in AI systems. This article employs legal research methods and examines the legal frameworks adopted in several jurisdictions. The findings indicate a shift from traditional data protection approaches toward governance models based on data control rights, accountability, and digital financial supervision. On that basis, the article proposes a legal framework for the protection of personal data in Vietnam's digital finance sector.

Keywords: Digital finance, legal framework, personal data.

* Corresponding author.

E-mail address: tranxuannhat2001@gmail.com

<https://doi.org/10.25073/2588-1167/vnuls.4879>

Khung pháp lý về bảo vệ dữ liệu cá nhân trong lĩnh vực tài chính số: kinh nghiệm quốc tế và hàm ý cho Việt Nam

Trần Xuân Nhật^{1,*}, Nguyễn Trần Anh Dũng²

¹Trường Đại học Ngân hàng Hồ Chí Minh, 36 Tôn Thất Đạm, Sài Gòn, Thành phố Hồ Chí Minh, Vietnam

²Trường Đại học Phương Đông, 171 Trung Kính, Yên Hòa, Hà Nội, Việt Nam

Nhận ngày 28 tháng 5 năm 2026

Chỉnh sửa ngày 15 tháng 7 năm 2026; Chấp nhận đăng ngày 25 tháng 9 năm 2026

Tóm tắt: Tài chính số kích thích việc thu thập dữ liệu cá nhân và việc kiếm tiền từ dữ liệu, vì dữ liệu là đối tượng của quyền riêng tư và là một tài sản có giá trị kinh tế. Ngoài những lợi ích của việc cá nhân hóa dịch vụ và quản lý tài chính, còn có những rủi ro liên quan đến vi phạm dữ liệu, gian lận tài chính và thiên vị thuật toán AI. Bài viết này sử dụng các phương pháp nghiên cứu pháp lý và đánh giá các khung pháp lý của một số quốc gia. Kết quả chỉ ra sự chuyển dịch từ bảo vệ dữ liệu truyền thống sang quản trị dựa trên quyền kiểm soát dữ liệu, trách nhiệm giải trình và giám sát tài chính số. Dựa trên đó, một khung pháp lý bảo vệ dữ liệu tài chính số cho Việt Nam được đề xuất.

Từ khóa:

Từ khóa: Dữ liệu cá nhân, khung pháp lý, tài chính số.

1. Mở đầu

Chuyển đổi số (CDS) đã hoàn toàn thay đổi cấu trúc của hệ thống tài chính thế giới. Công nghệ tài chính hiện đại, ngân hàng số, ngân hàng mở, trí tuệ nhân tạo (AI), dữ liệu lớn và các công nghệ khác giúp tối ưu hóa dịch vụ tài chính và cá nhân hóa trải nghiệm khách hàng lên một tầm cao mới [1]. Dữ liệu cá nhân (DLCN) là nền tảng cơ bản của hệ sinh thái tài chính số (TCS) hiện đại và rất quan trọng cho việc nhận diện khách hàng, đánh giá tín dụng, quản trị rủi ro (QTRR), tránh gian lận và các sản phẩm tài chính thông minh [2].

Trong nền kinh tế số, DLCN đang trở thành đối tượng điều chỉnh quan trọng của pháp luật tài chính số. Thông qua AI và dữ liệu lớn, doanh nghiệp (DN) TCS và ngân hàng số khai thác dữ liệu giao dịch và dữ liệu hành vi để phát triển hệ

thống chấm điểm tín dụng, dự báo khả năng vay vốn, định giá động và cá nhân hóa dịch vụ tài chính dẫn tới dữ liệu ngày càng trở thành nguồn lực cốt lõi tạo giá trị tài chính và lợi thế cạnh tranh trong hệ sinh thái TCS cần được pháp luật hỗ trợ và điều chỉnh.

DLCN ngày càng bị thương mại hóa [3]. Trong lĩnh vực TCS, dữ liệu hành vi tài chính (behavioral finance data) được khai thác để xây dựng hồ sơ tín dụng, đánh giá khả năng thanh toán và cá nhân hóa sản phẩm tài chính. Xử lý dữ liệu thời gian thực giúp Fintech mở rộng khả năng đánh giá tín dụng nhưng cũng làm gia tăng rủi ro xâm phạm quyền riêng tư.

Nhiều vụ vi phạm dữ liệu quy mô lớn cho thấy tính cấp thiết của bảo vệ DLCN trong TCS. Theo IBM, tài chính thuộc nhóm ngành có chi phí vi phạm dữ liệu cao nhất toàn cầu. Các sự cố rò rỉ dữ liệu gây thiệt hại tài chính và làm gia

* Tác giả liên hệ.

Địa chỉ email: tranxuannhat2001@gmail.com

<https://doi.org/10.25073/2588-1167/vnuls.4879>

tăng rủi ro danh tiếng, rủi ro vận hành và rủi ro hệ thống [4]. Bảo vệ DLCN không chỉ là vấn đề quyền riêng tư mà còn gắn với QTRR tài chính và an ninh kinh tế số. Hoạt động Fintech cần cân bằng giữa thúc đẩy đổi mới sáng tạo và bảo đảm tuân thủ pháp luật về bảo vệ dữ liệu. Mở rộng chia sẻ dữ liệu có thể thúc đẩy tiếp cận tài chính nhưng cũng làm gia tăng chi phí tuân thủ về bảo vệ dữ liệu, an ninh mạng và quản trị AI. Quản trị dữ liệu (QTDL) trong TCS ngày càng gắn với mô hình Quản trị-Rủi ro-Tuân thủ (GRC), kết hợp QTDL, kiểm soát rủi ro công nghệ và tuân thủ pháp luật.

Quy định Bảo vệ dữ liệu chung của Liên minh Châu Âu (GDPR) đã đưa ra một số nguyên tắc cơ bản về quyền kiểm soát DLCN, trách nhiệm giải trình và minh bạch trong xử lý dữ liệu [5]. Singapore, Hoa Kỳ và Trung Quốc cũng đã phát triển các cơ chế pháp lý riêng cho DLCN trong hệ sinh thái Fintech và TCS, các mô hình này cho thấy xu hướng tăng cường quyền kiểm soát dữ liệu của chủ thể dữ liệu và trách nhiệm của tổ chức xử lý dữ liệu.

Tại Việt Nam, sự phát triển của thanh toán điện tử, ngân hàng số và Fintech đang làm gia tăng mạnh lượng DLCN được thu thập và xử lý. Mặc dù Luật Bảo vệ DLCN 2025 và Nghị định số 356/2025/NĐ-CP tạo nền tảng pháp lý cho bảo vệ DLCN, khung pháp lý hiện đã ban hành nhưng vẫn còn khoảng trống liên quan đến QTDL TCS, trách nhiệm giải trình AI, Open banking và kiểm soát dữ liệu xuyên biên giới [6,7]. Luật Bảo vệ DLCN 2025 đã bước đầu hình thành cơ sở pháp lý cho hoạt động xử lý dữ liệu trong môi trường số thông qua các nguyên tắc như xử lý đúng mục đích, giới hạn phạm vi thu thập và trách nhiệm giải trình của chủ thể xử lý dữ liệu. Luật đồng thời ghi nhận các quyền cơ bản của chủ thể dữ liệu, bao gồm quyền được biết, quyền đồng ý, quyền truy cập, chỉnh sửa và yêu cầu xóa dữ liệu. Đối với lĩnh vực tài chính số, các quy định về xử lý dữ liệu nhạy cảm, đánh giá tác động xử lý dữ liệu và chuyển dữ liệu xuyên biên giới tác động trực tiếp đến hoạt động ngân hàng số và Fintech. Dù vậy, pháp luật hiện hành vẫn chưa quy định rõ trách nhiệm pháp lý đối với quyết định tự động của AI, cơ chế kiểm

toán thuật toán cũng như việc phân bổ trách nhiệm dữ liệu giữa các chủ thể cung ứng dịch vụ tài chính số.

Các nghiên cứu tại Việt Nam chủ yếu tập trung vào quyền riêng tư, an ninh mạng và bảo vệ NTD trong thương mại điện tử, trong khi nghiên cứu chuyên sâu về bảo vệ DLCN trong lĩnh vực TCS vẫn còn hạn chế, chưa xem xét đầy đủ dữ liệu như một tài sản kinh tế, một đối tượng của cơ chế quản lý dữ liệu tài chính số (financial data governance) và kiểm soát rủi ro thuật toán (algorithmic risk governance) [8]. Nghiên cứu so sánh kinh nghiệm quốc tế về bảo vệ DLCN trong TCS tại Việt Nam còn hạn chế. Khoảng trống nghiên cứu này cho thấy cần kết hợp tiếp cận luật học với phân tích công nghệ tài chính và cơ chế kiểm soát dữ liệu số. Nghiên cứu này tập trung vào ba vấn đề: thứ nhất, từ bảo mật DLCN đến quản trị dữ liệu TCS; thứ hai, sự tích hợp của luật pháp, quản lý tài chính và quản trị công nghệ trong bối cảnh hệ sinh thái tài chính số; và thứ ba, các phương pháp tiếp cận sáng tạo đối với luật pháp Việt Nam dựa trên các mô hình quản trị dữ liệu dựa trên rủi ro thay vì các mô hình bảo vệ dữ liệu truyền thống được đề xuất áp dụng trong bối cảnh Việt Nam.

2. Cơ sở lý thuyết và tổng quan nghiên cứu

2.1. Bảo vệ dữ liệu cá nhân trong tài chính số

DLCN là thông tin về một cá nhân có thể được nhận dạng trực tiếp hoặc gián tiếp thông qua các yếu tố nhận dạng như tên, số điện thoại, tài khoản ngân hàng, dữ liệu sinh trắc học hoặc hành vi trực tuyến [5]. Trong TCS, DLCN không chỉ bao gồm thông tin nhận dạng cơ bản mà còn mở rộng đến dữ liệu giao dịch, tín dụng và hành vi tiêu dùng. DLCN là đối tượng cần được bảo vệ trong khuôn khổ quyền riêng tư của con người. Quyền đối với dữ liệu cá nhân được xem là một bộ phận quan trọng của quyền về sự riêng tư, bảo đảm cho cá nhân khả năng kiểm soát việc thu thập, sử dụng, lưu trữ và chia sẻ thông tin liên quan đến mình trong môi trường số [9]. Dữ liệu cá nhân được sử dụng rộng rãi trong các hệ thống

chăm điểm tín dụng, đánh giá rủi ro và ra quyết định tự động trong lĩnh vực tài chính. Việc khai thác dữ liệu thông qua các mô hình phân tích và thuật toán học máy cho phép các tổ chức tài chính dự báo hành vi khách hàng và hỗ trợ quá trình ra quyết định. Do đó, bảo vệ dữ liệu cá nhân cần được tiếp cận không chỉ từ góc độ quyền riêng tư và quyền con người mà còn từ góc độ quản trị dữ liệu, minh bạch thuật toán và quản trị rủi ro trong môi trường số [10].

Theo Nghị định 13/2023/NĐ-CP, DLCN bao gồm dữ liệu cơ bản và dữ liệu nhạy cảm, trong đó dữ liệu tài chính (DLTC) và thông tin tài khoản ngân hàng thuộc nhóm cần được bảo vệ nghiêm ngặt hơn [11]. Sự phát triển của Fintech, AI và dữ liệu lớn đang thúc đẩy mô hình tài chính dựa trên dữ liệu, cho phép DN phân tích hành vi khách hàng theo thời gian thực nhằm tối ưu hóa QTRR và mở rộng khả năng tiếp cận tín dụng [2]. Việc ứng dụng AI trong TCS đòi hỏi hoàn thiện cơ chế kiểm soát và trách nhiệm pháp lý đối với thuật toán, trong đó nhiều quyết định như chăm điểm tín dụng và phát hiện gian lận được thực hiện tự động. Mô hình “hộp đen” có thể dẫn đến thiếu minh bạch và phát sinh nguy cơ xâm phạm quyền và lợi ích hợp pháp của chủ thể dữ liệu. Trong các hoạt động chăm điểm tín dụng dựa trên AI, các quyết định tự động có thể ảnh hưởng đáng kể đến khách hàng trong khi cơ chế ra quyết định của thuật toán thường thiếu tính minh bạch và khó giải thích (Wachter et al., 2017). Đồng thời, sự gia tăng các hoạt động xử lý và chuyển dữ liệu cá nhân đòi hỏi các tổ chức phải bảo đảm trách nhiệm giải trình, quản trị dữ liệu và kiểm soát rủi ro nhằm bảo vệ quyền riêng tư của chủ thể dữ liệu [12].

2.2. Kinh nghiệm quốc tế về bảo vệ dữ liệu cá nhân trong lĩnh vực tài chính số

2.2.1. Liên minh châu Âu và mô hình GDPR

Về bảo vệ DLCN, Liên minh Châu Âu đã thông qua Quy định Bảo vệ dữ liệu chung (GDPR) vào năm 2018 [5]. Như đã đề cập, GDPR thiết lập các nguyên tắc minh bạch, giới hạn mục đích và tối thiểu hóa dữ liệu trong hoạt động xử lý dữ liệu. GDPR cho phép cá nhân

kiểm soát DLCN của họ thông qua quyền truy cập, chỉnh sửa, xóa và phản đối các quyết định xử lý dữ liệu tự động. GDPR cũng sẽ làm tăng chi phí tuân thủ pháp lý và hoạt động cho các doanh nghiệp Fintech và các công ty khởi nghiệp công nghệ tài chính.

GDPR có tác động mạnh mẽ đến các hoạt động an ninh thông tin. Các tổ chức tài chính phải áp dụng các mô hình “Bảo mật theo thiết kế” và “Bảo mật theo mặc định” bao gồm bảo vệ quyền riêng tư ngay từ đầu khi phát triển một hệ thống. Các biện pháp trừng phạt với mức phạt lên đến 4% doanh thu toàn cầu của công ty cũng được áp dụng và đặt rất nhiều áp lực lên các DN để tuân thủ bảo vệ DLCN [13]. GDPR đã trở thành mô hình tham chiếu quan trọng cho nhiều quốc gia, trong đó có Việt Nam, trong quá trình hoàn thiện pháp luật về bảo vệ dữ liệu cá nhân và quản trị dữ liệu trong bối cảnh chuyển đổi số [5,14,15].

2.2.2. Singapore và mô hình QTDL linh hoạt

Singapore là một trong những quốc gia châu Á xây dựng tương đối sớm khung pháp lý bảo vệ DLCN thông qua Đạo luật bảo vệ DLCN (Personal Data Protection Act gọi tắt là PDPA) [16]. Khác với cách tiếp cận mang tính quyền riêng tư mạnh như GDPR, Singapore áp dụng mô hình cân bằng giữa đổi mới sáng tạo và quản lý dữ liệu nhằm hỗ trợ phát triển nền kinh tế số và TCS [17].

Singapore nổi bật với cơ chế “Hộp cát quy định” (Regulatory Sandbox) nhằm tạo cơ sở pháp lý thử nghiệm cho hoạt động Fintech do Cơ quan tiền tệ Singapore (Monetary Authority of Singapore - MAS) triển khai, cho phép DN Fintech thử nghiệm sản phẩm trong môi trường pháp lý kiểm soát nhằm cân bằng giữa đổi mới sáng tạo và kiểm soát rủi ro DLTC. Tuy nhiên mô hình này cũng tiềm ẩn nguy cơ “lợi dụng khoảng trống pháp lý” (regulatory arbitrage) để né tránh nghĩa vụ tuân thủ.

PDPA yêu cầu DN phải có sự đồng ý của người dùng trước khi xử lý DLCN, đồng thời quy định trách nhiệm bảo mật và thông báo vi phạm dữ liệu. MAS cũng ban hành các hướng dẫn về QTRR công nghệ và an ninh mạng đối với ngân

hàng số và DN Fintech. Nhiều quốc gia Đông Nam Á cũng đang từng bước hoàn thiện pháp luật bảo vệ DLCN nhằm đáp ứng yêu cầu phát triển kinh tế số và QTDL xuyên biên giới. Xu hướng chung của ASEAN là tăng cường trách nhiệm của tổ chức xử lý dữ liệu, bảo đảm quyền kiểm soát dữ liệu của cá nhân và hài hòa hóa tiêu chuẩn bảo vệ dữ liệu trong khu vực [18].

2.2.3. Hoa Kỳ và cách tiếp cận theo lĩnh vực

Không giống mô hình QTDL thống nhất của EU, Hoa Kỳ áp dụng cơ chế quản lý dữ liệu mang tính phân tán và định hướng thị trường. Thay vì ban hành một đạo luật chung về bảo vệ DLCN, Hoa Kỳ quản lý theo từng lĩnh vực, từng bang và kết hợp với cơ chế tự điều chỉnh của DN. Luật Gramm-Leach-Bliley (GLBA) yêu cầu các tổ chức tài chính minh bạch về hoạt động thu thập, chia sẻ dữ liệu khách hàng và thực hiện các biện pháp bảo mật phù hợp [19]. Ủy ban Thương mại Liên bang (FTC) và Cục Bảo vệ Tài chính Người tiêu dùng (CFPB) giám sát các hoạt động khai thác dữ liệu của các doanh nghiệp tài chính và các nền tảng công nghệ. Sự phát triển của Open Banking và AI đang đặt ra nhiều vấn đề pháp lý liên quan đến quyền kiểm soát và chia sẻ dữ liệu tài chính. Nhiều bang đã ban hành Đạo luật Quyền riêng tư của Người tiêu dùng California (CCPA), cho phép cư dân biết thông tin nào đang được thu thập và yêu cầu xóa bỏ. Luật liên bang và tiểu bang không được tập trung, vì vậy việc tuân thủ rất khó khăn cho các doanh nghiệp; tuân thủ rất tốn kém ở nhiều bang [20].

2.2.4. Trung Quốc kiểm soát dữ liệu trong nền kinh tế nền tảng

Trung Quốc đã phát triển một mô hình kiểm soát dữ liệu rất tập trung với Luật bảo vệ thông tin cá nhân (PIPL) 2021. PIPL yêu cầu các công ty công nghệ và các nền tảng Fintech phải có sự đồng ý rõ ràng của người dùng trước khi xử lý DLCN và áp đặt các quy định nghiêm ngặt về việc chuyển dữ liệu ra nước ngoài [21].

Với lượng dữ liệu tài chính khổng lồ do các công ty công nghệ như Ant Group hay Tencent nắm giữ, Trung Quốc coi việc bảo vệ dữ liệu là vấn đề về quyền riêng tư và an ninh quốc gia, chủ quyền dữ liệu và nền kinh tế nền tảng. PIPL thể

hiện xu hướng kết hợp giữa bảo vệ DLCN và bảo đảm chủ quyền dữ liệu quốc gia vì nó không phụ thuộc vào các công ty công nghệ lớn. Vì vậy, quốc gia này đang đẩy nhanh giám sát thuật toán, kiểm soát dữ liệu số chiến lược và giám sát việc khai thác dữ liệu bởi AI trong các lĩnh vực TCS.

2.3. Thực trạng khung pháp lý bảo vệ dữ liệu cá nhân trong lĩnh vực tài chính số tại Việt Nam

2.3.1. Hệ thống pháp luật hiện hành

Việt Nam từng bước xây dựng khung pháp lý về bảo vệ DLCN nhằm đáp ứng yêu cầu CDS và phát triển kinh tế số. Trước khi ban hành Nghị định 13/2023/NĐ-CP [11], các quy định về DLCN được phân tán trong nhiều văn bản như Bộ luật Dân sự, Luật An toàn thông tin mạng và Luật An ninh mạng, chủ yếu mang tính nguyên tắc và chưa hình thành cơ chế bảo vệ dữ liệu thống nhất, đặc biệt trong lĩnh vực TCS [22–24].

Trong ngân hàng số, bảo vệ dữ liệu ngày càng gắn với quản trị tuân thủ và rủi ro vận hành. Nhiều tổ chức tín dụng sử dụng mô hình 'Ba tuyến phòng thủ' để giám sát cách dữ liệu khách hàng được xử lý [25], và DLCN hiện là một trong những khía cạnh được quan tâm bậc nhất về an ninh dữ liệu [26]. An ninh thông tin và quyền riêng tư là cốt lõi của quản trị ngân hàng số. Với sự phát triển của eKYC, thanh toán điện tử và dịch vụ ngân hàng trực tuyến, các vụ rò rỉ dữ liệu và tấn công mạng đang gia tăng trong môi trường số, đòi hỏi quản lý pháp lý tốt hơn và an ninh dữ liệu tại Việt Nam [27].

Luật Bảo vệ DLCN 2025 [6] hiện là văn bản pháp lý chính cho bảo vệ DLCN tại Việt Nam và đưa ra các nguyên tắc xử lý dữ liệu, quyền của đối tượng dữ liệu và trách nhiệm của các nhà xử lý dữ liệu. Dữ liệu tài chính và thông tin tài khoản ngân hàng là DLCN nhạy cảm cần được bảo vệ nghiêm ngặt hơn, và các cơ chế đánh giá tác động xử lý dữ liệu và kiểm soát chuyển dữ liệu xuyên biên giới được đưa ra. Nghị định 356/2025/NĐ-CP thể hiện xu hướng chuyển từ mô hình bảo vệ quyền riêng tư hiện tại sang kiểm soát dữ liệu dựa trên trách nhiệm và QTRR dữ liệu. Các quy định mới tăng cường cơ chế đánh giá tác động xử lý dữ liệu và kiểm soát dữ liệu

xuyên biên giới trong lĩnh vực Fintech [7].

Sự gia tăng giao dịch thanh toán số làm phát sinh yêu cầu hoàn thiện cơ chế pháp lý về bảo mật dữ liệu tài chính. Cải thiện luật về bảo vệ DLCN nên được thực hiện thông qua một hệ thống pháp lý tích hợp, tổ chức xử lý dữ liệu tốt hơn và thực thi hiệu quả trong bối cảnh số [28].

2.3.2. Hạn chế và thách thức pháp lý

Mặc dù khung pháp lý về bảo vệ DLCN ở Việt Nam đã có nhiều thay đổi tích cực, việc kiểm soát dữ liệu trong lĩnh vực TCS vẫn được điều chỉnh bởi các văn bản dưới luật, dẫn đến sự bất ổn pháp lý và chi phí tuân thủ cho các công ty Fintech, đặc biệt là trong xử lý dữ liệu xuyên biên giới, trong khi cơ chế thực thi và giám sát dữ liệu vẫn chưa được phối hợp. Theo UNCTAD, có rất ít nguồn lực cho cơ chế giám sát và phối hợp dữ liệu quốc tế để kiểm soát các công ty công nghệ xuyên quốc gia [29]. Việt Nam hiện gặp khó khăn trong kiểm soát hoạt động xử lý dữ liệu xuyên biên giới của các nền tảng công nghệ tài chính.

AI trong đánh giá tín dụng, phân tích hành vi tiêu dùng và cá nhân hóa dịch vụ tài chính cũng đặt ra những rủi ro về phân biệt đối xử theo thuật toán và khai thác dữ liệu quá mức. Các hệ thống AI thiếu minh bạch và thiên vị dữ liệu (thiên vị thuật toán) có thể dẫn đến sự bất bình đẳng trong việc tiếp cận tín dụng số và nguy cơ loại trừ tài chính đối với một số nhóm người dùng nhất định. Pháp luật Việt Nam hiện vẫn chưa xây dựng đầy đủ cơ chế kiểm toán thuật toán, minh bạch hóa quyết định tự động và trách nhiệm giải trình AI trong lĩnh vực TCS.

Dù nền tảng pháp lý quan trọng cho QTDL Việt Nam đã được tạo lập thông qua Luật Bảo vệ DLCN 2025 và Nghị định 356/2025/NĐ-CP nhưng khung pháp lý hiện nay vẫn chưa hình thành đầy đủ cơ chế quản trị chuyên biệt đối với Fintech và AI tài chính. Các vấn đề như quyền được giải thích quyết định tự động, quản trị API trong Open Banking và trách nhiệm giải trình AI vẫn chưa được quy định đầy đủ, tạo ra khoảng trống quản trị trong bối cảnh tài chính dựa trên dữ liệu ngày càng phát triển. Nhiều nghiên cứu tại Việt Nam cũng cho rằng sự phát triển của AI

đang thúc ép hoàn thiện pháp luật về quyền riêng tư, bảo vệ DLCN và trách nhiệm giải trình thuật toán. Pháp luật của Việt Nam cần sớm xây dựng cơ chế quản trị AI minh bạch, tăng cường kiểm soát hoạt động xử lý dữ liệu tự động và bảo đảm quyền của chủ thể dữ liệu trong môi trường AI [14].

3. Định hướng hoàn thiện khung pháp lý bảo vệ dữ liệu cá nhân trong lĩnh vực tài chính số tại Việt Nam

3.1. Hoàn thiện cơ chế pháp lý điều chỉnh dữ liệu tài chính số trên cơ sở Luật Bảo vệ dữ liệu cá nhân

Trong bối cảnh DLCN ngày càng trở thành nguồn tài nguyên chiến lược của nền kinh tế số, Việt Nam cần hoàn thiện cơ chế QTDL theo hướng QTRR và thích ứng linh hoạt thay vì áp dụng mô hình quản lý cứng. Xu hướng lập pháp quốc tế hiện chuyển từ bảo vệ quyền riêng tư truyền thống sang quản trị dữ liệu dựa trên trách nhiệm giải trình và minh bạch thuật toán. Pháp luật cần xác định rõ phạm vi DLCN trong môi trường TCS và tiếp cận theo hướng “quyền kiểm soát dữ liệu” của cá nhân. Xem xét bổ sung nguyên tắc “trách nhiệm giải trình dữ liệu”, yêu cầu ngân hàng số, DN Fintech và nền tảng thanh toán chứng minh tính hợp pháp của hoạt động xử lý dữ liệu. Pháp luật cần bổ sung quyền xóa dữ liệu và quyền phản đối quyết định tự động và “quyền được giải thích” đối với các quyết định thuật toán trong chấm điểm tín dụng và đánh giá rủi ro khách hàng. Đây là nền tảng quan trọng của quản trị AI minh bạch nhằm hạn chế rủi ro từ các mô hình “hộp đen” (black-box AI) trong TCS.

3.2. Thiết lập cơ chế quản lý pháp lý chuyên biệt đối với tài chính số, AI và Open Banking

Khung pháp lý hiện nay chưa thiết lập đầy đủ cơ chế điều chỉnh chuyên biệt cho Fintech và AI tài chính, trong khi TCS vận hành theo mô hình “Tài chính dựa trên dữ liệu”. Cần xây dựng cơ chế pháp lý riêng cho hoạt động xử lý dữ liệu trong Fintech, Open Banking và AI tài chính.

Hoàn thiện quy định về chia sẻ DLTC trong Ngân hàng mở theo nguyên tắc đồng ý minh bạch và có thể rút lại của người dùng, bên cạnh đó, xác định rõ trách nhiệm của ngân hàng, DN Fintech và các bên trung gian khi xảy ra rò rỉ dữ liệu. Cần xây dựng cơ chế kiểm soát AI trong tài

chính, đặc biệt đối với các hệ thống chấm điểm tín dụng và phân tích hành vi khách hàng. Sự thiếu hụt các cơ chế kiểm toán thuật toán và tính minh bạch trong việc ra quyết định tự động có thể dẫn đến thiên vị thuật toán, phân biệt dữ liệu và nguy cơ từ chối dịch vụ tài chính không minh bạch.

Bảng 1: Đề xuất khung pháp luật bảo vệ DLCN trong lĩnh vực TCS ở Việt Nam

Nhóm ưu tiên	Văn bản pháp luật/ cơ chế quản lý	Tình trạng hiện nay	Định hướng bổ sung và hoàn thiện
Ưu tiên cấp bách	Luật Bảo vệ DLCN	Cần hoàn thiện	Hoàn thiện hướng QTRR và thích ứng linh hoạt (<i>risk-based and adaptive regulation</i>), không sao chép nguyên mẫu GDPR. Cần quy định: phân tầng dữ liệu theo mức độ rủi ro; quyền kiểm soát dữ liệu; quyền được giải thích quyết định thuật toán; trách nhiệm giải trình AI; QTDL TCS; cơ chế xử lý dữ liệu xuyên biên giới và trách nhiệm bồi thường vi phạm dữ liệu.
Ưu tiên cấp bách	Quy định về Open Banking/ Open API	Chưa có	Khung pháp lý riêng cho Open Banking, bao gồm: tiêu chuẩn quản trị API, nguyên tắc chia sẻ dữ liệu, xác thực truy cập, bảo mật luồng dữ liệu và cơ chế phân bổ trách nhiệm pháp lý giữa ngân hàng, TCS và bên thứ ba khi xảy ra sự cố dữ liệu.
Ưu tiên cấp bách	Quy định pháp lý về AI tài chính	Chưa có	Quy định <i>Đạo đức AI</i> và <i>Quản trị AI có trách nhiệm</i> , bao gồm: kiểm toán thuật toán, đánh giá tác động AI, giải thích quyết định tự động, chống sai lệch thuật toán và hạn chế nguy cơ loại trừ tài chính.
Ưu tiên cấp bách	Quy định về TCS và Sandbox	Chưa hoàn chỉnh	Hoàn thiện cơ chế Sandbox cho TCS nhằm cân bằng giữa đổi mới sáng tạo và kiểm soát rủi ro dữ liệu. Bổ sung quy định về quản trị dữ liệu, RegTech, SupTech và trách nhiệm an ninh dữ liệu của DN thử nghiệm công nghệ tài chính.
Trung hạn	Luật Các tổ chức tín dụng	Đã có	Bổ sung chương riêng về QTDL ngân hàng số, mô hình “Ba tuyến phòng thủ”, trách nhiệm QTRR dữ liệu và nghĩa vụ thông báo sự cố rò rỉ dữ liệu cho khách hàng và cơ quan quản lý.
Trung hạn	Luật An ninh mạng	Đã có	Hoàn thiện quy định về chủ quyền dữ liệu (<i>data sovereignty</i>) và QTDL chiến lược quốc gia. Việc lưu trữ dữ liệu nội địa nên áp dụng theo hướng phân tầng dữ liệu chiến lược thay vì yêu cầu bản địa hóa đại trà đối với mọi loại DLTC.
Trung hạn	Luật An toàn thông tin mạng	Đã có	Bổ sung tiêu chuẩn kỹ thuật bắt buộc đối với bảo mật DLTC; cơ chế ứng cứu sự cố dữ liệu; đánh giá an ninh dữ liệu định kỳ và kiểm toán hệ thống AI tài chính.
Trung hạn	Luật Giao dịch điện tử 2023	Đã có	Hoàn thiện quy định về eKYC, xác thực sinh trắc học, hợp đồng thông minh và bảo vệ dữ liệu trong giao dịch TCS.
Trung hạn	Luật Cạnh tranh 2018	Đã có nhưng chưa tiếp cận dữ liệu	Bổ sung cơ chế kiểm soát độc quyền dữ liệu và lạm dụng dữ liệu thị trường của các nền tảng số lớn. Cần xem dữ liệu là yếu tố tạo quyền lực thị trường trong nền kinh tế số và bổ sung cơ chế chống độc quyền dữ liệu.
Trung hạn	Luật Bảo vệ quyền lợi NTD	Đã có	Bổ sung quyền dữ liệu số của NTD; quyền từ chối quảng cáo tài chính cá nhân hóa; kiểm soát Thiết kế thao túng (<i>dark pattern design</i>) và cơ chế đồng ý dữ liệu minh bạch.

Dài hạn	Cơ quan giám sát DLCN quốc gia	Chưa có cơ quan độc lập chuyên trách	Thành lập cơ quan bảo vệ DLCN độc lập với chức năng thanh tra, kiểm toán dữ liệu, giám sát AI tài chính và xử lý tranh chấp dữ liệu xuyên biên giới.
Dài hạn	Cơ chế QTDL xuyên biên giới	Chưa đầy đủ	Xây dựng cơ chế QTDL xuyên biên giới phù hợp với CPTPP, EVFTA và xu hướng “Luồng dữ liệu tự do với sự tin cậy” cân bằng giữa tự do lưu chuyển dữ liệu phục vụ thương mại số và yêu cầu bảo vệ chủ quyền dữ liệu quốc gia.
Dài hạn	Luật Công nghệ số/ Luật Công nghiệp công nghệ số	Chưa hoàn thiện toàn diện	Bổ sung quy định về QTDL lớn, đạo đức dữ liệu, trách nhiệm nền tảng AI và quản trị hệ sinh thái TCS dựa trên dữ liệu.

3.3. Hoàn thiện cơ chế kiểm soát dữ liệu xuyên biên giới và chủ quyền dữ liệu quốc gia

Một thách thức lớn hiện nay là DLTC của người Việt Nam ngày càng được lưu trữ và xử lý trên hạ tầng điện toán đám mây xuyên quốc gia do các tập đoàn công nghệ nước ngoài cung cấp. Pháp luật Việt Nam vẫn chưa hoàn thiện cơ chế kiểm soát chuyển dữ liệu xuyên biên giới và bảo đảm chủ quyền dữ liệu quốc gia trong bối cảnh thương mại số và hội nhập quốc tế ngày càng mở rộng. Trong bối cảnh Việt Nam tham gia CPTPP và EVFTA, việc áp dụng cơ chế lưu trữ dữ liệu nội địa (data localization) quá rộng có thể làm gia tăng chi phí vận hành của DN số, hạn chế dòng chảy dữ liệu phục vụ thương mại điện tử và phát sinh xung đột với nguyên tắc tự do lưu chuyển dữ liệu. Khung pháp lý về dữ liệu xuyên biên giới cần được thiết kế theo hướng cân bằng giữa bảo vệ chủ quyền dữ liệu (data sovereignty) và bảo đảm lưu chuyển dữ liệu an toàn phục vụ phát triển kinh tế số.

Cần thiết lập cơ chế pháp lý rõ ràng về điều kiện chuyển DLTC ra nước ngoài. Các hoạt động chuyển dữ liệu cần đáp ứng đầy đủ ba điều kiện: (1) Có sự đồng ý rõ ràng của chủ thể dữ liệu; (2) Có đánh giá tác động chuyển dữ liệu xuyên biên giới; (3) Quốc gia hoặc tổ chức tiếp nhận phải đáp ứng mức độ bảo vệ dữ liệu tương đương. (4) Đối với DLTC nhạy cảm hoặc dữ liệu có liên quan trực tiếp đến an ninh tài chính quốc gia, Việt Nam cần áp dụng cơ chế phân tầng dữ liệu chiến lược nhằm xác định nhóm dữ liệu cần lưu trữ hoặc sao lưu tại Việt Nam. Yêu cầu lưu trữ dữ liệu nội địa không nên áp dụng đại trà mà cần

dựa trên mức độ rủi ro, giá trị chiến lược của dữ liệu và tác động đối với an ninh tài chính quốc gia. Cách tiếp cận này giúp giảm phụ thuộc vào hạ tầng dữ liệu nước ngoài nhưng vẫn bảo đảm tính linh hoạt cho thương mại số và dịch vụ tài chính xuyên biên giới. Cần tăng cường hợp tác quốc tế trong thực thi pháp luật dữ liệu số đối với tội phạm công nghệ cao, gian lận tài chính và mua bán dữ liệu xuyên biên giới.

3.4. Nâng cao cơ chế thực thi pháp luật và trách nhiệm của các doanh nghiệp số

Hiệu quả thực thi pháp luật hiện vẫn là hạn chế đáng kể của cơ chế bảo vệ DLCN tại Việt Nam. Việc mua bán DLCN, rò rỉ dữ liệu khách hàng và khai thác dữ liệu trái phép vẫn tiếp tục diễn ra, và các hình phạt chưa đủ mạnh để ngăn chặn những hành động này. Việt Nam chưa phát triển được hệ sinh thái tuân thủ dữ liệu trong lĩnh vực TCS. Cần phát triển một cơ chế thực thi mạnh mẽ hơn theo các hướng sau: (1) Tăng cường các hình phạt hành chính đối với vi phạm bảo vệ dữ liệu; (2) Bồi thường dân sự cho thiệt hại DLCN; (3) Xem xét trách nhiệm hình sự đối với các hoạt động buôn bán dữ liệu quy mô lớn; (4) Thiết lập cơ chế kiểm tra tuân thủ dữ liệu định kỳ cho các công ty Fintech và ngân hàng số. Cần từng bước thiết lập cơ chế tuân thủ dữ liệu theo chuẩn mực pháp lý quốc tế trong doanh nghiệp tài chính số, chẳng hạn như: vai trò của nhân viên bảo vệ dữ liệu (DPO), cơ chế giám sát tuân thủ nội bộ, hệ thống theo dõi kiểm toán dữ liệu, và kiểm toán dữ liệu định kỳ cho các hệ thống AI và các nền tảng xử lý dữ liệu quy mô lớn.

4. Kết luận

Công nghệ tài chính, ngân hàng mở và AI đang thay đổi cấu trúc hoạt động của hệ thống tài chính hiện đại. Lợi ích của tối ưu hóa dịch vụ cùng với trải nghiệm khách hàng cá nhân hóa và môi trường TCS cũng làm tăng nguy cơ rò rỉ dữ liệu, gian lận tài chính và khai thác thông tin cá nhân quá mức. Bảo vệ DLCN hiện là yêu cầu pháp lý quan trọng nhằm bảo đảm an ninh tài chính và ổn định thị trường số. DLCN trong TCS cần được xem như một phần của quản trị TCS với QTRR dữ liệu và quản trị thuật toán trong hoạt động Fintech và hệ thống AI tài chính. Nhiều hệ thống pháp luật hiện chuyển trọng tâm từ bảo vệ quyền riêng tư sang kiểm soát hoạt động xử lý dữ liệu và trách nhiệm giải trình của chủ thể xử lý dữ liệu.

Tại Việt Nam, hệ thống văn bản pháp luật đã tạo nền tảng pháp lý quan trọng cho QTDL trong môi trường số. Khung pháp lý hiện hành vẫn chưa hoàn thiện cơ chế chuyên biệt đối với Fintech, Open Banking và AI tài chính, đặc biệt liên quan đến dữ liệu xuyên biên giới, trách nhiệm giải trình thuật toán và minh bạch quyết định tự động. Căn cứ vào bối cảnh, nghiên cứu đề xuất Việt Nam tiếp tục hoàn thiện cơ chế QTDL TCS theo hướng QTRR, tăng cường trách nhiệm giải trình thuật toán và nâng cao quyền kiểm soát dữ liệu của người dùng nhằm bảo đảm niềm tin, ổn định tài chính và phát triển bền vững nền kinh tế số.

Tài liệu tham khảo

- [1] Zetzsche DA, Arner DW, Buckley RP. Decentralized finance. *J Financ Regul* 2020;6:172-203. <https://doi.org/10.1093/jfr/fjaa010>.
- [2] Arner D, Barberis J, Buckley R. The evolution of fintech: a new post-crisis paradigm? 2016.
- [3] Zuboff S. Automatefin-fonnate: The two faces of intelligent technology. *Organ Dyn* 1985;14:5-18. [https://doi.org/10.1016/0090-2616\(85\)90033-6](https://doi.org/10.1016/0090-2616(85)90033-6).
- [4] IBM. Cost of a Data Breach Report 2025 The AI Oversight Gap think report. 2025.
- [5] [5] European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). 2016.
- [6] Quốc hội. Luật Bảo vệ dữ liệu cá nhân năm 2025 số 91/2025/QH15. Hà Nội: 2025.
- [7] Chính phủ. Nghị định số 356/2025/NĐ-CP. 2025.
- [8] Yeung K. Algorithmic Regulation: A Critical Interrogation. *Regul Gov* 2018;12:505-23. [https://doi.org/10.1111/\(ISSN\)1748-5991](https://doi.org/10.1111/(ISSN)1748-5991).
- [9] Vũ Công Giao, Lê Trần Như Tuyên. Bảo vệ quyền đối với dữ liệu cá nhân trong pháp luật quốc tế, pháp luật ở một số quốc gia và giá trị tham khảo cho Việt Nam. *Tạp Chí Nghiên Cứu Lập Pháp* 2020.
- [10] Wachter S, Mittelstadt B, Floridi L. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *Int Data Priv Law* 2017;38:50-7. <https://doi.org/10.1609/aimag.v38i3.2741>.
- [11] Chính phủ. Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân. Hà Nội: 2023.
- [12] Kuner C. *Transborder Data Flows and Data Privacy Law*. Oxford University Press; 2013.
- [13] Voigt P, von dem Bussche A. *The EU General Data Protection Regulation (GDPR)* 2017. <https://doi.org/10.1007/978-3-319-57959-7>.
- [14] Trần Thị Thu Phương. Quy định chung của Liên minh châu Âu về bảo vệ dữ liệu cá nhân và một số khuyến nghị đến Quốc hội, Chính phủ và doanh nghiệp Việt Nam. *Tạp Chí Nghiên Cứu Lập Pháp* 2022.
- [15] Phạm Thị Dinh. Quản trị ngân hàng số tại Việt Nam và Liên minh Châu Âu: So sánh chính sách bảo vệ dữ liệu và an ninh mạng trong bối cảnh chuyển đổi số 2025;2A:201-9.
- [16] Attorney-General's Chambers of Singapore. *Personal Data Protection Act 2012*. 2012.
- [17] Greenleaf G. *Asian Data Privacy Laws: Trade and Human Rights Perspectives*. Oxford University Press; 2014.
- [18] Nguyễn Thị Kim Ngân. Pháp luật của một số quốc gia Đông Nam Á về bảo vệ dữ liệu cá nhân và các gợi ý cho Việt Nam. *Tạp Chí Nghiên Cứu Lập Pháp* 2019.
- [19] United States Congress. *Gramm Leach Bliley Act (Public Law 106-102)*. 1999.
- [20] California Legislature. *California Consumer Privacy Act (CCPA)*. 2018.
- [21] People's Republic of China. *Personal Information Protection Law of the People's Republic of China*. 2021.
- [22] Quốc hội. Bộ Luật Dân sự số 91/2015/QH13. 2015.

- [23] Quốc hội. Luật an ninh mạng 116/2025/QH15. 2025.
- [24] Quốc hội. Luật an toàn thông tin mạng. 2015.
- [25] Basel Committee on Banking Supervision. Digitalisation of finance. 2024.
- [26] The Institute of Internal Auditors (IIA). Three lines position paper - IIA sept. 2024 update. 2024.
- [27] Nehru V, Swanson E, Dubey A. A new database on human capital stock in developing and industrial countries: Sources, methodology, and results. *J Dev Econ* 1995;46:379–401. [https://doi.org/10.1016/0304-3878\(94\)00054-G](https://doi.org/10.1016/0304-3878(94)00054-G).
- [28] Bạch Thị Nhã Nam. Hướng tiếp cận và hoàn thiện pháp luật bảo vệ dữ liệu cá nhân tại Việt Nam trước tác động lập pháp của thế giới và khu vực. *Tạp Chí Luật Học* 2022:67–81.
- [29] UNCTAD. Digital economy report 2024.