KHUNG PHÁP LÝ VỀ BẢO VỆ THÔNG TIN KHÁCH HÀNG CỦA TỔ CHỨC TÍN DỤNG TRONG NỀN KINH TẾ SỐ

PHAN LÊ NGỌC CHÂU*

Việc bảo vệ dữ liệu khách hàng của các tổ chức tín dụng trong môi trường kinh tế số đóng vai trò quan trọng trong việc thúc đẩy tài chính, góp phần phát triển bền vững hệ thống tài chính quốc gia. Tại Việt Nam, cùng với sự gia tăng nhanh chóng của các dịch vụ tài chính số, vấn đề bảo vệ dữ liệu cá nhân của khách hàng đã nhận được sự quan tâm ngày càng lớn từ các bên liên quan, song vẫn chưa được ưu tiên đúng mức, đặc biệt trong việc xây dựng và hoàn thiện hệ thống pháp luật điều chỉnh. Bài viết hướng đến việc đánh giá khung pháp lý hiện hành về bảo vệ dữ liệu khách hàng tại các tổ chức tín dụng, dựa trên cơ sở tổng hợp các công trình nghiên cứu trước đây và phân tích các quy định pháp luật đang có hiệu lực.

Từ khóa: *Dịch vụ tài chính; bảo vệ thông tin khách hàng; tổ chức tín dụng; khung pháp lý; Việt Nam.*

The protection of customer data by credit institutions in the digital economy plays an important role in promoting finance and contributing to the sustainable development of the national financial system. In Vietnam, amid the rapid growth of digital financial services, protecting customers' personal data has received increasing attention from stakeholders, yet it has not received adequate priority, particularly in the development and improvement of the legal framework governing digital financial services. The article aims to evaluate the current legal framework for the protection of customer data in credit institutions, based on a synthesis of previous studies and an analysis of the currently applicable legal regulations.

Keywords: *Financial services; customer information protection; credit institutions; legal framework; Vietnam.*

NGÀY NHẬN: 07/01/2026 NGÀY PHẢN BIỆN, ĐÁNH GIÁ: 19/5/2026 NGÀY DUYỆT: 18/6/2026

DOI: https://doi.org/10.59394/qlnn.365.2026.1536

1. Đặt vấn đề

Bảo vệ dữ liệu cá nhân đã trở thành trụ cột của pháp luật quốc tế từ cuối thế kỷ XX, khởi đầu với Nguyên tắc hướng dẫn bảo vệ quyền riêng tư của Tổ chức Hợp tác và Phát triển kinh tế (OECD) năm 1980 (OECD, 2012a)[1] và được nâng tầm khi Liên minh châu Âu (EU) ban hành Quy định chung về bảo vệ dữ liệu năm 2016 - chuẩn mực toàn cầu với phạm vi áp dụng ngoài lãnh thổ và mức phạt tối đa 4% doanh thu toàn cầu (EU, 2016)[2], (GDPR, 2025)[3].

Tại Việt Nam, sự bùng nổ của dịch vụ tài chính số và tài chính khiến dữ liệu khách hàng ngày càng đa dạng song cũng nhạy cảm

* *NCS của Trường Đại học Luật TP. Hồ Chí Minh*

hơn. Khách hàng luôn ở vị thế bất lợi so với tổ chức cung cấp dịch vụ trong việc kiểm soát thông tin cá nhân, khiến họ dễ đối mặt với rủi ro rò rỉ, lạm dụng dữ liệu, thậm chí thiệt hại tài chính nếu không được bảo vệ đầy đủ (Akerlof, 1978)[4]. Vì vậy, bảo vệ dữ liệu cá nhân không chỉ là quyền lợi của riêng khách hàng mà còn là điều kiện thiết yếu cho sự phát triển bền vững của toàn bộ thị trường tài chính (OECD, 2020)[5]. Trong bối cảnh mới này, bài viết tập trung phân tích khung pháp lý và thực trạng bảo vệ dữ liệu cá nhân khách hàng trong lĩnh vực tài chính - ngân hàng tại Việt Nam, từ đó, đóng góp vào việc hoàn thiện pháp luật về bảo vệ dữ liệu cá nhân trong thời gian tới.

2. Lý thuyết về khung pháp lý bảo vệ thông tin khách hàng của tổ chức tín dụng trong nền kinh tế số

Trong bối cảnh số hóa sâu rộng, bảo vệ dữ liệu cá nhân là nội dung cốt lõi bảo đảm quyền con người, sự ổn định của hệ thống tài chính - ngân hàng và niềm tin khách hàng (OECD, 2012a)[6]. Nguyên tắc pháp quyền đòi hỏi mọi hoạt động thu thập, xử lý, chia sẻ dữ liệu phải minh bạch, có giám sát và bồi thường thực chất. Bảo vệ thông tin khách hàng nhằm giải quyết bất cân xứng thông tin giữa khách hàng và tổ chức tín dụng (Akerlof, 1978)[7], từ đó, giảm rủi ro gian lận trong môi trường tài chính số ngày càng phức tạp (OECD, 2018)[8], (Adegbite, 2025)[9].

Dựa vào các tài liệu trên, khung lý thuyết toàn diện về bảo vệ thông tin khách hàng của tổ chức tín dụng trong nền kinh tế số được xây dựng trên 5 nguyên tắc cốt lõi sau:

Một là, minh bạch và tiết lộ thông tin đầy đủ. Theo Akerlof (1978)[10], tổ chức tín dụng phải cung cấp thông tin rõ ràng, dễ hiểu về cách xử lý dữ liệu nhằm giảm bất cân xứng thông tin. Nguyên tắc này hình thành từ *Đạo luật báo cáo tín dụng công bằng* năm 1970 tại Hoa Kỳ, được mở rộng qua *Đạo luật Hiện đại hóa dịch vụ tài chính* năm 1999 và được nâng tầm trong Quy định chung về bảo vệ dữ liệu của EU năm 2016 với yêu cầu thông tin phải "ngắn gọn và dễ hiểu" - phản ánh sự tiến hóa từ bảo vệ thụ động sang minh bạch chủ động (EU, 2016)[11], (GDPR, 2025)[12].

Hai là, đồng ý rõ ràng và quyền kiểm soát của khách hàng. Xử lý dữ liệu phải dựa trên sự đồng ý tự nguyện, có đầy đủ thông tin, kèm theo quyền truy cập và xóa bỏ dữ liệu. Quyền kiểm soát được hoàn thiện qua Quy định chung về bảo vệ dữ liệu năm 2016 với yêu cầu đồng ý "rõ ràng và chủ động" và quyền "được lãng quên", đặc biệt sau sự kiện Cambridge Analytica năm 2018 (EU, 2016)[13], (GDPR, 2025)[14].

Ba là, tối thiểu hóa dữ liệu và giới hạn mục đích sử dụng. Chỉ thu thập dữ liệu ở mức cần thiết và dùng đúng mục đích đã thông báo, ngăn chặn lạm dụng. Nguyên tắc này có nguồn gốc từ *Hướng dẫn Quyền riêng tư* của OECD năm 1980 (sửa đổi năm 2013), được củng cố qua *Chỉ thị bảo vệ dữ liệu* của EU năm 1995 và hoàn thiện trong Quy định chung về bảo vệ dữ liệu năm 2016 với tiêu chí dữ liệu phải "phù hợp, liên quan và giới hạn ở mức cần thiết" (OECD, 2012a)[15], (EU, 2016)[16].

Bốn là, bảo mật và an ninh dữ liệu mạnh mẽ. Tổ chức phải áp dụng các biện pháp kỹ thuật như mã hóa, kiểm soát truy cập để ngăn ngừa rò rỉ dữ liệu (Adegbite, 2025)[17]. Yêu cầu bảo mật liên tục được nâng cấp qua các thời kỳ - đặc biệt sau các vụ rò rỉ lớn, như: Heartland Payment Systems năm 2008 và được chuẩn hóa trong Quy định chung về bảo vệ dữ liệu năm 2016 với nghĩa vụ thông báo vi phạm trong vòng 72 giờ (EU, 2016)[18].

Năm là, trách nhiệm giải trình và thực thi hiệu quả. Tổ chức phải chứng minh tuân thủ và chịu chế tài nghiêm khắc từ cơ quan giám sát độc lập (OECD & G20, 2011)[19]. Cơ chế này phát triển từ các yêu cầu báo cáo tuân thủ đơn giản, đến đỉnh cao là Quy định chung về bảo vệ dữ liệu năm 2016 với các công cụ như đánh giá tác động bảo vệ dữ liệu, cán bộ bảo vệ dữ liệu chuyên trách và mức phạt lên đến 4% doanh thu toàn cầu (EU, 2016)[20], (GDPR,

2025)[21], qua đó khẳng định trách nhiệm giải trình là yêu cầu thiết yếu để bảo đảm tuân thủ bền vững.

3. Khung pháp lý về bảo vệ thông tin khách hàng của tổ chức tín dụng trong nền kinh tế số tại Việt Nam

Bảo vệ thông tin khách hàng của tổ chức tín dụng trong nền kinh tế số là yếu tố cốt lõi bảo đảm an toàn, minh bạch và ổn định hệ thống tài chính; đồng thời, củng cố niềm tin khách hàng và thúc đẩy phát triển kinh tế số bền vững. Theo đó, có bốn giai đoạn chính sau:

(1) *Giai đoạn khởi đầu (2006 - 2017):* nền tảng manh mún, thiếu hệ thống. Pháp luật tiếp cận bảo vệ dữ liệu theo hướng phân tán qua *Luật Giao dịch điện tử* năm 2005, *Luật Công nghệ thông tin* năm 2006 và *Luật Các tổ chức tín dụng* năm 2010. Các văn bản này chỉ đặt ra nghĩa vụ bảo mật chung, chưa định nghĩa dữ liệu cá nhân, chưa phân loại mức độ nhạy cảm và chưa có quyền chủ thể dữ liệu - phản ánh thực trạng chung của nhiều quốc gia đang phát triển thời kỳ chưa chịu áp lực số hóa đủ lớn. Tuy nhiên, đây là giai đoạn Việt Nam bắt đầu tiếp cận Nguyên tắc Hướng dẫn quyền riêng tư của OECD[22] và khuyến nghị của Ngân hàng Thế giới (WB)[23] về bảo vệ người tiêu dùng tài chính, tạo tiền đề tư duy cho các cải cách tiếp theo.

(2) *Giai đoạn củng cố (2018 - 2022):* từ kinh nghiệm quốc tế, xây khung cưỡng chế. *Luật An ninh mạng* năm 2018 tạo ra khung pháp lý an toàn thông tin có tính bắt buộc. Tuy nhiên, các nghiên cứu so sánh đã chỉ ra, khung pháp lý giai đoạn này của Việt Nam, (tương tự nhiều quốc gia Đông Nam Á cùng thời điểm vẫn thiếu ba yếu tố mà OECD (2018)[24], WB (2017a)[25] coi là bắt buộc với một hệ thống bảo vệ dữ liệu hiệu quả: quyền chủ thể dữ liệu rõ ràng, cơ quan giám sát độc lập và cơ chế bồi thường thực chất. Đây là khoảng trống pháp lý được ghi nhận nhất quán trong các đánh giá học thuật về hệ thống pháp luật dữ liệu Việt Nam trước năm 2023 (Tran et al., 2024)[26], (Asia Legal, 2025)[27].

(3) *Giai đoạn pháp luật hóa (2023 - 2024):* tiệm cận chuẩn mực toàn cầu. Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ là bước ngoặt quan trọng, lần đầu tiên Việt Nam có văn bản chuyên biệt định nghĩa dữ liệu nhạy cảm (bao gồm: thông tin định danh, tài khoản và giao dịch ngân hàng), quy định nguyên tắc xử lý dữ liệu, nghĩa vụ báo cáo vi phạm và điều kiện chuyển dữ liệu ra nước ngoài (tại Điều 2, Điều 9, Điều 23, Điều 24). Nghị định số 13/2023/NĐ-CP thực chất là sự kết hợp giữa hai mô hình pháp lý: mô hình châu Âu (nguyên tắc tối thiểu hóa dữ liệu, giới hạn mục đích và trách nhiệm giải trình từ Quy định chung về bảo vệ dữ liệu) và mô hình Hoa Kỳ (tiếp cận theo ngành, linh hoạt về cơ chế tuân thủ) được điều chỉnh phù hợp đặc thù quản trị trong nước (Tran et al., 2024)[28]. Tiếp đến, Thông tư số 50/2024/TT-NHNN ngày 31/10/2024 của Ngân hàng Nhà nước Việt Nam đã cụ thể hóa yêu cầu bảo mật ngân hàng số theo hướng áp dụng tiêu chuẩn ISO/IEC 27001 và khung an ninh mạng NIST vào quy định ngành tài chính (Điều 5 - 8). Tuy nhiên, điểm hạn chế của Nghị định số 13/2023/NĐ-CP còn thiếu nền tảng luật chuyên ngành làm trụ cột, khiến hiệu lực thực thi còn bị giới hạn và khoảng trống này được nhiều nhà nghiên cứu pháp lý quốc tế nêu ra (Oxford Internet Policy, 2025)[29], (Future of Privacy Forum, 2025)[30].

(4) *Giai đoạn định hình thể chế (từ năm 2025):* kiến tạo kỷ nguyên mới. *Luật Bảo vệ dữ liệu cá nhân* năm 2025 (có hiệu lực từ ngày 01/01/2026) đánh dấu sự trưởng thành vượt bậc, từ bảo vệ phân tán, thụ động sang bảo vệ toàn diện và có hệ thống. Phân tích của Oxford Internet Policy (2025)[31] nhận định đây là văn bản pháp lý toàn diện nhất từ trước đến nay của Việt Nam, xác lập tám nguyên tắc cốt lõi tương đồng với Quy định chung về bảo vệ dữ liệu: hợp pháp, minh bạch, giới hạn mục đích, tối thiểu hóa, chất lượng dữ liệu, toàn vẹn, bảo mật và trách nhiệm giải trình (Điều 4 *Luật Bảo vệ dữ liệu cá nhân* năm 2025).

Về mặt kỹ thuật lập pháp, *Luật Bảo vệ dữ liệu cá nhân* năm 2025 kế thừa có chọn lọc từ ba nguồn kinh nghiệm quốc tế: cấu trúc quyền chủ thể từ Quy định chung về bảo vệ dữ liệu của EU; cơ chế xuyên biên giới từ Quy tắc bảo vệ dữ liệu xuyên biên giới APEC và cách tiếp cận dựa trên rủi ro từ *Luật Bảo vệ dữ liệu cá nhân* của Singapore (PDPA 2012, sửa đổi 2021)[32] đã tạo mô hình hài hòa phù hợp vị trí của Việt Nam trong chuỗi giá trị số toàn cầu (Nguyen et al., 2024)[33], (Future of Privacy Forum, 2025)[34]. Đáng chú ý, *Luật Bảo vệ dữ liệu cá nhân* năm 2025 bổ sung căn cứ xử lý dữ liệu dựa trên "lợi ích hợp pháp", tiệm cận Quy định chung về bảo vệ dữ liệu và lần đầu tiên đưa vào khái niệm pháp lý về mã hóa và khử nhận dạng, tạo nền tảng kỹ thuật pháp lý cho ứng dụng trí tuệ nhân tạo (AI) và điện toán đám mây trong ngân hàng số (Điều 9, Điều 27). Nghị định số 356/2025/NĐ-CP ngày 31/12/2025 của Chính phủ hướng dẫn thi hành chi tiết, mở rộng phạm vi dữ liệu nhạy cảm và đặt nền tảng kiểm soát AI trong bảo vệ dữ liệu (Điều 3, Điều 5 và Điều 12).

Như vậy, khung pháp lý bảo vệ thông tin khách hàng của tổ chức tín dụng trong nền kinh tế số Việt Nam mang đặc trưng phân tán theo ngành và tích hợp đa tầng - một đặc điểm không phải riêng Việt Nam mà được ghi nhận ở nhiều quốc gia đang phát triển trong giai đoạn chuyển đổi số (Nguyen et al., 2024)[35]. Thay vì có một văn bản tách riêng bảo vệ người tiêu dùng tài chính số, pháp luật Việt Nam xây dựng theo mô hình khung chuyên ngành lồng ghép: *Luật Bảo vệ quyền lợi người tiêu dùng* năm 2023 đặt nền tảng quyền chung, trong khi bảo vệ dữ liệu cụ thể được điều chỉnh từ hệ thống luật chuyên ngành, gồm: *Luật Các tổ chức tín dụng* năm 2024, *Luật Dữ liệu* năm 2024, *Luật Bảo vệ dữ liệu cá nhân* năm 2025 và các văn bản hướng dẫn, như: Nghị định số 13/2023/NĐ-CP, Nghị định 356/2025/NĐ-CP, Thông tư số 50/2024/TT-NHNN. Trong nghiên cứu của Nguyen et al. (2024)[36] chỉ ra sự phân tán quy định trên 19 văn bản pháp lý khác nhau trước năm 2023 là nguyên nhân căn bản, dẫn đến khoảng trống thực thi và xung đột pháp lý trong lĩnh vực tài chính số.

4. Thực trạng bảo vệ thông tin khách hàng của tổ chức tín dụng trong nền kinh tế số hiện nay

Luật Bảo vệ dữ liệu cá nhân năm 2025 quy định các nguyên tắc cốt lõi, như: hợp pháp, minh bạch, giới hạn mục đích, tối thiểu hóa dữ liệu, chính xác, toàn vẹn, bảo mật và trách nhiệm. Các tổ chức tín dụng tại Việt Nam đã tăng cường bảo vệ thông tin khách hàng trong nền kinh tế số. Đến tháng 11/2025, ngành Ngân hàng đã xác thực hơn 137 triệu hồ sơ khách hàng cá nhân theo Đề án 06, góp phần nâng cao an ninh dữ liệu[37]. Các biện pháp cụ thể bao gồm: (1) Áp dụng xác thực sinh trắc học (vân tay, khuôn mặt) bắt buộc cho giao dịch chuyển khoản từ 10 triệu VND/lần hoặc 20 triệu VND/ngày[38]; (2) Sử dụng tiêu chuẩn quốc tế như ISO/IEC 27001, PCI DSS, NIST CFS để bảo mật hệ thống ngân hàng số[39]; (3) Giám sát và phát hiện gian lận: hệ thống của Ngân hàng Nhà nước Việt Nam đã cảnh báo gần 600.000 tài khoản có dấu hiệu lừa đảo, bảo vệ hơn 2.780 tỷ VND và 2,26 triệu khách hàng[40]. Đối với dữ liệu tín dụng, Ngân hàng Nhà nước Việt Nam khẳng định hệ thống của các tổ chức tín dụng hoạt động độc lập với Trung tâm Thông tin Tín dụng Quốc gia (CIC) nhưng vẫn yêu cầu đánh giá tác động khi chuyển giao dữ liệu.

Năm 2025, chứng kiến nhiều vụ rò rỉ dữ liệu nghiêm trọng, ảnh hưởng đến niềm tin của khách hàng và chỉ trong 6 tháng đầu năm, gần 8,5 triệu tài khoản người dùng Việt Nam bị đánh cắp, chiếm 1,7% toàn cầu, với 191 trường hợp bán dữ liệu, gấp ba lần năm 2024. Nổi bật là vụ hack CIC vào tháng 9/2025: nhóm hacker Shiny Hunters tuyên bố bán hơn 160 triệu hồ sơ, bao gồm dữ liệu cá nhân và tài chính từ 52 triệu khách hàng cá nhân và 1,2 triệu doanh nghiệp; vụ việc này yêu cầu các tổ chức tín dụng phải thông báo cho cơ

quan chức năng và khách hàng nếu dữ liệu bị ảnh hưởng; tội phạm mạng ngày càng tinh vi, với 155 triệu hồ sơ bị rò rỉ và 4,5 triệu tài khoản bị xâm phạm, tăng 21% so với năm trước[41]. Bên cạnh đó, thiếu đồng bộ pháp lý giữa các luật, tiêu chuẩn dữ liệu chưa thống nhất và chế tài chưa đủ mạnh so với quốc tế (như GDPR), trong khi công nghệ phát triển nhanh (AI, Blockchain, điện toán đám mây) vượt quá tốc độ cập nhật quy định, dẫn đến lỗ hổng trong chuyển giao dữ liệu xuyên biên giới[42].

Kết quả cho thấy, tiến bộ đáng ghi nhận trong pháp lý và kỹ thuật nhưng thách thức lớn vẫn còn từ tội phạm mạng ngày càng tinh vi. Thực trạng bảo vệ thông tin khách hàng của tổ chức tín dụng tại Việt Nam đến cuối năm 2025 đang trong giai đoạn chuyển tiếp và được quy định rõ trong *Luật Bảo vệ dữ liệu cá nhân* năm 2025, tuy nhiên, cần được thực thi mạnh mẽ hơn để đối phó hiệu quả với các rủi ro của kinh tế số.

5. Một số khuyến nghị chính sách

Trong bối cảnh nền kinh tế số phát triển với tốc độ chưa từng có, bảo vệ thông tin khách hàng của tổ chức tín dụng không còn là vấn đề kỹ thuật hay thủ tục hành chính đơn thuần. Đây là yêu cầu sống còn đối với sự ổn định của hệ thống tài chính quốc gia, là điều kiện tiên quyết duy trì niềm tin xã hội vào khu vực ngân hàng và là thước đo năng lực quản trị nhà nước trong kỷ nguyên dữ liệu toàn cầu. Để nâng cao hiệu quả bảo vệ thông tin khách hàng và bảo đảm quyền dữ liệu cá nhân, cần có những cải cách pháp lý và chính sách công toàn diện.

Một là, tăng cường tính pháp điển hóa hệ thống pháp luật. Cần cụ thể hóa *Luật Bảo vệ dữ liệu cá nhân* năm 2025 bằng một nghị định hướng dẫn thống nhất, tránh việc mỗi bộ, ngành ban hành quy định riêng. Theo đó, ban hành Bộ Quy tắc ứng xử ngành Ngân hàng để điều chỉnh các vấn đề đặc thù: (1) Lưu trữ dữ liệu tín dụng; (2) Phân tích hành vi tiêu dùng; (3) Chia sẻ với công ty bảo hiểm. Bên cạnh đó, xây dựng điều khoản hợp đồng mẫu cho tất cả các giao dịch chuyển dữ liệu qua biên giới, từng bước pháp điển hóa toàn bộ quy định vào *Bộ luật Bảo vệ dữ liệu cá nhân* trong tương lai, nâng tính dự báo, tiên liệu và ổn định.

Hai là, thiết lập cơ quan giám sát dữ liệu độc lập (DPA). Thành lập Cơ quan Bảo vệ dữ liệu quốc gia (Vietnam DPA) trực thuộc Chính phủ (đại diện Việt Nam trong các khuôn khổ hợp tác dữ liệu quốc tế, như: APEC, CBPR với EU) nhưng có cơ chế hoạt động độc lập, cụ thể về chức năng giám sát tuân thủ của tài chính tín dụng; tiếp nhận khiếu nại từ cá nhân; ban hành hướng dẫn kỹ thuật; hợp tác quốc tế về chuyển dữ liệu xuyên biên giới; bảo đảm ngân sách độc lập; nhân sự chuyên môn để tránh xung đột lợi ích. Đây là mắt xích còn thiếu duy nhất trong toàn bộ hệ thống giám sát hiện tại.

Ba là, hài hòa pháp luật Việt Nam với chuẩn mực quốc tế. Tiếp tục sửa đổi, bổ sung *Luật An ninh mạng, Luật Giao dịch điện tử* để phù hợp với chuẩn quốc tế, như: xây dựng cơ chế SCCs (Điều khoản hợp đồng mẫu) cho chuyển dữ liệu ra nước ngoài; quy định công nhận BCRs (Quy tắc nội bộ ràng buộc) cho tập đoàn đa quốc gia cũng như quy định về áp dụng và công nhận chuẩn ISO/IEC 27001/27701, PCI DSS, NIST Privacy Framework. Trước mắt, cần tăng mức phạt vi phạm lên tương đương 2 - 4% doanh thu hằng năm của tổ chức, công khai danh sách vi phạm trên cổng thông tin quốc gia và bắt buộc báo cáo đánh giá tác động bảo vệ dữ liệu định kỳ.

Bốn là, đổi mới chính sách công hỗ trợ thực thi. Chú trọng việc ban hành hướng dẫn kỹ thuật chi tiết: mã hóa, xác thực đa yếu tố, phân quyền truy cập; đồng thời, chuẩn hóa quy trình theo PDCA (Plan-Do-Check-Act). Bên cạnh đó, thành lập Quỹ hỗ trợ bảo mật dữ liệu với nguồn lực ưu tiên cho các tổ chức tín dụng nhỏ (đây là khu vực dễ tổn thương nhất nhưng lại ít được hỗ trợ nhất); tiếp tục đào tạo nhân lực pháp chế, công nghệ thông tin và cấp chứng chỉ nghề bắt buộc (chứng

chỉ ISO 27001/27701) cho toàn bộ ngân hàng số đến năm 2027 và đào tạo đội ngũ cán bộ bảo vệ dữ liệu chuyên trách không phải là chi phí mà đó là khoản đầu tư có tỷ suất sinh lời cao nhất trong thời đại dữ liệu. Tiếp tục phát triển cổng thông tin giám sát cộng đồng để khách hàng báo cáo vi phạm dữ liệu khi thực hiện giao dịch.

6. Kết luận

Như vậy, với việc phân tích và đưa ra các khuyến nghị, bài viết khẳng định, cải cách pháp lý hiệu quả phải tiến hành đồng thời trên cả thể chế, pháp luật và kỹ thuật, không thể làm riêng lẻ từng phần. Thực tế, mỗi vụ rò rỉ dữ liệu ngân hàng không chỉ gây thiệt hại tài chính tức thời mà còn gây xói mòn đến sự tin tưởng của khách hàng. Ngược lại, mỗi bước hoàn thiện khung pháp lý đều tích lũy thêm niềm tin đó. Khi khách hàng thực sự được bảo vệ, khu vực tài chính sẽ bền vững hơn, tài chính toàn diện sẽ sâu rộng hơn và kinh tế số Việt Nam sẽ có nền móng vững chắc để đóng góp 2 - 3% tổng sản phẩm quốc nội vào năm 2030. Chính vì vậy, khi khung pháp lý về bảo vệ dữ liệu, đặc biệt là bảo vệ thông tin khách hàng của tổ chức tín dụng mạnh mẽ đó chính là điều kiện để phát triển trong nền kinh tế số bền vững❐

Chú thích:

1, 6, 15, 22. OECD (2012a). *G20 high-level principles on financial consumer protection.* OECD Publishing, tr. 7 - 16.

2, 11, 13, 16, 18, 20. EU (2016). *Quy định chung về bảo vệ dữ liệu (General Data Protection Regulation - GDPR).*

3, 12, 14, 21. GDPR.eu (2025). *Tóm tắt quy định bảo vệ dữ liệu chung (General Data Protection Regulation)*, tr. 1 - 8.

4, 7, 10. Akerlof, G. A. (1978). *The market for "lemons": Quality uncertainty and the market mechanism.* In Uncertainty in economics (pp. 235 - 251). Academic Press.

5. OECD (2020). *Financial consumer protection policy approaches in the digital age: Protecting consumers' assets, data and privacy.* OECD Publishing, tr. 11 - 14.

8, 24. OECD (2018). *G20/OECD policy guidance on financial consumer protection approaches in the digital age.* OECD Publishing, tr. 21 - 25.

9, 17. Adegbite, M. A. (2025). *Data privacy and data security challenges in digital finance.* Journal of Digital Security and Forensics, 2(1), tr. 4 - 17.

19. OECD & G20 (2011). *High-level principles on financial consumer protection.* OECD Publishing, tr. 9 - 12.

23. World Bank (2013). *Global financial inclusion and consumer protection (FICP) survey.* World Bank, tr. 3 - 5.

25. World Bank (2017a). *Good practices for financial consumer protection.* World Bank, tr. 15 - 18.

26, 28. Tran, T. T., et al. (2024). *Some legal aspects of personal data protection in the world - experience for Vietnam.* Cogent Social Sciences, 10(1). https://doi.org/10.1080/23311886.2024.2414872, tr. 6 - 9.

27. *Comparative analysis of Vietnam draft law on personal data protection and GDPR and their impact on the legal framework.* https://asialegal.vn, truy cập ngày 08/3/2026, tr. 2 - 5.

29, 31. Oxford Internet Policy (2025). *Latent policies for the codification of Vietnamese personal data protection law.* International Data Privacy Law. https://doi.org/10.1093/idpl/ipaf013, tr. 8 - 11.

30, 34. Future of Privacy Forum (2025, December). *Making sense of Vietnam's latest data protection and governance regime.* https://fpf.org, truy cập ngày 08/3/2026.

32. PDPA 2012 (sửa đổi 2021). *Đạo luật Bảo vệ dữ liệu cá nhân của Singapore.* (Personal Data Protection Act - PDPA).

33, 35, 36. *Addressing fragmentation in Vietnam's data protection laws: A comparative analysis with GDPR and ASEAN frameworks.* https://reference-global.com, truy cập ngày 08/3/2026.

37. *Đề án 06 tạo chuyển biến mạnh: Ngân hàng xác thực hơn 137 triệu hồ sơ khách hàng.* https://thoibaotaichinhvietnam.vn, ngày 27/11/2025.

38. *Bảo vệ tài khoản khách hàng trong thời đại kinh tế số.* https://tuoitre.vn, ngày 14/6/2025.

39, 42. *Data confidentiality and privacy in e-banking services: Legal perspectives and current practices in Vietnam.* https://vietnamlawmagazine.vn, ngày 12/6/2025.

40. *Phát hiện gần 600.000 tài khoản ngân hàng có dấu hiệu lừa đảo.* https://www.vietnamplus.vn, ngày 25/12/2025.

41. *Rò rỉ dữ liệu - Bóng ma ám ảnh doanh nghiệp.* https://baodautu.vn, ngày 22/9/2025.