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

***Phạm Thị Dinh*[1]**
Email: phamdinhcnsh@hou.edu.vn

Ngày tòa soạn nhận được bài báo: 19/05/2025
Ngày phản biện đánh giá: 21/07/2025
Ngày bài báo được duyệt đăng: 29/08/2025

DOI: 10.59266/houjs.2025.695

Tóm tắt: *Trong bối cảnh chuyển đổi kinh tế số, ngân hàng số đang trở thành trụ cột quan trọng của hệ thống tài chính tại Việt Nam. Tuy nhiên, sự phát triển nhanh chóng này cũng đặt ra yêu cầu cấp thiết về hai yếu tố then chốt đảm bảo sự bền vững của ngân hàng số bao gồm quản trị dữ liệu cá nhân và an ninh mạng. Bài viết này tiến hành so sánh khung pháp lý liên quan đến bảo mật dữ liệu và an ninh mạng giữa Việt Nam và Liên minh Châu Âu (EU), tập trung vào các văn bản như Nghị định 13/2023/NĐ-CP, Luật An ninh mạng tại Việt Nam và GDPR, DORA tại EU. Thông qua việc phân tích các điểm khác biệt về chế tài, quyền người dùng, cơ chế giám sát và phản ứng với sự cố dữ liệu, bài viết chỉ ra những khoảng trống chính sách tại Việt Nam. Bên cạnh đó, một số trường hợp thực tiễn từ ngân hàng số Việt Nam cũng được phân tích để làm rõ mức độ tuân thủ và ứng dụng. Trên cơ sở đó, bài viết đề xuất một số khuyến nghị cụ thể và có tính khả thi nhằm hoàn thiện khung pháp lý và nâng cao năng lực ứng phó với rủi ro an ninh mạng trong bối cảnh ngân hàng số ngày càng phổ biến.*

Từ khóa*: an ninh mạng, bảo vệ dữ liệu, DORA, GDPR, ngân hàng số*

I. Mở đầu

Trong làn sóng chuyển đổi số toàn cầu, ngành ngân hàng đang đóng vai trò tiên phong trong việc ứng dụng công nghệ nhằm tối ưu hóa hoạt động và nâng cao trải nghiệm khách hàng. Tại Việt Nam, ngân hàng số đang phát triển mạnh mẽ nhờ sự kết hợp giữa tiến bộ công nghệ, sự gia tăng người dùng Internet và định hướng chiến lược của Chính phủ trong phát triển kinh tế số với sự ra đời của các ngân hàng số như TNEX, Cake by VPBank, Timo, cùng sự nâng cấp ứng dụng số tại các ngân hàng truyền thống như Vietcombank, MB Bank, Techcombank. Theo báo cáo của Boston Consulting Group (2024), Việt Nam là một trong những thị trường ngân hàng số tăng trưởng nhanh nhất Đông Nam Á, với tỷ lệ giao dịch số chiếm hơn 90% tại nhiều ngân hàng thương mại (Boston Consulting Group, 2024).

Tuy nhiên, cùng với tốc độ phát triển đó là nhu cầu ngày càng cấp thiết trong việc xây dựng môi trường pháp lý phù hợp

[1] Trường Đại học Mở Hà Nội

nhằm đảm bảo an toàn dữ liệu người dùng, bảo vệ quyền riêng tư, và tăng cường năng lực phòng ngừa, phản ứng trước các rủi ro số. Bởi lẽ, trong ngân hàng số, mọi hoạt động đều xoay quanh hạ tầng công nghệ và dữ liệu cá nhân - những yếu tố rất dễ bị tổn thương nếu thiếu cơ chế giám sát và bảo vệ phù hợp. Tại Việt Nam, mặc dù đã ban hành một số văn bản pháp lý quan trọng như Luật An ninh mạng (2018) và Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, nhưng việc thực thi và giám sát vẫn còn nhiều thách thức (Government of Vietnam, 2023).

Việc lựa chọn Liên minh Châu Âu (EU) làm đối tượng so sánh trong bài viết này xuất phát từ một số lý do sau:

Trước hết, EU là khu vực tiên phong trong việc ban hành các văn bản pháp lý toàn diện và chi tiết về bảo vệ dữ liệu cá nhân cũng như quản trị rủi ro kỹ thuật số trong lĩnh vực tài chính. Hai văn bản nổi bật là Quy định Bảo vệ Dữ liệu Chung (GDPR) và Đạo luật Khả năng Phục hồi Kỹ thuật số (DORA) không chỉ có phạm vi áp dụng rộng mà còn có ảnh hưởng lớn đến chính sách của nhiều quốc gia khác, kể cả ngoài châu Âu.

Khác với Hoa Kỳ, nơi có hệ thống pháp luật phân quyền theo từng bang, hoặc các quốc gia châu Á, nơi khung pháp lý còn đang trong quá trình hình thành, EU là một trong số ít khu vực có cơ chế điều phối pháp luật tập trung, có cơ quan giám sát chuyên biệt, và các chế tài cụ thể, rõ ràng. Điều này tạo điều kiện thuận lợi để quan sát một mô hình khung pháp lý "liên quốc gia" với tính thực thi cao và nhiều kinh nghiệm đã được ghi nhận.

Bên cạnh đó, Việt Nam và EU cũng có mối quan hệ hợp tác ngày càng sâu rộng về kinh tế và pháp lý, đặc biệt sau khi Hiệp định thương mại tự do Việt Nam - EU (EVFTA) và Hiệp định bảo hộ đầu tư EVIPA được ký kết. Điều này khiến cho việc tham khảo chính sách của EU trở nên thiết thực và có cơ sở để vận dụng chọn lọc phù hợp với bối cảnh trong nước.

Với những lý do trên, việc phân tích khung pháp lý của EU không nhằm đề cao hay áp đặt một mô hình pháp lý cụ thể, mà là để đưa ra một nguồn tham chiếu có tính thực tiễn cao, từ đó giúp gợi mở định hướng xây dựng chính sách tại Việt Nam theo cách linh hoạt và phù hợp hơn với điều kiện phát triển trong nước.

Bài viết này tập trung so sánh khung pháp lý giữa Việt Nam và EU, đồng thời phân tích thực tiễn triển khai và đề xuất một số giải pháp phù hợp cho Việt Nam.

II. Cơ sở lý luận

Nghiên cứu này được xây dựng trên các nền tảng lý thuyết sau:

Quản trị dữ liệu (Data Governance): Đây là quá trình quản lý sự sẵn có, khả năng sử dụng, tính toàn vẹn và tính bảo mật của dữ liệu trong một tổ chức. Các nguyên tắc cốt lõi của quản trị dữ liệu bao gồm tính minh bạch, trách nhiệm giải trình, và bảo vệ dữ liệu, vốn là trọng tâm của các quy định như GDPR.

Khả năng phục hồi hoạt động kỹ thuật số (Digital Operational Resilience): Lý thuyết này nhấn mạnh khả năng của một tổ chức trong việc xây dựng, đảm bảo và kiểm thử năng lực công nghệ để chống chịu, phản ứng và phục hồi sau các sự cố vận hành kỹ thuật số. Đây là triết lý trung tâm của DORA, mở rộng từ an ninh mạng truyền thống sang quản lý rủi ro toàn diện từ bên thứ ba và khả năng vận hành liên tục.

Lý thuyết về quyền riêng tư (Privacy Theory): Quyền riêng tư được công nhận là một quyền cơ bản của con người, bao gồm quyền kiểm soát thông tin cá nhân của một người. Nghị định 13/2023/NĐ-

CP và GDPR đều thể hiện rõ nguyên tắc này khi trao cho người dùng các quyền như quyền được biết, quyền truy cập, và quyền xóa dữ liệu.

III. Phương pháp nghiên cứu

Để đạt được mục tiêu đề ra, bài viết sử dụng phương pháp so sánh luật học (Comparative Legal Analysis). Đây là phương pháp chủ đạo, được dùng để đối chiếu, phân tích các điểm tương đồng và khác biệt giữa hệ thống pháp luật của Việt Nam (Luật An ninh mạng, Nghị định 13/2023/NĐ-CP, Thông tư 09/2020/TT-NHNN) và EU (GDPR, DORA).

Ngoài ra bài viết còn sử dụng phương pháp nghiên cứu tài liệu (documentary), tổng hợp và phân tích thông tin từ các nguồn tài liệu đa dạng, bao gồm: văn bản pháp quy, các báo cáo chuyên ngành của cơ quan quản lý nhà nước (Bộ Thông tin và Truyền thông, Ngân hàng Nhà nước) và các tổ chức quốc tế (BCG, EIOPA), cũng như các báo cáo an ninh mạng của các công ty công nghệ uy tín.

Các ví dụ thực tiễn từ hoạt động của ngân hàng số tại Việt Nam như TNEX, Cake by VPBank, MB Bank được sử dụng để minh họa cho sự tác động của khung pháp lý đến thực tiễn triển khai và những thách thức còn tồn tại.

IV. Kết quả nghiên cứu và thảo luận

4.1. Đối chiếu khung pháp lý giữa Việt Nam và Liên minh Châu Âu

4.1.1. Khung pháp lý: Định hướng chung nhưng khác biệt về cấu trúc

Cả Việt Nam và EU đều nhận thức rõ tầm quan trọng của việc xây dựng cơ chế pháp lý cho hoạt động ngân hàng số. Trong khi EU đã hình thành một hệ thống văn bản điều chỉnh đồng bộ, nổi bật là GDPR và DORA, thì tại Việt Nam, các quy định liên quan chủ yếu nằm trong Luật An ninh mạng (2018), Thông tư 09/2020/TT-NHNN, và gần đây là Nghị định 13/2023/NĐ-CP. Các văn bản tại Việt Nam đã thể hiện rõ nỗ lực cập nhật trước bối cảnh chuyển đổi số, đặc biệt trong việc xác lập nguyên tắc xử lý dữ liệu và nâng cao yêu cầu kỹ thuật bảo vệ thông tin. Tuy nhiên, các quy định này vẫn đang được triển khai từng bước và chưa tích hợp thành một khung pháp lý thống nhất dành riêng cho lĩnh vực ngân hàng số.

4.1.2. Giám sát và ứng phó rủi ro: Khác biệt về cơ chế báo cáo và quản lý chuỗi cung ứng

Một trong những điểm khác biệt đáng chú ý là cơ chế giám sát và phản ứng với các rủi ro kỹ thuật số. Tại EU, về báo cáo sự cố, GDPR yêu cầu các tổ chức tài chính buộc phải có quy trình báo cáo sự cố trong vòng 72 giờ, thực hiện kiểm thử định kỳ, và tuân thủ chế tài rõ ràng dưới sự giám sát của các cơ quan chuyên trách. Về quản lý bên thứ 3, DORA đưa ra các quy định nghiêm ngặt đối với việc giám sát nhà cung cấp dịch vụ công nghệ thông tin (ICT), yêu cầu các tổ chức tài chính phải đánh giá rủi ro và chịu trách nhiệm trực tiếp đối với các rủi ro phát sinh từ chuỗi cung ứng công nghệ.

Tại Việt Nam, việc giám sát được thực hiện bởi nhiều cơ quan với vai trò khác nhau. Dù hệ thống này phù hợp với cấu trúc quản lý hiện hành, nhưng trong thực tế triển khai, nhiều tổ chức tài chính vẫn đang trong quá trình hoàn thiện năng lực ứng phó. Tương tự quy định 72 giờ của GDPR, Việt Nam cũng đã chính thức áp dụng khung thời gian này cho việc báo cáo vi phạm dữ liệu cá nhân (theo Điều 24, Nghị định 13/2023/NĐ-CP). Tuy nhiên, điểm khác biệt cốt lõi nằm ở cơ chế thực thi và cơ quan tiếp nhận. Trong khi GDPR yêu cầu báo cáo cho một cơ quan bảo vệ dữ liệu độc lập (DPA), thì

quy định của Việt Nam yêu cầu thông báo cho Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao của Bộ Công an và có thể thêm các cơ quan quản lý nhà nước chuyên ngành. Điều này có thể tạo ra thách thức về tính đồng bộ và thống nhất trong phối hợp xử lý sự cố trên diện rộng, đặc biệt trong các tình huống có liên quan đến nhiều ngành nghề và địa phương khác nhau. Về quản lý bên thứ ba, Thông tư 09/2020/TT-NHNN của Ngân hàng Nhà nước đã đề cập đến việc kiểm soát rủi ro khi sử dụng dịch vụ công nghệ thông tin từ bên thứ ba, bao gồm yêu cầu đánh giá rủi ro và ràng buộc hợp đồng. Tuy nhiên, các quy định hiện tại chưa có cơ chế giám sát độc lập và chế tài mạnh mẽ như DORA (ví dụ như kiểm tra năng lực, phê duyệt trước, xử phạt cụ thể), trong khi các ngân hàng và tổ chức tài chính tại Việt Nam vẫn đang phụ thuộc vào cam kết hợp đồng với các nhà cung cấp giải pháp công nghệ bên ngoài.

Theo báo cáo từ Viettel Cyber Security (2024), tình trạng rò rỉ dữ liệu và tấn công mạng vẫn diễn ra, trong đó ngành tài chính nằm trong nhóm có nguy cơ cao. Điều này phản ánh nhu cầu tăng cường phối hợp giữa các bên liên quan nhằm nâng cao khả năng phản ứng và phục hồi trên nền tảng số.

4.1.3. Quyền người dùng: Nền tảng pháp lý và thực tiễn truyền thông

Về quyền dữ liệu cá nhân, Nghị định 13/2023/NĐ-CP đã xác lập rõ quyền được biết, quyền đồng ý, quyền truy cập, chỉnh sửa, và xóa dữ liệu. Đây là bước tiến quan trọng trong việc bảo vệ người dùng trong môi trường số. Tuy nhiên, ở cấp độ tiếp cận thực tế, việc phổ biến các quyền này đến người dân vẫn cần được đẩy mạnh hơn. Nhiều khách hàng sử dụng dịch vụ ngân hàng số chưa thật sự nắm rõ thông tin về quyền của mình, đặc biệt trong các tình huống liên quan đến xác thực sinh trắc học hoặc hành vi tài chính. Điều này cho thấy tầm quan trọng của việc kết hợp giữa quy định pháp lý và hoạt động truyền thông chính sách hướng đến người dân.

Từ đối chiếu trên, có thể thấy Việt Nam đang tiến gần hơn đến các chuẩn mực quốc tế trong lĩnh vực quản trị ngân hàng số.Việt Nam và EU đều chia sẻ mục tiêu bảo vệ người dùng và dữ liệu trong ngân hàng số, nhưng khác biệt rõ rệt về cấu trúc hệ thống, cơ chế giám sát và mức độ phổ cập quyền người dùng. Trong khi EU có hệ thống đồng bộ, chuyên sâu với các cơ quan giám sát độc lập, Việt Nam vẫn đang từng bước hoàn thiện, đặc biệt trong khâu thực thi và truyền thông đến người dân. Đây là cơ sở quan trọng để đề xuất các bước điều chỉnh chính sách phù hợp hơn với thực tiễn trong nước.

4.2. Chế tài và cơ quan thực thi

Sự khác biệt giữa Việt Nam và Liên minh Châu Âu thể hiện rõ ở mô hình cơ quan thực thi và công cụ chế tài. EU ưu tiên tính độc lập của cơ quan giám sát và răn đe tài chính dựa trên doanh thu, trong khi Việt Nam lồng ghép bảo vệ dữ liệu vào khung an ninh - trật tự, với chế tài hiện hành chủ yếu là xử phạt hành chính. Khác biệt này phản ánh hai cách tiếp cận về vai trò của pháp luật trong bảo vệ dữ liệu cá nhân: một bên nhấn mạnh bảo vệ quyền của chủ thể dữ liệu qua giám sát độc lập, bên kia đề cao an ninh và trật tự công.

Tại EU, GDPR thiết lập cơ chế phạt hai bậc, với mức phạt tối đa có thể lên tới 20 triệu euro hoặc 4% doanh thu toàn cầu của năm trước đó (lấy mức cao hơn). Mức răn đe tài chính khổng lồ này đi kèm một "hộp công cụ" khắc phục linh hoạt, cho phép cơ quan chức năng đưa ra cảnh báo, yêu cầu chấm dứt xử lý dữ liệu, hoặc đình chỉ các luồng dữ liệu xuyên biên giới. Việc thực thi

được giao cho các Cơ quan Bảo vệ Dữ liệu (DPA) quốc gia độc lập và được điều phối ở cấp EU để bảo đảm tính nhất quán. Quan trọng hơn, các DPA không chỉ đóng vai trò thực thi bị động mà còn chủ động tư vấn, hướng dẫn doanh nghiệp, tạo ra một môi trường tuân thủ mang tính hợp tác.

Ở Việt Nam, việc bảo vệ dữ liệu hiện do nhiều cơ quan phối hợp, trong đó A05 (Bộ Công an) giữ vai trò trung tâm xử lý vi phạm. Mô hình tập trung vào an ninh này giúp xử lý hiệu quả các vụ việc có yếu tố hình sự, nhưng mô hình đa cơ quan cũng tiềm ẩn thách thức về sự thiếu nhất quán trong áp dụng quy định và có thể làm chậm quá trình phản ứng sự cố do cần phối hợp liên ngành. Về chế tài, mức phạt hành chính theo Nghị định 15/2020/NĐ-CP, mức phạt hành chính nhìn chung là không đáng kể so với quy mô doanh thu của các tổ chức tài chính lớn, nên hiệu ứng răn đe tài chính còn hạn chế. Do đó, hiệu ứng răn đe tài chính còn hạn chế, đặt ra yêu cầu cần chuẩn hóa quy trình và nâng cao tính khách quan khi xử lý các tình huống dân sự thường nhật về quyền dữ liệu.

4.3. Từ chính sách đến thực tiễn tại Việt Nam

4.3.1. Triển khai thực tiễn: Những bước đi tích cực

Một số ngân hàng số như TNEX (thuộc MSB) hay Cake by VPBank đã tích cực áp dụng các tiêu chuẩn bảo mật trong phát triển hệ thống. TNEX sử dụng công nghệ xác thực đa lớp và mã hóa dữ liệu đầu-cuối không chỉ là lựa chọn công nghệ mà còn là hành động tuân thủ trực tiếp các yêu cầu về an toàn hệ thống thông tin trong Thông tư 09/2020/TT-NHNN. Cake, bên cạnh việc xác minh eKYC, còn tích hợp cảnh báo gian lận giao dịch trong thời gian thực để giảm thiểu rủi ro. Tương tự, MB Bank - dù không phải ngân hàng số độc lập - đã đầu tư mạnh vào nền tảng số hóa và hệ thống AI giám sát giao dịch bất thường. Đây là những ví dụ cho thấy các tổ chức tài chính tại Việt Nam đang có xu hướng đẩy mạnh năng lực kỹ thuật để thích ứng với khung pháp lý đang hoàn thiện.

4.3.2. Khó khăn thực tiễn: Từ kỹ thuật đến nhận thức người dùng

Tuy vậy, không ít ngân hàng vẫn gặp khó khăn trong việc chuyển hóa các quy định thành năng lực triển khai hiệu quả. Việc kiểm thử an ninh mạng, phản ứng sự cố hay kiểm soát truy cập dữ liệu vẫn chưa đồng đều giữa các đơn vị. Thêm vào đó, vấn đề nhận thức của người dùng cũng là rào cản đáng kể. Nhiều khách hàng chưa hiểu rõ các quyền dữ liệu cá nhân của mình khi sử dụng ngân hàng số, dẫn đến việc dễ dàng cung cấp thông tin nhạy cảm, không kiểm soát được việc chia sẻ dữ liệu với bên thứ ba, hoặc không biết cách phản ứng khi có dấu hiệu bị lừa đảo.

Ví dụ, khi Thông tư 17/2024/TT-NHNN yêu cầu xác thực sinh trắc học trong giao dịch số, một bộ phận khách hàng bày tỏ sự lo lắng và lúng túng do chưa nhận được thông tin rõ ràng từ ngân hàng về cách thức thực hiện, quyền từ chối hoặc phương án thay thế.

4.3.3. Khoảng trống giữa pháp lý - truyền thông - ứng dụng

Từ thực tiễn này, có thể thấy một trong những khoảng trống lớn hiện nay chính là sự thiếu kết nối giữa chính sách ban hành, hoạt động truyền thông của tổ chức tín dụng, và khả năng tương tác của người dùng cuối. Nếu các quyền về dữ liệu cá nhân không được truyền tải rõ ràng, thì dù hệ thống pháp lý có tiên tiến đến đâu cũng khó đạt được hiệu quả bảo vệ thực sự trong thực tiễn.

4.4. Thảo luận

Kết quả so sánh trên cho thấy những khoảng trống pháp lý tại Việt Nam đang tạo ra các thách thức cụ thể trong thực tiễn. Việc thiếu một cơ chế giám sát bên thứ ba chặt chẽ như DORA khiến các ngân hàng Việt Nam, dù đã có những bước đi tích cực, vẫn đối mặt với rủi ro tiềm ẩn. Chẳng hạn, các ngân hàng số như TNEX và Cake by VPBank áp dụng các công nghệ hiện đại như xác thực đa lớp và eKYC , hay MB Bank đầu tư vào AI để giám sát giao dịch, nhưng sự an toàn của các nền tảng này phụ thuộc rất nhiều vào các nhà cung cấp giải pháp công nghệ. Khi không có khung giám sát độc lập, ngân hàng và người dùng phải dựa chủ yếu vào cam kết trong hợp đồng.

Bên cạnh đó, khoảng trống giữa pháp lý và nhận thức người dùng là rất lớn. Dù Nghị định 13 đã trao quyền cho người dân, nhiều khách hàng vẫn chưa hiểu rõ quyền của mình khi sử dụng ngân hàng số, dẫn đến việc dễ dàng cung cấp thông tin nhạy cảm. Sự lúng túng của người dân khi được yêu cầu xác thực sinh trắc học theo quy định mới là một minh chứng rõ ràng cho thấy sự thiếu kết nối giữa việc ban hành chính sách và hoạt động truyền thông, giáo dục người dùng.

V. Đề xuất chính sách và giải pháp

Để giải quyết các khoảng trống đã phân tích và thúc đẩy sự phát triển an toàn của ngân hàng số, Việt Nam cần một lộ trình cải cách đồng bộ, kết hợp giữa hoàn thiện pháp lý, tăng cường thực thi và nâng cao nhận thức cộng đồng.

Trước hết, việc củng cố nền tảng pháp lý là yêu cầu tiên quyết. Mặc dù Nghị định 13/2023/NĐ-CP là một bước tiến quan trọng, Việt Nam cần nghiên cứu xây dựng một Luật Bảo vệ dữ liệu cá nhân hoàn chỉnh. Việc nâng cấp từ nghị định lên thành luật sẽ tạo ra hành lang pháp lý ở cấp độ cao nhất, tương xứng với tầm quan trọng của dữ liệu trong nền kinh tế số và tăng cường tính răn đe. Song song với đó, các cơ quan quản lý cần ban hành những văn bản hướng dẫn chi tiết cho riêng lĩnh vực tài chính - ngân hàng, nhằm làm rõ các khái niệm về dữ liệu tài chính, quy trình xử lý và chế độ báo cáo, giúp các tổ chức tín dụng triển khai một cách thống nhất và hiệu quả.

Bên cạnh việc hoàn thiện khung pháp lý, nâng cao hiệu quả giám sát và phản ứng sự cố là yếu tố sống còn. Cần thiết lập một tổ công tác liên ngành bao gồm Ngân hàng Nhà nước, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05 - Bộ Công an), và Bộ Thông tin và Truyền thông. Cơ chế phối hợp này sẽ giúp chuẩn hóa quy trình ứng phó, chia sẻ thông tin về các mối đe dọa và điều phối xử lý khủng hoảng trên toàn ngành, đảm bảo phản ứng nhanh chóng và đồng bộ khi sự cố xảy ra, thay vì để các ngân hàng tự xử lý một cách riêng lẻ.

Cuối cùng, không một hệ thống nào có thể hiệu quả nếu thiếu sự tham gia của người dùng cuối. Các ngân hàng và cơ quan quản lý cần phối hợp triển khai những chiến dịch truyền thông đa kênh để nâng cao nhận thức của người dân về các quyền dữ liệu của họ. Thay vì các văn bản khó hiểu, thông tin cần được truyền tải qua các hình thức trực quan, sinh động như infographic, video ngắn trên mạng xã hội và thông báo ngay trên ứng dụng ngân hàng. Đồng thời, cần yêu cầu các tổ chức tín dụng phải minh bạch hóa chính sách sử dụng dữ liệu, trình bày các điều khoản một cách ngắn gọn, dễ hiểu, giúp khách hàng đưa ra quyết định một cách có ý thức và chủ động bảo vệ thông tin cá nhân của mình.

VI. Kết luận

Ngân hàng số đang trở thành một trụ cột quan trọng trong hệ thống tài chính

hiện đại. Để phát triển an toàn và bền vững, cần một khung pháp lý hiệu lực, hiệu quả và phù hợp với điều kiện thực tế. Bài viết cho thấy những điểm tương đồng và khác biệt giữa Việt Nam và EU. Việc tham khảo có chọn lọc kinh nghiệm từ GDPR và DORA, kết hợp với các giải pháp chính sách cụ thể và đồng bộ như đã đề xuất, sẽ là chìa khóa giúp Việt Nam hoàn thiện chính sách, nâng cao năng lực cạnh tranh và củng cố niềm tin của người dùng trong tiến trình chuyển đổi số.

Tài liệu tham khảo:

[1]. Boston Consulting Group. (2024). *Global FinTech: Prudence, Profits and Growth*. Retrieved from https://www.bcg.com/publications/2024/global-fintech-prudence-profits-and-growth

[2]. European Insurance and Occupational Pensions Authority (EIOPA). (2023). *Digital Operational Resilience Act (DORA)*. Retrieved from https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

[3]. European Union. (2016). *General Data Protection Regulation (GDPR)*. Retrieved from https://gdpr.eu

[4]. Government of Vietnam. (2018). *Law on Cybersecurity No. 24/2018/QH14*. Retrievedfromhttps://vanban.chinhphu.vn/?docid=206114&pageid=27160

[5]. Government of Vietnam. (2023). *Decree No. 13/2023/ND-CP on Personal Data Protection*. Retrieved from https://www.heliolegal.com/en/nghi-dinh-so-13-2023-nd-cp-ve-bao-ve-du-lieu-ca-nhan-2/

[6]. NCS Group. (2024). *Báo cáo an ninh mạng năm 2024*. Retrieved from https://ncsgroup.vn/wp-content/uploads/2025/01/NCS-Bao-cao-an-ninh-mang-2024.pdf

[7]. State Bank of Vietnam. (2020). *Circular No. 09/2020/TT-NHNN on Information System Security in Banking Activities*. Retrieved from https://thuvienphapluat.vn/van-ban/Tien-te-Ngan-hang/Thong-tu-09-2020-TT-NHNN-an-toan-he-thong-thong-tin-trong-hoat-dong-ngan-hang-455885.aspx

[8]. Vietnam Investment Review. (2024). *Companies wary of cybersecurity threats*. Retrieved from https://vir.com.vn/companies-wary-of-cybersecurity-threats-110913.html

[9]. VnEconomy. (2024). *Tình hình an ninh mạng Việt Nam 2024: Doanh nghiệp không thể chủ quan*. Retrieved from https://vneconomy.vn/tinh-hinh-an-ninh-mang-viet-nam-2024-doanh-nghiep-khong-the-chu-quan.htm

Phụ Lục:

1. Khung pháp lý tại Việt Nam

Nhận thức được tầm quan trọng của việc bảo vệ dữ liệu trong bối cảnh ngân hàng số, Việt Nam đã từng bước hoàn thiện khung pháp lý liên quan. Một số văn bản đáng chú ý bao gồm:

+ Luật An ninh mạng (2018): đặt nền móng pháp lý cho việc bảo vệ hệ thống thông tin quan trọng, trong đó có ngành ngân hàng.

+ Thông tư 09/2020/TT-NHNN của Ngân hàng Nhà nước: quy định yêu cầu tối thiểu về an toàn hệ thống thông tin trong hoạt động ngân hàng, bao gồm quản lý truy cập, giám sát hệ thống, bảo vệ dữ liệu và phản ứng sự cố.

+ Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân: quy định các nguyên tắc và trách nhiệm trong việc thu thập, xử lý, lưu trữ, chuyển giao dữ liệu cá nhân - trong đó có dữ liệu tài chính và hành vi người dùng.

Các văn bản này cho thấy Việt Nam đã bước đầu cho việc định hình hành lang pháp lý bảo vệ dữ liệu cá nhân trong thời đại số. Tuy nhiên, hệ thống hiện hành vẫn còn phân tán, cần tiếp tục hoàn thiện về tính thống nhất, giám sát, và thực thi. Theo số liệu từ Bộ Thông tin và Truyền thông, trong quý I năm 2024, đã có 2.372 sự cố tấn công mạng vào hệ thống thông tin tại Việt Nam, cho thấy mức độ rủi ro vẫn còn

hiện hữu (Vietnam Investment Review, 2024). Những con số này đặt ra yêu cầu phải tiếp tục hoàn thiện các tiêu chuẩn kỹ thuật, nâng cao năng lực quản lý và giám sát thực thi pháp luật trong lĩnh vực ngân hàng số.

So với các khuôn khổ pháp lý quốc tế như GDPR của Liên minh Châu Âu với các nguyên tắc rõ ràng và cơ chế giám sát độc lập khung pháp lý Việt Nam vẫn đang trong quá trình điều chỉnh và hoàn thiện. Những kinh nghiệm quốc tế có thể là tài liệu tham khảo hữu ích cho Việt Nam trong việc xây dựng một hệ thống pháp lý có khả năng đáp ứng linh hoạt sự phát triển của công nghệ ngân hàng số, đồng thời bảo vệ hiệu quả người dùng.

2. Khung pháp lý tại Liên minh Châu Âu (EU)

Tại Liên minh Châu Âu, khuôn khổ pháp lý được xây dựng trên hai văn bản nền tảng: Quy định chung về Bảo vệ Dữ liệu (GDPR), nhằm bảo vệ dữ liệu cá nhân, và Đạo luật về Khả năng Phục hồi Hoạt động Kỹ thuật số (DORA), nhằm đảm bảo sự ổn định của ngành tài chính trước các rủi ro kỹ thuật số. Cả hai văn bản này đều có tính cưỡng chế cao, phạm vi rộng và có chế tài rõ ràng, đồng thời trao quyền mạnh mẽ cho người dùng và yêu cầu doanh nghiệp phải kiểm thử an toàn định kỳ. Hệ thống này tạo nên sự minh bạch và tin cậy trong hoạt động ngân hàng số.

Được chính thức áp dụng từ tháng 5 năm 2018, GDPR là một trong những quy định nghiêm ngặt nhất trên thế giới về bảo vệ dữ liệu cá nhân. Văn bản này không chỉ áp dụng cho các tổ chức tại EU mà còn mở rộng phạm vi điều chỉnh đối với mọi tổ chức xử lý dữ liệu cá nhân của công dân EU, dù tổ chức đó đặt trụ sở ở bất kỳ đâu (European Union, 2016). GDPR thiết lập các nguyên tắc cốt lõi trong quản lý dữ liệu, bao gồm: tính minh bạch, giới hạn mục đích, tối thiểu hóa dữ liệu, bảo mật và trách nhiệm giải trình. Quy định này cũng trao cho người dùng quyền kiểm soát mạnh mẽ hơn đối với dữ liệu cá nhân của họ như quyền truy cập, chỉnh sửa, xóa ("quyền được lãng quên") và phản đối việc xử lý dữ liệu. Đặc biệt, GDPR yêu cầu báo cáo vi phạm dữ liệu trong vòng 72 giờ kể từ khi phát hiện sự cố, đồng thời áp dụng chế tài nghiêm ngặt, có thể lên tới 20 triệu euro hoặc 4% doanh thu toàn cầu của doanh nghiệp.

Bên cạnh bảo vệ dữ liệu cá nhân, EU cũng chú trọng tới việc đảm bảo khả năng vận hành liên tục và phục hồi kỹ thuật số trong các tổ chức tài chính thông qua DORA - Digital Operational Resilience Act, có hiệu lực từ tháng 1 năm 2025. DORA yêu cầu các tổ chức tài chính (bao gồm ngân hàng, công ty bảo hiểm, công ty FinTech…) phải xây dựng năng lực phục hồi kỹ thuật số toàn diện. Điều này bao gồm: đánh giá rủi ro công nghệ thông tin, kiểm thử an ninh mạng, giám sát nhà cung cấp dịch vụ bên thứ ba (Third-Party ICT Providers) và báo cáo định kỳ về các sự cố vận hành kỹ thuật số nghiêm trọng (EIOPA, 2023). DORA nhấn mạnh tính liên kết giữa an ninh mạng, rủi ro công nghệ và hệ thống tài chính, giúp tạo ra sự đồng bộ trong giám sát và quản trị hệ thống ngân hàng số ở cấp khu vực.

DIGITAL BANKING GOVERNANCE IN VIETNAM AND THE EUROPEAN UNION: A COMPARATIVE STUDY OF DATA PROTECTION AND CYBERSECURITY POLICIES IN THE CONTEXT OF DIGITAL TRANSFORMATION

Pham Thi Dinh[2]

Abstract: *In the context of the digital economic transition, digital banking is emerging as a key pillar of the financial system in Vietnam. However, this rapid development presents urgent demands for two critical components ensuring the sustainability of digital banking: personal data governance and cybersecurity. This paper conducts a comparative analysis of the legal frameworks related to data protection and cybersecurity between Vietnam and the European Union (EU), with a focus on key regulations such as Decree No. 13/2023/ND-CP and the Cybersecurity Law in Vietnam, as well as the GDPR and DORA in the EU. By examining differences in regulatory enforcement, user rights, oversight mechanisms, and responses to data breaches, the study highlights notable policy gaps in Vietnam. Furthermore, selected case studies from Vietnamese digital banks are analyzed to assess the level of compliance and implementation. Based on these findings, the paper offers specific and feasible recommendations to improve the regulatory framework and enhance resilience against cybersecurity risks amid the growing prevalence of digital banking.*

Keywords: *cybersecurity, data protection, DORA, GDPR, digital banking*

---

[2] Hanoi Open University