AN TOÀN DỮ LIỆU CÁ NHÂN TRONG HỆ THỐNG NGÂN HÀNG THƯƠNG MẠI VIỆT NAM

NGUYỄN THANH NGUYÊN

Bài viết này đánh giá thực trạng về bảo mật thông tin khách hàng trong hệ thống ngân hàng thương mại và làm rõ hơn những vấn đề lý luận về bảo mật an toàn dữ liệu cá nhân trong các ngân hàng thương mại Việt Nam. Bằng phương pháp nghiên cứu định tính dựa trên nguồn dữ liệu thứ cấp như: các công trình nghiên cứu, các tài liệu nghiên cứu liên quan, các báo cáo chuyên môn của các cơ quan quản lý nhà nước và các ngân hàng thương mại, bài viết tiến hành phân tích, so sánh, tổng hợp thông tin để làm cơ sở đưa ra các nhận định, đánh giá thực trạng về tính bảo mật an toàn dữ liệu cá nhân. Đồng thời, bài viết đề xuất các giải pháp để bảo mật an toàn dữ liệu cá nhân trong hệ thống các ngân hàng thương mại.

Từ khóa: An toàn, bảo mật, dữ liệu cá nhân

PERSONAL DATA PRIVACY IN THE VIETNAM'S COMMERCIAL BANK SYSTEM

Nguyen Thanh Nguyen

This article evaluates the status of customer information security in the commercial banking system and clarifies theoretical issues regarding the security of personal data in Vietnamese commercial banks. Using a qualitative research method based on secondary data sources such as research papers, related research documents, specialized reports from state management agencies, and commercial banks, the article analyzes, compares, and synthesizes information to provide a basis for making assessments of the current state of personal data security. Additionally, the article proposes solutions for ensuring the security of personal data in the systems of commercial banks.

Keywords: Security, privacy, personal data

Ngày nhận bài: 14/3/2024
Ngày hoàn thiện biên tập: 21/3/2024
Ngày duyệt đăng: 28/3/2024

Giới thiệu

Dữ liệu cá nhân là thông tin quan trọng, rất có giá trị, và là yếu tố quyết định sự thành công trong hệ thống ngân hàng thương mại Việt Nam (NHTM). Khi các NHTM đẩy mạnh đa dạng hóa dịch vụ số nhằm phục vụ khách hàng tốt hơn phù hợp với nền kinh tế số, thì việc chuyển đổi số thành công hay không đều có mối liên quan mật thiết và cùng chiều đến an toàn dữ liệu cá nhân của khách hàng. Tuy nhiên, dữ liệu cá nhân được thể hiện trên các dịch vụ trực tuyến cũng là đích đến của tội phạm mạng. Chỉ tính riêng năm 2022, Việt Nam ghi nhận 12.935 trường hợp lừa đảo trực tuyến, trong đó 75% lừa đảo tài chính, 25% đánh cắp dữ liệu cá nhân để lừa đảo tài chính. Các hình thức lừa đảo phổ biến: (i) Chiếm đoạt tài khoản, tội phạm chiếm quyền tài khoản mạng xã hội (Zalo, Fcarbook, Tiktok...) để gửi tin nhắn lừa đảo, lừa chuyển tiền, lừa nạn nhân truy cập/click vay tín dụng đen lãi suất cao; (ii) Giả mạo thương hiệu NHTM để nhắn tin, gửi email lừa đảo; giả mạo trang web để lừa cung cấp thông tin, lừa giao dịch, lừa cài mã độc qua đường link; (iii) Giả danh cơ quan chức năng gọi điện lừa đảo, tạo nick giả để lừa, giả mạo sàn thương mại điện tử, sàn tiền ảo để lừa tiền nhà đầu tư. Ngoài ra, còn các chiêu thức lừa đảo khác như: Giả mạo ngân hàng lừa trúng thưởng để lấy tài khoản, mã OTP; Giả mạo công an yêu cầu cung cấp thông tin tài khoản để điều tra hoặc yêu cầu chuyển tiền vào tài khoản công an (giả) để chứng minh; Giả mạo người thân nhờ nhận hộ tiền hoặc vay tiền... Từ thực tiễn trên, việc nghiên cứu an toàn dữ liệu cá nhân trong hệ thống NHTM Việt Nam là cần thiết.

Một số nghiên cứu và văn bản pháp lý về an toàn dữ liệu cá nhân

An toàn dữ liệu cá nhân là vấn đề quan trọng trong công tác bảo mật thông tin của các NHTM và luôn được các nhà quản lý quan tâm hàng đầu. Chỉ có NHTM bảo mật thông tin cá nhân một cách khoa học thì mới có thể bảo vệ an toàn dữ liệu cá nhân của

khách hàng, đây cũng là bảo vệ an toàn tài sản của NHTM. Các NHTM phải chịu sức ép từ việc bị đánh cắp dữ liệu cá nhân do việc đẩy mạnh triển khai thực hiện ngân hàng số trong nền kinh tế số hiện nay đều hiểu rõ sự cần thiết việc bảo mật an toàn hệ thống dữ liệu cá nhân; hệ thống dữ liệu này là tài sản quan trọng nhất vì nó quyết định sự tồn tại của NHTM. Với tầm quan trọng đó, đã có nhiều nghiên cứu liên quan tới an toàn dữ liệu cá nhân, cụ thể: Đề tài "Nghiên cứu về mật mã an toàn thông tin" của Hoàng Trọng Ngãi (2015) đã nghiên cứu về lưu trữ ảnh DICOM trong cơ sở dữ liệu một cách an toàn; "Nghiên cứu giải pháp xác thực và bảo mật trong trao đổi tài liệu trên môi trường mạng giữa các cơ quan nhà nước" của Trịnh Xuân Hoàng (2012) đã trình bày bảo mật tài liệu trong trao đổi văn bản trên môi trường mạng giữa các cơ quan nhà nước và ứng dụng thành công tại tỉnh Thái Bình; Đề tài "Pháp luật quốc tế và thực tiễn về xử lý tội phạm công nghệ cao – kinh nghiệm cho Việt Nam" của Thân Trọng Ngọc Trâm (2019) đã hệ thống hóa các vấn đề lý luận và thực tiễn xử lý tội phạm công nghệ cao ở quốc tế và rút ra kinh nghiệm cho Việt Nam nhằm nâng cao bảo mật an toàn dữ liệu cá nhân.

Tại Việt Nam, ngày 17/4/2023, Chính phủ ban hành Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân. Nghị định nêu rõ nghĩa vụ của bên kiểm soát, xử lý dữ liệu như sau: phải có sự đồng ý rõ ràng, tự nguyện, và hiểu rõ của chủ thể dữ liệu; phải thông báo xử lý dữ liệu...; phải có biện pháp ngăn chặn thu thập, chuyển giao, mua, bán trái phép dữ liệu cá nhân; khi cung cấp cho NHTM, cá nhân khác phải có sự đồng ý của chủ thể dữ liệu; phải xóa dữ liệu cá nhân khi có yêu cầu; phải chuyển giao dữ liệu cá nhân theo quy định của pháp luật khi chia, tách, sáp nhập...

Phương pháp nghiên cứu

Để đánh giá thực tiễn về an toàn dữ liệu cá nhân trong hệ thống NHTM, nhóm tác giả khảo sát một số NHTM và khách hàng ở TP. Hồ Chí Minh để thu thu thập thông tin về thực trạng an toàn dữ liệu cá nhân qua phát phiếu điều tra, phỏng vấn trực tiếp, qua điện thoại, thư điện tử... và sử dụng số liệu từ các báo cáo, các nguồn khác đã được công bố. Từ lý luận kết hợp với khảo sát thực tế và phân tích, so sánh, tổng hợp thông tin làm cơ sở đưa ra các nhận định, đánh giá thực trạng an toàn dữ liệu cá nhân nhằm phục vụ cho việc nâng cao tính bảo mật dữ liệu cá nhân trong hệ thống NHTM, qua đó đề xuất một số giải pháp hoàn thiện tính an toàn dữ liệu cá nhân.

Thực trạng an toàn dữ liệu cá nhân trong hệ thống NHTM

Để đánh giá thực trạng an toàn dữ liệu cá nhân trong hệ NHTM hiện nay, tác giả tiến hành đánh giá qua các góc nhìn sau:

Thứ nhất, dữ liệu là cốt lõi của chuyển đổi số, khi các NHTM chuyển đổi số càng chuyên sâu, đòi hỏi lượng dữ liệu càng lớn nên yêu cầu xử lý dữ liệu càng cao, do đó rủi ro an toàn dữ liệu càng lớn.

Khi trí tuệ nhân tạo phát triển mạnh mẽ thì dữ liệu và xử lý dữ liệu trở thành linh hồn của trí tuệ nhân tạo trong thời đại số, hay nói cách khác dữ liệu là cốt lõi của chuyển đổi số. Do đó, bất kỳ NHTM nào muốn chuyển đổi số thành công đều phải quan tâm đến dữ liệu và an toàn dữ liệu. Hiện nay, rất nhiều hoạt động của ngân hàng số phụ thuộc vào dữ liệu cá nhân hoặc dữ liệu riêng của NHTM như: mở tài khoản, xác thực giao dịch, xác định khách hàng, phân tích rủi ro, cung cấp dịch vụ tài chính… vì thế để cắt giảm chi phí vận hành và để có thể tiếp cận được nhiều khách hàng hơn, các lãnh đạo ra quyết định nhanh chóng và chính xác hơn, thì hệ thống ngân hàng số nói riêng và hệ thống NHTM nói chung càng phải tích cực chuyển đổi số chuyên sâu hơn nữa. Chuyển đổi số là một trong những mục tiêu được quan tâm hàng đầu tại các NHTM hiện nay, khi chuyển đổi số được chú trọng thì sẽ góp phần thúc đẩy văn hóa làm việc thay đổi theo chiều hướng tích cực, thay đổi phương thức điều hành, lãnh đạo, quy trình làm việc. Tuy nhiên, khi các NHTM chuyển đổi số càng chuyên sâu, thì đòi hỏi lượng dữ liệu đáp ứng ngày càng lớn nên yêu cầu xử lý dữ liệu càng cao, do đó rủi ro an toàn dữ liệu càng lớn.

Thứ hai, vi phạm dữ liệu tại Việt Nam và trên thế giới tăng nhanh. Trong những năm qua, thế giới đã xuất hiện nhiều vụ án lớn về lộ, lọt, đánh cắp, mua bán dữ liệu cá nhân. Điển hình như: Năm 2013, Yahoo bị đánh cắp 3 tỷ tài khoản người dùng; Năm 2016, Uber bị đánh cắp thông tin 57 triệu người dùng và đã phải trả USD 100.000 cho tin tặc để xóa dữ liệu bị đánh cắp và giữ im lặng vụ vi phạm; Năm 2017, Friend Finder Networks bị đánh cắp 412 triệu tài khoản người dùng; Tháng 4/2021, Facebook bị lộ dữ liệu cá nhân 533 triệu người dùng; Tháng 9/2022, Optus (Australia) bị đánh cắp dữ liệu cá nhân của 9,8 triệu khách hàng (chiếm 40% dân số); Tháng 10/2022, sàn thương mại điện tử Carousell của Singapore bị lộ dữ liệu của 1,95 triệu người dùng...

Ở Việt Nam cũng có nhiều vụ án lớn về lộ, lọt, đánh cắp, mua bán dữ liệu cá nhân: Công ty Công nghệ và Internet hàng đầu Việt Nam (VNG) để lộ

hơn 163 triệu tài khoản khách hàng; Thế giới di động và Điện máy xanh để lộ hơn 5 triệu email và hàng chục nghìn thông tin thẻ thanh toán; Việt Nam Airline để lộ 411 nghìn tài khoản thành viên Bông Sen Vàng; Một ngân hàng Việt Nam để lộ thông tin 2 triệu khách hàng; Facebook để lộ thông tin 50 triệu người dùng Việt Nam...

Theo Bộ Công An, từ năm 2019 – 2020 có 1.300 GB dữ liệu cá nhân của hàng tỷ lượt cá nhân Việt Nam bị mua bán trái phép. Tuy nhiên, đây chỉ là bề nổi của tảng băng, bởi thực tế còn rất nhiều vụ việc chưa được phát hiện. Các vụ lộ, lọt dữ liệu này chủ yếu đến từ các cuộc tấn công mạng nhằm đánh cắp tài sản có giá trị lớn, điều này sẽ làm ảnh hưởng nghiêm trọng đến uy tín hay thương hiệu của hệ thống NHTM, khách hàng sẽ mất niềm tin do không được bảo vệ, gây ra tổn thất lớn về tài chính cho cả khách hàng và các NHTM. Đồng thời, quá trình vận hành của các NHTM bị đình trệ, thậm chí, có thể đối mặt với cả pháp lý khi để lộ, lọt thông tin.

Thứ ba, thiệt hại cho nền kinh tế do chi phí xử lý vi phạm dữ liệu rất lớn và ngày càng tăng. Trung bình trên thế giới, chi phí để xử lý cho một sự cố vi phạm dữ liệu có xu hướng gia tăng trong khoảng từ 3,5 đến 4 triệu USD. Ở Việt Nam, chưa có thống kê về chi phí trung bình để xử lý một sự cố vi phạm dữ liệu. Tuy nhiên, trong những năm qua, Việt Nam đã xảy ra tình trạng lộ, lọt thông tin làm thất thoát tài sản cho cá nhân và NHTM, điều này làm phát sinh chi phí xử lý vi phạm dữ liệu cho các NHTM đã bị đánh cắp hay bị xâm nhập dữ liệu. Bất kỳ NHTM nào cũng đều muốn tối ưu chi phí ở mức thấp nhất để có thể đạt hiệu suất lợi nhuận cao nhất, nhưng điều này không thật sự dễ dàng khi các NHTM phải gánh thêm chi phí xử lý vi phạm dữ liệu; chi phí này sẽ ảnh hưởng rất lớn đến hiệu quả hoạt động kinh doanh và tác động mọi mặt đến tình hình kinh doanh; khả năng cạnh tranh cả các NHTM bị vi phạm dữ liệu sẽ bị suy giảm, bị mất niềm tin từ khách hàng, thị phần hoạt động bị thu hẹp, thậm chí bị đóng cửa.

Nguyên nhân dữ liệu cá nhân bị đánh cắp

Thực tế cho thấy, dữ liệu cá nhân bị đánh cắp là do những nguyên nhân sau:

Thứ nhất, do yếu tố phi kỹ thuật (nguyên nhân này thường chiếm tỷ trọng lớn) được biểu hiện như sau: Các NHTM thu thập nhiều dữ liệu nhưng không đầu tư đủ để bảo vệ an toàn; Lộ, lọt thông tin từ nhân viên quản lý dữ liệu, lấy cắp vì mục đích riêng, mua bán trái phép; bên thứ ba cấu kết với nhân viên quản lý dữ liệu của NHTM để được chia sẻ dữ liệu trái phép; Lừa đảo trực tuyến nhằm mục đích thu thập thông tin cá nhân, thu thập thông qua việc tạo các trang web, tài khoản mạng xã hội; Nhận thức về bảo vệ thông tin cá nhân của người dùng còn thấp; chủ thể thông tin bất cẩn, cung cấp tùy tiện, đặc biệt trên mạng xã hội.

Thứ hai, do yếu tố kỹ thuật, được thể hiện thông qua: Các hệ thống thông tin chưa phê duyệt và triển khai đầy đủ các phương án bảo đảm an toàn thông tin theo cấp độ; Các hệ thống thông tin không được đầu tư các giải pháp phù hợp để bảo đảm an toàn, an ninh mạng, dẫn đến bị tấn công, khai thác, đánh cắp dữ liệu; Nhận thức của bên kiểm soát, bên xử lý dữ liệu và người quản trị hệ thống thấp, không tuân thủ quy định dẫn đến bị tấn công, khai thác, đánh cắp dữ liệu.

Giải pháp bảo mật an toàn dữ liệu cá nhân

Để bảo mật an toàn dữ liệu cá nhân trong hệ thống NHTM Việt Nam tác giả đề xuất một số giải pháp sau:

Một là, người dùng – chủ thể dữ liệu cần bảo vệ, gìn giữ thông tin cá nhân nhằm hạn chế rủi ro trên môi trường mạng, thông qua thực hiện các việc sau: Hiểu rõ và thực hiện các quyền của chủ thể dữ liệu đối với thông tin cá nhân của mình; Cảnh giác với đường link giả mạo, email, tin nhắn lạ, các trang web có yêu cầu điền thông tin cá nhân; chỉ cung cấp thông tin cá nhân cho các NHTM tin cậy và thực sự cần; Không truy cập, tải file, cung cấp thông tin cá nhân ở các trang web không rõ nguồn gốc; Sử dụng mật khẩu mạnh cho mọi tài khoản, các mật khẩu mạnh (đủ dài, có nhiều loại ký tự, không trùng nhau trên các dịch vụ, định kỳ thay đổi); Sử dụng xác thực nhiều lớp nếu có thể, xác thực 2 lớp qua email, số điện thoại, trình xác thực để tạo OTP; Không đăng nhập số tài khoản của mình trên các thiết bị công cộng, thiết bị lạ có khả năng gắn key logger, cảnh giác với wifi miễn phí; Cài đặt phần mềm diệt vius trên máy tính (có thể sử dụng defender mặc định của Windows) và trên điện thoại để tránh nhiễm mã độc; Không cài đặt ứng dụng, phần mềm crack không rõ nguồn gốc; Cảnh giác với chiêu thức lừa đảo qua mạng.

Hai là, các NHTM – bên kiểm soát dữ liệu bảo vệ tài sản quan trọng nhất, giá trị nhất đó chính là bảo vệ dữ liệu cá nhân, thông qua thực hiện các nhiệm vụ sau:

- Tuân thủ quy định pháp luật: các NHTM cần phải nghiên cứu kỹ để tuân thủ các quy định pháp luật tại Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, đặc biệt là các yêu cầu về an toàn hệ

thống, quy trình, hồ sơ đánh giá tác động... Đồng thời, thực hiện đầy đủ các biện pháp đảm bảo an toàn thông tin theo cấp độ (Nghị định số 85/2017/NĐ-CP; Thông tư số 12/2022/TT-BTTTT...).

- Ban hành quy định, chính sách an toàn thông tin và bảo vệ dữ liệu cá nhân cụ thể, tường minh; thông qua ban hành đầy đủ các quy chế, quy định bảo vệ thông tin cá nhân; quy trình, thủ tục, hướng dẫn khai thác thông tin cá nhân; công bố rộng rãi, tập huấn và có chế tài bắc buộc; thiết lập các chính sách và quy trình quản lý quyền truy cập, khai thác dữ liệu cho từng đối tượng nhân viên; phân loại dữ liệu cá nhân và thực hiện các biện pháp bảo vệ tương ứng với mức độ nhạy cảm.

- Đào tạo và nâng cao nhận thức cho nhân viên và khách hàng, bằng cách thường xuyên tập huấn, nâng cao nhận thức; đào tạo về quy định, yêu cầu trong xử lý dữ liệu cá nhân, quy trình bảo mật và quy định pháp luật; đảm bảo tất cả nhân viên đều nhận thức đầy đủ, được hướng dẫn chi tiết, hiểu rõ và tuân thủ các quy định bảo vệ dữ liệu cá nhân; tăng cường công tác truyền thông, kết nối thông tin đến khách hàng về bảo vệ dữ liệu cá nhân.

- Đầu tư các giải pháp an toàn hệ thống và bảo vệ dữ liệu như: triển khai các giải pháp kỹ thuật an toàn, bảo mật mạnh mẽ và tổ chức phù hợp để đảm bảo mức độ bảo mật dữ liệu cá nhân và an toàn cho hệ thống thông tin của NHTM; tăng cường các kỹ thuật an toàn, mã hóa, hệ thống chứng thực, hạn chế truy cập giám sát hệ thống; tăng cường giải pháp sát thực khách hàng cho dịch vụ trực tuyến: SMS OTP, Soft OTP, Token OTP, Sinh trắc học, Chữ ký số; cập nhật phần mềm định kỳ để bảo vệ chống lại các mối đe dọa mạng và tin tặc.

- Đánh giá, quản trị rủi ro và sẵn sàng ứng phó: cần thường xuyên đánh giá rủi ro và có giải pháp quản trị rủi ro liên quan đến dữ liệu cá nhân; thường xuyên phân tích các mối đe dọa tiềm ẩn, xác định điểm yếu trong hệ thống và đảm bảo triển khai các giải pháp sẵn sàng ứng phó; xây dựng các kế hoạch kiểm tra, giám sát việc bảo vệ dữ liệu cá nhân; xây dựng các trung tâm dữ liệu dự phòng, các giải pháp lưu trữ và phục hồi dữ liệu hiện đại; sẵn sàng các phương án ứng cứu sự cố: phòng chống tấn công từ chối dịch vụ (Dos, DDos), tấn công APT, chống mã độc, botnet...; tham gia mạng lưới ứng cứu sự cố an toàn mạng quốc gia. Tăng cường khả năng phối hợp, hỗ trợ ứng cứu, sẵn sàng tham gia hỗ trợ giải quyết sự cố khi có yêu cầu.

Ba là, thực hiện quy trình đảm bảo an toàn thông tin và bảo vệ dữ liệu thông qua việc xây dựng các chính sách, quản lý rủi ro, tiêu chuẩn tại các NHTM, nên triển khai bảo mật an toàn dữ liệu cá nhân theo quy trình sau:

An toàn hạ tầng -> An toàn ứng dụng -> An toàn dữ liệu -> khách hàng

Bốn là, chú trọng hài hòa ba yếu tố trọng tâm: quy trình – công nghệ - khách hàng. Trong đó, khâu yếu nhất trong 3 yếu tố trên đó chính là yếu tố khách hàng, vì khách hàng thường chủ quan nên có thể dẫn đến những hành vi bất cẩn như: mật khẩu yếu; nhận thức về an toàn thông tin, bảo vệ dữ liệu kém; nhân sự trong các hệ thống NHTM có kỹ năng bảo vệ yếu; chính sách, quy chế lỗi thời; thiếu kinh phí cập nhật, nâng cấp; thiếu sự quan tâm, kiểm tra, đốc thúc từ cấp trên.

Kết luận

An toàn dữ liệu cá nhân không những là tài sản quan trọng của các NHTM, mà còn là tài sản của quốc gia. Vì thế, hệ thống NHTM cần chú trọng bảo mật tuyệt đối an toàn dữ liệu cá nhân để bảo vệ an toàn tuyệt đối về tài chính của khách hàng; khi dữ liệu cá nhân được bảo vệ an toàn thì chi phí hoạt động của ngân hàng sẽ được tối ưu hóa do không phải gánh chịu chi phí xử lý vi phạm thông tin, từ đó, hiệu quả hoạt động của ngân hàng sẽ được nâng cao, giúp ngân hàng phát triển và tăng trưởng bền vững. Để làm được điều này, ngân hàng cần khuyến cáo người dùng - chủ thể dữ liệu cần phải bảo vệ, gìn giữ thông tin cá nhân nhằm hạn chế rủi ro trên môi trường mạng. Đồng thời, NHTM nên thường xuyên kiểm soát dữ liệu để bảo vệ tài sản quan trọng nhất, giá trị nhất đó chính là bảo vệ dữ liệu cá nhân; song song đó, cần phải thực hiện quy trình đảm bảo an toàn thông tin và bảo vệ dữ liệu thông qua việc xây dựng các chính sách, quản lý rủi ro, tiêu chuẩn tại các NHTM thông qua việc chú trọng hài hòa ba yếu tố trọng tâm: quy trình – công nghệ - khách hàng.

Tài liệu tham khảo:

1. *Báo cáo về chi phí xử lý vi phạm dữ liệu năm 2019 của Ponemon;*
2. *Thân Trọng Ngọc Trâm, Nguyễn Hoàng Hoài Thương, Dương Thị Mỹ Nhi (2019), Pháp luật quốc tế và thực tiễn về xử lý tội phạm công nghệ cao - Kinh nghiệm cho Việt Nam, Đề tài nghiên cứu khoa học, Trường Đại học Luật, Đại học Huế;*
3. *Thùy An (2024), Gần 1.300 GB dữ liệu cá nhân bị thu thập mua bán trái phép, https://vtv.vn/cong-nghe/gan-1300-gb-du-lieu-ca-nhan-bi-thu-thap-mua-ban-trai-phep-20240111113730914.htm.*

Thông tin tác giả:

Nguyễn Thanh Nguyên

Giảng viên Khoa Tài chính – Ngân hàng – Kế toán, Trường Đại học Hùng Vương TP. Hồ Chí Minh

Email: nguyennt@dhv.edu.vn