Tạp chí Khoa học Đại học Huế: Khoa học Xã hội và Nhân văn
ISSN 2588-1213
Tập 134, Số 6S-1, 2025, *Tr. 141–154*; **DOI:** 10.26459/hueunijssh.v134i6S-2.7547

KINH NGHIỆM QUỐC TẾ VỀ BẢO VỆ DỮ LIỆU NGƯỜI TIÊU DÙNG SỬ DỤNG DỊCH VỤ NGÂN HÀNG SỐ VÀ GỢI Ý CHO VIỆT NAM

Trần Thế Hệ

Trường Đại học Luật, Đại học Huế, Đường Võ Văn Kiệt, TP Huế, Việt Nam

* Tác giả liên hệ: **Trần Thế Hệ** <tranthehe@hueuni.edu.vn>

(*Ngày nhận bài: 31-05-2024; Ngày chấp nhận đăng: 09-12-2024*)

Tóm tắt. Cùng với sự phát triển của công nghệ, các tổ chức cung cấp dịch vụ ngân hàng số đã và đang tích lũy, nắm nhiều dữ liệu của người tiêu dùng để phục vụ cho hoạt động của tổ chức mình. Dữ liệu người tiêu dùng trong lĩnh vực ngân hàng số được sử dụng ngày càng nhiều sẽ tiềm ẩn rủi ro cho người tiêu dùng, tổ chức cung ứng dịch vụ và Nhà nước. Bảo vệ dữ liệu người tiêu dùng sử dụng dịch vụ ngân hàng số trở thành một vấn đề quan trọng cần được quan tâm trong quá trình thực hiện nền kinh tế số và tài chính toàn diện ở Việt Nam. Trong bài viết này, tác giả nghiên cứu các quy định, thực thi các quy định về bảo vệ dữ liệu người tiêu dùng sử dụng dịch vụ ngân hàng số của Liên minh Châu Âu và một số quốc gia trên thế giới; thực trạng bảo vệ dữ liệu người tiêu dùng sử dụng dịch vụ ngân hàng số ở Việt Nam, từ đó đề xuất một số gợi ý hoàn thiện pháp luật Việt Nam.

Từ khóa: Ngân hàng số, dịch vụ ngân hàng số, dữ liệu người tiêu dùng, bảo vệ dữ liệu người tiêu dùng

DATA PROTECTION OF CONSUMERS USING DIGITAL BANKING SERVICES: INTERNATIONAL EXPERIENCE AND SUGGEST FOR VIETNAM

Tran The He

University of Law, Hue University, Vo Van Kiet St., Hue City, Vietnam

Correspondence to **Tran The He** <tranthehe@hueuni.edu.vn>

(*Received: May 31, 2024; Accepted: December 09, 2024*)

Abstract. Companies offering digital banking services have been gathering and storing a lot of consumer data in tandem with the advancement of technology to support their business operations. Consumer data is being used more and more in the world of digital banking, which might be dangerous for customers, service providers, and the government. In the course of adopting a digital economy and comprehensive finance in Vietnam, protecting customer data when utilizing digital banking services has emerged as a critical issue that requires attention. In this article, the author researches regulations and enforcement of regulations on consumer data protection using digital banking services in Europe and some countries around the world; Current status of consumer data protection using digital banking services in Vietnam, thereby proposing some suggest for Vietnam.

Keywords: Digital banking, digital banking services, consumer data, consumer data protection

1. Đặt vấn đề

Trên thế giới nói chung và Việt Nam nói riêng, nền kinh tế số đang phát triển với tốc độ nhanh chóng, từ đó mang lại nhiều cơ hội nhưng cũng đặt ra không ít thách thức cho lĩnh vực ngân hàng số (NHS), trong đó có thách thức liên quan đến việc bảo vệ quyền lợi người tiêu dùng (NTD) sử dụng dịch vụ NHS, đặc biệt là bảo vệ dữ liệu người tiêu dùng (DLNTD) sử dụng dịch vụ NHS. Liên quan đến vấn đề này, pháp luật Liên minh châu Âu và pháp luật một số quốc gia trên thế giới đã có những quy định khá sớm để bảo vệ quyền lợi NTD dịch vụ tài chính số, NHS và bảo vệ dữ liệu NTD khi tham gia lĩnh vực đó. Tại Việt Nam để bảo vệ NTD chủ yếu dựa trên căn cứ pháp lý là Luật Bảo vệ quyền lợi NTD năm 2023, tuy nhiên những quy định trong văn bản pháp lý này không có quy định về bảo vệ quyền lợi NTD sử dụng dịch vụ ngân hàng nói chung và bảo vệ dữ liệu NTD sử dụng dịch vụ NHS nói riêng, trong khi đó các văn bản pháp luật điều chỉnh trong lĩnh vực ngân hàng mặc dù cũng có những quy định về bảo vệ quyền lợi của khách hàng nhưng những quy định đó còn những hạn chế, bất cập và chưa đầy đủ để bảo vệ NTD, dữ liệu của NTD.

Ngày 17/4/2023, Chính phủ đã ban hành Nghị định số 13/2023/NĐ-CP về Bảo vệ dữ liệu cá nhân có hiêu lực thi hành ngày 01/7/2023 tuy nhiên trong văn bản này đang có những quy định chưa thật sự phù hợp và từ đó tạo ra xung đột với các quy định trong lĩnh vực ngân hàng như các quy định về về các chủ thể tham gia vào quy trình xử lý dữ liệu cá nhân của khách hàng; đồng ý xử lý dữ liệu một phần; về dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm; quyền của các chủ thể dữ liệu... Dựa trên việc tiếp cận và phân tích pháp luật của Liên minh châu Âu, pháp luật một số quốc gia trên thế giới về bảo vệ DLNTD sử dụng dịch vụ ngân hàng số từ đó đề xuất một số khuyến nghị trong việc xây dựng hoàn thiện pháp luật tại Việt Nam.

2. Khái quát về bảo vệ dữ liệu người tiêu dùng sử dụng dịch vụ ngân hàng số

Trong thời đại ngày nay, thuật ngữ NHS đã trở nên phổ biến trong đời sống xã hội. Tương tự như các ngân hàng truyền thống, NHS thực hiện các hoạt động ngân hàng, đó chính là việc kinh doanh, cung ứng thường xuyên một hoặc một số nghiệp vụ như: Nhận tiền gửi, cấp tín dụng, cung ứng dịch vụ thanh toán qua tài khoản. Tuy nhiên, khác với những ngân hàng truyền thống thực hiện các giao dịch ngân hàng chủ yếu dựa trên các điểm giao dịch vật lý thì NHS lại cung cấp các sản phẩm dịch vụ ngân hàng trên nền tảng công nghệ số, thông qua internet, điện thoại di động thông minh, máy tính bảng và có thể cả mạng xã hội [2]. Theo Khoản 1 Điều 2 Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân đã định nghĩa: Dữ liệu cá nhân là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể. Dữ liệu cá nhân gồm có dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm. Theo Khoản 1 Điều 3 Luật Bảo về quyền lợi NTD năm 2023 thì: NTD là người mua, sử dụng sản phẩm, hàng hóa, dịch vụ cho mục đích tiêu dùng, sinh hoạt của cá nhân, gia đình, cơ quan, tổ chức và không vì mục đích thương mại. Theo Khoản 38 Điều 4 Luật Các tổ chức tín dụng năm 2024, tổ chức tín dụng là tổ chức kinh tế có tư cách pháp nhân thực hiện một, một số hoặc tất cả các hoạt động ngân hàng. Như vậy, NTD sử dụng các dịch vụ do tổ chức tín dụng cung cấp để thỏa mãn mục đích tiêu dùng, sinh hoạt của cá nhân, gia đình, cơ quan, tổ chức trong các nghiệp vụ mà tổ chức tín dụng thực hiện được xem là khách hàng sử dụng dịch vụ của tổ chức tín dụng.

Pháp luật Việt Nam hiện nay chưa đưa ra định nghĩa về bảo vệ DLNTD sử dụng dịch vụ NHS, trên cơ sở khái niệm về NHS, NTD và dữ liệu cá nhân, tác giả đưa ra khái niệm về bảo vệ DLNTD sử dụng dịch vụ NHS, theo đó: Bảo vệ DLNTD sử dụng dịch vụ NHS là tổng thể các quy phạm pháp luật đảm bảo quyền lợi hợp pháp về thông tin cho NTD sử dụng dịch vụ NHS, qua đó ngăn chặn các hành vi gian lận, trái pháp luật hoặc hưởng lợi bất hợp pháp về thông tin khi NTD tham gia các giao dịch với các tổ chức cung ứng dịch vụ NHS.

Khi các chủ thể kinh doanh NHS sử dụng DLNTD sẽ góp phần: (i) nâng cao hiệu suất hoạt động, cải thiện dịch vụ; (ii) đánh giá được khả năng, nhu cầu và thị hiếu của NTD mà không cần đến những dữ liệu truyền thống; (iii) giảm thiểu hạn chế rào cản về địa lý, gia tăng sự canh tranh khi cung cấp các dịch vụ NHS; (iv) nâng cao hiệu quả quản lý nhà nước về NHS. Tuy nhiên, bên cạnh những lợi ích như trên thì DLNTD cũng có những rủi ro, hạn chế như: (i) đối với nhà cung cấp khi thu thập DLNTD sẽ có rủi ro bảo mật dữ liệu, rủi ro an ninh mạng (bị hack, trộm cắp thông tin…) dẫn đến hoạt động kinh doanh bị gián đoạn và có thể bị tiết lộ trái phép, sử dụng sai mục đích gây thiệt hại cho NTD; (ii) đối với NTD khi sử dụng dịch vụ NHS, do hạn chế về sự hiểu biết nên NTD không kiểm soát được dữ liệu của mình dẫn tới mất kiểm

soát khi cung cấp hoặc bị chủ chể khác đánh cắp dễ dàng mà NTD không hay biết, DLNTD trở thành một "món hàng" được mua bán trên thị trường; (iii) đối với nhà nước thông qua ban hành pháp luật và giám sát bảo vệ DLNTD sử dụng dịch vụ NHS không đồng đều giữa các quốc gia, chưa theo kịp với sự phát triển của công nghệ hay thiếu sự phối hợp giữa các cơ quan chức năng đối với các loại hình dịch vụ NHS mới nên không kiểm soát được DLNTD.

3. Kinh nghiệm Liên minh châu Âu và một số quốc gia trên thế giới về bảo vệ dữ liệu người tiêu dùng sử dụng dịch vụ ngân hàng số

Tổng hợp từ kinh nghiệm của Liên minh châu Âu và một số quốc gia trên thế giới cho thấy, khung thành phần các yếu tố để thực hiện đầy đủ và hiệu quả bảo vệ DLNTD sử dụng dịch vụ NHS bao gồm [1]: (i) chính sách và môi trường pháp lý; (ii) phát triển sản phẩm và chuyển giao dịch vụ; (iii) nhận thức, khiếu nại và giải quyết của NTD; (iv) giám sát và thực thi; (v) phân khúc dễ bị tổn thương và rủi ro bất khả kháng. Theo đó:

Thứ nhất, về chính sách và môi trường pháp lý.

Hiện nay, trên thế giới có hơn 80 quốc gia đã ban hành luật bảo vệ dữ liệu [3]. Nghiên cứu chính sách và môi trường pháp lý của Liên minh châu Âu và một số quốc gia trên thế giới cho thấy có sự khác biệt trong các quy định liên quan đến dữ liệu với những cách tiếp cận mang tính đặc thù như sau:

- Khu vực châu Âu và Anh: Ngày 14/4/2016, Nghị viện châu Âu đã ban hành Quy định chung về bảo vệ dữ liệu (General Data Protection Regulation – GDPR), quy định này có hiệu lực ngày 25/5/2018. Mục tiêu mà GDPR hướng tới là bảo vệ dữ liệu cá nhân, xử lý dữ liệu cá nhân, chuyển giao dữ liệu tự do của cá nhân tại Liên minh châu Âu. Quy định này được áp dụng trực tiếp trên lãnh thổ các quốc gia thành viên. Đối với Vương quốc Anh, trước là thành viên của Liên minh châu Âu, năm 2016 người dân bỏ phiếu rời Liên minh châu Âu (được gọi là Brexit), năm 2018 quốc gia này đã ban hành Đạo luật về bảo vệ dữ liệu cá nhân vào năm 2018 (Data Protection Act 2018). Đạo luật này về cơ bản chuyển hóa các quy định của Liên minh châu Âu về bảo vệ dữ liệu cá nhân vào pháp luật quốc gia và cho phép tiếp tục áp dụng quy định của GDPR trên lãnh thổ quốc gia mặc dù Anh đã rời khỏi Liên minh châu Âu. GDPR đặt ra các nghĩa vụ của các tổ chức đối với việc xử lý dữ liệu cá nhân mà họ thu thập và xử lý. Theo đó, việc xử lý dữ liệu cá nhân phải được thực hiện trên cơ sở sự chấp thuận của chủ thể dữ liệu cá nhân hoặc trên cơ sở hợp đồng với người này; việc xử lý dữ liệu cá nhân phải được thực hiện trên cơ sở tôn trọng các quyền cơ bản của cá nhân. Quy định này áp dụng cả đối với các tổ chức có trụ sở, hoạt động ở bên ngoài lãnh thổ của Liên minh châu Âu khi họ hướng tới mục tiêu hoặc thu thập các dữ liệu liên quan đến người dân sống ở Liên minh châu Âu thì đều thuộc phạm vi điều chỉnh của Liên minh châu Âu [4]. Đối với ngân hàng mở, chỉ thị về dịch vụ thanh toán Châu Âu được sửa đổi năm 2019 (PSD2) yêu cầu các ngân hàng cung cấp quyền truy cập

vào thông tin tài khoản ngân hàng của khách hàng và bắt đầu thanh toán cho các nhà cung cấp bên thứ ba chỉ khi được sự đồng ý từ khách hàng.

- Tại Hoa kỳ: Thông qua Đạo luật hiện đại hóa dịch vụ tài chính (Gramm-Leach-Bliley) áp dụng cho các tổ chức tài chính và các doanh nghiệp cung cấp các sản phẩm và dịch vụ tài chính; Ủy ban Thương mại Liên bang (FTC) thúc đẩy việc bảo vệ dữ liệu cá nhân của NTD và có thể điều tra và xử lý các trường hợp không tuân thủ. Tuy nhiên, ở Mỹ không có chính sách sử dụng hoặc bảo mật dữ liệu quốc gia toàn diện vì vậy các bang phải xây dựng luật một cách độc lập. Năm 2018 California là bang đầu tiên thông qua Đạo luật về Quyền riêng tư của NTD. California thay đổi các yêu cầu về cách các doanh nghiệp trong tiểu bang xử lý dữ liệu và đặt tiền lệ cho các bang khác xem xét xây dựng luật tương tự. Trên cơ sở đó, có 11 bang khác của Hoa Kỳ bao gồm Maryland, New Jersey và Washington… gần đây đã đưa ra văn bản luật tương tự như: Đạo luật bảo vệ dữ liệu của NTD tại Virginia; Đạo luật về quyền riêng tư của Colorado...

- Khu vực Châu Á – Thái Bình Dương: Trung Quốc có các luật liên quan đến quyền sử dụng dữ liệu cá nhân bao gồm Luật Hình sự, Luật Dân sự và Luật An ninh mạng; Nhật Bản có Ủy ban bảo vệ thông tin cá nhân giám sát việc sửa đổi bổ sung Luật Bảo vệ thông tin cá nhân năm 2015; Úc có Quy định giám sát ngân hàng mở đã được ban hành bởi Bộ Ngân khố tháng 8/2017.

Nhật Bản là quốc gia đầu tiên trong số các nước ở Châu Á ban hành Đạo luật Bảo vệ dữ liệu cá nhân năm 2003 (APPI), có hiệu lực ngày 01 tháng 4 năm 2005 và được sửa đổi bổ sung năm 2017 cho phù hợp với GDPR năm 2016 của Châu Âu [5]. APPI được áp dụng đối với những nhà quản lý doanh nghiệp xử lý các thông tin cá nhân (Business operator handling personal information). Cụ thể hơn, nhà quản lý doanh nghiệp này có thể là thể nhân hay pháp nhân sử dụng dữ liệu thông tin cá nhân nhằm mục đích kinh doanh, ngoại trừ: i) các cơ quan nhà nước; ii) Chính quyền địa phương; (iii) những cơ quan hành chính được sáp nhập; và iv) những tổ chức hành chính độc lập ở địa phương. Phạm vi của APPI cũng mở rộng tới cả những pháp nhân nước ngoài thu thập và xử lý thông tin cá nhân tại Nhật Bản. Thêm vào đó, thậm chí nếu một pháp nhân nước ngoài không được thành lập tại Nhật Bản, một vài điều khoản trong APPI cũng sẽ được áp dụng đối với pháp nhân đó khi cung cấp sản phẩm hay dịch vụ cho cá nhân tại Nhật Bản và thu thập, xử lý dữ liệu cá nhân đó.

Tại khu vực Đông Nam Á, ngoại trừ Singapore và Việt Nam đã có đạo luật riêng về Bảo vệ dữ liệu cá nhân thì các quốc gia còn lại cũng chưa có Luật Bảo vệ dữ liệu cá nhân mà được quy định trong các văn bản quy phạm pháp luật như Hiến pháp, Luật, Nghị định và Thông tư theo đó:

- Indonesia: Bí mật đời tư, bí mật dữ liệu cá nhân là một quyền công dân, được quy định tại Điều 28G Hiến pháp năm 1945: Mỗi người đều có quyền tự bảo vệ bản thân, gia đình,

sự tôn trọng, nhân phẩm và tài sản của mình. Mỗi người đều có quyền được bảo đảm an ninh và sự bảo vệ khỏi các mối đe dọa sợ hãi để làm, hay không làm, một điều gì đó cấu thành một quyền con người.

- Thái Lan cũng chưa ban hành một đạo luật chuyên biệt về bảo vệ dữ liệu cá nhân. Tuy nhiên, khuôn khổ pháp lý bảo vệ dữ liệu cá nhân được xác lập bởi các văn bản pháp luật như: Hiến pháp Thái Lan năm 2007, các đạo luật chuyên ngành của Thái Lan như Bộ luật Dân sự và Thương mại, Luật Viễn thông, Luật Ngân hàng, Luật Kinh doanh Tài chính, Luật Giao dịch điện tử… Các văn bản này đều xác lập cơ chế bảo vệ đối với dữ liệu cá nhân trước các hành động thu thập, sử dụng, tiết lộ, chuyển giao thông tin một cách bất hợp pháp.

- Singapore: Nghị viện Singapore đã thông qua Luật Bảo vệ dữ liệu cá nhân ngày 15/10/2012. Luật công nhận quyền của các cá nhân trong việc bảo vệ các dữ liệu cá nhân của chính họ, đồng thời thừa nhận sự cần thiết của việc các tổ chức tiến hành thu thập, sử dụng và tiết lộ thông tin cá nhân vì những mục đích phù hợp với những hoàn cảnh nhất định. Bên cạnh Luật Bảo vệ dữ liệu cá nhân, một số văn bản pháp luật chuyên ngành của Singapore cũng quy định về vấn đề này như: Luật An ninh mạng và máy tính; Luật Bí mật công vụ, Luật Thống kê; Luật Giao dịch điện tử, Luật Ngân hàng, Luật Viễn thông…

Thứ hai, về phát triển sản phẩm và chuyển giao dịch vụ.

Tổ chức cung ứng và bên thứ ba phải có quy trình quản trị rủi ro nội bộ liên quan đến dữ liệu NHS, tại Nhật Bản Cơ quan dịch vụ tài chính (JFSA) đã khuyến khích các tổ chức tài chính tăng cường quản lý an ninh mạng thông qua hướng dẫn giám sát được công bố trên trang web cung cấp các quan điểm của giám sát như: Ban giám đốc có nhận ra tầm quan trọng của an ninh mạng trong bối cảnh các cuộc tấn công mạng ngày càng tinh vi, xảo quyệt và đã đưa ra môi trường giám sát cần thiết; các tổ chức tài chính có đưa ra hệ thống quản lý an ninh mạng thích hợp cũng như thiết lập các cơ cấu tổ chức và quy tắc; các tổ chức tài chính có phát triển các kế hoạch dự phòng chống lại các cuộc tấn công mạng tiềm ẩn, tiến hành diễn tập và xem xét các kế hoạch đó hay không. JFSA cũng tiến hành cuộc diễn tập thường niên cho toàn ngành tài chính (Delta Wall) từ năm 2016 nhằm tăng cường an ninh mạng trong ngành, năm 2017 có đến 100 tổ chức tài chính quy mô từ lớn đến nhỏ tham gia cuộc diễn tập [6].

Thứ ba, về tăng cường nhận thức, khiếu nại và giải quyết của NTD.

Tại Đức, Bộ Tư pháp liên bang và bảo vệ người dùng đã xuất bản tài liệu toàn diện về quyền của NTD với dữ liệu của họ, hướng dẫn cách tránh cung cấp dữ liệu không cần thiết và cách sử dụng mạng internet an toàn, tài liệu có phiên bản tải xuống miễn phí và thông tin phù hợp với cả người cao tuổi; cơ quan Giám sát tài chính liên bang Đức cung cấp cho NTD hướng dẫn sử dụng dữ liệu cá nhân khi sử dụng dịch vụ tài chính, tổ chức hội thảo trực tuyến cho người cao tuổi phổ biến Chỉ thị dịch vụ thanh toán lần thứ 2 (PSD2) năm 2019. Tại Bồ Đào Nha, hiểu biết về tài chính kỹ thuật số là một trong những mục tiêu chiến lược của Ngân hàng trung

ương 2017-2020, năm 2018 Ngân hàng trung ương đã phát động chiến dịch giáo dục tài chính kỹ thuật số và các biện pháp phòng ngừa rủi ro khi sử dụng dịch vụ tài chính số với người trẻ. Tại Tây Ban Nha, trang web chiến lược quốc gia cung cấp thông tin cần thiết liên quan đến bảo vệ thông tin cá nhân trong giao dịch trực tuyến, một phần về bảo vệ thông tin cá nhân được bao gồm trong chương trình giáo dục tài chính dành cho các trường học và học sinh từ 14 đến 18 tuổi.

Thứ tư, về vấn đề giám sát và thực thi.

Đối với giám sát và thực thi, các tiêu chuẩn và quy tắc ứng xử bảo vệ dữ liệu theo định hướng của ngành vẫn là một vấn đề mới trong các dịch vụ tài chính kỹ thuật số, các tiêu chuẩn được đưa ra phải khả thi và hướng dẫn cụ thể cho các nhà cung cấp và các bên liên quan trong ngành. Vào tháng 9/2018, OECD đã thành lập nhóm chuyên gia hơn 50 thành viên về AI đại diện cho 20 Chính phủ và các nhà lãnh đạo đến từ các lĩnh vực doanh nghiệp, lao động, xã hội, khoa học để phát triển bộ nguyên tắc về AI. Theo đó khuyến nghị của OECD về AI đã được phê duyệt vào tháng 6/2019 trong đó bao gồm 2 nguyên tắc đặc biệt có liên quan đến dữ liệu cá nhân và dịch vụ tài chính: AI phải lấy con người làm giá trị trung tâm và đối xử công bằng, các hoạt động AI phải thực hiện cung cấp thông tin minh bạch và chi tiết về hệ thống phân tích, kết quả và cách tương tác với hệ thống [7].

Thứ năm, về phân khúc dễ bị tổn thương.

Một số quốc gia như Ấn Độ, Mexico, Nam Phi, Peru đã xây dựng bộ phận thanh tra chính thức như một bộ phận để giải quyết tranh chấp cho NTD tài chính trong đó có bao gồm nhóm người dùng yếu thế (người nghèo, phụ nữ nông thôn…). Tại Mexico, Ủy ban quốc gia về Bảo vệ người sử dụng dịch vụ tài chính *(Condusef)* đã khởi động chương trình *"Financial Education Programme in your institution (EFI)"* vào năm 2010 với hơn 310 tổ chức trên toàn quốc tham gia. Người sử dụng lao động được tham gia chương trình miễn phí, chi phí do Condusef đài thọ từ ngân sách được Bộ Tài chính quy định. Chương trình được thiết kế để tích hợp bất kỳ công ty nào có nhu cầu cung cấp giao dịch tài chính và nâng cao năng lực tài chính của người lao động, và được gửi qua các kênh kỹ thuật số nội bộ như email của công ty, bảng tin và các kênh liên lạc nội bộ.

4. Thực trạng về bảo vệ dữ liệu người tiêu dùng sử dụng dịch vụ ngân hàng số tại Việt Nam

Việt Nam là một trong những quốc gia có tốc độ phát triển và ứng dụng internet cao nhất thế giới. Theo các báo cáo và thống kê đầu năm 2023, Việt Nam có tổng cộng 77,93 triệu người dùng internet (chiếm 79,1% dân số) [8]. Trong lĩnh vực ngân hàng, NHS được cho là mảng kinh doanh riêng hướng đến phân khúc khách hàng mới, độc lập với hoạt động kinh doanh truyền thống. Điển hình là Timo của VPBank, LiveBank của TPBank. Đây được coi là mô hình NHS

hoàn toàn tự động 24/7 có thể thực hiện gần như đầy đủ các giao dịch như một chi nhánh truyền thống mà khách hàng không cần phải tiếp xúc trực tiếp với nhân viên ngân hàng. Những ngân hàng có quy mô lớn như Vietcombank, VietinBank, BIDV, ACB, MB… thì tập trung chuyển đổi số các hoạt động kinh doanh truyền thống kết hợp với việc tạo ra những sản phẩm, kênh dịch vụ mới cho khách hàng, đồng thời khai thác những mảng kinh doanh mới trên cơ sở kết hợp với các ứng dụng Fintech. Quá trình chuyển đổi số của các ngân hàng lớn thường gắn liền với việc nâng cấp căn bản hệ thống hạ tầng công nghệ thông tin, đặc biệt công nghệ lõi (Core Banking). Điển hình là VietinBank với Core Sunshine (2017), YOLO của VPBank cho NHS (tách biệt với hệ thống hiện tại). Các ngân hàng thương mại cũng đã có sự liên kết với nền tảng thanh toán chung để khai thác triệt để lợi thế và sức mạnh của công nghệ số trong hoạt động ngân hàng. Chuyển đổi số của các ngân hàng thương mại Việt Nam còn giúp mở rộng sự hợp tác giữa ngân hàng với các doanh nghiệp Fintech hay các "ông lớn" công nghệ như Google, Facebook… để mang lại lợi ích cho ngân hàng cũng như khách hàng. Đây chính là nền tảng quan trọng để tiến dần đến trạng thái kết nối vạn vật (IoT). Một số hoạt động điển hình như: VietinBank kết hợp với Opportunity Network trong cung cấp nền tảng số cho doanh nghiệp, Vietcombank với M-Service trong thanh toán, MBB – Startup Fintech trong cung cấp dịch vụ ngân hàng, VPB – Fintech Weezi trong thanh toán chuyển tiền qua mạng xã hội, Techcombank – Fastcash chuyển tiền qua mạng Facebook… [9].

Tuy nhiên, tình trạng lộ, lọt, hoạt động đánh cắp, mua bán dữ liệu cá nhân diễn ra phổ biến ở hầu hết các quốc gia trên thế giới trong đó có Việt Nam. Theo ghi nhận từ Cổng Cảnh báo An toàn thông tin Việt Nam, năm 2022, diễn ra hơn 12.935 trường hợp lừa đảo trực tuyến, với 2 loại hình chính là lừa đảo để đánh cắp thông tin cá nhân và lừa đảo tài chính [11]. Theo thống kê của hãng bảo mật quốc tế, Việt Nam nằm trong nhóm 3 quốc gia bị tấn công mạng nhiều nhất tại khu vực châu Á – Thái Bình Dương; chỉ riêng 6 tháng đầu năm 2023, các cơ quan chức năng đã phát hiện gần 17 triệu cảnh báo dấu hiệu hoạt động tấn công mạng (tăng 240% so với cùng kỳ năm 2022), trong đó có 208 hệ thống thông tin của cơ quan Nhà nước, các bộ, ban, ngành bị tin tặc tấn công nhằm mục đích đánh cắp thông tin, dữ liệu, tài liệu bí mật nhà nước thuộc nhiều lĩnh vực. Nổi lên là các chiến dịch tấn công mạng nguy hiểm của các tin tặc có nguồn gốc từ nước ngoài, sử dụng 15 biến thể mã độc nguy hiểm, trong đó có các loại mã độc hiện đại, có khả năng vô hiệu hóa các phần mềm bảo vệ để "nằm vùng" lâu dài, thâm nhập sâu vào các hệ thống, đáng chú ý có sự câu kết, móc nối giữa tin tặc trong và ngoài nước. Cơ quan chức năng cũng phát hiện hơn 4.000 nguồn khởi phát thông tin xấu độc, thu hút hơn 82 triệu lượt tiếp cận, tương tác thông tin, chủ yếu trên các nền tảng mạng xã hội, với hàng nghìn tài khoản, "hội nhóm" có hàng triệu lượt người theo dõi. Tình trạng lộ, mất tài liệu bí mật nhà nước trên không gian mạng tiếp tục được phát hiện, trong 3 năm qua, cơ quan chức năng đã phát hiện, xử lý hơn 150 vụ việc với 710 đầu tài liệu bị lộ, trong đó có nhiều tài liệu thuộc danh mục tài liệu mật, tối mật, tuyệt mật. Trong 6 tháng đầu năm 2023, đã phát hiện 25 vụ đăng tải, truyền đưa thông tin, tài liệu bí mật nhà nước trên không gian mạng với 58 đầu tài liệu mật;

hơn 200 GB dữ liệu nội bộ, tài liệu nhạy cảm của các cơ quan, đơn vị thuộc các bộ, ngành, địa phương bị lộ, lọt, rao bán trên các diễn đàn, hội nhóm [10].

Thực trạng bảo vệ DLNTD NHS tại Việt Nam đang tồn tại một số hạn chế sau:

Thứ nhất, quy định pháp luật về bảo vệ dữ liệu cá nhân chưa đồng nhất với các quy định pháp luật ngân hàng.

Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính Phủ về bảo vệ dữ liệu cá nhân là bước đột phá về bảo đảm quyền con người trong chuyển đổi số, khắc phục những tồn tại, bất cập trong thực tiễn bảo đảm, bảo vệ, bảo mật dữ liệu cá nhân. Đây cũng là văn bản bảo vệ DLNTD trong hoạt động NHS tại Việt Nam. Tuy nhiên, hoạt động ngân hàng của các tổ chức tín dụng được điều chỉnh bởi các quy định pháp luật chuyên ngành như: Luật Các tổ chức tín dụng năm 2010 được sửa đổi, bổ sung năm 2017, Luật Phòng chống rửa tiền năm 2022; Nghị định 117/2018/NĐ-CP về giữ bí mật, cung cấp thông tin khách hàng của tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, Thông tư số 09/2020/TT-NHNN của Ngân hàng Nhà nước quy định về an toàn hệ thống thông tin trong hoạt động ngân hàng. Theo đó, đối với hoạt động ngân hàng, việc xử lý dữ liệu tác động tới dữ liệu cá nhân, như: Thu thập, ghi, phân tích, xác nhận, lưu trữ, chỉnh sửa, công khai, kết hợp, truy cập, truy xuất, thu hồi, mã hóa, giải mã, sao chép, chia sẻ, truyền đưa, cung cấp, chuyển giao, xóa, hủy dữ liệu cá nhân hoặc các hành động khác có liên quan là tất yếu nhằm cung cấp dịch vụ cho khách hàng và quản lý rủi ro trong hoạt động ngân hàng, bảo đảm an toàn an ninh của hệ thống tiền tệ nên nhiều hoạt động xử lý dữ liệu khách hàng cá nhân không thể và không cần sự chấp thuận của khách hàng trong khi đó tại Khoản 2, Điều 3 và Khoản 1, Điều 9 của Nghị định 13/2023/NĐ-CP quy định chủ thể có quyền được biết về việc xử lý dữ liệu cá nhân của mình. Hay tại Khoản 2, Điều 9 Nghị định 13/2023/NĐ-CP quy định chủ thể có quyền không đồng ý xử lý dữ liệu cá nhân của mình; chủ thể có quyền xóa, truy cập, yêu cầu hạn chế xử lý dữ liệu, phản đối xử lý dữ liệu, trừ trường hợp Luật khác có quy định khác tại Điều 9. Như vậy, sẽ vướng mắc, bất cập nếu áp dụng Nghị định cứng nhắc và không có hướng dẫn thống nhất.

Thứ hai, Việt Nam cũng chưa có cơ quan quản lý độc lập đối với bảo vệ NTD tài chính.

Hiện nay, có 5 cơ quan có thể tham gia bảo vệ NTD dịch vụ tài chính: Ngân hàng Nhà nước Việt Nam (trong lĩnh vực ngân hàng, Ngân hàng Nhà nước Việt Nam lập Vụ Thanh tra hành chính, giải quyết khiếu nại, tố cáo và phòng, chống tham nhũng (trực thuộc Cơ quan Thanh tra, giám sát ngân hàng) với trách nhiệm thanh tra hành chính và xử lý những khiếu nại, tố cáo liên quan đến các cá nhân, tổ chức trực thuộc Ngân hàng Nhà nước Việt Nam quản lý trực tiếp. Do đó, đối với những khiếu nại của người dân về dịch vụ tài chính sẽ do đơn vị nêu trên giải quyết và báo cáo lại với Ngân hàng Nhà nước Việt Nam), Ủy ban Chứng khoán Nhà nước, Cục Quản lý, giám sát bảo hiểm, Cục Cạnh tranh và Bảo vệ người tiêu dùng (trực thuộc Bộ Công thương) và Hội bảo vệ Người tiêu dùng. Tuy nhiên, các khiếu nại, tranh chấp được

giải quyết bởi nhiều cơ quan chức năng nhưng lại thiếu đi sự phân định rành mạch về chức năng, nhiệm vụ cũng như chỉ định cơ quan đầu mối phụ trách nên việc khiếu nại, xử lý tranh chấp chưa được thỏa đáng, khiến NTD phải đưa ra toà án để giải quyết.

Thứ ba, các quy định pháp luật xử lý vi phạm quyền DLNTD chưa thực sự phù hợp.

Theo Điều 66 Nghị định số 174/2013/NĐ-CP ngày 13/11/2013 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, công nghệ thông tin và tần số vô tuyến điện quy định mức phạt tiền nặng nhất đối với vi phạm quyền về sự riêng tư là 70 triệu, theo pháp luật hình sự là 200 triệu đồng (Điều 288 Bộ luật Hình sự năm 2015, sửa đổi, bổ sung năm 2017). Trong khi đó, GDPR áp dụng mức phạt lên tới 20 triệu Euro hoặc 4% doanh thu toàn cầu hàng năm. Tháng 7/2019, hãng hàng không British Airway của Anh bị Liên minh Châu Âu phạt 228 triệu USD sau khi bị tin tặc đánh cắp thông tin cá nhân và dữ liệu tài chính của hàng trăm nghìn khách hàng. Mỹ Tháng 7/2019, Facebook bị Ủy ban thương mại Mỹ (FTC) phạt 5 tỷ USD vì bê bối dữ liệu Cambridge Analytica để lộ dữ liệu của hơn 50 triệu người dùng hay tháng 9/2019, FTC đã phạt Google 150 triệu USD vì thu thập dữ liệu trẻ em trái phép qua ứng dụng YouTube [12]. Từ sự so sánh này, có thể thấy mức phạt trong luật pháp Việt Nam còn quá nhẹ so với mức độ nguy hại và hậu quả của hành vi xâm phạm quyền này.

Thứ tư, nhận thức về bảo vệ dữ liệu cá nhân của NTD còn thấp.

Nhiều thông tin sinh trắc học, lý lịch cá nhân, mối quan hệ, tình trạng sức khỏe, tài chính của khách hàng được đăng tải công khai, trở thành nguồn để các phần mềm thu thập dữ liệu cho thấy nhận thức bảo vệ các tài sản dữ liệu cá nhân của một bộ phận không nhỏ khách hàng còn thấp, nhiều khách hàng không nắm rõ bản chất các sản phẩm dịch vụ tài chính trực tuyến dẫn đến bị lạm dụng thông tin cá nhân không kiểm soát. Bản thân mỗi cá nhân cần hiểu quyền với thông tin cá nhân của mình cũng như nghĩa vụ với việc bảo vệ thông tin của người khác.

Thứ năm, lưu trữ, bảo quản, xử lý DLNTD của tổ chức cung ứng dịch vụ NHS còn hạn chế.

Thực tế tại Việt Nam, các ngân hàng hiện đang tiếp cận quản trị dữ liệu theo hai phương pháp chủ đạo là đổi mới sáng tạo, tự động hóa quy trình kinh doanh và kiểm soát dữ liệu để phục vụ mục đích tuân thủ, cải thiện hiệu quả hoạt động. Trong vòng 2 năm trở lại đây, năng lực quản trị dữ liệu đã phát triển vượt bậc tại nhiều định chế tài chính trên toàn cầu, tuy vậy đối với ngân hàng trong nước vẫn còn một khoảng cách rất xa để đáp ứng kịp thời các nhu cầu kinh doanh và tuân thủ. Theo khảo sát của PwC năm 2019, phần lớn các ngân hàng Việt Nam vẫn đang ở trong giai đoạn đầu tiên trong lộ trình triển khai quản trị dữ liệu toàn hàng: dưới 50% ngân hàng đã xây dựng chính sách và quy trình quản lý dữ liệu toàn hàng hay quy định vai trò của các bên có liên quan đến dữ liệu; trên 66% ngân hàng chưa vận hành quy định các tiêu chí đánh giá để đo lường chất lượng dữ liệu; chỉ 18% ngân hàng đã xây dựng kiến trúc công nghệ để hỗ trợ quản lý dữ liệu toàn hàng [13].

5. Gợi ý cho Việt Nam

Trên cơ sở kinh nghiệm của Liên minh châu Âu và một số quốc gia đi trước về bảo vệ DLNTD. Căn cứ vào thực trạng pháp luật và thực hiện pháp luật về bảo vệ DLNTD ở Việt Nam. Tác giả kiến nghị các nhóm giải pháp sau:

Thứ nhất, hoàn thiện chính sách và môi trường pháp lý về bảo vệ DLNTD.

Một là, vấn đề bảo vệ DLNTD cần được xác định là một trong những nội dung chính của chiến lược phát triển kinh tế số và chiến lược tài chính toàn diện của quốc gia. Cùng với đó là hoàn thiện khung pháp lý liên quan đến bảo vệ NTD tài chính, trong ngắn hạn phải bổ sung các quy định về bảo vệ NTD tài chính trong Luật bảo vệ quyền lợi người tiêu dùng, về lâu dài cần ban hành một Đạo luật bảo về quyền lợi NTD tài chính cho phù hợp với thông lệ quốc tế. Cùng với đó là hoàn thiện các quy định về bảo vệ DLNTD trong Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính Phủ về bảo vệ dữ liệu cá nhân cho phù hợp với các quy định trong pháp luật ngân hàng.

Hai là, nên thành lập cơ quan chuyên trách về bảo vệ NTD tài chính trong đó có lĩnh vực NHS, cùng với đó cần có cơ chế hợp tác giải quyết tranh chấp khiếu nại về DLNTD NHS, cơ chế chia sẻ thông tin giữa các cơ quan quản lý nhà nước liên quan cần được quy định cụ thể trong văn bản pháp luật hướng dẫn thực hiện Nghị định bảo vệ dữ liệu cá nhân.

Ba là, Ngân hàng nhà nước Việt Nam cần có quy định và chế tài yêu cầu các tổ chức cung ứng dịch vụ NHS tích hợp các điều khoản về quyền riêng tư và bảo vệ dữ liệu người dùng vào các chính sách sản phẩm hiện có, minh bạch và công khai các điều khoản và điều kiện cung cấp sản phẩm dịch vụ đối với khách hàng như quy trình khôi phục, chia sẻ dữ liệu NTD, phạt vi phạm và thông tin khác..., có các chính sách nội bộ về quyền riêng tư dữ liệu và bảo vệ dữ liệu, có các điều khoản ràng buộc quyền riêng tư và bảo vệ dữ liệu đối với bên thứ 3 hợp tác cung cấp sản phẩm dịch vụ NHS.

Thứ hai, trách nhiệm của Nhà nước đối với vấn đề bảo vệ DLNTD.

Một là, cần tăng cường hoạt động thanh tra, giám sát đối với các chủ thể thực hiện cung ứng dịch vụ NHS, đồng thời xử lý nghiêm các chủ thể vi phạm về bảo vệ DLNTD trong hoạt động NHS.

Hai là, tuyên truyền, nâng cao nhận thức về bảo vệ dữ liệu cho NTD đặc biệt là NTD yếu thế về dịch vụ NHS với các rủi ro có thể phát sinh với dữ liệu cá nhân trong giao dịch NHS thông qua các phương tiện truyền thông.

Thứ ba, đối với các tổ chức cung cấp dịch vụ NHS.

Một là, cần thực thi đúng và đầy đủ các quy định pháp luật đối với quản lý DLNTD, xây dựng các quy trình quản trị rủi ro nội bộ liên quan đến bảo vệ DLNTD, đưa ra các biện pháp khắc phục trong trường hợp xảy ra các sự cố an ninh mạng gây phương hại cho NTD.

Hai là, nâng cấp hạ tầng ứng dụng dịch vụ số và chú trọng quản lý an ninh mạng. Tổ chức cung ứng dịch vụ NHS cần quan tâm đến việc nâng cấp hạ tầng dịch vụ số tránh những sự cố kỹ thuật, đồng thời, xây dựng và nâng cấp hệ thống an ninh, bảo mật ở mức cao. Triển khai đồng bộ các giải pháp bảo vệ, phòng, chống lộ, lọt dữ liệu trên toàn bộ hệ thống thông tin; tăng cường kiểm tra, giám sát toàn bộ quy trình đặc biệt là khâu có tiềm ẩn phát sinh rủi ro về an toàn thông tin. Xây dựng các quy trình, kịch bản và tổ chức diễn tập định kỳ ứng phó với các sự cố, rủi ro mất an toàn thông tin để nâng cao năng lực ngăn chặn, giảm các tác động tiêu cực, hậu quả của các cuộc tấn công mạng.

Ba là, cần nâng cao chất lượng nguồn nhân lực ngành tài chính ngân hàng thời kinh tế số, nhằm đào tạo nguồn nhân lực công nghệ cao trong hệ thống NHS, góp phần hướng dẫn, thông tin, hỗ trợ NTD dịch vụ NHS chính xác, nhanh chóng, đầy đủ và minh bạch.

Thứ tư, đối với người tiêu dùng sử dụng dịch vụ NHS.

Mỗi NTD sử dụng dịch vụ NHS phải có trách nhiệm bảo vệ dữ liệu của cá nhân mình, chủ động phòng chống sự gian lận, tránh bị kẻ gian lừa đảo lợi dụng chiếm doạt dữ liệu cá nhân; không nên cung cấp thông tin bảo mật các dịch vụ NHS, bảo vệ và thay đổi thường xuyên mật khẩu truy cập các dịch vụ NHS bảo đảm theo nguyên tắc an toàn; không truy cập các trang web không đáng tin cậy, hoặc nhập vào bất kỳ đường link nào yêu cầu cung cấp, cập nhật thông tin cá nhân và thông tin dịch vụ NHS; đọc kỹ các điều khoản hợp đồng trước khi chấp nhận sử dụng các dịch vụ NHS…

6. Kết luận

Thông qua việc tìm hiểu pháp luật, thực thi pháp luật về bảo vệ DLNTD sử dụng dịch vụ NHS của Liên minh châu Âu và một số quốc gia trên thế giới cho thấy rằng ở Việt Nam, NHS mặc dù còn khá mới, tuy nhiên NHS là xu hướng phát triển tất yếu của ngân hàng. Bảo vệ DLNTD sử dụng dịch vụ NHS là chìa khóa then chốt quyết định sự ổn định và phát triển của các NHS. Bảo vệ dữ liệu cá nhân nói chung và DLNTD sử dụng dịch vụ NHS nói riêng đang còn yếu. Điều này xuất phát từ nhiều nguyên nhân khác nhau, song không thể phủ nhận một trong những nguyên nhân đó là sự thiếu hoàn thiện của các quy định pháp luật và thực thi pháp luật về bảo vệ DLNTD sử dụng dịch vụ NHS. Hoàn thiện pháp luật về bảo vệ DLNTD sử dụng dịch vụ NHS là hết sức quan trọng và cần thiết, cùng với các giải pháp về kỹ thuật, công

nghệ, con người… là vấn đề được chú trọng nhằm đảm bảo sự phát triển hệ thống ngân hàng trong tương lai ở Việt Nam.

TÀI LIỆU THAM KHẢO

1. AFI (2020), *Policy model on consumer protection for digital financial services*, truy cập tại: https://www.afi-global.org/publications/3465/Policy-Model-on-Consumer-Protection-for-Digital-Financial-Services, truy cập ngày 15/12/2023.
2. Thiếu Quang Hiệp (2020), Phát triển ngân hàng số ở Việt Nam: Thực trạng và đề xuất, *Tạp chí Tài chính*, Kỳ 2 – tháng 6/2020.
3. Báo cáo *"Vai trò, tầm quan trọng của công tác bảo vệ dữ liệu cá nhân trong thời đại số"*, Hội thảo chia sẻ kinh nghiệm về bảo vệ dữ liệu cá nhân trên không gian mạng, tập trung vào nhóm đối tượng yếu thế tại Việt Nam, Bộ Công an, Liên minh Châu Âu, Hà Nội, 2020, tr. 3.
4. Liên minh Châu Âu (2016), *Quy định chung về bảo vệ dữ liệu (GDPR) của Liên minh Châu Âu*.
5. *Bảo vệ dữ liệu ở Nhật Bản để phù hợp với GDPR*, truy cập tại: https://www.skadden.com/insights/publications/2018/09/quarterly-insights/data-protection-in-japan-to-align-with-gdpr, truy cập ngày 20/12/2023.
6. *Kinh nghiệm quản lý chuyển đổi số ngành Ngân hàng tại một số quốc gia châu Á và hàm ý chính sách cho Việt Nam*, truy cập tại: https://tapchinganhang.gov.vn/kinh-nghiem-quan-ly-chuyen-doi-so-nganh-ngan-hang-tai-mot-so-quoc-gia-chau-a-va-ham-y-chinh-sach-cho.htm, truy cập ngày 20/12/2023.
7. OECD (2018), *G20/OECD Policy Guidance on Financial Consumer Protection Approaches in the Digital Age*, truy cập tại: https://www.oecd.org/finance/G20-OECD-Policy-Guidance-Financial-Consumer-Protection-Digital-Age-2018.pdf, truy cập ngày 25/12/2023.
8. *Internet Việt Nam 2023: Số liệu mới nhất và xu hướng phát triển, truy cập tại*, https://www.vnetwork.vn/vi/news/internet-viet-nam-2023-so-lieu-moi-nhat-va-xu-huong-phat-trien, truy cập ngày 25/12/2023.
9. https://tapchinganhang.gov.vn/phat-trien-ngan-hang-so-o-viet-nam-buc-tranh-hien-tai-va-trien-vong.htm, truy cập ngày 15/02/2024.

10. *An toàn, an ninh mạng: Thực trạng và khuyến cáo*, truy cập tại: https://vjst.vn/vn/_layouts/15/ICT.Webparts.TCKHCN/mt_poup/Intrangweb.aspx?IdNews=8126, truy cập ngày 20/02/2024.
11. *Chế tài xử lý các hành vi vi phạm quy định bảo vệ dữ liệu cá nhân*, truy cập tại: https://antoanthongtin.vn/chinh-sach---chien-luoc/che-tai-xu-ly-cac-hanh-vi-vi-pham-quy-dinh-bao-ve-du-lieu-ca-nhan-107563, truy cập ngày 23/02/2024.
12. *Ngân hàng hướng tới khai thác quản trị dữ liệu để thúc đẩy tăng trưởng*, truy cập tại: https://bankingplus.vn/ngan-hang-huong-toi-khai-thac-quan-tri-du-lieu-de-thuc, truy cập ngày 23/02/2024.
13. *World Retail Banking report 2021*, truy cập tại: https://www.capgemini.com/news/press-releases/world-retail-banking-report-2021-to-create-new-value-banks-can-adopt-banking-as-a-service-to-embed-finance-in-consumer-lifestyles/, truy cập ngày 25/02/2024.
14. *Triển khai các chương trình giáo dục tài chính cho người lao động tại các nước OECD*, truy cập tại: https://sbv.gov.vn/webcenter/portal/vi/menu/fm/ddnhnn/nctd/nctd_chitiet?leftWidth=20%25&showFooter=false&showHeader=false&dDocName=SBV511808&rightWidth=0%25&centerWidth=80%25&_afrLoop=31877580298384023#%40%3F_afrLoop%3D31877580298384023%26centerWidth%3D80%2525%26dDocName%3DSBV511808%26leftWidth%3D20%2525%26rightWidth%3D0%2525%26showFooter%3Dfalse%26showHeader%3Dfalse%26_adf.ctrl-state%3D7fkrtghgz_9., truy cập ngày 28/02/2024.