BẢO ĐẢM AN TOÀN THÔNG TIN TRONG GIAO DỊCH ĐIỆN TỬ THEO PHÁP LUẬT MỘT SỐ QUỐC GIA VÀ ĐỀ XUẤT CHO VIỆT NAM[1]

NGUYỄN THỊ LONG* - HOÀNG MẠNH CƯỜNG**

Tóm tắt: Bài viết tập trung nghiên cứu pháp luật một số quốc gia trên thế giới về bảo đảm an toàn thông tin trong giao dịch điện tử. Thông qua đó, đề xuất các nội dung hoàn thiện khung pháp lý về bảo đảm an toàn thông tin trong giao dịch điện tử tại Việt Nam.

Từ khoá: Định danh điện tử, chữ ký điện tử, an toàn, thông tin, giao dịch điện tử, dữ liệu

Ngày nhận bài: 29/3/2023; Biên tập xong: 22/5/2023; Duyệt đăng: 24/7/2023

ENSURING INFORMATION SECURITY IN ELECTRONIC TRANSACTIONS IN SOME NATIONS' LEGAL REGULATION AND RECOMMENDATIONS FOR VIETNAM

Abstract: The article focuses on studying the laws of some countries around the world on ensuring information security in electronic transactions. Thereby, proposing solutions to improve the legal framework on ensuring information security in electronic transactions in Vietnam.

Keywords: Electronic identity, electronic signature, safety, information, electronic transactions, data

Received: Mar 29th, 2023; Editing completed: May 22nd, 2023; Accepted for publication: Jul 24th, 2023

1. Sự cần thiết của việc nghiên cứu pháp luật về bảo đảm an toàn thông tin trong giao dịch điện tử

Theo Báo cáo kinh tế Internet khu vực Đông Nam Á của Google dự báo thương mại điện tử Việt Nam sẽ đạt khoảng 29 tỷ USD vào năm 2025 với mức tăng trưởng 34% so với năm 2020. Nền kinh tế số tại Việt Nam từ 03 tỷ USD năm 2015 đã tăng lên 12 tỷ USD vào năm 2019 và 14 tỷ USD năm 2020[2]. Trong nền kinh tế số, giao dịch điện tử là yếu tố chủ đạo kết nối các chủ thể với nhau. Luật Giao dịch điện tử (GDĐT) năm 2005 đã ghi nhận giá trị pháp lý của GDĐT thông qua thông điệp dữ liệu, chữ ký điện tử. Từ quy định của luật này, các lĩnh vực xây dựng quy định hướng dẫn tạo thuận lợi cho các giao dịch dân sự, thương mại và giảm thiểu thủ tục hồ sơ hành chính[3].

Thương mại điện tử và sự gia tăng số lượng các GDĐT cũng kéo theo nhiều rủi ro, đặc biệt là những rủi ro trong an toàn thông tin GDĐT, ảnh hưởng tiêu cực các bên tham gia. Việc lộ lọt dữ liệu khách hàng dẫn đến tình trạng tráo hàng, đổi hàng, giao hàng kém chất lượng, giả mạo khách hàng thân thiết để trục lợi xảy ra thường xuyên… Sau gần 16 năm thực hiện, đến nay Luật GDĐT năm 2005 về bảo đảm an toàn thông tin trong GDĐT cũng đang bộc lộ những bất cập, nhiều nội dung không còn phù hợp với thực tế phát triển, xây dựng nền kinh tế số của Việt Nam trong

---

[1] Bài báo này được thực hiện trong khuôn khổ đề tài của Trường Đại học Luật Hà Nội, *"Pháp luật Việt Nam về bảo đảm an toàn thông tin trong giao dịch điện tử"* và được thực hiện bởi nhóm tác giả: Nguyễn Thị Long, Hoàng Mạnh Cường – MSSV: 440958, Lê Thúy Anh, MSSV: 440953, sinh viên trường Đại học Luật Hà Nội.

[2] Xem: Nhĩ Anh (2021), *"Doanh thu thương mại điện tử Việt Nam tăng trưởng 18%"*, Link truy cập: https://vneconomy.vn/doanh-thu-thuong-mai-dien-tu-viet-nam-tang-truong-18.htm, ngày truy cập: 14/3/2022.

** Email: Longnt@hlu.edu.vn*
Thạc sĩ, Giảng viên Khoa Pháp luật Dân sự, Trường Đại học Luật Hà Nội
*** Email: Cuongdtm123@gmail.com*
Sinh viên Khoa Pháp luật Hình sự, Trường Đại học Luật Hà Nội

[3] Link truy cập: https://duthaoonline.quochoi.vn/Pages/dsduthao/chitietduthao.aspx?id=7399, ngày truy cập: 23/3/2023.

giai đoạn tới. Cụ thể:

Một là, Luật GDĐT năm 2005 chưa đề cập đến quy định về giá trị pháp lý cho một số yếu tố quan trọng trong GDĐT như: Thông điệp dữ liệu an toàn, chữ ký điện tử và chứng thực chữ ký điện tử, tổ chức, cá nhân GDĐT, xác thực thông tin người GDĐT, quá trình tập hợp thông tin về người GDĐT, chủ thể GDĐT và thông tin về chủ thể GDĐT, dịch vụ tin cậy và nhà cung cấp dịch vụ tin cậy. Luật cũng chưa có quy định làm rõ giá trị pháp lý và chứng cứ của thông điệp dữ liệu khi việc lưu trữ của thông điệp dữ liệu đã được chuyển đổi với bản giấy.

Hai là, Luật GDĐT năm 2005 chưa đồng bộ với một số nội dung về an toàn thông tin mạng và an ninh mạng quy định tại Luật An toàn thông tin mạng năm 2015 và Luật An ninh mạng năm 2018. Luật GDĐT năm 2005 cũng chưa quy định cụ thể về an toàn cho dữ liệu, an toàn thông tin trong GDĐT[4]. Luật còn thiếu quy định về an toàn sử dụng công nghệ, kỹ thuật trong GDĐT nhằm tránh được các rủi ro cho người dùng do rò rỉ thông tin, dữ liệu; chuyển đổi hình thức giữa văn bản giấy và thông điệp dữ liệu; quy định về giá trị pháp lý của chữ ký điện tử chưa tạo điều kiện cho các chủ thể tự lựa chọn loại chữ ký điện tử phù hợp với nhu cầu về tính khả dụng và độ an toàn; quy định về sử dụng và công nhận chữ ký điện tử nước ngoài còn chưa phù hợp thực tiễn[5]…

Ba là, một số quy định của Luật GDĐT cần được điều chỉnh đảm bảo cập nhật với các quy định mới của Luật An toàn thông tin mạng, Luật An ninh mạng và Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân. Những quy định cần đảm bảo thống nhất liên quan điến quyền và nghĩa vụ của chủ thể dữ liệu cá nhân nói chung và quyền của chủ thể này khi tham gia vào GDĐT. Đặc biệt, các chủ thể xử lý dữ liệu cá nhân liên quan đến GDĐT cũng cần chú trọng tuân thủ quy định về đảm bảo an toàn thông tin cho chủ thể dữ liệu là người tham gia GDĐT.

Từ những vấn đề được đề cập ở trên cho thấy, việc nghiên cứu nội dung bảo đảm an toàn thông tin trong GDĐT nói chung và việc nghiên cứu kinh nghiệm của các quốc gia trên thế giới về bảo đảm an toàn thông tin trong GDĐT là thực sự cần thiết.

2. Pháp luật của Singapore về bảo đảm an toàn thông tin trong giao dịch điện tử

GDĐT ở Singapore đã và đang phát triển mạnh mẽ, ngày càng đóng vai trò quan trọng trong sự phát triển kinh tế của đất nước này. Năm 1998, Singapore cho ban hành *Luật Giao dịch điện tử (Electronic Transaction Act (ETA) 1998)*[6] nhằm mục đích giải quyết các vướng mắc, khó khăn về mặt pháp lý khi các chủ thể tham gia vào các giao dịch trong một môi trường phi giấy tờ và không tiếp xúc trực tiếp với nhau. Năm 2010, ETA đã được cập nhật để phù hợp hơn với hướng dẫn của Liên Hợp Quốc về giao tiếp điện tử[7].

Về nghĩa vụ bảo mật của các bên chủ thể tham gia: Theo Điều 28 Luật GDĐT Singapore, một người không được tiết lộ bất kỳ thông tin nào mà người đó có được khi thực hiện nhiệm vụ của mình hoặc thực hiện quyền của mình theo Đạo luật này, trừ các trường hợp: Việc tiết lộ đó được thực hiện với sự cho phép của người lấy thông tin từ đó hoặc, nếu thông tin là thông tin bí mật của người thứ ba, với sự cho phép của người thứ ba; cho mục đích quản lý hoặc

[4] Link truy cập: https://duthaoonline.quochoi.vn/Pages/dsduthao/chitietduthao.aspx?id=7399, ngày truy cập: 23/3/2023.

[5] Link truy cập: https://duthaoonline.quochoi.vn/Pages/dsduthao/chitietduthao.aspx?id=7399, ngày truy cập: 23/3/2023.

[6] Xem: Electronic Transactions Act 1998, Link truy cập: https://sso.agc.gov.sg/Acts-Supp/25-1998/Published?DocDate=19980710&ProvIds=pr22-, truy cập ngày: 15/3/2023

[7] Xem: Electronic Transactions Act 2010. Link truy cập: https://sso.agc.gov.sg/Act/ETA2010?ProvIds=al-#al-, ngày truy cập: 15/3/2023

thực thi Đạo luật này; với mục đích hỗ trợ bất kỳ công chức hoặc viên chức nào của bất kỳ hội đồng quản lý nào khác trong việc điều tra hoặc truy tố bất kỳ hành vi phạm tội nào theo bất kỳ luật thành văn nào; hoặc tuân thủ yêu cầu của bất kỳ tòa án hoặc bất kỳ luật thành văn nào.

Ngoài ra, *về trách nhiệm của nhà cung cấp dịch vụ mạng:* Luật GDĐT của Singapore đã dành riêng một Phần cho vấn đề này và quy định rằng một nhà cung cấp dịch vụ mạng sẽ không phải chịu trách nhiệm hình sự hay dân sự về nội dung thông tin của bên thứ ba khi họ chỉ đóng vai trò là người cung cấp quyền truy cập. Khi một nhà cung cấp dịch vụ mạng tham gia vào các hoạt động không khác với hoạt động của những nhà khai thác thông thường khác như các công ty điện thoại hoặc các công ty bưu chính thì họ cũng cần được bảo đảm rằng họ sẽ được đối xử tương tự như vậy đối với các hoạt động đó. Tuy nhiên, điều khoản này sẽ không ảnh hưởng tới các nghĩa vụ của nhà cung cấp dịch vụ mạng quy định trong các cơ chế cấp giấy phép hoặc các văn bản pháp luật, chẳng hạn như việc xin giấy phép từ cơ quan quản lý nhà nước của Singapore. Điều khoản này cũng không làm ảnh hưởng đến nghĩa vụ của các nhà cung cấp dịch vụ mạng trong các hợp đồng hay các quy định pháp luật về việc xoá bỏ hay từ chối truy cập vào những nội dung không được phép. Và như vậy thì các nhà cung cấp dịch vụ mạng sẽ vẫn phải chịu trách nhiệm về nội dung các thông tin của chính mình hoặc nội dung của bên thứ ba do họ đưa lên hoặc chấp nhận[8].

Về chế tài xử lý hành vi vi phạm nói chung: Theo Điều 33 Luật GDĐT Singapore, bất kỳ người nào phạm tội theo Đạo luật này mà không có hình phạt nào được quy định rõ ràng sẽ phải chịu mức phạt tiền không quá 20.000 đô la hoặc bị phạt tù có thời hạn không quá 06 tháng hoặc cả hai. Bên cạnh đó, quyền truy tố đối với các hành vi vi phạm Đạo luật này chỉ được đặt ra khi có được sự đồng ý của Công tố viên, và thẩm quyền xét xử bất kỳ hành vi phạm tội nào theo Đạo luật này, kể cả trái với Bộ luật Tố tụng hình sự năm 2010 đều thuộc về thẩm quyền xét xử của Tòa án quận và Tòa án này có quyền áp dụng hình phạt đầy đủ hoặc các biện pháp trừng phạt đối với hành vi vi phạm.

Như vậy, Luật GDĐT của Singapore đã tạo một môi trường pháp lý khá an toàn cho các GDĐT. Đạo luật này đã xoá bỏ được những trở ngại trong các quy định pháp luật hiện hành và tạo được lòng tin cho các doanh nghiệp, cá nhân khi tham gia vào GDĐT với các quy định về bảo đảm an toàn thông tin trong GDĐT rõ ràng, chi tiết. So với các quốc gia khác, trong đó có cả Việt Nam thì cách làm của Singapore mang tính tổng thể hơn nhiều vì nội dung của Luật GDĐT bao trùm rất nhiều lĩnh vực liên quan. Với việc ban hành Đạo luật này và việc sửa đổi bổ sung đối với các văn bản luật khác, Singapore có thể phát triển mạnh mẽ GDĐT và trở thành một trong những trung tâm GDĐT phát triển trên thế giới. Đây là điều vô cùng đáng được ghi nhận và pháp luật Việt Nam cần nghiên cứu, tiếp thu và căn cứ vào tình hình thực tiễn của Việt Nam để đưa ra các quy định về bảo đảm an toàn thông tin trong GDĐT.

3. Pháp luật của Thái Lan về bảo đảm an toàn thông tin trong giao dịch điện tử

Gần đây Luật GDĐT năm 2019[9] (ETA) đã được ban hành thay thế cho các phiên bản Luật GDĐT cũ và đã có hiệu lực bắt đầu từ ngày 15/4/2019. Đạo luật này ra đời với mục đích giảm thiểu, xóa bỏ những vướng mắc liên quan đến GDĐT và hài hòa pháp luật trong nước với Công ước của Liên Hợp Quốc về sử dụng thông tin điện tử trong hợp đồng quốc tế, cụ thể:

Về chủ thể chuyên trách thực hiện việc giám sát và bảo đảm an toàn thông tin trong giao dịch

[8] Đỗ Thị Thu Hằng (2009), *Pháp luật về hợp đồng điện tử ở Việt Nam*, Luận văn Thạc sĩ Luật học, Đại học Quốc gia, Hà Nội.

[9] Xem: Electronic Transaction Act (No.3), B. E. 2562 (2019).

điện tử, ETA trao một số nhiệm vụ và quyền hạn cho Ủy ban Giao dịch Điện tử (một cơ quan của Bộ Kinh tế Kỹ thuật số và Xã hội) những quyền hạn như: Phê duyệt các kế hoạch chiến lược liên quan đến GDĐT; thúc đẩy và hỗ trợ bất kỳ hoạt động nào phù hợp với các kế hoạch chiến lược; xác định các tiêu chuẩn công nghệ đối với các GDĐT; giám sát các doanh nghiệp kinh doanh dịch vụ điện tử; và yêu cầu thông tin hoặc tài liệu từ bất kỳ người nào liên quan đến hoạt động của các doanh nghiệp dịch vụ điện tử. ETA cho phép các viên chức có thẩm quyền được vào doanh nghiệp trong giờ hành chính để kiểm tra và thu thập thông tin cũng như thu giữ và tịch thu tài liệu, bằng chứng hoặc bất kỳ thứ nào khác có thể liên quan đến các hành vi phạm tội theo ETA hoặc các luật liên quan.

Bên cạnh đó, *đối với các doanh nghiệp kinh doanh dịch vụ liên quan đến giao dịch điện tử* sẽ chịu sự quản lý của Cơ quan Phát triển Giao dịch Điện tử (ETDA). Khi xác định doanh nghiệp kinh doanh dịch vụ điện tử nào phải tuân theo các yêu cầu về thông báo, đăng ký và cấp phép, ETDA sẽ xem xét tác động tiềm tàng của hoạt động kinh doanh dịch vụ điện tử và sự phù hợp của việc giám sát và thực hiện các biện pháp ngăn ngừa thiệt hại phù hợp với mức độ nghiêm trọng của tranh chấp nếu có xảy ra.

Các quy tắc, thủ tục và điều kiện cho các doanh nghiệp kinh doanh dịch vụ điện tử do ETDA áp đặt sẽ được quy định bởi nghị định của hoàng gia và các hình phạt đối với việc không tuân thủ các nghị định của hoàng gia về kinh doanh dịch vụ điện tử như sau:

Một là, tạm ngừng kinh doanh hoặc xóa thông báo của doanh nghiệp khỏi danh sách, tùy từng trường hợp, do không tuân thủ yêu cầu thông báo;

Hai là, phạt tiền lên đến 01 triệu THB[10] nếu không tuân thủ yêu cầu đăng ký; và

Ba là, phạt tiền lên tới 02 triệu THB nếu không tuân thủ yêu cầu cấp phép.

Nếu một bên bị phạt theo các điểm 1, 2 hoặc 3 ở trên và tái phạm trong vòng 01 năm, đăng ký hoặc giấy phép của họ có thể bị thu hồi.

Các hình phạt hình sự đối với việc điều hành một doanh nghiệp kinh doanh dịch vụ liên quan đến GDĐT mà không có đăng ký hoặc giấy phép đã được thêm vào trong ETA và không chỉ bao gồm tiền phạt mà còn có khả năng bị phạt tù. Nếu không đăng ký có thể bị phạt tù đến 02 năm, phạt tiền lên đến 200.000 THB hoặc cả hai, trong khi không có giấy phép sẽ bị phạt tù đến 03 năm, phạt tiền lên đến đến 300.000 THB hoặc cả hai.

Như vậy, những thay đổi nêu trên đối với ETA rất được các doanh nghiệp hoan nghênh vì các bản sửa đổi cập nhật luật của Thái Lan về GDĐT phù hợp với các tiêu chuẩn được chấp nhận rộng rãi hiện nay như được thể hiện trong Công ước của Liên Hợp Quốc về sử dụng phương tiện liên lạc điện tử trong hợp đồng quốc tế. Điều này sẽ tăng thêm tính linh hoạt cho việc thực hiện các giao dịch kinh doanh thông qua các phương tiện điện tử và đơn giản hóa quá trình hài hòa hóa các thông lệ trong khu vực và trên toàn cầu.

4. Đánh giá chung quy định pháp luật của các quốc gia về bảo đảm an toàn thông tin trong giao dịch điện tử

Qua quá trình nghiên cứu, xem xét, đánh giá nội dung của pháp luật Singapore, Thái Lan với pháp luật Việt Nam về bảo đảm an toàn thông tin trong GDĐT, nhóm tác giả nhận thấy có những điểm tương đồng và đặc trưng trong nội dung về bảo đảm an toàn thông tin trong GDĐT như sau:

Về điểm tương đồng, trong Luật GDĐT của các quốc gia đều thông thường:

Một là, về chữ ký điện tử: Hình thành các quy định về tạo tác chữ ký điện tử và lưu trữ chữ ký điện tử.

Hai là, về chế tài áp dụng cho hành vi vi

[10] THB: Baht, đơn vị tiền tệ của Thái Lan.

phạm: Pháp luật các quốc gia đều kết hợp sử dụng chế tài phạt vi phạm hành chính và điều khoản phạt vi phạm hợp đồng đối với hành vi xâm phạm thông tin cá nhân của người tham gia GDĐT.

Tuy nhiên pháp luật các nước có những nét đặc trưng sau:

Thứ nhất, pháp luật về GDĐT của Thái Lan đã đề cập tới chủ thể chuyên trách tiếp nhận những vụ việc liên quan đến GDĐT như Ủy ban Giao dịch Điện tử với nhiệm vụ, quyền hạn cụ thể: Hỗ trợ, giám sát các doanh nghiệp kinh doanh dịch vụ điện tử…, hay quy định chi tiết các quy tắc, thủ tục và điều kiện cho các doanh nghiệp kinh doanh dịch vụ điện tử hoạt động và chế tài nếu có hành vi vi phạm.

Thứ hai, Luật GDĐT của Singapore đã đưa ra những quy tắc nhằm làm rõ quyền và nghĩa vụ của các bên tham gia trong một GDĐT. Quy tắc thực hành chung trong Luật GDĐT của Singapore cũng chứa đựng các điều khoản điều chỉnh việc ký kết hợp đồng qua các phương tiện điện tử thông qua việc quy định về thời gian, địa điểm gửi và nhận thông tin điện tử. Đạo luật này còn quy định về giá trị pháp lý của các bản ghi và chữ ký điện tử, cùng với độ an toàn của chúng, quy định thủ tục bảo mật và cung cấp quy trình bảo mật cụ thể... Luật GDĐT của Singapore đã tương đối bao quát mọi trường hợp, mọi khía cạnh của GDĐT, đặc biệt là vấn đề bảo mật.

5. Một số đề xuất hoàn thiện pháp luật bảo đảm an toàn thông tin trong giao dịch điện tử xuất phát từ kinh nghiệm thế giới

Thứ nhất, bảo đảm an toàn thông tin trong giai đoạn giao kết GDĐT

Một là, cần bổ sung Điều 4 Luật GDĐT năm 2005 các định nghĩa về *"chữ ký điện tử"*, *"chữ ký số"*, *"chữ ký quét"*, *"chữ ký hình ảnh"*, *"chữ ký điện tử an toàn"* nhằm hướng pháp luật điều chỉnh rộng rãi, phong phú các dạng chữ ký điện tử, căn cứ để cơ quan có thẩm quyền xem xét về tính hợp pháp của các hình thức đó.

Đối với *chữ ký số*: (i) Các bên sử dụng nền tảng, thiết bị chuyên dụng do nhà cung cấp dịch vụ chứng thực chữ ký số cung cấp để tạo chữ ký số; (ii) sau đó, chữ ký số đó được đính kèm theo phương thức điện tử với hợp đồng cần được ký kết. Trên thực tế, chữ ký số ít được sử dụng trong việc ký kết các hợp đồng lớn và phức tạp mà chủ yếu được sử dụng khi bên ký kết nộp tờ khai hải quan, tờ khai bảo hiểm xã hội, nộp thuế qua mạng, xuất hóa đơn điện tử hoặc khi tổ chức, cá nhân thực hiện các GDĐT qua hệ thống ngân hàng trực tuyến.

Đối với *chữ ký quét:* (i) Hợp đồng được in bởi người ký từ tệp dữ liệu và người ký của mỗi bên ký vào bản cứng của hợp đồng đó bằng mực ướt; (ii) sau đó, hợp đồng với các chữ ký trên đó được chuyển thành dạng điện tử (ví dụ: bằng cách quét) và bản sao quét của hợp đồng đã ký (là tệp dữ liệu điện tử) được gửi đến bên đối tác qua email.

Đối với *chữ ký hình ảnh:* (i) Một bên ký kết chèn hình ảnh chữ ký của mình vào ô chữ ký của tệp dữ liệu điện tử của hợp đồng; (ii) sau đó, tệp dữ liệu điện tử của hợp đồng (cùng với chữ ký hình ảnh trên đó) được gửi đến bên đối tác qua email. Chữ ký ảnh thường được sử dụng trong các hợp đồng không có giá trị lớn nhưng được ký kết thường xuyên và khi người ký không có mặt tại địa điểm có thể in và ký hợp đồng bằng chữ ký mực ướt[11].

Hai là, bổ sung thêm Chương III Luật GDĐT năm 2005 với các điều luật quy định về hình thức định danh điện tử và xác thực điện tử để từ đó các chủ thể tham gia GDĐT có căn cứ để áp dụng các biện pháp bảo mật phù hợp.

Đề án phát triển ứng dụng dữ liệu về dân cư, định danh và xác thực điện tử phục vụ chuyển đổi số quốc gia giai đoạn 2022-2025, tầm nhìn đến năm 2030 cho thấy tính

[11] Xem: Trương Nhật Quang, "Ký kết hợp đồng thông qua phương thức điện tử", *Tạp chí Nghiên cứu lập pháp*, Số 10/2020, tr.19-24.

cấp thiết cần bổ sung về định danh, xác thực điện tử trong Luật GDĐT, từ đó phạm vi điều chỉnh của Luật trở nên bao quát và toàn diện hơn nhằm đảm bảo yếu tố bảo mật và an toàn thông tin. Trong một mạng lưới tín nhiệm, việc "xác thực" là một cách để đảm bảo rằng người dùng chính là người mà họ nói họ là, và người dùng hiện đang thi hành những chức năng trong một hệ thống, trên thực tế, chính là người đã được ủy quyền để làm những việc đó. Xác thực là khâu đặc biệt quan trọng để bảo đảm an toàn cho hoạt động của một hệ thống thông tin. Xác thực đa nhân tố là sự kết hợp tối thiểu của hai trong ba yếu tố sau đây: (i) Something that you have: Những gì mà chỉ bạn mới có. Ví dụ: Thiết bị token của ngân hàng; (ii) Something that you are: Những gì thuộc về sinh trắc của bạn. Ví dụ như đồng tử, tròng mắt, dấu vân tay hay giọng nói của bạn...; (iii) Something that you know: Những gì mà chỉ bạn mới biết. Là những thông tin mà một mình bạn tạo ra như: Tên đăng nhập, mật khẩu đăng nhập, tên người thân của bạn… Xác thực đa nhân tố thường hay được sử dụng trong lĩnh vực như kinh doanh online, ngân hàng, mạng xã hội... Hiện nay, trong xác thực đa nhân tố, nhân tố đầu tiên được sử dụng thường là mật khẩu do người dùng cài đặt, còn nhân tố thứ hai thường là mật khẩu sử dụng một lần (OTP)[12]. Chú trọng bối cảnh, việc sử dụng các dữ liệu xung quanh thao tác ký nhằm đem lại khả năng định danh chủ thể tốt hơn, từ đó tăng cường khả năng xác định giá trị pháp lý và giá trị chứng cứ của thông điệp dữ liệu được ký. Quy định bắt buộc về xác thực hai yếu tố thông qua các phương pháp như mật khẩu, sinh trắc học, Token và mã OTP[13] .

[12] Xem: Đặng Xuân Bảo, Trần Thị Xuyên, Hoàng Thu Phương, Nguyễn Thị Hồng Hà, "Nghiên cứu xây dựng hệ thống xác thực đa nhân tố cho website", *Tạp chí Khoa học và Công nghệ Đại học Thái Nguyên*, 2020.

[13] Xem: Nguyễn Đức Nhượng, Vũ Thị Hương Giang (2017), *"Xác thực cho các ứng dụng Chính phủ điện tử"*, Luận văn Thạc sĩ, Trường Đại học Bách Khoa.

Thứ hai, hoàn thiện pháp luật bảo mật trong giai đoạn thực hiện GDĐT

Ngoài những kiến nghị tại giai đoạn giao kết, tại giai đoạn thực hiện sửa đổi, bổ sung thêm Điều 46 tại Chương 6 Luật GDĐT năm 2005:

Một là, điều kiện để GDĐT được an toàn. Có quy định tại các văn bản pháp luật liên quan về bảo mật đáp ứng đủ điều kiện trong các giai đoạn đặc biệt ở giai đoạn thực hiện giúp các chủ thể dễ dàng tiếp cận với hợp đồng điện tử đã giao kết với các yêu cầu nhất định nhằm thực hiện các nghĩa vụ trong hợp đồng đã giao kết trong trường hợp thuận lợi:

(i) Yêu cầu *"ghi"* - bên thứ 3 không được phép copy lại văn bản và gửi nhiều lần đến người nhận mà người gửi không hề hay biết.

(ii) Yêu cầu *"chữ ký"* - người nhận cần phải xác định người gửi và kiểm tra xem người gửi đó có thực sự gửi thông tin đi hay không.

(iii) Yêu cầu *"toàn vẹn"* - người nhận cần có khả năng xác định được thông tin có bị thay đổi trong quá trình truyền thông tin hay không.

Hai là, bổ sung quy định tại Điều 37 Luật GDĐT năm 2005 về trách nhiệm và quyền của các bên khi tiếp cận và nhiệm vụ thực hiện nghĩa vụ bảo đảm an toàn thông tin trong GDĐT đó.

Thứ ba, hoàn thiện pháp luật bảo đảm an toàn thông tin trong giai đoạn chấm dứt GDĐT

Một là, bổ sung quy định tại Điều 13 Luật Lưu trữ năm 2011 về chuyển đổi tài liệu giấy sang tài liệu điện tử: Phương thức chuyển đổi, điều kiện đáp ứng của tài liệu điện tử sau khi chuyển đổi, giá trị của tài liệu điện tử sau khi chuyển đổi từ tài liệu giấy.

Hai là, mở rộng phạm vi điều chỉnh quy định tại Điều 1 Luật Lưu trữ năm 2011 trong hoạt động lưu trữ ở lĩnh vực tư, để từ đó hình thành cơ sở chứng cứ khi các bên

xảy ra tranh chấp. Về phạm vi điều chỉnh, Luật quy định về hoạt động lưu trữ; quyền và nghĩa vụ của cơ quan, tổ chức, cá nhân trong hoạt động lưu trữ trong lĩnh vực tư và công;

Ba là, bổ sung về quy định trách nhiệm của các chủ thể liên quan trong giai đoạn chấm dứt tại Điều 35 Luật GDĐT năm 2005 "Chủ thể tham gia phải có trách nhiệm với thông điệp dữ liệu, không được tiết lộ những thông tin hoặc các giao dịch cần bảo mật trong các giai đoạn".

Thứ tư, đề xuất hoàn thiện pháp luật chữ ký trong GDĐT

Một là, bổ sung quy định bắt buộc về tiêu chuẩn áp dụng đối với chữ ký điện tử tại Nghị định số 130/2018/NĐ-CP ngày 27/9/2018 quy định chi tiết thi hành Luật GDĐT về chữ ký số và dịch vụ chứng thực chữ ký số, Thông tư số 16/2019/TT-BTTTT quy định về Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa, Thông tư số 22/2020/TT-BTTTT ngày 07/9/2020 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số. Theo đó cần bổ sung quy định áp dụng bắt buộc đối với Trust CA Timestamp, đây là công nghệ có giá trị cao về chống gian lận, giả mạo trong GDĐT, đảm bảo tính pháp lý khi lưu trữ tài liệu điện tử lâu dài, xác thực tài liệu dài hạn, tin cậy cả sau khi chứng thư số hết hạn, giúp thay thế hoàn toàn bản giấy, không phải in ấn, thay thế kho lưu trữ giấy bằng kho lưu trữ điện tử[14].

Hai là, yêu cầu áp dụng bắt buộc xác thực đa yếu tố (Multi-Factor Authentication) là phương thức xác thực dựa trên nhiều yếu tố xác thực kết hợp. Mức độ an toàn bảo mật sẽ càng cao khi số yếu tố xác thực càng nhiều. Khi số yếu tố xác thực lớn thì hệ thống càng phức tạp, kéo theo chi phí đầu tư và duy trì vận hành tốn kém, đồng thời lại bất tiện cho người sử dụng. Với hệ thống GDĐT ở thời điểm hiện tại đang sử dụng xác thực đơn vị qua yếu tố những gì thực thể biết sử dụng username và password. Vì vậy để áp dụng mô hình xác thực hai yếu tố (2FA) cho người dùng tác giả sử dụng phương pháp xác thực dựa trên phương pháp "thực thể biết gì" sử dụng tên đăng nhập (username) và mật khẩu (password) kết hợp với một phương pháp xác thực dựa vào "thực thể thừa hưởng gì"; hoặc "thực thể sở hữu gì" nhằm cân bằng hai mục tiêu vừa đảm bảo an toàn thông tin vừa tiết kiệm chi phí giao dịch[15].

Ba là, bổ sung điều luật quy định chuyển đổi hình thức giữa văn bản giấy và thông điệp dữ liệu; quy định về sử dụng và công nhận chữ ký điện tử nước ngoài còn chưa phù hợp thực tiễn; việc sử dụng các chứng từ điện tử đã được ký bằng chữ ký điện tử trong các vụ việc tại Tòa án./.

TÀI LIỆU THAM KHẢO

1. Đặng Xuân Bảo, Trần Thị Xuyên, Hoàng Thu Phương, Nguyễn Thị Hồng Hà, "Nghiên cứu xây dựng hệ thống xác thực đa nhân tố cho website", *Tạp chí Khoa học và Công nghệ Đại học Thái Nguyên*, 2020.

2. Đỗ Thị Thu Hằng (2009), *"Pháp luật về hợp đồng điện tử ở Việt Nam"*, Luận văn Thạc sĩ Luật học, Đại học Quốc gia Hà Nội.

3. Nguyễn Đức Nhượng, Vũ Thị Hương Giang (2017), *"Xác thực cho các ứng dụng Chính phủ điện tử"*, Luận văn Thạc sĩ, Trường Đại học Bách Khoa.

4. Trương Nhật Quang, "Ký kết hợp đồng thông qua phương thức điện tử", *Tạp chí Nghiên cứu lập pháp*, Số 10/2020.

[14] Xem: Thảo Anh, *"Bảo đảm an toàn thông tin trong giao dịch điện tử và ứng dụng di động trong nền kinh tế số"*, 2021, Link truy cập: https://www.mic.gov.vn/mic_2020/Pages/TinTuc/148719/Bao-mat-giao-dich-dien-tu-va-ung-dung-di-dong-trong-nen-kinh-te-so.html, ngày truy cập: 16/3/2022.

[15] Xem: Nguyễn Đức Nhượng, Vũ Thị Hương Giang (2017), tlđd chú thích 16.