VẤN ĐỀ AN TOÀN THÔNG TIN VÀ AN NINH MẠNG TRONG GIAO DỊCH ĐIỆN TỬ

Nguyễn Mai Bộ
TS. Tổng cục Chính trị Quân đội nhân dân

Thông tin bài viết:
Từ khóa: An toàn thông tin mạng, an ninh mạng, giao dịch điện tử.

Lịch sử bài viết:
Nhận bài : 30/08/2022
Biên tập : 18/09/2022
Duyệt bài : 19/09/2022

Tóm tắt:
Trong phạm vi bài viết này, tác giả kiến nghị sửa đổi nội dung ở một số điều khoản trong Dự thảo Luật Giao dịch điện tử (*sửa đổi*) nhằm hoàn thiện các quy định về an toàn thông tin mạng và an ninh mạng trong giao dịch điện tử, bảo đảm tính thống nhất của hệ thống pháp luật Việt Nam.

Article Infomation:
Keywords: Network information security; network security; electronic transactions.

Article History:
Received : 30 Aug. 2022
Edited : 18 Sep. 2022
Approved : 19 Sep. 2022

Abstract:
Within the scope of this article, the author provides recommendations for amendments of the provisions under a number of articles in the draft Law on Electronic Transactions (amended) in order to improve regulations on network information safety and network security in electronic transactions, to ensure the consistency of the Vietnamese legal system.

1. An toàn thông tin mạng và an ninh mạng trong giao dịch điện tử

Vấn đề an toàn thông tin mạng và an ninh mạng trong giao dịch điện tử xuất phát từ bản chất của "giao dịch điện tử là giao dịch được thực hiện bằng phương tiện điện tử"[1] trên môi trường điện tử (là: môi trường mạng theo Luật Công nghệ thông tin; mạng theo Luật An toàn thông tin mạng; và là không gian mạng theo Luật An ninh mạng). Trong đó, một trong những đối tượng tác động của Luật Giao dịch điện tử là "thông điệp dữ liệu" và "Thông điệp dữ liệu là thông tin được tạo ra, được gửi đi, được nhận và được lưu trữ bằng phương tiện điện tử" [2]. Theo quy định tại Luật Công nghệ thông tin, thì chỉ có khái niệm "Thông tin số là thông tin được tạo lập

[1] Xem: Khoản 1 Điều 2 Dự thảo Luật Giao dịch điện tử (*sửa đổi*) - Dự thảo.
[2] Xem: Khoản 3 Điều 2 Dự thảo.

bằng phương pháp dùng tín hiệu số"[3]. Trong Luật An toàn thông tin mạng có khái niệm "Hệ thống thông tin là tập hợp phần cứng, phần mềm, và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, tryền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng (và mạng công nghệ thông tin là tập hợp các phương pháp khoa học, công nghệ và công cụ kỹ thuật hiện đại để sản xuất, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin số) [4]. Như vậy:

- Theo Dự thảo Luật Giao dịch điện tử (sửa đổi) thì Luật Giao dịch điện tử điều chỉnh: (1) Giao dịch điện tử; (2) Thành phần cơ bản của giao dịch điện tử (Thông điệp dữ liệu; Dịch vụ tin cậy như chữ ký điện tử, dịch vụ tin cậy như dịch vụ cấp dấu thời gian, dịch vụ chứng thực thông điệp dữ liệu và dịch vụ chữ kỹ số công cộng; Hệ thống thông tin phục vụ giao dịch điện tử; An toàn thông tin mạng và An ninh mạng trong giao dịch điện tử); (3) Biện pháp bảo đảm và chính sách thúc đẩy giao dịch điện tử.

- Luật An toàn thông tin mạng điều chỉnh hoạt động an toàn thông tin mạng, là hoạt động bảo vệ thông tin và hệ thống thông tin trên mạng tránh bị truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin (trừ hệ thống thông tin quan trọng về an ninh quốc gia do Luật An ninh mạng điều chỉnh).

- Luật Công nghệ thông tin điều chỉnh hoạt động ứng dụng, các biện pháp bảo đảm ứng dụng công nghệ thông tin (với nghĩa công nghệ thông tin là tập hợp các phương pháp khoa học, công nghệ và công cụ kỹ thuật hiện đại để sản xuất, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin số)...

Vì vậy, vấn đề an toàn thông tin mạng và an ninh mạng trong giao dịch điện tử chỉ nên quy định trong Luật Giao dịch điện tử theo phương pháp viện dẫn Luật Công nghệ thông tin, Luật An toàn thông tin mạng và Luật An ninh mạng.

Vấn đề an toàn thông tin mạng và an ninh mạng trong giao dịch điện tử được quy định tại Chương VII Dự thảo Luật Giao dịch điện tử (sửa đổi). Theo đó:

- Điều 53 "Bảo đảm an toàn thông tin mạng và an ninh mạng" Dự thảo quy định: "*Cơ quan, tổ chức, cá nhân tuân thủ quy định của pháp luật về an toàn thông tin mạng và an ninh mạng khi tiến hành các giao dịch điện tử*". Tác giả cho rằng, nội dung quy định nêu trên mới chỉ là nghĩa vụ của của cơ quan, tổ chức, cá nhân trong việc tuân thủ quy định của pháp luật về an toàn thông tin mạng và an ninh mạng khi tiến hành các giao dịch điện tử mang tính thụ động mà chưa thể hiện được quyền chủ động của các cơ quan quản lý nhà nước trong việc bảo đảm an toàn thông tin mạng và an ninh mạng. Mặt khác, theo quy định tại khoản 4 Điều 3 "Giải thích từ ngữ" của Dự thảo, thì một trong những đối tượng

[3] Xem: Khoản 2 Điều 4 Luật Công nghệ thông tin.
[4] Xem: Khoản 2 Điều 3 Luật An toàn thông tin mạng và khoản 2 Điều 4 Luật Công nghệ thông tin.

tác động của Luật này là phương tiện điện tử *(là phần cứng, phần mềm... hoặc phương tiện điện tử khác hoạt động dựa trên công nghệ thông tin, công nghệ điện, điện tử, kỹ thuật số, từ tình, tuyền dẫn, quan học, điện từ hoặc công nghệ khác tương tự)*. Và việc bảo đảm an toàn *phần cứng, phần mềm... hoặc phương tiện điện tử khác hoạt động dựa trên công nghệ thông tin*... lại được thực hiện theo Luật Công nghệ thông tin. Do vậy, cần sửa đổi theo hướng quy định việc bảo đảm an toàn thông tin trong giao dịch điện tử không chỉ được thực hiện theo quy định của Luật An toàn thông tin mạng và Luật An ninh mạng mà còn được thực hiện theo quy định của Luật Công nghệ thông tin.

Từ những lý do trên, tác giả kiến nghị sửa đổi Điều 53 Dự thảo như sau:

"Điều... Bảo đảm an toàn mạng, an toàn thông tin mạng và an ninh mạng trong giao dịch điện tử

1. Việc bảo đảm an toàn mạng, an toàn thông tin mạng và an ninh mạng trong giao dịch điện tử được thực hiện theo quy định của Luật Công nghệ thông tin, Luật An toàn thông tin mạng và Luật An ninh mạng.

2. Cơ quan, tổ chức, cá nhân tuân thủ quy định của pháp luật về an toàn mạng, an toàn thông tin mạng và an ninh mạng khi tiến hành các giao dịch điện tử".

Đồng thời, nghiên cứu (nếu có thể được), thì gộp nội dung quy định tại Điều 53 vào Điều 52 "Biện pháp bảo vệ giao dịch điện tử", hoặc chỉ giữ lại khoản 1 Điều 53 (mà tác giả đã kiến nghị sửa đổi) và chuyển lên thành một khoản của Điều 4 "Nguyên tắc chung tiến hành giao dich điện tử".

- Điều 54 "Bảo vệ thông điệp dữ liệu" của Dự thảo quy định:

"1. Thông điệp dữ liệu được phân loại và bảo đảm an toàn thông tin mạng dựa trên mức độ quan trọng.

2. Thông điệp dữ liệu thuộc phạm vi bí mật nhà nước tuân thủ quy định của pháp luật về bảo vệ bí mật nhà nước và cơ yếu.

3. Trách nhiệm của của Bộ Thông tin và Truyền thông:

a) Phối hợp với các bộ, cơ quan Trung ương và các địa phương xây dựng, ban hành hoặc trình cấp có thẩm quyền ban hành và tổ chức thực hiện văn bản quy phạm pháp luật, tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn thông điệp dữ liệu;

b) Tổ chức đánh giá rủi ro, giám sát và cảnh báo sớm về an toàn thông điệp dữ liệu;

c) Điều phối quốc gia công tác ứng cứu khẩn cấp sự cố mất an toàn thông tin mạng đối với thông điệp dữ liệu.

4. Trách nhiệm của cơ quan nhà nước:

a) Phân loại, xác định danh mục thông điệp dữ liệu theo mức độ quan trọng và thực hiện các biện pháp bảo đảm an toàn thông điệp dữ liệu theo quy định;

b) Trong trường hợp ủy thác cho doanh nghiệp xây dựng và vận hành hệ thống lưu trữ và xử lý thông điệp dữ liệu, cơ quan nhà nước chịu trách nhiệm giám sát bên được ủy thác thực hiện các nghĩa vụ bảo đảm an toàn thông điệp dữ liệu.

5. Trách nhiệm của bên xử lý dữ liệu:

a) Thiết lập hệ thống bảo đảm an toàn thông điệp dữ liệu toàn trình, áp dụng các biện pháp kỹ thuật bảo đảm an toàn thông điệp dữ liệu theo quy định;

b) Thông báo kịp thời cho người dùng về sự cố mất an toàn thông điệp dữ liệu và báo cáo Bộ Thông tin và Truyền thông theo quy định;

c) Tuân thủ quy định của pháp luật về xử lý dữ liệu, chỉ định người phụ trách bảo đảm an toàn thông điệp dữ liệu và thiết lập bộ phận chịu trách nhiệm bảo đảm an toàn thông điệp dữ liệu".

Tác giả cho rằng quy định tại khoản 1 và khoản 2: "*Thông điệp dữ liệu được phân loại và bảo đảm an toàn thông tin mạng dựa trên mức độ quan trọng. Thông điệp dữ liệu thuộc phạm vi bí mật nhà nước tuân thủ quy định của pháp luật về bảo vệ bí mật nhà nước và cơ yếu*" có một số bất cập sau:

Thứ nhất, việc phân loại thông điệp dữ liệu thực chất là phân loại thông tin. Theo quy định tại Điều 9 "Phân loại thông tin" và Điều 21 "Phân loại theo cấp độ an toàn hệ thống thông tin" của Luật An toàn thông tin mạng, thì về cơ bản việc phân loại thông tin được thực hiện theo thuộc tính "*bí mật để có biện pháp bảo vệ phù hợp*" và phân loại cấp độ an toàn hệ thống thông tin là việc xác định cấp độ an toàn theo cấp độ từ 1 đến 5 để áp dụng biện pháp kỹ thuật quản lý và kỹ thuật nhằm bảo vệ hệ thống thông tin phù hợp theo cấp độ. Như vậy, việc Dự thảo quy định "*Thông điệp dữ liệu được phân loại và bảo đảm an toàn thông tin mạng dựa trên mức độ quan trọng*" là không đồng bộ với quy định của Luật An toàn thông tin mạng. Tiêu chí phân loại thông điệp dữ liệu "*...dựa trên mức độ quan trọng*" là không chính xác, vì một thông điệp dữ liệu cụ thể có thể là quan trọng đối với cơ quan, tổ chức, cá nhân này nhưng lại không quan trọng đối với cơ quan, tổ chức, cá nhân khác. Mặt khác, "thông điệp dữ liệu" là một trong những thành phần cơ bản của giao dịch điện tử. Do vậy, việc phân loại thông điệp dữ liệu với nghĩa là phân loại thông tin trong hệ thống thông tin đã được thực hiện theo quy định của Luật An toàn thông tin mạng. Đồng thời, "thông điệp dữ liệu" đã là đối tượng được bảo vệ theo quy định của Luật Công nghệ thông tin, Luật An toàn thông tin mạng, Luật An ninh mạng và cũng đã được quy định tại Điều 53 Dự thảo. Cho nên, về kỹ thuật lập pháp, đề nghị nghiên cứu sự cần thiết quy định tại khoản 1 Điều 54 Dự thảo trong mối tương quan với quy định đã có tại Điều 53 Dự thảo.

Thứ hai, quy định *thông điệp dữ liệu thuộc phạm vi bí mật nhà nước tuân thủ quy định của pháp luật về bảo vệ bí mật nhà nước và cơ yếu* là chưa thật chính xác. Bởi lẽ, giao dịch điện tử là giao dịch được thực hiện bằng phương tiện điện tử, trong đó thông điệp dữ

liệu được tạo ra, được gửi đi, được nhận và được lưu trữ bằng phương tiện điện tử. Theo quy định của Luật Bảo vệ bí mật nhà nước thì thông tin thuộc phạm vi bí mật nhà nước được phân loại và bảo vệ theo quy định của pháp luật bảo vệ bí mật nhà nước. Việc bảo vệ bí mật nhà nước được thực hiện theo nguyên tắc nghiêm cấm: "*Truyền đưa bí mật nhà nước trên phương tiện thông tin, viễn thông trái với quy định của pháp luật về cơ yếu; Đăng tải, phát tán bí mật nhà nước trên phương tiện thông tin đại chúng, mạng Internet, mạng máy tính và mạng viễn thông*"[5]. Đặt giả sử là trong thông điệp dữ liệu giao dịch điện tử có nội dung thuộc phạm vi bí mật nhà nước, thì việc đăng tải, phát tán bí mật nhà nước trên phương tiện thông tin đại chúng, mạng Internet, mạng máy tính và mạng viễn thông đã là hành vi bị nghiêm cấm.

Còn việc truyền đưa bí mật nhà nước trên phương tiện thông tin, viễn thông trái với quy định của pháp luật về cơ yếu. Theo đó, việc truyền thông tin bí mật nhà nước qua các phương tiện thông tin, viễn thông phải mã hóa bằng mật mã của cơ yếu. Do vậy, tác giả kiến nghị Cơ quan soạn thảo nghiên cứu quy định tại khoản 2 Điều 54 Dự thảo vì không thuộc nội hàm của Chương "An toàn thông tin và an ninh mạng trong giao dich điện tử". Nếu thực sự là cần thiết thì phải có quy định về bảo vệ bí mật nhà nước đối với "thông điệp dữ liệu trong giao dich điện tử, thì chỉ nên quy định theo phương pháp viện dẫn "*...được thực hiện theo pháp luật về bảo vệ bí mật nhà nước*".

+ Khoản 3 và khoản 4 quy định về trách nhiệm của Bộ Thông tin và Truyền thông và trách nhiệm của cơ quan nhà nước trong việc quản lý "thông điệp dữ liệu". Xuất phát từ quan điểm "*Thông điệp dữ liệu là thông tin được tạo ra, được gửi đi, được nhận và được lưu trữ bằng phương tiện điện tử*" [6] và vấn đề được nêu tại khoản 3 và 4 Điều 54 Dự thảo được đề cập trên phương diện (và thuộc nội hàm của chương) an toàn thông tin và an ninh mạng trong giao dịch điện tử, thì nội dung quy định về trách nhiệm của Bộ Thông tin và Truyền thông tại khoản 3 và 4 Điều 54 Dự thảo chính là trách nhiệm của: Bộ Thông tin và Truyền thông, được quy định tại Điều 14 và khoản 2 Điều 52 Luật An toàn thông tin mạng; Bộ, ngành khác được quy định tại các khoản từ khoản 3 đến khoản 11 Luật An toàn thông tin mạng.

Mặt khác, về trách nhiệm của cơ quan nhà nước trong việc "*Phân loại, xác định danh mục thông điệp dữ liệu theo mức độ quan trọng và thực hiện các biện pháp bảo đảm an toàn thông điệp dữ liệu theo quy định*", thì tiêu chí phân loại thông điệp dữ liệu "*...dựa trên mức độ quan trọng*" là không chính xác.

+ Về quy định tại khoản 5 "Trách nhiệm xử lý dữ liệu", thì:

Khoản 11 Điều 3 Dự thảo quy định "*Dữ liệu là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự*"

[5] Xem: Điều 5 và Điều 8 Luật Bảo vệ bí mật nhà nước năm 2018.
[6] Xem: Khoản 3 Điều 2 Dự thảo.

và khoản 2 Điều 1 Dự thảo quy định "*Luật này không quy định về nội dung của giao dịch*". Cho nên "dữ liệu" cần được hiểu theo nghĩa là bộ phận "cấu trúc" của "Thông điệp dữ liệu" và việc bảo đảm an toàn dữ liệu cũng là một bộ phận của việc bảo đảm an toàn thông điệp giữ liệu. Cho nên, cần nghiên cứu về sự cần thiết phải có quy định này hay không khi đã sửa đổi Điều 52 như tác giả đề xuất.

Mặt khác, về ngôn ngữ thì khoản 15 Điều 3 của Dự thảo quy định "Xử lý dữ liệu là một hoặc nhiều hành động tác động tới dữ liệu hoặc thông điệp dữ liệu như thu thập, ghi, phân tích, lưu trữ, chỉnh sửa, truy cập, truy xuất, thu hồi, mã hóa, giải mã, sao chép, chia sẻ, truyền đưa, chuyển giao, xóa, hủy dữ liệu hoặc các hành động khác có liên quan". Do vậy, các nội dung quy định tại khoản 5 Điều này chưa bao hàm hết trách nhiệm "của bên xử lý dữ liệu" đối với các hoạt động xử lý dữ liệu quy định tại khoản 15 Điều 3 của Dự thảo.

2. Một số nội dung khác của Dự thảo

- *Thứ nhất*, đề nghị giải thích lại từ "xử lý dữ liệu" - khoản 15 Điều 3 Dự thảo. Bởi lẽ, với giải thích tại khoản 11 Điều 3 Dự thảo "*Dữ liệu là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự*" thì "xử lý dữ liệu" chỉ là những tác động tới thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự. Nếu vẫn cần thiết giữ lại nội dung giải thích "*...là một hoặc nhiều hành động tác động tới dữ liệu hoặc thông điệp dữ liệu như thu thập, ghi, phân tích, lưu trữ, chỉnh sửa, truy cập, truy xuất, thu hồi, mã hóa, giải mã, sao chép, chia sẻ, truyền đưa, chuyển giao, xóa, hủy dữ liệu hoặc các hành động khác có liên quan*", thì cần phải thay từ được giải thích "*xử lý dữ liệu*" bằng một từ khác.

- *Thứ hai*, chuyển nội dung tại điểm a khoản 3 Điều 54 lên Điều 6 Dự thảo "Nội dung quản lý nhà nước về giao dich điện tử" (nếu việc giữ lại nội dung điểm a khoản 3 Điều 54 Dự thảo là cần thiết); đồng thời, bổ sung nội dung quản lý an ninh mạng vào khoản 6 Điều 6 Dự thảo.

- *Thứ ba*, cần chỉ rõ "theo quy định của pháp luật" nào ở tất cả các điều luật có cụm từ này, như khoản 2 Điều 10, điểm a khoản 3 Điều 14, khoản 2 Điều 23, khoản 1 Điều 28, khoản 2 Điều 34 Dự thảo...

- *Thứ tư*, (nếu cần thiết giữ lại nội dung khoản 3 và 4 Điều 54) thì chuyển các nội dung đó về Điều 7 Dự thảo "Trách nhiệm quản lý nhà nước về hoạt động giao dich điện tử".

- *Thứ năm*, nghiên cứu sửa đổi tên và nội dung Điều 13 Dự thảo "Thông điệp dữ liệu có giá trị làm chứng cứ" để chỉ rõ đây là chứng cứ giao dịch điện tử, để phân biệt với chứng cứ trong tố tụng dân sự, tố tụng hình sự.

- *Thứ sáu*, khoản 18 Điều 3 Dự thảo sử dụng từ "Nền tảng số" và giải thích là "hệ thống thông tin tạo môi trường mạng...". Tuy nhiên, khoản 17 Điều này lại sử dụng từ "Môi trường điện tử" là chưa đồng bộ về mặt ngôn ngữ. Mặt khác, tại Chương VI "Hệ thống thông tin phục vụ giao dịch điện tử" lại không sử dụng từ "Nền tảng số" mà dùng "hệ thống thông tin" cho thấy sự không cần thiết phải giải thích từ "Nền tảng số" ■