VNU Journal of Science: Legal Studies, Vol. 38, No. 3 (2022) 74-82

VNU Journal of Science: Legal Studies

Journal homepage: https://js.vnu.edu.vn/LS

Original Article

The Impact of the Policy of Digital Transformation on Ensuring the Right of Access to Information

Nguyen Trong Diep[1,*], Nguyen Tien Dat[2]

[1]*VNU School of Law, 144 Xuan Thuy, Cau Giay, Hanoi, Vietnam*

[2]*Academy of Policy and Development, Nam An Khanh, Hoai Duc, Hanoi, Vietnam*

Received 24 Jannuary 2022
Revised 10 June 2022; Accepted 01 July 2022

Abstract: The right of access to information is one of the human rights, recognized by all nations of the world, based on the legislative recognition of the freedom of information in Sweden since 1766. This human right establishes the people's trust and determines the political stability of each nation. This paper presents some basic contents and analyses the theoretical, practical and legal basis to ensure the right to access information in the era of digital transformation in Vietnam.

Keywords: Access to information, human right, digital transformation.

*Corresponding author.
Email address: dieptrongnguyen@yahoo.com

https://doi.org/10.25073/2588-1167/vnuls.4444

Tác động của chính sách chuyển đổi số với bảo đảm quyền tiếp cận thông tin

Nguyễn Trọng Điệp[1,*], Nguyễn Tiến Đạt[2]

[1]*Khoa Luật, Đại học Quốc gia Hà Nội, 144 Xuân Thuỷ, Cầu Giấy, Hà Nội, Việt Nam*
[2]*Học viện Chính sách và Phát triển, Nam An Khánh, Hoài Đức, Hà Nội, Việt Nam*

Nhận ngày 24 tháng 02 năm 2022
Chỉnh sửa ngày 10 tháng 6 năm 2022; Chấp nhận đăng ngày 01 tháng 7 năm 2022

Tóm tắt: Quyền tiếp cận thông tin là một trong những quyền con người quan trọng, được ghi nhận ở hầu hết các quốc gia trên thế giới, và được biết đến khá sớm với Đạo luật Tự do báo chí năm 1766 ở Thụy Điển. Quyền này tạo lập nên niềm tin của nhân dân, góp phần hình thành sự ổn định chính trị của một quốc gia. Bài viết đề cập tới một số nội dung cơ bản, nghiên cứu cơ sở lý luận, thực tiễn bảo đảm quyền tiếp cận thông tin trong bối cảnh chuyển đổi số ở Việt Nam.

Từ khóa: Tiếp cận thông tin; Quyền con người; Chuyển đổi số.

1. Mở đầu

Chuyển đổi số được thế giới và Việt Nam nhìn nhận như xu thế tất yếu không thể đảo ngược đặc biệt trong bối cảnh toàn cầu đối mặt với diễn biến phức tạp của dịch bệnh và tác động mạnh của Cách mạng công nghiệp 4.0. Khái niệm "nền kinh tế chia sẻ" ra đời đặt ra yêu cầu bảo vệ tốt hơn quyền con người trên không gian mạng, trong đó quyền tiếp cận thông tin là một trong các nhóm quyền chịu tác động mạnh bởi xu hướng này. Để đáp ứng yêu cầu bảo vệ quyền tiếp cận thông tin, Luật Tiếp cận thông tin ra đời năm 2016 cụ thể hóa nội dung được đề cập trong Hiến pháp năm 2013 và phù hợp nội dung Tuyên ngôn toàn thế giới về quyền con người năm 1948 của Liên Hợp Quốc, Công ước quyền dân sự và chính trị năm 1966 mà Việt Nam là thành viên. Bài viết tập trung phân tích một số vấn đề lý luận liên quan tới quyền tiếp cận thông tin trong bối cảnh chuyển đổi số và những tồn tại và rủi ro cho quyền tiếp cận thông tin trên không gian mạng trong bối cảnh hoàn thiện pháp luật Việt Nam hiện nay.

2. Quyền tiếp cận thông tin trong bối cảnh số

2.1. Quá trình hình thành và phát triển của quyền tiếp cận thông tin

Khái niệm "Thông tin" (tiếng Anh: information) được giải thích trong Từ điển Oxford English Dictionary là điều mà người ta đánh giá hoặc nói đến; là tri thức, tin tức. Theo tiếng Latin, "Infomatio" - gốc của từ "Information" có 02 nghĩa, một để chỉ hành động tạo ra một hình dạng (forme), hai là sự truyền đạt một ý tưởng, một khái niệm hay một biểu tượng. Theo quan điểm triết học, "thông tin" là sự phản ánh của tự nhiên và xã hội bằng ngôn từ, ký hiệu, hình ảnh… Theo Khoản 1 Điều 2 Luật Tiếp cận

*Tác giả liên hệ.
Địa chỉ email: dieptrongnguyen@yahoo.com

https://doi.org/10.25073/2588-1167/vnuls.4444

thông tin năm 2016, thông tin là "tin, dữ liệu được chứa đựng trong văn bản, hồ sơ, tài liệu có sẵn, tồn tại dưới dạng bản viết, bản in, bản điện tử, tranh, ảnh, bản vẽ, băng, đĩa, bản ghi hình, ghi âm hoặc các dạng khác do cơ quan nhà nước tạo ra". Từ đó, tiếp cận thông tin được hiểu là "việc đọc, xem, nghe, ghi chép, sao chép, chụp thông tin" (khoản 3 Điều 2 Luật Tiếp cận thông tin). Trong cách tiếp cận của Liên minh Châu Âu, Quy định bảo vệ dữ liệu chung (GDPR) 2016/679 hướng tới khái niệm "thông tin" được xác định trong phạm vi hẹp - là các "dữ liệu cá nhân" gồm bất kể thông tin gì liên quan đến một thể nhân được nhận dạng hoặc có thể được nhận dạng "chủ thể"; một thể nhân có thể được nhận dạng là người có thể được nhận dạng trực tiếp hay gián tiếp bằng việc tham chiếu số định danh hay một hoặc các yếu tố riêng về vật lý, sinh lý, tâm thần, kinh tế, văn hóa và xã hội.

Các nhà nghiên cứu đều thống nhất khởi nguồn của quyền tiếp cận thông tin xuất phát từ trào lưu bảo đảm "Tự do thông tin" (tiếng Anh: freedom of information) chính thức được ghi nhận đầu tiên tại Thụy Điển thông qua Đạo luật Tự do báo chí năm 1766 - đạo luật được ghi nhận là sớm nhất trong tổng số 100 quốc gia trên thế giới có luật về tự do thông tin. Theo đó, Đạo luật mở ra quyền tiếp cận tài liệu công cho công dân nhưng cũng giới hạn lạm dụng tự do ngôn luận để xâm phạm lợi ích Nhà nước.

Tuy nhiên, một cách chính thức, tự do thông tin chỉ được nhìn nhận như một quyền cơ bản của con người thông qua Tuyên bố của Đại hội đồng Liên hợp quốc theo Nghị quyết 59 ngày 04/12/1946, theo đó: "Tự do thông tin là quyền cơ bản của con người và là nền tảng cho tất cả các quyền tự do được Liên hợp quốc tôn vinh".

Tuyên ngôn Nhân quyền Liên hợp quốc năm 1948 tiếp tục khẳng định và thừa nhận quyền tự do thông tin như một trong những quyền cơ bản của con người đòi hỏi các quốc gia trên thế giới phải đảm bảo. Theo đó, Điều 19 Tuyên ngôn ghi nhận quyền này dưới 02 góc độ: quyền tự do biểu đạt và quyền tự do tìm kiếm và tiếp nhận "Mọi người đều có quyền tự do ngôn luận và bày tỏ ý kiến; kể cả tự do bảo lưu quan điểm mà không bị can thiệp; cũng như tự do tìm kiếm, tiếp nhận và truyền bá các ý tưởng và thông tin bằng bất kỳ phương tiện truyền thông nào và không giới hạn về biên giới".

Tiếp đó, Điều 19 Công ước quốc tế về các quyền dân sự và chính trị năm 1966 một lần nữa tái khẳng định nội hàm quyền tiếp cận thông tin và nghĩa vụ các quốc gia thành viên trong xây dựng khuôn khổ pháp lý để đảm bảo quyền này: *"Mọi người đều có quyền tự do ngôn luận. Quyền này bao gồm tự do tìm kiếm, tiếp nhận, và truyền đạt mọi thông tin, ý kiến, không phân biệt lĩnh vực, hình thức tuyên truyền bằng miệng, bằng bản viết, in, hoặc dưới hình thức nghệ thuật, thông qua bất kỳ phương tiện thông tin đại chúng nào tùy theo sự lựa chọn của họ"*. Đồng thời, Công ước cũng mở ra một cơ chế hạn chế quyền con người - một trong những phương thức đã được áp dụng trong Hiến pháp Việt Nam năm 2013 nhằm tạo cơ sở để đảm bảo tốt hơn quyền này với 02 ngoại lệ gồm: i) Hạn chế để đảm bảo tôn trọng quyền hoặc uy tín của người khác và ii) Hạn chế để bảo vệ an ninh quốc gia hoặc trật tự công cộng, hoặc y tế hoặc đạo đức công cộng. Trong các lĩnh vực khác, quyền tiếp cận thông tin cũng được đề cập trong Công ước của Liên hợp quốc về chống tham nhũng năm 2003; Tuyên bố Rio de Janeiro về Môi trường và phát triển năm 1992; Nguyên tắc Johannesburg về an ninh quốc gia, tự do ngôn luận và tiếp cận thông tin năm 1995; Công ước Châu Âu về tiếp cận tư pháp trong các vấn đề môi trường năm 1998 (Công ước Aarhus)…

Dựa trên các cam kết được đề cập trong Tuyên ngôn và Công ước, các quốc gia trên thế giới đã nỗ lực trong xây dựng và hoàn thiện pháp luật để tăng cường bảo đảm quyền tiếp cận thông tin của công dân.

Liên minh Châu Âu trong các nỗ lực của mình đã ghi nhận quyền tiếp cận thông tin tại Điều 10 Công ước Châu Âu về quyền con người năm 1950; Điều 42 Hiến chương về các quyền cơ bản của Liên minh Châu Âu năm 2000; Điều 15 Hiệp ước về vận hành Liên minh Châu Âu.

Các văn kiện của Liên minh Châu Âu hướng tới các nhóm nội dung như: quyền tiếp cận các văn kiện của Liên minh Châu Âu; quyền sử dụng các thông tin chung theo lĩnh vực; quyền tiếp cận các thông tin về môi trường; quyền đối với dữ liệu cá nhân (đặc biệt là việc ban hành và thực thi Nghị định 95/46/EC về bảo vệ dữ liệu cá nhân trong đó có đề cập tới quyền tiếp cận thông tin).

Hoa Kỳ xây dựng Đạo luật về Tự do thông tin vào năm 1966 dưới thời Tổng thống Lyndon B.Johnson, và tiếp tục phát triển với Đạo luật sửa đổi về Tự do thông tin điện tử được Tổng thống Bill Clinton ký ban hành năm 1996. Trên cơ sở đó, chính quyền các bang ở Hoa Kỳ cũng phát triển và mở rộng quyền tiếp cận thông tin theo đặc thù mỗi bang.

Ở Châu Á, Nhật Bản xây dựng Luật Tiếp cận thông tin của các cơ quan hành chính năm 1999 và có hiệu lực áp dụng từ năm 2001. Hàn Quốc ban hành Đạo luật về Bảo mật thông tin năm 1996 trên cơ sở phán quyết của Tòa án Hiến pháp Hàn Quốc năm 1989. Thái Lan ban hành Đạo luật Thông tin chính thức năm 1997; Ấn Độ ban hành Đạo luật về Quyền thông tin năm 2005. Ở Trung Quốc, một số địa phương có ban hành quy định về tự do thông tin như Quảng Châu, Thượng Hải; Hồng Kông xây dựng Bộ luật về ứng xử năm 1996 có đề cập tới quyền tiếp cận thông tin. Ngoài ra, các khu vực khác trên thế giới cũng ghi nhận khung pháp lý quốc tế về quyền tiếp cận thông tin như: Điều 9 Hiến chương Châu Phi về quyền con người; Điều 13 Hiến chương Châu Mỹ về quyền con người…

Qua đó cho thấy tiến trình phát triển và mở rộng của các quy định về tiếp cận thông tin trên phạm vi thế giới.

2.2. Quyền tiếp cận thông tin theo pháp luật Việt Nam

Tại Việt Nam, Hiến pháp năm 1992 của thời kỳ Đổi mới đã đề cập tới quyền tiếp cận thông tin trong hệ thống các quyền con người, quyền công dân hiến định. Kế thừa giá trị đó, Điều 25 Hiến pháp năm 2013 quy định "Công dân có quyền tự do ngôn luận, tự do báo chí, tự do tiếp cận thông tin, hội họp, lập hội, biểu tình. Việt thực hiện các quyền này do pháp luật quy định". Đây là tiền đề để Việt Nam thời gian qua nỗ lực xây dựng và hoàn thiện cơ sở pháp lý để thực thi quyền tiếp cận thông tin thông qua ban hành các văn bản Luật chuyên ngành như: Luật Đất đai năm 2013; các Luật Doanh nghiệp năm 2014, năm 2020; các Luật Đầu tư năm 2014, năm 2020; Luật Trưng cầu ý dân năm 2015… và các văn bản sửa đổi bổ sung theo hướng mở rộng khả năng tiếp cận thông tin của người dân theo từng lĩnh vực cụ thể.

Luật Tiếp cận thông tin năm 2016 chính thức có hiệu lực từ 01/7/2018 được coi như bước tiến hoàn thiện cơ bản các quy định bảo vệ quyền tiếp cận thông tin của cá nhân, tổ chức, từng bước đề cập tới tiếp cận thông tin thông qua mạng điện tử. Theo đó, thông tin được tiếp cận được định nghĩa gồm tin, dữ liệu được chứa đựng trong văn bản, hồ sơ, tài liệu có sẵn, tồn tại dưới dạn bản viết, bản in, bản điện tử, tranh, ảnh, bản vẽ, băng, đĩa, bản ghi hình, ghi âm hoặc các dạng khác do cơ quan nhà nước tạo ra, được ký, đóng dấu hoặc xác nhận bằng văn bản. Luật Tiếp cận thông tin cũng phân định rõ ràng quyền tiếp cận thông tin của công dân với người nước ngoài.

Hoạt động tiếp cận thông tin qua mạng điện tử được hỗ trợ đáng kể bởi trước đó năm 2015 Quốc hội đã thông qua Luật An toàn thông tin mạng và sau đó năm 2018 thông qua Luật An ninh mạng. Năm 2018, Việt Nam cũng thông qua Luật Bảo vệ bí mật nhà nước trong đó làm rõ khái niệm bí mật nhà nước thuộc nhóm thông tin công dân không được tiếp cận.

3. Tác động của Chính sách chuyển đổi số và các kiến nghị chính sách pháp luật với Việt Nam

"Chuyển đổi số" (tiếng Anh: Digital transformation) gần đây được nhắc nhiều trong hệ thống các chính sách nhằm thúc đẩy Cuộc cách mạng công nghiệp lần thứ 4 tại Việt Nam. Chuyển đổi số được hiểu là quá trình khai thác các dữ liệu có được từ quá trình số hóa

(digitizing) rồi áp dụng các công nghệ để phân tích, biến đổi các dữ liệu đó và tạo ra các giá trị mới hơn. Nhìn nhận cốt lõi của Cuộc cách mạng công nghiệp lần thứ 4 là chuyển đổi số kết hợp số hóa, kết nối, siêu kết nối và xử lý dữ liệu thông minh, Bộ Chính trị đã ban hành Nghị quyết số 52-NQ/TW ngày 27/9/2019 về một số chủ trương, chính sách chủ động tham gia Cuộc cách mạng công nghiệp lần thứ tư đặt ra nhiệm vụ cấp bách phải đẩy nhanh quá trình chuyển đổi số. Ba đột phá chiến lược được đề cập trong Văn kiện Đại hội XIII của Đảng Cộng sản Việt Nam gồm hoàn thiện thể chế; phát triển nguồn nhân lực và xây dựng hạ tầng đều nhắc tới vai trò của chuyển đổi số.

Trên tinh thần đó, năm 2020, Thủ tướng Chính phủ đã ban hành Chỉ thị số 01/CT-TTg ngày 14/1/2020 về thúc đẩy phát triển công nghệ số Việt Nam, và ban hành Quyết định số 749/QĐ-TTg ngày 03/6/2020 phê duyệt "Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030", qua đó đặt mục tiêu chuyển đổi nhận thức và từng bước số hóa tài sản thông tin, tái cấu trúc quy trình nghiệp vụ, tổ chức và hình thành môi trường số.

Chính phủ Việt Nam đang nỗ lực thực thi chính sách Chuyển đổi số đặc biệt ưu tiên hướng tới cộng đồng doanh nghiệp. Diễn đàn Chuyển đổi số Việt Nam năm 2021 (Vietnam DX Summit 2021) cung cấp khung hướng dẫn chuyển đổi số cho các doanh nghiệp vừa và nhỏ trong 26 lĩnh vực, với khung cơ bản và khung chuyên dụng, chia 3 cấp độ quy mô doanh nghiệp từ siêu nhỏ tới vừa. Được biết, tính tới tháng 12/2020, doanh nghiệp vừa và nhỏ chiếm 98,1% trong tổng số 811.000 doanh nghiệp, đóng góp 45% GDP cả nước và bị tác động đáng kể bởi dịch bệnh COVID-19 khi mỗi tháng có 10.000 doanh nghiệp ngừng hoạt động.

Chỉ số chuyển đổi số được công bố hàng năm dựa trên 3 trụ cột gồm: Chính quyền số; Kinh tế số và Xã hội số là thước đó quá trình và nỗ lực của mỗi địa phương trong hiện thực hóa các nội dung của chính sách chung từ Chính phủ. Tuy nhiên, thực tiễn cho thấy còn nhiều rủi ro trong bảo đảm quyền tiếp cận thông tin trong triển khai chuyển đổi số, cụ thể:

Thứ nhất, rủi ro an toàn thông tin trên không gian mạng.

Với nền tảng của Cách mạng công nghiệp 4.0 là internet thì an toàn không gian mạng là điều kiện bắt buộc để bảo đảm quyền con người trong thụ hưởng giá trị của khoa học công nghệ. Tuy nhiên, có thể thấy vấn đề về bảo đảm quyền con người trong các nội dung của các chiến lược, kế hoạch của các Bộ, ngành và địa phương chưa được đề cập thỏa đáng đến vấn đề đảm bảo an toàn kết nối internet. Vấn đề nằm ở việc cơ sở pháp lý quan trọng để đảm bảo quyền con người trong một xã hội thông minh khi internet kết nối vạn vật là Luật An ninh mạng dù đã được thông qua từ năm 2018 tuy nhiên Nghị định hướng dẫn xử phạt hành vi vi phạm hành chính trong lĩnh vực an ninh mạng mới dừng ở dự thảo. Tình trạng này khiến các giao dịch, thông tin người dùng bị khai thác, và các vi phạm trên môi trường internet không thể được xử lý.

Trong nhóm quyền riêng tư được pháp luật bảo hộ, quyền bí mật thông tin (gồm hình ảnh, thông tin nhận diện cá nhân, gia đình; tình trạng sức khỏe, cảm xúc, gia đình, học tập, các mối quan hệ, nơi ở; thư từ, điện thoại, điện tín, các hình thức lưu trữ, trao đổi thông tin khác); quyền bảo vệ và được pháp luật bảo vệ chống lại các hành vi thu thập, khai thác, sử dụng, công bố thông tin, can thiệp vào đời sống riêng tư phải đối mặt với rủi ro từ môi trường mạng xã hội và từ những công cụ "kết nối vạn vật" được xây dựng dựa trên nền tảng các phần mềm ứng dụng trên điện thoại và máy tính. Trên thực tế, tất cả thông tin người dùng trên Facebook, Google, Snapchat, Instagram... đều được lưu trữ trong hồ sơ trực tuyến của người dùng do các công ty công nghệ nắm giữ. Rủi ro lợi dụng thông tin trên môi trường internet đã được cảnh báo và có thực tiễn trên thế giới: năm 2013, 3 tỷ người bị lộ thông tin tài khoản Yahoo; năm 2017, nhà mạng Verizon của Mỹ làm lộ 14 triệu bản ghi thông tin khách hàng … Ở Việt Nam, tình trạng nhà mạng

bán thông tin khách hàng để thu lợi không phải hiếm gặp.

Luật An toàn thông tin mạng năm 2015 (sửa đổi, bổ sung năm 2018) đã nghiêm cấm hành vi "Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật" tại Điều 7. Tuy nhiên, thống kê của Cục An toàn thông tin, Bộ Thông tin và Truyền thông cho thấy dự báo vào năm 2025, số lượng các cuộc tấn công mạng và mã độc mới sẽ tăng tương ứng 3 lần và 2,4 lần so với năm 2020; số lỗ hổng, điểm yếu mới xuất hiện cũng tăng gấp 1,75 lần. Báo cáo xếp hạng mức độ sẵn sàng bảo đảm an toàn thông tin mạng năm 2020 do Bộ Thông tin và Truyền thông công bố đối với 89 cơ quan, gồm 26 bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ (trừ các bộ: Công an, Quốc phòng, Thông tin và Truyền thông) và 63 tỉnh, thành phố trong cả nước, vẫn còn 5 bộ, ngành và 11 tỉnh, thành phố xếp loại C. Điều này cho thấy rủi ro an toàn thông tin trên môi trường mạng tại Việt Nam còn rất đáng lo ngại.

Thứ hai, cơ chế xử lý vi phạm pháp luật sử dụng, mua bán thông tin trên không gian mạng chưa hiệu quả.

Quyền bất khả xâm phạm đời sống riêng, quyền bảo vệ bí mật gia đình hay được yêu cầu tòa án tuyên bố thông tin tiêu cực về mình là không đúng sự thật... đã được quy định trong Bộ luật Dân sự 2015, có hiệu lực từ 1/1/2017. Năm 2017, Nghị định 49/2017/NĐ-CP sửa đổi Điều 15 Nghị định 25/2011/NĐ-CP hướng dẫn Luật viễn thông và Điều 30 Nghị định 174/2013/NĐ-CP 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 được ban hành. Nhưng chế tài cho hành vi nhà mạng để lộ, lọt thông tin khách hàng chưa rõ ràng, mức xử phạt 50-70 triệu tại Điều 30 Nghị định không quy định chế tài với hành vi để lộ, lọt thông tin và nếu có áp dụng thì chế tài không đủ sức răn đe. Việc bổ sung, sửa đổi mức chế tài là cần thiết nhằm xử lý nghiêm khắc các hành vi vi phạm. Ở mức độ hình sự, hành vi mua bán, trao đổi, tặng cho, sửa chữa, thay đổi hoặc công khai hóa thông tin riêng hợp pháp của cơ quan, tổ chức, cá nhân trên mạng máy tính, mạng viễn thông mà không được phép của chủ sở hữu thông tin nhằm thu lợi bất chính có thể bị phạt tiền cao nhất là 200 triệu đồng; phạt cải tạo đến 3 năm hoặc phạt tù từ 6 tháng đến 3 năm theo Điều 288 Bộ luật Hình sự năm 2015, sửa đổi năm 2017.

Thực tế xét xử hiện nay cho thấy các vụ việc tương tự có dấu hiệu gia tăng cả về quy mô và tính chất nguy hiểm. Tháng 6/2021, Công an tỉnh Phú Thọ đã khởi tố vụ án liên quan tới hành vi móc nối giữa Nguyễn Lê Thanh Tú (36 tuổi, TP Hồ Chí Minh) và Lê Trí Viễn (29 tuổi, Quảng Nam) để mua thông tin các công ty gồm: số tài khoản, mẫu dấu tròn, mẫu dấu tên chủ doanh nghiệp, mẫu chữ ký của chủ tài khoản và kế toán trưởng, sao kê tài khoản ngân hàng để thực hiện hành vi chiếm đoạt tài sản thông qua rút tiền mặt tại Ngân hàng TMCP Công Thương Việt Nam, chi nhánh Đền Hùng. Trước đó, tháng 5/2021, Dư Anh Quý (33 tuổi) và Lại Thị Phương (29 tuổi) đã bị khởi tố điều tra hành vi đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông. Theo đó, từ năm 2021, hai bị cáo này đã thu thập, chiếm đoạt, mua bán trái phép dữ liệu hàng tỷ thông tin về các cá nhân, tổ chức trên toàn quốc trong nhiều lĩnh vực (điện lực, ngân hàng; phụ huynh học sinh…) và rao bán công khai trên web, trang, nhóm trên mạng xã hội.

Thứ ba, quy trình xử lý dữ liệu thông tin chưa được đề cập trong các quy định pháp luật.

Xử lý thông tin dữ liệu (tiếng Anh: data information processing) được hiểu là một chuỗi công đoạn bao gồm: xác nhận, sắp xếp, tóm tắt, tập hợp, phân tích, báo cáo và phân loại theo các chuẩn mực pháp lý nghiêm ngặt. Ở Châu Âu, Quy định bảo vệ dữ liệu chung (GDPR) 2016/679 của Liên minh Châu Âu đặt ra sáu điều kiện cụ thể yêu cầu bên xử lý dữ liệu phải thoả mãn ít nhất một trong các điều kiện đó, bao gồm: (i) có chấp thuận của chủ thể dữ liệu cho mục tiêu cụ thể, (ii) có sự cần thiết để thực hiện hợp đồng có liên quan; (iii) để tuân thủ nghĩa vụ pháp lý của bên xử lý dữ liệu, (iv) cần thiết để bảo vệ

lợi ích sống còn của chủ thể dữ liệu hoặc một người khác, (v) cần thiết để thực hiện một công vụ vì lợi ích công; (vi) cần thiết vì lợi ích hợp pháp của bên khác với điều kiện không hạn chế quyền tự do cơ bản của chủ thể dữ liệu, đặc biệt quyền của trẻ em. Trong khi đó, Điều 17 Luật An toàn thông tin mạng của Việt Nam chỉ quy định duy nhất hai điều kiện nguyên tắc gồm: (i) Tiến hành thu thập thông tin cá nhân sau khi có sự đồng ý của chủ thể thông tin cá nhân về phạm vi, mục đích của việc thu thập và sử dụng thông tin đó; và (ii) Chỉ sử dụng thông tin cá nhân đã thu thập vào mục đích khác mục đích ban đầu sau khi có sự đồng ý của chủ thể thông tin cá nhân. Điều này dẫn tới thực tế bảo vệ an toàn thông tin ở Việt Nam còn hời hợt và chưa đủ mạnh để ngăn chặn các hành vi xâm phạm quyền và lợi ích chính đáng của công dân.

Thứ tư, thiếu vắng quy định ràng buộc trách nhiệm và nghĩa vụ của bên thu thập và xử lý dữ liệu thông tin.

Tiếp tục so sánh giữa pháp luật an toàn thông tin của Việt Nam và châu Âu cho thấy, GDPR có quy định 04 trách nhiệm và 04 nhóm nghĩa vụ mà bên thu thập và xử lý dữ liệu phải tuân thủ. Bốn trách nhiệm gồm: (i) Phải có hệ thống kỹ thuật và chính sách để bảo vệ dữ liệu; (ii) Chỉ thu thấp và xử lý dữ liệu trong phạm vi mục tiêu định trước; (iii) Báo cáo các khâu xử lý dữ liệu; (iv) Hợp tác bảo vệ dữ liệu cá nhân và quyền riêng tư. Bốn nhóm nghĩa vụ gồm: (i) Bảo đảm an toàn dữ liệu; (ii) Đánh giá tác động và tham vấn; (iii) Nhân sự bảo vệ dữ liệu; (iv) Xây dựng và tuân thủ Quy tắc ứng xử trong bảo vệ dữ liệu (Code of conduct). Việt Nam hiện nay quy định vấn đề này tại Điều 17 Luật An ninh mạng chỉ ghi nhận 03 nhóm nghĩa vụ gồm: có sự đồng ý của chủ thể thông tin; sử dụng vì mục đích ban đầu và không phát tán, chia sẻ khi chưa được đồng ý. Điều 46 Luật Giao dịch điện tử năm 2005 có bổ sung thêm về bảo mật thông tin trong giao dịch điện tử nhưng không làm rõ thêm các nghĩa vụ này. Điều này cho thấy còn chênh lệch khá lớn giữa quy định pháp luật Việt Nam với chuẩn mực quốc tế trong vấn đề này.

Thứ năm, thiếu đầu mối quản lý và giám sát dữ liệu thông tin.

Tại Việt Nam, hiện tại có 02 cơ quan bộ tham gia quản lý và đảm bảo an toàn dữ liệu và quyền riêng tư gồm Bộ Thông tin và Truyền thông và Bộ Công an. Tuy nhiên, do tính chất phức tạp trong quản lý thông tin mà các bộ, ngành khác cũng tham gia phụ trách an toàn thông tin chuyên ngành như: Bộ Quốc phòng; Ban Cơ yếu Chính phủ… thậm chí các Ủy ban nhân dân cấp tỉnh cũng xây dựng hướng dẫn về an toàn thông tin trên địa bàn phụ trách. Điều này không tránh khỏi tình huống mâu thuẫn, chồng chéo trong thẩm quyền quản lý và giải quyết các vụ việc phát sinh. Kinh nghiệm của nhiều quốc gia cho thấy việc tinh giảm đầu mối quản lý và phụ trách an toàn thông tin mạng là chìa khóa để nâng cao chất lượng nguồn lực cho công tác này. Theo yêu cầu của GDPR, mỗi nước thành viên của Liên minh Châu Âu phải chỉ định cơ quan đứng đầu và đại diện quốc tế trong hoạt động bảo vệ dữ liệu. Chẳng hạn, ở Đức là German Federal Commissioner for Data Protection and Freedom of Information – BfDI (Uỷ viên Liên bang Đức về Bảo vệ dữ liệu và Tự do thông tin), ở Pháp là National Commission for Freedom of Information – CNIL (Uỷ ban quốc gia về Tự do thông tin), và ở Anh là Information Commissioner - ICO (Uỷ viên phụ trách Thông tin).

Diễn biến dịch bệnh COVID-19, xu hướng làm việc tại nhà (Work From Home) và sự phát triển các thiết bị IoT (Internet of Things - mạng lưới các thiết bị được kết nối với Internet nhằm mục đích thu thập, chia sẻ dữ liệu cho nhau) của xu thế chuyển đổi số, các tác động kể trên đã và đang đòi hỏi pháp luật trong lĩnh vực này cần những đột phát mới như sau:

Thứ nhất, khắc phục những xung đột và trùng lặp trong cách hiểu giữa các quy định trong các văn bản quy phạm pháp luật.

Giữa các quy định của Luật An toàn thông tin mạng năm 2015 và Luật An ninh mạng năm 2018 còn những quy định gây cách hiểu trùng lặp. Cụ thể, Khoản 1 Điều 2 Luật An ninh mạng

năm 2018 đề cập phạm vi "An ninh là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân". Trong khi, Khoản 1 Điều 3 Luật An toàn thông tin mạng năm 2015 đề cập phạm vi An toàn thông tin mạng là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin. Những khác biệt cơ bản giữa 02 văn kiện pháp lý quan trọng này không phải dễ dàng phân tách nội hàm, đòi hỏi cần những tuyên truyền hoặc phân định rạch ròi nội hàm điều chỉnh để tránh nhầm lẫn trong áp dụng.

Thứ hai, đơn giản hóa cơ chế xử lý vi phạm và tăng cường tính răn đe và phòng ngừa chung.

Ứng dụng công nghệ trong thực thi pháp luật đã được ứng dụng trong nhiều lĩnh vực như: cân tải xe tự động; xử phạt nguội vi phạm giao thông; thu phí tự động… là tiền đề quan trọng để áp dụng đơn giản hóa cơ chế xử lý vi phạm trong lĩnh vực an toàn thông tin mạng và an ninh mạng. Thực tế, thủ tục rút gọn trong giải quyết vụ việc liên quan tới bảo vệ quyền lợi người tiêu dùng và thủ tục rút gọn, xét xử trực tuyến trong tố tụng dân sự đã được hướng dẫn cụ thể và bước đầu triển khai. Do đó, việc áp dụng cơ chế xử phạt linh hoạt và trực tuyến với các hành vi vi phạm với đầy đủ chứng cứ hợp pháp về hình ảnh, mã nguồn…là khả thi và có thể bước đầu thí điểm.

Thứ ba, bổ sung các quy định về xử lý dữ liệu thông tin của cá nhân và tổ chức.

Mặc dù quy định pháp luật xử lý các trường hợp vi phạm an toàn thông tin cá nhân/tổ chức đã có nhưng quy mô và tính chất mới dừng ở mức vụ việc đơn lẻ. Có một so sánh đã được TS. Chu Thị Hoa, Phó Viện trưởng Viện Khoa học pháp lý (Bộ Tư pháp) đưa ra gần đây đó là: mức phạt hành chính nặng nhất theo Nghị định 15/2020/NĐ-CP cho hành vi xâm phạm bí mật cá nhân tối đa chỉ là 1 tỷ VNĐ hoặc phạt tù đến 7 năm (Điều 288 Bộ luật Hình sự 2015) trong khi mức phạt theo GDPR lên tới 20 triệu EURO, tương đương 500 tỷ đồng [11]. Điều đó cho thấy mức phạt răn đe sẽ có ý nghĩa tác động đáng kể tới ý thức tuân thủ pháp luật của cá nhân, tổ chức trong bối cảnh việc xâm phạm dữ liệu riêng tư đem lại siêu lợi nhuận.

Thứ tư, bổ sung trách nhiệm và nghĩa vụ của bên thu thập và xử lý dữ liệu thông tin.

Pháp luật hiện nay cần sớm bổ sung những quy định ràng buộc trách nhiệm của đơn vị cung ứng dịch vụ hạ tầng mạng viễn thông/internet đối với hành vi thông đồng, thiếu giám sát nội dung sử dụng trái phép thông tin dữ liệu cá nhân. Việc bỏ qua quy định vai trò quan trọng và gần như quyết định của các nhà mạng - bên cung cấp dịch vụ mạng thông tin trong các vụ việc xâm phạm dữ liệu thông tin khách hàng mà mới tập trung xử lý bên sử dụng thông tin cuối. Có thể khẳng định hành vi vi phạm dữ liệu thông tin khách hàng không thể thực hiện được nếu có sự giám sát hiệu quả, triệt để đối với nội dung thông tin trên không gian mạng . Trong giai đoạn từ 2015 tới nay, các vụ việc xử phạt nhà cung cấp hạ tầng mạng viễn thông/internet mới chỉ dừng ở xử phạt hành chính vài trăm triệu tới hơn 1 tỷ đồng vì hành vi khuyến mại, quản lý thuê bao chưa phản ánh đúng thực tế "bát nháo" sử dụng thông tin dữ liệu cá nhân, tổ chức trên internet.

Thứ năm, thống nhất đầu mối quản lý và giám sát dữ liệu thông tin.

Trong bối cảnh Luật An ninh mạng gắn trách nhiệm đầu mối cho Bộ Công an, trong khi Luật An toàn thông tin mạng lại gắn trách nhiệm đầu mối cho Bộ Thông tin và Truyền thông thì việc thiết lập cơ chế phối hợp hoặc xây dựng thiết chế liên bộ là cần thiết nhằm giải quyết dứt điểm tình huống "dẫm chân nhau" giữa hai Bộ trong giải quyết các vụ việc vi phạm.

4. Kết luận

Trong bối cảnh chung của xu hướng chuyển đổi số đang diễn ra trên thế giới, khi những thành tựu công nghệ của Cuộc cách mạng công nghiệp 4.0 đã và đang tác động ngày càng mạnh mẽ đến Việt Nam, việc bảo đảm quyền tiếp cận thông tin

cũng như an toàn trong tiếp cận, sử dụng và khai thác nguồn dữ liệu thông tin vô giá là không dễ dàng. Tình trạng tiếp cận thông tin bất hợp pháp và vi phạm thông tin cá nhân trên không gian mạng càng trở nên phức tạp hơn khi đặt trong bối cảnh pháp luật quốc tế, khu vực và quốc gia đang gặp khó khi phải giải quyết các vấn đề tranh chấp "xuyên biên giới". Mặc dù trong 10 năm gần đây Việt Nam đã có nhiều nỗ lực xây dựng và hoàn thiện pháp luật nhằm điều chỉnh vấn đề này, các quy định nhìn chung chưa thực sự đi vào cuộc sống, khó thực thi và không tạo hiệu ứng cần thiết để giải quyết vấn đề.

Để đảm bảo hiệu quả thực thi pháp luật về quyền tiếp cận thông tin trong bối cảnh chuyển đổi số, việc thiết lập và xây dựng một đạo luật bao quát các vấn đề pháp lý phát sinh trên không gian mạng (quản lý thông tin; giám sát thông tin; kiểm soát an toàn và an ninh thông tin trên không gian mạng) đồng thời thu gọn đầu mối quản lý đa ngành về vấn đề an toàn - an ninh thông tin có lẽ cần được cân nhắc trong thời gian tới.

Tài liệu tham khảo

[1] T. T. T. Dung, Quá trình phát triển của quyền tiếp cận thông tin, Tạp chí Khoa học Pháp lý Việt Nam số 04(59)/2010 (2010) 14-21.

[2] P. T. T. Tuyền, Nguyên tắc bảo đảm quyền tiếp cận thông tin theo tinh thần của Luật Tiếp cận thông tin năm 2016, Tạp chí Nghiên cứu Lập pháp số 17(393) (2019).

[3] Bộ Tư pháp, Tài liệu Tập huấn chuyên sâu về Luật Tiếp cận thông tin, NXB Tư pháp, Hà Nội (2017)

[4] Đ. P. Tân, Về khái niệm thông tin và các thuộc tính làm nên giá trị của thông tin, Tạp chí Văn hóa - Nghệ thuật, số 3/2001.

[5] V. C. Giao, L. T. N. Tuyên, Bảo vệ quyền đối với dữ liệu cá nhân trong pháp luật quốc tế, pháp luật một số quốc gia và giá trị tham khảo cho Việt Nam, Tạp chí Nghiên cứu Lập pháp số 09 (409), tháng 5/2020.

[6] N. T. Q. Anh, V. C. Giao, N. M. Hương, L. K. Tùng, Quyền về sự riêng tư, NXB Chính trị Quốc gia Sự Thật, Hà Nội, 2018.

[7] N. Sơn, Bảo đảm quyền tiếp cận thông tin của công dân trong hoạt động của cơ quan hành chính nhà nước, Tạp chí Công Thương.

[8] H. M. Hội, Bảo đảm quyền tiếp cận thông tin của công dân - thực trạng và một số kiến nghị, Tạp chí Nghiên cứu Lập pháp số 5(309), tháng 3/2016.

[9] H. M. Sơn, Bảo đảm quyền tiếp cận thông tin theo tinh thần của Hiến pháp năm 2013, Cổng thông tin Ban Nội chính Trung ương (noichinh.vn), truy cập 14/2/2016.

[10] N. H. Ly, Pháp luật hiện hành của Việt Nam về bảo vệ dữ liệu, thông tin cá nhân và quyền riêng tư, Cổng thông tin Ban Cơ yếu Chính phủ (nacis.gov.vn), truy cập ngày 25/12/2020.

[11] Nguyên nhân của vấn nạn mua bán dữ liệu cá nhân trên không gian mạng (Vietnamnet)