

BẢO VỆ DỮ LIỆU, THÔNG TIN CÁ NHÂN TRÊN MÔI TRƯỜNG SỐ CỦA MỘT SỐ QUỐC GIA VÀ NHỮNG GỢI MỞ ĐỐI VỚI VIỆT NAM

LƯƠNG THỊ HỒNG HƯƠNG (*)
NÔNG THỊ LÝ (**)
NGUYỄN ANH THƯ (***)

Tóm tắt: Trong những năm gần đây, vấn đề để lộ dữ liệu, thông tin cá nhân trên môi trường số ở Việt Nam rất đáng báo động, gây ảnh hưởng tiêu cực đến mỗi cá nhân, cũng như của xã hội. Bài viết nghiên cứu việc bảo vệ dữ liệu, thông tin cá nhân trên môi trường số của một số quốc gia trên thế giới, đây là những kinh nghiệm và gợi mở đối với Việt Nam để tiếp tục có giải pháp phù hợp, hiệu quả nhằm bảo vệ dữ liệu, thông tin cá nhân trên môi trường số hiện nay.

Từ khóa: Bảo vệ dữ liệu; kinh nghiệm; môi trường số; thông tin cá nhân.

Abstract: In recent years, the issue of revealing data and personal information in the digital environment in Vietnam has been very alarming, causing negative impacts on individuals and society. This paper reviews the protection of data and personal information in the digital environment of some countries around the world, and draws out the experience lessons for Vietnam to continue taking appropriate and effective solution to protect data and personal information in today's digital environment.

Keywords: Data protection; experience; digital environment; personal information.

Ngày nhận bài: 24/10/2023 Ngày biên tập: 30/11/2023 Ngày duyệt đăng: 22/02/2024

1. Một số khái niệm về dữ liệu, thông tin cá nhân và môi trường số

1.1. Dữ liệu cá nhân, thông tin cá nhân

Hiện nay, vẫn còn nhiều ý kiến chưa thống nhất về khái niệm thông tin cá nhân (TTCN) và khái niệm dữ liệu cá nhân (DLCN). Có quan điểm cho rằng, TTCN chính là DLCN, hoặc DLCN rộng hơn TTCN. Để hiểu rõ TTCN là gì, một số nhà khoa học phân tích dưới dạng thuật ngữ hợp thành bởi hai từ “thông tin” và “cá nhân”. Thông tin là một danh từ được hiểu là điều được truyền đi cho biết, tin truyền đi. Cá nhân là người riêng lẻ, phân biệt với tập thể hoặc xã hội. Điều đó có thể hiểu những thông tin về một người riêng lẻ, phân biệt với người đó đối với những người khác chính là

TTCN. Dưới góc độ luật học, TTCN là khái niệm gắn liền với quyền riêng tư. Điều 3 Luật An toàn thông tin mạng năm 2015 định nghĩa: “Thông tin cá nhân là thông tin gắn với việc xác định danh tính của một người cụ thể”; khoản 13, Điều 3 Nghị định số 52/2013/NĐ-CP về thương mại điện tử nêu rõ: “Thông tin cá nhân là các thông tin góp phần định danh một cá nhân cụ thể, bao gồm tên, tuổi, địa chỉ nhà riêng, số điện thoại, thông tin y tế, số tài khoản, thông tin về các giao dịch thanh toán cá nhân và những thông tin khác mà cá nhân mong muốn giữ bí mật”.

Về DLCN, Công ước số 108 năm 1981 của Hội đồng châu Âu nêu rõ: “Dữ liệu cá nhân có nghĩa là bất kỳ thông tin liên quan đến một cá nhân được xác định hoặc mang tính chất cá nhân”. Trong khi đó, Tổ chức Hợp tác và Phát triển Kinh tế định nghĩa: “Dữ liệu cá nhân là bất kỳ thông tin liên

(*), (**) *Học viện Tòa án*

(***) *ThS; Trưởng khoa Khoa Đào tạo thẩm phán, Học viện Tòa án*

quan đến một cá nhân được xác định hoặc có thể nhận dạng”. Quy định chung về bảo mật dữ liệu cá nhân (GDPR) của Liên minh châu Âu quy định: “Dữ liệu cá nhân được hiểu là tất cả các thông tin liên quan đến một cá nhân được nhận diện hoặc có thể được nhận diện, dù trực tiếp hay gián tiếp”. Đó có thể là những thông tin liên quan đến tên, số chứng minh thư, dữ liệu về nơi cư trú, số điện thoại, hoặc bất kỳ một hoặc những yếu tố đặc biệt nào liên quan đến việc nhận diện về thể chất, tâm lý, sinh lý, di truyền, kinh tế, văn hóa hoặc xã hội của cá nhân.

Ở Việt Nam, khoản 1, Điều 2 Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, quy định: “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 bao gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm”.

Từ cơ sở nghiên cứu tài liệu và các quan điểm cũng như quy định của pháp luật hiện hành, cho thấy giữa TTCN và DLCN là hai thuật ngữ có nhiều điểm tương đồng liên quan đến quyền con người, nhất là quyền riêng tư. Tuy nhiên, vẫn có sự khác biệt, vì vậy cần có quy định cụ thể, bởi vì khi xác định phạm vi khái niệm giúp hạn chế tình trạng phạm tội cũng như để áp dụng trong quá trình thực hiện chế tài.

1.2. Môi trường số

Môi trường số, hay còn gọi là môi trường kỹ thuật số là môi trường truyền thông tích hợp, nơi các thiết bị kỹ thuật số giao tiếp, quản lý nội dung và hoạt động. Khái niệm này dựa trên các hệ thống điện tử kỹ thuật số được tích hợp và triển khai cho cộng đồng toàn cầu. Môi trường số là một không gian sống, trong đó công nghệ số đã chuyển phương thức sản xuất truyền thống trong hệ thống công nghiệp sang phương thức áp dụng các công nghệ với những trụ cột, như: dữ liệu lớn, internet kết nối vạn vật, công nghệ điện toán đám mây...⁽¹⁾. Môi trường số là thế giới kết nối nhờ công nghệ trong không gian giữa người với người nhằm tạo ra sự kết nối và tương tác lẫn nhau đáp ứng nhu cầu của con người trong cuộc sống.

2. Thực tiễn áp dụng pháp luật về bảo vệ dữ liệu cá nhân, thông tin cá nhân trên môi trường số ở Việt Nam

Trong lĩnh vực hình sự, pháp luật đã quy định những hình phạt với hành vi xâm phạm quyền riêng tư của người khác, trong đó có thông tin của cá nhân trên không gian mạng. Điều 159 Bộ luật Hình sự năm 2015 quy định: “Xâm phạm bí mật hoặc an toàn thư tín, điện thoại, điện tín hoặc hình thức trao đổi thông tin riêng tư của người khác” có thể bị phạt tù tới 03 năm, với hành vi đưa hoặc sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông có thể chịu hình phạt cao nhất lên tới 07 năm tù.

Trong lĩnh vực dân sự, Điều 34 Bộ luật Dân sự năm 2015 quy định cá nhân có quyền đối với hình ảnh của mình. Việc sử dụng hình ảnh của cá nhân phải được người đó đồng ý, đây là quyền nhân thân được pháp luật ghi nhận và bảo vệ. Chỉ trong một số trường hợp pháp luật cho phép như sử dụng hình ảnh vì lợi ích quốc gia, dân tộc, lợi ích công cộng; sử dụng từ các hoạt động công cộng, bao gồm hội nghị, hội thảo, hoạt động thi đấu thể thao, biểu diễn nghệ thuật và hoạt động công cộng khác mà không làm tổn hại đến danh dự, nhân phẩm, uy tín của người có hình ảnh. Điều 38 Bộ luật Dân sự năm 2015 cũng ghi nhận quyền về đời sống riêng tư, bí mật cá nhân, bí mật gia đình... Đây là những quy định cụ thể, điều chỉnh chung trong lĩnh vực dân sự nhằm bảo đảm quyền nhân thân của cá nhân nói chung và quyền riêng tư nói riêng. Luật An toàn thông tin mạng năm 2015 được ban hành với nhiều quy định bảo vệ TTCN trên môi trường phức tạp này. Luật quy định rõ về nguyên tắc bảo vệ TTCN trên mạng, thu thập và sử dụng TTCN, cập nhật, sửa đổi và hủy bỏ TTCN yêu cầu bảo đảm an toàn TTCN trên mạng và trách nhiệm của cơ quan quản lý nhà nước trong bảo vệ TTCN trên mạng.

Tuy nhiên, hệ thống pháp luật của Việt Nam hiện nay quy định về xử lý vi phạm DLCN và TTCN còn nhiều vướng mắc, bất cập. Đặc biệt trong bối cảnh hiện nay, thông tin, dữ liệu người dùng ngày càng trở nên quan trọng, có giá trị như một “tài sản” cùng mức độ phát triển của công nghệ làm cho nhiều người quan ngại về vấn đề bảo mật thông tin. Công tác quản lý nhà nước với hoạt động của

các trang mạng xã hội như facebook, tiktok... chưa được chặt chẽ; rất dễ để tìm kiếm thông tin của một cá nhân trên mạng xã hội, thậm chí là dữ liệu nhạy cảm; tình trạng DLCN được mang ra rao bán khắp nơi. Mặt khác, do tính kết nối không có biên giới của internet nên việc áp dụng pháp luật để bảo vệ DLCN của người dùng gặp nhiều khó khăn. Các trường hợp vi phạm quyền DLCN không được phát hiện, xử lý kịp thời hoặc các cơ quan quản lý còn lúng túng trong vấn đề áp dụng chế tài phù hợp. Đồng thời, các văn bản pháp luật về bảo vệ DLCN

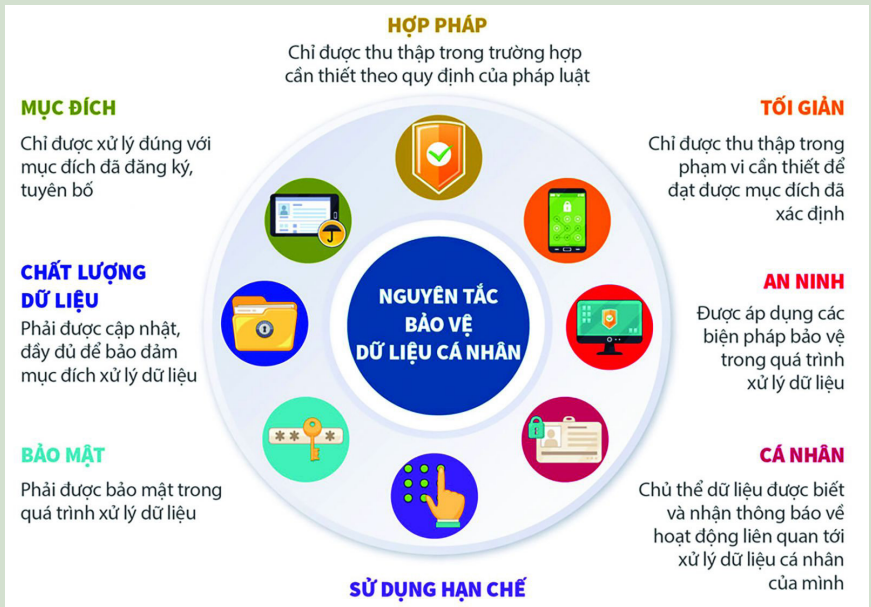
chưa dự liệu được hết những tình huống trong thực tế, nhất là việc thu thập, xử lý thông tin với đối tượng là trẻ em. Cơ chế, cách thức thu thập thông tin mà các website/ứng dụng di động đang thực hiện chưa quy định rõ ràng, trong đó có quy định về lấy ý kiến khách hàng khi thu thập thông tin; mức xử phạt với các hành vi vi phạm chưa đủ sức răn đe.v.v.

3. Kinh nghiệm bảo vệ dữ liệu cá nhân, thông tin cá nhân của một số tổ chức, quốc gia và những gợi mở đối với Việt Nam

3.1. Kinh nghiệm của một số tổ chức, quốc gia

3.1.1. Liên minh châu Âu (EU) có khung pháp lý về bảo vệ DLCN rất nghiêm ngặt và hiệu quả, theo mô hình tiếp cận tất yếu.

Trọng tâm của mô hình này là đề cao quyền riêng tư của cá nhân. Các hoạt động thu thập, quản lý, sử dụng TTCN được các cơ quan quản lý điều chỉnh chặt chẽ. Các nước thành viên tuân thủ và nội luật hóa những quy định chung của Hội đồng châu Âu, thể hiện qua việc ban hành một đạo luật riêng về bảo vệ thông tin (hoặc dữ liệu) để quy định cụ thể, toàn diện tất cả những vấn đề có liên quan. Tháng 5/2018, EU đã ban hành Luật Bảo vệ dữ liệu chung châu Âu (GDPR) áp dụng chung cho tất cả các quốc gia thành viên. GDPR yêu cầu các doanh



8 nguyên tắc bảo vệ dữ liệu cá nhân (nguồn: Dự thảo Nghị định Quy định về bảo vệ dữ liệu cá nhân của Bộ Công an).

nh nghiệp phải tuân thủ các quy định cụ thể, rõ ràng về cách thu thập TTCN, địa điểm lưu trữ dữ liệu, loại hình dữ liệu được phép chia sẻ, các công ty nằm ngoài lãnh thổ châu Âu cũng phải chấp hành các quy định này. Tất cả các tổ chức, cá nhân có liên quan phải tuân thủ các điều kiện nghiêm ngặt trong quá trình thu thập và quản lý dữ liệu.

3.1.2. Nhật Bản đã ban hành Đạo luật bảo vệ thông tin cá nhân (APPI) năm 2003, có hiệu lực từ tháng 4/2005, được sửa đổi năm 2015, với những sửa đổi quan trọng tiếp theo có hiệu lực năm 2022.

Đây là đạo luật được thiết kế để bảo vệ TTCN của công dân Nhật Bản. Bất cứ ai nhận được dữ liệu, TTCN của công dân nước này đều phải tuân thủ đầy đủ các quy định của APPI, nếu không sẽ có nguy cơ bị kiện tụng. Cụ thể, APPI có phạm vi áp dụng rộng bao gồm cả những pháp nhân nước ngoài khi thu thập và xử lý TTCN ở Nhật Bản. Tại khoản 4 Điều 2 của Đạo luật xác định APPI áp dụng cho nhà quản lý doanh nghiệp có thể ở dạng thể nhân hay pháp nhân sử dụng dữ liệu, TTCN với mục đích kinh doanh. Các doanh nghiệp đều phải tuân thủ APPI khi thu thập và xử lý thông tin. Tuy nhiên, APPI cũng có sự linh động khi ngoại lệ một số trường hợp không áp dụng đối với

các cơ quan nhà nước chính quyền địa phương, cơ quan hành chính được sáp nhập, những tổ chức hành chính độc lập ở địa phương và các nhà văn chuyên nghiệp, báo chí, học giả, các đảng phái chính trị và các nhóm tôn giáo.

Đồng thời, APPI thiết lập quy định mở nhằm tôn trọng quyền định đoạt của cá nhân về dữ liệu và thông tin của chính họ. Cụ thể, chỉ được cung cấp dữ liệu, TTCN cho bên thứ ba khi được sự đồng ý từ chính cá nhân. Theo đó, nếu không có sự cho phép của chính họ thì sẽ không được phép cung cấp thông tin bằng bất cứ cách thức nào cho bên thứ ba. Bên thứ ba được xác định dưới dạng thể nhân, pháp nhân thậm chí là các công ty dưới dạng nhà quản lý doanh nghiệp, góp phần vào việc thể hiện sự tự chủ, quyết định của cá nhân. Việc chuyển DLCN cho bên thứ ba ở nước ngoài hoặc ngay tại chính Nhật Bản đều phải tuân thủ các yêu cầu theo quy định của APPI, đồng thời nếu có sự đồng ý của việc chuyển nhượng này của người ủy thác thì người chuyển nhượng cũng chỉ được cung cấp những dữ liệu, TTCN của người đó trong giới hạn nhất định đã được quy định cụ thể⁽²⁾.

3.1.3. Hoa Kỳ là quốc gia có hệ thống bảo mật thông tin lâu đời và hiệu quả nhất thế giới.

Mặc dù không có một đạo luật riêng về bảo vệ DLCN ở cấp độ liên bang, nhưng ở từng ngành, từng lĩnh vực của Hoa Kỳ đã xây dựng được nhiều văn bản điều chỉnh cụ thể. Với đối tượng là trẻ em, pháp luật Hoa Kỳ có Luật Bảo vệ quyền về sự riêng tư trực tuyến của trẻ em (COPPA), luật này giúp cho cha mẹ của trẻ có thể kiểm soát các hành vi thu thập DLCN đối với con của họ. Trong lĩnh vực y tế, Luật về trách nhiệm giải trình và trách nhiệm bảo hiểm y tế (HIPPA) đảm bảo tất cả dữ liệu chăm sóc sức khỏe cho bệnh nhân được an toàn. Pháp luật của Hoa Kỳ thường theo mô hình ủng hộ các luật chuyên ngành để điều chỉnh cụ thể mà không quá đặt nặng những quy tắc bảo vệ dữ liệu chung. Mô hình tiếp cận bảo vệ TTCN tại Hoa Kỳ kết hợp hài hòa giữa bảo vệ TTCN và đảm bảo quyền lợi cho các chủ thể khác. Cơ chế pháp lý được xây dựng theo hướng cởi mở hơn với những TTCN thông thường và tập trung bảo vệ cho những TTCN nhạy cảm. Vì vậy, quy định pháp lý về bảo vệ TTCN thường dần trải trong các luật và văn bản chuyên ngành.

3.2. Những gợi mở đối với Việt Nam

Thứ nhất, Nhà nước ta cần có sự thống nhất trong vấn đề bảo vệ DLCN, TTCN; quy định thống nhất khái niệm TTCN và phân định rõ giữa TTCN và DLCN. Đồng thời, xây dựng các quy định chú trọng đến quyền và nghĩa vụ của các chủ thể, nhất là các bên thứ ba khi thực hiện hành vi khai thác, sử dụng dữ liệu TTCN đáp ứng kịp thời những yêu cầu của tiêu chuẩn quốc tế hiện hành.

Thứ hai, cần phân loại từng DLCN, mức độ rủi ro và biện pháp xử lý hiệu quả khi DLCN bị tiết lộ và sử dụng vào những mục đích không chính đáng. Vấn đề định danh cá nhân trong môi trường số cũng cần được bổ sung đầy đủ như tên người dùng trên mạng xã hội, địa chỉ IP, các loại dấu vân tay của thiết bị, ảnh và video. Với những thông tin mang tính nguyên tắc chung, cần được tiếp tục cụ thể hóa và làm rõ trong những văn bản dưới luật như các nghị định, thông tư, văn bản hướng dẫn...

Thứ ba, Việt Nam chưa có một văn bản luật nào quy định trực tiếp vấn đề bảo vệ DLCN, mà được điều chỉnh trong một số văn bản pháp luật chuyên ngành. Hiện nay, Việt Nam vẫn đang hướng tới thắt chặt, kiểm soát thông tin, DLCN cho người dùng, kể cả là thông tin thông thường hay dữ liệu nhạy cảm.

Thứ tư, tăng cường tuyên truyền nhằm nâng cao ý thức của người dân khi sử dụng mạng xã hội và các môi trường khác DLCN dễ dàng bị lộ. Các cơ quan quản lý, thực thi pháp luật cần kiểm soát chặt chẽ các trang mạng xã hội để phát hiện những sai phạm; có hình thức xử lý nghiêm các tổ chức, cá nhân vi phạm các quy định, nhất là hoạt động thu thập, mua bán trái phép DLCN. Đồng thời, khi tham gia vào môi trường mạng, mỗi cá nhân rất cần được bảo vệ bởi pháp luật, nhưng đồng thời phải có ý thức tự bảo vệ thì mới thực sự đảm bảo quyền riêng tư đối với DLCN của mình./.

Ghi chú:

(1) Xem <https://www.quanlynhanuoc.vn/2022/07/05/cong-dan-so-trong-moi-truong-so>.

(2) Japan - Data Protection Overview (2022), xem tại: <https://www.dataguidance.com/notes/japan-data-protection-overview>, 18/04/2022.