MÔ HÌNH QUẢN LÝ QUYỀN RIÊNG TƯ TRONG THỊ TRƯỜNG DỮ LIỆU VÀ MỘT VÀI GỢI Ý HOÀN THIỆN QUY ĐỊNH PHÁP LUẬT VIỆT NAM

TRẦN NGỌC TUẤN*

Ngày nhận bài: 19/06/2021

Ngày phản biện: 27/06/2021

Ngày đăng bài: 30/09/2021

Tóm tắt:

Trong bối cảnh của sự phát triển vượt bậc của hệ thống dữ liệu, dữ liệu lớn đã đặt ra yêu cầu phải có các giải pháp quản lý hiệu quả. Một trong những yêu cầu cấp bách được đặt ra là làm thế nào để hạn chế sự xâm phạm quyền riêng tư trong hoạt động quản lý dữ liệu. Bài viết phân tích các vấn đề pháp lý liên quan đến quyền riêng tư trong thị trường dữ liệu, lý thuyết mô hình quản lý quyền riêng tư. Bên cạnh đó, bài viết còn làm rõ tính cấp thiết của việc bảo vệ quyền riêng tư trong bối cảnh của thị trường dữ liệu ở Việt Nam, từ đó đưa ra một số đề xuất các nguyên tắc quản lý dữ liệu cũng như kiến nghị về việc hoàn thiện các quy định của pháp luật Việt Nam về vấn đề này.

Từ khóa:

Bảo mật, dữ liệu, quyền riêng tư, mô hình quản lý quyền riêng tư, thị trường dữ liệu.

Abstract:

In the significant development of data systems, big data has posed a requirement for practical solutions to manage. One of the urgent requirements is how to limit the invasion of privacy in data management activities. The article analyzes legal issues related to privacy in the data market, theory, and privacy management model. In addition, the article also clarifies the urgency of protecting privacy in the context of the data market in Vietnam, thereby making some recommendations on data management principles and knowledge recommendations on the improvement of the provisions of Vietnamese law on this issue.

Keywords*:*

Data, data market, privacy management model, privacy, security.

1. Đặt vấn đề

Ngày nay, các dịch vụ trực tuyến phát sinh các vấn đề mang tính hệ thống do thu thập và xử lý dữ liệu cá nhân tràn lan, đặc biệt là sự hình thành, phát triển sôi động của thị trường dữ liệu. Với cuộc Cách mạng công nghiệp 4.0, dữ liệu lớn (Big data) trở thành tài sản thông

* NCS., Trường Đại học Sài Gòn; Email: tntuan@sgu.edu.vn

tin với khối lượng dữ liệu lớn, tốc độ cao và đa dạng[1]. Những vấn đề này, đặt ra những thách lớn cho các nhà làm luật cũng như các nhà cung cấp dịch vụ trong việc xây dựng một hệ thống quản lý và bảo vệ quyền riêng tư hiệu quả trong bối cảnh của cuộc Cách mạng công nghiệp 4.0 và những biến động của hoàn cảnh thế giới. Trên thực tế, có rất nhiều mô hình khả thi khác nhau để giải quyết vấn đề này, nhưng không có các quy định chặt chẽ trong các lĩnh vực cụ thể[2]. Bài viết này, tác giả khái quát mô hình quản lý quyền riêng tư (PMM) để tạo ra một bộ công cụ quản lý bổ sung, "thông minh" để thay đổi các động lực của những người dùng trên thị trường và đề xuất một vài giải pháp trong việc hoàn thiện quy định của pháp luật trong việc bảo vệ quyền riêng tư của người dùng trên các thị trường dữ liệu hiện nay.

2. Các vấn đề về quy định bảo mật dữ liệu trong thị trường dữ liệu

Khái niệm thị trường dữ liệu (A data marketplace or data market) được đề cập như là nơi để người ta mua bán dữ liệu. Một trong những "sản phẩm" của thị trường này phải kể đến đó là "dữ liệu cá nhân" - cái mà gắn với quyền riêng tư của mỗi người. Hầu như các nhà cung cấp dịch vụ mạng Internet đều thực hiện mô hình "cài đặt quyền riêng tư mặc định" trong việc chấp nhận sử dụng dịch vụ, qua đó thúc đẩy người dùng "chia sẻ"" dữ liệu của họ một cách hợp pháp, nhưng đằng sau đó là vấn đề sử dụng, khai thác, bảo mật dữ liệu lại được đặt ra. Do đó, thách thức đầu tiên trong việc đưa ra các quy định về quyền riêng tư của dữ liệu là do tính chủ quan của nó, điều này gây khó khăn cho việc xác định các quy tắc về dữ liệu.

Vấn đề đầu tiên để bảo mật dữ liệu cá nhân đó là đánh giá quyền riêng tư. Ngày nay, có nhiều mô hình đánh giá dựa trên những tiêu chuẩn xã hội nhất định[3]. Tiêu chuẩn xã hội như vậy có thể được hiểu là một tập hợp các lựa chọn về quyền riêng tư[4] mà một cá nhân có thể áp dụng, điều này sẽ không gây tranh cãi đối với hầu hết các thành viên trong xã hội[5]. Một số tác giả phân chia xã hội thành các thái độ riêng tư khác nhau, chẳng hạn như những người theo chủ nghĩa bảo mật quyền riêng tư, những người thực dụng và không quan tâm[6]. Cuối cùng, ý thức về quyền riêng tư khác nhau trên toàn cầu (Cộng đồng chung châu Âu và Hoa Kỳ, Trung Quốc) và cả giữa các quốc gia cụ thể[7] trong việc thực hiện các quy định bảo vệ quyền riêng tư của cá nhân. Thực tế cho thấy, với sự phát triển như vũ bão của cuộc Cách mạng công nghiệp 4.0,

[1] Lê Thị Thúy Nga (2020), *Bảo vệ quyền đối với đời sống riêng tư, bí mật cá nhân, bí mật gia đình trong bối cảnh Cách mạng công nghiệp 4.0*, Tạp chí Dân chủ và pháp luật, số 3, tr.5.

[2] J. Braithwaite (2017), Types of Responsiveness' in P. Drahi's (ed), *Regulatory Theory: Foundations and Applications*, ANU Press, Acton, p.118.

[3] N.A. Moreham (2016), *The Nature of Privacy Interest' in N.A. Moreham and M. Warby (eds),* The Law of Privacy and the Media, Oxford University Press, Oxford 2016, p.42, pp.49-51; H.T. Gomez-Arostegui (2005), "Defining Private Life under the European Convention on Human Rights by Referring to Reasonable Expectations", 35 *California Western International Law Journal*, p.153.

[4] Lưu ý rằng thử nghiệm pháp lý về kỳ vọng hợp lý về quyền riêng tư không chỉ là điều này; N.A. Moreham (2016), above n. 3, pp.50-51.

[5] E.g. *Hosking v Runting* (2004), NZCA 34, para. 250 per J Tipping.

[6] A.F. Westin (2003), "Social and Political Dimensions of Privacy", 59 *Journal of Social Issues* 431, p.445; see also the discussion in J.M. Urban and C.J. Hoofnagle (2014), "The Privacy Pragmatic as Privacy Vulnerable", *SSRN*, http://papers.ssrn.com/abstract=2514381.

[7] Điều này đã được thảo luận rộng hơn trong B.-J. Koops, B.C. Newell, T. Timan, I. Škorvánek, T. Chokrevski and M. Galič (2016), "A Typology of Privacy", *SSRN*, http://papers.ssrn.com/ abstract=2754043.

hàng loạt các dịch vụ, ứng dụng trực tuyến ra đời từng giờ từng phút trên CH Play[8] hay App Store[9] mang tính toàn cầu khi mà gần như ai có tài khoản và điện thoại kết nối Internet đều có thể tiếp cận được. Điều này đã đặt ra nhu cầu cần có một số quy tắc để điều chỉnh "tiêu chuẩn" về quyền riêng tư từ các nhà cung cấp dịch vụ theo lựa chọn chủ quan của từng người, và từng xã hội cụ thể.

Ngoài ra, đối với các quy định về bảo vệ quyền riêng tư trong môi trường dữ liệu (trong việc đưa ra các quy tắc và thực thi chúng) chúng đặt ra vấn đề kiểm soát thực tế đối với thông tin[10]. Có nhiều phương thức khác nhau để thu thập thông tin, giữa truyền thống và hiện đại với các ứng dụng của khoa học công nghệ[11]. Vì vậy, trọng tâm của quy định về quyền riêng tư của dữ liệu là quản lý việc thu thập và sử dụng dữ liệu, điều này cần được thực hiện ở nơi lưu trữ những dữ liệu đó[12]. Phạm vi quản lý phải bảo gồm dữ liệu gốc (thô), liên quan đến dữ liệu, kiểm soát dữ liệu và bảo vệ việc dữ liệu được chuyển giao. Nguyên tắc giới hạn gián tiếp việc sử dụng dữ liệu của người kiểm soát dữ liệu bằng các quy tắc pháp lý cũng cần được đặt ra. Điều này cần dựa trên việc có được sự đồng ý của chủ thể dữ liệu[13] để sử dụng dữ liệu cho một mục đích cụ thể được tiết lộ tại thời điểm đưa ra sự đồng ý này.

Để giải quyết những vấn đề được miêu tả ở trên trong thị trường dữ liệu hiện nay, cần có một mô hình cụ thể để có thể giải quyết hài hoà các quyền lợi của các bên liên quan cũng như thúc đẩy sự đầu tư, nghiên cứu từ việc khai thác dữ liệu để tạo ra những tri thức mới cho xã hội.

3. Mô hình quản lý quyền riêng tư (PMM)

PMM[14] là một tập hợp các chức năng cần thiết để quản lý quá trình bảo mật. PMM tạo thành một mô hình lý thuyết để thực hiện sự lựa chọn tự điều khiển đối với quá trình quản lý dữ liệu. Quản lý quyền riêng tư yêu cầu:

---

[8] CH Play là cửa hàng của Google Play đáp ứng đa dạng các ứng dụng và trò chơi cho hàng tỷ chiếc điện thoại sử dụng hệ điều hành Android tại hơn 190 quốc gia và vùng lãnh thổ lớn nhỏ trên toàn thế giới. CH là viết tắt của từ "Cửa Hàng". Khi người dùng ngôn ngữ tiếng Việt máy sẽ hiển thị tên CH Play còn khi chuyển sang ngôn ngữ tiếng Anh thì sẽ là Google Play. Đến với CH Play người dùng có thể tải về vô vàn ứng dụng Android miễn phí một cách nhanh chóng và tiện lợi.

[9] App Store mang đến cho mọi người trên khắp thế giới một nơi an toàn và đáng tin cậy để khám phá các ứng dụng đáp ứng các tiêu chuẩn cao của Apple về quyền riêng tư, bảo mật và nội dung.

[10] D.J. Solove (2008), *Understanding Privacy*, Harvard University Press, Cambridge, MA, p.28; D. boyd (2012), "Networked Privacy", 10 *Surveillance & Society* 348, p.349; J.W. DeCew (1997), *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Cornell University Press, Ithaca, p.53.

[11] Lê Thị Giang (2018), *Quyền riêng tư đối với thông tin cá nhân*, Tạp chí Kiểm sát, số 17, tr.18.

[12] Vì lý do bảo mật, các nhà cung cấp dịch vụ có vị trí tốt hơn để giữ an toàn cho dữ liệu so với người dùng cá nhân, B. Schneier (2018), *Click Here to Kill Everybody: Security and Survival in a Hyper- connected World*, W.W. Norton & Company, New York, p.111.

[13] Sometimes knowledge is enough, see OECD (2013), *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, p.7.

[14] Đây là phần mở rộng và sửa đổi của mô hình được mô tả trong M. Betkier (2016), *Individual Privacy Management 21*, Media and Arts Law Review, 315, p.323. Các thay đổi bao gồm ví dụ: tiêu chí đánh giá, sự thích ứng của việc lập kế hoạch với việc sử dụng bên ngoài và năng động của các chính sách quyền riêng tư, liên kết tốt hơn với nền tảng lý thuyết, các loại dữ liệu mới và sử dụng dữ liệu.

- Kiểm soát: Đảm bảo khả năng giám sát quá trình và phản ánh trạng thái của luồn dữ liệu.

- Lập kế hoạch: Đảm bảo khả năng xem xét những vấn đề sẽ xảy ra và đặt mục tiêu (chính sách cá nhân).

- Tổ chức: Như cấu trúc các thông số chính của quá trình và truy cập dữ liệu cá nhân để thực hiện các chức năng khác.

Quyền riêng tư được hiểu là "không ai chịu can thiệp một cách tùy tiện vào cuộc sống riêng tư, gia đình, nơi ở hoặc thư tín, cũng như bị xúc phạm danh dự, nhân phẩm của cá nhân. Với sự phát triển của internet, việc bảo vệ các giá trị riêng tư vấp phải nhiều khó khăn, điều này đặt ra yêu cầu về việc quản lý nó một cách hiệu quả trên mọi lĩnh vực[15]. Quản lý quyền riêng tư phải là một quá trình. Chủ thể dữ liệu phải được chủ động và ưu tiên so với các bên còn lại về quyền riêng tư được sử dụng làm cài đặt bảo mật mặc định, nghĩa là chính sách này sẽ ghi đè lên bất kỳ "cài đặt hệ thống" nào do nhà cung cấp dịch vụ cung cấp. Trong PMM, cài đặt quyền riêng tư nên được thiết lập và giám sát từ bên ngoài hệ thống Công nghệ thông tin và truyền thông của các nhà cung cấp dịch vụ. Bằng cách này, các cá nhân có thể lấy lại quyền đối với dữ liệu của chính họ, giả sử rằng những dữ liệu và hệ thống Công nghệ thông tin và truyền thông đang nắm giữ chúng được khai thác đúng cách.

Việc tổ chức cũng bao gồm việc cung cấp cho các chủ thể dữ liệu các giao diện cho phép họ truy cập các cài đặt quyền riêng tư của mình và thao tác các cài đặt đó (để thực hiện việc kiểm soát và lập kế hoạch). Cần có hai giao diện - Giao diện người dùng (UI) và Giao diện lập trình ứng dụng (API).

Giao diện người dùng phải được chủ thể dữ liệu định hướng quản lý dữ liệu trực tiếp và Giao diện lập trình ứng dụng phải được định hướng quản lý tự động bằng một số phần mềm tự động bên ngoài được sử dụng bởi chủ thể dữ liệu hoặc bên thứ ba thay mặt họ. Đây là cách mà chính sách bảo mật của cá nhân được đưa vào hệ thống Công nghệ thông tin và giao tiếp của các nhà cung cấp dịch vụ. Để đảm bảo hoạt động của mô hình này, cần cơ chế kiểm soát riêng biệt.

Kiểm soát[16] là một tập hợp rộng hơn các hoạt động liên quan đến việc xem và thay đổi các thông số của quy trình bảo mật. Các chủ thể dữ liệu phải thông qua một chức năng kiểm soát để cho phép xử lý các loại dữ liệu cá nhân khác nhau của họ (tức là thu thập và sử dụng chúng). Sự khác biệt giữa chức năng kiểm soát của PMM và sự đồng ý là sự đồng ý cho phép sử dụng dữ liệu từ trước cho các mục đích được xác định trước bởi các nhà cung cấp dịch vụ (và thường do họ đơn phương thay đổi sau đó), trong khi chức năng kiểm soát cho phép thu thập dữ liệu được tiêu chuẩn hóa cụ thể các loại dữ liệu và cách sử dụng cụ thể của dữ liệu, mang lại cho chủ thể dữ liệu khả năng liên tục để thay đổi các quyết định đó trong quá trình

[15] Phùng Trung Tập (2019), *Cơ sở pháp lý bảo đảm quyền về đời sống tiêng tư, bí mật cá nhân, bí mật gia đình,* Tạp chí Dân chủ và pháp luật, số 7, tr.15.
[16] M. Betkier (2016), above n.14, pp.327-329.

sử dụng dịch vụ của các ứng dụng. Hơn nữa, việc kiểm soát phải cho phép của các chủ thể dữ liệu giám sát những dữ liệu đó và việc sử dụng chúng và phản ánh việc sử dụng đó để định hình lại các mục tiêu về quyền riêng tư của chính họ (trong việc lập kế hoạch)[17]. Tuy nhiên, một số hành động sẽ không thể thực hiện được đối với dữ liệu và việc sử dụng dữ liệu cần thiết cho các mục tiêu công cộng. Ví dụ, không thể xóa dữ liệu dành riêng cho việc thực thi pháp luật trong khung thời gian mà chúng sẽ có sẵn theo luật liên quan. Tuy nhiên, không có lý do gì để ẩn những dữ liệu đó khỏi các chủ thể dữ liệu[18] hoặc cho phép các hoạt động sử dụng khác của những dữ liệu đó chống lại quyền tự chủ về thông tin của chủ thể dữ liệu. Để làm tốt điều này, đòi hỏi cần có sự nâng cao vai trò của hoạt động của các cơ quan, tổ chức, phải nhận diện và phân loại được các hình thức bí mật dữ liệu[19].

Các hoạt động này tương tự như các hoạt động quản lý kinh doanh và cho phép các chủ thể dữ liệu phản ánh về việc đạt được các mục tiêu của họ và điều chỉnh các quyết định của họ cho phù hợp với hoàn cảnh bên ngoài. Ý tưởng đằng sau điều này là các chức năng này sẽ cho phép họ quản lý dữ liệu của mình một cách hiệu quả và không chỉ có sự kiểm soát[20]. Do đó, theo cách này, ở một mức độ nào đó, các chủ thể dữ liệu có thể xác định chắc chắn (và quyết định) ai biết những gì về họ.

PMM sẽ tạo thành một cơ chế riêng biệt với sự đồng ý áp dụng cho các nhà cung cấp dịch vụ Internet có khả năng vi phạm quyền tự chủ về dữ liệu. Theo quan điểm này, các doanh nghiệp sẽ triển khai và duy trì cấu trúc và giao diện tổ chức dữ liệu cần thiết cho phép các cá nhân quản lý dữ liệu của họ từ bên ngoài môi trường của nhà cung cấp dịch vụ. Việc quản lý có thể được thực hiện bởi các chủ thể dữ liệu được hỗ trợ bởi các bên thứ ba. Để tham gia vào mối quan hệ với một nhà cung cấp dịch vụ trực tuyến như vậy, khi ký kết hợp đồng trực tuyến, chủ thể dữ liệu phải cho phép nhà cung cấp dịch vụ đó nhập cài đặt chính sách dữ liệu người dùng (chính sách bảo mật cá nhân) từ một hệ thống được kiểm soát trực tiếp hoặc gián tiếp bởi người dùng. Theo cách này, cài đặt bảo mật mặc định của người dùng được ưu tiên hơn cài đặt mặc định của dịch vụ trực tuyến.

Việc triển khai PMM có thể không nhấn mạnh đến thủ tục đồng ý quá phức tạp.[21] Do đó, sự đồng ý có thể rất đơn giản vì nó không phải là cách duy nhất mà các chủ thể dữ liệu có thể thực hiện quyền tự chủ của họ. Những lợi ích có thể có của việc giới thiệu một công cụ

[17] Điều này có một số điểm tương đồng với tầm nhìn của hệ thống y tế được mô tả trong J. Zittrain (2000), "What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication Symposium: Cyberspace and Privacy: A New Legal Paradigm", *Stanford Law Review 1201*, pp.1243-44.

[18] Có thể có một số trường hợp trong đó chủ thể dữ liệu không thể truy cập được dữ liệu (ví dụ, bí mật nhà nước, bảo vệ chủ thể dữ liệu dễ bị tổn thương), nhưng những trường hợp này nên được coi là ngoại lệ mặc định.

[19] Thái Vĩnh Thắng (2017), *Bảo vệ quyền riêng tư ở Hoa Kỳ, Pháp và những kinh nghiệm cho Việt Nam*, Tạp chí Luật học, số 8, tr.98.

[20] Cf. O. Tene and J. Polonetsky (2013), *Privacy and Big Data: Making Ends Meet*, Stanford Law Review Online 25, p.261.

[21] Bằng cách cung cấp thêm thông tin không cần thiết và nhiều thông báo đồng ý riêng biệt.

dựa trên PMM để quản lý quyền riêng tư đã được phân tích ở trên. Để được thực hiện, PMM yêu cầu sự kết hợp của các chức năng được cung cấp bởi một mô hình kinh doanh cụ thể và các công cụ công nghệ hiện đại.

Tuy nhiên, mô hình đòi hỏi phải đáp ứng các mục tiêu liên quan giá trị của quyền riêng tư. Đầu tiên, việc thực hiện các phương tiện bổ sung để quản lý quyền riêng tư có thể được biện minh bởi nhu cầu đảm bảo tôn trọng các giá trị cá nhân, chẳng hạn như quyền tự quyết hoặc quyền tự chủ[22]. Theo nghĩa này, PMM rõ ràng nhằm tăng cường quyền tự chủ của các cá nhân bằng cách cho người dùng các công cụ để quản lý dữ liệu cá nhân của họ. Cách giải thích như vậy có thể sẽ có hiệu lực ở những quốc gia nơi các giá trị tự do rất quan trọng. Điều này có vẻ nghịch lý, bởi vì niềm tin vào tự do cá nhân thường đi đôi với niềm tin rằng Chính phủ không nên điều tiết thị trường vì không có lý do gì để Chính phủ biết rõ hơn những gì là lợi ích của cá nhân[23]. Vì các vấn đề về quyền riêng tư có tính hệ thống, chúng yêu cầu một giải pháp hệ thống như PMM. Thứ hai, việc thực hiện PMM là cần thiết để bảo vệ dữ liệu công cộng[24]. Các lý thuyết về lợi ích công cộng quy định rằng các giá trị như công bằng, phân phối lại[25], đoàn kết xã hội hoặc ngăn cản sự phụ thuộc của xã hội[26] là những lý do hợp lệ để điều chỉnh. Quyền riêng tư có thể được coi là một giá trị phù hợp với danh sách này. Thứ ba, mô hình PMM có thể được sử dụng để bảo vệ các nhóm dễ bị tổn thương[27].

Những cân nhắc này cho thấy sự phân bổ quyền riêng tư trong xã hội không đồng đều và các nhóm dễ bị các vấn đề về quyền riêng tư có thể khác với những nhóm bị ảnh hưởng bởi sự phân bổ của cải không đồng đều. Những người này có thể được tìm thấy ở hầu hết mọi tầng lớp xã hội và rất khó để đưa ra các quy tắc pháp lý nhằm bảo vệ họ.[28]

Việc triển khai PMM cũng có thể tăng cường quyền tự chủ của chủ thể dữ liệu trong quan điểm kinh tế để khắc phục các vấn đề của thị trường dữ liệu. Các lý do cho điều này có thể liên quan đến việc không tuân thủ các điều kiện quan trọng đối với lý thuyết thị trường: tiếp cận thông tin đầy đủ về hàng hóa, cạnh tranh hoàn hảo hoặc không có tác động của ngoại lực[29]. Thị trường trực tuyến cho dữ liệu cá nhân có thể không tuân thủ bất kỳ điều kiện nào trong ba điều kiện này. PMM nhằm mục đích duy trì cơ chế thị trường như là công cụ chính cho các thỏa thuận về quyền riêng tư và chỉ đưa ra các quy định để giúp thị trường vận hành.

[22] See e.g. C.R. Sunstein (1990), *After the Rights Revolution: Reconceiving the Regulatory State*, Harvard University Press, Cambridge, MA, p.35.
[23] C.R. Sunstein (1990), above n. 22, p.36.
[24] A.I. Ogus (2004), *Regulation: Legal Form and Economic Theory*, Hart Publishing, Oxford, p.54.
[25] B. Morgan and K. Yeung (2007), *An Introduction to Law and Regulation*, Cambridge University Press, Cambridge, p. 26.
[26] C.R. Sunstein (1990), above n.22, pp.61-64.
[27] Cf. C.R. Sunstein (1990), above n.18, pp.61-64.
[28] Imilarly, see E. Mik (2016), *The Erosion of Autonomy in Online Consumer Transactions*, Law, Innovation and Technology 1, p.14.
[29]A.I. Ogus (2004), *Regulation: Legal Form and Economic Theory*, Hart Publishing, Oxford, p.54.

Điều này có thể đạt được bằng cách giải quyết các vấn đề được nêu liên quan đến sự bất cân xứng của thông tin và thẩm quyền[30].

Bên cạnh đó, thị trường dữ liệu cá nhân có xu hướng tạo ra các công ty khổng lồ tích hợp theo chiều dọc và chiếm một phần lớn thị trường toàn cầu. Điều này ở một mức độ nào đó có thể được khắc phục bằng cách giới thiệu PMM, thứ sẽ tăng khả năng cạnh tranh trên thị trường[31]. Điều này là do PMM xây dựng lại một cơ chế bị loại bỏ khỏi một số mô hình kinh doanh trong đó khách hàng có quyền yêu cầu để giải quyết các vấn đề. PMM làm tăng sức mua của người tiêu dùng bằng cách cân bằng sự bất cân xứng thông tin, tăng khả năng kiểm soát dữ liệu của họ và giảm sự phụ thuộc của họ vào các nhà cung cấp dịch vụ cụ thể. Các hệ thống máy tính sẽ hỗ trợ điều này và tác động mạnh mẽ tới việc cần ban hành quy định cụ thể để quản lý, thu thập và xử lý thông tin[32]. Vì vậy, việc thực hiện PMM giúp tăng cường khả năng cạnh tranh của thị trường và những cơ hội kinh doanh tiềm năng cho các nhà cung cấp dịch vụ nảy sinh khi triển khai mô hình này, đồng thời, việc áp dụng PMM góp phần thúc đẩy nền kinh tế số.

4. Vấn đề bảo vệ dữ liệu ở thị trường Việt Nam hiện nay và kiến nghị hoàn thiện

4.1. Vấn đề bảo vệ dữ liệu ở thị trường Việt Nam hiện nay

Việt Nam là quốc gia đang phát triển, khoa học - công nghê đang tiếp cận với các xu thế chung của thế giới. Lĩnh vực an ninh mạng, an toàn thông điệp dữ liệu ở Việt Nam không là cụm từ tuyệt đối. Thực trạng cho thấy, vấn đề xâm phạm, "mua bán" dữ liệu mà không được sự đồng ý của chủ thể dữ liệu, tác động đến đời sống riêng tư của các cá nhân diễn ra khá phức tạp. Nhận định về tình trạng này, thông thường, nó liên quan đến tính có chủ ý của người có hành vi và mục đích từ các hành vi này[33].

Cụm từ "mua bán tràn lan", "công khai" thông tin dữ liệu không còn quá xa lạ trong nền kinh tế Việt Nam. Không phải là hiếm gặp khi trường hợp các cá nhân nhận được cuộc gọi bất ngờ từ một công ty bất động sản, công ty tài chính hay bảo hiểm mà trước đó họ chưa từng liên hệ với các đơn vị này. Vậy có bao giờ người dùng tự hỏi, các doanh nghiệp này lấy thông tin của mình từ đâu hay không. Câu trả lời nằm ở nội dung "mua bán dữ liệu". Và đương

[30] Cf. with a similar idea 'MyData', A. Poikola, K. Kuikkaniemi and O. Kuittinen (2014, *My Data*, Ministry of Transport and Communications; also, a similar idea of re-organising relations between individuals and vendors to guarantee independence from those vendors, see 'Project VRM', 2 February 2019, https://cyber.harvard.edu/projectvrm/Main_Page, accessed 19 February 2019. For more on this, see D. Searls (2012), *The Intention Economy: When Customers Take Charge*, Harvard Business Review Press, Boston, MA, p.134.

[31] Similarly, 'data mobility' in Ctrl-Shift (2018), *Data Mobility: The Personal Data Portability Growth Opportunity for the UK Economy*, Ctrl-Shift Ltd, London, p.36; see also "The Next Capitalist Revolution", *The Economist*, 17 November 2018, p.13.

[32] Thái Thị Tuyết Dung (2012), *Quyền riêng tư trong thời đại công nghệ thông tin*, Tạp chí Nghiên cứu Lập pháp, số 9 (217), tr.15.

[33] Vương Thanh Thúy (2017), *Về quyền riêng tư của cá nhân trong pháp luật hiện nay*, Tạp chí Quản lý nhà nước, số 263, tr.49.

nhiên chủ thể dữ liệu chưa bao giờ được hỏi "công ty A chuyển thông tin thu được này cho bên thứ ba được không?".

Giữa tháng 5 vừa qua, Cơ quan cảnh sát điều tra Bộ Công an khởi tố một cá nhân về tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông. Hai bị can này tổ chức một đường dây chiếm đoạt, mua bán, sử dụng trái phép gần 1.300 GB dữ liệu, chứa hàng tỷ thông tin về các cá nhân, tổ chức trên toàn quốc. Đặc biệt, "cơ quan chức năng xác định có dấu hiệu về sự thiếu trách nhiệm, buông lỏng quản lý của một số cơ quan, tổ chức, doanh nghiệp trong việc quản lý thông tin, dữ liệu cá nhân về khách hàng"[34]. Các dữ liệu chiếm đoạt mua bán thuộc hầu hết các lĩnh vực, bao gồm: danh sách cán bộ, danh bạ nội bộ của các cán bộ, tập đoàn kinh tế, khách hàng các ngân hàng, công ty lớn của nhà nước… Các thông tin có cả giấy tờ tùy thân, địa chỉ, số điện thoại, chức vụ công tác… Thậm chí, nhiều đối tượng còn cam kết khai thác, truy cập vào chính xác dữ liệu theo yêu cầu của người mua và được rao bán công khai trên các trang mạng xã hội như Facebook, Zalo, Instagram,… mà chưa bị các cơ quan chức năng kiểm tra, giám sát.

Thống kê "cho thấy có tới 80% nguyên nhân lộ, lọt thông tin cá nhân xuất phát từ chính sự bất cẩn của người dùng"[35]. Hầu hết thông tin cá nhân như ngày tháng năm sinh, trường học, nơi làm việc, nơi ở,... kê khai trên tài khoản mạng xã hội như Facebook, YouTube, Instagram đều do chính người sử dụng tự đưa lên và để ở chế độ mở. Thị trường "mua bán dữ liệu" nước ta diễn ta một cách "âm thầm" với chủ thể dữ liệu và "công khai" đối với bên thứ ba. Người tiêu dùng - chủ thể dữ liệu không hề biết được rằng thông tin của mình đang bị "mua bán" sôi nổi trên thị trường. Thông tin đó gắn liền với cá nhân họ, có thể ảnh hưởng đến quyền riêng tư, đời sống cá nhân của chủ thể dữ liệu. Đây là điều đáng lo ngại đối với môi trường mạng kỹ thuật ở Việt Nam hiện nay.

4.2. Kiến nghị hoàn thiện

Trên cơ sở phân tích các quy định về quyền riêng tư đối với dữ liệu và mô hình PMM, tác giả có một số kiến nghị hoàn thiện pháp luật như sau:

Một là, quyền riêng tư cá nhân được quy định tại Điều 38 Bộ luật Dân sự 2015 (BLDS) Quyền về đời sống riêng tư, bí mật cá nhân, bí mật gia đình. Trong đó, quy định giới hạn của quyền riêng tư về thông tin trong 2 trường hợp: (1) Có sự đồng ý của cá nhân trong việc công khai thông tin. Cá nhân là người sở hữu thông tin; đồng thời việc công khai hay bảo mật thông tin tác động trực tiếp đến cuộc sống của họ nên họ là các chủ thể được quyết định việc có thông tin công khai hay không; (2) Trường hợp luật có quy định về việc bắt buộc phải công khai thông tin cá nhân. Tuy nhiên, điều luật lại không quy định cụ thể việc đồng ý cho phép sử dụng những thông tin bằng hình thức nào. Do đó, để sử dụng hoặc phổ biến thông tin của

[34] https://plo.vn/phap-luat/mua-ban-du-lieu-ca-nhan-de-nhu-mua-rau-987783.html, ngày truy cập 10/6/2021.
[35] https://plo.vn/phap-luat/mua-ban-du-lieu-ca-nhan-de-nhu-mua-rau-987783.html, ngày truy cập 10/6/2021.

chủ thể cần phải có sự đồng ý rõ ràng với mục đích tương ứng và sự đồng ý phải là tự nguyện, thể hiện rõ ràng chủ ý được dự định cho việc tiếp cận thông tin và không được giả định, nghĩa là mục đích sử dụng phải cụ thể, xác định được phạm vi, đối tượng và tôn trọng các giá trị nhân thân của chủ thể thông tin. Do đó, để đảm bảo việc bảo vệ quyền riêng tư cá nhân trong thị trường dữ liệu thì việc bổ sung quy định này cần đặt ra. Như tác giả phân tích tại mô hình PMM, việc quy định cụ thể phương thức đồng ý và thay đổi sự đồng ý đối với các thông tin trong vòng đời dữ liệu là rất quan trọng, điều này giúp cho chủ thể dữ liệu chủ động trong việc xác định các giới hạn cho các bên liên quan trong việc tiếp cận dữ liệu của mình.

Hai là, quyền riêng tư của cá nhân trong thị trường dữ liệu liên quan rất nhiều lĩnh vực khác nhau đối với dữ liệu cá nhân, điều này dẫn đến bất cập là việc sử dụng dữ liệu không cần sự đồng ý của chủ thể dữ liệu, hay nói cách khác là những hạn chế khác đối với quyền riêng tư phải được dẫn chiếu trong các trường hợp luật có quy định khác chứ không phải như trường hợp pháp luật có quy định khác trong việc hạn chế quyền riêng tư của chủ thể dữ liệu. Do đó, việc xây dựng luật về dữ liệu cá nhân cần được nghiên cứu. Bởi lẽ, quy định chung về quyền riêng tư tại BLDS 2015 không đủ điều chỉnh các vấn đề phát sinh trong thị trường dữ liệu mới nổi hiện nay khi mà các luật chuyên ngành chưa điều chỉnh hoặc điều chỉnh chưa cụ thể thì phải áp dụng luật chung là BLDS 2015 để giải quyết.

Ba là, dự thảo lần 2 Nghị định quy định về bảo vệ dữ liệu cá nhân 2021[36] đang lấy kiến nhân dân có quy định biện pháp bảo vệ dữ liệu cá nhân tại Điều 17 Biện pháp kỹ thuật và Điều 18 Xây dựng quy định bảo vệ dữ liệu cá nhân nhưng hai quy định này vẫn chưa thể hiện trách nhiệm cụ thể của bên xử lý dữ liệu, chủ sở hữu dữ liệu trong việc thực hiện các chính sách để đảm bảo việc bảo vệ dữ liệu cá nhân, đặc biệt là quyền riêng tư về dữ liệu. Do đó, tác giả đề xuất cần bổ sung quy định điều khoản về quyền riêng tư về dữ liệu trong biện pháp bảo vệ dữ liệu cá nhân tại Chương 3 của dự thảo lần 2 Nghị định quy định về bảo vệ dữ liệu cá nhân 2021 bao gồm ba điều khoản riêng biệt về xây dựng tuyên bố chung, xây dựng mã (code) và bộ phận có chức năng bảo vệ dự liệu cá nhân.

Thứ nhất, các chủ thể liên quan trong thị trường dữ liệu phải xây dựng tuyên bố chung (Quy chế) trong hoạt động của mình

"Tuyên bố chung" đề cập đến các chuẩn mực nội bộ (đối với xã hội hoặc ngành) được thực thi bởi các thành viên khác của cộng đồng đó. Điều này bao gồm tất cả các cách tiếp cận để điều chỉnh quyền riêng tư thông qua các nghĩa vụ tự đặt ra thường không ràng buộc. Đôi khi ranh giới của những gì được coi là tự điều chỉnh rất mơ hồ, vì nó có thể được thực thi bởi Chính phủ và có thể có hình thức quy định hoặc thậm chí là quy định tổng hợp (nơi Chính phủ giám sát quá trình quản lý rủi ro)[37]. Việc yêu cầu các chủ thể liên quan trong thị trường

[36] https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Du-thao-Nghi-dinh-quy-dinh-ve-bao-ve-du-lieu-ca-nhan-465185.aspx, ngày truy cập 10/6/2021.
[37] R. Baldwin, M. Cave and M. Lodge, above n. 2, p. 147; A. Freiberg, above n. 2, pp.33-37.

dữ liệu phải xây dựng tuyên bố chung (quy chế) sẽ giúp thể hiện rõ việc triển khai và thực thi các quy định của pháp luật về dữ liệu, từ đó góp phần chỉ ra điểm mấu chốt về những gì doanh nghiệp có thể sẵn sàng cung cấp và những công cụ nào được họ coi là thích hợp nhất (có thể là tối ưu về chi phí) trong việc thực thi chính sách bảo vệ dữ liệu cá nhân, đặc biệt là quyền riêng tư về dữ liệu. Đó cũng là công cụ để các chủ thể liên quan trong thị trường dữ liệu thể hiện trách nhiệm của mình đối với xã hội.

Thứ hai, xây dựng Mã (Code)

Mã là một phương pháp tác động đến hành vi thông qua việc thiết kế các cấu trúc vật lý hoặc logic của các hệ thống công nghệ thông tin và giao tiếp, loại bỏ hoặc giới hạn các lựa chọn bằng cách cho phép hoặc vô hiệu hóa các hành động nhất định. Mã hoạt động theo cách xác định quyền và nghĩa vụ của các bên và do đó như một quy tắc tương đương với luật. Trong thị trường dữ liệu hiện nay, việc đảm bảo chính sách bảo vệ dữ liệu cá nhân cần áp dụng những phương pháp mang tính khoa học kỹ thuật chuyên ngành. Do đó, việc yêu cầu xây dưng mã (code) là một phần bắt buộc trong biện pháp bảo vệ dữ liệu cá nhân của các chủ thể liên quan, tác giả cho rằng điều này là phù hợp với xu thế chung khi mà các biện pháp khoa học kỹ thuật phải được ứng dụng để giải quyết các vấn đề cụ thể trong thị trường dữ liệu. Thông qua cơ chế này, giúp cho các chủ thể dữ liệu dễ dàng đưa ra quyết định hoặc hướng dẫn đối với dữ liệu của họ. Những gì được phép có thể nhìn thấy và truy cập được; những gì không được phép chỉ đơn giản là không xảy ra. Không có sự bất tuân theo quy định của "mã". Hơn nữa, "mã" có thể được thay đổi "nhanh chóng", như trong trường hợp thiết bị kết nối, các thiết bị được kết nối từ xa với nhà sản xuất hoặc nhà cung cấp của họ sẽ tự động cài đặt hoặc thay đổi mã[38]. Khi nó được thay đổi, trong nháy mắt mọi người được đưa ra một loạt các lựa chọn khác nhau, và những gì có trước đây không còn tồn tại nữa.

Thứ ba, bộ phận có chức năng bảo vệ dự liệu cá nhân

Đối với bộ phận có chức năng bảo vệ dự liệu cá nhân, tác giả cho rằng việc quy định điều luật riêng biệt sẽ là căn cứ cụ thể để các chủ thể liên quan triển khai thực hiện thống nhất và hiệu quả. Từ mô hình quản lý quyền riêng tư (PMM) mà tác giả đã phân tích, việc xây dựng dựng mô hình quản lý quyền riêng tư sẽ giúp các doanh nghiệp chủ động trong hoạt động quản lý, kỹ thuật, vật lý ở từng cấp độ đối với dữ liệu. Trên cơ sở đó, một bộ phận kỹ thuật chuyên trách chịu trách nhiệm chính trong việc triển khai các hoạt động liên quan đến dữ liệu. Điều này sẽ đảm bảo việc chủ thể dữ liệu, cơ quan quản lý nhà nước dễ dàng trao đổi, giải quyết khi có yêu cầu, cũng như quy kết trách nhiệm cụ thể cho từng cá nhân dễ dàng.

5. Kết luận

Để hình thành và duy trì một cộng đồng nào đó dù nhỏ nhất cũng phải xây dựng được những nguyên tắc nhất định. Điều đó quan trọng hơn cả tìm kiếm một thủ lĩnh. Thủ lĩnh có

[38] J. Zittrain (2008), *Perfect Enforcement On Tomorrow's Internet*, R. Brownsword and K. Yeung (eds)", p. 125-56, p.132.

thể bị đốn hạ bởi nhiều hình thức khác nhau nhưng nguyên tắc thì không phụ thuộc một cá nhân nào. Tính cấp thiết của việc xây dựng một cơ chế quản lý kiểm soát dữ liệu trong thị trường dữ liệu là có. Do đó, cần có sự nghiên cứu đầu tư các nguyên tắc về mô hình quản lý để góp phần nâng cao nếp sống văn minh, bảo vệ quyền lợi tốt hơn cho từng cá nhân trong thị trường dữ liệu hiện nay.

DANH MỤC TÀI LIỆU THAM KHẢO

1. Thái Thị Tuyết Dung (2012), *Quyền riêng tư trong thời đại công nghệ thông tin*, Tạp chí Nghiên cứu Lập pháp, số 9 (217).

2. Nguyễn Ngọc Điện (2018), *Quyền được tiếp cận thông tin và quyền bất khả xâm phạm về cuộc sống riêng tư*, Tạp chí Nghiên cứu lập pháp, số 15 (367).

3. Lê Thị Giang (2018), *Quyền riêng tư đối với thông tin cá nhân*, Tạp chí Kiểm sát, số 17.

4. Lê Thị Thúy Nga (2020), *Bảo vệ quyền đối với đời sống riêng tư, bí mật cá nhân, bí mật gia đình trong bối cảnh Cách mạng công nghiệp 4.0*, Tạp chí Dân chủ và Pháp luật, số 3.

5. Phùng Trung Tập (2019), *Cơ sở pháp lý bảo đảm quyền về đời sống tiêng tư, bí mật cá nhân, bí mật gia đình*, Tạp chí Dân chủ và Pháp luật, số 7.

6. Thái Vĩnh Thắng (2017), *Bảo vệ quyền riêng tư ở Hoa Kỳ, Pháp và những kinh nghiệm cho Việt Nam*, Tạp chí Luật học số 8.

7. Vương Thanh Thúy (2017), *Về quyền riêng tư của cá nhân trong pháp luật hiện nay*, Tạp chí Quản lý nhà nước, số 263.

8. A.F. Westin (2003), *Social and Political Dimensions of Privacy*, 59 Journal of Social Issues 431.

9. A.I. Ogus, *Regulation: Legal Form and Economic Theory*, Hart Publishing, Oxford 2004.

10. M. Betkier *(*2016*), Individual Privacy Management 21*, *Media and Arts Law Review* 315.

11. B. Morgan and K. Yeung, *An Introduction to Law and Regulation*, Cambridge University Press, Cambridge 2007.

12. *Boilerplate: The Foundation of Market Contracts*, Cambridge University Press, New York 2007.

13. C.J. Bennett and C.D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, 2nd ed., MIT Press, Cambridge, MA 2006.

14. Cf. O. Tene and J. Polonetsky (2013), *Privacy and Big Data: Making Ends Meet*, 66 Stanford Law Review Online 25.

15. D. Boyd, *Networked Privacy* (2012) 10 *Surveillance & Society* 348.

16. D. Searls, *The Intention Economy: When Customers Take Charge*, Harvard Business Review Press, Boston, MA 2012.

17. D.J. Solove, *Understanding Privacy*, Harvard University Press, Cambridge, MA 2008.

18. E. Mik, *The Erosion of Autonomy in Online Consumer Transactions* (2016) 8 *Law, Innovation and Technology* 1.

19. F.H. Cate and V. Mayer-Schönberger, *Notice and Consent in a World of Big Data* (2013) 3 *International Data Privacy Law* 67.

20. E. Mik, *The Erosion of Autonomy in Online Consumer Transactions (2016)* 8 *Law, Innovation and Technology* 1.

21. G. Laurie, *Genetic Privacy: A Challenge to Medico-legal Norms*, Cambridge University Press, Cambridge 2002.

22. H.T. Gomez-Arostegui (2005), *Defining Private Life under the European Convention on Human Rights by Referring to Reasonable Expectations*' 35 California Western International Law Journal 153.

23. J. Braithwaite, 'Types of Responsiveness' in P. Drahi's (ed), *Regulatory Theory: Foundations and Applications*, ANU Press, Acton 2017.

24. J.W. DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Cornell University Press, Ithaca 1997.

25. J.M. Urban and C.J. Hoofnagle, 'The Privacy Pragmatic as Privacy Vulnerable' (2014) *SSRN*, http://papers.ssrn.com/abstract=2514381.

26. M. von Grafenstein, *The Principle of Purpose Limitation in Data Protection Laws: The Risk-Based Approach, Principles, and Private Standards as Elements for Regulating Innovation*, Nomos, Baden-Baden 2018.

27. N.A. Moreham, 'The Nature of Privacy Interest' in N.A. Moreham and M. Warby (eds), *The Law of Privacy and the Media*, Oxford University Press, Oxford 2016, p.42, pp.49-51.

28. https://plo.vn/phap-luat/mua-ban-du-lieu-ca-nhan-de-nhu-mua-rau-987783.html, ngày truy cập 10/6/2021.

29. https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Du-thao-Nghi-dinh-quy-dinh-ve-bao-ve-du-lieu-ca-nhan-465185.aspx, ngày truy cập 10/6/2021.