

PHÁP LUẬT VỀ ĐIỆN TOÁN Đám Mây TRONG THƯƠNG MẠI ĐIỆN TỬ Ở MỘT SỐ QUỐC GIA VÀ VIỆT NAM

Nguyễn Mai Linh*

Ngô Thị Hương Giang**

Nguyễn Quý Cảnh**

Nguyễn Phương Anh**

* Giảng viên Trường Đại học Luật Hà Nội

** Sinh viên Khóa 42 Trường Đại học Luật Hà Nội.

Thông tin bài viết:

Từ khóa: Điện toán đám mây, thương mại điện tử, Luật An ninh mạng năm 2018.

Lịch sử bài viết:

Nhận bài : 01/12/2020

Biên tập : 18/12/2020

Duyệt bài : 21/12/2020

Article Information:

Keywords: Cloud computing, electronic commerce, Law on Cybersecurity of 2018.

Article History:

Received : 01 Dec. 2020

Edited : 18 Dec. 2020

Approved : 21 Dec. 2020

Tóm tắt:

Cùng với sự phát triển của Internet, điện toán đám mây (cloud computing) ngày càng khẳng định vị trí của mình trong việc cung cấp cho người dùng một không gian mạng để lưu trữ dữ liệu cá nhân. Bên cạnh những lợi ích mà điện toán đám mây mang lại, còn tồn tại nhiều vấn đề pháp lý bất cập liên quan đến việc đảm bảo an toàn dữ liệu cá nhân cũng như thẩm quyền của các cơ quan nhà nước trong việc can thiệp, truy cập, kiểm soát các hoạt động liên quan đến dữ liệu. Trong phạm vi bài viết này, các tác giả phân tích các quy định của pháp luật điều chỉnh điện toán đám mây trong thương mại điện tử ở một số quốc gia như Hoa Kỳ, Trung Quốc và đưa ra một số gợi mở đối với Việt Nam.

Abstract:

With the development of the internet, cloud computing plays an important role in offering a massive pool as cyber space of resources and services for cloud users to utilize for storing and processing their data. Cloud computing brings many benefits, however, some legal issues which are insufficient such as the security of personal data and the rights of authorities in intervening, accessing and controlling activities related to data users. This article provides analysis of the provisions governing on cloud computing in electronic commerce in some countries such as the United States, China and also provides related recommendations for Viet Nam.

Điện toán đám mây (ĐTĐM) là mô hình dịch vụ cho phép người dùng truy cập tài nguyên điện toán dùng chung (mạng, server, lưu trữ, ứng dụng, dịch vụ) thông qua kết nối mạng một cách dễ dàng, mọi lúc mọi nơi, theo yêu cầu¹. Tài nguyên ĐTĐM có thể được thiết lập hoặc hủy bỏ nhanh chóng bởi người dùng mà không cần sự can thiệp của nhà cung cấp dịch vụ². Ở mô hình ĐTĐM,

mọi khả năng liên quan đến công nghệ thông tin (CNTT) đều được cung cấp dưới dạng các “dịch vụ”, cho phép người sử dụng truy cập các dịch vụ công nghệ từ một nhà cung cấp nào đó “trong đám mây” mà không cần phải có các kiến thức, kinh nghiệm về công nghệ đó, cũng như không cần quan tâm đến các cơ sở hạ tầng phục vụ công nghệ đó³. Nói tóm lại, ĐTĐM là một mô hình cung cấp tài

¹ Jansen.W. Grance.T, “Guidelines on security and privacy in public cloud computing”, NIST Special Publication 800-144, December 2011, <http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf>, truy cập ngày 15/11/2020.

² Johndavid Kerr, “Cloud computing: legal and privacy issues”, 2010, https://www.g-casa.com/conferences/vietnam/paper/JDK_CLOUDING_9_21_10_Paper-1%5B11%5D.pdf, truy cập ngày 15/11/2020.

³ <https://www.nist.gov/>, truy cập ngày 16/11/2020.

nguyên máy tính cho người dùng thông qua Internet.

1. Quy định của pháp luật về điện toán đám mây trong thương mại điện tử tại một số quốc gia

1.1. Hoa Kỳ

Hoa Kỳ là quốc gia tiên phong ứng dụng điện toán đám mây (ĐTĐM) trong thương mại điện tử (TMĐT) nói riêng cũng như trong công cuộc xây dựng chính phủ điện tử nói chung. Hoa Kỳ đã rất thành công trong nỗ lực ứng dụng ĐTĐM cho chính quyền liên bang. Pháp luật Hoa Kỳ tập trung quy định về quyền riêng tư và bảo mật dữ liệu, chia làm bốn mảng chính và có hơn 15 văn bản pháp luật điều chỉnh vấn đề này:

Thứ nhất, tiết lộ thông tin bắt buộc cho chính phủ

Cơ sở dữ liệu trên ĐTĐM có thể chịu các mức độ bảo vệ khác nhau tùy vào dạng thông tin mà nó lưu trữ. Tuy nhiên, theo Luật Đám mây của Hoa Kỳ (The Clarifying Lawful Overseas Use of Data Act - CLOUD Act) 2018⁴, Chính phủ Hoa Kỳ có thể tiếp cận với các thông tin này. Theo đó, các cơ quan tình báo Hoa Kỳ có quyền truy cập vào dữ liệu được lưu trữ bởi các công ty Hoa Kỳ trong một số trường hợp nhất định dù nơi đặt

máy chủ chứa dữ liệu ở đâu. Quy định này đã đẩy lên mối lo ngại của EU khi Hoa Kỳ ngày càng giành quyền kiểm soát tất cả các thiết bị trong TMĐT⁵. Ngoài ra, các vấn đề liên quan đến tiết lộ thông tin bắt buộc cho Chính phủ còn được quy định cụ thể theo từng lĩnh vực khác nhau như: Luật về quyền riêng tư của truyền thông điện tử (The Electronic Communications Privacy Act - ECPA)⁶, Luật Truyền thông được lưu trữ (The Stored Communications Act - SCA)⁷, Luật Yêu nước⁸, Nguyên tắc Thực hành thông tin công bằng (fair information practice principles – FIPPs) của Ủy ban Thương mại liên bang Hoa Kỳ (Federal Trade Commission - FTC)⁹.

Thứ hai, bảo mật dữ liệu và thông báo vi phạm

Vấn đề bảo mật dữ liệu và thông báo vi phạm gồm các nội dung: “Làm thế nào để nhà cung cấp dịch vụ đám mây bảo vệ dữ liệu của khách hàng?”; “Làm thế nào để khách hàng có thể bảo mật được dữ liệu khi lưu trữ thông tin trên nền tảng ĐTĐM?” và “Làm thế nào để bảo vệ quyền đưa ra khiếu nại của khách hàng khi quyền bảo mật đám mây của họ bị xâm phạm?”¹⁰.

Ba vấn đề này đều được điều chỉnh bởi Luật Tăng cường an ninh mạng và Bảo vệ

⁴ H.R.4943 - CLOUD Act, 115th Congress (2017-2018), <https://www.congress.gov/bill/115th-congress/house-bill/4943/text>, truy cập ngày 12/11/2020.

⁵ <https://bnews.vn/sieu-quyen-luc-ve-dien-toan-dam-may-cua-my-khien-eu-lo-lang/165378.html>. Lý giải cho sự việc trên là bởi: Các thể nhân lớn ở EU như Deutsche Bank, Lufthansa, Orange, Renault, Volkswagen hay cả Bộ Y tế Pháp đều sử dụng các nền tảng cung cấp điện toán đám mây đến từ Hoa Kỳ như Google Cloud, Amazon Web Services, hay Microsoft.

⁶ Đạo luật này đưa ra các biện pháp bảo vệ người tiêu dùng chống lại quyền truy cập của Chính phủ vào thư điện tử và các dữ liệu điện toán khác do các bên (Ví dụ: Nhà cung cấp dịch vụ Internet) nắm giữ.

⁷ Đạo luật này đề cập đến việc tiết lộ thông tin tự nguyện và bắt buộc liên quan đến hồ sơ giao dịch và truyền thông điện tử được lưu trữ do các nhà cung cấp dịch vụ internet hoặc bên thứ ba nắm giữ; <https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121>.

⁸ Đạo luật được ban hành vào năm 2001 và được sửa đổi vào năm 2005 bao gồm các điều khoản cho phép FBI truy cập vào hồ sơ kinh doanh bằng cách buộc các nhà cung cấp đám mây cung cấp hồ sơ.

⁹ Các nguyên tắc này đề cập đến việc thu thập, sử dụng thông tin cá nhân, chất lượng dữ liệu, bảo mật, tính minh bạch,... làm cơ sở cho nhiều khuyến nghị về quyền riêng tư mà các cơ quan liên bang đưa ra.

¹⁰ Gopi Tatapudi, *Cloud Computing And Privacy Regulations: An Exploratory Study On Issues And Implications*, https://www.researchgate.net/publication/266870158_Cloud_Computing_And_Privacy_Regulations_An_Exploratory_Study_On_Issues_And_Implications.

dữ liệu người tiêu dùng năm 2006. Theo đó, Luật quy định: (1) Cấm truy cập hoặc điều khiển từ xa một máy tính được bảo vệ mà không được phép lấy thông tin; (2) Mở rộng phạm vi “máy tính được bảo vệ”, gồm cả các máy tính liên quan đến các vấn đề về TMĐT hoặc liên lạc giữa các tiểu bang cũng như là nước ngoài; (3) Mở rộng định nghĩa về “lừa đảo”, bao gồm lừa đảo trên môi trường máy tính; (4) Xác định tội tống tiền, đe dọa quyền truy cập mà không được phép (hoặc vượt quá quyền truy cập được phép của) dữ liệu lưu trữ; (5) Áp dụng hình phạt hình sự đối với âm mưu lừa đảo trên môi trường máy tính; (6) Phạt tiền hoặc phạt tù nếu không thông báo cho cơ quan mật vụ Hoa Kỳ hoặc Cục Điều tra liên bang (FBI) về một vi phạm an ninh lớn trong hệ thống máy tính, với mục đích cản trở cuộc điều tra về vi phạm đó, nếu vi phạm đó gây ra nguy cơ đánh cắp thông tin đáng kể¹¹.

Ngoài ra, còn có các văn bản pháp luật điều chỉnh từng lĩnh vực cụ thể như: Luật Quyền riêng tư và Quyền giáo dục gia đình (The Family Education Rights and Privacy Act - FERPA); Luật Gramm-Leach Bliley (The Gramm Leach Bliley Act - GLBA); Luật Trách nhiệm giải trình và Cung cấp bảo hiểm y tế (The Health Insurance Portability and Accountability Act - HIPAA)¹².

Thứ ba, khả năng truy cập, truyền và lưu trữ dữ liệu

Khi sử dụng dịch vụ ĐTĐM, các dữ liệu mà khách hàng đăng tải lên không đơn thuần như việc vận chuyển các đối tượng thông thường mà việc truy cập, truyền tải hay lưu

trữ dữ liệu của họ trên môi trường không gian mạng phải tuân thủ theo những quy định cụ thể của chính quyền Hoa Kỳ. Liên quan đến vấn đề này, Hoa Kỳ đã ban hành các văn bản như: Luật Tự do thông tin (FOIA); Dữ liệu ngành thẻ thanh toán; Tiêu chuẩn bảo mật (PCIDSS); Quy tắc thực hành thông tin công bằng của FTC¹³. Theo đó, trong quan hệ giữa nhà cung ứng và người sử dụng dịch vụ ĐTĐM, cần phải làm rõ quyền của các công ty và người tiêu dùng trong việc truy cập vào dữ liệu trên nền tảng ĐTĐM, cũng như các quyền liên quan đến xử lý dữ liệu trên nền tảng ĐTĐM bởi nhà cung cấp dịch vụ. Ví dụ, Quy tắc thực hành thông tin công bằng của FTC quy định nhà cung cấp dịch vụ ĐTĐM sẽ phải tuân theo các chế tài FTC khi lưu trữ thông tin người tiêu dùng trên đám mây nếu họ không làm đúng như công bố của mình với người tiêu dùng về vị trí và cách thức lưu trữ và bảo mật thông tin.

Thứ tư, quyền tài phán liên quan đến địa điểm lưu trữ dữ liệu

Các quy định chủ yếu liên quan đến việc xác định quyền tài phán liên quan tới các văn bản pháp luật như: Tiêu chuẩn bảo mật thẻ thanh toán (PCIDSS), Luật Sarbanes-Oxley; Quy định của NARA (Mục 36 của Bộ luật quy định liên bang) và Thực hành thông tin công bằng của FTC¹⁴. Theo đó, những quy định trong các văn bản pháp luật này sẽ xác định các tranh chấp thương mại điện tử được giải quyết theo pháp luật tiểu bang nơi đặt cơ sở máy chủ, nơi nhà cung cấp dịch vụ ĐTĐM đặt trụ sở hay nơi cư trú của khách hàng sử dụng dịch vụ đó.

¹¹ <https://www.congress.gov/bill/109th-congress/house-bill/5318/summary/00>, truy cập ngày 12/11/2020.

¹² HoganLovells, *Cloud Computing: A Primer on Legal Issues, Including Privacy and Data Security*., 2010, http://www.cisco.com/web/about/doing_business/legal/privacy_compliance/docs/CloudPrimer.pdf, truy cập ngày 12/11/2020.

¹³ Jansen.W. Grance.T, *Guidelines on security and privacy in public cloud computing*, NIST Special Publication 800-144, December 2011, <http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf>, truy cập ngày 15/11/2020.

¹⁴ Jansen.W. Grance.T, “*Guidelines on security and privacy in public cloud computing*”, NIST Special Publication 800-144, December 2011, <http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf>, truy cập ngày 15/11/2020.

1.2. Trung Quốc

Thực tế phát triển của TMĐT nói chung và ĐTĐM nói riêng đòi hỏi Chính phủ Trung Quốc có những chính sách phù hợp với sự phát triển của khoa học công nghệ, đồng thời tạo ra một môi trường pháp lý công bằng cho sự phát triển đó. Cho đến nay, Trung Quốc vẫn chưa có khung pháp lý đồng bộ điều chỉnh các vấn đề pháp lý liên quan đến ĐTĐM.

Thứ nhất, nghĩa vụ thông báo thông tin người dùng cho Chính phủ

Ở Trung Quốc, các quyền đối với dữ liệu cá nhân được coi là quyền con người, nghĩa là quyền của một cá nhân đối với dữ liệu cá nhân của họ sẽ không bị can thiệp bởi cơ quan có thẩm quyền của Chính phủ Trung Quốc - có tư cách là cơ quan kiểm soát dữ liệu lớn nhất, thu thập, xử lý, lưu và sử dụng thông tin cá nhân¹⁵. Mặc dù Hiến pháp Trung Quốc hạn chế quyền tiếp cận đối với dữ liệu người dùng, nhưng một số quy định của pháp luật đã vượt ra ngoài giới hạn này. Ví dụ, Điều 25 Luật Thương mại điện tử năm 2019¹⁶ cho phép Chính phủ yêu cầu các nhà khai thác TMĐT cung cấp dữ liệu thương mại điện tử, bao gồm thông tin cá nhân, quyền riêng tư và bí mật kinh doanh và các nhà khai thác TMĐT không thể từ chối yêu cầu cung cấp thông tin của Chính phủ¹⁷. Trên thực tế, Chính phủ Trung Quốc vẫn là cơ quan kiểm soát tối cao vì họ kiểm soát các kết

nối Internet giữa lãnh thổ của mình và thế giới bên ngoài¹⁸, bằng việc sử dụng một phần mềm riêng Wechat¹⁹.

Thứ hai, bảo vệ thông tin người dùng

Các yêu cầu về bảo vệ thông tin người dùng được quy định tại Luật An ninh mạng Trung Quốc (2017)²⁰; theo đó, các nhà cung cấp sản phẩm và dịch vụ mạng thu thập thông tin người dùng có nghĩa vụ thông báo cho người dùng và phải nhận được sự đồng ý của họ. Theo quy định của Luật, thông tin cá nhân và các dữ liệu quan trọng được các nhà khai thác thông tin thu thập phải được lưu trữ trong nước; nghĩa là, các công ty nước ngoài muốn khai thác thông tin phải lắp đặt máy chủ tại Trung Quốc. Tuy nhiên, Luật cũng quy định một trường hợp ngoại lệ là thông tin có thể được cung cấp nếu sau khi xử lý không có cách nào để xác định danh tính một cá nhân cụ thể (nghĩa là không thể nhận được “sự đồng ý” từ phía người dùng)²¹.

Bên cạnh đó, người dùng có quyền yêu cầu đặt câu hỏi để xem xét tính đúng đắn về hành vi cũng như yêu cầu bên cung ứng dịch vụ xóa thông tin của mình trong trường hợp thông tin không chính xác hoặc được sử dụng cho mục đích không được thỏa thuận. Ngoài ra, trộm cắp và việc bán bất hợp pháp dữ liệu cá nhân đã được hình sự hóa ở Trung Quốc²². Những hình phạt vi phạm này khắc nghiệt

¹⁵ Zhang Xinbao, *From Privacy to Personal Information: The Theory and System to Re-balance Interest*, 3 *Zhongguo Faxue (China Legal Sci.)* 38, 39 (2015).

¹⁶ Luật Thương mại điện tử Trung Quốc năm 2019, <https://npcobserver.com/legislation/e-commerce-law/>.

¹⁷ Điều 25, Luật Thương mại điện tử Trung Quốc năm 2019, <https://npcobserver.com/legislation/e-commerce-law/>.

¹⁸ Samuel Woodhams, *The Rise of Internet Sovereignty and the End of the World Wide Web?*, *Globe Post* (Apr. 23, 2019), <https://theglobepost.com/2019/04/23/internet-sovereignty/>, truy cập ngày 12/11/2020.

¹⁹ WeChat Shares Consumer Data With Chinese Government, *PYMNTS* (September 25, 2017), <https://www.pymnts.com/safety-and-security/2017/wechat-hands-over-user-data-to-chinese-government-amid-privacy-concerns/>.

²⁰ Luật An ninh mạng Trung Quốc năm 2017, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/>.

²¹ Điều 42, Luật An ninh mạng Trung Quốc năm 2017, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/>.

²² Samuel Yang, *The New China Cybersecurity Law Why Companies Should Care But Not Panic?*, *Anjie Law Firm* (Nov. 14, 2016), <http://en.anjielaw.com/downloadRepository/28473463-0ae9-4768-8e77-2051e73d3434.pdf>, truy cập ngày 12/11/2020.

hơn nhiều so với những hình phạt trước đây như cảnh cáo, ra lệnh sửa chữa, phạt tiền lên đến 1 triệu NDT, thậm chí là giam giữ đối với cá nhân có hành vi vi phạm²³.

Thứ ba, bảo vệ quyền sở hữu trí tuệ

Theo quy định của Luật Thương mại điện tử năm 2019, nếu chủ sở hữu của quyền sở hữu trí tuệ (SHTT) cho rằng nhà điều hành trên nền tảng (an operator on platform) đã vi phạm quyền SHTT của mình có thể thông báo cho nhà điều hành nền tảng đó (platform operator) và yêu cầu chủ thể thực hiện các biện pháp sơ bộ cần thiết (preliminary measures), chẳng hạn như xóa hoặc sàng lọc thông tin về vi phạm bị cáo buộc, ngắt kết nối các trang web liên quan hoặc chấm dứt giao dịch hoặc dịch vụ. Nếu nhà điều hành nền tảng không kịp thời thực hiện các biện pháp sơ bộ cần thiết khi nhận được thông báo, thì nhà điều hành trên nền tảng đó phải chịu trách nhiệm về các thiệt hại bổ sung và có thể bị phạt tiền từ 50.000 NDT đến 2 triệu NDT²⁴.

Tuy nhiên, trên thực tiễn, việc áp dụng những quy định này còn gặp nhiều hạn chế, chẳng hạn như dữ liệu người dùng có thể được coi là quyền tác giả trong bối cảnh bảo hộ quyền SHTT hay không, phải đáp ứng được những điều kiện nào để được coi là tác phẩm gốc, nhãn hiệu hoặc bằng sáng chế. Trong vụ tranh chấp *Shanghai Hantao Information Consultation Co. vs. Aibang Juxin (Beijing) Technology Co*²⁵, Tòa án nhân dân Bắc Kinh cho rằng nếu một nhận xét của người dùng cung cấp thể hiện suy nghĩ, tính cách ban đầu của họ, cảm xúc và trải nghiệm, nhận xét này sẽ được coi là một tác phẩm theo Luật Bản quyền của Trung Quốc. Tuy nhiên, trong

trường hợp này, nguyên đơn đã không chứng minh được rằng mọi nhận xét trên nền tảng của mình đều đáp ứng yêu cầu về tính độc đáo và sáng tạo để được coi là tác phẩm theo Luật Bản quyền của Trung Quốc. Như vậy, rất khó để có thể chứng minh cho việc bảo hộ quyền tác giả trừ khi có đủ sự sáng tạo trong việc phát triển cơ sở dữ liệu thông tin thực tế²⁶.

Nhìn chung, pháp luật về ĐTĐM của Trung Quốc và Hoa Kỳ có những điểm chung sau đây:

Một là, Chính phủ vẫn luôn là chủ thể nắm quyền kiểm soát đối với thông tin người dùng; *hai là*, chủ thể có hành vi xâm phạm đến dữ liệu người dùng không chỉ phải chịu xử lý vi phạm hành chính mà còn có thể chịu trách nhiệm hình sự; *ba là*, việc áp dụng quy định về quyền SHTT vẫn gặp nhiều khó khăn trong thực tế.

2. Pháp luật về điện toán đám mây trong thương mại điện tử ở Việt Nam

Ở Việt Nam, thuật ngữ “điện toán đám mây” ra đời giữa năm 2007 cũng không phải để nói về một phong trào mới, mà để tổng hợp lại các hướng đi của cơ sở hạ tầng thông tin vốn đã và đang diễn ra từ mấy năm qua. ĐTĐM là một giải pháp toàn diện cung cấp CNTT như một dịch vụ. Nó là một giải pháp điện toán thông qua Internet cung cấp tài nguyên chia sẻ tại máy chủ cho người sử dụng. Các máy tính trong các đám mây được cấu hình để làm việc cùng nhau và các ứng dụng khác nhau sử dụng sức mạnh điện toán tập hợp như chúng đang chạy trên một hệ thống duy nhất. Thuật ngữ “điện toán đám mây”

²³ Đoạn 3, Điều 64, Luật An ninh mạng Trung Quốc, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/>.

²⁴ Điều 42, Điều 45, Điều 84 Luật Thương mại điện tử Trung Quốc năm 2019, <https://npcobserver.com/legislation/e-commerce-law/>.

²⁵ *Shanghai Hantao Information Consultation Co. v. Aibang Juxin (Beijing) Technology Co.*, 2010, Hai Min Chu Zi no. 4253 (Beijing Haidian People’s Ct. 2010), China.

²⁶ *Feist Publ’ns, Inc. v. Rural Telephone Serv. Co.*, 499 U.S. 340, 363 (1991), Tòa cho rằng, để một cá nhân có thể được bảo hộ quyền tác giả đối với dữ liệu cá nhân của mình khi và chỉ khi đáp ứng đủ điều kiện về tính sáng tạo trong việc phát triển cơ sở dữ liệu đó trên nền tảng thực tế.

được định nghĩa tại điểm d khoản 5 Điều 2 Luật An ninh mạng Việt Nam 2018²⁷. Theo đó, ĐTĐM được xem là một trong các cơ sở hạ tầng CNTT không gian mạng quốc gia, là nền tảng cung cấp hệ thống cơ sở vật chất, kỹ thuật để tạo lập, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên không gian mạng. Về cơ bản, cách tiếp cận về ĐTĐM của Việt Nam giống với những quan điểm của các nhà nghiên cứu đã đưa ra trước đó, là mô hình dịch vụ cung cấp cho người dùng một khoảng không gian rộng lớn cho phép họ có thể lưu trữ, truyền tải thông tin cá nhân. Pháp luật Việt Nam không đưa ra một khái niệm mới về ĐTĐM. Đây có thể được coi là một sự tiếp thu kinh nghiệm từ các quốc gia trên thế giới - đặc biệt là Hoa Kỳ - nơi khởi nguồn phát triển của ĐTĐM.

Các vấn đề pháp lý về ĐTĐM trong TMĐT được điều chỉnh bởi một số văn bản pháp luật như: Luật An ninh mạng, Luật Giao dịch điện tử, Luật An toàn thông tin mạng, Luật Công nghệ thông tin, Luật Bảo vệ quyền lợi Người tiêu dùng... và các văn bản hướng dẫn thi hành, cụ thể như sau:

Thứ nhất, bảo mật thông tin cá nhân

Trong bối cảnh TMĐT nói chung và ĐTĐM nói riêng được dự đoán sẽ bùng nổ trong thời gian tới, việc bảo mật thông tin cá nhân của người sử dụng là một vấn đề cần được quan tâm. Hiến pháp năm 2013 đã hiến định quyền bảo vệ thông tin bí mật cá nhân²⁸. Sau đó, quyền này được cụ thể

hóa trong các văn bản pháp luật chuyên ngành như: Bộ Luật Dân sự 2015²⁹; Luật An toàn thông tin mạng năm 2015 đưa các nguyên tắc bảo vệ quyền về sự riêng tư dữ liệu, quy định về thu thập, sử dụng, sửa đổi, xóa thông tin cá nhân cùng với trách nhiệm của Chính phủ trong việc bảo vệ dữ liệu riêng tư, yêu cầu sự đồng ý của chủ sở hữu trước khi xử lý thông tin cá nhân (bao gồm thu thập, chỉnh sửa, sử dụng, lưu trữ, cung cấp, chia sẻ hoặc lan truyền), đồng thời quy định tổ chức, cá nhân xử lý thông tin cá nhân có trách nhiệm bảo mật thông tin và phải công bố chính sách sử dụng và bảo vệ thông tin được xử lý³⁰; Luật An ninh mạng năm 2018 yêu cầu các doanh nghiệp cung cấp dịch vụ trên không gian mạng tại Việt Nam phải thông báo trực tiếp cho người dùng nêu dữ liệu của họ bị vi phạm, bị hư hỏng hoặc bị mất³¹.... Bên cạnh đó, pháp luật Việt Nam cũng quy định cụ thể về chế tài để xử lý những hành vi xâm phạm đến dữ liệu cá nhân, ví dụ, Bộ luật Hình sự năm 2015³² sự quy định về “*Tội đưa hoặc sử dụng trái phép thông tin trên mạng máy tính, viễn thông*”.

Thứ hai, bảo vệ quyền sở hữu trí tuệ

Việt Nam đã ban hành rất nhiều văn bản luật, nghị định, thông tư điều chỉnh về vấn đề bảo vệ quyền SHTT như Luật SHTT năm 2009, Nghị định số 99/2013/NĐ-CP quy định xử lý vi phạm xâm phạm quyền trên Internet³³, Nghị định số 28/2017/NĐ-CP sửa đổi, bổ sung một số điều của Nghị định

²⁷ Khoản 5 Điều 2 Luật An ninh mạng năm 2018.

²⁸ Điều 21 Hiến Pháp năm 2013 quy định: “1. Mọi người có quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân và bí mật gia đình; có quyền bảo vệ danh dự, uy tín của mình. Thông tin về đời sống riêng tư, bí mật cá nhân, bí mật gia đình được pháp luật bảo đảm an toàn. 2. Mọi người có quyền bí mật thư tín, điện thoại, điện tín và các hình thức trao đổi thông tin riêng tư khác. Không ai được bóc mở, kiểm soát, thu giữ trái luật thư tín, điện thoại, điện tín và các hình thức trao đổi thông tin riêng tư của người khác”.

²⁹ Khoản 1 Điều 38 Bộ luật Dân sự năm 2015: “1. Đời sống riêng tư, bí mật cá nhân, bí mật gia đình là bất khả xâm phạm và được pháp luật bảo vệ”.

³⁰ Điều 8 Luật An toàn thông tin mạng năm 2015.

³¹ Điều 41 Luật An ninh mạng năm 2018.

³² Điều 159, Điều 288 Bộ luật Hình sự năm 2015.

³³ Điều 10 Nghị định số 99/2013/NĐ-CP quy định xử phạt vi phạm hành chính trong lĩnh vực sở hữu công nghiệp.

số 131/2013/NĐ-CP quy định về xử phạt vi phạm hành chính về quyền tác giả và quyền liên quan,... Đặc biệt, Luật SHTT năm 2009 đã được sửa đổi, bổ sung một số điều năm 2019³⁴ cùng với các văn bản khác có liên quan đã chú trọng hơn đến vấn đề SHTT trong môi trường TMĐT.

Ngoài các quy định của pháp luật, ở Việt Nam, bảo hộ quyền SHTT còn được điều chỉnh bởi các điều ước quốc tế đa phương, song phương mà Việt Nam là thành viên trong lĩnh vực này như: Hiệp định TRIPS, Hiệp định giữa Việt Nam và Hoa Kỳ về thiết lập quan hệ quyền tác giả năm 1997; Hiệp định giữa Việt Nam và Thụy Sĩ về bảo hộ quyền sở hữu trí tuệ và hợp tác trong lĩnh vực sở hữu trí tuệ năm 1999...

Pháp luật dù có quy định cụ thể đến đâu nhưng trên thực tế, khi áp dụng vẫn còn tồn tại nhiều điểm hạn chế và pháp luật về ĐTĐM trong TMĐT của Việt Nam cũng vậy. Nhằm tiếp tục hoàn thiện pháp luật về ĐTĐM trong TMĐT của Việt Nam, trên cơ sở kinh nghiệm của Hoa Kỳ và Trung Quốc, chúng tôi đề xuất một số giải pháp sau đây:

Một là, về bảo mật thông tin cá nhân

Thực tế, trong thời gian qua, việc tự bảo vệ thông tin cá nhân của mình còn rất hạn chế. Những vụ việc các công ty, người sử dụng Việt Nam bị các hacker tấn công gây tổn thất về kinh tế và tinh thần nghiêm trọng diễn ra khá phổ biến. Chính vì vậy, trong thời gian tới, công tác tuyên truyền, nâng cao ý thức bảo vệ thông tin cá nhân, bí mật cá nhân cần được đẩy mạnh, trang bị kiến thức và giúp họ chủ động bảo vệ thông tin của mình. Đồng thời, các cơ quan có thẩm quyền cần có biện pháp chủ động bảo vệ thông tin bí mật cá nhân trong kỷ nguyên công nghệ số.

Hai là, về quyền sở hữu trí tuệ

Để thực thi quyền SHTT một cách hiệu quả, pháp luật SHTT Việt Nam cần có các

quy định về quyền tác giả, quyền liên quan trong môi trường Internet; bổ sung quy định nhằm minh bạch hóa thông tin trên các website TMĐT, tăng cường trách nhiệm đối tượng tham gia giao dịch TMĐT. Bên cạnh các giải pháp pháp lý và công nghệ, cần tiếp tục nâng cao năng lực cho các cơ quan thực thi và tuyên truyền rộng rãi đến người sử dụng các quy định của pháp luật SHTT để nâng cao ý thức bảo vệ quyền từ phía người sử dụng. Các chủ thể có quyền cần áp dụng các biện pháp công nghệ để bảo vệ quyền của mình và chủ động trong việc yêu cầu xử lý xâm phạm khi có hành vi xâm phạm quyền của mình.

Ba là, xây dựng khung pháp lý về ĐTĐM

Theo xu hướng chung của thế giới, Chính phủ cần xây dựng một khung pháp lý chung nhất điều chỉnh về ĐTĐM để làm nền tảng cho quan hệ pháp lý với khách hàng. Các quy định này cần có mối liên hệ mật thiết với quá trình đàm phán, soạn thảo hợp đồng cung ứng dịch vụ ĐTĐM giữa nhà cung ứng dịch vụ và khách hàng. Đó có thể là những quy định cơ bản liên quan đến quá trình đánh giá, đàm phán hợp đồng, những quy định về lựa chọn hợp đồng mẫu hoặc cũng có thể là những quy định kết hợp giữa hai hình thức trên. Bởi bản chất của ĐTĐM khá phức tạp so với dịch vụ Internet truyền thống nên các điều khoản hợp đồng mẫu có thể được các bên xem xét và tiếp tục đàm phán để đạt được một thỏa thuận phù hợp nhất với nguyện vọng của các bên. Theo đó, những điều khoản cần đặc biệt chú ý liên quan đến thông báo vi phạm; truy cập, truyền tải dữ liệu và lưu trữ dữ liệu; cũng như các quy định về kiểm soát dữ liệu trên nền tảng ĐTĐM. Ngoài ra, văn bản cũng có thể bao gồm những nội dung về quyền riêng tư, bảo vệ dữ liệu cá nhân, bảo vệ thông tin người dùng trong TMĐT nói chung và ĐTĐM nói riêng ■

³⁴ Luật số 42/2019/QH14 ngày 14 tháng 6 năm 2019 của Quốc hội sửa đổi, bổ sung một số điều của Luật Kinh doanh bảo hiểm, Luật Sở hữu trí tuệ, có hiệu lực kể từ ngày 01 tháng 11 năm 2019.