

Mã số: 468

Ngày nhận: 14/12/2017

Ngày gửi phản biện lần 1: 24 /1 /2018

Ngày gửi phản biện lần 2:

Ngày hoàn thành biên tập: 29/1/2017

Ngày duyệt đăng: 30/1/2017

TRÁCH NHIỆM XÃ HỘI CỦA CÁC DOANH NGHIỆP SỐ ĐỐI VỚI VẤN ĐỀ BẢO VỆ DỮ LIỆU CÁ NHÂN KHÁCH HÀNG TRONG KỶ NGUYÊN 4.0: NHÌN TỪ KHÍA CẠNH PHÁP LÝ VÀ THỰC THI

Nguyễn Hồng Quân¹

Tóm tắt

Trải qua 20 năm xây dựng và phát triển công nghệ số ở Việt Nam, một thế hệ các doanh nghiệp hoạt động trên nền tảng công nghệ này đã xuất hiện vừa đem lại nhiều tiện ích nhưng cũng tiềm ẩn những rủi ro cho khách hàng trong quá trình thực hiện các giao dịch. Đặc biệt, khi gần đây, nhiều khách hàng đã phát hiện thông tin cá nhân của mình bị phát tán, trao đổi, mua bán một cách công khai từ các nhà cung cấp dịch vụ và đã gây ra nhiều hậu quả, phiền toái và tiềm ẩn nhiều rủi ro cho khách hàng. Vấn đề bảo vệ dữ liệu cá nhân đã được quy định tại một số văn bản quy phạm pháp luật của Nhà nước cùng với cơ chế xử phạt khi vi phạm. Tuy nhiên, hơn bao giờ hết, hiệu quả chỉ có thể đạt được khi các doanh nghiệp số và các chủ thể tham gia phải có ý thức cao. Đặc biệt doanh nghiệp cần coi đây là trách nhiệm xã hội (Corporate Social Responsibility - CSR) của mình khi khách hàng đã tin cậy và cung cấp những thông tin cá nhân (những điều bí mật đời tư) cho mình. Bài viết nhằm hệ thống hóa một số quan điểm bảo vệ dữ liệu cá nhân gắn với CSR của doanh nghiệp số, quy định pháp luật về bảo vệ dữ liệu cá nhân ở Việt Nam, tình hình bảo vệ dữ liệu cá nhân trên mạng, những thông tin cá nhân ở các cấp độ và khuyến nghị đối với Nhà nước, doanh nghiệp trong vấn đề bảo vệ thông tin cá nhân.

Abstract

Over 20 years of building and developing digital technology in Vietnam, a new generation of enterprises operating on the technology platform has grown up and brought many benefits but are also involved in numerous risks to the customers in transaction. In particular, personal data of customers has been dispersed, exchanged, purchased publicly from service providers and has caused numerous consequences, nuisances and potential risks for customers. The protection of personal data of customers has been stipulated in some legal documents and the mechanism of punishment. However, efficiency can only be achieved when digital enterprises and stakeholders are highly aware of the importance of privacy. These points to the need of businesses taking it as their social responsibility

¹ Trường Đại học Ngoại thương, Email: quannah@ftu.edu.vn

when customers trust and provide personal information (privacy) for them. This paper aims to systematize some views on personal data protection associated with CSR (Corporate Social Responsibility), the law on personal data protection in Vietnam, the protection of privacy on the internet, personal information at various levels and recommendations to the government and digital enterprises on the protection of personal information.

Keywords: Trách nhiệm xã hội, Doanh nghiệp số, Bảo vệ dữ liệu cá nhân, Privacy, CSR

Đặt vấn đề

Chúng ta đang sống ở trong kỷ nguyên số với nền tảng công nghệ thông tin và các ứng dụng kết nối, kinh doanh tiên tiến, hiện đại dựa trên sự tích hợp và hội tụ công nghệ số đã tạo nên sự thay đổi lớn về mọi mặt cho xã hội. Cuộc cách mạng Công nghiệp 4.0 (hay còn gọi là Cuộc cách mạng Công nghiệp lần thứ tư) đã được toàn Thế giới quan tâm và đón nhận một cách nhanh chóng. Đối với các nước đang phát triển như Việt Nam thì đây là một cơ hội mới để có thể tiếp cận và đón đầu nhằm tạo một vị thế mới trong khi các nền tảng của các cuộc cách mạng trước vẫn có thể tiếp tục được duy trì. Sự phát triển của Công nghệ thông tin (CNTT) và Thương mại điện tử (TMĐT) đã cho ra đời các mô hình doanh nghiệp mới, những doanh nghiệp được xây dựng, vận hành và phát triển dựa trên nền tảng CNTT hay còn gọi là các “doanh nghiệp số” với cách tiếp cận, giao tiếp và tương tác trực tuyến thông qua các phương tiện điện tử hiện đại kết nối với mạng Internet và các mạng mở.

Trong kỷ nguyên 4.0, dữ liệu và thông tin của cá nhân khách hàng không chỉ đơn thuần là thông tin để giao tiếp và thực hiện các hoạt động kinh doanh mà còn là “tài sản” của mỗi doanh nghiệp. Chính vì sự quan trọng của dữ liệu cá nhân khách hàng và quyền riêng tư đã đặt các doanh nghiệp số hóa phải thực hiện trách nhiệm xã hội của mình trong việc bảo vệ các dữ liệu – những thông tin khách hàng đã cung cấp khi họ thực hiện các giao dịch với doanh nghiệp một cách nghiêm túc và chủ động thông qua các cơ chế và hạ tầng bảo mật phù hợp nhằm tránh sự truy cập, tấn công, thu thập, trao đổi bất hợp pháp các dữ liệu cá nhân khách hàng.

1. Trách nhiệm xã hội của doanh nghiệp số trong kỷ nguyên 4.0

Trong thời gian gần đây, các quan điểm mới về phát triển kinh tế và quản trị doanh nghiệp đang được nghiên cứu và đưa vào áp dụng ở rất nhiều quốc gia trên thế giới, CSR (Corporate Social Responsibility - Trách nhiệm xã hội của doanh nghiệp) cũng được giới học thuật và doanh nghiệp đặc biệt quan tâm và trở thành một hướng nghiên cứu, ứng dụng mới nhằm duy trì sự phát triển lâu dài, đem lại lợi ích tối đa cho cộng đồng xã hội và các bên liên quan. Vấn đề CSR cũng đã được xem xét một cách cụ thể với các khía cạnh có liên quan và tác động trực tiếp với doanh nghiệp chứ không còn là cách hiểu một cách chung nhất như trước đây. Hiện nay, đã có nhiều tổ chức quốc tế đưa ra các tiêu chí CSR điển hình như: Hướng dẫn của OECD về tập đoàn đa quốc gia, Thỏa ước toàn cầu của Liên hợp quốc (UNGC), Tiêu chuẩn ISO 26000, Tiêu chuẩn GRI G4, Tiêu chuẩn EU về CSR, Tiêu chuẩn CSR của Nhật Bản. Theo tiêu chuẩn CSR của Nhật Bản, khi thực hiện CSR doanh nghiệp cần phải thực hiện các nội dung cụ thể sau đây:

- **Tuân thủ pháp luật và đạo đức kinh doanh:** Tuân thủ các chuẩn mực đạo đức kinh doanh; Tuân thủ pháp luật.

- **Minh bạch thông tin:** Cung cấp thông tin kịp thời, phù hợp và hữu ích cho các bên liên quan và duy trì các kênh thông tin hai chiều; Quản lý thông tin dữ liệu một cách phù hợp.

- **Chất lượng và an toàn:** Đảm bảo yêu cầu an toàn và chất lượng đối với sản phẩm cũng như phương pháp để sản xuất ra sản phẩm đó.

- **Lao động và quyền con người:** Tôn trọng quyền con người của các đối tượng chịu ảnh hưởng từ hoạt động của doanh nghiệp; Tôn trọng nhân viên, người lao động.

- **Môi trường:** Quan tâm đến vấn đề môi trường trong các hoạt động kinh doanh; Cung cấp thông tin về môi trường trong hoạt động của doanh nghiệp.

- **Hoạt động từ thiện:** Tham gia tích cực vào các hoạt động từ thiện làm cho cộng đồng phát triển bền vững và lành mạnh.



Hình 1. Các khía cạnh CSR theo quan điểm của Nhật Bản

Nguồn: Tác giả tổng hợp, năm 2017

Có sự khác biệt nào giữa doanh nghiệp thực hiện CSR và tuân thủ pháp luật? Đây là vấn đề quan trọng quyết định đến việc triển khai các hoạt động CSR trong mỗi doanh nghiệp. Nếu các doanh nghiệp quan niệm rằng việc thực hiện CSR chẳng qua là tuân thủ các quy định của pháp luật về kinh doanh, bảo vệ môi trường và pháp luật có liên quan đến các vấn đề xã hội thì đây mới chỉ thực hiện CSR ở dưới góc độ tuân thủ tối thiểu, ví dụ như việc đảm bảo các tiêu chuẩn xả thải của các nhà máy tại các khu công nghiệp theo đúng quy định của pháp luật về

môi trường hay các quy định về mức lương tối thiểu cho người lao động tại các doanh nghiệp, hay đầu tư hệ thống máy chủ hoặc phần mềm để đảm bảo an toàn dữ liệu cho khách hàng. Tuy nhiên, khi các doanh nghiệp quan niệm thực hiện CSR thì các nội dung và công việc triển khai không chỉ dừng lại ở vấn đề tuân thủ pháp luật mà là tuân thủ tốt hơn các quy định của pháp luật; các chỉ tiêu không chỉ đạt mà còn vượt yêu cầu so với quy định của pháp luật đề ra; vấn đề an toàn dữ liệu cho khách hàng không chỉ dừng lại ở việc đầu tư đủ hệ thống máy chủ hay phần mềm mà đằng sau hệ thống đó là một sự đảm bảo an toàn thông tin ở mức độ cao với sự tham gia của đội ngũ nhân sự đầy trách nhiệm và kinh nghiệm. Bên cạnh đó, thực hiện CSR còn thực hiện các khía cạnh không quy định trong pháp luật, các hoạt động và việc làm có ý nghĩa và đem lại lợi ích cho cộng đồng sẽ xuất hiện trong quá trình doanh nghiệp ra quyết định để xây dựng một môi trường và xã hội kinh doanh và tiêu dùng bền vững mà khi đó các doanh nghiệp số cũng không phải là ngoại lệ.

Xét ở khía cạnh CSR, việc bảo vệ thông tin cá nhân của khách hàng đối với các doanh nghiệp trong kỷ nguyên 4.0 đảm bảo cho các khía cạnh:

Thứ nhất, bảo vệ thông tin cá nhân nhằm thực hiện tính tuân thủ của doanh nghiệp đối với người tiêu dùng và khách hàng và bảo vệ thông tin cá nhân cũng cần sự tuân thủ của đối tác kinh doanh trong hệ thống thông qua các cam kết của doanh nghiệp trong việc bảo vệ thông tin cá nhân cũng như việc xây dựng các hạ tầng kỹ thuật để thực hiện tốt công việc này. Bên cạnh đó, ngoài việc bảo vệ tốt thông tin cá nhân của khách hàng, doanh nghiệp cần loại bỏ các hành động xâm phạm đến các dữ liệu thuộc quyền quản lý và sử dụng của các doanh nghiệp đối tác và tôn trọng quyền sở hữu trí tuệ của các doanh nghiệp.

Thứ hai, ở khía cạnh minh bạch hóa thông tin: doanh nghiệp sẽ cung cấp đầy đủ thông tin cần thiết cho các dịch vụ khách hàng; Cung cấp thông tin phù hợp, hữu ích về hàng hóa và dịch vụ (Mô tả đầy đủ thông tin trong hợp đồng, nhãn hàng, quy cách, giá cả, điều kiện bảo hành, điều kiện giao hàng, điều kiện đổi – trả lại hàng, hiển thị cách sử dụng sản phẩm an toàn, chính xác).

Bên cạnh đó, vấn đề bảo vệ dữ liệu và sự riêng tư của người tiêu dùng cũng đã được quy định rất rõ tại mục 6.7.7 của ISO 26000: 2010 *“Việc bảo vệ dữ liệu và sự riêng tư của người tiêu dùng nhằm bảo vệ quyền riêng tư của người tiêu dùng bằng việc giới hạn các loại thông tin thu thập cũng như cách thức thông tin được lấy, sử dụng và bảo mật. Sự gia tăng việc sử dụng truyền thông điện tử (bao gồm cả các giao dịch tài chính) và thử nghiệm gen, cũng như sự tăng trưởng về cơ sở dữ liệu quy mô rộng, làm gia tăng mối quan ngại về sự riêng tư của người tiêu dùng có thể được bảo vệ như thế nào, đặc biệt là về thông tin nhận dạng cá nhân”*. Đây cũng chính là những nội dung quan trọng để các doanh nghiệp số có thể thực hiện CSR dưới khía cạnh bảo vệ thông tin cho khách hàng. Chính vì vậy, có thể khẳng định rằng việc thực hiện tốt công tác bảo vệ dữ liệu cá nhân của khách hàng là một hoạt động quan trọng nhằm thực hiện tốt các tiêu chí CSR của doanh nghiệp số, giúp cho doanh nghiệp số có một môi trường kinh doanh lành mạnh và có sự phát triển bền vững trong tương lai.

2. Một số quy định pháp lý liên quan tới bảo vệ thông tin cá nhân

2.1. Quy định về thông tin cá nhân ở Bộ luật Dân sự Việt Nam 2015

Theo các quy định tại Điều 38 của Bộ luật này đã cho thấy: “Quyền bí mật đời tư của cá nhân được tôn trọng và được pháp luật bảo vệ” hay “Thư tín, điện thoại, điện tín, các hình thức thông tin điện tử khác của cá nhân được bảo đảm an toàn và bí mật”. Do vậy mà việc thu thập, lưu giữ, sử dụng, công khai thông tin liên quan đến đời sống riêng tư, bí mật cá nhân phải được người đó đồng ý, việc thu thập, lưu giữ, sử dụng, công khai thông tin liên quan đến bí mật gia đình phải được các thành viên gia đình đồng ý. Khi triển khai ký kết các hợp đồng (bao gồm cả hợp đồng điện tử) thông qua các hình thức khác nhau như qua trang web, email, hợp đồng soạn sẵn đưa lên mạng hay các hình thức khác thì các bên trong hợp đồng không được tiết lộ thông tin về đời sống riêng tư, bí mật cá nhân, bí mật gia đình của nhau mà mình đã biết được trong quá trình xác lập, thực hiện hợp đồng.

Bên cạnh các quy định trên, nhằm bảo vệ thông tin cá nhân, đặc biệt khi tham gia vào các trang mạng xã hội như Facebook, Twitter, Zalo, ... tại Điều 32 của Bộ luật Dân sự năm 2015 cũng đã quy định “Việc sử dụng hình ảnh của cá nhân phải được người đó đồng ý” hay “Việc sử dụng hình ảnh của người khác vì mục đích thương mại thì phải trả thù lao cho người có hình ảnh”. Tuy nhiên, Luật cũng quy định một số trường hợp sử dụng hình ảnh cá nhân mà không cần có sự đồng ý của người có hình ảnh hoặc người đại diện theo pháp luật của họ vì lợi ích quốc gia, dân tộc, lợi ích công cộng; 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

Như vậy, việc đăng tải, sử dụng hình ảnh của người khác trên mạng xã hội mà không tuân thủ các quy định nêu trên là hành vi vi phạm pháp luật. Khi đó, người có hình ảnh (hoặc người đại diện hợp pháp của họ) có quyền yêu cầu tòa án ra quyết định buộc người vi phạm, cơ quan, tổ chức, cá nhân có liên quan phải thu hồi, tiêu hủy, chấm dứt việc sử dụng hình ảnh, bồi thường thiệt hại và áp dụng các biện pháp xử lý khác theo quy định của pháp luật. Trường hợp hành vi này xâm phạm, gây ra thiệt hại về danh dự, nhân phẩm, uy tín, thì người vi phạm có trách nhiệm bồi thường thiệt hại cho người có hình ảnh theo quy định tại Điều 592 Bộ luật Dân sự 2015

Bảng 1. Các văn bản quy phạm pháp luật có liên quan đến bảo vệ thông tin cá nhân

Tên văn bản	Năm ban hành	Góc độ tiếp cận	Điều khoản
Bộ luật dân sự Việt Nam	24/11/2015	Quy định về nội dung thông tin cá nhân	Điều 32, điều 38
Luật An toàn thông tin mạng	19/11/2015	Quy định về kỹ thuật về thông tin trên mạng	Điều 16, 17, 18, 19, 20
Luật Công nghệ thông tin	29/06/2006	Quy định về khai thác và lưu trữ thông tin	Điều 21, 22

Nguồn: Tác giả tổng hợp, năm 2017

2.2. Quy định bảo vệ thông tin cá nhân tại Luật an toàn thông tin mạng năm 2015

Định nghĩa về thông tin cá nhân tại Điểm 15, Điều 3, Luật An toàn thông tin mạng ngày 19/11/2015 đã đưa ra “Thông tin cá nhân là thông tin gắn với việc xác định danh tính của một người cụ thể”. Quy định về việc bảo vệ thông tin cá nhân, tại Mục 2 (từ Điều 16 đến 20), Chương 2 đề cập tới các nội dung như: nguyên tắc bảo vệ thông tin cá nhân trên mạng; Thu thập và sử dụng thông tin cá nhân; Cập nhật, sửa đổi và hủy bỏ thông tin cá nhân; Bảo đảm an toàn thông tin cá nhân trên mạng; Trách nhiệm của cơ quan quản lý nhà nước trong bảo vệ thông tin cá nhân trên mạng.

Cơ sở pháp lý trên đây về bảo vệ thông tin cá nhân trên mạng ở nước ta đặt ra bốn vấn đề dưới đây.

- Về nguyên tắc bảo vệ thông tin cá nhân trên mạng

Để cho thông tin cá nhân được bảo vệ tốt nhất, các cá nhân cần phải tự bảo vệ thông tin cá nhân của mình cũng như tuân thủ các quy định của pháp luật về cung cấp thông tin cá nhân khi sử dụng dịch vụ trên mạng. Điều này rất quan trọng vì khi các cá nhân tự bảo đảm, kiểm soát một cách có ý thức đối với thông tin cá nhân sẽ ngăn chặn được những rủi ro trong suốt quá trình tương tác trực tuyến, đặc biệt là qua mạng xã hội. Bên cạnh đó, đối với những cơ quan, tổ chức, cá nhân xử lý thông tin cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng đối với thông tin do mình xử lý và tổ chức, cá nhân xử lý thông tin cá nhân phải xây dựng và công bố công khai biện pháp xử lý, bảo vệ thông tin cá nhân của tổ chức, cá nhân mình. Chính vì vậy, khi tiến hành cung cấp thông tin qua mạng trong quá trình giao dịch, các cá nhân cũng cần phải nắm rõ các thông tin được công bố của các cơ quan, tổ chức, cá nhân về những biện pháp xử lý, bảo vệ thông tin để tránh những rủi ro đối với các thông tin cá nhân mình cung cấp.

- Về vấn đề thu thập và sử dụng thông tin cá nhân

Luật cũng đã quy định rõ về trách nhiệm của các tổ chức, cá nhân đối với việc thu thập thông tin cá nhân chỉ được phép 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 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. Đặc biệt, các tổ chức và cá nhân không được cung cấp, chia sẻ, phát tán thông tin cá nhân mà mình đã thu thập, tiếp cận, kiểm soát cho bên thứ ba, trừ trường hợp có sự đồng ý của chủ thể thông tin cá nhân đó hoặc theo yêu cầu của cơ quan nhà nước có thẩm quyền. Bên cạnh đó, cơ quan nhà nước chịu trách nhiệm bảo mật, lưu trữ thông tin cá nhân do mình thu thập và chủ thể thông tin cá nhân có quyền yêu cầu tổ chức, cá nhân xử lý thông tin cá nhân cung cấp thông tin cá nhân của mình mà tổ chức, cá nhân đó đã thu thập, lưu trữ. Với những quy định này, hướng tới việc đảm bảo thông tin cá nhân một cách tối đa, tránh việc xâm phạm, phát tán, trao đổi nhằm các mục đích khác ngoài mục đích ban đầu đã cam kết.

- Vấn đề cập nhật, sửa đổi và hủy bỏ thông tin cá nhân

Chủ thể thông tin cá nhân có quyền yêu cầu tổ chức, cá nhân xử lý thông tin cá nhân cập nhật, sửa đổi, hủy bỏ thông tin cá nhân của mình mà tổ chức, cá nhân đó đã thu thập, lưu trữ hoặc ngừng cung cấp thông tin cá nhân của mình cho bên thứ ba. Ngay khi nhận được yêu cầu của chủ thể thông tin cá nhân về việc cập nhật, sửa đổi, hủy bỏ thông tin cá nhân hoặc đề nghị ngừng cung cấp thông tin cá nhân

nhân cho bên thứ ba, tổ chức, cá nhân xử lý thông tin cá nhân có trách nhiệm: Thực hiện yêu cầu và thông báo cho chủ thể thông tin cá nhân hoặc cung cấp cho chủ thể thông tin cá nhân quyền tiếp cận để tự cập nhật, sửa đổi, hủy bỏ thông tin cá nhân của mình; Áp dụng biện pháp phù hợp để bảo vệ thông tin cá nhân, thông báo cho chủ thể thông tin cá nhân đó trong trường hợp chưa thực hiện được yêu cầu do yếu tố kỹ thuật hoặc yếu tố khác. Tổ chức, cá nhân xử lý thông tin cá nhân phải hủy bỏ thông tin cá nhân đã được lưu trữ khi đã hoàn thành mục đích sử dụng hoặc hết thời hạn lưu trữ và thông báo cho chủ thể thông tin cá nhân biết, trừ trường hợp pháp luật có quy định khác.

- Bảo đảm an toàn thông tin cá nhân trên mạng

Để đảm bảo an toàn thông tin trên mạng, các tổ chức, cá nhân xử lý thông tin cá nhân phải áp dụng biện pháp quản lý, kỹ thuật phù hợp để bảo vệ thông tin cá nhân do mình thu thập, lưu trữ; tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn thông tin mạng. Khi xảy ra hoặc có nguy cơ xảy ra sự cố an toàn thông tin mạng, tổ chức, cá nhân xử lý thông tin cá nhân cần áp dụng biện pháp khắc phục, ngăn chặn trong thời gian sớm nhất.

2.3. Quy định tại Luật Công nghệ thông tin 2006

Về bản chất, các quy định của Luật An toàn thông tin mạng cũng đã căn cứ trên cơ sở các quy định của Luật Công nghệ thông tin đã ban hành nên về cơ bản một số quy định đã có sự thông nhất giữa 2 luật này như quy định về thu thập, xử lý và sử dụng thông tin cá nhân trên môi trường mạng (quy định ở Điều 21 của Luật CNTT và Điều 18 của Luật An toàn thông tin mạng) là thống nhất.

Đối với việc lưu trữ, cung cấp thông tin cá nhân trên môi trường mạng, Luật CNTT năm 2006 cũng đã quy định tương đối rõ ràng “cá nhân có quyền yêu cầu tổ chức, cá nhân lưu trữ thông tin cá nhân của mình trên môi trường mạng thực hiện việc kiểm tra, đính chính hoặc hủy bỏ thông tin đó” và “tổ chức, cá nhân không được cung cấp thông tin cá nhân của người khác cho bên thứ ba, trừ trường hợp pháp luật có quy định khác hoặc có sự đồng ý của người đó”. Nếu xảy ra những thiệt hại do hành vi vi phạm trong việc cung cấp thông tin cá nhân cá nhân có quyền yêu cầu bồi thường thiệt hại.

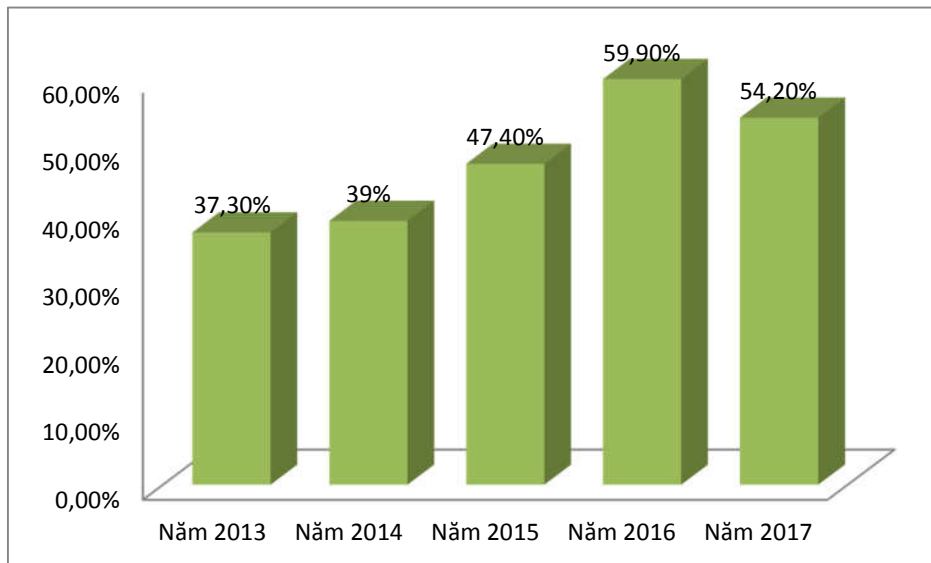
Như vậy cho tới nay, pháp luật Việt Nam cũng đã có quy định tương đối cụ thể và rõ ràng về vấn đề bảo vệ thông tin cá nhân qua các Bộ luật và Luật ở các góc độ khác nhau. Tuy nhiên, thương mại điện tử là xuyên biên giới nên để quy định này thực sự được thực thi một cách hiệu quả thì đòi hỏi một cơ chế giám sát, quản lý và xử lý vi phạm cũng ở cấp độ xuyên quốc gia chứ không chỉ dừng lại ở phạm vi lãnh thổ Việt Nam.

3. Tình hình bảo vệ dữ liệu cá nhân của các doanh nghiệp số ở Việt Nam

3.1. Tình hình an toàn thông tin cá nhân ở Việt Nam trong những năm gần đây

Theo báo cáo tổng hợp kết quả điều tra, đánh giá thực trạng an toàn thông tin (ATTT) tại Việt Nam năm 2016 của Hiệp hội An toàn thông tin Việt Nam (VNISA), Chỉ số ATTT Việt Nam (Vietnam Information Security Index) 2016 là 59,9% - tăng 12,5% so với mức 47,4% năm 2015 (chỉ số này các năm 2014 và 2013 lần lượt là 39% và 37,3%) và lần đầu tiên vượt mức trung bình 50% của thế giới.

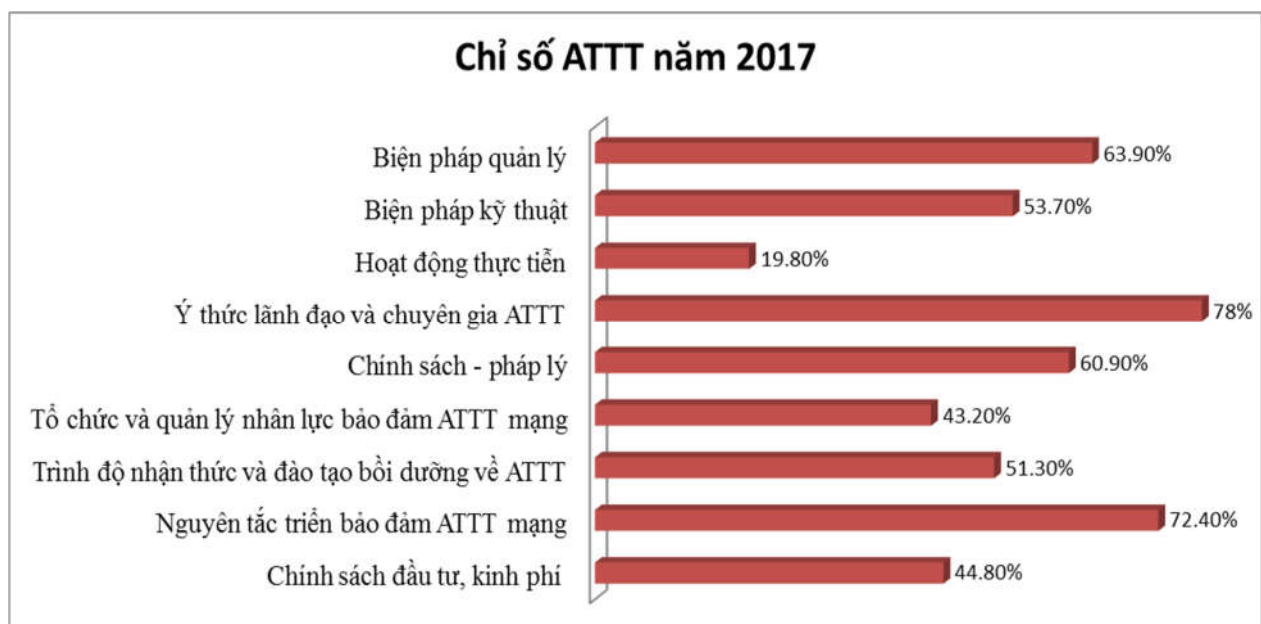
Chỉ số này có xu hướng tăng từ năm 2013-2016, tuy nhiên, đến năm 2017 chỉ số ATTT lại giảm xuống còn 54,20% do VNISA đã có sự thay đổi về các thức đo lường chỉ số và phương pháp khảo sát.



Hình 2. Chỉ số an toàn thông tin qua các năm 2013-2017

Nguồn: Cục An toàn thông tin, năm 2017

Theo đó, từ năm 2017, việc đo lường chỉ số an toàn thông tin sẽ dựa trên 09 chỉ số thành phần kết quả cụ thể: Chính sách đầu tư, kinh phí (44,8%); Nguyên tắc triển bảo đảm ATTT mạng (72,4%); Trình độ nhận thức và đào tạo bồi dưỡng về ATTT (51,3%); Tổ chức và quản lý nhân lực bảo đảm ATTT mạng (43,2%); Chính sách - pháp lý (60,9%); Ý thức lãnh đạo và chuyên gia ATTT (78%);



Hoạt động thực tiễn (19,8%); Biện pháp kỹ thuật (53,7%); và Biện pháp quản lý (63,9%).

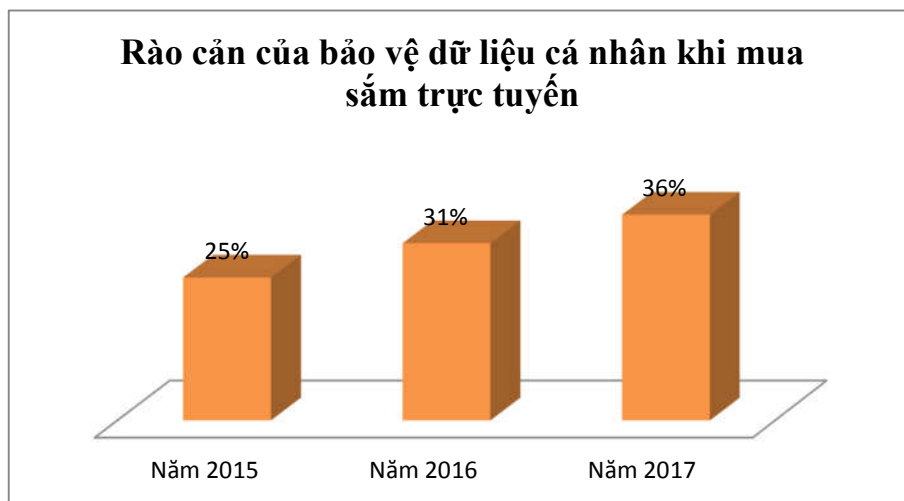
Hình 3. Chỉ số An toàn thông tin thành phần năm 2017

Nguồn: Cục An toàn thông tin, năm 2017

Từ kết quả khảo sát, đánh giá bước đầu cho thấy xu hướng phát triển ATTT là tích cực, ảnh hưởng của Luật ATTT mạng và các quy định pháp lý mới. Tuy nhiên, các doanh nghiệp đều đặc biệt yếu trong các khâu thiết lập và thực thi chính sách ATTT một mặt do nguồn nhân lực còn mỏng về số lượng, yếu về chuyên môn, mặt khác là do kinh phí đầu tư cho ATTT còn rất hạn chế. Điều này cũng cho thấy khả năng tuân thủ pháp luật ATTT của các doanh nghiệp mới chỉ đạt được mức trung bình theo yêu cầu chứ chưa thực sự như mong đợi của cộng đồng. Từ đó có thể thấy, góc độ thực thi CSR ở khía cạnh ATTT đối với dữ liệu cá nhân của khách hàng sẽ là một trở ngại lớn cho các doanh nghiệp số của Việt Nam trong thời gian tới.

3.2. Vấn đề bảo vệ dữ liệu cá nhân của khách hàng ngày càng trở nên quan trọng

Bên cạnh đó, vấn đề mất an toàn thông tin cá nhân cũng gia tăng cùng với sự tăng trưởng của doanh thu thương mại điện tử Việt Nam trong những năm vừa qua. Vấn đề bảo vệ dữ liệu cá nhân của khách hàng được coi là một yêu cầu quan trọng đối với các doanh nghiệp kinh doanh trực tuyến và đây cũng là trở ngại trong mua sắm trực tuyến nếu doanh nghiệp không có biện pháp bảo vệ dữ liệu cá nhân cho khách hàng.



Hình 4. Tỷ lệ khách hàng lo ngại về dữ liệu cá nhân khi mua hàng trên mạng

Nguồn: Báo cáo Thương mại điện tử Việt Nam, năm 2015, 2016, 2017

Trước năm 2015, vấn đề về bảo vệ dữ liệu cá nhân chưa phải là lo ngại của khách hàng khi tham gia mua sắm trực tuyến, các trở ngại chủ yếu tập trung vào một số khía cạnh như: khó kiểm soát chất lượng hàng hóa, uy tín của người bán hay không đủ thông tin để đưa ra quyết định mua hàng. Từ năm 2015, vấn đề về bảo vệ dữ liệu cá nhân ngày càng được người mua hàng trực tuyến quan tâm thể hiện ở mức độ lo ngại có xu hướng tăng từ 25% (năm 2015), 31% (năm 2016) và lên tới 36% vào năm 2017. Những lo ngại về vấn đề dữ liệu cá nhân của khách hàng gia tăng xuất phát từ việc lộ thông tin cá nhân (khách hàng thường xuyên phải nhận tin nhắn, điện thoại quảng cáo hay các thư rác quảng cáo qua

email) và hệ thống bảo mật thông tin của các doanh nghiệp đối với các thông tin khách hàng cung cấp trong quá trình mua hàng là chưa cao. Bên cạnh đó, không loại trừ khả năng thông tin của khách hàng bị các doanh nghiệp “bán” cho bên thứ ba sử dụng vào các mục đích quảng cáo, truyền thông và một số mục đích khác.

Điều này cho thấy, công tác bảo vệ dữ liệu cá nhân dưới khía cạnh pháp lý và khía cạnh trách nhiệm xã hội doanh nghiệp ở Việt Nam chưa được tốt và có xu hướng báo động khi mà mức độ lo ngại từ phía người tiêu dùng đang có sự gia tăng đáng kể. Nguyên nhân của vấn đề này xuất phát từ nhận thức từ phía doanh nghiệp, khách hàng và cộng đồng đối với vấn đề bảo vệ dữ liệu cá nhân, từ cơ chế giám sát và chế tài xử lý vi phạm đối với các quy định có liên quan tới bảo vệ dữ liệu cá nhân, từ giải pháp công nghệ bảo vệ an toàn thông tin và dữ liệu cá nhân và một số nguyên nhân khác.

4. Một số kiến nghị thực hiện trách nhiệm xã hội trong việc bảo vệ dữ liệu cá nhân

4.1. Đối với cơ quan quản lý Nhà nước

- *Nên xem xét và ban hành Nghị định về bảo vệ thông tin và dữ liệu cá nhân:* Trên cơ sở Luật An toàn thông tin Mạng, cho tới nay, các cơ quan của Chính phủ đã bắt tay vào ban hành các Nghị định hướng dẫn thực thi Luật bao gồm: Bộ Quốc phòng được giao chủ trì soạn thảo 2 văn bản: Nghị định của Chính phủ quy định chi tiết và thi hành Luật An toàn thông tin mạng về kinh doanh sản phẩm, dịch vụ mật mã dân sự, xuất khẩu, nhập khẩu sản phẩm mật mã dân sự (Danh mục sản phẩm, dịch vụ mật mã dân sự; Danh mục sản phẩm mật mã dân sự xuất khẩu, nhập khẩu theo giấy phép kèm theo Nghị định); Nghị định của Chính phủ quy định chi tiết về ngăn chặn xung đột thông tin trên mạng. Bộ Công an chủ trì soạn thảo Nghị định của Chính phủ quy định chi tiết về trách nhiệm và các biện pháp ngăn chặn hoạt động sử dụng mạng để khủng bố. Còn với Bộ TT&TT, cơ quan này được phân công chủ trì soạn thảo 4 văn bản quy định chi tiết thi hành Luật An toàn thông tin mạng gồm: Nghị định của Chính phủ quy định chi tiết về tiêu chí, thẩm quyền, trình tự, thủ tục xác định cấp độ an toàn hệ thống thông tin và trách nhiệm bảo đảm an toàn hệ thống thông tin theo từng cấp độ; Nghị định của Chính phủ quy định chi tiết về điều kiện cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng; Quyết định của Thủ tướng Chính phủ ban hành Phương án ứng cứu thảm họa thông tin quan trọng quốc gia; Quyết định của Thủ tướng Chính phủ ban hành Danh mục hệ thống thông tin quan trọng quốc gia.

Tuy nhiên, vấn đề bảo vệ thông tin cá nhân lại không được các cơ quan quan tâm đúng mức trong khi đó vấn đề này lại được các nước khác đặc biệt quan tâm. Bên cạnh đó, tình hình vi phạm và xâm hại thông tin cá nhân ở Việt Nam lại đang xảy ra một cách phổ biến và càng đáng báo động khi mà số người sử dụng Internet, điện thoại thông minh và mạng xã hội ngày càng tăng ở Việt Nam. Vì vậy, Chính phủ cần ban hành Nghị định về bảo vệ thông tin cá nhân nhằm đưa ra các quy định một cách cụ thể và rõ ràng hơn nữa cho các đối tượng tham gia bao gồm: cơ quan, tổ chức, doanh nghiệp và cá nhân.

4.2. Đối với Hiệp hội doanh nghiệp, chuyên gia và các bên liên quan

- *Ban hành bộ tiêu chí CSR về bảo vệ dữ liệu cá nhân:* Cơ quan quản lý nhà nước, Hiệp hội Thương mại điện tử, Phòng Thương mại và Công nghiệp Việt Nam và các tổ chức xã hội nghề nghiệp

khác có thể tham khảo và đưa ra các tiêu chí về bảo vệ thông tin và thông tin cá nhân dưới khía cạnh bộ tiêu chí CSR cho các doanh nghiệp số ở nước ta. Trên thực tế, các doanh nghiệp số đang hoạt động trên một môi trường rất đặc thù và luôn tiềm ẩn rất nhiều yếu tố rủi ro cho các bên tham gia do tính xác thực của thông tin trong trao đổi và giao dịch. Chính vì vậy, bộ quy tắc ứng xử CSR cho các doanh nghiệp số sẽ là bộ tiêu chí tham khảo có tính tự nguyện cho các doanh nghiệp và cũng nhằm mục đích nâng cao ý thức và tinh thần xã hội của các doanh nghiệp này để xây dựng một xã hội trực tuyến văn minh và an toàn. Để tiến hành thiết lập bộ tiêu chí CSR về bảo vệ thông tin cá nhân, các cơ quan tổ chức có thể tham khảo các nguyên tắc bảo vệ thông tin cá nhân đã được APEC (Diễn đàn kinh tế Thái Bình Dương) đã đưa ra từ năm 2004 với 09 nguyên tắc chính bao gồm: (1) Nguyên tắc ngăn ngừa thiệt hại, (2) Nguyên tắc thông báo trước, (3) Giới hạn phạm vi thu thập dữ liệu cá nhân, (4) Nguyên tắc sử dụng dữ liệu cá nhân, (5) Quyền lựa chọn của chủ thể dữ liệu cá nhân, (6) Tính toàn vẹn của dữ liệu cá nhân, (7) An ninh, an toàn dữ liệu cá nhân, (8) Tiếp cận và điều chỉnh dữ liệu cá nhân, (9) Trách nhiệm của các bên liên quan.

- *Phổ biến, tuyên truyền, nâng cao nhận thức và biểu dương những doanh nghiệp số thực hiện tốt việc tuân thủ và bảo vệ tốt dữ liệu cá nhân.* Hiện nay, có rất nhiều các hoạt động tuyên truyền, xúc tiến thương mại do các tổ chức và cơ quan thực hiện, tuy nhiên, ở khía cạnh bảo vệ dữ liệu cá nhân trên môi trường trực tuyến nói riêng và các hoạt động kinh doanh trực tuyến nói chung có vẻ ít được các cơ quan, tổ chức quan tâm tuyên truyền và khuyến khích phong trong “kinh doanh trực tuyến an toàn” trong thời gian vừa qua. Mặc dù, vấn đề an toàn trên môi trường kinh doanh trực tuyến đã được các cơ quan nhà nước và xã hội rất quan tâm khi mà tỷ lệ doanh thu trực tuyến ở Việt Nam đang có tốc độ tăng trưởng rất cao (trên 20%/năm, doanh số bán lẻ trực tuyến trên 5 tỷ USD, năm 2017). Đây là một nội dung rất quan trọng mà các cơ quan quản lý nhà nước, Hiệp hội ngành hàng và có tổ chức có liên quan cần đặc biệt quan tâm trong thời gian tới.

4.3. Với các doanh nghiệp số

Việc nhận thức đúng đắn vai trò và tầm quan trọng của thông tin cá nhân và việc tự nguyện bảo vệ thông tin cá nhân của khách hàng đối với các doanh nghiệp kinh doanh trực tuyến là vô cùng quan trọng. Một mặt giúp cho doanh nghiệp tạo lập được uy tín đối với khách hàng mặt khác, đây còn là một tài nguyên quý giá để doanh nghiệp thực hiện các hoạt động kinh doanh trực tuyến. Muốn vậy doanh nghiệp cần tiến hành một số biện pháp sau đây để bảo vệ thông tin cá nhân của khách hàng:

- *Doanh nghiệp cần xây dựng và thông báo chính sách bảo vệ thông tin cá nhân* của doanh nghiệp mình đăng lên website ngay trong mục đăng ký thành viên (hoặc tại các trang nội dung mà doanh nghiệp muốn các cá nhân cung cấp thông tin khi truy cập). Tại chính sách này, doanh nghiệp phải nêu rõ mục đích của việc thu thập thông tin cá nhân để làm gì? Các cam kết về việc bảo vệ thông tin cá nhân và giữ bí mật thông tin cá nhân, trách nhiệm của doanh nghiệp về việc lộ thông tin cá nhân, v.v... Việc đưa ra một chính sách bảo vệ thông tin cá nhân không chỉ khẳng định uy tín và trách nhiệm của doanh nghiệp đối với các thông tin này mà còn tạo lòng tin cho khách hàng trong việc cung cấp thông tin cá nhân của mình một cách chính xác từ đó giúp doanh nghiệp có thể thuận tiện trong việc gửi các thông tin kinh doanh cần thiết theo đúng mong muốn của khách hàng.

- *Không tiết lộ thông tin cá nhân đặc biệt là email lên website của doanh nghiệp.* Có rất nhiều doanh nghiệp hoặc các trang thông tin điện tử, Cổng thương mại điện tử do sơ xuất hoặc cố tình đưa thông tin của các cá nhân hoặc tổ chức kinh doanh rất chi tiết lên website đặc biệt là email. Điều này có một ưu điểm là tiện giao dịch và liên hệ cho các đối tác và tạo ra một xã hội thông tin. Tuy nhiên, điều này lại giúp cho các tổ chức và cá nhân thu thập thông tin để bán lại hoặc sử dụng chúng vào các mục đích khác. Hậu quả là các thông tin cá nhân bị lộ, các cá nhân liên tục nhận được các cuộc điện thoại hoặc email quảng cáo mà chúng ta gọi là spam mail không mong muốn. Việc đưa thông tin cá nhân và tổ chức lên mạng là cần thiết, tuy nhiên, các doanh nghiệp nên đưa các thông tin cần thiết và thuần túy về giao dịch ví dụ như: tên người đại diện, điện thoại cơ quan của họ, fax, email của cơ quan, v.v... không nên đưa thông tin thực sự mang tính cá nhân như điện thoại di động, email cá nhân hoặc blog riêng tư. Các doanh nghiệp hoạt động thương mại điện tử như các sàn giao dịch thương mại điện tử, các mạng xã hội, diễn đàn và các loại hình khác, tài sản lớn nhất của các loại hình này đó chính là cộng đồng. Cộng đồng ở đây có thể là các doanh nghiệp hoặc các cá nhân, mà ở đó thông tin của doanh nghiệp và thông tin của cá nhân luôn là tài nguyên để các doanh nghiệp này khai thác. Chính vì vậy, các doanh nghiệp hoạt động trong lĩnh vực này luôn đăng tải nội dung thông tin của các doanh nghiệp và cá nhân trên cổng thông tin của mình để kết nối các thành viên của họ hoặc với các thành viên trong cộng đồng. Đây cũng là đầu mối để các doanh nghiệp chuyên thu thập và kinh doanh thông tin cá nhân tìm đến để thu thập, chính vì vậy, việc đảm bảo thông tin cá nhân đối với các doanh nghiệp này càng trở nên cần thiết nhằm hạn chế việc thu thập các thông tin cá nhân của các doanh nghiệp khác. Đối với các doanh nghiệp hoạt động trong lĩnh vực này nên thiết kế 2 chế độ cung cấp thông tin cá nhân: thông tin công khai cho tất cả người truy cập có thể tham chiếu (gồm các thông tin cơ bản của cá nhân và tổ chức), thông tin công khai cho các thành viên khi họ đăng nhập vào tài khoản (cho phép các thành viên có thể giao dịch với nhau thông qua tài khoản của mình).

- *Xây dựng chế độ bảo mật cho cơ sở dữ liệu của doanh nghiệp:* Việc xây dựng chế độ bảo mật cho cơ sở dữ liệu là vô cùng quan trọng đối với doanh nghiệp đặc biệt là các doanh nghiệp có lưu trữ các thông tin quan trọng trong đó có thông tin cá nhân của khách hàng. Tuy nhiên, sẽ có những gói bảo mật có thể giúp cho doanh nghiệp bảo vệ an toàn dữ liệu và dữ liệu cá nhân của doanh nghiệp mình tùy thuộc vào tầm quan trọng và chi phí đầu tư mà doanh nghiệp có thể lựa chọn. Các doanh nghiệp cần lựa chọn ngay cách thức bảo mật và bảo vệ dữ liệu của mình ngay khi tiến hành lưu giữ các dữ liệu, tránh tình trạng “mất bò mới lo làm chuồng”.

- *Cần xây dựng quy trình bảo vệ thông tin cá nhân một cách khoa học:* Để đảm bảo các thông tin cá nhân của khách hàng được an toàn, doanh nghiệp số cần xây dựng một trình tự công việc và phân trách nhiệm cho những người chịu trách nhiệm một cách cụ thể với một số nội dung cụ thể như: Yêu cầu kiểm tra, rà soát, đánh giá đảm bảo an toàn thông tin chung; Phân công bộ phận kỹ thuật thực hiện hoặc lựa chọn đơn vị đủ năng lực để triển khai; Xây dựng kế hoạch kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin cá nhân; Thực hiện kiểm tra, rà soát, đánh giá đảm bảo an toàn thông tin cá nhân; Lập báo cáo, nguy cơ, rủi ro, lỗ hổng, mã độc gây mất an toàn thông tin cá nhân; Tiến hành xử lý các vấn đề nghiệp vụ; Lập Báo cáo tổng hợp.

5. Kết luận

Dữ liệu thông tin cá nhân là “tài sản” quan trọng của các doanh nghiệp số hóa và cũng là quyền “bất khả xâm phạm” của cá nhân. Trong khi hoạt động kinh doanh trực tuyến đang có tốc độ phát triển nhanh chóng thì việc tham gia vào môi trường trực tuyến của các cá nhân ngày càng tăng, cùng với đó, một lượng thông tin cá nhân khổng lồ được đưa lên môi trường mạng để thực hiện các giao dịch mua bán, trao đổi. Để đảm bảo an toàn và hạn chế những rủi ro đối với các thông tin cá nhân luôn cần có sự tham gia của các bên có liên quan với các biện pháp đồng bộ bao gồm cả vấn đề về con người, công nghệ, quy trình, thiết bị, hệ thống quản lý,... và hơn thế nữa là quan điểm nhận thức thống nhất, đúng đắn của các doanh nghiệp số - là những đơn vị trực tiếp tiếp nhận, quản lý và sử dụng “nguồn tài nguyên” này với tinh thần “vì một xã hội trực tuyến an toàn và hiệu quả”. Không coi thế giới ảo là “ảo” và thực hiện các hành động lợi dụng thế giới ảo để đem lại những “lợi ích thực” bằng việc sử dụng chính dữ liệu cá nhân của khách hàng cung cấp ra thị trường hoặc thiếu trách nhiệm trong vấn đề bảo vệ dữ liệu cá nhân của khách hàng. Thực hiện tốt việc bảo vệ dữ liệu cá nhân với tinh thần CSR, chắc chắn các doanh nghiệp số sẽ nhận được sự tin tưởng của khách hàng và nâng cao được giá trị thương hiệu của mình trên môi trường trực tuyến.

Tài liệu tham khảo

1. Cục An toàn thông tin – Bộ Thông tin và Truyền thông, *Báo cáo An toàn thông tin Việt Nam*, 2015.
2. Cục An toàn thông tin – Bộ Thông tin và Truyền thông, *Cẩm nang an toàn thông tin*, 2015;
3. Cục Thương mại điện tử và Công nghệ thông tin – Bộ Công Thương, *Báo cáo Thương mại điện tử Việt Nam*, 2017.
4. Cục Thương mại điện tử và Công nghệ thông tin, *tài liệu Diễn đàn Cách mạng Công nghiệp lần thứ IV*, 2017.
5. Bộ Công Thương, *Những nguyên tắc cơ bản về bảo vệ dữ liệu cá nhân trong thương mại điện tử*, 2008.
6. Quốc hội Việt Nam, *Bộ luật dân sự*, 2015, từ www.na.gov.vn.
7. Quốc hội Việt Nam, *Luật An toàn thông tin mạng*, 2015, từ www.na.gov.vn.
8. Quốc hội Việt Nam, *Luật Công nghệ*, 2006, www.na.gov.vn.
9. KEIDANREN (2010), *Chapter of Corporate Behavior*, September 14, 2010.
10. Nguyễn Thu Thủy & Nguyễn Hồng Quân (2017), *Hoạt động trách nhiệm xã hội của doanh nghiệp Nhật Bản và bài học kinh nghiệm cho Việt Nam*, Nhà xuất bản Dân Trí.
11. Vân Anh (2017), *Nguyên cơ mất an toàn thông tin mạng của doanh nghiệp vừa và nhỏ Việt Nam rất cao*, từ <http://ictnews.vn/cntt/bao-mat/bo-gd-dt-tang-bang-khen-cho-3-doi-xuat-sac-nhat-cuoc-thi-sinh-vien-voi-attt-2017-161773.ict>, truy cập 14/12/2017.
12. Tiêu chuẩn quốc gia TCVN ISO 26000:2013 (ISO 26000:2010) về Hướng dẫn về trách nhiệm xã hội, <http://hethongphapluatvietnam.net/tieu-chuan-quoc-gia-tcvn-iso-26000-2013-iso-26000-2010-ve-huong-dan-ve-trach-nhiem-xa-hoi.html>, truy cập ngày 26/01/2018.