**Bảo vệ thông tin người tiêu dùng**

**1. Thông tin của người tiêu dùng**

Trong cơ chế thị trường, để giành được lợi thế, các nhà cung cấp phải phục vụ tốt nhất cho các khách hàng của mình. Để xác lập và tiến hành giao dịch, người tiêu dùng và doanh nghiệp phải cung cấp cho nhau những thông tin tối thiểu về mình như tên, địa chỉ liên lạc, đối tượng giao dịch, địa chỉ giao hàng, phương tiện thanh toán... Khi đó, người tiêu dùng luôn được khuyến khích cung cấp nhiều thông tin để thuận lợi hơn cho việc tư vấn lựa chọn sản phẩm phù hợp. Chẳng hạn với một sản phẩm thời trang, nhà thiết kế không chỉ cần đến tên, tuổi của người tiêu dùng mà còn là công việc, địa vị xã hội, các thông số hình thể… để có được một sản phẩm phù hợp nhất với túi tiền, nhu cầu, thẩm mỹ của họ. Sự đa dạng trong nhu cầu của con người cũng như trong sự phát triển của các loại hình hàng hóa, dịch vụ càng làm cho việc khai thác thông tin khách hàng trở nên cần thiết nhưng cũng phức tạp, đa dạng hơn. Trong nhiều trường hợp, thông tin còn tế nhị và riêng tư hơn như tình trạng bệnh tật, sở thích, thói quen cá nhân...

Người tiêu dùng, theo nghĩa phổ biến, đó là các cá nhân mua hàng hóa dịch vụ với mục đích tiêu dùng và không có ý định tái cung cấp[1]. Theo đó, những thông tin của người tiêu dùng cũng có thể được hiểu là những thông tin cá nhân. Điểm khác biệt giữa các thông tin cá nhân với thông tin người tiêu dùng là ở chỗ, thông tin của người tiêu dùng được thu thập và lưu trữ bởi các doanh nghiệp trong quá trình xác lập giao dịch với người tiêu dùng hoặc qua các khảo sát thị trường của họ.

Những thông tin khách hàng đã thu thập được lưu trữ, quản lý có thể cho phép doanh nghiệp một mặt đáp ứng được nhu cầu của khách hàng trong một giao dịch trước mắt, nhưng mặt khác nó cũng tạo điều kiện để doanh nghiệp có thể dễ dàng tiếp cận với khách hàng cũ của mình thông qua việc khai thác cơ sở dữ liệu khách hàng sẵn có.Lưu trữ thông tin khách hàng chính là một phương thức để duy trì mối quan hệ bạn hàng ổn định cho nhà cung cấp đối với khách hàng truyền thống, bảo đảm giữ vững thị phần của họ một cách tiết kiệm. Thay vì phải mở rộng quảng bá thương hiệu, tiếp thị sản phẩm, doanh nghiệp chỉ cần dò tìm trong cơ sở dữ liệu sẵn có và liên lạc với khách hàng cũ. Đồng thời, để mở rộng thị phần, doanh nghiệp cũng cần điều tra, thu thập thông tin để đánh giá được thị hiếu, khuynh hướng mua sắm của khách hàng để từ đó có những điều chỉnh thích hợp hoạt động kinh doanh của mình hướng tới những khách hàng tiềm năng.

Xây dựng và khai thác cơ sở dữ liệu khách hàng là những thao tác quan trọng đối với doanh nghiệp mà kinh tế học gọi là “quản lý quan hệ khách hàng” (hay customer relationship management *-* CRM). Thông qua CRM, các doanh nghiệp tiếp cận và giao tiếp với khách hàng có hệ thống và hiệu quả nhằm phục vụ khách hàng tốt hơn. Các mục tiêu mà CRM hướng tới là tìm kiếm, thu hút, giành niềm tin khách hàng mới, duy trì những đối tác đã có, lôi kéo khách hàng cũ trở lại, giảm chi phí tiếp thị và mở rộng dịch vụ khách hàng.Thông qua hệ thống quan hệ khách hàng, các thông tin của khách hàng sẽ được cập nhật và được lưu trữ trong hệ thống quản lý cơ sở dữ liệu. Bằng việc dò tìm, phân tích dữ liệu, doanh nghiệp có thể xác định danh sách khách hàng tiềm năng và lâu năm để đề ra những chiến lược chăm sóc khách hàng hợp lý. Hiện nay, rất nhiều các doanh nghiệp phát hành thẻ tích điểm nhằm ưu đãi khách hàng truyền thống của mình, đồng thời có thể cập nhật nhanh chóng cơ sở dữ liệu khách hàng hiện có và thu hút thêm khách hàng mới. Ngoài ra, thông qua cơ sở dữ liệu của mình, doanh nghiệp còn có thể xử lý các vấn đề vướng mắc của khách hàng nhanh chóng và hiệu quả.

**2. Thông tin của người tiêu dùng và quyền riêng tư**

Khi ý thức tư hữu của con người được hình thành, bất luận sự tương tác giữa con người với nhau có mức độ cao như thế nào, thì nhu cầu về sự riêng tư, kín đáo, không chia sẻ một khía cạnh, một vấn đề nào đó của cá nhân luôn tồn tại. Ngay cả khi hội nhập vào xã hội một cách tích cực, minh bạch hóa thông tin ở mức cao như trong các mạng xã hội, người ta vẫn luôn mong muốn mình không bị theo dõi bởi người khác. Người ta luôn cố gắng dành cho mình quyền tiết lộ, chia sẻ về bản thân mình với những đối tượng nhất định chứ không phải tất cả mọi người. Con người hiện đại sẽ tiếp tục phải tự cân bằng nhu cầu riêng tư với mong muốn chia sẻ, liên kết với người khác phù hợp với môi trường sống của mình[2].

Quyền riêng tư (right to privacy), đến nay đã được thừa nhận rộng rãi là một quyền con người, được pháp luật các quốc gia và quốc tế bảo vệ. Tuyên ngôn Quốc tế Nhân quyền (UDHR) năm 1948 khẳng định: "không ai phải chịu sự 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 hoặc uy tín cá nhân. Mọi người đều có quyền được pháp luật bảo vệ chống lại sự can thiệp và xâm phạm như vậy"[3]. Quyền riêng tư được tái khẳng định trong Công ước Quốc tế về các Quyền Dân sự và Chính trị (ICCPR 1966). Điều luật này ngăn chặn những hành vi xâm phạm tùy tiện và bất hợp pháp vào đời tư, gia đình, nhà ở, thư tín, danh dự, uy tín của mọi người mà có thể do các quan chức nhà nước hay do những chủ thể khác gây ra[4].

Quyền riêng tư, dù vậy, không phải là quyền tuyệt đối, nó có thể bị hạn chế trong những trường hợp nhất định vì lợi ích chung của xã hội. Lẽ đương nhiên, những hạn chế, can thiệp này phải được minh định trong luật và thực thi một cách nghiêm ngặt. Để bảo đảm bảo vệ đời tư hiệu quả, mỗi cá nhân cần có quyền được biết những thông tin cá nhân của mình được thu thập, lưu giữ bởi chủ thể nào, ở đâu và nhằm mục đích gì. Thêm vào đó, mỗi cá nhân cũng cần có quyền yêu cầu sửa chữa hoặc xóa bỏ thông tin cá nhân của mình nếu thông tin đang được lưu trữ không chính xác, hoặc bị thu thập hay lưu trữ một cách trái pháp luật. Bảo vệ quyền riêng tư đối với thông tin cá nhân của con người thường được các quốc gia quy định thành pháp luật *bảo vệ dữ liệu cá nhân (personal data protection)* hay còn gọi là *bảo vệ bí mật đời tư (personal confidence).*

Về phạm vi, bảo vệ dữ liệu cá nhân hẹp hơn việc bảo vệ quyền riêng tư ở chỗ dữ liệu cá nhân chỉ liên quan đến “dữ liệu” tức là việc thu thập và sử dụng các thông tin cá nhân mà không bao gồm các quyền về tự do thân thể, quyền bất khả xâm phạm về nơi ở. Bảo vệ dữ liệu cá nhân khởi đầu dùng để chỉ việc bảo vệ dữ liệu có liên quan đến cá nhân trước sự lạm dụng. Bảo vệ dữ liệu cá nhân dựa trên nguyên tắc mỗi người đều có *quyền tự quyết định* là ai, khi nào và dữ liệu cá nhân nào của mình được phép cho người khác biết.

*Thông tin của người tiêu dùng là một bộ phận của lĩnh vực bảo vệ dữ liệu cá nhân.* Điểm khác biệt giữa bảo vệ thông tin người tiêu dùng và bảo vệ dữ liệu cá nhân là ở phạm vi của nó: thông tin người tiêu dùng được thu thập, quản lý bởi các doanh nghiệp nhằm thực hiện hoặc hướng tới thực hiện các hoạt động bán hàng hóa, dịch vụ tiêu dùng; các dữ liệu cá nhân, ngược lại, có phạm vi rộng hơn, nó không bị giới hạn bởi các hoạt động cung cấp hàng hóa, dịch vụ tiêu dùng mà còn cả những lĩnh vực không liên quan đến thương mại. Ví dụ, linh mục có thể thu thập thông tin từ người xưng tội; cảnh sát có thể thu thập thông tin về nhân thân của những người liên quan đến vi phạm pháp luật hoặc những người tham gia tố tụng khác. Như vậy, bảo vệ thông tin của người tiêu dùng có cơ sở từ quyền riêng tư của con người.

Người tiêu dùng, trong đa số các trường hợp, sẽ buộc phải cung cấp những thông tin cá nhân cho các doanh nghiệp để phục vụ các giao dịch. Với mục tiêu giành lợi thế cạnh tranh, nhìn chung cơ sở dữ liệu khách hàng thường được các doanh nghiệp bảo mật chặt chẽ. Tuy vậy, vấn đề trọng tâm của tất cả các doanh nghiệp chính là lợi nhuận, họ sẽ không thể chi tiêu một cách vô hạn định cho công tác bảo mật thông tin khách hàng, ngoài ra, cạnh tranh không phải lúc nào cũng được duy trì một cách tuyệt đối, các doanh nghiệp vẫn thường có xu hướng liên kết, hợp tác hoặc thỏa hiệp, chia sẻ tài nguyên thông tin để cùng thu được lợi nhuận cao hơn.

Cần nhìn nhận là cơ sở dữ liệu cá nhân được hình thành chủ yếu từ sự tin cậy của khách hàng trong quan hệ đối với doanh nghiệp, bởi vậy, việc chia sẻ thông tin khách hàng giữa các doanh nghiệp được xem là hành vi *bội tín* với khách hàng. Ngoài ra, những thông tin cá nhân do doanh nghiệp thu thập được nếu sơ ý hoặc cố ý tiết lộ cho bên thứ ba thì hoàn toàn có thể đem lại những bất lợi cho khách hàng. Chẳng hạn, sẽ rất khó khăn cho một người trong giao tiếp xã hội nếu bác sĩ của anh ta tiết lộ rằng anh ta mắc bệnh xã hội, mọi người sẽ có đánh giá không tốt về anh ta cho dù việc mắc bệnh không có nguyên nhân từ các tệ nạn xấu. Một ví dụ khác về sự bất tiện trong đời sống của người tiêu dùng là khi số điện thoại hoặc email bị tiết lộ, anh ta có thể bị quấy rầy khi phải nhận những cuộc gọi, tin nhắn, thư điện tử quảng cáo không mong muốn. Việc tiết lộ hay chia sẻ thông tin này cũng có thể bị lợi dụng bởi những kẻ xấu nhằm bôi nhọ danh dự khách hàng hoặc đánh cắp tài sản của họ thông qua việc sử dụng các thông số tài khoản hoặc thẻ tín dụng, thẻ mua hàng của họ. Tuy nhiên, vấn đề cốt yếu của việc tiết lộ hoặc chia sẻ thông tin khách hàng, kể cả thông tin tốt, mà không được sự đồng thuận của họ, chính là vi phạm quyền riêng tư của người tiêu dùng.

**3. Những phương thức cơ bản bảo vệ thông tin người tiêu dùng**

Bảo vệ thông tin người tiêu dùng là một nhiệm vụ của nhiều lĩnh vực như đạo đức, pháp luật. Ngay trong lĩnh vực pháp luật, bảo vệ thông tin người tiêu dùng cũng là một lĩnh vực liên ngành. Kinh nghiệm quốc tế cho thấy, bảo vệ thông tin người tiêu dùng chủ yếu được đặt trong nhóm quy định về bảo vệ dữ liệu cá nhân.

Các phương thức điều chỉnh lĩnh vực pháp luật này đều hướng tới việc thu thập, khai thác cơ sở dữ liệu thông tin cá nhân một cách đàng hoàng, chính đáng, tôn trọng quyền con người, tôn trọng pháp luật và các giá trị đạo đức, nhân văn. Nói cách khác, pháp luật hướng tới sự đúng mực trong việc hình thành và khai thác thông tin cá nhân.

*Những hoạt động thông tin đúng mực* *(fair information practices - FIPs)*[5] là khái niệm lần đầu tiên được xuất hiện năm 1973 trong Báo cáo của Ủy ban cố vấn ngoại trưởng về hệ thống dữ liệu cá nhân tự động (US Secretary's Advisory Committee on Automated Personal Data Systems)[6]. Một báo cáo tương tự của Ủy ban này vào năm 1977 đã đưa ra một số nguyên tắc quan trọng về những hoạt động thông tin đúng mực. Những nguyên tắc này (fair information practice principles –FIPPs) bao gồm cả những yêu cầu về nội dung như mục đích, giới hạn, chất lượng thu thập thông tin; và thủ tục thông tin như trình tự truy cập và chấp thuận xử lý thông tin[7]. Các nguyên tắc hoạt động thông tin đúng mực này sau đó đã được sử dụng rộng rãi trong pháp luật bảo vệ quyền con người và tiếp tục phát triển.

Đến năm 1980, OECD đã biên soạn bản hướng dẫn về các nguyên tắc của những hoạt động thông tin đúng mực (Guidelines on Fair Information Practice Principles – FIPPs). Bộ FIPPs của OECD gồm 8 nguyên tắc, tuy không phải là một đạo luật nhưng chúng có ý nghĩa rất quan trọng trong bảo vệ quyền riêng tư cũng như bảo vệ dữ liệu cá nhân của các nước với tính cách là nguồn tham khảo. Các nguyên tắc FIPPs của OECD bao gồm:

*Thu thập có giới hạn:*Việc thu thập dữ liệu cá nhân và bất kỳ dữ liệu nào như vậy cần được thực hiện bằng các phương tiện hợp pháp và công bằng, và khi thích hợp, với những kiến ​​thức hoặc sự đồng ý của đối tượng dữ liệu.

*Chất lượng dữ liệu:*Dữ liệu cá nhân có liên quan đến mục đích mà chúng có thể được sử dụng và mức độ cần thiết cho các mục đích, phải chính xác, đầy đủ và phải được cập nhật.

*Mục đích thu thập được xác định chi tiết:*Các mục đích thu thập dữ liệu cá nhân phải được xác định không muộn hơn thời gian thu thập dữ liệu và sau đó sử dụng giới hạn trong việc thực hiện những mục đích đó; sẽ là không phù hợp nếu việc thu thập như trên khi thay đổi mục đích.

*Sử dụng giới hạn:*Dữ liệu cá nhân không được tiết lộ, làm sẵn để sử dụng cho các mục đích khác hơn so với những mục đích ban đầu, ngoại trừ trường hợp có sự đồng ý của chủ dữ liệu hoặc do pháp luật quy định

*An toàn dữ liệu:*Dữ liệu cá nhân phải được bảo vệ bằng các biện pháp bảo vệ an ninh hợp lý chống lại các rủi ro như mất mát hoặc truy cập trái phép, sử dụng, tiêu hủy, sửa đổi, bổ sung hoặc tiết lộ dữ liệu.

*Nguyên tắc công khai:*Cần có một chính sách chung cởi mở về sự phát triển, thực hành và các chính sách đối với dữ liệu cá nhân; phương tiện cho việc thiết lập cơ sở dữ liệu cá nhân và mục đích chính của việc sử dụng chúng, cũng như danh tính và địa chỉ người điều khiển dữ liệu phải được xác định trước.

*Sự tham gia của cá nhân:*Một cá nhân có quyền nhận được xác nhận từ người quản lý dữ liệu về việc có hoặc không có dữ liệu liên quan đến anh ta; được thông báo khi dữ liệu liên quan đến mình trong khoảng thời gian hợp lý, với một thái độ tử tế và theo hình thức dễ hiểu đối với anh ta, không phải chịu lệ phí một cách quá đáng; được thông báo lý do nếu các yêu cầu trên không được chấp nhận và được quyền phản đối các lý do đó; được phản đối các dữ liệu liên quan đến mình và yêu cầu xóa, sửa chữa hoặc cập nhật dữ liệu đó.

*Trách nhiệm giải trình:*Người quản lý dữ liệu phải có được trách nhiệm tuân thủ các biện pháp để bảo đảm hiệu lực cho các nguyên tắc đã nêu ở trên.

Năm 1995, Liên minh châu Âu ban hành chỉ thị số 95/46/EC về bảo vệ dữ liệu. Đây là một chỉ thị rộng được thông qua bởi Liên minh châu Âu; được thiết kế để bảo vệ sự riêng tư của tất cả các dữ liệu cá nhân của công dân EU được thu thập và sử dụng cho mục đích thương mại, đặc biệt nó liên quan đến xử lý, sử dụng hay trao đổi những dữ liệu đó. Nói cách khác, Chỉ thị 95/46 dành trọng tâm cho việc bảo vệ thông tin người tiêu dùng. Ngoài những nguyên tắc FIPPs như hướng dẫn của OECD, Chỉ thị 95/46 còn thành lập một khuôn khổ rộng lớn, trong đó đặt ra những giới hạn về việc thu và sử dụng các dữ liệu cá nhân, và đòi hỏi mỗi nước thành viên thiết lập một cơ quan độc lập chịu trách nhiệm cho việc bảo vệ dữ liệu quốc gia. Chỉ thị nghiêm cấm việc chuyển giao thông tin cá nhân được bảo vệ bên ngoài EU, trừ khi nước tiếp nhận áp dụng bảo vệ pháp lý tương tự. Mỗi quốc gia EU đã thành lập một cơ quan bảo vệ dữ liệu có thẩm quyền điều tra các khiếu nại, phạt tiền, khởi tố tội phạm và yêu cầu các doanh nghiệp thay đổi việc thực hành xử lý thông tin.

Năm 2016, Nghị viện châu Âu ban hành Quy định chung về bảo vệ dữ liệu (General Data Protection Regulation – GDPR) và có hiệu lực từ ngày 25/5/2018. Theo GDPR, việc thu thập dữ liệu và xử lý dữ liệu phải có sự đồng thuận của các cá nhân trừ khi có ít nhất một căn cứ hợp pháp để thực hiện. Những căn cứ hợp pháp là:

- Nếu chủ thể dữ liệu đã đồng ý xử lý dữ liệu cá nhân của mình;

- Thực hiện các nghĩa vụ theo hợp đồng với chủ thể dữ liệu hoặc cho các nhiệm vụ theo yêu cầu của đối tượng dữ liệu đang trong quá trình ký kết hợp đồng;

- Tuân thủ các nghĩa vụ pháp lý của một chủ thể quản lý dữ liệu;

- Bảo vệ lợi ích sống còn của chủ thể dữ liệu hoặc cá nhân khác;

- Thực hiện nhiệm vụ vì lợi ích công cộng hoặc chính quyền;

- Vì lợi ích hợp pháp của người kiểm soát dữ liệu hoặc bên thứ ba, trừ khi những lợi ích này bị chồng lấn với lợi ích của chủ thể dữ liệu hoặc quyền của người đó theo Hiến chương về các quyền cơ bản của EU (đặc biệt là trường hợp quyền trẻ em)[8].

- Người chủ thể dữ liệu có quyền rút lại việc đã đồng thuận của mình với điều kiện rút lại không khó khăn hơn điều kiện mà họ đã chấp thuận. Người xử lý dữ liệu không được từ chối quyền rút lại của chủ dữ liệu[9].

Việc không tuân thủ GDPR sẽ bị phạt rất nặng. Cụ thể, sai phạm đối với các chuẩn mực cốt lõi về xử lý dữ liệu, vi phạm các quyền cá nhân hoặc chuyển dữ liệu ra khỏi EU mà không đảm bảo các bảo vệ tương đương sẽ bị phạt tới 20 triệu Euro hoặc 4% doanh thu hàng năm trên toàn cầu[10].Sai phạm trong việc tuân thủ với các yêu cầu về kỹ thuật và tổ chức như đánh giá tác động, thông báo sự cố mất an toàn thông tin sẽ bị phạt tới 10 triệu Euro hoặc 2% doanh thu hàng năm trên toàn cầu[11]. Vụ kiện gần đây nhất trong khuôn khổ GDPR là Tổ chức người tiêu dùng châu Âu European Consumer Organisation (BEUC) đã kiện Google vì đã theo dõi vị trí của người tiêu dùng mà không được sự đồng thuận thực tế của họ. BEUC nại ra rằng, Google đã "lừa đảo" làm người dùng bật tùy chọn về “ghi nhớ lịch sử di chuyển” và không thông báo đầy đủ cho người dùng về việc bật như vậy để làm gì. Như vậy, sự đồng ý không được tự nguyện đưa ra. Vụ việc này có thể làm Google đối mặt với án phạt 4% doanh thu hàng năm và có thể lên đến 4 tỷ đô la. Trước đó, Facebook cũng đã bị tố giác về vi phạm điều kiện bảo mật thông tin và làm ảnh hưởng đến 25 triệu người dùng[12].

Đến nay, đã có khoảng 90 quốc gia trên thế giới ban hành luật có liên quan đến bảo vệ thông tin cá nhân dưới những hình thức khác nhau[13]. Có nước ban hành luật riêng về bảo vệ dữ liệu và được cụ thể hóa trong các luật chuyên ngành khác; cũng có nước ghi nhận quy định chung trong hiến pháp, luật dân sự và cụ thể hóa rải rác trong các luật như trường hợp của Việt Nam với Bộ luật Dân sự 2015 (Điều 38) và Luật Bảo vệ quyền lợi người tiêu dùng 2010 (Điều 6).

**4. Bảo vệ thông tin người tiêu dùng ở Việt Nam**

Hiến pháp, Bộ luật Dân sự, Luật Bảo vệ người tiêu dùng và nhiều văn bản pháp luật chuyên ngành như các luật về viễn thông, công nghệ thông tin, giao dịch điện tử của Việt Nam đều đã có quy định về quyền cơ bản của công dân và bảo vệ thông tin cá nhân. Hiến pháp năm 2013 quy định: “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”[14].

 Điều 38 Bộ luật Dân sự quy định: “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”[15].

Luật Giao dịch điện tử năm 2005 cũng xác định nghĩa vụ của cơ quan, tổ chức trong bảo đảm bí mật thông tin và không được chia sẻ thông tin của người khác mà mình tiếp cận hoặc kiểm soát được trong giao dịch điện tử nếu không được sự đồng ý của họ, trừ trường hợp pháp luật có quy định khác[16].

Luật Bảo vệ quyền lợi người tiêu dùng năm 2010 quy định: “Người tiêu dùng được bảo đảm an toàn, bí mật thông tin của mình khi tham gia giao dịch, sử dụng hàng hóa, dịch vụ, trừ trường hợp cơ quan nhà nước có thẩm quyền yêu cầu.

Trường hợp thu thập, sử dụng, chuyển giao thông tin của người tiêu dùng thì doanh nghiệp có trách nhiệm:

a) Thông báo rõ ràng, công khai trước khi thực hiện với người tiêu dùng về mục đích hoạt động thu thập, sử dụng thông tin của người tiêu dùng;

b) Sử dụng thông tin phù hợp với mục đích đã thông báo với người tiêu dùng và phải được người tiêu dùng đồng ý;

c) Bảo đảm an toàn, chính xác, đầy đủ khi thu thập, sử dụng, chuyển giao thông tin của người tiêu dùng;

d) Tự mình hoặc có biện pháp để người tiêu dùng cập nhật, điều chỉnh thông tin khi phát hiện thấy thông tin đó không chính xác;

đ) Chỉ được chuyển giao thông tin của người tiêu dùng cho bên thứ ba khi có sự đồng ý của người tiêu dùng, trừ trường hợp pháp luật có quy định khác”[17].

Luật An toàn thông tin mạng năm 2015 quy định việc “cập nhật, sửa đổi và hủy bỏ thông tin cá nhân” thì 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. Theo đó, ngay khi nhận được yêu cầu, tổ chức, cá nhân xử lý thông tin cá nhân có trách nhiệm thực hiện yêu cầu và thông báo lại 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 do tổ chức, cá nhân xử lý thông tin cá nhân đang lưu trữ. Tổ chức, cá nhân xử lý thông tin còn phải áp dụng các biện pháp phù hợp để bảo vệ thông tin cá nhân; thông báo lại 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. Luật cũng quy định 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[18]. Luật cũng quy định thiết lập kênh thông tin trực tuyến, xử lý các phản ánh của người dân về các vấn đề bảo vệ thông tin cá nhân[19].

Gần đây nhất, Luật An ninh mạng năm 2018 cũng quy định về phòng chống gián điệp mạng, bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng. Đồng thời Luật cũng quy định trách nhiệm của các cơ quan nhà nước trong lĩnh vực này[20].

Từ các quy định trên, có thể thấy quy định của pháp luật Việt Nam trong bảo vệ thông tin người tiêu dùng đã theo khá sát với các nguyên tắc FIPPs. Đồng thời, chúng cũng không có quá nhiều khác biệt với GDPR ở điều kiện chấp nhận cho phép thu thập, xử lý dữ liệu của người tiêu dùng.

Bên cạnh các quy định về quyền và nghĩa vụ của người chủ dữ liệu, người thu thập, xử lý dữ liệu, pháp luật Việt Nam còn quy định những chế tài xử phạt đối với các hành vi phát tán, chia sẻ thông tin cá nhân, tùy theo mức độ, hành vi mà tổ chức, cá nhân vi phạm sẽ bị xử lý vi phạm hành chính hoặc xử lý trách nhiệm hình sự. Chẳng hạn, theo Nghị định 174/2013/NĐ-CP của Chính phủ, hành vi mua bán trao đổi trái phép thông tin riêng của người sử dụng dịch vụ viễn thông, có thể bị phạt từ 50 - 70 triệu đồng[21]. Những người có hành vi vi phạm này, tùy vào tính chất, mức độ vi phạm có thể bị xử lý theo Bộ luật Hình sự năm 2015, sửa đổi, bổ sung năm 2017 về tội “Đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông” với khung hình phạt cao nhất là 7 năm tù[22].

Những hành động chiếm đoạt tài khoản viễn thông, ứng dụng, dịch vụ gia tăng trên mạng, chia sẻ mật khẩu, mã truy cập có thể bị phạt đến 20 triệu đồng; trộm cắp, mua bán, trao đổi, tiết lộ, sử dụng trái phép thông tin thẻ tín dụng của người khác hoặc truy cập bất hợp pháp vào mạng hoặc thiết bị số của người khác chiếm quyền điều khiển; can thiệp vào chức năng hoạt động của thiết bị số; lấy cắp, thay đổi, hủy hoại, làm giả dữ liệu hoặc sử dụng trái phép các dịch vụ có thể bị phạt từ 30 đến 50 triệu đồng bên cạnh việc bồi thường thiệt hại[23].

Việc xâm phạm bí mật hoặc an toàn thư tín, điện thoại, điện tín hoặc các hình thức trao đổi thông tin riêng tư khác của người khác có thể bị phạt tiền từ 20 triệu đến 50 triệu đồng, bị phạt cải tạo không giam giữ đến 3 năm, bị phạt tù từ 1 đến 3 năm, hoặc chịu hình phạt bổ sung về cấm đảm nhiệm chức vụ từ 1 đến 5 năm[24].

Như vậy, pháp luật Việt Nam cũng đã có các chế tài khá nghiêm khắc với các đối tượng thu thập, sử dụng trái phép các thông tin cá nhân của người tiêu dùng. Tuy nhiên trên thực tế, hầu như chưa có vụ việc nào trong lĩnh vực này được xử lý nếu không gây thiệt hại cho nạn nhân.

**5. Những rủi ro trong bảo vệ thông tin người tiêu dùng**

Như đã trình bày trên đây, bảo vệ thông tin của người tiêu dùng là một phần của bảo vệ quyền riêng tư của con người. Khi lựa chọn một mô hình hay cách thức điều chỉnh nào, chúng ta cũng cần đến hệ thống các nguyên tắc FIPPs. Sẽ tương đối khó khăn và không hiệu quả nếu chúng ta tách bạch việc bảo vệ quyền riêng tư của người tiêu dùng thành một nhóm quy định riêng bên ngoài những quyền con người.

Khi một người tham gia vào các hoạt động giao dịch hoặc tương tác trên truyền thông xã hội, có rất nhiều thông tin cá nhân có thể bị rò rỉ.Đó có thể là ngày tháng năm sinh, nơi làm việc, nơi học tập, địa chỉ gia đình, các thành viên trong gia đình mình, thậm chí là số chứng minh thư, số bằng lái xe, số hộ chiếu... và nguy hiểm hơn nữa là các thông tin về thẻ tín dụng. Tất cả những thông tin trên đều có thể bị đánh cắp hoặc chia sẻ bất hợp pháp và gây ảnh hưởng đến bản thân và những người thân của họ.

*- Nguy cơ đến từ các nhà cung cấp dịch vụ mạng xã hội*

Việc sử dụng mạng xã hội hiện nay là hoàn toàn miễn phí, nhưng đổi lại theo điều khoản sử dụng dịch vụ, người dùng sẽ phải chia sẻ thông tin cá nhân của mình với nhà cung cấp dịch vụ và có thể là với cả các bên đối tác của trang mạng này. Tuy không phải trả tiền, nhưng các quảng cáo của bên thứ ba thường hướng đến các người dùng phù hợp với các đặc điểm nhân thân của họ. Những hành động tương tác (like hay comment) đều được lưu lại, phân tích thông qua những thuật toán để làm rõ người dùng này quan tâm đến điều gì, từ đó, những quảng cáo sẽ xuất hiện tương ứng. Không sai khi cho rằng, các mạng xã hội đã “bán dữ liệu cá nhân” của người dùng cho các hãng quảng cáo.

*- Nguy cơ đến từ các điều kiện giao dịch khó hiểu*

Nguy cơ này đến từ một bên thứ ba, có thể do chính các tổ chức, cá nhân này tự ý thu thập thông tin về người tiêu dùng. Có không ít các ứng dụng trò chơi đặt ra các tùy chọn để người dùng quyết định đồng ý cho chúng truy cập thông tin cá nhân trên các tài khoản mạng xã hội thì mới được sử dụng ứng dụng đó. Chẳng hạn các ứng dụng bói toán đòi người dùng Facebook phải cho truy cập danh sách bạn bè, số điện thoại, email thì người dùng mới được thực hiện việc bói. Sau khi thu thập được dữ liệu, chủ sở hữu ứng dụng kia làm điều gì, người dùng khó có thể kiểm soát. Đã có không ít các vụ hack tài khoản mạng xã hội để lừa đảo chiếm đoạt thẻ nạp tiền điện thoại trả trước bị phát hiện và những hậu quả bất lợi cho người dùng còn chưa thể biết có dừng lại ở đó hay không.

Hiện nay, các điều kiện giao dịch chung phải đăng ký tại cơ quan quản lý ngành công thương chỉ dừng ở phạm vi 9 hàng hóa, dịch vụ thiết yếu theo Nghị định 99/2011/NĐ-CP của Chính phủ; Quyết định 02/2012/QĐ-TTg; Quyết định 35/2015/QĐ-TTg, Quyết định 38/2018/QĐ-TTg của Thủ tướng Chính phủ là: cung cấp điện sinh hoạt; cung cấp nước sạch sinh hoạt; truyền hình trả tiền; thuê bao điện thoại cố định; thuê bao di động trả sau, dịch vụ thông tin di động mặt đất (hình thức thanh toán: trả trước); kết nối Internet; vận chuyển hành khách đường hàng không; vận chuyển hành khách đường sắt; mua bán căn hộ chung cư, các dịch vụ sinh hoạt do đơn vị quản lý khu chung cư cung cấp. Đây là một lượng rất nhỏ các loại điều kiện giao dịch chung mà người tiêu dùng phải đối mặt trong các giao dịch.

Ngoài thủ tục đăng ký tại các cơ quan công thương, việc khởi kiện các điều kiện giao dịch chung không công bằng với người tiêu dùng chưa thể thực hiện bởi hình thức khởi kiện tập thể, khởi kiện của tổ chức bảo vệ người tiêu dùng chưa được thừa nhận chính thức.

*- Dữ liệu không chỉ có trên môi trường mạng*

Có thể thấy môi trường mạng là nơi có nhiều rủi ro nhất, tuy nhiên dữ liệu cá nhân nói chung và thông tin người tiêu dùng nói riêng được khai báo và quản lý ở những nền tảng khác. Ngay cả trong trường hợp thu thập thông tin không vì mục đích thương mại như hồ sơ công dân tại các cơ quan quản lý, nếu không được kiểm soát, chúng hoàn toàn có thể bị truy cập và sử dụng cho các mục đích thương mại, ví dụ: dữ liệu đăng ký khai sinh hoàn toàn có thể bị lạm dụng, khai thác trong các hoạt động tiếp thị thực phẩm và đồ dùng trẻ em. Do vậy, Luật An toàn thông tin mạng, Luật An ninh mạng, tuy đã rất cố gắng tiến tới chuẩn mực thế giới nhưng vẫn không thể coi là đủ. Gần đây, đề xuất của Ủy ban nhân dân thành phố Hà Nội về việc thí điểm thu giá dịch vụ đối với việc cung cấp, chia sẻ các dữ liệu dân cư đối với các ngành như ngân hàng, công chứng và một số lĩnh vực khác[25], về bản chất là bán dữ liệu của công dân cho doanh nghiệp mà chưa được sự đồng thuận của họ.

**6. Kiến nghị**

Quyền riêng tư của người tiêu dùng sẽ không thể được bảo vệ một cách nghiêm túc nếu các quyền nhân thân, quyền bí mật đời tư trong luật dân sự không được thực thi. Điều cần làm trước tiên là ghi nhận và thực hiện những nguyên tắc thực hành thông tin đúng mực FIPPs của tất cả các chủ thể thu thập, quản lý và sử dụng các thông tin cá nhân, kể cả các cơ quan quản lý nhà nước.

Từ góc độ pháp lý, để giải quyết vấn đề bảo vệ quyền riêng tư của người tiêu dùng, cần kiểm soát chặt chẽ các điều khoản sử dụng dịch vụ để bảo đảm sự “đồng ý” hay “cho phép” truy cập và khai thác các dữ liệu cá nhân mang tính thực chất; cần mở rộng thêm phạm vi kiểm soát các điều kiện giao dịch chung, không nên chỉ dừng ở 9 hàng hóa, dịch vụ như hiện nay bởi nguy cơ mất an toàn thông tin của người tiêu dùng có thể xảy ra ở bất cứ các giao dịch nào.

Mặc dù các chế tài xử lý của Việt Nam không nhẹ, nhưng hầu như chỉ được áp dụng khi có thiệt hại lớn. Các trường hợp khác, rất ít khi các nạn nhân lên tiếng. Nên chăng, trao quyền theo dõi, khiếu nại, khởi kiện cho các tổ chức bảo vệ người tiêu dùng để kịp thời phát hiện và lên tiếng, yêu cầu cơ quan nhà nước bảo vệ. Điều này sẽ tăng khả năng phát hiện các vi phạm từ chính các đối tượng được bảo vệ.

Cơ chế khởi kiện tập thể của người tiêu dùng, khởi kiện của các tổ chức xã hội bảo vệ người tiêu dùng cũng cần được cân nhắc và quy định chi tiết bởi không có cơ quan quản lý nào có thể thực hiện hết việc cho đăng ký các điều kiện giao dịch chung và kiểm soát chúng có vi phạm quyền riêng tư của người tiêu dùng hay không; thu hút sự tham gia của khu vực tư vào giải quyết vấn đề chung là cách làm phù hợp hiện nay, không chỉ vì việc tiết kiệm ngân sách nhà nước./.

[1] Theo Luật Bảo vệ quyền lợi của người tiêu dùng 2010, tại Điều 3.1. “người tiêu dùng” không được định nghĩa là các cá nhân mà chỉ là “người” một cách chung chung. Điều này hàm ngụ có thể các tổ chức hoặc nhóm cá nhân mua hàng hóa, dịch vụ cho mục đích tiêu dùng cũng được xem là “người tiêu dùng”.

[2] Xem thêm: Alan Westin, *Privacy and Freedom,* Bodley Head, 1970, trang 7.

[3] UDHR 1948, Điều 12.

[4] ICCPR 1966, Điều 17.1.

[5] Chưa có khái niệm tương tự ở Việt Nam nên trong khuôn khổ đề tài này chúng tôi tạm dịch *fair information practices* là *những hoạt động thông tin đúng mực* để diễn tả tính chất tử tế, tôn trọng quyền con người, tôn trọng pháp luật và tôn trọng các giá trị đạo đức, nhân văn.

[6] US Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers and the Rights of Citizens, Chapter IV: Recommended Safeguards for Administrative Personal Data Systems (1973).

[7] Fred H. Cate: The Failure ofFair Information Practice Principles, in trong cuốn: Consumer protection in the age of “information economy”, edited by Jane K. Winn, Ashgate Publishing Ltd. 2006, p. 341

[8] GDPR, điều 6.

[9] GDPR, điều 7.3. và 7.4.

[10] GDPR, điều 83.4

[11] GDPR, điều 83.5 và 83.6.

[12] BEUC, Thông cáo báo chí ngày 27/11/2018 tại: <https://www.beuc.eu/publications/consumer-groups-across-europe-file-complaints-against-google-breach-gdpr/html>, truy cập ngày 30/11/2018.

[13] Graham Greenleaf: *Global data privacy laws: 89 countries, and accelerating,* Queen Mary University of London, School of LawLegal Studies Research Paper No. 98/2012, p. 1.

[14] Hiến pháp 2013, Điều 21.1.

[15] Bộ luật Dân sự 2015, Điều 38.

[16] Luật Giao dịch điện tử 2005, Điều 46.2.

[17] Luật Bảo vệ quyền lợi người tiêu dùng 2010, Điều 6.

[18] Luật An toàn thông tin mạng, Điều 18.

[19] Luật An toàn thông tin mạng, Điều 20.1.

[20] Luật An ninh mạng 2018, điều 17.

[21] Nghị định 174/2013/NĐ-CP, Điều 66.5.a.

[22] Bộ luật Hình sự 2015, sửa đổi 2017, Điều 288.

[23] Nghị định 174/2013/NĐ-CP, Điều 73.

[24] Bộ luật Hình sự 2015, sửa đổi 2017, Điều 159.

[25] *Hà Nội đề nghị chia sẻ dữ liệu dân cư cho các ngành khác để thu tiền,* tại <https://thanhnien.vn/thoi-su/ha-noi-de-nghi-chia-se-du-lieu-dan-cu-cho-cac-nganh-khac-de-thu-tien-979148.html>, truy cập ngày 30/11/2018.

***Bài viết được đăng tải trên Ấn phẩm Tạp chí Nghiên cứu Lập pháp số 12 (388), tháng 6/2019***