QUYỀN RIÊNG TƯ VÀ BẢO VỆ DỮ LIỆU CÁ NHÂN[1]

Danny Duy Vo

Luật sư, Mekong Vime JSC Group

Nguyễn Thị Thu Trang

Giảng viên, Trường Đại học Kinh tế - Tài chính Tp. Hồ Chí Minh

Tóm tắt: Sự phát triển của trí tuệ nhân tạo (Artificial Intelligence - AI) và phát triển của mạng xã hội tác động tới nhiều mặt của đời sống xã hội. Tuy vậy, sự hình thành AI và phát triển của mạng xã hội trong cuộc sống có thể xâm phạm tới quyền riêng tư nói chung và dữ liệu cá nhân nói riêng. Bài viết này đề cập tới Quy định chung về bảo vệ dữ liệu của Châu Âu (GDPR) và Hoa Kỳ để thấy được những ưu điểm và bất cập. Từ đó, tác giả rút ra bài học kinh nghiệm cho Việt Nam nhằm bảo vệ hiệu quả dữ liệu cá nhân và quyền riêng tư trong kỷ nguyên số.

Từ khóa: *quyền riêng tư, bảo vệ dữ liệu cá nhân, EU, Hoa Kỳ.*

1. Quyền riêng tư và dữ liệu cá nhân dưới góc nhìn của pháp luật quốc tế

Quyền riêng tư và dữ liệu cá nhân của cá nhân được pháp luật bảo vệ và bất khả xâm phạm. Đây là quyền nhân thân gắn liền với mỗi cá nhân. Theo đó, Quyền riêng tư nói chung và quyền được bảo vệ dữ liệu cá nhân nói riêng là quyền cơ bản của con người. Cụ thể:

Tại Điều 12 Tuyên ngôn Nhân quyền quốc tế năm 1948 (UDHR) như sau: "*Không ai phải chịu sự can thiệp một cách tuỳ tiện vào cuộc sống riêng tư, ... Mọi người đều được pháp luật bảo vệ chống lại sự xúc phạm và can thiệp như vậy*".

Tiếp đến, tại Công ước quốc tế về các quyền Dân sự và Chính trị (ICCPR) 1966 một lần nữa khẳng định tại Điều 17 rằng: ""*Không ai bị can thiệp một cách tuỳ tiện hoặc bất hợp pháp vào đời sống riêng tư, gia đình, nhà ở, thư tín, hoặc bị xâm phạm bất hợp pháp đến danh dự và uy tín. Mọi người đều có quyền được pháp luật bảo vệ chống lại những can thiệp hoặc xâm phạm như vậy"*. Trong đó, Điều 17 (ICCPR) được làm rõ khá chi tiết về việc bảo vệ quyền riêng tư tại Bình luận

[1] Một phần nội dung về dữ liệu cá nhân trong bài viết này kế thừa kết quả nghiên cứu của tác giả Nguyễn Thị Thu Trang được công bố tại: Nguyễn Thị Thu Trang (2022), "Bảo vệ dữ liệu cá nhân trong kỷ nguyên trí tuệ nhân tạo - Kinh nghiệm của Châu Âu và kiến nghị hoàn thiện pháp luật Việt Nam", *Tạp chí Luật học*, 10(269).

chung số 16 thông qua tại phiên họp lần thứ 31 năm 1988 của Ủy ban Nhân quyền Liên Hợp Quốc: (i) Mục đích: nhằm 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 các thể nhân và pháp nhân khác gây ra (đoạn 1). (ii) Nghĩa vụ của các quốc gia thành viên: Các quốc gia thành viên có nghĩa vụ ngăn chặn cả các quan chức nhà nước và các thể nhân hay pháp nhân khác có những hành động xâm phạm tùy tiện và bất hợp pháp như vậy (đoạn 9). (iii) Ngoại lệ: những can thiệp hợp pháp vào đời tư phải được quy định trong pháp luật, và phải phù hợp với các quy định khác của ICCPR (đoạn 3). Rõ ràng, theo quy định ở Điều 17 tiếp cận quyền riêng tư sau:

Thứ nhất, về thư tín: tính toàn vẹn và bảo mật của thư tín phải được bảo đảm cả về mặt pháp lý và thực tế. Thư phải được giao tận tay người nhận mà không bị chặn lại hoặc xâm phạm. Ngoài ra, việc theo dõi, đọc hoặc các biệt pháp khác thông qua AI hoặc nền tảng mạng xã hội nhằm xâm phạm tới thư tín đều bị coi là xâm phạm tới đời sống riêng tư của cá nhân – hành vi bất hợp pháp.

Thứ hai, về nơi ở: Việc xâm phạm nơi ở cũng được xem là xâm phạm tới quyền riêng riêng tư trừ các trường hợp ngoại lệ nêu trên.

Thứ ba, về thân thể: Việc khám xét thân thể phải theo cách thức phù hợp để bảo đảm nhân phẩm của người bị khám xét; người khám xét phải cùng giới tính với người bị khám xét.[2]

Thứ tư, về thu thập và lưu giữ thông tin[3]: việc thu thập và lưu giữ các thông tin cá nhân trong máy tính, các ngân hàng dữ liệu và các thiết bị khác, cho dù là bởi các quan chức nhà nước hay các thể nhân, pháp nhân khác, đều phải được quy định trong pháp luật. Nhà nước phải có những biện pháp hiệu quả để bảo đảm rằng những thông tin cá nhân đó không rơi vào tay những người không được pháp luật cho phép và không bị sử dụng vào các mục đích trái với Công ước. Để bảo đảm bảo vệ đời tư một cách hiệu quả, mỗi cá nhân cần có quyền được biết liệu thông tin cá nhân của mình có bị thu thập, lưu giữ bởi chủ thể nào không và nếu có, thì ở đâu, nhằm mục đích gì, chủ thể quản lý thông tin cá nhân của mình là ai? 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. Vì sự an toàn của tất cả mọi người trong xã hội, quyền về sự riêng tư không phải là quyền tuyệt đối. Tuy nhiên, các quốc gia chỉ nên thu thập thông tin về đời tư nếu như những thông tin đó là thiết yếu để bảo đảm lợi ích chung của xã hội như được thừa nhận trong ICCPR.

Như đã nêu ở trên, với sự phát triển mạnh mẽ của AI và mạng xã hội, với mục đích khác

[2] Đoạn 8, Bình luận chung số 16 thông qua tại phiên họp lần thứ 31 năm 1988 của Ủy ban Nhân quyền Liên Hợp Quốc.
[3] Đoạn 10, Bình luận chung số 16 thông qua tại phiên họp lần thứ 31 năm 1988 của Ủy ban Nhân quyền Liên Hợp Quốc

nhau của khối tư nhân cũng như nhà nước, quyền riêng nói chung và dữ liệu cá nhân nói riêng của con người đã, đang và sẽ bị xâm phạm. Vì vậy, xây dựng hành lang pháp lý ở quốc gia, khu vực và toàn cầu nhằm bảo vệ quyền riêng tư và dữ liệu cá nhân trong kỷ nguyên trí tuệ nhân tạo là thực sự cần thiết. Trong phạm vi bài viết này, chúng tôi đề cập tới quy định về pháp luật của EU và Hoa Kỳ để thấy được điểm phù hợp và bất cập. Từ đó, chúng tôi có cơ sở để đề xuất những giải pháp, kiến nghị nhằm bảo vệ hiệu quả quyền riêng tư và dữ liệu cá nhân và giúp hoàn thiện pháp luật Việt Nam về vấn đề nêu trên.

2. Bảo vệ quyền riêng tư và dữ liệu cá nhân theo pháp luật Hoa Kỳ và EU

Pháp luật Hoa Kỳ bảo vệ quyền riêng tư và dữ liệu cá nhân tương đối toàn diện. Hệ thống pháp luật Hoa Kỳ có nhiều văn bản pháp luật quy định về bảo vệ quyền riêng tư và dữ liệu cá nhân: Luật riêng tư về y tế (Health privacy laws); Luật riêng tư về tài chính (Financial privacy laws); Luật riêng tư trên Internet (Online privacy laws); Luật riêng tư trong giao tiếp (Communication privacy laws); Luật riêng tư thông tin (Information privacy laws); Bảo vệ riêng tư tại nhà (Privacy in one's home).

Các nước thuộc Liên minh Châu Âu (EU) cũng có những văn bản quy định về bảo vệ quyền riêng tư và dữ liệu cá nhân khá toàn diện. Trong đó, Quy định chung về bảo vệ dữ liệu (General Data Protection Regulation - GDPR) - Luật bảo vệ dữ liệu mới của Liên minh Châu Âu có hiệu lực vào ngày 25 tháng 5 năm 2018 là văn bản nổi bật về bảo vệ dữ liệu cá nhân. GDPR áp dụng cho các tổ chức thuộc Liên minh Châu Âu và ngoài Liên minh Châu Âu sử dụng hoặc xử lý dữ liệu cá nhân về những người sống ở Liên minh Châu Âu.[4] Các quy định của GDPR được điều chỉnh để phù hợp với những thay đổi trong công nghệ; nhóm thông tin được sử dụng để giao dịch trên kênh ảo; tính chất xuyên biên giới của việc thu thập, xử lý và sử dụng cơ sở dữ liệu.[5] Nhiệm vụ chính của GDPR là đảm bảo quyền riêng tư của các thể nhân, với quy định cụ thể sau: (i) Đối tượng được bảo vệ là cá nhân; (ii) Nguyên tắc xử lý dữ liệu cá nhân công bằng, minh bạch,…; (iii) Nêu lên điều kiện xử lý dữ liệu hợp pháp; (iv) Quyền truy cập, cải chính và lãng quên, … của chủ thể dữ liệu; (v) Nghĩa vụ của các bên liên quan (người kiểm soát, người xử lý và người bảo vệ dữ liệu) tới dữ liệu cá nhân; (vi) Hoạt động của cơ quan giám sát và Hội đồng bảo vệ dữ liệu cá nhân; (vii) Trách nhiệm pháp lý của chủ thể vi phạm.

3. Thực trạng bảo vệ quyền riêng tư và dữ liệu cá nhân tại Việt Nam

[4] See Commission Regulation 2016/679 of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR], Art. 3(1) and 3(2).

[5] See Mazurek, G. & Małagocka, K. (2019), "Are we down to zero-one code? Perception of privacy and data protection in the context of the development of artificial intelligence", *Journal of Management Analytics*, Vol.6 (4), p. 351.

Thứ nhất, chưa thống nhất cách hiểu về "bí mật đời tư": Theo điều 38 Bộ luật Dân sự năm 2015 ghi nhận: "đời sống riêng tư, bí mật cá nhân, bí mật gia đình là bất khả xâm phạm và được pháp luật bảo vệ". Theo đó: (i) 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, trừ trường hợp luật có quy định khác. (ii) Đối với, thư tín, điện thoại, điện tín, cơ sở dữ liệu điện tử và các hình thức trao đổi thông tin riêng tư khác của cá nhân được bảo đảm an toàn và bí mật. Việc bóc mở, kiểm soát, thu giữ thư tín, điện thoại, điện tín, cơ sở dữ liệu điện tử và các hình thức trao đổi thông tin riêng tư khác của người khác chỉ được thực hiện trong trường hợp luật quy định. (iii) 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, trừ trường hợp có thỏa thuận khác.

Hiện nay chưa có định định cụ thể về "bí mật đời tư" do đó trên thực có nhiều quan điểm khác nhau về vấn đề này. Chính điều này dẫn đến vướng mắc, khó khăn trong việc xác định hành vi xâm phạm bí mật đời tư.

Thứ hai, Việt Nam không có đạo luật hoặc văn bản pháp lý riêng biệt quy định về bảo vệ dữ liệu cá nhân. Quy định về bảo vệ dữ liệu cá nhân được ghi nhận rải rác ở nhiều văn bản pháp luật khác nhau tại Việt Nam. Theo quy định tại Điều 21 Hiến pháp năm 2013, mọi người có quyền bất khả xâm phạm về đời sống riêng tư, trong đó bao gồm cả bí mật cá nhân, bí mật gia đình, bí mật thư tín, điện thoại, điện tín và các hình thức trao đổi thông tin riêng tư khác. Với quy định này, Hiến pháp Việt Nam xác định bảo vệ quyền riêng tư cũng chứa đựng bảo vệ dữ liệu cá nhân. Các văn bản pháp luật khác đã cụ thể hóa về bảo vệ quyền riêng tư như: Bộ luật Dân sự, Bộ luật Hình sự, Bộ luật Tố tụng hình sự, Bộ luật Tố tụng dân sự, Luật Xuất bản, Luật Phòng, chống HIV/AID, ... Một số văn bản pháp luật của Việt Nam ghi nhận rõ hơn về bảo vệ dữ liệu cá nhân như Luật an toàn thông tin mạng, Luật an ninh mạng, Luật công nghệ thông tin, ... nhưng thiếu tính hệ thống:

(i) Luật an toàn thông tin mạng dành Mục 2 gồm 5 điều (Điều 16-22) để quy định về bảo vệ thông tin cá nhân. Theo đó, chủ thể xử lý thông tin cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng đối với thông tin do mình xử lý; xây dựng và công bố công khai biện pháp xử lý, bảo vệ thông tin cá nhân.[6]Chủ thể xử lý thông tin cá nhân có trách nhiệm thu thập thông tin cá nhân 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; sử dụng thông tin đúng mục đích; Không được cung cấp, chia sẻ, phát tán thông tin cá

[6] Xem Điều 16 (2&3) Luật an toàn thông tin mạng Việt Nam 2015.

nhân mà mình đã thu thập, tiếp cận, kiểm soát cho bên thứ ba trừ trường hợp luật có quy định khác.[7] Ngoài ra, 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.[8] 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.[9]Rõ ràng, các quy định của Luật an toàn thông tin mạng Việt Nam tương đồng với những quy định của GDPR về bảo vệ thông tin cá nhân.

(ii) Luật công nghệ thông tin: Tổ chức, cá nhân tham gia phát triển công nghệ thông tin có trách nhiệm bảo đảm quyền và lợi ích hợp pháp của chủ sở hữu cơ sở dữ liệu và không gây cản trở cho việc sử dụng cơ sở dữ liệu đó khi thực hiện hành vi tái sản xuất, phân phối, quảng bá, truyền đưa, cung cấp nội dung hợp thành cơ sở dữ liệu đó.[10]Việc thu thập, xử lý va ứng dụng thông tin cá nhân trên môi trường mạng phải được sự đồng ý của cá nhân đó. Chủ thể thu thập, xử lý và ứng dung thông tin có trách nhiệm: Thông báo cho người đó biết về hình thức, phạm vi, địa điểm và mục đích của việc thu thập, xử lý và sử dụng thông tin cá nhân của người đó; Sử dụng đúng mục đích thông tin cá nhân thu thập được và chỉ lưu trữ những thông tin đó trong một khoảng thời gian nhất định theo quy định của pháp luật hoặc theo thoả thuận giữa hai bên; Tiến hành các biện pháp quản lý, kỹ thuật cần thiết để bảo đảm thông tin cá nhân không bị mất, đánh cắp, tiết lộ, thay đổi hoặc phá huỷ; Tiến hành ngay các biện pháp cần thiết khi nhận được yêu cầu kiểm tra lại, đính chính hoặc hủy bỏ theo quy định của pháp luật; Không được cung cấp thông tin cá nhân của người khác cho bên thứ ba trừ trường hợp pháp luật có quy định khác.[11]Qua các quy định nêu trên cho thấy, Luật công nghệ thông tin Việt Nam tương đồng với những quy định của GDPR về bảo vệ thông tin cá nhân.

(iii) Luật an ninh mạng: Chủ quản hệ thống thông tin có trách nhiệm triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn, phối hợp xử lý hành vi gián điệp mạng, xâm phạm bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin và kịp thời gỡ bỏ thông tin liên quan đến hành vi này.[12] Doanh nghiệp cung cấp dịch vụ trên không gian mạng tại Việt Nam có trách nhiệm áp dụng các giải pháp kỹ thuật và các biện pháp cần thiết khác nhằm bảo

[7] Xem Điều17 (1) Luật an toàn thông tin mạng Việt Nam 2015.
[8] Xem Điều17 (1) Luật an toàn thông tin mạng Việt Nam 2015.
[9] Xem Điều 17 (1) Luật an toàn thông tin mạng Việt Nam 2015.
[10] Xem Điều 9(2b) Luật công nghệ thông tin Việt Nam 2006.
[11] Xem Điều 21(2) & 22(2) Luật công nghệ thông tin Việt Nam 2006.
[12] Xem Điều 17(2b-c) Luật an nịnh mạng Việt Nam 2018.

đảm an ninh cho quá trình thu thập thông tin, ngăn chặn nguy cơ lộ, lọt, tổn hại hoặc mất dữ liệu; trường hợp xảy ra hoặc có nguy cơ xảy ra sự cố lộ, lọt, tổn hại hoặc mất dữ liệu thông tin người sử dụng, cần lập tức đưa ra giải pháp ứng phó, đồng thời thông báo đến người sử dụng.[13]Những quy định này của Luật an ninh mạng Việt Nam tương đồng với quy định của GDPR về bảo vệ dữ liệu cá nhân.

Thứ ba, một số văn bản quy định về trách nhiệm pháp lý đối với chủ thể vi phạm dữ liệu cá nhân: (i) Trách nhiệm bồi thường thiệt hại: Chủ thể gây thiệt hại do vi phạm quy định về bảo vệ quyền riêng tư nói chung và dữ liệu cá nhân nói riêng được quy định trong Bộ luật Dân sự Việt Nam và các luật chuyên ngành liên quan. (ii) Trách nhiệm hành chính: Theo Nghị định số 15/2020/NĐ-CP quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử, mức phạt cao nhất là 70 triệu đồng đối với hành vi vi phạm quy định về bảo đảm an toàn thông tin cá nhân trên mạng.[14] (iii) Trách nhiệm hình sự: Đối với tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông, người phạm tội có thể bị phạt cao nhất đến 200 triệu đồng.[15] Rõ ràng, các loại trách nhiệm pháp lý được áp dụng đối với chủ thể vi phạm theo pháp luật Việt Nam là tương đồng với GDPR. Tuy vậy, mức phạt hành chính và hình sự áp dụng đối với chủ thể vi phạm là khá thấp so với quy định của GDPR (lên tới 20 triệu euro).

Thứ tư, trách nhiệm pháp lý do xâm phạm quyền riêng tư: Hành vi xâm phạm bí mật đời tư là hành vi vi phạm pháp luật, tùy vào mức độ sẽ bị xử phạt hành chính hoặc truy cứu trách nhiệm hình sự. Các hành vi dưới đây thường xâm phạm quyền riêng tư như: Đăng hồ sơ cá nhân của người khác lên các mạng xã hội; dùng các giấy tờ tùy thân của người khác mà không xin phép; Đăng ảnh riêng tư lên mạng; Chia sẻ các tư liệu trong cơ quan/ công ty khi không được phép; Công bố chuyện riêng tư của người khác;…[16]

Thứ năm, thói quen của người dân: Người dân chưa hiểu về quyền riêng tư và dữ liệu cá nhân. Có nhiều người cho rằng họ có quyền tự do, tự cho là ngôn luận nên có hành động can thiệp vào quyền riêng tư của chủ thể khác. Cụ thể, các cá nhân thu thập, sử dụng, công khai các thông tin liên quan đến quyền riêng tư của người khác mà không được người đó đồng ý.

4. Một số giải pháp, kiến nghị nhằm bảo vệ hiệu quả quyền riêng tư và dữ liệu cá nhân.

[13] Xem Điều 41(1c) Luật an ninh mạng Việt Nam 2018.
[14] Xem Điều 86 Nghị định số 15/2020/NĐ-CP quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử.
[15] Xem Điều 288 Bộ luật hình sự Việt Nam 2015, sửa đổi năm 2017.
[16] Hành vi ít chưa nguy hiểm sẽ truy cứu trách nhiệm hành chính. Hành vi nguy hiểm cho xã hội có thể áp dụng Điều 159 Bộ luật Hình sự 2015 sửa đổi năm 2017 để truy cứu trách nhiệm pháp lý.

Việt Nam đang chuyển mình một cách nhanh chóng sang nền kinh tế số. Với sự tăng trưởng của thương mại điện tử, những quá trình "số" hóa nhanh chóng này đã ảnh hưởng nhiều đến đời sống riêng tư và dữ liệu cá nhân của người dân. Năm 2023, Chính phủ đã ban hành Nghị định 13/2023/NĐ-CP để điều chỉnh các quan hệ phát sinh từ việc thu thập, xử lý dữ liệu cá nhân. Ghi nhận thêm 11 quyền mới cho cá nhân (điều 9), Nghị định 13/2023 là quyết sách kịp thời của nhà quản lý để kỹ trị và đảm bảo quyền riêng tư của người dân trong bối cảnh mới.

Với chiến lược phát triển AI đến năm 2030 của Việt Nam được nêu ở trên cho thấy Việt Nam đã, đang và sẽ phát triển AI mạnh mẽ. Sự phát triển AI và mạng xã hội sẽ kéo theo yêu cầu bảo vệ quyền riêng tư và dữ liệu cá nhân. Hệ thống pháp luật Việt Nam hiện hành chưa quy định một cách toàn diện và phù hợp đối với chủ thể vi phạm dữ liệu cá nhân. Từ thực trạng pháp luật Việt Nam, so sánh và tham khảo quy định bảo vệ dữ liệu của EU và Hoa Kỳ, chúng tôi đề xuất một số giải pháp và kiến nghị sau:

Thứ nhất, hệ thống hóa thành một văn bản pháp luật riêng nhằm bảo vệ dữ liệu cá nhân. Nên chăng, Việt Nam xây dựng Luật bảo vệ dữ liệu với những nội dung chính tham khảo GDPR của EU và Hoa Kỳ, cụ thể: (1) Chủ thể dữ liệu được bảo vệ: cá nhân công dân Việt Nam hoặc những người đang cư trú tại Việt Nam. (ii) Đối tượng bảo vệ: dữ liệu vị trí, số nhận dạng trực tiếp và các dạng thông tin khác có thể được sử dụng để xác định chủ thể dữ liệu một cách trực tiếp hoặc gián tiếp, ngoài dữ liệu nhận dạng cổ điển như tên và số nhận dạng của cá nhân. (iii) Các nguyên tắc bảo vệ dự liệu: hợp pháp, công khai, minh bạch, đúng mục đích, giới hạn mục đích,... (iv) Quyền chủ thể dữ liệu: truy cập, chuyển dữ liệu, điều chỉnh, xóa, lãng quên,… (v) Nhiệm vụ và quyền hạn của các chủ thể bảo vệ dữ liệu: người kiểm soát, người xử lý, người bảo vệ dữ liệu, ... (vi) Nhiệm vụ quyền hạn của cơ quan bảo vệ dữ liệu: Cơ quan giám sát bảo vệ giữ liệu quốc gia. (vii) Trách nhiệm pháp lý do vi phạm bảo vệ dữ liệu: bồi thường thiệt hại, hành chính và hình phạt. (viii) Các quy định liên quan khác.

Thứ hai, thành lập cơ quan giám sát xử lý dữ liệu (Cơ quan bảo vệ dữ liệu) chuyên trách. Các quốc gia thuộc EU cũng thành lập các cơ quan chuyên trách để bảo vệ dữ liệu như: Latvia thành lập cơ quan thanh tra nhà nước về dữ liệu Latvia; Tây Ban Nha thành lập Cơ quan bảo vệ dữ liệu; Pháp thành lập Ủy ban quốc gia về tin học và tự do; Bỉ thành lập Ủy ban bảo mật dữ liệu, ... Việc thành lập cơ quan bảo vệ dữ liệu độc lập giúp hoạt động giám sát, bảo vệ dữ liệu trong nước đạt hiệu quả cao. Thêm vào đó, cơ quan bảo vệ dữ liệu này là đầu mối hợp tác với các cơ quan bảo vệ dữ liệu của các quốc gia khác trong việc giám sát xử lý dữ liệu ở nước ngoài nhưng liên quan đến dữ liệu của công dân quốc gia mình. Chính vì lẽ đó, Việt Nam nên thành lập cơ quan bảo vệ dữ liệu

độc lập thuộc hệ thống cơ quan thanh tra hoặc thuộc Bộ khoa học công nghệ.

Thứ ba, những quy định về bảo vệ dữ liệu cá nhân hiện được quy định trong các luật như Luật an ninh mạng, Luật an toàn thông tin mạng, Luật công nghệ thông tin, Luật bảo vệ quyền lợi người tiêu dùng, … sẽ được pháp điển hóa vào quy định của Luật bảo vệ dữ liệu Việt Nam.

Thứ tư, nâng mức xử phạt hành chính và hình sự đối với chủ thể có hành vi vi phạm dữ liệu cá nhân. Bởi vì, những vi phạm trong lĩnh vực công nghệ nói chung và AI nói riêng về bảo vệ dữ liệu cá nhân có tác động rất lớn đến đời sống của chủ thể dữ liệu và đến trật tự công cộng. Do đó, nâng mức xử phạt hành chính và hình sự đối với hành vi vi phạm này là thực sự cần thiết để trừng phạt đối với chủ thể vi phạm và răn đe đối với chủ thể khác.

Thứ năm, tuyên truyền để nâng cao ý thức của người dân trong việc tôn trọng và bảo vệ quyền riêng tư và dữ liệu cá nhân.

Thứ sáu, "bí mật đời tư" có thể hiểu là bí mật đời sống riêng tư, bí mật cá nhân, bí mật gia đình.

TÀI LIỆU THAM KHẢO

1. Bộ luật hình sự Việt Nam 2015, sửa đổi năm 2017.
2. Bộ luật Dân sự 2015
3. Bình luận chung số 16 thông qua tại phiên họp lần thứ 31 năm 1988 của Ủy ban Nhân quyền Liên Hợp Quốc.
4. Công ước quốc tế về các quyền Dân sự và Chính trị (ICCPR) 1966
5. Commission Regulation 2016/679 of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
6. Luật an toàn thông tin mạng Việt Nam 2015.
7. Luật công nghệ thông tin Việt Nam 2006.
8. Luật an ninh mạng Việt Nam 2018.
9. Nghị định số 15/2020/NĐ-CP quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử.
10. Tuyên ngôn Nhân quyền quốc tế năm 1948 (UDHR)

11. Mazurek, G. & Małagocka, K. (2019), "Are we down to zero-one code? Perception of privacy and data protection in the context of the development of artificial intelligence", *Journal of Management Analytics*, Vol.6 (4).