MỘT SỐ VẤN ĐỀ VỀ BẢO VỆ QUYỀN RIÊNG TƯ TRONG KHÔNG GIAN INTERNET

Lã Khánh Tùng

Khoa Luật-ĐHQGHN

Internet ngày càng đóng vai trò quan trọng trong đời sống nhân loại, có vai trò tích cực thúc đẩy dân chủ, tự do và các quyền con người. Cạnh đó, Internet đặt ra nhiều vấn đề, thách thức, trong đó có những thách thức liên quan đến việc bảo vệ quyền riêng tư của cá nhân. Bài viết này phân tích sơ bộ khuôn khổ pháp lý toàn cầu về quyền riêng tư trên Internet, thực tiễn xung đột giữa bảo vệ quyền riêng tư với an ninh công cộng tại một số quốc gia, và nêu bật một khoảng trống pháp lý ở Việt Nam bảo vệ chống lại sự xâm phạm quyền riêng tư trên không gian Internet, đặc biệt là việc giới hạn quyền chưa được quy định đầy đủ trong luật, trái với nguyên tắc nêu tại Hiến pháp 2013 "quyền con người, quyền công dân chỉ có thể bị hạn chế theo quy định của luật" (Khoản 2, Điều 14).

I. KHÁI QUÁT VỀ INTERNET VÀ QUYỀN RIÊNG TƯ

1. Khuôn khổ pháp luật quốc tế

Từ một mạng lưới của Bộ Quốc phòng Hoa Kỳ được hình thành từ cuối thập niên 1960, Internet đã trở thành một mạng lưới truyền thông toàn cầu thiết yếu. Do tính chất xuyên biên giới của nó, Internet khiến cho rất khó, nhiều khi là không thể, xác định được thông tin đã được chuyển đến những ai, ở những quốc gia nào. Tốc độ và phạm vi truyền tải Internet cũng diễn ra rất nhanh, vượt ra ngoài tầm kiểm soát của một người chỉ trong thời gian không đến một giây.[1]

Việc bảo vệ quyền riêng tư trong không gian kỹ thuật số được quan tâm ở quy mô quốc tế dường như chậm hơn so với pháp luật nhiều quốc gia. Pháp luật nhiều nước đã phát triển nhanh chóng để điều chỉnh lĩnh vực này. Một số nước mở rộng phạm vi điều

[1] Xem thêm: Toby Mendel et al, *Global Survey on Internet Privacy and Freedom of Expression*, UNESCO, 2012, trang 51.

chỉnh của luật về dữ liệu cá nhân, như Luật Bảo vệ Dữ liệu cá nhân của Pháp 1978, Luật Bảo vệ Dữ liệu cá nhân của Arghentina 2000...Hoa Kỳ áp dụng Luật Riêng tư Truyền thông điện tử (Electronic Communication Privacy Act – ECPA, 1986), trong truyền thống chỉ áp dụng đối với các hành vi nghe lén điện thoại, nay mở rông sang áp dụng bảo vệ chống lại việc theo dõi trực tuyến. Quốc gia này cũng ban hành Luật Bảo vệ riêng tư trực tuyến của trẻ em (2000), Luật Bảo vệ riêng tư và dữ liệu điện thoại (2006)...Tuy nhiên, Luật An ninh Nội địa (thường được gọi là PATRIOT Act) đã làm suy giảm nhiều quy định bảo vệ quyền riêng tư, gồm cả các quy định trong ECPA.

Ở phạm vi khu vực, Liên minh châu Âu đã đi đầu trong việc phát triển khuôn khổ pháp lý và thể chế liên quan, bao gồm các quy định về bảo vệ dữ liệu (*Data Protection Directive / Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*), 1995, được thay thế bởi *General Data Protection Regulation – GDPR*, 2016) và Ủy viên về Bảo vệ dữ liệu (*European Commission Data Protection Officer*)... Cạnh đó, tổ chức OECD đã thông qua "Hướng dẫn của OECD về bảo vệ riêng tư và dữ liệu cá nhân xuyên biên giới" (*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980), và "Hướng dẫn của OECD về bảo vệ người tiêu dùng trong bối cảnh thương mại điện tử" (*OECD Guidelines for Consumer Protection in the Context of Electronic Commerce*, 1999).

Ở phạm vi quốc tế, dù quyền riêng tư nói chung đã được bảo vệ tại Điều 12 Tuyên ngôn nhân quyền phổ quát (1948), Điều 17 Công ước quốc tế về các quyền dân sự và chính trị (1966), các thỏa thuận về xác định về các nghĩa vụ của nhà nước bảo vệ quyền riêng tư trên internet cũng đã được hình thành. Năm 1989, Đại Hội đồng Liên Hợp quốc đã thông qua Các hướng dẫn về quy định về hồ sơ dữ liệu cá nhân được số hóa.[2] Năm 2011, Báo cáo viên đặc biệt về thúc đẩy và bảo vệ quyền tự do quan điểm và biểu đạt, Frank La Rue, trong báo cáo thường niên của mình cũng đã đề cập đến quyền riêng tư chủ yếu từ khía cạnh như là điều cần thiết để các cá nhân thể hiện mình một cách tự do

[2] Guidelines for the Regulation of Computerized Personal Data Files, G.A. res. 44/132, 44 U.N. GAOR Supp. (No. 49) at 211, U.N. Doc. A/44/49 (1989).

(chẳng hạn như nhiều cá nhân muốn ẩn danh khi tham gia vào các cuộc tranh luận công cộng). [3]

Tuy nhiện, văn kiện nổi bật nhất quy mô toàn cầu, được Đại Hội đồng Liên Hợp quốc thông qua vào năm 2013, là nghị quyết 68/167 về quyền riêng tư trong thời đại kỹ thuật số. Nghị quyết khẳng định rằng các quyền con người trong đời sống thực (offline) cũng phải được bảo vệ trực tuyến (online) và kêu gọi tất cả các quốc gia tôn trọng và bảo vệ quyền riêng tư trong truyền thông kỹ thuật số. Nó cũng kêu gọi tất cả các quốc gia xem xét các thủ tục, thông lệ và luật pháp liên quan đến theo dõi truyền thông, xâm nhập và thu thập dữ liệu cá nhân, nhấn mạnh nhu cầu của các quốc gia đảm bảo thực hiện đầy đủ và hiệu quả các nghĩa vụ của mình theo luật nhân quyền quốc tế.

Báo cáo của Văn phòng Cao ủy Nhân quyền Liên Hợp quốc về Quyền riêng tư trong thời đại kỹ thuật số (2014) đã phân tích các vấn đề như: quyền được bảo vệ chống lại sự can thiệp tùy tiện hoặc bất hợp pháp đối với quyền riêng tư về thư tín (bao gồm thư điện tử), phạm vi bảo vệ (trong và ngoài biên giới, đối với công dân và người nước ngoài), các cơ chế theo dõi, giám sát độc lập; quyền có cơ chế khắc phục hiệu quả; vai trò của các doanh nghiệp...[4] Báo cáo lưu ý đến tình trạng thiếu minh bạch của các chính phủ trong các chính sách, pháp luật và thực hành theo dõi, đồng thời kêu gọi các tòa án quốc gia và khu vực tham gia vào kiểm tra tính hợp pháp của các chính sách và biện pháp theo dõi điện tử.[5] Cạnh đó, báo cáo khuyến nghị cần có sự tham gia liên tục của các bên liên quan để giải quyết hiệu quả các thách thức với quyền riêng tư trong bối cảnh công nghệ truyền thông hiện đại. Quá trình đó cần có đối thoại giữa các bên liên quan, bao gồm nhà nước, xã hội dân sự, các tổ chức khoa học và kỹ thuật, khu vực kinh doanh, các nhà nghiên cứu và chuyên gia về nhân quyền.[6]

---

[3] Báo cáo thường niên 2011 của Báo cáo của Báo cáo viên đặc biệt về thúc đẩy và bảo vệ quyền tự do quan điểm và biểu đạt, Frank La Rue, A/HRC/17/27, ngày 16/5/2011.

[4] Báo cáo của Văn phòng Cao ủy Nhân quyền (OHCHR) Liên Hợp quốc về quyền riêng tư trong thời đại kỹ thuật số, 2014, A /HRC/27/37.

[5] Như trên, đoạn 48.

[6] Như trên, đoạn 49.

Ngoài ra, Báo cáo viên Đặc biệt về việc thúc đẩy và bảo vệ quyền con người và các quyền tự do cơ bản trong khi chống khủng bố đã nhiều lần lên tiếng về việc bảo vệ quyền riêng tư khi chống khủng bố. Trong báo cáo thường niên năm 2009 gửi đến Hội đồng Nhân quyền, Báo cáo viên Martin Schenin nhấn mạnh cần bảo vệ quyền riêng tư trong cuộc chiến chống khủng bố, với sự tuân thủ các nguyên tắc là: 1) Can thiệp tối thiểu vào quyền riêng tư; 2) Khi hạn chế quyền riêng tư cần có mục đích cụ thể, hạn chế việc sử dụng thông tin thu thập được vào mục đích khác (mục đích thứ cấp); 3) Việc tiếp cận thông tin của cơ quan công quyền phải hợp pháp và chịu sự giám sát do luật định; 4) Minh bạch và liêm chính; 5) Hiện đại hóa hiệu quả (không được nhân danh hiện đại hóa việc theo dõi để giảm thiểu các bảo đảm bảo vệ riêng tư).[7]

2. Một số loại vi phạm tại các quốc gia trên thế giới

Tại các quốc gia, chủ thể vi phạm quyền riêng tư trên Internet có thể là các chủ thể công quyền (các cơ quan nhà nước) hoặc các chủ thể tư (như cá nhân, doanh nghiệp và các tổ chức khác). Một số hình thức vi phạm quyền riêng tư trên Internet nổi bật là:

Thứ nhất, các cơ quan nhà nước theo dõi, thu thập thông tin cá nhân. Sau sự kiện 9/11/2001, cuộc chiến chống khủng bố toàn cầu và nhu cầu bảo đảm an ninh đã làm gia tăng sự giám sát, theo dõi của các nhà nước đối với các phương tiện truyền thông, mạng internet. Đặc biệt, nhờ những công bố gây choáng váng của Edward J. Snowden trong năm 2013 và 2014, người ta biết được quy mô theo dõi toàn cầu khổng lồ của Cơ quan An ninh Quốc gia Hoa Kỳ (*National Security Agency - NSA*), Tổng cục Truyền thông của Anh (*Government Communications Headquarters - GCHQ*), Liên minh FVEY (Five Eyes/ giữa 5 quốc gia Úc, New Zealand, Canada, Hoa Kỳ và Anh). Các cơ quan này đã tiếp cận rất lớn vào Internet toàn cầu (bao gồm email, lịch sử truy cập trang web), ghi âm, xác định địa điểm các cuộc gọi, danh bạ điện tử của cá nhân và nhiều nội dung truyền thông kỹ thuật số khác[8]... Sự kiện chấn động này một mặt làm cho các quốc

[7] Báo cáo thường niên 2009 của Báo cáo viên Đặc biệt về việc thúc đẩy và bảo vệ quyền con người và các quyền tự do cơ bản trong khi chống khủng bố, A/HRC/13/37.

[8] Amnesty International, *Edward Snowden is a hero not a traitor*, Petition: https://www.amnesty.org/

gia phải điều chỉnh về phương thức và kỹ thuật thu thập thông tin, mặt khác thúc đẩy phong trào chống lại sự theo dõi của nhà nước (với quan điểm rằng một "nhà nước theo dõi "surveillance state" là không cần thiết để bảo đảm an ninh chung). Cạnh đó, tình trạng các cơ quan nhà nước kiểm duyệt Internet cũng diễn ra tương đối phổ biến, không chỉ ở các quốc gia thiếu dân chủ, mà cả ở các nước Tây phương với nền dân chủ lâu đời.

Thứ hai, các doanh nghiệp cung cấp dịch vụ Internet đồng lõa với nhà nước, hoặc chủ động xâm phạm quyền riêng tư. Yahoo đã bị chỉ trích về nhiều loại vi phạm quyền của người sử dụng ở quy mô khác nhau. Tại Trung Quốc, một số nhà báo, nhà hoạt động nhân quyền đã bị truy tố, xét xử, dựa trên những thông tin mà cơ quan nhà nước lấy được từ Yahoo. Năm 2005, tòa án tỉnh Hồ Nam đã kết án Shi Tao, một phóng viên, 10 năm tù về tội "cung cấp bí mật nhà nước cho nước ngoài". Năm 2007, vợ của một tù nhân kiện Yahoo tại Mỹ về hành vi đồng lõa với sự tra tấn của chính quyền Trung Quốc.[9] Không chỉ Yahoo, nhiều doanh nghiệp khác như Microsoft Corp, Google. Inc, Skype, cũng đã bị các tổ chức bảo vệ nhân quyền cáo buộc đã "hỗ trợ" sự kiểm duyệt của chính quyền.[10]

Thứ ba, vi phạm của các cá nhân, doanh nghiệp như mua bán, truyền tải dữ liệu, hình ảnh cá nhân. Tại nhiều nước, nhiều cá nhân, giới báo chí đã xâm phạm quyền riêng tư bằng cách truyền tải thông tin, hình ảnh cá nhân trên Internet. Nhiều cá nhân, đặc biệt là các nhân vật nổi tiếng đã trở thành nạn nhân của vi phạm loại này (như các scandal lộ video sex của diễn viên Hoa Kỳ Paris Hilton năm 2003, lộ ảnh của diễn viên Hồng Kong Edison Chen vào năm 2008, lộ clip của Hoàng Thùy Linh năm 2007...)

II. BẢO VỆ QUYỀN RIÊNG TƯ TRONG KHÔNG GIAN INTERNET TRƯỚC CÁC CƠ QUAN NHÀ NƯỚC TẠI VIỆT NAM

1. Một khoảng trống pháp luật bảo vệ quyền riêng tư tại Việt Nam

[9] *Advocates Sue Yahoo In Chinese Torture Case,*

Washington Post , 19/4/2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/04/18/AR2007041802510.html?hpid=moreheadlines

[10] Human Rights Watch, "Race to the Bottom: Corporate Complicity in Chinese Internet Censorship", 2006.

Hệ thống pháp lý bảo vệ quyền riêng tư tại Việt Nam đã được cập nhật đáng kể cùng với tiến trình tự do hóa kinh tế, hiện đại hóa cơ sở hạ tầng, bao gồm hạ tầng công nghệ và Internet. Tuy nhiên, liên quan đến việc bảo vệ trước sự vi phạm quyền riêng tư của các cơ quan công quyền, dù là về quyền riêng tư về nhà ở, thư tín, nhìn chung hệ thống pháp luật vẫn có sự ưu tiên bảo vệ an ninh, trật tự hơn là quyền cá nhân. Các quy định của pháp luật vẫn nặng về quy định thẩm quyền can thiệp của các cơ quan nhà nước, mà nhẹ về bảo vệ quyền riêng tư cá nhân, đặc biệt là rất thiếu cơ chế bảo vệ, chế tài độc lập, hữu hiệu đối với các vi phạm. Đang tồn tại những văn bản dưới luật giới hạn quyền, trái với nguyên tắc nêu tại Hiến pháp 2013 "quyền con người, quyền công dân chỉ có thể bị hạn chế theo quy định của luật" (Khoản 2, Điều 14).

a. Các quy định có tính nguyên tắc bảo vệ quyền riêng tư

Trên nguyên tắc, quyền riêng tư đã được nhiều quy định trong hiến pháp và pháp luật Việt Nam bảo vệ, một số quy định xuất hiện từ khá sớm. Kể từ Hiến pháp 1959 (tại Điều 28), các hiến pháp về sau đều có các quy định bảo vệ quyền riêng tư về nhà ở và thư tín. [11] Pháp luật dân sự Việt Nam cũng đã có sự quan tâm đến quyền này (như Điều 34 Bộ luật Dân sự 1995 - Quyền đối với bí mật đời tư, Điều 38 Bộ luật Dân sự 2015 - Quyền về đời sống riêng tư, bí mật cá nhân, bí mật gia đình...). Tuy nhiên, cho đến gần đây hầu như không có đạo luật nào quy định đầy đủ về thủ tục ghi âm, ghi hình bí mật bởi các cơ quan nhà nước, cũng như về sự can thiệp, theo dõi của các cơ quan đó đến thư tín cá nhân, bao gồm thư tín, truyền thông trên Internet, một số quy định chỉ dừng ở mức độ nguyên tắc.

Năm 2015, lần đầu tiên Bộ luật Tố tụng Hình sự (2015) đã bổ sung Chương XVI về "Biện pháp điều tra tố tụng đặc biệt". Theo đó, sau khi khởi tố vụ án, trong quá trình điều tra, người có thẩm quyền tiến hành tố tụng có thể áp dụng các biện pháp: *Ghi âm, ghi hình bí mật; Nghe điện thoại bí mật; Thu thập bí mật dữ liệu điện tử.* Phạm vi áp dụng biện pháp điều tra tố tụng đặc biệt đối được xác định tương đối hẹp, chỉ đối với các trường hợp: *Tội xâm phạm an ninh quốc gia, tội phạm về ma túy, tội phạm về tham nhũng, tội khủng bố, tội rửa tiền; Tội phạm khác có tổ chức thuộc loại tội phạm đặc biệt nghiêm trọng* (Điều 224).

[11] Hiến pháp 1959, Điều 28 quy định "pháp luật bảo đảm nhà ở của công dân nước Việt Nam dân chủ cộng hòa không bị xâm phạm, thư tín được giữ bí mật". Hiến pháp 1980, Điều 71 quy định: "Công dân có quyền bất khả xâm phạm về chỗ ở. Không ai được tự ý vào chỗ ở của người khác nếu người đó không đồng ý, trừ trường hợp được pháp luật cho phép. Việc khám xét chỗ ở phải do đại diện cơ quan Nhà nước có thẩm quyền tiến hành, theo quy định của pháp luật. Bí mật thư tín, điện thoại, điện tín được bảo đảm."

Tuy nhiên, các biện pháp đặc biệt trên đây chỉ liên quan đến lĩnh vực tố tụng hình sự, nhiều lĩnh vực khác vẫn chưa được các đạo luật quy định rõ ràng. Như một tác giả ngành công an đã phần nào chỉ ra: "Quy định biện pháp điều tra đặc biệt trong Bộ luật Tố tụng Hình sự không làm triệt tiêu việc áp dụng các biện pháp này với tư cách là các biện pháp nghiệp vụ chuyên ngành được quy định trong các luật về tổ chức và hoạt động của cơ quan nhà nước (như Luật Công an nhân dân, Luật an ninh quốc gia, Luật hải quan, Luật phòng, chống khủng bố)".[12] Tuy nhiên, ngay cả trong các luật mà tác giả nêu, "các biện pháp nghiệp vụ chuyên ngành" cũng không được quy định đầy đủ về căn cứ, thẩm quyền, thủ tục áp dụng.

Hai đạo luật có tính hệ thống trong lĩnh vực này là Luật Viễn thông (2009) và Luật An toàn thông tin mạng (2015). Một mặt, hai luật đều nêu các nguyên tắc bảo vệ thông tin cá nhân. Mặt khác, cả hai luật lại có một số căn cứ và quy định khái quát về việc có thể giới hạn quyền riêng tư "theo quy định của pháp luật khác có liên quan". Trong Luật Viễn thông (2009), Điều 6 về bảo đảm bí mật thông tin quy định: 3. Thông tin riêng chuyển qua mạng viễn thông công cộng của mọi tổ chức, cá nhân được bảo đảm bí mật. Việc kiểm soát thông tin trên mạng viễn thông do cơ quan nhà nước có thẩm quyền thực hiện theo quy định của pháp luật (Khoản 3); Doanh nghiệp viễn thông không được tiết lộ thông tin riêng liên quan đến người sử dụng dịch vụ viễn thông, bao gồm tên, địa chỉ, số máy gọi, số máy được gọi, vị trí máy gọi, vị trí máy được gọi, thời gian gọi và thông tin riêng khác mà người sử dụng đã cung cấp khi giao kết hợp đồng với doanh nghiệp, trừ các trường hợp sau đây: ....c) Khi có yêu cầu của cơ quan nhà nước có thẩm quyền theo quy định của pháp luật (khoản 4).

Luật An toàn thông tin mạng (2015) xác định các nguyên tắc bảo đảm an toàn thông tin mạng bao gồm: khi xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức (Khoản 3, Điều 4). Các hành vi bị nghiêm cấm bao gồm hành vi thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân (khoản 5, Điều 7). Đặc biệt, Luật bao gồm Chương II về Bảo đảm an toàn thông tin mạng, Mục 2 về bảo vệ thông tin cá nhân, đã quy định về các khía cạnh: nguyên tắc bảo vệ thông tin cá nhân trên mạng, thu thập và sử dụng thông tin cá nhân, bảo đảm an toàn thông tin cá nhân trên mạng... 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 (Khoản 3, Điều 17).

[12] Trần Đình Nhã, Biện pháp điều tra tố tụng đặc biệt, trong sách "Những nội dung mới trong Bộ luật Tố tụng Hình sự năm 2015", Nguyễn Hòa Bình (Chủ biên), Nxb. Chính trị quốc gia, 2016, trang 291.

Tuy nhiên, các căn cứ giới hạn trong cả hai đạo luật chỉ được nêu khái quát, hoặc dẫn chiếu đến "quy định khác liên quan". Luật Viễn thông (2009), Điều 5 về bảo đảm an toàn cơ sở hạ tầng viễn thông và an ninh thông tin, quy định doanh nghiệp viễn thông "có trách nhiệm cung cấp điểm truy nhập mạng viễn thông và các điều kiện kỹ thuật, nghiệp vụ cần thiết khác để cơ quan đó thực hiện nhiệm vụ kiểm soát và bảo đảm an ninh thông tin" (khoản 6) và "có trách nhiệm thực hiện yêu cầu của cơ quan nhà nước có thẩm quyền, tiến hành ngăn chặn khẩn cấp và ngừng cung cấp dịch vụ viễn thông đối với trường hợp bạo động, bạo loạn, sử dụng dịch vụ viễn thông xâm phạm an ninh quốc gia, chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam" (khoản 7). Tuy nhiên, Luật An toàn thông tin mạng dẫn chiếu đến các quy định khác, theo đó "việc xử lý thông tin cá nhân phục vụ mục đích bảo đảm quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội hoặc không nhằm mục đích thương mại được thực hiện theo quy định khác của pháp luật có liên quan" (khoản 5, Điều 16).

Năm 2009, Bộ luật Hình sự Việt Nam đã có những sửa đổi, bổ sung tích cực nhằm chống lại sự xâm phạm vào quyền riêng tư trên Internet. Hai tội danh được bổ sung là "Tội truy cập bất hợp pháp vào mạng máy tính, mạng viễn thông, mạng Internet hoặc thiết bị số của người khác" (Điều 226a) và "Tội sử dụng mạng máy tính, mạng viễn thông, mạng Internet hoặc thiết bị số thực hiện hành vi chiếm đoạt tài sản" (Điều 226b). Cạnh đó, Điều 226 cũ cũng được sửa đổi từ "Tội sử dụng trái phép thông tin trên mạng và trong máy tính" thành "Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông, mạng Internet". Tuy nhiên, thực tiễn các đối tượng bị truy cứu trách nhiệm hình sự về tội truy cập bất hợp pháp vào mạng máy tính, mạng viễn thông, mạng Internet hoặc thiết bị số trong những năm qua chủ yếu là những cá nhân kinh doanh phần mềm nghe lén điện thoại.[13] Dường như chưa thấy thông tin về việc xử lý hành vi truy cập Internet bởi cá nhân hoặc công chức nào tại Việt Nam.

b. Thẩm quyền của các cơ quan quốc phòng và bảo vệ an ninh

Các "quy định khác" đó thể hiện tương đối nổi bật trong các đạo luật như Luật An ninh quốc gia (2004), Luật Quốc phòng (2005), Luật Công an nhân dân (2014). Một mặt, các luật này đều khẳng định các lĩnh vực quốc phòng, bảo vệ an ninh quốc gia và hoạt động của công an đều phải hoạt động theo nguyên tắc "tuân thủ Hiến pháp, pháp luật, bảo đảm... quyền và lợi ích hợp pháp của tổ chức, cá nhân" (Khoản 1, Điều 5 Luật

[13] Một số trường hợp đã bị khởi tố là: Lê Viết Tám (quận Thanh Xuân, Hà Nội) bị Công an Hà Nội bắt ngày 13/5/2014, do kinh doah phần mềm nghe lén Myspy; Nguyễn Văn Nguyên (quận Tân Phú, TP.Hồ Chí Minh) và 4 đồng phạm bị Cục Cảnh sát phòng chống tội phạm sử dụng công nghệ cao tại TP.HCM (C50B) bắt ngày 18/11/2015, do kinh doanh phần mềm, cung cấp dịch vụ nghe lén; Huỳnh Ngọc Đến (huyện Hóc Môn, TP.HCM) bị C50 bắt đầu năm 2017, do kinh doanh phần mềm nghe lén.

An ninh quốc gia, Khoản 3, Điều 5 Luật Công an nhân dân...). Mặt khác, các quy định về nội dung, điều kiện, thẩm quyền, trình tự, thủ tục áp dụng các biện pháp có thể hạn chế quyền cá nhân chỉ được nêu về nguyên tắc và lại dẫn chiếu "do pháp luật quy định".

Theo Điều 15 Luật An ninh quốc gia (2004), các biện pháp cơ bản bảo vệ an ninh quốc gia bao gồm "vận động quần chúng, pháp luật, ngoại giao, kinh tế, khoa học - kỹ thuật, nghiệp vụ, vũ trang". Nội dung, điều kiện, thẩm quyền, trình tự, thủ tục và trách nhiệm áp dụng các biện pháp quy định này "do pháp luật quy định". Điều 17, về quyền và nghĩa vụ của công dân trong bảo vệ an ninh quốc gia, quy định công dân phải thực hiện yêu cầu của cơ quan chuyên trách bảo vệ an ninh quốc gia theo quy định của pháp luật; giúp đỡ, tạo điều kiện cho cơ quan và người có trách nhiệm tiến hành các biện pháp phòng ngừa, phát hiện, ngăn chặn, đấu tranh với hoạt động xâm phạm an ninh quốc gia (khoản 5 và 6).

Điều 24, Luật An ninh quốc gia quy định cơ quan chuyên trách bảo vệ an ninh quốc gia được quyền: a) Sử dụng các biện pháp nghiệp vụ theo quy định của pháp luật; b) Yêu cầu cơ quan, tổ chức, cá nhân cung cấp thông tin, tài liệu, đồ vật khi có căn cứ xác định liên quan đến hoạt động xâm phạm an ninh quốc gia; d) Yêu cầu cơ quan, tổ chức bưu chính, viễn thông, hải quan bóc mở hoặc giao thư tín, điện tín, bưu phẩm, bưu kiện, hàng hoá để kiểm tra khi có căn cứ xác định trong đó có thông tin, tài liệu, chất nổ, vũ khí, vật phẩm khác có nguy hại cho an ninh quốc gia; đ) Kiểm tra phương tiện giao thông, phương tiện thông tin, máy tính, mạng máy tính, đồ vật, tài liệu, hàng hoá, chỗ ở, nơi làm việc hoặc các cơ sở khác của cơ quan, tổ chức, cá nhân khi có căn cứ xác định liên quan đến hoạt động xâm phạm an ninh quốc gia;

Tương tự, Luật Công an nhân dân (2014, thay thế cho Luật năm 2005) quy định quyền hạn của Công an nhân dân bao gồm "áp dụng các biện pháp vận động quần chúng, pháp luật, ngoại giao, kinh tế, khoa học - kỹ thuật, nghiệp vụ, vũ trang để bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội theo quy định của pháp luật"; "yêu cầu cơ quan, tổ chức, cá nhân cung cấp thông tin, tài liệu, đồ vật khi có căn cứ xác định liên quan đến hoạt động xâm phạm an ninh quốc gia, trật tự, an toàn xã hội theo quy định của pháp luật" (khoản 13 và 15, Điều 15).

Luật Quốc phòng (2005), Khoản 2, Điều 40 quy định về việc Bộ Bưu chính - Viễn thông, Bộ Văn hoá - Thông tin, các cơ quan thông tin đại chúng trong phạm vi nhiệm vụ, quyền hạn của mình có trách nhiệm phối hợp với Bộ Quốc phòng giúp Chính phủ xây dựng và tổ chức thực hiện kế hoạch bảo đảm thông tin liên lạc, thông tin tuyên truyền phục vụ quốc phòng trong thời bình và thời chiến.

Trong Luật Phòng, chống khủng bố (2013), một số biện pháp phòng ngừa, phát hiện khủng bố liên quan đến tiếp cận thông tin và các biện pháp "nghiệp vụ, kỹ thuật". Cụ thể, Điều 25 quy định về kiểm soát hoạt động xuất bản, báo chí, bưu chính, viễn

thông và các hình thức thông tin khác, theo đó cơ quan và người có thẩm quyền trong hoạt động xuất bản, báo chí, bưu chính, viễn thông và các hình thức thông tin khác có trách nhiệm kiểm soát, phát hiện, ngăn chặn, xử lý kịp thời hành vi lợi dụng hoạt động này để khủng bố. Theo Khoản 2, Điều 28 Lực lượng chống khủng bố có trách nhiệm triển khai các biện pháp nghiệp vụ, kỹ thuật để phát hiện khủng bố; hướng dẫn, giúp đỡ cơ quan, tổ chức, cá nhân nhận biết về khủng bố và cách thức phát hiện, báo tin, tố giác về khủng bố.

Luật Hải quan (2014) có quy định cơ quan hải quan có quyền *"á*p dụng biện pháp, kỹ thuật nghiệp vụ để thu thập thông tin" (khoản 2, Điều 95), bên cạnh cách biện pháp yêu cầu tổ chức, cá nhân cung cấp thông tin liên quan đến hoạt động xuất khẩu, nhập khẩu, xuất cảnh, nhập cảnh, quá cảnh; khai thác các nguồn thông tin khác có liên quan...

Như vậy, có thể thấy nhìn chung quy định trong các đạo luật liên quan thiên về bảo vệ an ninh, trật tự công cộng, mà sự quan tâm dường như ít hơn đến bảo vệ quyền cá nhân. Nhiều quy định vẫn chỉ có tính nguyên tắc liên quan đến "các biện pháp nghiệp vụ" và để cho các văn bản dưới luật quy định (nếu có). Dưới tinh thần của Khoản 2, Điều 14 Hiến pháp – việc hạn chế quyền con người phải do luật quy định - tình trạng này cần phải được khắc phục nhanh chóng.

2. Khuyến nghị hoàn thiện pháp luật bảo vệ quyền riêng tư tại Việt Nam

Qua một số phân tích trên, đối chiếu với các khuyến nghị của các cơ quan Liên Hợp quốc, đặc biệt là tại báo cáo của Văn phòng Cao ủy Nhân quyền Liên Hợp quốc về Quyền riêng tư trong thời đại kỹ thuật số (2014), tác giả cho rằng khuôn khổ chính sách và pháp luật Việt Nam có thể được hoàn thiện theo một số hướng sau:

- Xây dựng, ban hành một đạo luật quy định rõ ràng về nội dung, điều kiện, thẩm quyền, trình tự, thủ tục áp dụng các biện pháp giám sát, theo dõi thư tín, truyền thông Internet của cá nhân, cũng như cơ chế giám sát, khiếu nại, khiếu kiện trong trường hợp có sự vi phạm. Tiến trình xây dựng văn bản này cần được tổ chức công khai, có sự tham gia của các cơ quan nghiên cứu, tổ chức xã hội và báo chí.

- Về thể chế, cần sớm xây dựng cơ quan chuyên trách bảo vệ quyền riêng tư và dữ liệu cá nhân với thẩm quyền xem xét khiếu nại, thực hiện quyền thanh tra, giám sát, cũng như thực hiện các nghiên cứu nhằm hoàn thiện chính sách, pháp luật, thúc đẩy quyền riêng tư.

TÀI LIỆU THAM KHẢO

1. Báo cáo của Văn phòng Cao ủy Nhân quyền (OHCHR) Liên Hợp quốc về quyền riêng tư trong thời đại kỹ thuật số, 2014, A /HRC/27/37
2. Báo cáo của Báo cáo viên đặc biệt về thúc đẩy và bảo vệ quyền tự do quan điểm và biểu đạt, 2011, A/HRC/17/27
3. Báo cáo của Báo cáo viên Đặc biệt về việc thúc đẩy và bảo vệ quyền con người và các quyền tự do cơ bản trong khi chống khủng bố, 2009, A/HRC/13/37
4. Nguyễn Thị Thu Vân, *Pháp luật và tổ chức thực thi pháp luật về cơ chế bảo đảm quyền bảo vệ dữ liệu cá nhân trên internet và môi trường số* (chuyên đề 6, đề tài nghiên cứu khoa học cấp Bộ "Cơ chế bảo đảm thực hiện quyền bí mật dữ liệu cá nhân")
5. Toby Mendel et al, *Global Survey on Internet Privacy and Freedom of Expression*, UNESCO, 2012
6. *Privacy in International Law: Regulating the Internet*, Groningen Journal of International Law, Vol. 2, Issue 2, 2014.