BẢO VỆ QUYỀN RIÊNG TƯ TRÊN MÔI TRƯỜNG MẠNG Ở VIỆT NAM: MỘT SỐ VẤN ĐỀ LÝ LUẬN VÀ KIẾN NGHỊ HOÀN THIỆN PHÁP LUẬT

TRẦN MẠNH TOÀN
Khoa Lý luận chính trị và pháp luật,
Trường Đại học Kinh tế - Kỹ thuật Công nghiệp

Nhận bài ngày 10/01/2026. Sửa chữa xong 25/02/2026. Duyệt đăng 26/02/2026.

Abstract

The rapid development of digital technologies and the expansion of cyberspace have significantly increased the risks of privacy violations, raising urgent concerns regarding the protection of human rights in contemporary society. In Viet Nam, the right to privacy has been recognized in the Constitution and several sectoral legal instruments. However, in an increasingly complex digital environment, the current legal framework still reveals limitations in terms of coherence, effectiveness, and practical enforceability. This article examines key theoretical and legal issues related to protecting privacy rights in cyberspace in Viet Nam, focusing on the conceptualization of the right to privacy, existing legal protection mechanisms, and emerging practical challenges. On that basis, it proposes recommendations to improve the legal framework for protecting privacy rights online, thereby contributing to the safeguarding of human rights and enhancing the effectiveness of state governance in the context of digital transformation.

Keywords: *Cyberspace, digital transformation, human rights, legal protection, privacy rights.*

1. Đặt vấn đề

Trong bối cảnh chuyển đổi số diễn ra sâu rộng, môi trường mạng đã trở thành không gian cơ bản để cá nhân thực hiện các hoạt động học tập, lao động, giao tiếp và tham gia đời sống xã hội. Bên cạnh những lợi ích to lớn mà công nghệ số mang lại, nguy cơ xâm phạm quyền riêng tư của cá nhân ngày càng gia tăng, xuất phát từ khả năng thu thập, lưu trữ, xử lý và kết nối dữ liệu cá nhân ở quy mô lớn của cả khu vực công và khu vực tư. Dữ liệu cá nhân trong môi trường số không còn giới hạn ở các thông tin định danh truyền thống mà mở rộng sang dữ liệu hành vi, dữ liệu vị trí, lịch sử tương tác và các dữ liệu có thể được kết hợp để suy luận hồ sơ cá nhân, qua đó làm suy giảm đáng kể quyền tự chủ và quyền kiểm soát thông tin của mỗi cá nhân.

Trên bình diện quốc tế, quyền riêng tư được thừa nhận là một quyền con người cơ bản, đòi hỏi Nhà nước không chỉ có nghĩa vụ kiềm chế các can thiệp tùy tiện hoặc bất hợp pháp của cơ quan công quyền mà còn phải thiết lập các cơ chế pháp lý hữu hiệu nhằm bảo vệ cá nhân trước các hành vi xâm phạm từ các chủ thể tư nhân, đặc biệt là các doanh nghiệp và nền tảng số nắm giữ quyền lực dữ liệu lớn [4, tr. 35-36; 11, tr. 102-110]. Trong kỷ nguyên số, sự phát triển của các công nghệ giám sát, thu thập và xử lý dữ liệu quy mô lớn đặt ra yêu cầu ngày càng nghiêm ngặt về tính hợp pháp, tính cần thiết, tính tương xứng và trách nhiệm giải trình của các biện pháp tác động tới quyền riêng tư nhằm bảo đảm sự cân bằng hợp lý giữa lợi ích công cộng và việc bảo vệ quyền con người [5, tr. 171-173].

Ở Việt Nam, quyền riêng tư đã được ghi nhận ở cấp độ hiến định và được cụ thể hóa trong nhiều lĩnh vực pháp luật khác nhau. Tuy nhiên, thực tiễn cho thấy việc bảo vệ quyền riêng tư trên môi trường mạng vẫn đang đối mặt với nhiều thách thức, thể hiện ở sự phân tán của các quy định pháp luật, thiếu tính liên thông giữa các cơ chế bảo vệ cũng như khoảng cách đáng kể giữa quyền được

Email: tmtoan@uneti.edu.vn

DOI: 10.64410/BJXJ2531

ghi nhận trên văn bản và khả năng thực thi hiệu quả trong đời sống số. Trong bối cảnh đó, việc tiếp cận quyền riêng tư không chỉ như một quyền nhân thân theo nghĩa truyền thống mà còn như một quyền gắn liền với quản trị dữ liệu và trách nhiệm của các chủ thể xử lý dữ liệu, trở thành yêu cầu cấp thiết cả về phương diện lý luận và thực tiễn. Trên cơ sở đó, bài viết tập trung phân tích một số vấn đề lý luận về bảo vệ quyền riêng tư trên môi trường mạng ở Việt Nam, làm rõ nội hàm của quyền riêng tư, các dạng xâm phạm điển hình và cơ chế bảo vệ pháp lý hiện hành. Từ đó, bài viết đề xuất một số kiến nghị nhằm hoàn thiện pháp luật về bảo vệ quyền riêng tư trên môi trường mạng, hướng tới bảo đảm quyền con người một cách thực chất và nâng cao hiệu quả quản lý nhà nước trong bối cảnh chuyển đổi số hiện nay.

2. Một số vấn đề lý luận về quyền riêng tư trên môi trường mạng

2.1. Khái niệm quyền riêng tư

Quyền riêng tư trên môi trường mạng có thể được hiểu là quyền của cá nhân được bảo vệ trước mọi sự can thiệp tùy tiện hoặc bất hợp pháp đối với đời sống riêng tư trong bối cảnh thông tin cá nhân được tạo lập, thu thập, lưu trữ, xử lý và truyền tải bằng công nghệ số. Nền tảng chuẩn mực quốc tế của quyền này được ghi nhận tại Điều 17 ICCPR: "Không ai bị đặt dưới sự can thiệp tùy tiện hoặc bất hợp pháp vào đời sống riêng tư, gia đình, nhà ở hoặc thư tín…" và mọi người có quyền được pháp luật bảo vệ trước sự can thiệp đó [5, tr. 171-173].

Điểm quan trọng là Ủy ban Nhân quyền Liên Hợp Quốc nhấn mạnh quyền riêng tư phải được bảo đảm không chỉ trước hành vi của cơ quan nhà nước mà cả trước can thiệp từ cá nhân hoặc pháp nhân, doanh nghiệp nắm giữ quyền lực dữ liệu rất lớn [13, tr. 1- 4].

Từ góc độ lý luận quyền con người, quyền riêng tư trên môi trường mạng mang hai chiều cạnh cơ bản. Một mặt, đây là quyền "phòng vệ", đòi hỏi Nhà nước và các chủ thể khác không được xâm phạm đời sống riêng tư của cá nhân một cách tùy tiện. Mặt khác, quyền riêng tư còn mang tính "tích cực", yêu cầu Nhà nước phải thiết lập khuôn khổ pháp lý và cơ chế bảo vệ hữu hiệu nhằm ngăn ngừa, phát hiện và xử lý các hành vi xâm phạm quyền riêng tư trong không gian số [3, Điều 1- 3]. Cách tiếp cận hai chiều này đặc biệt có ý nghĩa trong bối cảnh các chủ thể tư nhân, nhất là các doanh nghiệp công nghệ và nền tảng số ngày càng nắm giữ quyền lực lớn trong việc thu thập và khai thác dữ liệu cá nhân.

2.2. Quyền riêng tư và quyền kiểm soát dữ liệu cá nhân

Trong môi trường mạng, quyền riêng tư có mối liên hệ chặt chẽ với quyền kiểm soát dữ liệu cá nhân. Nếu như cách tiếp cận truyền thống thường nhấn mạnh việc bảo vệ các thông tin mang tính "bí mật" thì cách tiếp cận hiện đại đặt trọng tâm vào quyền của cá nhân được biết, được quyết định và được kiểm soát cách thức dữ liệu của mình được xử lý [11, tr. 102-110]. Dữ liệu cá nhân trong không gian số không chỉ bao gồm dữ liệu định danh mà còn bao gồm dữ liệu hành vi, dữ liệu vị trí, dữ liệu suy luận, vốn có khả năng phản ánh toàn diện đời sống cá nhân ngay cả khi không tiết lộ trực tiếp danh tính. Theo cách tiếp cận này, xâm phạm quyền riêng tư không chỉ xảy ra khi thông tin cá nhân bị công khai trái phép mà còn có thể phát sinh từ các hoạt động thu thập quá mức, xử lý không minh bạch, sử dụng dữ liệu ngoài mục đích đã thông báo hoặc chia sẻ dữ liệu cho bên thứ ba mà không có sự đồng ý hợp pháp của chủ thể dữ liệu [2, Điều 2; Điều 11; 11, tr. 102-110]. Do đó, việc bảo vệ quyền riêng tư trên môi trường mạng cần được đặt trong khuôn khổ quản trị dữ liệu, với trọng tâm là trách nhiệm của các chủ thể xử lý dữ liệu và khả năng thực thi các quyền của cá nhân.

2.3. Nội dung quyền riêng tư trên môi trường mạng

Quyền riêng tư trên môi trường mạng thường được cấu thành bởi ba phương diện có mối liên hệ chặt chẽ với nhau.

Thứ nhất, quyền riêng tư thông tin (informational privacy), phản ánh quyền của cá nhân đối với các dữ liệu liên quan đến mình, bao gồm dữ liệu định danh, dữ liệu liên lạc, dữ liệu vị trí, dữ liệu hành vi và cả các dữ liệu có thể được sử dụng để suy luận hồ sơ cá nhân.

Thứ hai, quyền bảo mật trong giao tiếp và liên lạc, không chỉ bao gồm nội dung trao đổi mà còn bao hàm các "dấu vết giao tiếp" như thời điểm, tần suất và đối tượng liên hệ, vốn có khả năng tái dựng đời sống cá nhân ngay cả khi nội dung được bảo mật.

Thứ ba, quyền tự quyết dữ liệu theo nghĩa vận hành, theo đó cá nhân có quyền được biết dữ liệu của mình được xử lý như thế nào, có quyền truy cập, chỉnh sửa, xóa, phản đối, rút lại sự đồng ý và yêu cầu trách nhiệm giải trình từ các chủ thể xử lý dữ liệu [11, tr. 102-110].

Trong pháp luật Việt Nam, cách tiếp cận này bước đầu được phản ánh thông qua việc ghi nhận tương đối đầy đủ các quyền của chủ thể dữ liệu như quyền truy cập, quyền rút lại sự đồng ý và quyền yêu cầu xóa dữ liệu, tạo cơ sở pháp lý cho việc tăng cường kiểm soát của cá nhân đối với dữ liệu cá nhân trong môi trường số [2, Điều 9; Điều 11; Điều 16].

Trên bình diện quốc tế, các nghị quyết của Đại hội đồng Liên Hợp Quốc về quyền riêng tư trong kỷ nguyên số đã nhiều lần cảnh báo rủi ro từ các hoạt động giám sát và thu thập dữ liệu ở quy mô lớn, đồng thời kêu gọi các quốc gia rà soát khuôn khổ pháp luật và thực tiễn nhằm bảo đảm các biện pháp tác động tới dữ liệu cá nhân phù hợp với các nghĩa vụ về quyền con người [13, tr. 3-6].

2.4. Các dạng xâm phạm quyền riêng tư trên môi trường mạng

Các dạng xâm phạm quyền riêng tư trên môi trường mạng có thể được nhận diện một cách hệ thống theo logic của "vòng đời dữ liệu" cá nhân, từ khâu thu thập, xử lý, chia sẻ đến lưu trữ và bảo mật. Ở giai đoạn thu thập, xâm phạm quyền riêng tư thường phát sinh khi dữ liệu được thu thập vượt quá mục đích đã thông báo, không cần thiết cho việc cung cấp dịch vụ hoặc được thực hiện thông qua các thủ thuật thiết kế giao diện và điều khoản sử dụng khiến sự đồng ý của cá nhân trở nên mang tính hình thức hơn là tự nguyện và có hiểu biết.

Ở giai đoạn sử dụng và kết hợp dữ liệu, rủi ro xâm phạm quyền riêng tư gia tăng khi dữ liệu cá nhân bị sử dụng cho các mục đích khác với mục đích ban đầu hoặc bị kết hợp từ nhiều nguồn khác nhau để suy luận thông tin nhạy cảm, hình thành hồ sơ hành vi và mô hình dự đoán cá nhân. Các thực hành này có thể dẫn đến hệ quả sâu rộng như gia tăng nguy cơ phân biệt đối xử, thao túng lựa chọn hoặc tác động bất cân xứng tới quyền tự chủ của cá nhân trong không gian số.

Ở giai đoạn chia sẻ và chuyển giao dữ liệu, xâm phạm quyền riêng tư thể hiện ở việc dữ liệu cá nhân bị bán, trao đổi hoặc chuyển giao cho bên thứ ba mà không có căn cứ pháp lý rõ ràng cũng như các hình thức chia sẻ nội bộ trong hệ sinh thái dịch vụ mà cá nhân không được thông tin đầy đủ hoặc không có khả năng kiểm soát. Trong nhiều trường hợp, chính sự thiếu minh bạch của các dòng chảy dữ liệu đã làm suy yếu đáng kể khả năng thực thi quyền của chủ thể dữ liệu.

Ở giai đoạn lưu trữ và bảo đảm an ninh dữ liệu, xâm phạm quyền riêng tư xảy ra khi dữ liệu cá nhân bị lưu giữ kéo dài vượt thời hạn cần thiết, cơ chế quản trị truy cập và bảo mật không đầy đủ, dẫn đến rò rỉ hoặc bị khai thác trái phép. Hệ quả của các vi phạm này không chỉ dừng ở việc mất kiểm soát dữ liệu mà còn kéo theo các hành vi lừa đảo, mạo danh, quấy rối hoặc công khai trái phép thông tin nhận dạng cá nhân nhằm gây áp lực xã hội, đe dọa hoặc tổn hại đến danh dự và đời sống riêng tư của cá nhân trên không gian mạng.

2.5. Cơ chế bảo vệ quyền riêng tư trên môi trường mạng

Bảo vệ quyền riêng tư trên môi trường mạng đòi hỏi một cơ chế pháp lý được thiết kế theo hướng hệ thống, kết hợp giữa phòng ngừa và khắc phục, giữa bảo vệ quyền cá nhân và bảo đảm lợi ích công cộng. Trong cấu trúc pháp luật Việt Nam, các cơ chế này có thể được khái quát thành bốn "kênh" cơ bản: tự bảo vệ của cá nhân, cơ chế dân sự, cơ chế hành chính và cơ chế hình sự; mỗi kênh đảm nhận một chức năng bảo vệ khác nhau nhưng có mối quan hệ bổ trợ lẫn nhau.

Thứ nhất, cơ chế tự bảo vệ giữ vai trò nền tảng và mang tính phòng ngừa, cho phép cá nhân chủ động kiểm soát rủi ro xâm phạm quyền riêng tư thông qua việc quản trị cài đặt quyền riêng tư, kiểm soát quyền truy cập ứng dụng, sử dụng xác thực đa yếu tố, hạn chế chia sẻ dữ liệu cũng như thực hiện

các quyền rút lại sự đồng ý, xóa dữ liệu hoặc yêu cầu gỡ bỏ nội dung. Cơ chế này được củng cố về mặt pháp lý thông qua việc ghi nhận các quyền của chủ thể dữ liệu, qua đó tăng cường khả năng tự kiểm soát dữ liệu cá nhân trong môi trường số [2, Điều 9; Điều 11; Điều 16].

Thứ hai, cơ chế dân sự hướng tới việc khôi phục quyền bị xâm phạm và bù đắp các tổn thất phát sinh. Người bị xâm phạm quyền riêng tư có thể yêu cầu chấm dứt hành vi vi phạm, gỡ bỏ thông tin, xin lỗi hoặc cải chính công khai và bồi thường thiệt hại về vật chất, tinh thần. Nền tảng của cơ chế này là nguyên tắc tôn trọng đời sống riêng tư và yêu cầu có sự đồng ý của chủ thể khi thu thập, lưu giữ, sử dụng và công bố thông tin, trừ trường hợp luật định [9, Điều 38].

Thứ ba, cơ chế xử lý hành chính nhằm bảo đảm tuân thủ pháp luật một cách kịp thời và hiệu quả, thông qua việc xử phạt vi phạm hành chính trong lĩnh vực an toàn thông tin, bảo vệ dữ liệu cá nhân và quản lý dịch vụ internet, kèm theo các biện pháp khắc phục hậu quả như buộc gỡ bỏ thông tin hoặc thu hồi, hủy dữ liệu thu thập trái phép. Cơ chế này có ưu thế ở tính linh hoạt và khả năng răn đe tức thời, phù hợp với đặc thù lan truyền nhanh của các hành vi vi phạm trên môi trường mạng [1, Điều 4, Điều 101].

Thứ tư, cơ chế hình sự là biện pháp bảo vệ ở mức độ cao nhất, áp dụng đối với các hành vi xâm phạm quyền riêng tư có tính chất nguy hiểm cho xã hội, có tổ chức hoặc gây hậu quả nghiêm trọng như xâm nhập trái phép, chiếm đoạt hoặc phát tán trái phép dữ liệu cá nhân. Cơ chế này nhằm bảo vệ trật tự, an toàn xã hội và thực hiện chức năng phòng ngừa chung [10, Điều 289].

Nhìn tổng thể, quyền riêng tư chỉ thực sự có khả năng thực thi trong đời sống số khi bốn cơ chế nêu trên được vận hành đồng bộ: cá nhân có công cụ tự bảo vệ; có con đường dân sự để phục hồi quyền và bồi thường; có cơ chế hành chính để cưỡng chế tuân thủ; và có xử lý hình sự đối với các hành vi nguy hiểm xã hội theo tiêu chí luật định.

Cách tiếp cận quyền riêng tư trong môi trường số nêu trên cũng phù hợp với các khuyến nghị của Liên Hợp Quốc và các tổ chức quốc tế, theo đó nhấn mạnh nghĩa vụ của Nhà nước trong việc thiết lập khuôn khổ pháp lý đầy đủ nhằm kiểm soát hoạt động xử lý dữ liệu quy mô lớn và tăng cường trách nhiệm giải trình của các chủ thể nắm giữ quyền lực dữ liệu [7, phần 1]. Các báo cáo và nghị quyết quốc tế đều cảnh báo rằng các hoạt động giám sát, thu thập và phân tích dữ liệu hàng loạt, nếu không được kiểm soát bằng các tiêu chí về tính hợp pháp, cần thiết và tương xứng, có thể dẫn đến xâm phạm nghiêm trọng quyền riêng tư và các quyền con người khác trong môi trường số, qua đó đặt ra yêu cầu các quốc gia phải thường xuyên rà soát và hoàn thiện pháp luật nhằm bảo đảm sự phù hợp với các chuẩn mực nhân quyền quốc tế [13, tr. 4-6].

3. Một số kiến nghị hoàn thiện pháp luật về bảo vệ quyền riêng tư trên môi trường mạng ở Việt Nam

Một số nghiên cứu trong nước chỉ ra rằng, mặc dù quyền riêng tư và bảo vệ dữ liệu cá nhân đã được ghi nhận trong nhiều văn bản pháp luật, song việc bảo vệ quyền riêng tư trên môi trường mạng ở Việt Nam vẫn còn những hạn chế nhất định, thể hiện ở nhận thức xã hội chưa đầy đủ và cơ chế thực thi còn phân tán [6, tr. 218-220]. Bên cạnh đó, các công trình nghiên cứu cũng cho thấy hệ thống pháp luật hiện hành vẫn thiếu các biện pháp kiểm soát hiệu quả đối với các chủ thể xử lý dữ liệu quy mô lớn, đặc biệt là trong bối cảnh chuyển đổi số và sự gia tăng quyền lực dữ liệu của các doanh nghiệp công nghệ, qua đó đặt ra yêu cầu tiếp tục hoàn thiện pháp luật và tăng cường hiệu quả bảo vệ quyền riêng tư trong thời gian tới [12, tr. 191-193].

3.1. Hoàn thiện khung khái niệm và phạm vi bảo vệ quyền riêng tư trong môi trường số

Trong bối cảnh chuyển đổi số, việc hoàn thiện khung khái niệm pháp lý về quyền riêng tư cần phản ánh đầy đủ sự thay đổi của đối tượng và phương thức xâm phạm quyền. Quyền riêng tư trong môi trường số không còn chỉ gắn với việc bảo vệ bí mật đời sống cá nhân theo nghĩa truyền thống mà ngày càng gắn chặt với quyền kiểm soát dữ liệu cá nhân trong toàn bộ vòng đời xử lý dữ liệu. Do đó, pháp

luật cần tiếp cận quyền riêng tư như một quyền có nội hàm động, thể hiện mối liên hệ hữu cơ giữa quyền nhân thân và cơ chế quản trị dữ liệu trong không gian số [11, tr. 102-110].

Theo hướng này cần làm rõ và chuẩn hóa các phương diện cốt lõi của quyền riêng tư, bao gồm: riêng tư thông tin; bảo mật giao tiếp và liên lạc; và quyền tự quyết dữ liệu theo nghĩa vận hành, cho phép cá nhân được biết, được lựa chọn và được kiểm soát cách thức dữ liệu của mình được xử lý. Việc xác định rõ các phương diện này không chỉ bảo đảm tính thống nhất trong áp dụng pháp luật mà còn tạo cơ sở pháp lý rõ ràng cho việc thực thi các quyền của chủ thể dữ liệu trên thực tế [2, Điều 9].

Bên cạnh đó, phạm vi bảo vệ quyền riêng tư cần được mở rộng để bao trùm cả các hoạt động xử lý dữ liệu không trực tiếp xâm phạm "bí mật đời tư" nhưng có khả năng tác động sâu rộng đến quyền tự chủ và phẩm giá cá nhân như phân tích dữ liệu hành vi, suy luận hồ sơ cá nhân hoặc ra quyết định tự động. Cách tiếp cận này góp phần thu hẹp khoảng cách giữa chuẩn mực quốc tế và pháp luật trong nước, đồng thời khắc phục cách hiểu giản lược quyền riêng tư chỉ như "bí mật đời tư" theo nghĩa truyền thống [11, tr. 102-110].

3.2. Tăng cường bảo đảm tính minh bạch, đồng ý có hiểu biết và trách nhiệm giải trình trong xử lý dữ liệu

Pháp luật cần tiếp tục cụ thể hóa các yêu cầu về minh bạch và sự đồng ý có hiểu biết của chủ thể dữ liệu trong toàn bộ vòng đời xử lý dữ liệu, đặc biệt ở các khâu thu thập, sử dụng cho mục đích thứ cấp và chia sẻ dữ liệu với bên thứ ba. Minh bạch cần được hiểu theo nghĩa thực chất, bảo đảm cá nhân có thể nhận biết dữ liệu nào đang được xử lý, vì mục đích gì và bởi chủ thể nào.

Bên cạnh việc ghi nhận các quyền của cá nhân, cần tăng cường nghĩa vụ giải trình của các chủ thể xử lý dữ liệu theo các nguyên tắc bảo vệ dữ liệu hiện đại. Đồng thời, các biện pháp xử lý dữ liệu phải đáp ứng yêu cầu về tính hợp pháp, cần thiết và không mang tính tùy tiện theo chuẩn mực quốc tế về quyền con người [5, tr. 171-173]. Ủy ban Nhân quyền Liên Hợp Quốc cũng nhấn mạnh rằng mọi sự can thiệp vào quyền riêng tư phải được đặt dưới cơ chế kiểm soát chặt chẽ và bảo đảm chống lạm dụng quyền lực [13, tr. 3-4]. Bên cạnh đó, cần hạn chế tình trạng "đồng ý hình thức" bằng cách bảo đảm khả năng lựa chọn thực chất và quyền rút lại sự đồng ý mà không phát sinh hệ quả bất hợp lý [2, Điều 11]. Cách tiếp cận này góp phần kiểm soát quyền lực dữ liệu ngày càng tập trung vào các nền tảng và doanh nghiệp công nghệ trong kỷ nguyên số [11, tr. 102-110].

3.3. Hoàn thiện cơ chế thực thi và tăng cường hiệu quả bảo vệ quyền riêng tư

Để quyền riêng tư có khả năng thực thi thực chất trong môi trường số cần tiếp tục hoàn thiện và tăng cường tính liên thông giữa các cơ chế bảo vệ dân sự, hành chính và hình sự. Ở lĩnh vực dân sự, cần làm rõ cách thức xác định thiệt hại và áp dụng các biện pháp khắc phục phù hợp với đặc thù xâm phạm quyền riêng tư trên môi trường mạng, qua đó bảo đảm khả năng phục hồi quyền cho cá nhân bị xâm phạm. Ở lĩnh vực hành chính, cần bảo đảm tính kịp thời và hiệu quả của các biện pháp xử phạt, gắn với các biện pháp khắc phục hậu quả nhằm ngăn ngừa tái phạm [9, Điều 38]. Đối với cơ chế hình sự, việc áp dụng cần được giới hạn đối với các hành vi có tính chất nguy hiểm cho xã hội, có tổ chức hoặc gây hậu quả nghiêm trọng nhằm bảo đảm tính nhân đạo và tránh hình sự hóa tràn lan [10, Điều 289].

3.4. Tăng cường phối hợp thể chế và nâng cao nhận thức xã hội về quyền riêng tư

Bên cạnh việc hoàn thiện quy phạm pháp luật, hiệu quả bảo vệ quyền riêng tư trên môi trường mạng phụ thuộc đáng kể vào mức độ phối hợp giữa các cơ quan quản lý nhà nước có liên quan. Việc phân định rõ chức năng, thẩm quyền và cơ chế phối hợp liên ngành là điều kiện cần thiết để khắc phục tình trạng phân tán trách nhiệm và chồng chéo trong thực thi, qua đó nâng cao tính thống nhất và hiệu lực của hoạt động bảo vệ quyền riêng tư [6, tr. 218-220].

Song song với đó, cần chú trọng các biện pháp nâng cao nhận thức xã hội về quyền riêng tư và bảo vệ dữ liệu cá nhân giúp cá nhân hiểu đúng và sử dụng hiệu quả các quyền của mình trong môi trường

số. Việc kết hợp giữa hoàn thiện pháp luật, tăng cường phối hợp thể chế và nâng cao nhận thức xã hội không chỉ góp phần xây dựng một cơ chế bảo vệ quyền riêng tư bền vững mà còn phù hợp với yêu cầu bảo đảm quyền con người trong bối cảnh chuyển đổi số hiện nay [5, tr. 171-173].

4. Kết luận

Sự phát triển mạnh mẽ của công nghệ số và môi trường mạng đã làm biến đổi sâu sắc cách thức tạo lập, thu thập và xử lý thông tin cá nhân, qua đó đặt ra những thách thức mới đối với việc bảo vệ quyền riêng tư của cá nhân. Trong bối cảnh đó, quyền riêng tư không còn chỉ được hiểu như một quyền nhân thân gắn với bí mật đời sống cá nhân theo nghĩa truyền thống mà ngày càng gắn chặt với quyền kiểm soát dữ liệu cá nhân và trách nhiệm của các chủ thể xử lý dữ liệu trong toàn bộ vòng đời dữ liệu. Trên cơ sở phân tích một số vấn đề lý luận về quyền riêng tư trên môi trường mạng, bài viết đã làm rõ nội hàm của quyền riêng tư trong bối cảnh số, nhận diện các dạng xâm phạm điển hình và khái quát các cơ chế bảo vệ pháp lý hiện hành. Qua đó cho thấy, mặc dù pháp luật Việt Nam đã có những bước tiến quan trọng trong việc ghi nhận và bảo vệ quyền riêng tư, song vẫn còn tồn tại khoảng cách nhất định giữa chuẩn mực quyền con người, yêu cầu của môi trường số và khả năng thực thi trên thực tế. Từ những phân tích trên, bài viết đề xuất một số kiến nghị hoàn thiện pháp luật theo hướng chuẩn hóa khung khái niệm và phạm vi bảo vệ quyền riêng tư, tăng cường yêu cầu minh bạch, sự đồng ý có hiểu biết và trách nhiệm giải trình trong xử lý dữ liệu, hoàn thiện cơ chế thực thi và nâng cao hiệu quả phối hợp thể chế, đồng thời chú trọng nâng cao nhận thức xã hội về quyền riêng tư và bảo vệ dữ liệu cá nhân. Các kiến nghị này góp phần bảo đảm quyền riêng tư được bảo vệ một cách thực chất, không chỉ trên phương diện ghi nhận pháp lý mà cả trong đời sống số hằng ngày của cá nhân.

Có thể khẳng định rằng, việc bảo vệ quyền riêng tư trên môi trường mạng là một quá trình liên tục, đòi hỏi sự kết hợp đồng bộ giữa hoàn thiện pháp luật, nâng cao hiệu quả thực thi và thay đổi nhận thức xã hội. Trong bối cảnh chuyển đổi số đang diễn ra mạnh mẽ ở Việt Nam, việc tiếp tục nghiên cứu và hoàn thiện pháp luật về bảo vệ quyền riêng tư có ý nghĩa quan trọng không chỉ đối với việc bảo đảm quyền con người mà còn đối với việc xây dựng một môi trường số an toàn, tin cậy và phát triển bền vững.

Tài liệu tham khảo

[1] Chính phủ (2020). *Nghị định số 15/2020/NĐ-CP, ngày 03/02/2020 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.*

[2] Chính phủ (2023). *Nghị định số 13/2023/NĐ-CP, ngày 17/4/2023 về bảo vệ dữ liệu cá nhân.*

[3] Council of Europe (2018). *Convention 108+ – Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.* Strasbourg.

[4] De Hert, P., & Gutwirth, S. (2009). *Privacy, data protection and law enforcement.* Computer Law & Security Review, 25(1).

[5] International Covenant on Civil and Political Rights (1966). *Adopted by the United Nations General Assembly on 16 December 1966, entered into force on 23 March 1976.* United Nations Treaty Series, Vol. 999.

[6] Nguyễn Đăng Dung (2018). *Quyền con người, quyền công dân trong Nhà nước pháp quyền.* NXB Chính trị Quốc gia - Sự thật, Hà Nội.

[7] OECD (2013). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* OECD Publishing, Paris.

[8] Quốc hội (2013). *Hiến pháp nước Cộng hòa xã hội chủ nghĩa Việt Nam.* Thông qua ngày 28/11/2013.

[9] Quốc hội (2015). *Bộ luật Dân sự.* Luật số 91/2015/QH13, ngày 24/11/2015.

[10] Quốc hội (2017). *Luật sửa đổi, bổ sung một số điều của Bộ luật Hình sự số 100/2015/QH13.* Luật số 12/2017/QH14, ngày 20/6/2017.

[11] Solove, D. J. (2008). *Understanding Privacy.* Harvard University Press, Cambridge, MA.

[12] Trần Ngọc Đường (2017). *Bảo vệ quyền con người trong pháp luật Việt Nam.* NXB Chính trị Quốc gia - Sự thật, Hà Nội.

[13] UN Human Rights Committee (1988). *General Comment No. 16: Article 17 (Right to Privacy).* UN Doc. HRI/GEN/1/Rev.1.

[14] United Nations General Assembly (2014). *Resolution 68/167: The Right to Privacy in the Digital Age.* A/RES/68/167.