

BẢO ĐẢM QUYỀN RIÊNG TƯ VỀ DỮ LIỆU CÁ NHÂN TRONG NỀN KINH TẾ DỮ LIỆU Ở VIỆT NAM

BÙI THỊ HƯƠNG

Viện Nhà nước và Pháp luật

- Viện Hàn lâm Khoa học Xã hội Việt Nam

Institute of State and Law, Vietnam Academy of Social Sciences

Email: Huongbui1984@gmail.com

Ngày nhận bài: 21/7/2026

Ngày sửa bài: 12/8/2026

Ngày duyệt đăng bài: 23/8/2026

Tóm tắt:

Dữ liệu đóng vai trò quan trọng trong nền kinh tế dữ liệu. Tuy nhiên, ở chiều ngược lại, mô hình kinh doanh lấy việc khai thác dữ liệu làm trọng tâm tối đa hóa việc thu thập thông tin, tạo ra sự xung đột trực diện với nguyên tắc bảo vệ quyền riêng tư về dữ liệu. Do vậy, trên cơ sở phân tích các quy định pháp luật bảo đảm quyền riêng tư về dữ liệu cá nhân trong nền kinh tế dữ liệu, bài viết nêu ra những thực trạng và từ đó đưa ra một số giải pháp về pháp lý và tổ chức thực hiện để bảo đảm quyền riêng tư về dữ liệu cá nhân trong nền kinh tế dữ liệu ở Việt Nam.

Từ khóa: quyền riêng tư, dữ liệu cá nhân, kinh tế dữ liệu

Ensuring personal data privacy in Vietnam's data economy

Abstract:

Data plays an important role in the data economy. However, business models centered on data exploitation seek to maximize information collection, creating a direct conflict with the principles of data privacy protection. Through an analysis of legal provisions safeguarding personal data privacy in the data economy, this article examines the current situation in Vietnam and proposes legal and implementation-related solutions to ensure personal data privacy.

Keywords: privacy, personal data, data economy

1. Đặt vấn đề

Trong bối cảnh chuyển đổi số và sự phát triển mạnh mẽ của nền kinh tế dữ liệu, dữ liệu cá nhân ngày càng trở thành nguồn lực quan trọng đối với hoạt động kinh doanh, quản trị và cung cấp dịch vụ. Tuy nhiên, việc thu thập, phân tích và khai thác dữ liệu cá nhân với quy mô ngày càng lớn cũng làm gia tăng nguy cơ xâm phạm đảm quyền riêng tư (QRT) của cá nhân. Thực tiễn này đặt ra yêu cầu hoàn thiện cơ chế pháp lý nhằm cân bằng giữa lợi ích khai thác dữ liệu và yêu cầu bảo vệ QRT. Ở Việt Nam, pháp luật về bảo vệ dữ liệu cá nhân đã từng bước được hoàn thiện, song vẫn còn những vấn đề cần tiếp tục nghiên cứu, đặc biệt trong bối cảnh hình thành và phát triển nền kinh tế dữ liệu. Vì vậy, việc nghiên cứu bảo đảm QRT về dữ liệu cá nhân trong nền kinh tế dữ liệu ở Việt Nam có ý nghĩa cả về lý luận và thực tiễn.

2. Pháp luật về bảo đảm quyền riêng tư trong nền kinh tế dữ liệu

Trên phạm vi toàn cầu, quy định trực tiếp về phát triển kinh tế dữ liệu và bảo đảm QRT hiện nay chưa có một quy định riêng. Khi đề cập đến riêng tư về dữ liệu chúng ta có hướng dẫn của OECD về việc chuyển dữ liệu xuyên biên giới (OECD, 2013), đưa ra 8 nguyên tắc cốt lõi mà mỗi quốc gia cần tuân thủ: (1) Hạn chế thu thập; (2) Chất lượng dữ liệu; (3) Xác định mục đích; (4) Hạn chế sử dụng; (5) Bảo vệ an ninh; (6) Công khai; (7) Tham gia cá nhân; (8) Trách nhiệm giải trình.

OECD nhấn mạnh thêm trong một nền kinh tế dữ liệu việc bảo vệ QRT không thể thực hiện bằng các mệnh lệnh hành chính cực đoan làm triệt tiêu dòng chảy dữ liệu, mà đòi hỏi phải giải quyết bằng các chiến lược (OECD, 2013):

- + Xây dựng khung pháp lý bảo đảm QRT trong nền kinh tế dữ liệu.
- + Khuyến khích sử dụng các công nghệ tăng cường QRT.
- + Thúc đẩy các giải pháp hợp đồng mẫu cho việc chuyển dữ liệu xuyên biên giới trực tuyến.
- + Nâng cao nhận thức và giáo dục người dùng về QRT trực tuyến.

Dưới góc độ pháp lý, để giải quyết mâu thuẫn giữa phát triển kinh tế số và bảo vệ quyền con người, các khu vực và quốc gia trên thế giới đã phát triển những mô hình lập pháp khác nhau để bảo vệ QRT.

2.1. Về bảo vệ dữ liệu của Liên minh Châu Âu (GDPR)

Quy định chung về bảo vệ dữ liệu của EU (GDPR - Quy định (EU) 2016/679): Được coi là “tiêu chuẩn vàng” toàn cầu. GDPR xác lập các nguyên tắc xử lý dữ liệu chặt chẽ và ghi nhận các quyền đột phá như Quyền được lãng quên (Điều 17) và Quyền di chuyển dữ liệu (Điều 20). GDPR áp dụng chế tài nghiêm khắc (phạt đến 20 triệu Euro hoặc 4% tổng doanh thu toàn cầu hằng năm) và có hiệu lực ngoài lãnh thổ (Điều 3(2)).

Hoa Kỳ: Hoa Kỳ lựa chọn mô hình lập pháp phân tán và tiếp cận theo định hướng thị trường. Ở cấp độ liên bang, Hoa Kỳ không có một đạo luật bảo vệ dữ liệu cá nhân toàn diện mà quy định rải rác trong các luật chuyên ngành (như Luật Bảo mật thông tin y tế - HIPAA, Luật Bảo vệ QRT trực tuyến của trẻ em - COPPA, Luật Báo cáo tín dụng công bằng - FCRA) (Kalash, 2026).

Tuy nhiên, trước áp lực của tình trạng lộ lọt thông tin, các bang tại Mỹ đã chủ động ban hành các đạo luật nghiêm khắc riêng biệt. Điển hình là bang California với Đạo luật QRT của người tiêu dùng California (California Consumer Privacy Act - CCPA) - (California Department of Justice), đạo luật mang nhiều nét tương đồng với GDPR khi trao cho người tiêu dùng quyền được biết rõ những thông tin nào đang bị thu thập, quyền từ chối việc mua bán dữ liệu cá nhân (opt-out), quyền yêu cầu xóa dữ liệu và quyền không bị phân biệt đối xử khi thực hiện các QRT của mình. Mô hình của Mỹ cho thấy, sự dịch chuyển dần từ việc thả nổi thị trường sang việc thiết lập các giới hạn để bảo vệ người tiêu dùng trong nền kinh tế số.

2.2. Pháp luật về bảo đảm QRT về dữ liệu trong nền kinh tế dữ liệu ở Việt Nam

Hiến pháp năm 2013: Điều 21 khẳng định quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân, bí mật gia đình và yêu cầu pháp luật bảo đảm an toàn các thông tin này.

Bộ luật Dân sự năm 2015: Điều 38 quy định đời sống riêng tư, bí mật cá nhân, bí mật gia đình được pháp luật bảo vệ; việc thu thập, lưu giữ, sử dụng, công khai thông tin về các nội dung này phải có sự đồng ý của người có liên quan.

Trên môi trường số: chúng ta có các quy định bảo đảm QRT về dữ liệu cá nhân ở Luật Bảo vệ dữ liệu cá nhân năm 2025, các quyền của chủ thể dữ liệu quy định tại Điều 4 (được biết, đồng ý/rút lại đồng ý, xem/chỉnh sửa, yêu cầu xóa/hạn chế xử lý, khiếu nại, yêu cầu bồi thường). Và các quy định bảo đảm QRT về dữ liệu được quy định cụ thể trong các điều khoản của Luật và Nghị định số 356/2025/NĐ-CP hướng dẫn thi hành luật đã phân biệt rõ dữ liệu cá nhân nhạy cảm và dữ liệu cá nhân cơ bản, đồng thời có quy định trách nhiệm của tổ chức, cá nhân (Điều 9-23, 29-30 và NĐ 356): trong các khâu thu thập, mã hóa, chỉnh sửa, xóa dữ liệu; nghĩa vụ của nền tảng truyền thông trực tuyến, blockchain trong bảo vệ dữ liệu.

Một số lĩnh vực khác cũng có quy định bảo vệ QRT về dữ liệu cá nhân như:

Luật Bảo vệ quyền lợi người tiêu dùng 2023 quy định nghiêm ngặt về việc thu thập, sử dụng thông tin của người tiêu dùng từ Điều 15-20 với các yêu cầu cụ thể: doanh nghiệp phải công khai chính sách bảo vệ dữ liệu, chỉ thu thập, sử dụng thông tin khi có sự đồng ý và đúng mục đích đã thông báo; không được chia sẻ cho bên thứ ba nếu chưa được phép. Người tiêu dùng có quyền kiểm tra, chỉnh sửa, hủy bỏ, chuyển giao dữ liệu; Đồng thời, chủ thể kinh doanh phải có biện pháp ngăn chặn truy cập trái phép và báo cáo cơ quan chức năng trong vòng 24 giờ khi xảy ra sự cố mất an toàn dữ liệu.

Luật Thương mại điện tử 2025 và Nghị định số 248/2026/NĐ-CP ngày 30/6/2026 quy định một số điều của Luật Thương mại Điện tử yêu cầu các bên phải xây dựng và công khai chính sách bảo vệ thông tin cá nhân. Điều 5 Nghị định gồm các nội dung: a) Mục đích, phạm vi thu thập thông tin của người sử dụng; b) Phạm vi sử dụng thông tin; c) Thời gian lưu trữ thông tin hoặc phương pháp xác định thời gian lưu trữ thông tin; d) Tổ chức, cá nhân có thể được tiếp cận thông tin cá nhân;

Điều 6, Nghị định 248/2026/NĐ-CP quy định chủ quản nền tảng phải: Áp dụng ... để bảo đảm an toàn ... thông tin cá nhân của người tiêu dùng (điểm g, khoản 1).

Luật Viễn thông 2023: Điều 6 quy định: 3. Thông tin riêng... cá nhân chuyển qua mạng viễn thông công cộng được bảo đảm bí mật.

4. Doanh nghiệp... không được tiết lộ thông tin riêng.... đến người sử dụng dịch vụ viễn thông, bao gồm thông tin thuê bao viễn thông (tên, địa chỉ, số thuê bao viễn thông và thông tin riêng khác mà người sử dụng cung cấp khi giao kết hợp đồng với doanh nghiệp)...

Trong lĩnh vực tài chính - ngân hàng

Luật Các Tổ chức Tín dụng năm 2024, tại khoản 2 và 3 Điều 13, nhấn mạnh: “2. Tổ chức tín dụng ... phải bảo đảm bí mật thông tin khách hàng...

3. ...không được cung cấp thông tin khách hàng... trừ trường hợp có yêu cầu của cơ quan nhà nước có thẩm quyền theo quy định của luật hoặc được sự chấp thuận của khách hàng.”....

2.3. Những kết quả đạt được trong công tác bảo vệ QRT về dữ liệu cá nhân trong nền kinh tế dữ liệu

Thứ nhất, hệ thống pháp luật đồng bộ quy định bảo vệ QRT về dữ liệu của người tiêu dùng trong nền kinh tế dữ liệu.

Thứ hai, nhận thức xã hội được nâng cao. người dân Việt Nam hiện nay đã ý thức rõ rệt về giá trị của

dữ liệu và các quyền hợp pháp của mình, bắt đầu có thói quen phản ứng và từ chối cung cấp thông tin khi thấy không an toàn.

Thứ ba, doanh nghiệp chủ động chuyển đổi tư duy. Các tổ chức tài chính, ngân hàng, tập đoàn viễn thông và doanh nghiệp thương mại điện tử đã bắt đầu đầu tư nguồn lực lớn để rà soát quy trình, xây dựng lại các điều khoản bảo mật thông tin, chỉ định nhân sự phụ trách bảo vệ dữ liệu theo yêu cầu bắt buộc của pháp luật (Điều 33 Luật Bảo vệ Dữ liệu cá nhân và Điều 13-16 Nghị định số 356/2025).

Thứ tư, hiệu quả quản lý nhà nước được siết chặt. Cơ quan chuyên trách bảo vệ dữ liệu cá nhân (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - A05, Bộ Công an) đã tăng cường thanh tra, kiểm tra và triệt phá thành công nhiều đường dây mua bán dữ liệu cá nhân quy mô lớn, xử phạt nghiêm các hành vi vi phạm an toàn thông tin. Nghị định 356/2025/NĐ-CP còn quy định chi tiết về kiểm tra hoạt động bảo vệ dữ liệu cá nhân (Điều 31), bao gồm kiểm tra đột xuất không cần thông báo trước.

Thứ năm, hạ tầng dịch vụ công trực tuyến được gia cố. Các hệ thống thông tin quốc gia, đặc biệt là Cơ sở dữ liệu quốc gia về dân cư, luôn đặt tiêu chuẩn an toàn bảo mật ở mức độ cao nhất nhằm ngăn ngừa nguy cơ tấn công xâm nhập từ bên ngoài. Việt Nam cũng không ngừng mở rộng hợp tác quốc tế, ký kết các thỏa thuận về an ninh an toàn mạng để giải quyết các luồng dữ liệu xuyên biên giới, phù hợp với các cơ chế chuyển dữ liệu xuyên biên giới (APEC, 2019).

2.4. Những hạn chế và thách thức trong nền kinh tế dữ liệu

Dù đạt được những bước tiến lớn về mặt lập pháp, thực tế bảo đảm QRT trong nền kinh tế dữ liệu tại Việt Nam vẫn đối mặt với những lỗ hổng và rào cản:

Tình trạng lộ lọt, mua bán dữ liệu diễn ra phổ biến và tinh vi: Dữ liệu cá nhân bị rao bán công khai trên các hội nhóm mạng xã hội đen (Telegram, các diễn đàn ngầm) từ số điện thoại, thông tin định danh cá nhân cho đến dữ liệu số dư tài khoản ngân hàng. Ngay cả những cơ quan chuyên sâu việc lộ lọt thông tin cũng có thể xảy ra.

Xu hướng lạm dụng thu thập dữ liệu quá mức của các ứng dụng: Nhiều ứng dụng di động thông thường như trò chơi giải trí, chỉnh sửa ảnh hoặc app mua sắm lại đòi hỏi người dùng phải cấp quyền truy cập vào danh bạ, vị trí GPS theo thời gian thực và kho ảnh cá nhân. Nếu không đồng ý, người dùng sẽ bị từ chối quyền trải nghiệm dịch vụ.

Người dân còn thiếu hụt kỹ năng tự bảo vệ nghiêm trọng: người dùng internet tại Việt Nam vẫn duy trì thói quen chia sẻ thông tin cá nhân, hình ảnh căn cước công dân, thông tin cá nhân... lên mạng xã hội, tạo điều kiện thuận lợi cho các đối tượng lừa đảo công nghệ cao thực hiện các hành vi trục lợi.

Cơ chế giám sát và chế tài chưa đủ sức răn đe: Mặc dù Luật Bảo vệ dữ liệu cá nhân năm 2025 đã quy định mức phạt lên đến 5% doanh thu, nhưng các văn bản hướng dẫn chi tiết về xử phạt hành chính và hình sự đối với hành vi xâm phạm dữ liệu có lúc vẫn chưa bắt kịp với lợi nhuận khổng lồ mà các đối tượng thu được từ việc kinh doanh dữ liệu lậu.

Thách thức từ các nền tảng xuyên biên giới và công nghệ mới: Việc kiểm soát, chế tài các hành vi vi phạm QRT của các nền tảng công nghệ toàn cầu không có đại diện pháp lý đầy đủ tại Việt Nam luôn là bài toán đau đầu đối với các cơ quan quản lý. Thêm vào đó, sự trỗi dậy mạnh mẽ của Trí tuệ nhân tạo (AI) và Dữ liệu lớn (Big Data) đang tạo ra các hình thức giám sát kỹ thuật số tự động, thao túng tâm lý hành vi người dùng thông qua các thuật toán hộp đen tinh vi, gây khó khăn cho công tác phát hiện và xử lý.

3. Một số kiến nghị nhằm bảo đảm quyền riêng tư trong nền kinh tế dữ liệu tại Việt Nam

Để xây dựng một nền kinh tế dữ liệu phát triển bền vững, an toàn, vừa tạo ra giá trị thịnh vượng kinh tế cao vừa bảo vệ vững chắc QRT dữ liệu cá nhân, Việt Nam cần triển khai một số giải pháp sau:

Thứ nhất, hoàn thiện hệ thống pháp luật dựa trên nguyên tắc lấy con người làm trung tâm

Tiếp tục ban hành các văn bản hướng dẫn thi hành Luật Bảo vệ dữ liệu cá nhân năm 2025 nhằm làm rõ các quy trình kỹ thuật, biểu mẫu báo cáo đánh giá tác động và cơ chế vận hành của cơ quan chuyên trách. Nghị định số 356/2025/NĐ-CP đã bước đầu thực hiện điều này với các mẫu biểu cụ thể (Mẫu 01a-10) và quy định chi tiết về hồ sơ đánh giá tác động. Tuy nhiên, cần quy định phân định rõ ràng, cụ thể trách nhiệm pháp lý của từng chủ thể tham gia vào chuỗi xử lý dữ liệu bao gồm: Bên Kiểm soát dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân và Bên Kiểm soát và xử lý dữ liệu cá nhân (Điều 2 Luật Bảo vệ Dữ liệu cá nhân). Cần có hướng dẫn cụ thể về hợp đồng giữa các bên theo Điều 7 Nghị định 356/2025.

Hoàn thiện cơ chế khiếu kiện khi bị vi phạm: Thực tế đã có rất nhiều hành vi vi phạm pháp luật do quyền bảo vệ dữ liệu cá nhân bị xâm phạm nhưng cơ chế để khiếu nại, khiếu kiện bảo vệ quyền không hiệu quả. Hiện nay, khi các hành vi lừa đảo trên không gian mạng do các lỗ hổng bảo mật người dân được khuyến cáo đến Công an phường/xã nơi cư trú hoặc Phòng An ninh mạng và phòng, chống tội phạm công nghệ cao (PA05) thuộc Công an cấp tỉnh/thành phố (Nhân Dân, n.d.). Tuy nhiên, các vụ việc người dân trình báo được xử lý vô cùng ít.

Hoàn thiện chế tài hình sự: nên hình sự hóa các hành vi xâm phạm dữ liệu cá nhân trên môi trường số, có điều luật riêng về tội phạm xâm phạm dữ liệu cá nhân thay vì một số hành vi sẽ áp vào quy định của Điều 226 - Tội sử dụng trái phép trên mạng và trong máy tính như hiện nay.

Bảo đảm thực thi trọn vẹn và thực chất các quyền tối cao của công dân đối với dữ liệu của mình: quyền được biết, quyền truy cập, quyền chỉnh sửa, quyền phản đối xử lý và đặc biệt là cơ chế yêu cầu xóa dữ liệu cá nhân (quyền được lãng quên) trên môi trường số, theo đúng tinh thần Điều 4 và Điều 14 Luật Bảo vệ Dữ liệu cá nhân. Pháp luật Việt Nam phải luôn kiên định tiếp cận theo nguyên tắc lấy con người làm trung tâm, tạo dựng sự cân bằng hài hòa giữa phát triển kinh tế số với bảo vệ quyền con người.

Thứ hai, tăng cường quản trị dữ liệu và nâng cao trách nhiệm của cộng đồng doanh nghiệp

Các doanh nghiệp hoạt động trong nền kinh tế số cần thực hiện nghiêm túc các nghĩa vụ:

Minh bạch hóa tuyệt đối chính sách dữ liệu: Xây dựng các điều khoản bảo mật với ngôn từ rõ ràng, ngắn gọn, dễ hiểu; thông báo đầy đủ cho người dùng về mục đích, phạm vi, thời gian lưu trữ và các bên thứ ba có thể tiếp cận dữ liệu. Tuyệt đối không sử dụng các bẫy giao diện (dark patterns) để lừa dối người dùng ký chấp thuận. Yêu cầu này phù hợp với nguyên tắc minh bạch trong GDPR (Điều 12) và Điều 9 Luật Bảo vệ Dữ liệu cá nhân về sự đồng ý của chủ thể dữ liệu.

Tuân thủ nghiêm ngặt nguyên tắc tối thiểu hóa: Chỉ thực hiện thu thập đúng và đủ những trường dữ liệu thực sự cần thiết trực tiếp cho việc vận hành và cung cấp dịch vụ, chấm dứt triệt để tình trạng thu thập dữ liệu dư thừa, bao vây. Nguyên tắc này được khẳng định trong GDPR (Điều 5(1)(c)) và Luật Bảo vệ Dữ liệu cá nhân (Điều 3(2)).

Đầu tư hạ tầng an toàn bảo mật hiện đại: Chủ động áp dụng các công nghệ mã hóa tiên tiến, thiết lập các hệ thống tường lửa, phòng chống mã độc và định kỳ tổ chức diễn tập ứng phó sự cố an ninh mạng. Nâng cao năng lực và trách nhiệm giải trình trước cơ quan quản lý nhà nước và khách hàng khi xảy ra sự cố lộ lọt thông tin. Theo Điều 23 Luật Bảo vệ Dữ liệu cá nhân và Điều 28 Nghị định 356/2025, doanh nghiệp có nghĩa vụ thông báo vi phạm cho cơ quan chuyên trách trong vòng 72 giờ kể từ khi phát hiện.

Xây dựng cơ chế kiểm toán thuật toán: Đối với các doanh nghiệp ứng dụng hệ thống Trí tuệ nhân tạo (AI) và Dữ liệu lớn để phân tích hành vi, cần phải xây dựng quy trình đánh giá tác động QRT và kiểm toán

thuật toán định kỳ nhằm bảo đảm các quyết định tự động của máy tính không gây phân biệt đối xử hoặc xâm phạm thô bạo vào đời sống riêng tư của khách hàng. Điều 30 Luật Bảo vệ Dữ liệu cá nhân và Điều 10 Nghị định 356/2025 đã đặt ra các yêu cầu cụ thể đối với xử lý dữ liệu trong AI, yêu cầu phân loại rủi ro và tích hợp biện pháp bảo mật.

Thứ ba, nâng cao nhận thức, phổ cập kỹ năng số và giáo dục quyền số cho người dân

Đẩy mạnh truyền thông, giáo dục pháp luật về QRT và Luật Bảo vệ dữ liệu cá nhân năm 2025; trang bị kỹ năng số thiết yếu như bảo mật tài khoản, nhận diện lừa đảo, quản lý quyền truy cập và sử dụng mạng xã hội an toàn. Đồng thời, đưa giáo dục về “quyền số” và an toàn thông tin vào nhà trường, kết hợp phổ biến kiến thức trong cộng đồng.

Thứ tư, đẩy mạnh hợp tác quốc tế sâu rộng và thực chất

Do không gian mạng không có biên giới và dữ liệu liên tục lưu chuyển xuyên biên giới, bảo vệ QRT đòi hỏi Việt Nam tăng cường hợp tác quốc tế, chia sẻ kinh nghiệm với các quốc gia và tổ chức quốc tế như EU, APEC về quản trị dữ liệu và mô hình cơ quan bảo vệ dữ liệu độc lập. Đặc biệt, Việt Nam nên xem xét tham gia Hệ thống Quy tắc riêng tư xuyên biên giới APEC (APEC CBPR) - một cơ chế tự nguyện cho phép các doanh nghiệp được chứng nhận tuân thủ các tiêu chuẩn bảo vệ dữ liệu khi chuyển dữ liệu giữa các nền kinh tế thành viên (APEC 2019). Đồng thời, cần xây dựng cơ chế phối hợp, ký kết các hiệp định tương trợ tư pháp để điều tra, xử lý các vi phạm dữ liệu xuyên quốc gia, nhất là hành vi đánh cắp, tống tiền bằng dữ liệu của tội phạm mạng quốc tế.

4. Kết luận

Dữ liệu cá nhân đã vươn lên trở thành tài nguyên của nền kinh tế số. Tuy nhiên, sự thịnh vượng kinh tế này sẽ không thể bền vững và sẽ trở nên vô nghĩa nếu nó được xây dựng trên sự xâm phạm QRT và các quyền tự do cơ bản của con người. Việc bảo đảm QRT trong thời đại số không còn dừng lại ở một khẩu hiệu đạo đức hay một yêu cầu pháp lý đơn thuần, mà nó đã trở thành điều kiện tiên quyết, là viên gạch nền móng vững chắc để xây dựng một môi trường số an toàn, lành mạnh, tin cậy và phát triển bền vững cho toàn xã hội ■

Nghiên cứu này là sản phẩm của Đề tài khoa học cấp cơ sở năm 2026: “Pháp luật về bảo đảm quyền riêng tư của cá nhân trong môi trường số”, chủ nhiệm đề tài: ThS. Bùi Thị Hương.

TÀI LIỆU TRÍCH DẪN VÀ THAM KHẢO:

- Bảo Minh (2026). Phải làm gì khi bị lừa đảo trực tuyến. Báo Nhân dân <https://nhandan.vn/special/phai-lam-gi-khi-bi-lua-dao-truc-tuyen/index.html>
- APEC. (2019). APEC Cross-Border Privacy Rules (CBPR) System: Policies, Rules and Guidelines. Updated November 2019.
- California Department of Justice, Office of the Attorney General. (n.d.). California Consumer Privacy Act (CCPA). Truy cập tại: <https://www.oag.ca.gov/privacy/ccpa>
- Kalash, S. Y. (2026). Cross-Border Data Transfer Regimes: Current Landscape and Outlook Ahead. CIGI Papers, số 350, tháng 2/2026, tr. 8.
- Organisation for Economic Co-operation and Development (OECD). (2013). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD Publishing.