Cải cách pháp luật đáp ứng nhu cầu bảo vệ dữ liệu cá nhân trong chuyển đổi số

TS. Dương Kim Thế Nguyên ThS. Huỳnh Thiên Tứ ThS. Lê Thùy Khanh ThS. Mai Nguyễn Dũng

UEH University

CẢI CÁCH PHÁP LUẬT ĐÁP ỨNG NHU CẦU BẢO VỆ DỮ LIỆU CÁ NHÂN TRONG CHUYỂN ĐỔI SỐ

TS. Dương Kim Thế Nguyên

ThS. Huỳnh Thiên Tứ

ThS. Lê Thùy Khanh

ThS. Mai Nguyễn Dũng

Khoa Luật, Trường Đại Học Kinh Tế TP.HCM

TÓM TẮT

Sự bùng nổ của các thành tựu công nghệ đặt ra nhiều vấn đề về quyền riêng tư cá nhân, do lượng lớn dữ liệu mà các công nghệ này sử dụng trực tiếp đến từ thông tin cá nhân của người dùng. Nghiên cứu này nhằm chỉ ra nhu cầu điều chỉnh về mặt pháp lý đối với việc tiếp nhận thông tin và xử lý dữ liệu cá nhân trên cơ sở đánh giá tổng quan các quy định pháp luật hiện hành, đối sánh với các quy định bảo vệ dữ liệu cá nhân của một số nước trên thế giới. Qua nghiên cứu, nhóm tác giả đề xuất hai nhóm nguyên tắc lập quy nhằm cân bằng lợi ích giữa các chủ thể, đồng thời đề xuất sửa đổi, bổ sung các quy định pháp luật hiện hành theo hướng thống nhất ghi nhận quyền nhân thân đối với thông tin cá nhân, tách bạch cơ chế điều chỉnh giữa quan hệ xử lý dữ liệu cá nhân với dữ liệu công nghiệp, trung hòa xung đột thông qua cơ chế quy chuẩn, kiểm định, đánh giá tín nhiệm số đối với các chủ thể xử lý dữ liệu.

Từ khóa: *bảo vệ dữ liệu, dữ liệu cá nhân, dữ liệu công nghiệp, quyền riêng tư.*

1. ĐẶT VẤN ĐỀ

1.1 Vai trò của dữ liệu trong kỷ nguyên kinh tế số

Những năm gần đây, nền kinh tế toàn cầu đang đứng trước sự thay đổi với quy mô chưa từng thấy trong lịch sử. Quá trình định hình cuộc cách

mạng công nghiệp 4.0 (CMCN 4.0) đã và đang tạo ra những giá trị mới, được kì vọng sẽ mang đến sự thịnh vượng và thay đổi cán cân bình đẳng xã hội. Sự thay đổi này được đánh dấu bởi tốc độ đổi mới nhanh chóng của các công nghệ thông tin viễn thông hiện đại (information & communication technologies – ICTs), gắn liền với quy mô ứng dụng rộng khắp của chúng xuyên suốt mọi ngành, nghề, lĩnh vực trong đời sống kinh tế xã hội.

Ba trụ cột chính về mặt công nghệ đóng vai trò thúc đẩy mô hình phát triển của nền kinh tế số hiện đại lần lượt là mạng lưới viễn thông siêu kết nối (Internet of Things hay IoT), nền tảng dữ liệu lớn (big data) và các thuật toán xử lý hiện đại, thường được biết đến với cái tên "trí tuệ nhân tạo" (Artificial Intelligence, AI). Với tốc độ dẫn truyền không ngừng được cải thiện và gia tăng, mạng internet đang dần được ứng dụng rộng rãi để tạo ra hệ thống kết nối giữa các sản phẩm công nghệ phục vụ người dùng, rút ngắn khoảng cách giữa kĩ thuật công nghệ và nhu cầu đời sống thường nhật (Lasse Eriksson và c.s., 2019; Martti Mäntylä, 2019; Weber & Weber, 2010). Công nghệ AI, đặt nền tảng trên các kĩ thuật học máy (machine learning), học sâu (deep learning), có khả năng xử lý lượng dữ liệu đồ sộ và đưa ra quyết định một cách tự động dựa trên kết quả tổng hợp, phân loại và sắp xếp dữ liệu đầu vào một cách liên tục (Schwab & Davis, 2018; Wachter & Mittelstadt, 2019).

Tuy nhiên, để các công nghệ trên có thể vận hành đúng kì vọng, không thể bỏ qua vai trò trọng tâm của dữ liệu. Dữ liệu trở thành trung tâm của quá trình chuyển đổi số, khi chúng hàm chứa không chỉ kiến thức khoa học công nghệ, thông tin kế toán, tài chính, thị trường phục vụ cho mục đích kinh doanh, mà còn bao gồm các thông tin định danh gắn liền với cá nhân người dùng ngoài đời thực, từ họ tên, tuổi, giới tính, hộ tịch, dân tộc, quê quán, đến thói quen, sở thích, xu hướng, sức khỏe, v.v. Dữ liệu là "nguồn tài nguyên cốt yếu" trong nền kinh tế số (European Commission, 2017), là trụ cột trung tâm để phát triển hệ thống vận hành tự động, cải tiến quy trình cung cấp và duy trì dịch vụ (Sam Wrigley, Anette Alén-Savikko & Olli Pitkänen, 2019). Không hề là quá khi nói rằng, dữ liệu là động lực chính yếu trong quá trình chuyển đổi số.

1.2 Giá trị của dữ liệu và tính dễ tổn thương của dữ liệu cá nhân

Tầm quan trọng của dữ liệu đối với nền kinh tế số còn được thể hiện thông qua những giá trị kinh tế mang lại cho các chủ thể nắm quyền đối với dữ liệu. Các nhà nghiên cứu thuộc lĩnh vực kinh tế (Davenport & Bean, 2018; OECD, 2013), công nghệ thông tin (Ben Ayed, 2014; Chowdhury và c.s., 2018; Onik và c.s., 2019) và pháp lý (Bygrave, 2014; Craig & Ludloff, 2011; Hoeren, 2014; Malgieri & Custers, 2017; Martti Mäntylä, 2019; Purtova, 2012; XING Hui-Qiang, 2019) đều nhất trí rằng, trong kỷ nguyên số, mặc dù thông tin thu thập được từ nguồn dữ liệu "thô" trong đời thực (Nick Barrowman, 2018) không mang giá trị, nhưng các chủ thể xử lý khi thu thập dữ liệu theo những mục đích của họ đã tạo ra cho dữ liệu cá nhân này giá trị sử dụng tiềm năng bởi chúng được thu thập, phân tích và kết hợp lại với nhau thành kho dữ liệu lớn bằng các phương tiện thuật toán. Chính nhờ vào sự tập hợp thành dữ liệu lớn đã tăng khả năng khai thác và tạo nên những giá trị gia tăng. Trong lĩnh vực thương mại điện tử, dữ liệu được biến thành thông tin chuyên sâu bằng công nghệ phân tích dữ liệu lớn (BDA). Từ đó hỗ trợ công tác ra quyết định và giải quyết vấn đề phát sinh, mang lại giá trị cho doanh nghiệp (Akter & Wamba, 2016; Amit & Zott, 2017). Đối với mô hình kinh tế chia sẻ, công nghệ BDA là "bộ công cụ" của các chủ thể kinh doanh dịch vụ kết nối trung gian nhằm khai thác thông tin từ các bên tham gia vào mô hình chia sẻ, nhằm tiến hành phân loại, nhóm và kết nối các bên lại với nhau (Sedkaoui & Khelfaoui, 2020). Theo một khảo sát được tiến hành vào năm 2019, chỉ có 6% doanh nghiệp Việt Nam tham gia khảo sát thấy được tầm quan trọng của dữ liệu lớn (Cameron A. và c.s., 2019), tuy nhiên, theo Allied Market Research, vào năm 2019, thị trường BDA toàn cầu được định giá lên đến 193,14 tỷ USD (Rob Sobers, 2021).

Do mang giá trị gia tăng dần theo thời gian và theo thuật toán khai thác xử lý chúng, dữ liệu đã trở thành đối tượng của tội phạm an ninh mạng. Từ năm 2013 đến năm 2019, đã có 9.727.967.988 trường hợp hồ sơ dữ liệu bị mất hoặc bị đánh cắp trên toàn cầu; Ấn Độ, Trung Quốc và Hàn Quốc là ba quốc gia đứng đầu về số vụ vi phạm dữ liệu, trong khi Việt Nam đứng thứ hai trong nhóm từ 100.000 đến một triệu vụ (Rob Sobers, 2021). Vì lẽ đó, an toàn và an ninh dữ liệu đã trở thành một trong những mối quan tâm sâu sắc nhất trong chính sách chuyển đổi số ở khu vực công (Kramer và c.s., 2009; Schwab & Davis, 2018), bên cạnh đó, các doanh nghiệp dân

doanh đang chủ động hướng tới các kênh phòng ngừa rủi ro từ sự cố an toàn dữ liệu, điển hình như các sản phẩm bảo hiểm trách nhiệm dân sự trong trường hợp rò rỉ thông tin người dùng (Anderson & Moore, 2006; Pal và c.s., 2014).

Dữ liệu cá nhân chiếm tỷ trọng cao trong cơ sở dữ liệu lớn (Craig & Ludloff, 2011; Kalyvas & Overly, 2015; Malgieri, 2016), là đối tượng bị xâm phạm nghiêm trọng nhất, vì chúng liên quan trực tiếp đến thông tin nhân thân của cá nhân, có giá trị định danh và có thể bị lợi dụng để tiến hành các giao dịch giả mạo (Craig & Ludloff, 2011; Sam Wrigley, Anette Alén-Savikko & Olli Pitkänen, 2019; Truong và c.s., 2020). Sâu xa hơn, xâm phạm dữ liệu cá nhân là xâm phạm quyền riêng tư của con người (Schwartz, 2005). Ngay tại Việt Nam, tình trạng xâm phạm, đánh cắp và rao bán dữ liệu cá nhân trên mạng đã và đang diễn ra một cách công khai trên các diễn đàn mở, với mức độ ngày càng nghiêm trọng, quy mô ngày càng lớn và kĩ thuật tinh vi. Chỉ trong 6 (sáu) tháng đầu năm 2021, đã có hơn 3 (ba) vụ rao bán công khai dữ liệu cá nhân người dùng Việt Nam trên các diễn đàn với tổng dung lượng dữ liệu của 3 vụ là xấp xỉ 20GB. Cụ thể, vào ngày 17/1/2021, hơn 2GB cơ sở dữ liệu khách hàng, bao gồm tên, địa chỉ, số điện thoại, tài khoản, số dư… được rao bán. Tiếp đó, vào tháng 4/2021, dữ liệu của 2,8 triệu doanh nghiệp và 8,38 triệu công dân Việt Nam được rao bán công khai. Gần đây nhất, vào tháng 5/2021, 17 GB dữ liệu chứa ảnh chụp chứng minh thư nhân dân, căn cước công dân (sau đây gọi chung là ID), ảnh/video selfie của người Việt lại trở thành sản phẩm để mua bán. Các file này chứa tên, ngày sinh, ảnh đại diện, địa chỉ, email, số điện thoại, số ID của công dân, được rao bán với giá 9,000 USD (Anh Quân & Thành Luân, 2021).

1.3 Bối cảnh chính sách bảo vệ dữ liệu cá nhân tại Việt Nam

Nhận thức được tầm quan trọng của việc phát triển công nghệ và cơ sở dữ liệu lớn song song với công tác bảo vệ an toàn dữ liệu cá nhân, Quyết định số 2289/QĐ-TTg ban hành ngày 31/12/2020 của Thủ tướng chính phủ về ban hành chiến lược quốc gia về cách mạng công nghiệp lần thứ tư đến năm 2030 đã đề ra nhiệm vụ chiến lược cho các bộ, ngành, cơ quan, trong đó, chú trọng nâng cao nhận thức của tổ chức, người dân về bảo vệ dữ liệu cá nhân, quản trị dữ liệu, xây dựng hạ tầng cơ sở dữ liệu phục vụ công tác

chuyển đổi số song song với chính sách về dữ liệu mở, xây dựng các giải pháp chia sẻ dữ liệu, phát triển nền tảng tích hợp, kết nối, chia sẻ dữ liệu quốc gia để cùng khai thác, sử dụng, tạo thuận lợi cho thương mại hóa dữ liệu. Quyết định 749/QĐ-TTg phê duyệt "Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030" cũng đưa ra nhiệm vụ, giải pháp cụ thể nhằm tạo lập niềm tin, đảm bảo an toàn, an ninh mạng, bảo vệ dữ liệu cá nhân; trong đó gồm các nhiệm vụ lập pháp cụ thể như được trình bày trong Bảng 1.

Xây dựng chính sách phát triển và quy tắc ứng xử trong môi trường số	Xây dựng cơ chế quản trị rủi ro trong môi trường số	Chính sách bảo đảm an toàn, an ninh mạng
•Nghiên cứu kinh nghiệm quốc tế nhằm xây dựng bộ quy tắc ứng xử, tạo lập niềm tin trên môi trường số (Điểm (a), Mục 5, Phần IV, Quyết định 749/QĐ/TTg) •Xây dựng văn hóa số Việt Nam (Điểm (a), Mục 5, Phần IV, Quyết định 749/QĐ/TTg) •Xây dựng cơ chế hợp tác, đối thoại giữa nhà nước và các cơ quan, hiệp hội ngành nghề, doanh nghiệp (Điểm (b), Mục 5, Phần IV, Quyết định 749/QĐ/TTg)	•Xây dựng hệ thống đánh giá tín nhiệm đối với doanh nghiệp cung cấp dịch vụ trên môi trường số (Điểm (d), Mục 5, Phần IV, Quyết định 749/QĐ/TTg) •Thúc đẩy hoạt động bảo hiểm rủi ro trong chuyển đổi số, an toàn, an ninh mạng (Điểm (đ) Mục 5, Phần IV, Quyết định 749/QĐ/TTg)	•Yêu cầu các tổ chức, doanh nghiệp cung cấp hạ tầng và nền tảng số có sứ mệnh bảo đảm thông tin đáng tin cậy, an toàn, lành mạnh, phát triển hệ thống nền tảng, hạ tầng, mạng lưới gắn với bảo đảm an toàn, an ninh mạng, có khả năng tự sàng lọc, phát hiện tấn công, bảo vệ ở mức cơ bản (Điểm (c), Mục 5, Phần IV, Quyết định 749/QĐ/TTg) •Xây dựng, triển khai hệ thống giám sát, cảnh báo sớm nguy cơ, bảo vệ lợi ích chính đáng của cả người tiêu dùng và doanh nghiệp (Điểm (e), Mục 5, Phần IV, Quyết định 749/QĐ/TTg)

Bảng 2. Nhiệm vụ, giải pháp bảo vệ dữ liệu theo Quyết định 749/QĐ-TTg phê duyệt "Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030"

Nguồn: Tác giả minh họa từ Quyết định 749/QĐ-TTg

Trong bối cảnh đó, việc nghiên cứu đề xuất các giải pháp lập quy, lập pháp nhằm xây dựng cơ chế bảo vệ dữ liệu cá nhân là nhu cầu bức thiết, nhằm bảo vệ quyền riêng tư của người dùng song song với quá trình chuyển đổi số. Để đạt mục tiêu đó, cần phải trả lời hai câu hỏi sau: (1) liệu có một nền tảng nguyên tắc xuyên suốt để phát triển khung pháp lý về bảo vệ dữ liệu cá nhân ở Việt Nam; và (2) làm thế nào để xây dựng khung pháp lý về bảo vệ dữ liệu cá nhân nhằm phát huy hiệu quả việc bảo vệ quyền riêng tư của chủ thể dữ liệu trong tương quan với hoạt động xử lý dữ liệu của chủ thể xử lý.

Để trả lời câu hỏi thứ nhất, nghiên cứu sẽ tổng hợp các hướng tiếp cận hiện có liên quan đến bảo vệ quyền riêng tư cá nhân thông qua công tác bảo vệ dữ liệu nhằm chỉ ra hướng tiếp cận hợp lý để bảo vệ quyền riêng tư trong thời đại số. Khung pháp lý của Việt Nam hiện nay liên quan đến vấn đề bảo vệ dữ liệu người dùng sẽ được hệ thống hóa thông qua các quy định trong văn bản quy phạm pháp luật ở các cấp và nhiều lĩnh vực khác nhau, qua đó, nghiên cứu chỉ ra nhu cầu điều chỉnh cụ thể về mặt pháp lý đối với bảo vệ dữ liệu cá nhân ở Việt Nam.

Phương pháp so sánh luật được áp dụng xuyên suốt nghiên cứu, ở cấp độ luật Việt Nam và cấp độ luật quốc tế giữa các khu vực với nhau nhằm đối sánh khung pháp luật về bảo vệ dữ liệu cá nhân ở Việt Nam và một số hệ thống pháp luật trên thế giới, từ đó, tổng hợp các nguyên tắc chung mang tính định hướng trong bảo vệ dữ liệu.

Kết quả so sánh cũng sẽ được sử dụng để làm cơ sở trả lời câu hỏi thứ hai, cụ thể, đề xuất hai nhóm nguyên tắc chủ đạo trong việc ban hành văn bản quy phạm pháp luật, đồng thời đề xuất sửa đổi, bổ sung các quy định pháp luật hiện hành để thống nhất tuân thủ các nguyên tắc bảo vệ dữ liệu, tiến tới hài hòa hóa hệ thống pháp luật Việt Nam với các quy định tiến bộ của thế giới, tạo ra môi trường dữ liệu tiên tiến, bền vững, cơ chế chia sẻ dữ liệu an toàn, đảm bảo chủ quyền và an ninh dữ liệu cho Việt Nam.

2. BẢO VỆ DỮ LIỆU CÁ NHÂN: NHU CẦU ĐIỀU CHỈNH VỀ MẶT PHÁP LÝ

2.1 Từ quyền riêng tư đến bảo vệ dữ liệu: lược khảo cơ sở lý luận về bảo vệ dữ liệu cá nhân

Mặc dù khái niệm về quyền riêng tư đã được thai nghén, phát triển xuyên suốt trong lịch sử tư tưởng nhân loại (Moore, 2010; Westin, 1970), nhu cầu bảo vệ quyền riêng tư bằng các phương tiện pháp lý chỉ xuất hiện chính thức trên phạm vi toàn cầu vào những năm giữa thế kỉ XX, thông qua việc ghi nhận quyền riêng tư như một quyền tự nhiên của con người trong hai văn bản và điều ước quốc tế, lần lượt là Tuyên ngôn quốc tế về nhân quyền (Universal Declaration of Human Rights – UDHR, 1948) và Công

ước quốc tế về các quyền dân sự và chính trị (International Convenant on Civil and Political Rights – ICCPR, 1966)[13].

Trong thời đại số, sự phát triển của các công nghệ thu thập thông tin người dùng sau cuộc bùng nổ công nghệ thông tin và mạng internet vào thập niên 70 của thể kỉ trước đã đòi hỏi một sự nhận thức lại về quyền riêng tư và bảo vệ quyền riêng tư. Westin (1970) cho rằng quyền riêng tư cần được thể hiện thông qua bốn nội hàm, lần lượt là quyền được ở một mình (the right to be let alone), quyền được xây dựng quan hệ riêng tư, quyền ẩn danh, quyền bảo lưu khoảng cách khỏi hoạt động xã hội. Công nghệ số có khả năng tái dựng nhân dạng của người thực dưới hình thức điện tử, tạo ra một "nhân bản" của cá nhân trong môi trường internet, vì thế, sự tác động của công nghệ thông tin lên "nhân bản" này sẽ trực tiếp tác động đến danh dự, uy tín, nhân phẩm của cá nhân ngoài đời thực (Solove, 2000, 2007). Vì lý do trên, các công cụ pháp lý chống định danh cá nhân, bao gồm những quy định chặt chẽ về quy trình, thủ tục cung cấp thông tin định danh cá nhân để đưa vào hệ thống cơ sở dữ liệu, hay việc xác định tính bất hợp pháp của hành vi thu thập thông tin cá nhân mà chủ thể thông tin không biết, chính là các biện pháp nhằm bảo vệ quyền riêng tư của cá nhân (Bygrave, 2014; Moore, 2010; Schwartz, 2005). Trước tình hình đó, năm 1988, Ủy ban Nhân quyền Liên Hợp Quốc đã đưa ra giải thích nhằm bổ sung nội hàm của quyền riêng tư, theo đó, việc thu thập và lưu giữ các thông tin cá nhân trong máy tính, các cơ sở dữ liệu và thiết bị khác, dẫu được tiến hành bởi chủ thể nào, đều phải tuân thủ quy định của pháp luật (Refworld | CCPR General Comment No. 16, 1988).

Tuy nhiên, Helen Nissenbaum lại có cái nhìn khác về quyền riêng tư trong kỷ nguyên số. Trong thời đại công nghệ thông tin và kết nối không gián đoạn, thông tin cá nhân được truyền đưa qua khắp các nền tảng bằng các dòng lệnh liên tục, xuyên suốt và nhanh chóng. Không chỉ có thế, rủi ro thông tin cá nhân bị tiết lộ trái phép sẽ không bao giờ biến mất, bởi hai lý do là: thứ nhất, các hệ thống lưu trữ dữ liệu luôn phải đối diện với nguy cơ

[13] *Điều 12 UDHR: "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 dnh 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."*
Điều 17 ICCPR: "Không ai bị can thiệp một cách tùy 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". (Nguyễn và c.s., 2015)

thông tin bị rò rỉ, đánh cắp bởi nguyên nhân khách quan hoặc chủ quan; thứ hai, thông tin luôn để lại dấu vết tại các cơ sở dữ liệu, "trạm trung chuyển", thiết bị phần cứng trong quá trình lưu trữ, sử dụng, xử lý và truyền đưa (Bygrave, 2014; Schwartz, 2005; Solove, 2000, 2007). Sử dụng ứng dụng công nghệ thông tin, người dùng đã mặc nhiên đồng ý trao quyền kiểm soát, lưu trữ, xử lý dữ liệu vào tay các chủ thể vô hình trong môi trường ảo mà không thể biết hết các hệ quả nhãn tiền (Kang, 1997; Kramer và c.s., 2009). Lý thuyết của Helen Nissenbaum đặt nền tảng trên kiến giải rằng, thông tin luôn chuyển dịch không ngừng trong không gian ảo qua các giao dịch truyền đưa, vì vậy, bà lập luận rằng, thay vì tập trung vào nhu cầu bảo vệ "bí mật" hay "sự riêng tư" của chủ thể dữ liệu, khái niệm "quyền riêng tư" trong thời đại số nên được hiểu là **quyền của chủ thể cá nhân được yêu cầu các chủ thể khác phải áp dụng các quy trình phù hợp, chính đáng khi truyền đưa thông tin cá nhân của họ (appropriate flow of information)** qua các nền tảng phần cứng và hệ thống phần mềm khác nhau (H. Nissenbaum, 2011; H. F. Nissenbaum, 2010).

Nếu hiểu theo cách trên, bảo vệ dữ liệu cá nhân không phải là trao quyền định đoạt hoàn toàn cho chủ thể đối với thông tin cá nhân của mình được đưa vào sử dụng trong môi trường số. Thực tế, cách tiếp cận của một số khuông khổ pháp lý trên thế giới hiện nay vẫn đang trao quá nhiều quyền định đoạt cho chủ thể có thông tin được sử dụng, không chỉ đặt gánh nặng bảo vệ sự toàn vẹn và chính xác của dữ liệu cá nhân lên doanh nghiệp công nghệ số, mà còn tạo ra trở ngại bất hợp lý cho giao dịch điện tử khi buộc người xử lý phải tạo dựng cơ chế cho phép người dùng biết, can thiệp, cải chính, đến mức có quyền yêu cầu xóa sạch dữ liệu cá nhân ra khỏi hệ thống cơ sở dữ liệu của doanh nghiệp công nghệ số (Sam Wrigley, Anette Alén-Savikko & Olli Pitkänen, 2019). Bảo vệ dữ liệu theo hướng tiếp cận của Nissenbaum là bảo vệ tính chính xác của thông tin cá nhân trong quá trình xử lý, trao quyền cho chủ thể dữ liệu được biết mục đích, phương thức, đối tượng xử lý và truyền đưa thông tin, đồng thời tạo lập nghĩa vụ của chủ thể xử lý phải bảo đảm quá trình truyền đưa hợp pháp, phù hợp với nguyên tắc pháp quyền và đạo đức xã hội. Vì lý do trên, thay vì quá tập trung vào việc trao quyền can thiệp của người dùng cá nhân vào cơ sở dữ liệu kinh doanh của doanh nghiệp, pháp luật chỉ nên tạo dựng bộ nguyên tắc xuyên suốt đối với công tác xử lý và truyền đưa dữ liệu, trong đó, chú trọng ban hành các

quy chuẩn kĩ thuật và quy tắc ứng xử của các chủ thể tiến hành xử lý dữ liệu. (Tuomas Pöysti, 2019).

2.2 Khung pháp lý về bảo vệ dữ liệu cá nhân ở Việt Nam hiện nay

Tại Việt Nam, quyền riêng tư là một quyền hiến định, được ghi nhận tại Điều 21 của Hiến pháp (2013). Theo Hiến pháp, quyền riêng tư của cá nhân được thể hiện thông qua quyền về đời sống riêng tư, bí mật cá nhân, bí mật gia đình, danh dự, uy tín của bản thân; quyền giữ bí mật về thư tín, điện thoại, điện tín và các hình thức trao đổi thông tin riêng tư. Các quyền kể trên được pháp luật bảo vệ[14].

Theo cách định nghĩa này, quyền riêng tư cá nhân được pháp luật bảo vệ ở Việt Nam bao gồm hai nhóm: quyền riêng tư đối với thông tin về đời sống riêng tư, bí mật gia đình và quyền riêng tư đối với thông tin liên lạc trong đời sống xã hội. Quan điểm này được thể hiện nhất quán qua quy định tại Điều 38 Bộ luật Dân sự 2015, theo đó, việc thu thập, lưu trữ, sử dụng, công khai thông tin liên quan đến đời sống riêng tư, bí mật cá nhân phải được sự đồng ý của chủ thể (nguyên tắc đồng ý); đồng thời, quá trình thu thập thông tin liên quan đến cá nhân phải đảm bảo an toàn, bảo mật. Rõ ràng, quyền riêng tư của cá nhân ở Việt Nam hiện nay đang được tiếp cận theo hướng truyền thống, đề cao nguyên tắc giữ bí mật đối với thông tin định danh và thông tin về đời sống riêng tư của chủ thể.

Tuy nhiên, quy định tại BLDS chỉ mang tính nguyên tắc cơ bản và định hướng cho các văn bản quy phạm pháp luật chuyên ngành. Đặc biệt, BLDS đã không đưa ra những giả định xa hơn về các tình huống xử lý dữ liệu trong môi trường thương mại điện tử và kinh tế số. Ở Việt Nam hiện nay, chưa có một đạo luật thống nhất về bảo vệ dữ liệu cá nhân, trong đó đề ra các nguyên tắc cụ thể hơn cho hoạt động thu thập, lưu trữ, sử dụng, công khai thông tin (sau đây gọi chung là xử lý), cũng như các chế định rõ ràng về hành vi xâm phạm quyền riêng tư đối với thông tin cá nhân. Hiện tại, các quy định về bảo vệ dữ liệu cá nhân được ghi nhận rải rác thông qua các đạo luật chuyên ngành, như được trình bày trong bảng dưới đây.

---

[14] *Theo Điều 21 Hiến pháp (2013):*
"1. 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.
2. Mọi người có quyền bí mật thư tín, điện thoại, điện tín và các hình thức trao đổi thông tin riêng tư khác.Không ai được bóc mở, kiểm soát, thu giữ trái luật thư tín, điện thoại, điện tín và các hình thức trao đổi thông tin riêng tư của người khác"

Văn bản quy phạm pháp luật / Các Biện pháp bảo vệ dữ liệu	Luật Công nghệ Thông tin	Luật Bảo vệ Quyền lợi người tiêu dùng	Luật An toàn Thông tin mạng	Luật Giao dịch điện tử	Nghị định 52/2013/ NĐ-CP về thương mại điện tử
Xử lý dữ liệu phải xin phép và được sự đồng ý của chủ thể dữ liệu	Điều 21, 22	Điều 6	Khoản 15, 16, 17, Điều 3	Điều 46	Điểm (a), khoản 4, Điều 4
Sử dụng dữ liệu đúng mục đích và phù hợp với nguyên tắc, chuẩn mực	Khoản 1, Điều 15	Điểm (b), khoản 2, Điều 6	Chỉ áp dụng đối với mục đích thương mại (khoản 5 Điều 16, khoản 17 Điều 3)	Không rõ ràng	Chỉ áp dụng đối với mục đích thương mại đối với hành vi lưu trữ trong cơ sở dữ liệu (khoản 14, Điều 3)
Đảm bảo an toàn, bảo mật đối với dữ liệu trong quá trình xử lý	Không rõ ràng	Khoản 1, Điều 6	Điều 4, khoản 1 Điều 19	Không rõ ràng	Khoản 1, Điều 72
Công khai mục đích, phương thức, quy trình xử lý dữ liệu cho chủ thể dữ liệu được biết	Không rõ ràng	Điểm (a), khoản 2, Điều 6	Khoản 3 Điều 16	Không rõ ràng	Khoản 3 Điều 69

Bảng 3. Tổng quát các quy định pháp luật về bảo vệ dữ liệu cá nhân trong hệ thống pháp luật Việt Nam hiện nay

Nguồn: Tác giả tổng hợp từ các văn bản quy phạm pháp luật mở

Các quy định trên được tổng hợp chủ yếu từ các nguồn văn bản quy phạm pháp luật điều chỉnh quan hệ thương mại điện tử, giao dịch điện tử,

phát triển hạ tầng công nghệ và bảo vệ quyền lợi của người tiêu dùng. Ngoài ra, như phản ánh qua bảng đối sánh, hiện nay chưa có một khung khổ pháp lý rõ ràng, xuyên suốt giữa các văn bản quy phạm pháp luật trong hệ thống pháp luật Việt Nam về bảo vệ dữ liệu cá nhân. Phần lớn các quy định về bảo vệ dữ liệu hiện nay chỉ được xây dựng tích hợp trong hệ thống các quy tắc xử sự của các lĩnh vực chuyên ngành cụ thể.

2.3 Những bất cập của cơ chế bảo vệ dữ liệu cá nhân ở Việt Nam trong bối cảnh hiện nay

Thứ nhất, hướng tiếp cận của Việt Nam đối với việc bảo vệ dữ liệu đã bộc lộ bất cập. Như đã phân tích, hướng tiếp cận "tĩnh" - bảo vệ bí mật thông tin định danh và bí mật dữ liệu liên lạc tại nguồn thu thập, là bất khả thi trong quá trình chuyển đổi số dưới sự ảnh hưởng của cuộc CMCN 4.0 (Nick Barrowman, 2018; Schwab & Davis, 2018; Tristan Henderson & Burkhard Schafer, 2019). Hiện nay, cách ghi nhận của Hiến pháp 2013, Bộ luật Dân sự 2015 và các đạo luật mang tính nền tảng dẫn lối cho toàn bộ hệ thống pháp luật Việt Nam cho thấy hệ thống pháp luật Việt Nam vẫn tiếp cận bảo vệ quyền riêng tư theo hướng này. Ngoài ra, sự mơ hồ trong hướng tiếp cận còn thể hiện qua việc thiếu vắng chế định ghi nhận quyền nhân thân của chủ thể đối với thông tin cá nhân trong tổng thể hệ thống các chế định về quyền nhân thân ghi nhận tại BLDS.

Thứ hai, chưa có một khuôn khổ nguyên tắc thống nhất về bảo vệ dữ liệu cá nhân. Khảo sát sơ bộ hệ thống pháp quy của Việt Nam hiện nay, có thể nhận thấy sự thiếu vắng các nguyên tắc dẫn đường trong công tác lập pháp liên quan đến quan hệ bảo vệ dữ liệu cá nhân. Bốn tiêu chí được đưa ra để thực hiện đối sánh trong Bảng 2 lần lượt là (1) Nguyên tắc đồng ý của chủ thể dữ liệu; (2) Nguyên tắc sử dụng đúng mục đích, phù hợp với nguyên tắc, chuẩn mực đạo đức của xã hội; (3) Nguyên tắc đảm bảo an toàn, bảo mật đối với quá trình xử lý dữ liệu của cá nhân; (4) Nguyên tắc công khai mục đích, phương thức xử lý dữ liệu cho chủ thể biết. Đây là bốn nguyên tắc cơ bản, đề cao và bảo vệ quyền riêng tư của cá nhân trong môi trường số hiện nay. Ngoài bốn nguyên tắc kể trên, còn nhiều nguyên tắc mang tính bổ trợ khác, tất cả những nguyên tắc này đều được xây dựng trên nền tảng bảo vệ quyền riêng tư của con người. Tuy nhiên, như thể hiện qua Bảng 2, ngay cả trong bốn nguyên tắc cơ bản trên, các văn bản quy phạm pháp luật (VBQPPL) hiện nay cũng chưa thể hiện được sự đồng bộ và nhất quán. Tính thiếu đồng bộ của các quy định pháp luật cũng được phản ánh

qua các quy định rải rác, trải đều các văn bản thuộc các lĩnh vực khác nhau trong hệ thống pháp luật Việt Nam.

Thứ ba, chưa có một định nghĩa rõ ràng, thống nhất về dữ liệu cá nhân. Hiện nay, các văn bản quy phạm pháp luật vẫn sử dụng cụm từ "thông tin cá nhân" để thể hiện các quy định về bảo vệ dữ liệu cá nhân. Thực tế, "thông tin cá nhân" và "dữ liệu cá nhân" là hai khái niệm hoàn toàn khác nhau (Ritter & Mayer, 2017). Nếu "thông tin cá nhân" là khái niệm dùng để chỉ các thông tin sơ cấp, gắn liền với thực tế, gắn liền với bối cảnh, thì "dữ liệu cá nhân" cũng là các thông tin trên, nhưng đã được thu thập qua quy trình thu thập, lưu trữ, xử lý, kết hợp, phân loại, truyền đưa, bằng các thuật toán liên quan của một nền tảng số. "Dữ liệu cá nhân" là một cấu phần không tách rời của "dữ liệu công nghiệp", mang giá trị (Janeček & Malgieri, 2019; Malgieri & Custers, 2017), góp phần trực tiếp vào công tác ra quyết định trong hoạt động kinh doanh, gắn liền với mô hình kinh doanh (Sam Wrigley, Anette Alén-Savikko & Olli Pitkänen, 2019). Phân biệt rõ ràng, hợp lý giữa các khái niệm sẽ giúp đưa ra một phương pháp phân loại dựa trên tính năng sử dụng của các loại dữ liệu khác nhau, tạo nên cơ chế điều chỉnh pháp lý đúng đắn hơn trong bối cảnh chuyển đổi số.

Thứ tư, chưa có cơ chế giải quyết xung đột giữa quyền riêng tư của cá nhân người dùng và quyền sở hữu của của doanh nghiệp trong hoạt động chuyển đổi số. Thực chất, cơ chế bảo vệ dữ liệu theo hướng tiếp cận hiện nay tất yếu sẽ tạo nên rào cản chuyển đổi số của doanh nghiệp công nghệ, bởi lẽ người dùng cá nhân đang được trao quá nhiều quyền can thiệp vào cơ sở dữ liệu và gián tiếp tạo ra khó khăn cho mô hình kinh doanh của doanh nghiệp số (Ritter & Mayer, 2017; Tuomas Pöysti, 2019). Trong bối cảnh đó, việc phân định rõ quyền tài sản và cơ chế sở hữu của doanh nghiệp công nghệ đối với cơ sở dữ liệu công nghiệp là cần thiết, nhằm xác định rõ quyền tài sản của doanh nghiệp đối với các dữ liệu không trực tiếp xâm phạm quyền của chủ thể dữ liệu.

3. TỔNG QUAN CÁC HỆ THỐNG PHÁP LUẬT VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN TRÊN THẾ GIỚI

Trước nhu cầu điều chỉnh về mặt pháp lý, cần thiết đưa ra cái nhìn khái quát về hiện trạng lập pháp liên quan đến bảo vệ dữ liệu cá nhân của các hệ thống pháp luật trên thế giới, tạo cơ sở đối sánh với khung khổ pháp luật Việt Nam hiện nay, từ đó đưa ra đề xuất, kiến nghị lập pháp cho Việt Nam. Trong phạm vi bài viết này, Bộ quy định chung về bảo vệ dữ liệu

(General Data Protection Regulations – GDPR) của châu Âu, cùng hệ thống pháp luật Trung Quốc về vấn đề bảo vệ dữ liệu cá nhân sẽ được lựa chọn lược khảo và đối sánh. Các bộ quy tắc về bảo vệ dữ liệu khác sẽ được nhắc đến với vai trò là nguồn tham chiếu.

3.1 Bộ quy định chung về bảo vệ dữ liệu của Liên minh châu Âu (GDPR): chuẩn mực pháp lý về bảo vệ dữ liệu

Bộ Quy định chung về Bảo vệ Dữ liệu của Liên minh châu Âu (GDPR) là điều ước quốc tế giữa các thành viên trong khu vực châu Âu. Kế thừa những nguyên tắc chung về bảo vệ dữ liệu cá nhân được xác lập trong Công ước 108[15] và Chỉ thị 95/46/EC ban hành năm 1995, bộ GDPR là hệ thống quy định pháp luật mang tính ràng buộc pháp lý cao nhất trong công tác bảo vệ dữ liệu cá nhân ở châu Âu. Vươn xa hơn, các nguyên tắc và chuẩn mực về bảo vệ dữ liệu cá nhân tại châu Âu, được cụ thể hóa qua bộ quy định trong GDPR đã trở thành mẫu mực lập pháp cho các quy định về bảo vệ dữ liệu cá nhân khắp toàn cầu, trong đó có khu vực ASEAN (*The EU GDPR's Impact on ASEAN Data Protection Law*, 2019).

Bên cạnh các quy định thống nhất về khái niệm dữ liệu cá nhân (personal data), chủ thể dữ liệu (data subject), chủ thể nắm quyền kiểm soát dữ liệu (data controller), chủ thể xử lý dữ liệu (processor), hoạt động xử lý dữ liệu (processing), và "sự đồng ý" (consent), GDPR đã đưa ra nhiều quy định cụ thể về quyền nhân thân của chủ thể dữ liệu đối với thông tin cá nhân của mình, trong tương quan với các nghĩa vụ, trách nhiệm của chủ thể có quyền chiếm hữu và thực hiện xử lý đối với dữ liệu cá nhân.

Quyền của chủ thể dữ liệu	**Nghĩa vụ, trách nhiệm của chủ thể kiểm soát, chủ thể xử lý**
(a) *Nhóm quyền được biết*: bao gồm quyền được thông tin rõ ràng, chính xác liên quan đến hoạt động xử lý dữ liệu cá nhân của mình (Điều 12); quyền được biết mục đích, cách thức, lợi ích, chủ thể liên quan đến hoạt động xử lý dữ	Xây dựng và tích hợp các nguyên tắc về bảo vệ quyền riêng tư trong sản phẩm ứng dụng công nghệ của mình một cách mặc định, ngay từ lúc phác thảo kế hoạch xây dựng và phải thông tin rõ ràng, đầy đủ đến chủ thể dữ liệu (Điều 24, 25); Không chia sẻ dữ liệu và

[15] *Đây là điều ước quốc tế đầu tiên bao gồm các quy định pháp luật mang tính ràng buộc chung về xử lý dữ liệu cá nhân tự động, được ban hành vào năm 1981 và được sửa đổi, bổ sung dần qua các nghị định thư và vẫn có hiệu lực cho đến nay.*
Xem toàn văn Công ước 108 và các Nghị định thư tại: https://www.coe.int/en/web/data-protection/convention108-and-protocol

liệu cá nhân của mình (Điều 13); quyền được thông tin đầy đủ về chủ thể kiểm soát, xử lý dữ liệu trước khi cung cấp thông tin cá nhân (Điều 14);	tiến hành xử lý chung với các chủ thể khác trừ trường hợp được sự cho phép của chủ thể dữ liệu (Điều 28); Các thông tin về việc xử lý phải được thể hiện trong hợp đồng trao quyền hoặc trong các quy định pháp luật của quốc gia thành viên EU (Điều 28); Tiến hành kiểm định, đánh giá tác động đối với hoạt động xử lý dữ liệu (Điều 35, 42);
(b) *Nhóm quyền được tiếp cận, can thiệp:* bao gồm quyền được tiếp cận dữ liệu cá nhân của mình trong cơ sở dữ liệu của chủ thể nắm giữ, cũng như yêu cầu cải chính, xóa bỏ, phản đối, đưa ra hạn chế cụ thể đối với chủ thể kiểm soát, xử lý dữ liệu cá nhân của mình, và được nhận lại toàn vẹn, chính xác các dữ liệu của mình theo hệ thống phân loại, sắp xếp của cơ sở dữ liệu (Điều 15-16, 18-21);	Ghi nhận, sao lưu các hoạt động xử lý dữ liệu và thực hiện công khai, minh bạch hóa các phương thức giúp chủ thể dữ liệu thực hiện quyền tiếp cận, can thiệp (Điều 30-31);
(c) *Nhóm quyền về giữ bí mật và đời sống riêng tư*, bao gồm quyền lãng quên (quyền được xóa hoàn toàn khỏi hệ thống xử lý dữ liệu) (Điều 17); quyền được nằm ngoài đối tượng nhắm đến từ kết quả các quyết định đưa ra bởi thuật toán tự động, trong đó bao gồm việc tái định danh cá nhân (profiling) (Điều 22).	Bảo đảm an toàn, bảo mật, minh bạch đối với hệ thống và chu trình xử lý dữ liệu cá nhân, đảm bảo rằng dữ liệu được khử định danh (pseudonymisation), đảm bảo hệ thống có đủ khả năng phục hồi và tái tiếp cận trong trường hợp ngoài ý muốn, thường xuyên tiến hành kiểm định, đánh giá; tiến hành các bước cần thiết nhằm đảm bảo quyền của chủ thể dữ liệu (Điều 32)

Bảng 4. Đối sánh tương quan quyền và nghĩa vụ trong quan hệ xử lý dữ liệu theo GDPR.

Nguồn: Tác giả minh họa dựa trên tổng hợp các quy định của GDPR

Các quyền và nghĩa vụ đối ứng trên được xây dựng dựa trên bộ nguyên tắc khung về bảo vệ dữ liệu cá nhân, đã được quy định rõ từ Điều 5 đến Điều 11 của GDPR và đã được giải thích rõ tại Lời nói đầu (Recital) đoạn thứ 39 cùng văn bản. Cụ thể hơn, khi xây dựng khuôn khổ pháp lý cho việc bảo vệ dữ liệu cá nhân, các nước thành viên châu Âu cần tuân thủ các nguyên tắc nền tảng sau:

Một là, xử lý dữ liệu phải được thực hiện trên cơ sở hợp pháp, tuân thủ quy định của pháp luật về điều kiện, hình thức, thủ tục thu thập sự đồng ý của chủ thể dữ liệu và các mục đích khác được nêu rõ trong luật (Điều 5(1)(a) GDPR) (nguyên tắc hợp pháp);

Hai là, quy trình, cách thức, mục đích thu thập, lưu trữ, xử lý, truyền đưa và các hoạt động, lợi ích cũng như rủi ro có liên quan đến dữ liệu phải công khai, minh bạch theo hướng dễ tiếp cận, dễ hiểu, được diễn đạt bằng ngôn ngữ thông thường và bằng các phương thức thông thường để cá nhân biết đầy đủ *trước khi* cung cấp và trao quyền xử lý thông tin cá nhân của mình (Phụ lục 39) (nguyên tắc chủ thể thông tin biết);

Ba là, chủ thể xử lý dữ liệu chỉ được thu thập, xử lý dữ liệu nếu không thể đạt được mục đích bằng bất kì hành vi nào khác ngoài việc sử dụng thông tin cá nhân; nói cách khác, việc xử lý dữ liệu của cá nhân chỉ được để ở ưu tiên cuối cùng. Trong trường hợp buộc phải xử lý dữ liệu, chủ thể phải thu thập và xử lý thông tin cá nhân với số lượng tối thiểu, vừa đủ để đạt được mục đích của việc xử lý, trong khoảng thời gian ngắn nhất một cách hợp lý (nguyên tắc tối thiểu hóa dữ liệu);

Bốn là, quy trình xử lý dữ liệu phải đảm bảo dữ liệu được an toàn, bảo mật. Chủ thể xử lý dữ liệu cần tiến hành các quy trình, xây dựng các mô hình kĩ thuật cần thiết để ngăn chặn việc truy cập trái phép và sử dụng trái phép đến dữ liệu cá nhân và các thiết bị sử dụng để tiến hành xử lý dữ liệu (nguyên tắc an toàn, bảo mật).

Bốn nguyên tắc trên không chỉ đóng vai trò là kim chỉ nam cho hoạt động lập pháp tại các quốc gia trên thế giới, mà chúng còn được vận dụng để các doanh nghiệp chủ động xây dựng các bộ tiêu chí quản trị nội bộ đối với công tác xử lý dữ liệu (Ben Ayed, 2014; Truong và c.s., 2020), đảm bảo tính tuân thủ và tạo ra môi trường kinh doanh lành mạnh, đề cao giá trị quyền con người trong bối cảnh CMCN 4.0. Đối chiếu với các nguyên tắc về Bảo vệ quyền riêng tư được OECD tổng hợp và ban hành vào năm 2008

và 2013[16], các nguyên tắc trên đã được thể hiện đầy đủ, tinh gọn và hợp lý. Sâu xa hơn, bốn nguyên tắc trên là sự hiện thực hóa hai nguyên lý quan trọng trong nhận thức về quyền nhân thân của chủ thể, đó là *bảo vệ toàn vẹn phẩm cách con người*, và *quyền tự định đoạt đối với thông tin cá nhân của chính bản thân chủ thể* (Tuomas Pöysti, 2019).

Tuy nhiên, bên cạnh các thành tựu về mặt lập pháp, đã có nhiều nghiên cứu đưa ra phê phán đối với hệ thống quy định của GDPR. Phần lớn các nghiên cứu này cho rằng, các quy định của GDPR là bất khả thi trong bối cảnh công nghệ IoT, trí tuệ nhân tạo dần được ứng dụng rộng rãi để xử lý dữ liệu lớn (Craig & Ludloff, 2011; Higham, 2016; Hoeren, 2014). Tính chất bất khả thi được biện minh bởi thực tiễn áp dụng các quy định, thể hiện qua hai phương diện, *thứ nhất*, việc trao quyền cho chủ thể dữ liệu, đặc biệt là quyền can thiệp vào cách thức vận hành và quản trị hệ thống của chủ thể kinh doanh, thể hiện cụ thể qua quyền được yêu cầu trích xuất đầy đủ cách thể hiện dữ liệu cá nhân của mình trong hệ thống và quyền xóa bỏ toàn bộ dữ liệu liên quan đến cá nhân, sẽ gây ra thách thức đáng kể về mặt chi phí, khả năng công nghệ và mô hình quản trị của chủ thể xử lý (Ballardini và c.s., 2019; Malgieri, 2016; XING Hui-Qiang, 2019); *thứ hai*, trong bối cảnh hiện nay, khi sử dụng dữ liệu thứ cấp (secondary use of data), người sử dụng hoàn toàn không cần phải xử lý thông tin cá nhân trực tiếp, bởi các dữ liệu này đã được xử lý, khử đi các thông tin định danh cá nhân bằng thuận toán tự động và mạng lưới siêu liên kết, và có khả năng đem lại giá trị kinh tế cao cho chủ thể nắm quyền xử lý chúng; vì thế, trao quyền cho chủ thể dữ liệu là vô nghĩa, bởi chủ thể dữ liệu không thể hình dung được toàn diện các giá trị sử dụng phái sinh từ thông tin của mình, cũng như không thể làm gì hơn khi các dữ liệu thứ cấp phái sinh được sử dụng vào mục đích xấu (Sam Wrigley, Anette Alén-Savikko & Olli Pitkänen, 2019; Tristan Henderson & Burkhard Schafer, 2019; Wachter & Mittelstadt, 2019).

3.2 Quyền nhân thân đối với dữ liệu cá nhân: cải cách luật tư ở Trung Quốc và những tồn tại

Ngày 28/5/2020, Đại hội nhân dân toàn quốc Trung Quốc (gọi tắt là Nhân Đại, đây là cơ quan lập pháp, đại diện cho quyền lực của nhân dân

---

[16] 8 (tám) nguyên tắc về bảo vệ quyền riêng tư đối với thông tin cá nhân của OECD là: (1) Hạn chế thu thập dữ liệu; (2) Đảm bảo về chất (mục đích sử dụng) của dữ liệu; (3) Nêu rõ mục đích; (4) Hạn chế sử dụng; (5) Các biện pháp đảm bảo an toàn; (6) Minh bạch; (7) Sự tham gia của chủ thể dữ liệu; (8) chủ thể xử lý chịu trách nhiệm. Xem thêm tại: https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Trung Quốc) đã thông qua bộ Dân Pháp Điển (DPĐ) gồm 1260 điều thể hiện các quy phạm pháp luật điều chỉnh quan hệ nhân quyền, vật quyền và trái quyền ở Trung Quốc (TQ). Tại lần sửa đổi luật tư này, Dân Pháp Điển đã dành hẳn Thiên thứ bảy để quy định về quyền nhân thân, trong đó bao gồm các quy định bảo vệ quyền sống, sức khoẻ, quyền về họ tên, hình ảnh, danh dự, nhân phẩm của cá nhân trong xã hội. Đặc biệt, lần đầu tiên trong lịch sử, pháp luật dân sự Trung Quốc đã ghi nhận quyền riêng tư và quyền được bảo vệ đối với dữ liệu cá nhân tại Điều 1034, 1035 của DPĐ. Đây là một bước tiến đáng kể trong bối cảnh nền kinh tế TQ chuyển đổi số toàn diện, khi DPĐ đã tích hợp gần như đầy đủ các nguyên tắc bảo vệ dữ liệu và quyền riêng tư của OECD và GDPR vào hệ thống dân luật. Với việc xây dựng thêm dự thảo Luật bảo vệ thông tin cá nhân, TQ là một trong những nước châu Á đi đầu trong bảo vệ dữ liệu hiện nay.

Tại Điều 1032, DPĐ Trung Quốc đã quy định cá nhân được bảo vệ quyền riêng tư. Cụ thể hơn, nội hàm của quyền riêng tư đã được định nghĩa như sau: "[Quyền riêng tư là quyền được bảo vệ] …sự bình yên về mặt cuộc sống riêng tư của con người, cùng các không gian riêng mật, hoạt động riêng mật, thông tin riêng mật mà người đó không mong muốn người khác biết được". Từ "riêng mật" (私密) được dịch là "Tư mật" trong ngôn từ Hán Việt, là cụm từ bao hàm cả hai ý nghĩa là "riêng mình" và "bí mật". Đối chiếu với cách hiểu của Westin (1970) và Solove (2005) về quyền riêng tư, việc ghi nhận cá nhân có quyền riêng mật đối với thông tin ở Trung Quốc là cách nhìn nhận phù hợp, đồng bộ với cách hiểu về quyền riêng tư ghi nhận trong các văn bản quốc tế và thể hiện qua các nguyên tắc bảo vệ dữ liệu của GDPR.

Về bảo vệ dữ liệu, Điều 111 DPĐ quy định: "Thông tin cá nhân của mọi người được pháp luật bảo vệ. Bất kỳ tổ chức, cá nhân nào có nhu cầu thu thập thông tin cá nhân của người khác phải thực hiện thu thập và đảm bảo an toàn thông tin theo quy định của pháp luật, không thu thập, sử dụng, xử lý, truyền tải thông tin cá nhân của người khác một cách bất hợp pháp và không được mua bán trái phép, cung cấp hoặc tiết lộ thông tin cá nhân của người khác." Hiện thực hóa quy định mang tính nguyên tắc trên, hiện tại, Dự thảo Luật Bảo vệ Dữ liệu cá nhân Trung Quốc (Dự thảo)[17] đã quy định tại Điều 5 như sau: "Việc xử lý thông tin cá nhân phải được tiến hành bằng

[17] *Tham khảo Dự thảo bản gốc (Tiếng Trung Quốc) tại đây: https://www.dataguidance.com/sites/default/files/china_draft_personal_data_law.pdf*

phương thức hợp pháp, chính đáng, tuân thủ nguyên tắc uy tín, không được xử lý thông tin cá nhân bằng các phương thức gian dối, gây hiểu lầm". Dự thảo cũng quy định rõ nguyên tắc công khai, minh bạch, tối thiểu hóa và đúng mục đích (Điều 5-8, Điều 18). Đặc biệt, nguyên tắc chủ thể xử lý dữ liệu phải chịu trách nhiệm được ghi nhận rõ tại Điều 9 của cùng Dự thảo. Trên cơ sở các nguyên tắc trên, Dự thảo đã trao cho chủ thể thông tin cá nhân quyền được trưng cầu ý kiến trước khi cung cấp thông tin (Điều 14), quyền rút lại sự đồng ý đối với việc xử lý dữ liệu mà vẫn được sử dụng dịch vụ của chủ thể xử lý dữ liệu (Điều 16), thậm chí, cá nhân còn có quyền yêu cầu được thông tin rõ ràng và từ chối kết quả của các quyết định mang tính tự động trong hệ thống kĩ thuật có sử dụng thông tin cá nhân của mình (Điều 25).

Như vậy, hiện tại, bảo vệ dữ liệu cá nhân đã được ghi nhận trong Bộ luật Dân sự của Trung Quốc, theo đó, thông tin cá nhân của thể nhân thuộc đối tượng bảo vệ của pháp luật. Ngoài ra, quy định nói trên đã thể hiện được các nguyên tắc tương tự như bộ nguyên tắc khung của OECD và GDPR, đó là: (1) nguyên tắc hợp pháp; (2) nguyên tắc chủ thể thông tin biết (Điều 13, 14, 18 Dự thảo); (3) nguyên tắc tối thiểu hóa dữ liệu; (4) nguyên tắc an toàn.

Xét về tổng thể, các nguyên tắc được thể hiện trong Dự thảo là tương đồng với bộ nguyên tắc đưa ra trong OECD và GDPR, tuy nhiên, cần phải chú ý đến cách thể hiện nguyên tắc thứ tư trong Dự thảo. Mặc dù "Bảo mật" (security) luôn là một tiêu chí được đề cao ngay từ cơ sở lý luận về bảo vệ quyền riêng tư trong thời đại số, nhưng nguyên tắc "bảo mật" lại không được đề cao và thể hiện rõ trong Dự thảo này của Trung Quốc. Cụ thể hơn, câu lệnh tìm kiếm từ khóa cho từ "保密" (bảo mật, security) trong Dự thảo chỉ trả ra hai kết quả, ứng với từ khóa xuất hiện tại Điều 19 và Điều 35. Trớ trêu thay, Điều 19 và Điều 35 lại quy định trường hợp cho phép các chủ thể xử lý dữ liệu tiến hành xử lý trong bí mật, hay "bảo mật" quy trình xử lý dữ liệu. Nói cách khác, việc xử lý dữ liệu trong một số trường hợp mà theo quy định pháp luật là có thể hoặc cần phải giữ bí mật, thì chủ thể xử lý dữ liệu được quyền tiến hành mà không cần công khai, minh bạch, trưng cầu sự đồng ý của chủ thể có thông tin bị xử lý. Nếu chủ thể có thông tin không thể biết được thông tin của mình đang bị thu thập, xử lý, làm sao có cơ sở để khẳng định việc xử lý dữ liệu đã tuân thủ các nguyên tắc còn lại, chẳng hạn như nguyên tắc tối thiểu, nguyên tắc hợp pháp? Ngoại lệ này vô tình đã đi ngược lại với các nguyên tắc chung trong

việc bảo vệ quyền riêng tư của chủ thể dữ liệu, để mở khả năng bị lợi dụng để thực hiện các hành vi xử lý dữ liệu ngoài luồng pháp luật.

3.3 Nhận xét

Từ kết quả đối sánh, có thể thấy, xuất phát điểm của khung pháp lý về bảo vệ dữ liệu cá nhân ở châu Âu và Trung Quốc đều nhằm bảo vệ quyền riêng tư của cá nhân, trên cơ sở đề cao việc bảo vệ thông tin cá nhân trước sự thay đổi về mô hình ứng dụng của công nghệ thông tin trong CMCN 4.0. Từ cách tiếp cận bảo vệ dữ liệu cá nhân là bảo vệ quyền riêng tư, các quốc gia đã chung tay xây dựng nhiều bộ nguyên tắc liên quan đến hoạt động xử lý dữ liệu, trong đó, đề cao bốn nhóm nguyên tắc chính là nguyên tắc hợp pháp, nguyên tắc chủ thể biết, nguyên tắc tối thiểu và nguyên tắc an toàn, bảo mật. Trên cơ sở các nguyên tắc này, cả pháp luật châu Âu lẫn Trung Quốc đều quy định chủ thể xử lý có nghĩa vụ và trách nhiệm đối với hoạt động xử lý dữ liệu cá nhân, đồng thời trao cho chủ thể thông tin có quyền can thiệp vào quy trình, cách thức xử lý dữ liệu của chủ thể xử lý, đôi khi đi xa hơn đến mức cho phép chủ thể yêu cầu xóa toàn bộ dữ liệu chứa thông tin cá nhân của mình trong cơ sở dữ liệu, hay từ chối kết quả của quá trình tự động hóa trong hệ thống mà có sử dụng thông tin cá nhân của mình. Việc trao quyền quá nhiều vào tay chủ thể như hiện nay đã tạo ra hiện tượng "lạm phát ý chí chủ thể" (Consent-inflated), khiến chủ thể trở nên "lờn" với các thủ tục hỏi xin ý kiến đến mức không đạt được hiệu quả và ý nghĩa của thủ tục thu thập sự đồng ý nữa (H. Nissenbaum, 2011; Tuomas Pöysti, 2019). Nói một cách khác, hiệu lực của nguyên tắc ý chí chủ thể sẽ trở nên yếu đi, một mặt khác, sự bắt buộc có được ý chí chủ thể thông qua các giao dịch mang tính thủ tục đề ra trong luật sẽ tạo ra trở ngại không đáng có, ảnh hưởng đến quyền tự do kinh doanh và phát triển theo mô hình tăng trưởng mới trong cuộc CMCN 4.0 (Tuomas Pöysti, 2019). Đó là chưa kể trường hợp, cá nhân có thông tin được thu thập, xử lý khó có thể hiểu một cách toàn diện và đầy đủ khả năng ứng dụng của dữ liệu thông tin cá nhân vào hoạt động kinh doanh, nhất là đối với các dữ liệu phái sinh tổng hợp được nhờ các thuật toán hiện đại (Wachter & Mittelstadt, 2019).

Trong bối cảnh CMCN 4.0, quyền tài sản và cơ chế sở hữu đối với đối tượng là dữ liệu (nói chung) đóng vai trò quan trọng (Ballardini và c.s., 2019; Hoeren, 2014). Các nước châu Âu đã cùng hướng về khuôn khổ pháp lý nhằm tạo ra "dòng chảy xuyên suốt, không trở ngại" của các dữ liệu phi-cá nhân (European Commission, 2017). Tuy nhiên, đối với thông tin cá

nhân, việc ghi nhận quyền chủ thể đối với thông tin như một quyền nhân thân sẽ dẫn đến hệ quả là không thể đặt vấn đề quyền tài sản đối với dữ liệu cá nhân, bởi quyền nhân thân không thể trị giá được bằng tiền và không thể có cơ chế sở hữu đối với quyền nhân thân. Trong bối cảnh CMCN 4.0, với các công nghệ AI và dữ liệu lớn, khó có thể phân biệt được đâu là dữ liệu phi-cá nhân (non-personal data) và dữ liệu cá nhân (personal data) bởi dữ liệu là một khối thống nhất, được tái tạo và tái sử dụng liên tục trong hệ thống cơ sở dữ liệu với tốc độ nhanh chóng (Petteri Günther, 2019). Tuy nhiên, cách định nghĩa và giải thích khái niệm dữ liệu cá nhân theo cách tiếp cận của châu Âu, mà các nước còn lại trên thế giới đang lấy làm hình mẫu cho việc xây dựng khung pháp lý về bảo vệ dữ liệu cá nhân, là quá rộng. Áp dụng các quy định về bảo vệ dữ liệu dựa trên cách định nghĩa như hiện thời sẽ gây ra trở ngại lớn đến sự phát triển công nghệ mới nổi như IoT hoặc các thuật toán phân tích (Justickis, 2020; Sam Wrigley, Anette Alén-Savikko & Olli Pitkänen, 2019) Sự lạm phát ý chí chủ thể chỉ có thể gia tăng thêm gánh nặng vốn dĩ đã trầm trọng lên nhu cầu sản xuất kinh doanh của doanh nghiệp công nghệ, vốn là động lực chính trong quá trình chuyển đổi số.

4. ĐỀ XUẤT LẬP PHÁP ĐỐI VỚI NHU CẦU BẢO VỆ DỮ LIỆU CÁ NHÂN Ở VIỆT NAM

4.1 Đề xuất hai nhóm nguyên tắc định hướng cho pháp luật bảo vệ dữ liệu cá nhân

Thực hiện nhiệm vụ đề ra tại Nghị quyết 01/2021/NQ-CP, theo đó đổi mới tư duy toàn diện, hệ thống nhằm tạo động lực đổi mới sáng tạo, phát triển kinh tế số, cần hệ thống hóa và đề xuất các nguyên tắc chủ đạo cho tiến trình lập pháp liên quan đến hoạt động xử lý dữ liệu trong thời gian tới. Chúng tôi đề xuất hai nguyên tắc chính, mang tính định hướng cho công tác lập pháp như sau.

Thứ nhất, nguyên tắc đảm bảo pháp quyền xã hội chủ nghĩa, đồng bộ hóa hệ thống pháp luật nhằm kiến tạo môi trường thể chế linh hoạt, tạo động lực tăng trưởng trong cuộc CMCN 4.0.

Cụ thể, đối với Quốc hội và Chính phủ, thực hiện công tác lập pháp, quy định liên quan đến bảo vệ dữ liệu cá nhân phải xuất phát trên cơ sở tôn trọng pháp quyền, nhằm thực hiện đường lối, mục tiêu phát triển kinh tế, xã

hội được đề ra trong các văn kiện, quyết định mang tính chiến lược, thể hiện vai trò kiến tạo của thể chế trong công cuộc chuyển đổi số đáp ứng yêu cầu của CMCN 4.0. Trong quá trình xây dựng quy định liên quan đến bảo vệ dữ liệu cá nhân, Ủy ban pháp luật của Quốc hội, cùng với Bộ Tư pháp phải dựa trên cơ sở lý luận rõ ràng về quyền riêng tư trong bối cảnh CMCN 4.0, kết hợp đánh giá khả năng thực hiện và áp dụng trên thực tiễn gắn liền với trình độ khoa học, công nghệ quốc gia.

Thứ hai, đảm bảo chủ quyền quốc gia, cân bằng lợi ích giữa các chủ thể trên cơ sở đề cao tự do ý chí của các bên trong quan hệ pháp luật. Trên cơ sở nhận thức đúng đắn về nội hàm và phương pháp điều chỉnh của quan hệ tài sản và quan hệ nhân thân, pháp luật về bảo vệ dữ liệu cần thừa nhận quyền nhân thân của chủ thể dữ liệu một cách rõ ràng.

Về mặt lý luận, cần xác định chắn chắn rằng quan hệ pháp luật của cá nhân với các chủ thể khác liên quan đến thông tin cá nhân của mình là quan hệ nhân thân phi tài sản; bên cạnh đó, cần vạch định rõ cấu phần của các quan hệ pháp luật trong hoạt động xử lý dữ liệu cá nhân, bao gồm quan hệ tài sản và quan hệ nhân thân phi tài sản. Cụ thể hơn, cơ quan lập pháp phải xây dựng cơ chế thực thi quyền tài sản phù hợp của các chủ thể kinh doanh trong bối cảnh CMCN 4.0 liên quan đến dữ liệu thứ cấp, dữ liệu phái sinh và việc sử dụng chúng vào mục đích kinh doanh, sao cho lợi ích giữa hai bên chủ thể được cân bằng, đảm bảo quyền con người song song với việc mưu cầu các lợi ích kinh tế.

Để đạt được sự cân bằng đó, bên cạnh việc trao quyền tài phán cho các cơ quan công quyền trong các trường hợp cụ thể, theo yêu cầu dân sự xác định (Justickis, 2020), cần khuyến khích đẩy mạnh cơ chế bình đẳng thỏa thuận trên cơ sở ý chí tự do của các chủ thể trong quan hệ xử lý dữ liệu, từ việc thỏa thuận tại các bước sơ cấp như minh bạch thông tin, thủ tục thu thập, trao quyền, cho đến các quan hệ tranh chấp khởi phát trong quá trình thực hiện xử lý. Cần đổi mới tư duy lập pháp theo hướng trao quyền tự chủ, tự quyết cho các doanh nghiệp, cơ quan, tổ chức thực hiện xử lý dữ liệu cá nhân; khuyến khích doanh nghiệp, tổ chức đổi mới sáng tạo chủ động xây dựng quy chuẩn, đẩy mạnh công tác kiểm định, đánh giá tín nhiệm. Từ đó, vai trò của các phương pháp điều chỉnh đặc trưng của luật công và luật tư được phối hợp nhuần nhuyễn, đề cao chủ quyền quốc gia

trong công tác lập pháp, tạo dựng cơ sở hài hòa hóa pháp luật với hệ thống luật pháp quốc tế trong thời kì hội nhập.

4.2 Một số đề xuất cụ thể về mặt chính sách, pháp luật đáp ứng nhu cầu bảo vệ dữ liệu cá nhân trong chuyển đổi số ở Việt Nam

Hiện thực hóa hai nguyên tắc trên, chúng tôi đề xuất một số giải pháp lập pháp và ban hành, thực hiện chính sách trong thời gian tới như sau.

Đối với công tác lập pháp của Quốc hội:

Một là, cần thừa nhận quyền nhân thân của cá nhân đối với thông tin cá nhân thông qua quy định rõ ràng, chính xác, một nghĩa trong Bộ luật Dân sự Việt Nam. Hiện nay, quyền nhân thân của chủ thể đối với dữ liệu cá nhân chưa được quy định trong luật, nói cách khác, chưa có cơ sở pháp lý vững chắc để bảo vệ và xử lý đối với các hành vi vi phạm quyền nhân thân của chủ thể dữ liệu. Trong lần sửa đổi, bổ sung BLDS sắp tới, Quốc hội phải bổ sung thêm điều khoản về bảo vệ thông tin cá nhân và bảo vệ quyền nhân thân của chủ thể đối với thông tin cá nhân của mình.

Hai là, cần ban hành đạo luật riêng về bảo vệ dữ liệu cá nhân, trong đó, xây dựng tiêu chí phân loại dữ liệu cá nhân rõ ràng, chính xác để có phương pháp điều chỉnh phù hợp với từng loại dữ liệu. Hiện nay, chưa có sự phân loại giữa dữ liệu cá nhân và các dữ liệu phi-cá nhân (hay dữ liệu công nghiệp) trong luật. Hơn nữa, pháp luật hiện nay chưa có cái nhìn phù hợp đối với khái niệm "thông tin cá nhân" và "dữ liệu cá nhân", vốn là hai khái niệm với nội hàm khác nhau (Ballardini và c.s., 2019).

Đối với dữ liệu cá nhân, cần xây dựng cơ chế bảo vệ phù hợp nhằm cân bằng lợi ích giữa cá nhân người dùng và chủ thể xử lý dữ liệu phục vụ mục đích đổi mới sáng tạo. Đối với dữ liệu công nghiệp hay phi-cá nhân, cần thừa nhận quyền tài sản hợp lý của người chiếm hữu, sử dụng chúng, kiến tạo hành lang pháp lý nhằm tạo ra dòng chảy dữ liệu tự do giữa các thiết bị và cơ sở dữ liệu, là tiền đề để thúc đẩy chuyển đổi số và đổi mới mô hình tăng trưởng. Cụ thể, pháp luật cần thể hiện được nội dung phân loại như sau:

"Dữ liệu cá nhân là dữ liệu được ghi nhận trong cơ sở dữ liệu máy tính, được tổng hợp và xử lý từ các thông tin cá nhân đầu vào, do chính cá nhân mà thông tin ấy thể hiện cung cấp. Dữ liệu phi cá nhân là các dữ liệu khác đã được khử định danh, không thể hiện thông tin cá nhân và không thể được tái dựng, truy ngược về nhân thân cá nhân bằng bất kì hình thức nào,

có giá trị kinh tế, được sử dụng nhằm mục đích hợp pháp. Việc xử lý và truyền đưa dữ liệu phải tuân thủ quy định của pháp luật".

Ba là, xây dựng hệ thống quyền và nghĩa vụ đúng, gọn, rõ, đề cao phương pháp bình đẳng thỏa thuận trong các quan hệ xử lý dữ liệu. Theo đó, thay vì quy định theo hướng tiếp cận liệt kê, cố gắng đưa ra các giả định mang tính dự báo trong quy phạm, Luật bảo vệ dữ liệu cá nhân trong tương lai cần tập trung đưa ra các nguyên tắc tiền đề, mang tính định hướng cho việc phân định quyền và nghĩa vụ của các bên chủ thể. Mặc dù các nguyên tắc này không nhất thiết phải tương đồng hết thảy với các bộ nguyên tắc trong GDPR hay của Trung Quốc, hai nguyên tắc nền tảng liên quan đến quyền nhân thân cần được chú trọng ở vị trí cốt lõi trong việc xây dựng bộ nguyên tắc, đó là: *bảo vệ toàn vẹn phẩm cách con người*, và *quyền tự định đoạt đối với thông tin cá nhân thuộc chính người đó*.

Cụ thể hơn, các chủ thể dữ liệu cần được pháp luật ghi nhận các quyền sau đây:

(1) Quyền được thông tin rõ ràng, chính xác liên quan đến hoạt động xử lý dữ liệu cá nhân của mình. Cụ thể, trước khi tiến hành trao quyền xử lý thông tin cá nhân cho chủ thể cung cấp dịch vụ, người dùng cần được thông tin đúng, gọn, rõ về cách thức, phương pháp mà bên xử lý sẽ thực hiện để xử lý dịch vụ của mình, địa điểm và máy chủ chứa thông tin cá nhân của mình, các dự định mà chủ thể xử lý sẽ thực hiện đối với dữ liệu của mình, bao gồm việc sử dụng vào mục đích thương mại;

(2) Quyền được biết chủ thể chịu trách nhiệm tiến hành xử lý dữ liệu của mình. Trong thực tiễn, chủ thể tiến hành xử lý dữ liệu bao gồm chủ thể thu thập, chủ thể xử lý đầu vào, chủ thể cung cấp dịch vụ lưu trữ dữ liệu trong hệ thống cơ sở dữ liệu, chủ thể cung cấp dịch vụ viễn thông để tiến hành truyền đưa dữ liệu, v.v. Việc xác định rõ ràng, chính xác chủ thể nào tiến hành công đoạn nào của quá trình xử lý, kể cả chủ thể bên thứ ba, giúp người dùng thực thi quyền riêng tư trong bối cảnh chuyển đổi số, đồng thời, tạo cơ sở để xác định trách nhiệm gắn liền với chủ thể trong trường hợp xảy ra tranh chấp, khiếu nại, phản ánh;

(3) Quyền yêu cầu sửa đổi, cải chính và ngừng cấp quyền xử lý cho chủ thể xử lý dữ liệu cá nhân của mình. Việc sửa đổi, cải chính thông tin phải được tiến hành trên căn cứ cá nhân phát hiện bằng chứng về việc

thông tin của mình bị sai lệch, suy diễn, ảnh hưởng đến danh dự, nhân phẩm của cá nhân. Trong trường hợp có căn cứ chính đáng và có nguyện vọng hợp pháp, cá nhân có quyền hủy cấp quyền xử lý đối với chủ thể xử lý dữ liệu của mình mà không gặp bất kì trở ngại nào.

(4) Quyền khiếu nại, phản ánh, thể hiện ý kiến đối với việc xử lý dữ liệu của chủ thể xử lý và quyền được yêu cầu cung cấp chứng nhận kiểm định an toàn trong việc xử lý dữ liệu. Người tiêu dùng có quyền phản ánh các thiếu sót, sai phạm của chủ thể xử lý dữ liệu thông qua hai đường, một là trực tiếp khiếu nại, phản ánh đến chủ thể xử lý dữ liệu, hai là phản ánh đến cơ quan nhà nước quản lý việc xử lý dữ liệu để cơ quan quản lý tiếp nhận, xử lý và thực hiện các quy trình pháp lý đảm bảo cân bằng quyền lợi của người tiêu dùng và của chủ thể kinh doanh.

Cần lưu ý việc ghi nhận quyền của người dùng như trên không nên tạo ra cơ chế để người dùng can thiệp quá sâu vào quy trình xử lý dữ liệu của chủ thể xử lý, bởi lẽ sẽ gây ra những trở ngại quá mức đến điều kiện kinh doanh và môi trường kinh doanh của các chủ thể kinh doanh trong môi trường số. Đặc biệt, các phản ánh, khiếu nại của người dùng phải đặt cơ sở trên căn cứ vững chắc và có cơ sở để tránh gây trở ngại không đáng có đến quyền tự do kinh doanh của chủ thể xử lý.

Về phía công tác lập quy và thực hiện chính sách của các cơ quan quản lý:

Một là, xây dựng cơ chế cho phép và khuyến khích các doanh nghiệp, tổ chức tiến hành tự xây dựng bộ quy chuẩn kĩ thuật, an toàn, an ninh đối với quy trình, công nghệ và hệ thống cơ sở dữ liệu sử dụng cho công tác xử lý dữ liệu, để tạo cơ sở chủ động cho các doanh nghiệp thực hiện nghĩa vụ đối với dữ liệu mà họ xử lý. Các bộ quy chuẩn nói trên được đánh giá và kiểm định theo phương pháp mệnh lệnh trong lĩnh vực hành chính, thông qua các cơ quan chuyên trách quản lý hoạt động xử lý dữ liệu (sắp tới, dự kiến sẽ là Ủy ban bảo vệ dữ liệu cá nhân, là cơ quan trực thuộc Chính phủ, đặt tại Cục an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an), dựa trên các nguyên tắc tiền đề trong Luật bảo vệ dữ liệu cá nhân. Tuy nhiên, công tác kiểm định này cần được thực hiện trên cơ sở linh hoạt, tránh gây ra rào cản bất hợp lý đến quyền tự do kinh doanh của chủ thể trong nền kinh tế. Công tác kiểm định và đánh giá tín nhiệm sẽ tạo cơ sở giảm tải các thủ tục trưng cầu sự đồng ý ở những khâu không cần

thiết, giảm bớt gánh nặng về chi phí tuân thủ trong giao dịch liên quan đến hoạt động xử lý dữ liệu cá nhân. Ngoài ra, đây sẽ là cơ sở hình thức để các bên trong quan hệ xử lý dữ liệu dân sự thể hiện quan hệ tín thác, cũng là cơ sở xác lập và chứng cứ trong trường hợp chủ thể xử lý vi phạm nghĩa vụ tương ứng với quyền của chủ thể dữ liệu.

Như vậy, cơ quan quản lý cần phải phối hợp chặt chẽ với doanh nghiệp, tổ chức, cá nhân tiến hành xử lý dữ liệu cá nhân để tiến hành các quy trình đầu vào, thử nghiệm, cấp phép cho doanh nghiệp, tổ chức, cá nhân trước khi các chủ thể này tiến hành cung cấp dịch vụ mạng. Cụ thể hơn, cơ quan quản lý cần phải thực hiện các công tác sau:

(1) Ủy ban bảo vệ dữ liệu cá nhân cần ban hành một bộ tiêu chuẩn an toàn đối với hệ thống xử lý dữ liệu của cơ quan, tổ chức, cá nhân. Bộ tiêu chuẩn này sẽ đóng vai trò là một bộ tiêu chuẩn mẫu cho cơ quan, tổ chức, cá nhân tuân thủ trong quá trình xây dựng cơ sở hạ tầng phục vụ việc cung cấp dịch vụ, đảm bảo an toàn thông tin, đồng thời, có đầy đủ cơ chế kĩ thuật để thông báo, xin phép, cũng như cho phép người dùng thể hiện rõ ý chí chia sẻ và trao quyền lưu trữ thông tin trước khi tiến hành thu thập thông tin người dùng (thông qua các phương tiện như thông báo pop-up, thư điện tử, v.v). Để không tạo gánh nặng tuân thủ và hạn chế quyền tự do kinh doanh của tổ chức, cá nhân, việc tuân thủ bộ tiêu chuẩn này là không bắt buộc; tuy nhiên, nếu cơ quan, tổ chức, cá nhân tự xây dựng bộ tiêu chuẩn thì phải đảm bảo đáp ứng được các tiêu chuẩn kĩ thuật đưa ra trong bộ tiêu chuẩn này. Để khách quan, quá trình xây dựng bộ tiêu chuẩn phải tham vấn chuyên gia về công nghệ thông tin, thương mại điện tử, chuyên gia an ninh mạng và chuyên gia pháp lý. Bộ tiêu chuẩn cũng cần được kiểm tra, đánh giá lại định kỳ hằng năm.

(2) Ủy ban bảo vệ dữ liệu cá nhân và các cơ quan quản lý phối hợp thực hiện kiểm định, cấp chứng nhận an toàn và cấp giấy phép tiến hành xử lý thông tin cá nhân cho cơ quan, tổ chức, cá nhân tiến hành xử lý thông tin. Đội ngũ đánh giá, kiểm định và cấp phép cần bao gồm các nhân sự được đào tạo chuyên môn trong lĩnh vực công nghệ thông tin và an ninh mạng. Trong trường hợp chủ thể mời bên thứ ba tiến hành kiểm định, đánh giá thì bên thứ ba này phải được cấp chứng chỉ về chuyên môn, tuân thủ các quy tắc ứng xử phù hợp với đạo đức trên cơ sở trung thực, khách quan và chịu trách nhiệm. Sau khi được cấp Giấy chứng nhận, các chủ thể xử lý thông tin phải đính kèm ký hiệu, hình

ảnh hoặc bản sao dưới hình thức thông điệp dữ liệu của Giấy chứng nhận an toàn này tại nơi dễ thấy trên website và giao diện ứng dụng dịch vụ, trước khi thu thập thông tin cá nhân phục vụ mục đích xử lý.

Hai là, cần thiết lập bộ phận chuyên trách để tiếp nhận tin báo, khiếu nại về các trường hợp vi phạm nghĩa vụ trong xử lý dữ liệu cá nhân, hoặc các trường hợp rò rỉ dữ liệu hệ thống. Cơ quan này có nhiệm vụ tiếp nhận tin báo, khiếu nại, đồng thời chuyển cho bộ phận chuyên trách tiến hành điều tra, xác minh vụ việc, làm rõ trách nhiệm của các bên liên quan trong các vụ vi phạm. Trong trường hợp cần thiết, cơ quan này có thể can thiệp vào hoạt động xử lý dữ liệu theo hướng yêu cầu tạm ngưng xử lý, hoặc tiến hành các biện pháp ngăn chặn cần thiết nhằm bảo vệ quyền nhân thân của cá nhân có thông tin được xử lý. Để làm được điều này, cần tiến hành các giải pháp cụ thể sau:

(1) Cơ quan tiếp nhận tin báo có số điện thoại đường dây nóng, e-mail tiếp nhận tin báo và nhân sự thực hiện trực nhận tin 24/24. Để làm được điều này, cần hoàn thiện cơ sở dữ liệu và hệ thống công nghệ thông tin phục vụ việc tiếp nhận, xử lý phản ánh của người dùng. Cơ quan này phải cam kết giữ bí mật thông tin của người phản ánh trong suốt quá trình từ tiếp nhận đến xử lý phản ánh của người tiêu dùng.

(2) Cơ quan tiếp nhận tin báo có thể được tổ chức hoạt động trực thuộc Cục cạnh tranh và bảo vệ quyền lợi người tiêu dùng, hoặc trực thuộc Cục an ninh mạng và phòng chống tội phạm công nghệ cao, hoặc được tổ chức liên ngành theo nguyên tắc phân công, phối hợp trong hệ thống hành chính.

(3) Sau khi xử lý phản ánh, cơ quan này có trách nhiệm ban hành quyết định xử lý phản ánh trên cơ sở kiểm tra, xác minh và làm việc với tổ chức, cá nhân bị phản ánh. Quyết định xử lý phản ánh này là văn bản áp dụng pháp luật, cần được xem là chứng cứ hợp lệ và có thể sử dụng trong quá trình giải quyết tranh chấp phát sinh giữa người dùng và bên xử lý dữ liệu về sau.

Về phía doanh nghiệp, tổ chức, cá nhân khác có tiến hành xử lý dữ liệu cá nhân:

Trên cơ sở các nguyên tắc được xây dựng trong luật, các bên trong quan hệ xử lý chủ động thực hiện quyền và nghĩa vụ của mình theo đúng tinh thần quản lý, đề cao pháp quyền; cụ thể, Các doanh nghiệp, tổ chức chủ động tuân thủ các nguyên tắc trên ngay từ khâu khởi sự thiết lập hệ

thống và mô hình kinh doanh, sao cho nguyên tắc bảo vệ quyền riêng tư được tích hợp một cách mặc định vào thiết kế mô hình kinh doanh và công nghệ ngay từ đầu (privacy by design and by default) (Ben Ayed, 2014; Tamò-Larrieux, 2018). Các chủ thể cũng cần thiết lập một cơ chế dự phòng rủi ro và các biện pháp an toàn, bảo mật, sao cho khi có sự cố an ninh mạng xảy ra, dữ liệu cá nhân được đảm bảo cập nhật đầy đủ và an toàn trong một hệ thống sao lưu. Đây cũng là cơ sở để cơ quan quản lý tiến hành thủ tục kiểm định an toàn đối với công tác xử lý dữ liệu trong hệ thống.

Ngoài ra, các chủ thể tuyệt đối tuân thủ quy định được xây dựng trong Luật bảo vệ dữ liệu cá nhân, theo đó, chủ thể xử lý dữ liệu có nghĩa vụ tôn trọng quyền nhân thân của chủ thể thông tin, thông tin minh bạch mục đích, phương thức và hệ quả xử lý dữ liệu cá nhân cho chủ thể thông tin, chịu trách nhiệm đối với các vi phạm quyền nhân thân do lỗi của mình gây ra. Trong trường hợp bất khả kháng cần phải tiết lộ dữ liệu hoặc xảy ra các tai nạn ngoài ý muốn, chủ thể xử lý phải thông báo ngay lập tức đến người có thông tin đang được xử lý, trong trường hợp cần thiết, phải yêu cầu cơ quan chức năng can thiệp để đảm bảo tốt nhất quyền lợi của đôi bên trong quan hệ xử lý dữ liệu, đảm bảo lòng tin của chủ thể dữ liệu vào hệ thống cơ sở dữ liệu và an toàn mạng.

Ngoài ra, các chủ thể cần phải tôn trọng, tuân thủ các quy định về bảo vệ quyền lợi của người tiêu dùng theo Luật bảo vệ quyền lợi người tiêu dùng, cụ thể như sau:

(1) Khi xây dựng văn bản hoặc thông điệp điện tử để trưng cầu sự đồng ý của chủ thể dữ liệu ở khâu đầu vào, bên xử lý không được xây dựng các điều khoản khó hiểu, đa nghĩa, gây bất lợi cho người tiêu dùng (khoản 2, Điều 14 Luật bảo vệ quyền lợi người tiêu dùng), hay cho phép chủ thể xử lý có quyền giải thích đối với các điều khoản đó trong trường hợp điều khoản có nhiều cách hiểu khác nhau (điểm e, khoản 1, Điều 16 Luật bảo vệ quyền lợi người tiêu dùng).

(2) Trong quá trình cung cấp dịch vụ cho người dùng, chủ thể xử lý dữ liệu không được chấm dứt, hoãn hay tạm ngừng cung cấp dịch vụ với lý do phục vụ kiểm tra, đánh giá theo yêu cầu của phản ánh. Sâu xa hơn, chủ thể xử lý không được đặt người dùng vào tình thế phải chấp nhận chính sách xử lý thông tin mới được sử dụng dịch vụ (take it or leave it); trái lại, chủ thể cung cấp dịch vụ vẫn phải cung cấp dịch vụ cho người dùng dưới dạng người dùng phi thành viên, nếu người dùng

không đồng ý với chính sách xử lý dữ liệu, hoặc người dùng có phản ánh, khiếu nại đối với phương thức xử lý dữ liệu liên quan đến thông tin cá nhân của mình. Trong các trường hợp này, chủ thể cung cấp dịch vụ phải tự giải quyết hoặc phối hợp với cơ quan quản lý giải quyết yêu cầu của người dùng một cách trung thực, thiện chí.

5. KẾT LUẬN

Văn kiện Nghị quyết 52-NQ/TW ngày 27/09/2019 của Bộ Chính trị về một số chủ trương, chính sách chủ động tham gia cuộc cách mạng công nghiệp lần thứ tư đã nhận xét mức độ chủ động tham gia cuộc Cách mạng công nghiệp lần thứ tư của nước ta còn thấp vì thể chế, chính sách còn nhiều hạn chế và bất cập, khoa học - công nghệ và đổi mới sáng tạo chưa thực sự là động lực phát triển kinh tế - xã hội; hệ thống đổi mới sáng tạo quốc gia mới được hình thành, chưa đồng bộ và hiệu quả. Tại Quyết định 749/QĐ-TTg, Thủ tướng Chính phủ cũng quán triệt nhận thức thể chế, công nghệ là động lực của chuyển đổi số. Tại Quyết định 2289/QĐ-TTg cũng cho thấy cải cách pháp quy nhằm tạo chuẩn mực ứng xử phù hợp trong môi trường số, đặc biệt liên quan đến thông tin cá nhân, là vô cùng bức thiết.

Nghiên cứu này trả lời cho câu hỏi liệu có một nền tảng nguyên tắc xuyên suốt để phát triển khung pháp lý về bảo vệ dữ liệu cá nhân ở Việt Nam; và làm thế nào để xây dựng khung pháp lý về bảo vệ dữ liệu cá nhân nhằm phát huy hiệu quả việc bảo vệ quyền riêng tư của chủ thể dữ liệu trong tương quan với hoạt động xử lý dữ liệu của chủ thể xử lý. Kết quả nghiên cứu cho thấy, hướng tiếp cận bảo vệ quyền riêng tư dựa trên việc trao quyền tuyệt đối cho chủ thể dữ liệu trong việc giữ bí mật và định đoạt dữ liệu cá nhân là không hiệu quả, nếu không có nhận thức đúng đắn về quyền riêng tư trong bối cảnh CMCN 4.0 và bộ nguyên tắc rõ ràng trong việc xử lý dữ liệu cá nhân làm nền tảng. Từ kết quả trên, bài viết đề xuất hai nhóm nguyên tắc chủ đạo là đảm bảo pháp quyền xã hội chủ nghĩa, đồng bộ hóa hệ thống pháp luật và đảm bảo chủ quyền quốc gia, cân bằng lợi ích giữa các chủ thể trên cơ sở đề cao tự do ý chí của các bên trong quan hệ pháp luật. Bài viết cũng đưa ra bốn đề xuất cụ thể cho công tác lập pháp và thực hiện chính sách trong tương lai, bao gồm sửa đổi, bổ sung các quy định pháp luật trong Bộ luật Dân sự đi kèm với việc ban hành một văn bản pháp luật chuyên ngành, thống nhất về Bảo vệ dữ liệu cá nhân, trên tinh thần khuyến khích ý chí tự do của các bên chủ thể và kiểm soát hoạt động bảo vệ dữ liệu thông qua cơ chế quy chuẩn, kiểm định nhằm kiến tạo môi trường kinh doanh thông thoáng, phát huy năng lực đổi mới, sáng tạo của doanh nghiệp công nghệ trong quá trình chuyển đổi số.

TÀI LIỆU THAM KHẢO

1. Akter, S., & Wamba, S. F. (2016). Big data analytics in E-commerce: A systematic review and agenda for future research. *Electronic Markets*, *26*(2), 173–194. https://doi.org/10.1007/s12525-016-0219-0
2. Amit, R., & Zott, C. (2017). Value Drivers of e-Commerce Business Models. Trong *Creating Value: Winners in the New Business Environment* (tr 13–43). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781405164092.ch2
3. Anderson, R., & Moore, T. (2006). The Economics of Information Security. *Science*, *314*(5799), 610–613. https://doi.org/10.1126/science.1130992
4. Anh Quân & Thành Luân. (2021, Tháng Năm 19). *Vụ rò rỉ 17 GB dữ liệu người dùng Việt: Cách bảo vệ thông tin cá nhân*. Báo Thanh Niên. https://thanhnien.vn/content/MTA2OTA3OA==.html
5. Ballardini, R. M., Kuoppamäki, P., Pitkänen, O., & Future Regulation of Industrial Internet (Project) (B.t.v). (2019). Industrial Internet Solutions and Data Ownership Versus Control over Data. Trong *Regulating Industrial Internet through IPR, data protection and competition law*. Kluwer Law International B.V.
6. Ben Ayed, G. (2014). *Architecting User-Centric Privacy-as-a-Set-of-Services*. Springer International Publishing. https://doi.org/10.1007/978-3-319-08231-8
7. Bygrave, L. A. (2014). *Data privacy law: An international perspective* (First edition). Oxford University Press.
8. Cameron A., Pham T H, Altherton J, Nguyen D H, Nguyen T P, Tran S T, Nguyen T N, Trinh H Y, & Hajkowicz S. (2019). *Tương lai nền kinh tế số Việt Nam—Hướng tới năm 2030 và 2045*. CSIRO.
9. Chowdhury, M. J. M., Colman, A., Kabir, M. A., Han, J., & Sarda, P. (2018). Blockchain as a Notarization Service for Data Sharing with Personal Data Store. *Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering:*

Trustcom/BigDataSE 2018, 1330–1335. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00183

10. Craig, T., & Ludloff, M. E. (2011). *Privacy and big data*. O'Reilly Media, Inc.
11. Davenport, T. H., & Bean, R. (2018). *Big Companies Are Embracing Analytics, But Most Still Don't Have a Data-Driven Culture*. Harvard Business Review.
12. European Commission. (2017). *Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions "Building A European Data Economy"*. COM/2017/09 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A9%3AFIN
13. Higham, L. (2016). *Best Practices of Big Data Analytics Applied to PII Security*. https://dash.harvard.edu/handle/1/33825785
14. Hoeren, D. T. (2014). Big Data and the Ownership in Data: Recent Developments in Europe. *European Intellectual Property Review*, *36*(12), 4.
15. Janeček, V., & Malgieri, G. (2019). *Data Extra Commercium* (SSRN Scholarly Paper ID 3400620). Social Science Research Network. https://papers.ssrn.com/abstract=3400620
16. Justickis, V. (2020). Balancing Personal Data Protection with Other Human Rights and Public Interest: Between Theory and Practice. *Baltic Journal of Law & Politics*, *13*(1), 140–162. https://doi.org/10.2478/bjlp-2020-0006
17. Kalyvas, J. R., & Overly, M. R. (2015). *Big data: A business and legal guide*. CRC Press.
18. Kang, J. (1997). Information Privacy in Cyberspace Transactions. *Stanford Law Review*, *50*, 1193. https://heinonline.org/HOL/Page?handle=hein.journals/stflr50&id=1211&div=&collection=
19. Kramer, F. D., Starr, S. H., Wentz, L. K., & Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. Trong *Cyberpower and National Security*. Potomac Books, Inc.

20. Lasse Eriksson, Matti Rossi, J. P. Shim, & Carsten Sørensen. (2019). Business and Research Perspectives of Industrial Internet Applications. Trong R. M. Ballardini, P. Kuoppamäki, O. Pitkänen, & Future Regulation of Industrial Internet (Project) (B.t.v), *Regulating Industrial Internet through IPR, data protection and competition law*. Kluwer Law International B.V.

21. Malgieri, G. (2016). *"Ownership" of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?* (SSRN Scholarly Paper ID 2916079). Social Science Research Network. https://papers.ssrn.com/abstract=2916079

22. Malgieri, G., & Custers, B. (2017). *Pricing Privacy – The Right to Know the Value of Your Personal Data* (SSRN Scholarly Paper ID 3047257). Social Science Research Network. https://papers.ssrn.com/abstract=3047257

23. Martti Mäntylä. (2019). Industrial Internet Technologies. Trong R. M. Ballardini, P. Kuoppamäki, O. Pitkänen, & Future Regulation of Industrial Internet (Project) (B.t.v), *Regulating Industrial Internet through IPR, data protection and competition law*. Kluwer Law International B.V.

24. Moore, A. D. (2010). *Privacy rights: Moral and legal foundations*. Pennsylvania State University Press.

25. Nguyễn, Đ. D., Vũ Công Giao, & Lã, K. T. (2015). *Giáo trình lý luận và pháp luật về quyền con người* (Tái bản lần thứ hai có sửa chữa, bổ sung). Nhà xuất bản Chính trị quốc gia - sự thật.

26. Nguyễn Mạnh Thắng. (2018). Dẫn luận về đồng bộ hóa luật tư ở Việt Nam hiện nay. Trong *Đồng bộ hóa luật tư ở Việt Nam hiện nay*. NXB Công an Nhân dân.

27. Nick Barrowman. (2018). *Why Data Is Never Raw*. The New Atlantis. http://www.thenewatlantis.com/publications/why-data-is-never-raw

28. Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus*, *140*(4), 32–48. https://www.jstor.org/stable/23046912

29. Nissenbaum, H. F. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law Books.

30. OECD. (2013). *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value* (OECD Digital Economy Papers Số p.h 220; OECD Digital Economy Papers, Vol 220). https://doi.org/10.1787/5k486qtxldmq-en

31. Onik, M. M. H., Kim, C.-S., Lee, N.-Y., & Yang, J. (2019). Privacy-aware blockchain for personal data sharing and tracking. *Open Computer Science*, *9*(1), 80–91. https://doi.org/10.1515/comp-2019-0005

32. Pal, R., Golubchik, L., Psounis, K., & Hui, P. (2014). Will cyber-insurance improve network security? A market analysis. *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, 235–243. https://doi.org/10.1109/INFOCOM.2014.6847944

33. Petteri Günther. (2019). Industrial Internet Solutions and Data Ownership Versus Control over Data. Trong *Regulating Industrial Internet Through IPR, Data Protection and Competition Law*.

34. Purtova, N. (2012). *Property rights in personal data: A European perspective*. Kluwer Law International ; Sold and distributed in North, Central, and South America by Aspen Publishers.

35. Ritter, J., & Mayer, A. (2017). Regulating Data as Property: A Construction for Moving Forward. *Duke Law & Technology Review*, *16*(1), 220.

36. Rob Sobers. (2021). *The World in Data Breaches*. Varonis. https://www.varonis.com/blog/the-world-in-data-breaches/

37. Sam Wrigley, Anette Alén-Savikko & Olli Pitkänen. (2019). Finding the "Personal" in the Industrial Internet: Why Data Protection Law Still Matters. Trong R. M. Ballardini, P. Kuoppamäki, O. Pitkänen, & Future Regulation of Industrial Internet (Project) (B.t.v), *Regulating Industrial Internet through IPR, data protection and competition law*. Kluwer Law International B.V.

38. Schwab, K., & Davis, N. (2018). *Shaping the future of the fourth industrial revolution: A guide to building a better world* (First American edition). Currency.

39. Schwartz, P. M. (2005). *Property, Privacy, and Personal Data* (SSRN Scholarly Paper ID 721642). Social Science Research Network. https://papers.ssrn.com/abstract=721642

40. Sedkaoui, S., & Khelfaoui, M. (2020). *Sharing Economy and Big Data Analytics*. John Wiley & Sons.

41. Solove, D. J. (2000). Privacy and Power: Computer Databases and Metaphors for Information Privacy. *Stanford Law Review*, *53*, 1393. https://heinonline.org/HOL/Page?handle=hein.journals/stflr53&id=1411&div=&collection=

42. Solove, D. J. (2007). *The future of reputation: Gossip, rumor, and privacy on the Internet*. Yale University Press.

43. Tamò-Larrieux, A. (2018). *Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things* (Vol 40). Springer International Publishing. https://doi.org/10.1007/978-3-319-98624-1

44. *The EU GDPR's impact on ASEAN data protection law*. (2019). Financier Worldwide. https://www.financierworldwide.com/the-eu-gdprs-impact-on-asean-data-protection-law

45. Tristan Henderson & Burkhard Schafer. (2019). Data Protection, Certification and the Fourth Industrial Revolution. Trong R. M. Ballardini, P. Kuoppamäki, O. Pitkänen, & Future Regulation of Industrial Internet (Project) (B.t.v), *Regulating Industrial Internet through IPR, data protection and competition law*. Kluwer Law International B.V.

46. Truong, N. B., Sun, K., Lee, G. M., & Guo, Y. (2020). GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. *IEEE Transactions on Information Forensics and Security*, *15*, 1746–1761. https://doi.org/10.1109/TIFS.2019.2948287

47. Tuomas Pöysti. (2019). The IIoT and Design for Contextually Relevant Data Protection. Trong R. M. Ballardini, P. Kuoppamäki, O. Pitkänen, & Future Regulation of Industrial Internet (Project) (B.t.v), *Regulating Industrial Internet through IPR, data protection and competition law*. Kluwer Law International B.V.

48. *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, United Nations Human Rights Committee (1988) (testimony of UN Human Rights

Committee (HRC)). https://www.refworld.org/docid/453883f922.html

49. Wachter, S., & Mittelstadt, B. (2019). A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, *2019*, 494. https://heinonline.org/HOL/Page?handle=hein.journals/colb2019&id=506&div=&collection=
50. Weber, R. H., & Weber, R. (2010). *Internet of things: Legal perspectives*. Springer : Schulthess.
51. Westin, A. F. (1970). *Privacy and freedom*. Bodley Head.
52. XING Hui-Qiang. (2019). 大数据交易背景下个人信息财产权的分配与实现机制. Secress (安全内参）. https://www.secrss.com/article/15414