BỘ CÔNG AN
TRƯỜNG ĐẠI HỌC AN NINH NHÂN DÂN

BÀI DỰ THI

Tìm Hiểu

LUẬT DỮ LIỆU

Trong Công An Nhân Dân



NHÓM TÁC GIẢ DỰ THI:
Chiến sĩ An ninh dữ liệu số - T04

Quyển 1

PHÁP LUẬT VỀ DỮ LIỆU - THẾ GIỚI VÀ VIỆT NAM



TP. HỒ CHÍ MINH - NĂM 2025

BỘ CÔNG AN
TRƯỜNG ĐẠI HỌC AN NINH NHÂN DÂN

BÀI DỰ THI

Tìm hiểu

LUẬT DỮ LIỆU
TRONG CÔNG AN NHÂN DÂN

NHÓM TÁC GIẢ DỰ THI:
Chiến sĩ An ninh dữ liệu số - T04



Quyển 1

PHÁP LUẬT VỀ DỮ LIỆU - THẾ GIỚI VÀ VIỆT NAM

TP. HỒ CHÍ MINH - NĂM 2025

CHIẾN SĨ AN NINH DỮ LIỆU SỐ



PHẠM VĂN TỰ

Năm sinh: **29/05/1980** Giới tính: **Nam**
Dân tộc: **Kinh** Cấp bậc: **Thượng tá**
Chức vụ: **Giảng viên chính**
Đơn vị: **Khoa Ngoại ngữ - Tin học – Trường Đại học An ninh nhân dân**
Số điện thoại: **0938.950.948**



MAI HOÀNG NHU

Năm sinh: **10/09/2003** Giới tính: **Nam**
Dân tộc: **Kinh** Cấp bậc: **Học viên**
Đơn vị: **Trung đội D30B1 – Trường Đại học An ninh nhân dân**
Số điện thoại: **0814.768.391**



TỐNG GIA KHÁNH

Năm sinh: **16/12/2003** Giới tính: **Nam**
Dân tộc: **Kinh** Cấp bậc: **Học viên**
Đơn vị: **Trung đội D30B2 – Trường Đại học An ninh nhân dân**
Số điện thoại: **0904.369.038**



NGUYỄN XUÂN VƯỢNG

Năm sinh: **25/11/2003** Giới tính: **Nam**
Dân tộc: **Kinh** Cấp bậc: **Học viên**
Đơn vị: **Trung đội D30B2 – Trường Đại học An ninh nhân dân**
Số điện thoại: **0374.009.946**



ĐẶNG HOÀNG KHẢI

Năm sinh: **21/08/2003** Giới tính: **Nam**
Dân tộc: **Kinh** Cấp bậc: **Học viên**
Đơn vị: **Trung đội D30C2 – Trường Đại học An ninh nhân dân**
Số điện thoại: **0346.940.451**

Mục lục

LỜI MỞ ĐẦU 08

TÓM TẮT NỘI DUNG 11

Câu 1: Chính sách pháp luật về dữ liệu của các nước trên thế giới? Sự cần thiết, quan điểm, mục tiêu và chính sách xây dựng, hoàn thiện quy định pháp luật về dữ liệu tại Việt Nam? 16

1.1. CHÍNH SÁCH, PHÁP LUẬT VỀ DỮ LIỆU TRONG CÁC VĂN BẢN PHÁP LUẬT QUỐC TẾ 17

1.1.1. Công ước Quốc tế về các Quyền Dân sự và Chính trị (International Covenant on Civil and Political Rights - ICCPR) năm 1966 17

1.1.2. Hướng dẫn của Liên hợp quốc về Hồ sơ dữ liệu trên máy tính (UN Guidelines on Computerized Data Files) (Nghị quyết Đại hội đồng 45/95, ngày 14 tháng 12 năm 1990) 18

1.1.3. Một số văn bản của Ủy ban Liên Hợp Quốc về Luật Thương mại Quốc tế (UNCITRAL) 22

1.1.4. Công ước về Quyền Trẻ em (Convention on the Rights of the Child - CRC) năm 1989 25

1.2. CHÍNH SÁCH, PHÁP LUẬT VỀ DỮ LIỆU TẠI MỘT SỐ QUỐC GIA, KHU VỰC TRÊN THẾ GIỚI 29

1.2.1. Liên minh châu Âu 39

1.2.2. Hoa Kỳ 87

1.2.3. Trung Quốc 99

1.2.4. Hàn Quốc 123

1.2.5. Nhật Bản 134

1.2.6. Bỉ 144

1.2.7. Thổ Nhĩ Kỳ 163

1.2.8. Liên bang Nga 187

1.2.9. Ấn Độ 193

1.2.10. Đan Mạch 196

1.2.11. Úc 197

1.2.12. Các quốc gia Đông Nam Á (ASEAN) 200

1.2.13. Một số quốc gia khác 230

1.2.14. So sánh các mô hình chính sách pháp luật về dữ liệu và bài học kinh nghiệm cho Việt Nam 234

1.3. SỰ CẦN THIẾT XÂY DỰNG VÀ HOÀN THIỆN PHÁP LUẬT VỀ DỮ LIỆU Ở VIỆT NAM 257

1.3.1. Bối cảnh trong nước và quốc tế 257

1.3.2. Cơ sở chính trị 282

1.3.3. Cơ sở thực tiễn 315

1.4. QUAN ĐIỂM, MỤC TIÊU VÀ ĐỊNH HƯỚNG CHÍNH SÁCH XÂY DỰNG, HOÀN THIỆN PHÁP LUẬT VỀ DỮ LIỆU TẠI VIỆT NAM 336

1.4.1. Quan điểm chỉ đạo 336

1.4.2. Mục đích 343

1.4.3. Định hướng chính sách xây dựng, hoàn thiện pháp luật về dữ liệu tại Việt Nam 351

Câu 2: Quyền, nghĩa vụ và trách nhiệm của chủ thể dữ liệu, chủ sở hữu dữ liệu, chủ quản dữ liệu? Cơ chế bảo đảm thực hiện các quyền, nghĩa vụ này đối với tổ chức, cá nhân không phải là cơ quan nhà nước? 391

2.1. MỘT SỐ KHÁI NIỆM CÓ LIÊN QUAN 392

2.1.1. Dữ liệu 392

2.1.2. Chủ thể dữ liệu 423

2.1.3. Chủ sở hữu dữ liệu 428

2.1.4. Chủ quản dữ liệu 436

2.2. QUYỀN, NGHĨA VỤ VÀ TRÁCH NHIỆM CỦA CHỦ THỂ DỮ LIỆU, CHỦ SỞ HỮU DỮ LIỆU, CHỦ QUẢN DỮ LIỆU 438

2.2.1. Quyền, nghĩa vụ và trách nhiệm của chủ thể dữ liệu 438

2.2.2. Quyền, nghĩa vụ và trách nhiệm của chủ quản dữ liệu 464

2.2.3. Quyền, nghĩa vụ và trách nhiệm của chủ sở hữu dữ liệu 475

2.3. CƠ CHẾ BẢO ĐẢM THỰC HIỆN CÁC QUYỀN, NGHĨA VỤ TRÊN ĐỐI VỚI TỔ CHỨC, CÁ NHÂN KHÔNG PHẢI LÀ CƠ QUAN NHÀ NƯỚC 491

Câu 3: Quy định về hành vi bị nghiêm cấm trong Luật Dữ liệu năm 2024? Giải pháp xây dựng, hoàn thiện quy định pháp luật về xử lý vi phạm hành chính trong lĩnh vực dữ liệu? 500

3.1. MỘT SỐ HÀNH VI BỊ NGHIÊM CẤM TRONG PHÁP LUẬT VỀ DỮ LIỆU Ở MỘT SỐ QUỐC GIA TRÊN THẾ GIỚI 501

3.2. CÁC HÀNH VI BỊ NGHIÊM CẤM TRONG PHÁP LUẬT VỀ DỮ LIỆU TẠI VIỆT NAM 505

3.3. MỘT SỐ HẠN CHẾ, VƯỚNG MẮC TRONG QUY ĐỊNH CỦA PHÁP LUẬT VỀ XỬ LÝ VI PHẠM HÀNH CHÍNH VỀ DỮ LIỆU TẠI VIỆT NAM 522

3.4. MỘT SỐ GIẢI PHÁP HOÀN THIỆN QUY ĐỊNH PHÁP LUẬT VỀ XỬ LÝ VI PHẠM HÀNH CHÍNH TRONG LĨNH VỰC DỮ LIỆU 527

3.4.1. Nghiên cứu, xây dựng quy định của pháp luật về xử lý vi phạm hành chính trong lĩnh vực dữ liệu theo hướng bổ sung vào Luật Xử lý vi phạm hành chính các quy định liên quan đến xử lý vi phạm hành chính trong lĩnh vực dữ liệu; trên cơ sở đó, nghiên cứu, xây dựng Nghị định của Chính phủ quy định về xử phạt vi phạm hành chính trong lĩnh vực dữ liệu 527

3.4.2. Rà soát để đề xuất sửa đổi, bổ sung các văn bản quy phạm pháp luật khác có liên quan đến xử lý vi phạm hành chính trong lĩnh vực dữ liệu, bảo đảm tính thống nhất trong hệ thống văn bản quy phạm pháp luật có liên quan 539

3.4.3. Tổ chức thu thập thông tin, các ý kiến đề xuất xây dựng quy định về xử phạt hành chính đối với hành vi vi phạm pháp luật trên lĩnh vực dữ liệu 542

3.4.4. Tăng cường hợp tác quốc tế, tiếp thu các bài học kinh nghiệm quốc tế để hoàn thiện hơn việc xử lý vi phạm dữ liệu 546

DANH MỤC TÀI LIỆU THAM KHẢO 550

Lời mở đầu

"Dữ liệu là tài nguyên chiến lược của quốc gia trong kỷ nguyên số".

Trong bối cảnh cuộc Cách mạng công nghiệp lần thứ tư và chuyển đổi số sâu rộng, dữ liệu đang vươn lên thành nguồn lực cốt yếu của nền kinh tế và xã hội toàn cầu. Nhiều quốc gia trên thế giới đã sớm ban hành các chính sách, luật pháp nhằm quản lý, khai thác, sử dụng và bảo vệ dữ liệu: Luật Quản trị dữ liệu 2022 và Luật Dữ liệu 2023 của Châu Âu áp dụng chung cho 27 nước thành viên; Trung Quốc cũng đã lần lượt ban hành Luật An ninh mạng 2017, Luật An toàn dữ liệu 2021 và Luật Bảo vệ thông tin cá nhân 2021 tạo thành bộ khung pháp luật toàn diện về dữ liệu và quyền riêng tư. Điều này cho thấy dữ liệu ngày nay không chỉ là yếu tố kỹ thuật đơn thuần, mà đã trở thành tài sản chiến lược gắn liền với an ninh, chủ quyền và lợi thế cạnh tranh quốc gia. Cuộc cạnh tranh chiến lược toàn cầu về dữ liệu và công nghệ số hiện đang diễn ra quyết liệt hơn bao giờ hết, buộc mỗi quốc gia phải chú trọng củng cố nền tảng pháp lý và năng lực quản trị dữ liệu để không bị tụt hậu trong kỷ nguyên số.

Ở Việt Nam, Đảng và Nhà nước đã triển khai nhiều chủ trương, chính sách phát triển khoa học, công nghệ, nhất là những vấn đề liên quan đến xây dựng, tạo lập, kết nối, chia sẻ dữ liệu như Nghị quyết số 52-NQ/TW ngày 27/9/2019 của Bộ Chính trị về một số chủ trương, chính sách chủ động tham gia cuộc Cách mạng công nghiệp lần thứ tư; Văn kiện Đại hội Đảng lần thứ XIII; Chiến lược dữ liệu quốc gia quy định tại Quyết định số 142/QĐ-TTg ngày 02/02/2024 của Thủ tướng Chính phủ; Đề án xây dựng Trung tâm dữ liệu quốc gia quy định tại Nghị quyết số 175/NQ-CP ngày 30/10/2023 của Chính phủ; Quy hoạch hạ tầng thông tin và truyền thông thời kỳ 2021 - 2030,

tầm nhìn đến năm 2050 quy định tại Quyết định số 36/QĐ-TTg ngày 11/01/2024 của Thủ tướng Chính phủ. Tổng Bí thư Tô Lâm đã từng phát biểu: *"Chúng ta đang bước vào giai đoạn bình minh của kỷ nguyên số, thời kỳ dữ liệu đã trở thành tài nguyên, tư liệu sản xuất quan trọng, trở thành "năng lượng mới", thậm chí là "máu" của nền kinh tế số. Chuyển đổi số, với dữ liệu là trung tâm, đang làm thay đổi căn bản cách chúng ta sống, làm việc và phát triển"*. Thế nhưng trước đây, các quy định pháp luật liên quan đến dữ liệu ở nước ta còn rời rạc, thiếu tính thống nhất và chưa có một đạo luật riêng điều chỉnh toàn diện, dẫn đến tình trạng chồng chéo và để lại nhiều khoảng trống pháp lý. Việc ban hành Luật Dữ liệu năm 2024 đã tạo nên một bước ngoặt quan trọng, hình thành khuôn khổ pháp lý thống nhất cho việc quản lý, khai thác, chia sẻ và bảo vệ dữ liệu; song, việc tiếp tục hoàn thiện hệ thống pháp luật này vẫn là yêu cầu cấp bách, nhằm đáp ứng nhu cầu phát triển, bảo đảm an ninh, chủ quyền số và đáp ứng yêu cầu hội nhập quốc tế.

Vì lẽ đó, việc tham gia Cuộc thi ***"Tìm hiểu Luật Dữ liệu trong Công an nhân dân"*** do Bộ Công an tổ chức không chỉ là cơ hội để nâng cao nhận thức, mà còn là dịp để mỗi cán bộ, chiến sĩ, giảng viên và học viên nâng cao kiến thức, từ đó thực hiện tốt hơn chức trách, nhiệm vụ được giao. Trên cơ sở đó, cùng với mục đích góp phần phổ biến, tuyên truyền Luật Dữ liệu và các văn bản hướng dẫn thi hành, nhóm tác giả ***"Chiến sĩ An ninh dữ liệu số"*** đến từ Trường Đại học An ninh nhân dân, đã nghiêm túc nghiên cứu và xây dựng Bài dự thi thành 05 Quyển cùng các mô hình minh họa trực quan, sinh động, thể hiện đúng tinh thần đẩy mạnh chuyển đổi số trong bối cảnh hiện nay.

Trong đó, ***Quyển 1: Pháp luật về dữ liệu - Thế giới và Việt Nam***, đã phân tích, làm rõ nội dung của 03 câu hỏi sau đây:

Câu 1: Chính sách pháp luật về dữ liệu của các nước trên thế giới? Sự cần thiết, quan điểm, mục tiêu và chính sách xây dựng, hoàn thiện quy định pháp luật về dữ liệu tại Việt Nam?

Câu 2: Quyền, nghĩa vụ và trách nhiệm của chủ thể dữ liệu, chủ sở hữu dữ liệu, chủ quản dữ liệu? Cơ chế bảo đảm thực hiện các quyền, nghĩa vụ này đối với tổ chức, cá nhân không phải là cơ quan nhà nước?

Câu 3: Quy định về hành vi bị nghiêm cấm trong Luật Dữ liệu năm 2024? Giải pháp xây dựng, hoàn thiện quy định pháp luật về xử lý vi phạm hành chính trong lĩnh vực dữ liệu?

Với tinh thần nghiêm túc và trách nhiệm cao, chúng tôi hy vọng bài dự thi sẽ mang lại những đóng góp tích cực cho công tác triển khai thi hành Luật Dữ liệu trong toàn xã hội, đáp ứng yêu cầu của thực tiễn và mục tiêu xây dựng một quốc gia giàu mạnh, hùng cường trong kỷ nguyên số.

Nhóm tác giả trân trọng nhận được sự góp ý của Quý Ban giám khảo và Quý bạn đọc./.

Chào thân ái và quyết thắng!

Nhóm "Chiến sĩ An ninh dữ liệu số"

Trường Đại học An ninh nhân dân

Tóm tắt nội dung

QUYỂN 1: PHÁP LUẬT VỀ DỮ LIỆU - THẾ GIỚI VÀ VIỆT NAM

- Chiến sĩ An ninh dữ liệu số -

Nhằm giúp Quý Ban Giám khảo và Quý độc giả có góc nhìn tổng quan, sinh động và toàn diện khi nghiên cứu *Quyển 1: Pháp luật về dữ liệu - Thế giới và Việt Nam,* nhóm tác giả đã xây dựng bản tóm tắt nội dung ba câu hỏi 01, 02 và 03 như sau:

*** Câu 1: Chính sách pháp luật về dữ liệu của các nước trên thế giới? Sự cần thiết, quan điểm, mục tiêu và chính sách xây dựng, hoàn thiện quy định pháp luật về dữ liệu tại Việt Nam?**

Mở đầu cho bộ câu hỏi trong khuôn khổ Bài dự thi "Tìm hiểu Luật Dữ liệu trong Công an nhân dân" là một câu hỏi rất sâu sắc, mang tính nền tảng; là cơ sở để chúng ta có cái nhìn tổng quan, toàn diện khi nghiên cứu về sự cần thiết phải ban hành cũng như những nội dung trọng tâm được quy định tại Luật Dữ liệu năm 2024. Nghiên cứu chính sách pháp luật về dữ liệu của các nước trên thế giới là hết sức cần thiết để Việt Nam nắm bắt xu hướng quản trị dữ liệu hiện đại, học hỏi những kinh nghiệm lập pháp và thực thi đã được kiểm chứng từ các nền lập pháp, hành pháp và kinh tế lớn trên toàn thế giới; tránh lặp lại những hạn chế mà các quốc gia khác đã gặp phải. Nghiên cứu câu hỏi số 01, nhóm tác giả chia thành hai phần chính: ***(1)*** Chính sách, pháp luật về dữ liệu trong các văn bản pháp luật quốc tế; ***(2)*** Chính sách, pháp luật về dữ liệu tại một số quốc gia, khu vực trên thế giới; ***(3)*** Sự cần thiết xây dựng và hoàn thiện pháp luật về dữ liệu ở Việt Nam; ***(4)*** Quan điểm, mục tiêu và định hướng chính sách xây dựng, hoàn thiện pháp luật về dữ liệu tại Việt Nam.

- Phần thứ nhất, mục *"1.1. Chính sách, pháp luật về dữ liệu trong các văn bản pháp luật quốc tế"*, đã đề cập đến *một số văn bản, tiêu chuẩn và quy phạm pháp luật quốc tế* như Công ước Quốc tế về các Quyền Dân sự và Chính trị năm 1966; Hướng dẫn của Liên hợp quốc về Hồ sơ dữ liệu trên máy tính; một số văn bản của Ủy ban Liên Hợp Quốc về Luật Thương mại Quốc tế; Công ước về Quyền Trẻ em năm 1989. Một số quy định trong các văn bản, tiêu chuẩn và quy phạm pháp luật này có thể xem là nền tảng cho các quy định về dữ liệu ngày nay.

- Phần thứ hai, mục *"1.2. Chính sách, pháp luật về dữ liệu tại một số quốc gia, khu vực trên thế giới"*. Qua nghiên cứu các khung pháp lý về dữ liệu điển hình trên thế giới, nhóm tác giả đã chọn ra **24** quốc gia, khu vực điển hình, gồm Liên minh châu Âu, Hoa Kỳ, Trung Quốc, Hàn Quốc, Nhật Bản, Bỉ, Thổ Nhĩ Kỳ, Liên bang Nga, Ấn Độ, Đan Mạch, Úc, các quốc gia Đông Nam Á và một số quốc gia khác; từ đó, phân tích, đánh giá, rút ra những ưu điểm, hạn chế để làm cơ sở so sánh với Luật Dữ liệu ở Việt Nam.

- Phần thứ ba, mục *"1.3. Sự cần thiết xây dựng và hoàn thiện pháp luật về dữ liệu ở Việt Nam"*. Bối cảnh quốc tế với xu hướng toàn cầu hóa và sự trỗi dậy của kinh tế số, cùng với những chuyển biến sâu sắc trong đời sống kinh tế - xã hội trong nước, đã đặt ra yêu cầu cấp thiết về việc xây dựng một hành lang pháp lý toàn diện và thống nhất cho dữ liệu. Nhận thức rõ điều này, nhóm tác giả tiến hành phân tích sâu các cơ sở chính trị và thực tiễn, qua đó luận giải một cách có hệ thống những nguyên nhân cốt lõi, trả lời cho câu hỏi mang tính thời sự: ***vì sao việc xây dựng và hoàn thiện pháp luật về dữ liệu là một tất yếu khách quan tại Việt Nam trong giai đoạn hiện nay?***

- Phần thứ tư, mục *"1.4. Quan điểm, mục tiêu và định hướng chính sách xây dựng pháp luật về dữ liệu tại Việt Nam"*. Việc nghiên cứu quan điểm, mục tiêu và định hướng chính sách xây dựng, hoàn thiện pháp luật về

dữ liệu tại Việt Nam là một yêu cầu cấp thiết, bởi nó cung cấp một góc nhìn toàn diện về tầm nhìn chiến lược quốc gia trong kỷ nguyên số. Dữ liệu ngày nay không còn đơn thuần là thông tin mà đã trở thành một tài nguyên quốc gia cốt lõi, là *"máu"* của nền kinh tế số và là nền tảng cho sự phát triển của chính phủ số, xã hội số.

*** Câu 2: Quyền, nghĩa vụ và trách nhiệm của chủ thể dữ liệu, chủ sở hữu dữ liệu, chủ quản dữ liệu? Cơ chế bảo đảm thực hiện các quyền, nghĩa vụ này đối với tổ chức, cá nhân không phải là cơ quan nhà nước?**

Một trong những vấn đề trọng tâm, cốt lõi khi nghiên cứu văn bản Luật chính là *quyền, nghĩa vụ và trách nhiệm* của các chủ thể được luật đề cập đến; vì đây chính là linh hồn và cơ chế vận hành của pháp luật. Nếu không có các yếu tố này, văn bản luật chỉ là những nguyên tắc triết học suông, không có giá trị áp dụng vào đời sống. Câu hỏi số 02 mang ý nghĩa và giá trị thực tiễn sâu sắc, bởi mỗi tổ chức, cá nhân trong xã hội đều có thể trở thành chủ thể dữ liệu, chủ sở hữu dữ liệu hay chủ quản dữ liệu, và bị điều chỉnh bởi Luật Dữ liệu. Nghiên cứu vấn đề này, nhóm tác giả chia thành ba phần chính: ***(1)*** Một số khái niệm có liên quan; ***(2)*** Quyền, nghĩa vụ và trách nhiệm của chủ thể dữ liệu, chủ sở hữu dữ liệu, chủ quản dữ liệu; ***(3)*** Cơ chế bảo đảm thực hiện các quyền, nghĩa vụ trên đối với tổ chức, cá nhân không phải là cơ quan nhà nước.

- Phần thứ nhất, mục *"2.1. Một số khái niệm có liên quan"*, đưa ra *nhận thức chung về dữ liệu, chủ thể dữ liệu, chủ sở hữu dữ liệu và chủ quản dữ liệu.* Qua đó, giúp độc giả hiểu rõ được bản chất của các chủ thể này trước khi phân tích về **quyền, nghĩa vụ và trách nhiệm có liên quan.**

- Phần thứ hai, mục *"2.2. Quyền, nghĩa vụ và trách nhiệm của chủ thể dữ liệu, chủ sở hữu dữ liệu, chủ quản dữ liệu"*, được chia làm 3 tiết từ 2.2.1 đến 2.2.3 phân tích cụ thể, sâu sắc về quyền, nghĩa vụ và trách nhiệm của chủ

thể dữ liệu, chủ sở hữu dữ liệu và chủ quản dữ liệu trên cơ sở nghiên cứu, tổng hợp, hệ thống hóa các quyền, nghĩa vụ và trách nhiệm của các nhóm chủ thể trên đươc quy định tại các Điều, khoản độc lập trong Luật Dữ liệu.

- Phần thứ ba, mục *"2.3. Cơ chế bảo đảm thực hiện các quyền, nghĩa vụ trên đối với tổ chức, cá nhân không phải là cơ quan nhà nước"*. Như đã đề cập ở trên, không phải chỉ tổ chức, cá nhân là cơ quan nhà nước mới tiến hành các hoạt động có liên quan đến dữ liệu. Đối với các chủ thể không phải là cơ quan nhà nước, đôi lúc là những bên yếu thế trong xã hội, đòi hỏi phải có những cơ chế để đảm bảo rằng họ tuân thủ pháp luật, không đứng trên pháp luật và quyền lợi của người dân được bảo vệ một cách công bằng, tạo ra một môi trường kinh doanh, xã hội lành mạnh, dựa trên sự tuân thủ và tôn trọng lẫn nhau.

*** Câu 3: Quy định về hành vi bị nghiêm cấm trong Luật Dữ liệu năm 2024? Giải pháp xây dựng, hoàn thiện quy định pháp luật về xử lý vi phạm hành chính trong lĩnh vực dữ liệu?**

Việc quy định các hành vi bị nghiêm cấm trong Luật Dữ liệu cũng như quy định về xử lý vi phạm hành chính trong lĩnh vực dữ liệu là bắt buộc để tạo ra một *"ranh giới"* rõ ràng, giúp bảo vệ các quyền cơ bản, đảm bảo an ninh quốc gia, và xây dựng một môi trường số an toàn, minh bạch và đáng tin cậy cho tất cả mọi người. Nội dung câu hỏi số 03 gồm bốn phần chính sẽ làm sáng tỏ vấn đề trên, cụ thể:

- Phần thứ nhất, mục *"3.1. Một số hành vi bị nghiêm cấm trong pháp luật về dữ liệu ở một số quốc gia trên thế giới"*. Trước khi nghiên cứu, xây dựng các quy định về hành vi bị nghiêm cấm cho Luật Dữ liệu của Việt Nam, việc tham khảo pháp luật của các quốc gia, khu vực khác, nhất là Liên minh châu Âu, Trung Quốc và Hoa Kỳ, là cực kỳ quan trọng. Điều này không phải để sao chép, mà là để học hỏi, đối chiếu và xây dựng pháp luật vừa phù hợp

với bối cảnh Việt Nam, vừa phù hợp với các tiêu chuẩn chung của thế giới. Nói một cách đơn giản, chúng ta cần nhìn ra thế giới để biết họ đã làm gì đúng, gặp phải sai lầm ở đâu, và xu hướng chung đang đi về đâu, từ đó xây dựng cho mình một con đường tối ưu nhất.

- Phần thứ hai, mục *"3.2. Các hành vi bị nghiêm cấm trong pháp luật về dữ liệu tại Việt Nam"*, đã phân tích sâu sắc, chi tiết nội dung *04 nhóm hành vi bị nghiêm cấm* trong hoạt động dữ liệu trên cơ sở làm rõ 02 câu hỏi chính: ***(1)*** Hành vi này gồm các biểu hiện cụ thể nào? ***(2)*** Vì sao phải nghiêm cấm hoặc mục đích của việc nghiêm cấm hành vi này là gì?

- Phần thứ ba, mục *"3.3. Một số hạn chế, vướng mắc trong quy định của pháp luật về xử lý vi phạm hành chính về dữ liệu tại Việt Nam"*. Trên cơ sở rà soát, phân tích, đánh giá tổng quan, toàn diện các quy định pháp luật hiện hành về xử lý vi phạm hành chính có liên quan đến dữ liệu ở Việt Nam, nhóm tác giả mạnh dạn rút ra một số hạn chế, vướng mắc cần khắc phục trong thời gian tới.

- Phần thứ tư, mục *"3.4. Một số giải pháp hoàn thiện quy định pháp luật về xử lý vi phạm hành chính trong lĩnh vực dữ liệu"*, đã được nhóm tác giả sử dụng để trình bày *07 nhóm giải pháp* cốt lõi cùng với các ví dụ thực tiễn đã được kiểm chứng ở một số quốc gia, khu vực trên thế giới.

Trên đây là tóm tắt nội dung của ***Quyển 1: Pháp luật về dữ liệu - Thế giới và Việt Nam*** trong khuôn khổ Bài dự thi "Tìm hiểu Luật Dữ liệu trong Công an nhân dân". Kính mời quý Ban Giám khảo và quý độc giả cùng chuyển sang phần tiếp theo để đi sâu vào các nội dung chi tiết. Trân trọng./.

Câu 1

Chính sách pháp luật về dữ liệu của các nước trên thế giới? Sự cần thiết, quan điểm, mục tiêu và chính sách xây dựng, hoàn thiện quy định pháp luật về dữ liệu tại Việt Nam?



1.1. CHÍNH SÁCH, PHÁP LUẬT VỀ DỮ LIỆU TRONG CÁC VĂN BẢN PHÁP LUẬT QUỐC TẾ

1.1.1. Công ước Quốc tế về các Quyền Dân sự và Chính trị (International Covenant on Civil and Political Rights - ICCPR) năm 1966

Việt Nam đã ký kết và phê chuẩn tham gia ICCPR vào năm 1982. Đây là một văn bản pháp lý quốc tế ràng buộc trách nhiệm và quy định tất cả các quốc gia thành viên phải tôn trọng, thực hiện để đảm bảo quyền con người. Điều 17 ICCPR là một quy định pháp lý quốc tế cụ thể hóa Điều 12 UDHR (Tuyên ngôn Quốc tế về Nhân quyền năm 1948), đặt nền tảng cho quyền riêng tư cá nhân.

> *"1. Không ai bị can thiệp một cách tuỳ tiện hoặc bất hợp pháp vào đời sống riêng tư, gia đình, nhà ở, thư tín, hoặc bị xâm phạm bất hợp pháp đến danh dự và uy tín.*
>
> *2. Mọi người đều có quyền được pháp luật bảo vệ chống lại những can thiệp hoặc xâm phạm như vậy"*[1]

"Đời sống riêng tư" (privacy) trong ngữ cảnh hiện đại được hiểu là bao gồm quyền kiểm soát thông tin cá nhân của mỗi người. "Sự can thiệp một cách tùy tiện" và "xâm phạm bất hợp pháp" đối với đời sống riêng tư có thể được diễn giải bao gồm việc thu thập, xử lý, lưu trữ hoặc tiết lộ dữ liệu cá nhân mà không có cơ sở pháp lý rõ ràng, không có sự đồng ý của chủ thể dữ liệu (trừ các trường hợp đặc biệt được luật định), hoặc vượt quá mục đích đã định.

---

[1] *Công ước quốc tế về các Quyền dân sự và Chính trị (1966)* (Được thông qua và để ngỏ cho các quốc gia ký, phê chuẩn và gia nhập theo Nghị quyết số 2200 (XXI) ngày 16/12/1966 của Đại hội đồng Liên Hợp Quốc, Có hiệu lực ngày 23/3/1976. https://moj.gov.vn/tttp/tintuc/Lists/CongUocQuocTe/Attachments/10/1.% 20Cong% 20uoc%20 ICCPR%20-%20VN.pdf



Việt Nam đảm bảo thực thi tốt nhất quyền dân sự, chính trị theo Công ước Quốc tế về các Quyền Dân sự và Chính trị năm 1966 - Ảnh: VOV

"Thư tín" (correspondence) đặc biệt liên quan đến quyền riêng tư trong giao tiếp, ngày nay mở rộng sang các hình thức truyền tải thông tin trên không gian mạng như email, tin nhắn, cuộc gọi trực tuyến - nơi dữ liệu truyền tải cần được bảo vệ. Tại Khoản 2 của Điều này đã khẳng định mạnh mẽ rằng các quốc gia phải thiết lập các cơ chế pháp lý để cá nhân có thể tìm kiếm sự bảo vệ chống lại việc lạm dụng dữ liệu của họ. Điều này ngụ ý rằng các quốc gia phải xây dựng luật pháp quốc gia để điều chỉnh việc thu thập và sử dụng dữ liệu cá nhân. Đây là cơ sở cho các quyền của chủ thể dữ liệu (quyền truy cập, sửa đổi, xóa, phản đối) trong các luật bảo vệ dữ liệu hiện đại.

1.1.2. Hướng dẫn của Liên hợp quốc về Hồ sơ dữ liệu trên máy tính (UN Guidelines on Computerized Data Files) (Nghị quyết Đại hội đồng 45/95, ngày 14 tháng 12 năm 1990)

Hướng dẫn của Liên Hợp quốc về Hồ sơ dữ liệu trên máy tính là một trong những văn bản quốc tế đầu tiên cung cấp một bộ nguyên tắc toàn diện

cho việc bảo vệ dữ liệu cá nhân trên môi trường không gian mạng. Mặc dù không mang tính ràng buộc pháp lý, nó đã có ảnh hưởng sâu rộng đến việc hình thành các luật bảo vệ dữ liệu ở nhiều quốc gia, bao gồm các nguyên tắc cốt lõi, như:

(1) Nguyên tắc hợp pháp và công bằng: "Thông tin liên quan đến các cá nhân không được không được sử dụng cho mục đích trái với nguyên tắc của Hiến chương Liên Hợp Quốc", tức là không được thu thập hoặc xử lý một cách không công bằng hoặc trái pháp luật, điều này yêu cầu việc xử lý dữ liệu phải có cơ sở pháp lý và tuân thủ các chuẩn mực đạo đức.

(2) Nguyên tắc chính xác: "Thông tin cá nhân trên thực tế không bao giờ có thể đầy đủ, trong mọi trường hợp, việc cập nhật nên được thực hiện ít nhất mỗi năm một lần". Do đó, những người chịu trách nhiệm thu thập hoặc lưu giữ hồ sơ dữ liệu có nghĩa vụ kiểm tra thường xuyên tính chính xác và mức độ liên quan của dữ liệu đã ghi nhận, đảm bảo rằng dữ liệu được lưu giữ phải phản ánh đầy đủ nhất về sự vật, hiện tượng và được cập nhật thường xuyên, điều này nhấn mạnh tầm quan trọng của chất lượng dữ liệu.

(3) Nguyên tắc xác định mục đích: "Mục đích của việc thu thập thông tin về cá nhân phải được xác định rõ ràng, hợp pháp và được công bố hoặc thông báo cho người có liên quan". Dữ liệu chỉ nên được sử dụng cho mục đích đã nêu và không được giữ lâu hơn mức cần thiết. Bất kỳ việc sử dụng hoặc tiết lộ nào vượt quá mục đích đã chỉ định phải có sự đồng ý của người liên quan (OECD). Đây là nền tảng cho nguyên tắc giới hạn mục đích và giới hạn thời gian lưu trữ dữ liệu;

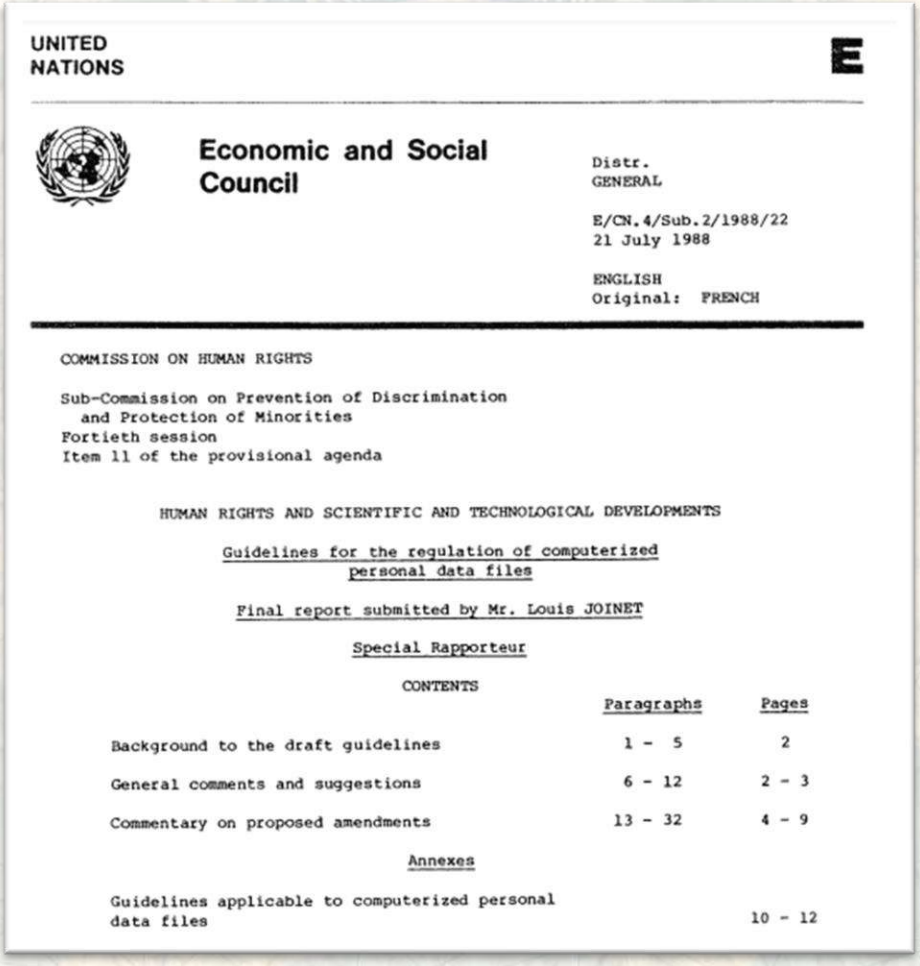
(4) Nguyên tắc tiếp cận của người có liên quan: "Mọi người có quyền biết liệu dữ liệu của mình có được ghi lại hay không và, nếu có, thì dữ liệu đó được ghi lại ở đâu và cho mục đích gì, và được truy cập vào dữ liệu đó

dưới dạng dễ hiểu… Cần có quy định rõ ràng về biện pháp khắc phục trong trường hợp có tranh chấp giữa người chịu trách nhiệm về hồ sơ và người có quyền tiếp cận hồ sơ". Hướng dẫn này cũng yêu cầu các biện pháp khắc phục để điều chỉnh việc tiếp cận dữ liệu bất hợp pháp, không cần thiết hoặc không chính xác. Đây là cơ sở cho quyền truy cập, chỉnh sửa và xóa dữ liệu của chủ thể dữ liệu;

(5) Nguyên tắc không phân biệt đối xử: Cấm thu thập dữ liệu "có khả năng gây ra sự phân biệt đối xử bất hợp pháp hoặc tùy tiện" (như dữ liệu về chủng tộc hoặc nguồn gốc dân tộc, màu da, đời sống tiên tư, quan điểm chính trị, tín ngưỡng tôn giáo, triết học hoặc các tín ngưỡng khác, tư cách thành viên của các hiệp hội hoặc công đoàn). Phân biệt đối xử được hiểu là những hành vi được đề cập tại đoạn I (a) và (b) Điều 1 của Công ước số 111 của Tổ chức Lao động Quốc tế (ILO) về *Phân biệt đối xử trong việc làm và nghề nghiệp* hoặc Điều 1, Đoạn 1 của Công ước UNESCO ngày 14/12/1960 về *Phòng ngừa phân biệt đối xử trong giáo dục*. Các văn kiện này coi bất kỳ "sự phân biệt, loại trừ hoặc ưu đãi... nào có tác dụng vô hiệu hóa hoặc làm suy yếu sự bình đẳng về cơ hội hoặc đối đãi", hoặc hơn nữa, vi phạm nguyên tắc bình đẳng về quyền được quy định tại Điều 2 và Điều 7 của Tuyên ngôn Quốc tế Nhân quyền;

(7) Nguyên tắc về quyền đưa ra ngoại lệ: Nguyên tắc này không phải là một "quyền" theo nghĩa trao quyền cho chủ thể dữ liệu, mà là nguyên tắc cho phép các quốc gia đưa ra các ngoại lệ hoặc giới hạn hợp pháp đối với các nguyên tắc bảo vệ dữ liệu đã nêu trước đó như quyền riêng tư, quyền truy cập dữ liệu. Cơ sở và điều kiện áp dụng ngoại lệ được quy định tại Đoạn 23, theo đó, mọi ngoại lệ đối với quyền riêng tư dữ liệu phải được quy định rõ ràng trong luật pháp quốc gia. Đồng thời, các biện pháp ngoại lệ này phải

đi kèm với các biện pháp bảo vệ phù hợp để giảm thiểu rủi ro lạm dụng hoặc vi phạm quá mức quyền riêng tư, như đã được đề xuất bởi một số quốc gia thành viên (Argentina, Cộng hòa Ả Rập Libya và Rwanda). Việc áp dụng ngoại lệ phải dựa trên cơ sở lợi ích cộng đồng hoặc an ninh quốc gia. Đoạn 24 nêu một số hình thức ngoại lệ đã xảy ra như: Hạn chế quyền tiếp cận đối với hồ sơ liên quan đến hình sự, quốc phòng và an ninh, hồ sơ các bệnh án trên lĩnh vực y tế.... Các quốc gia cần nới lỏng quy định về dữ liệu trên lĩnh vực hoạch định chính sách, nghiên cứu khoa học và thống kê nếu nó cản trở sự phát triển.



UNITED NATIONS

E

Economic and Social Council

Distr.
GENERAL

E/CN.4/Sub.2/1988/22
21 July 1988

ENGLISH
Original: FRENCH

COMMISSION ON HUMAN RIGHTS

Sub-Commission on Prevention of Discrimination
and Protection of Minorities
Fortieth session
Item 11 of the provisional agenda

HUMAN RIGHTS AND SCIENTIFIC AND TECHNOLOGICAL DEVELOPMENTS

Guidelines for the regulation of computerized personal data files

Final report submitted by Mr. Louis JOINET

Special Rapporteur

CONTENTS

	Paragraphs	Pages
Background to the draft guidelines	1 - 5	2
General comments and suggestions	6 - 12	2 - 3
Commentary on proposed amendments	13 - 32	4 - 9
Annexes		
Guidelines applicable to computerized personal data files		10 - 12

Hướng dẫn của Liên hợp quốc về Hồ sơ dữ liệu trên máy tính (UN Guidelines on Computerized Data Files) - Ảnh: Liên hợp quốc

(8) Nguyên tắc về bảo mật: Nguyên tắc này yêu cầu các biện pháp thích hợp để bảo vệ dữ liệu không chỉ khỏi các mối nguy hiểm tự nhiên (ví dụ: mất mát do tai nạn, hỏa hoạn, lũ lụt, phá hủy không mong muốn) mà còn chống lại các mối nguy hiểm do con người gây ra (Đoạn 26). Ngoài ra, quy định này còn đề cập các mối nguy hiểm khác do con người gây ra như các hành vi cố ý phá hoại, gây rối, làm hỏng dữ liệu hoặc truy cập trái phép bao gồm cả việc xâm nhập từ bên ngoài và việc lạm dụng quyền truy cập từ bên trong. Mục tiêu của nguyên tắc này là đảm bảo tính toàn vẹn, khả dụng và bảo mật của dữ liệu. Nó đòi hỏi các tổ chức và chính phủ phải áp dụng các biện pháp kỹ thuật và tổ chức phù hợp để bảo vệ dữ liệu cá nhân trong toàn bộ vòng đời của nó - từ khi thu thập, xử lý, lưu trữ cho đến khi hủy bỏ.

Ngoài ra, Hướng dẫn còn quy định *cơ chế Giám sát và chế tài* (Supervision and sanctions), yêu cầu chỉ định một cơ quan "chịu trách nhiệm giám sát việc tuân thủ các nguyên tắc đã nêu" và áp dụng "các biện pháp trừng phạt thích hợp" và *Luồng dữ liệu xuyên biên giới* (Transborder data flows) cho phép dữ liệu lưu thông tự do giữa các quốc gia khi các quốc gia đó có *"các biện pháp bảo vệ quyền riêng tư tương đương"*. Điều này đặt ra nền tảng cho các quy định về chuyển dữ liệu xuyên biên giới.

1.1.3. Một số văn bản của Ủy ban Liên Hợp Quốc về Luật Thương mại Quốc tế (UNCITRAL)

Trong bối cảnh xây dựng pháp luật về dữ liệu, vai trò của UNCITRAL chủ yếu nằm ở việc xây dựng một khuôn khổ pháp lý thuận lợi cho thương mại điện tử và các giao dịch kỹ thuật số, qua đó gián tiếp ảnh hưởng đến việc xử lý và bảo vệ dữ liệu. Các văn bản của UNCITRAL, dù không trực tiếp là luật bảo vệ dữ liệu cá nhân như ICCPR hay các nguyên tắc của UN Guidelines,

nhưng lại tập trung vào việc hài hòa hóa các quan hệ pháp luật thương mại quốc tế để tạo điều kiện thuận lợi cho các giao dịch xuyên biên giới.



Việt Nam là một thành viên của UNCITRAL - Ảnh: TTXVN

Một ví dụ điển hình là Luật mẫu của UNCITRAL về Thương mại điện tử năm 1996. Cụ thể, Điều 5 của Luật mẫu này khẳng định sự công nhận về mặt pháp lý của thông điệp dữ liệu, quy định rằng thông tin không bị từ chối hiệu lực pháp lý, giá trị hoặc khả năng thi hành chỉ vì nó tồn tại ở dạng thông điệp dữ liệu, nó có giá trị pháp lý tương đương với văn bản viết, nếu đáp ứng các yêu cầu nhất định, có thể được sử dụng để hình thành, thực hiện và chứng minh hợp đồng. Quy định này là nền tảng cho việc hợp pháp hóa các giao dịch và lưu trữ dữ liệu điện tử, từ đó tạo tiền đề cho sự cần thiết của các quy định về an toàn và bảo mật dữ liệu trong môi trường thương mại điện tử.

Tương tự, Luật Mẫu của UNCITRAL về Chữ ký điện tử năm 2001 cũng có liên quan mật thiết. Điều 6 quy định về sự tin cậy vào chữ ký điện tử, thiết lập các tiêu chí để xác định tính hợp lệ và tin cậy của chữ ký điện tử. Việc công nhận chữ ký điện tử và các phương tiện xác thực điện tử khác đòi hỏi các tiêu chuẩn cao về bảo mật và tính toàn vẹn của dữ liệu liên quan đến danh tính và ý chí của người ký. Điều này ngụ ý sự cần thiết phải bảo vệ dữ liệu định danh và các dữ liệu liên quan khác để đảm bảo tính hợp pháp và không thể chối bỏ của các giao dịch điện tử.

Ngoài ra, UNCITRAL cũng đã phát triển các văn bản khác nhằm hỗ trợ sự phát triển của kinh tế số. Các văn bản này bao gồm Công ước Liên Hợp Quốc về Sử dụng Truyền thông Điện tử trong Hợp đồng Quốc tế (2005), cung cấp khung pháp lý vững chắc cho việc ký kết hợp đồng điện tử trong thương mại quốc tế. Luật mẫu về Hồ sơ có thể chuyển nhượng điện tử (2017) áp dụng các nguyên tắc tương tự để cho phép sử dụng các tài liệu và công cụ có thể chuyển nhượng dưới dạng điện tử. Gần đây hơn, Luật mẫu về Quản lý danh tính và Dịch vụ tin cậy (2022) cung cấp khuôn khổ pháp lý thống nhất toàn cầu để xác định các cá nhân và pháp nhân trong các giao dịch điện tử, và Luật mẫu về Hợp đồng tự động (2024) bổ sung các văn bản trước đó bằng cách cung cấp cơ sở pháp lý cho việc ký kết hợp đồng điện tử sử dụng các hệ thống tự động, bao gồm cả trí tuệ nhân tạo. UNCITRAL cũng đã phê duyệt công bố một phân loại các vấn đề pháp lý liên quan đến kinh tế số, bao gồm trí tuệ nhân tạo, dữ liệu, nền tảng trực tuyến, tài sản kỹ thuật số và hệ thống phi tập trung, nhằm định hướng các đề xuất cho công việc trong tương lai[2].

[2] United Nations Commission on International Trade Law, *Electronic Commerce,* https://uncitral.un.org/en/texts/ecommerce, truy cập ngày 15/07/2025.

Như vậy, các văn bản của UNCITRAL tạo ra một môi trường pháp lý cho phép dữ liệu được trao đổi và lưu trữ một cách hợp pháp. Mặc dù trọng tâm không phải là quyền riêng tư, nhưng để đảm bảo tính hợp lệ và an toàn của các giao dịch thương mại, các nguyên tắc về tính toàn vẹn của dữ liệu, tính xác thực của thông điệp dữ liệu và khả năng xác định danh tính trong môi trường điện tử trở nên vô cùng quan trọng. UNCITRAL gián tiếp thúc đẩy việc phát triển các tiêu chuẩn về kỹ thuật và pháp lý nhằm đảm bảo rằng dữ liệu được xử lý một cách an toàn và đáng tin cậy trong các hoạt động thương mại quốc tế trên không gian mạng.

1.1.4. Công ước về Quyền Trẻ em (Convention on the Rights of the Child - CRC) năm 1989

Công ước về Quyền Trẻ em (CRC) là công ước nhân quyền được phê chuẩn rộng rãi nhất trong lịch sử. Được thông qua vào năm 1989, nó đặt ra một ý tưởng sâu sắc: trẻ em không chỉ là đối tượng thuộc về cha mẹ mà là những con người với các quyền riêng biệt. CRC bảo vệ và thực hiện các quyền của trẻ em, đảm bảo rằng tuổi thơ là một thời gian đặc biệt, được bảo vệ để trẻ em có thể lớn lên, học hỏi, vui chơi, phát triển và phát triển với phẩm giá. Mặc dù được thông qua trước khi môi trường kỹ thuật số phổ biến, các điều khoản của nó vẫn cung cấp một khuôn khổ pháp luật mạnh mẽ để bảo vệ quyền của trẻ em trong thế giới trực tuyến.

Về cơ sở pháp lý có liên quan đến dữ liệu của trẻ em, mặc dù CRC không đề cập trực tiếp đến thuật ngữ "môi trường kỹ thuật số" hay "dữ liệu cá nhân", nhiều điều khoản của Công ước đã đặt nền tảng quan trọng cho việc bảo vệ trẻ em trong không gian số hiện nay. Điển hình, tại *Điều 16 (Quyền riêng tư)*, Công ước quy định rằng *"Không trẻ em nào phải chịu sự can thiệp tùy tiện hoặc bất hợp pháp vào đời tư, gia đình, nhà ở hoặc thư*

tín… và trẻ em có quyền được pháp luật bảo vệ chống lại những sự can thiệp đó". Điều khoản này có thể được hiểu là cơ sở pháp lý rõ ràng để bảo vệ dữ liệu cá nhân, quyền riêng tư trong liên lạc trực tuyến, hồ sơ học tập, thông tin định danh và hình ảnh của trẻ em trên không gian mạng. Trách nhiệm bảo vệ này không chỉ đặt ra đối với nhà nước, mà còn mở rộng tới các nền tảng công nghệ, nhà phát triển ứng dụng, tổ chức giáo dục - những chủ thể có khả năng thu thập và xử lý dữ liệu trẻ em.

Bên cạnh đó, tại *Điều 13 (Quyền tự do ngôn luận và tiếp cận thông tin)*, quyền này bao gồm cả quyền tìm kiếm, tiếp nhận và truyền đạt thông tin "bằng bất kỳ phương tiện truyền thông nào", từ đó bao hàm cả môi trường kỹ thuật số. Trẻ em có quyền sử dụng Internet, mạng xã hội, ứng dụng học tập và các nền tảng trực tuyến để học hỏi, chia sẻ và phát triển cá nhân. Tuy nhiên, quyền này có thể được giới hạn theo các nguyên tắc cần thiết và hợp lý nhằm bảo vệ danh dự người khác, an ninh, đạo đức và trật tự công cộng - đặt ra yêu cầu cân bằng giữa tự do biểu đạt và trách nhiệm bảo vệ.

Tại *Điều 17 - Quyền tiếp cận thông tin phù hợp:* Công ước nhấn mạnh vai trò của các phương tiện thông tin trong việc thúc đẩy phúc lợi toàn diện cho trẻ em, đồng thời yêu cầu các quốc gia ban hành hướng dẫn và biện pháp bảo vệ trẻ khỏi nội dung độc hại. Trong môi trường kỹ thuật số, điều này đồng nghĩa với trách nhiệm thiết lập bộ lọc nội dung, công cụ kiểm soát cha mẹ, quy định phân loại độ tuổi và giáo dục truyền thông số để bảo vệ trẻ khỏi thông tin sai lệch, khiêu dâm, bạo lực hoặc mang tính cực đoan.

Về nghĩa vụ mở rộng về bảo vệ trẻ em khỏi các nguy cơ dữ liệu và không gian mạng, CRC còn đưa ra những nghĩa vụ rộng hơn về bảo vệ trẻ em khỏi các hình thức xâm hại, bóc lột và tổn thương - mà trong thời đại số có thể diễn ra dưới nhiều hình thức tinh vi. *Điều 19 - Bảo vệ khỏi bạo lực và*

lạm dụng: Bao gồm cả các hành vi bắt nạt qua mạng (cyberbullying), dụ dỗ trực tuyến (online grooming), truyền bá nội dung tự sát hoặc gây hại. Quốc gia phải có các công cụ pháp luật, kỹ thuật và giáo dục để ngăn ngừa và can thiệp hiệu quả. *Điều 32 - Bóc lột kinh tế:* Áp dụng để chống lại việc trẻ em bị sử dụng lao động trá hình trong các hoạt động số, như livestream, sản xuất nội dung mạng xã hội, chơi game kiếm tiền không kiểm soát, gây tổn hại cho sự phát triển lành mạnh của trẻ. *Điều 33 đến 36 - Phòng chống ma túy, lạm dụng tình dục, buôn người và bóc lột khác:* Những điều khoản này cung cấp cơ sở để xử lý các hành vi lạm dụng trẻ em trên môi trường mạng, như phát tán tài liệu lạm dụng tình dục trẻ em (CSAM), dụ dỗ mại dâm qua Internet, hay buôn bán trẻ em qua nền tảng số. Các nghĩa vụ nói trên khẳng định rõ ràng trách nhiệm của nhà nước trong việc điều chỉnh các hành vi xâm hại trẻ em trên môi trường số bằng biện pháp pháp lý (luật dữ liệu cá nhân, luật an ninh mạng, luật trẻ em), biện pháp tổ chức (thiết lập cơ quan giám sát, đường dây nóng, hệ thống lọc nội dung) và biện pháp giáo dục (nâng cao năng lực số của trẻ và phụ huynh).



Công ước Liên hợp quốc về quyền trẻ em - Ảnh: Liên hợp quốc

CRC còn khẳng định mạnh mẽ *"Trách nhiệm kép"* - vừa bảo vệ, vừa trao quyền của Nhà nước. Điểm đặc trưng của CRC là không chỉ bảo vệ trẻ em khỏi rủi ro, mà còn thúc đẩy khả năng tiếp cận và tham gia môi trường số một cách chủ động và tích cực. Điều này tạo ra trách nhiệm kép cho nhà nước và các chủ thể liên quan: vừa thiết lập rào chắn bảo vệ hiệu quả, vừa không tước đoạt quyền tự do biểu đạt, học tập, sáng tạo và tương tác xã hội của trẻ em. Thách thức nằm ở chỗ cần một cách tiếp cận cân bằng và lấy trẻ em làm trung tâm, ví dụ như xây dựng giao diện thân thiện với trẻ, thiết kế ứng dụng theo nguyên tắc quyền riêng tư theo mặc định (privacy by default), cơ chế kiểm soát độ tuổi tinh vi, và các quy định nghiêm ngặt về sự đồng ý (consent) - đặc biệt khi xử lý dữ liệu cá nhân của trẻ em cho mục đích quảng cáo, phân tích hành vi hoặc phát triển sản phẩm.

Không chỉ vậy, Một nguyên tắc xuyên suốt CRC là *"vì lợi ích tốt nhất của trẻ em"* (best interests of the child) - nguyên tắc này có ý nghĩa then chốt trong quá trình xây dựng và thực thi pháp luật dữ liệu cá nhân. Theo đó, mọi chính sách, quy định và hoạt động xử lý dữ liệu liên quan đến trẻ em phải ưu tiên tối đa phúc lợi, quyền và sự phát triển toàn diện của trẻ. Điều này đặt ra yêu cầu: ***(i)*** Thiết lập mức độ bảo vệ pháp lý cao hơn cho dữ liệu của trẻ em so với người lớn; ***(ii)*** Giới hạn việc sử dụng dữ liệu trẻ em cho mục đích thương mại, đặc biệt trong quảng cáo nhắm mục tiêu hoặc hồ sơ hóa hành vi người dùng; ***(iii)*** Bắt buộc sự đồng ý rõ ràng, có hiểu biết, không chỉ từ cha mẹ mà cần tính đến mức độ trưởng thành của trẻ; ***(iv)*** Áp dụng các nguyên tắc thiết kế phù hợp với trẻ em trong mọi nền tảng số mà trẻ có thể truy cập ("privacy by design", "safety by design").

Như vậy, CRC không chỉ là văn bản nhân quyền có tính nền tảng mà còn là cơ sở pháp lý và đạo lý vững chắc để các quốc gia, trong đó có Việt

Nam, xây dựng, hoàn thiện hệ thống pháp luật về dữ liệu, đặc biệt là trong việc thiết kế chính sách, pháp luật bảo vệ dữ liệu cá nhân của trẻ em trong kỷ nguyên số.



Ảnh: Báo Tin tức

1.2. CHÍNH SÁCH, PHÁP LUẬT VỀ DỮ LIỆU TẠI MỘT SỐ QUỐC GIA, KHU VỰC TRÊN THẾ GIỚI

Trong nhiều thập kỷ qua, dữ liệu đã và đang trở thành một yếu tố quan trọng trong mọi lĩnh vực của nền kinh tế toàn cầu. Từ ngành công nghiệp, dịch vụ tài chính đến y tế, giáo dục, dữ liệu không chỉ là một công cụ giúp các cơ quan, tổ chức và doanh nghiệp hoạt động hiệu quả hơn, mà còn đóng vai trò là tài sản chiến lược của xã hội. Việc thu thập, phân tích và sử dụng dữ liệu giúp các công ty cải thiện sản phẩm, tối ưu hóa quy trình và đáp ứng nhu cầu của khách hàng một cách cá nhân hóa và chính xác hơn.

Bên cạnh đó, sự phát triển của các công nghệ như trí tuệ nhân tạo (AI), học máy (machine learning), dữ liệu lớn (big data) và Internet of Things (IoT) đã đưa dữ liệu trở thành nguồn tài nguyên vô giá. Các nền tảng trực tuyến như Google, Facebook, Twitter (X), Instagram và các công ty công nghệ khác đang thu thập lượng dữ liệu khổng lồ mỗi ngày từ hành vi của người dùng. Điều này không chỉ tạo ra lợi nhuận khổng lồ mà còn làm tăng mức độ phụ thuộc của các quốc gia vào dữ liệu như một yếu tố cấu thành trong sự phát triển kinh tế và an ninh quốc gia.

Hiện nay, nhiều nước phát triển trên thế giới đã xây dựng các trung tâm dữ liệu tập trung và các hệ thống cơ sở dữ liệu quốc gia nhằm phát huy triệt để vai trò, giá trị của nguồn tài nguyên dữ liệu trong phục vụ quản trị quốc gia và phát triển kinh tế xã - hội; bảo đảm an ninh - quốc phòng. Hoạt động này đã trở thành xu thế tất yếu trên thế giới và nhiều nước coi đây là nội dung trọng tâm trong xây dựng chính phủ điện tử, phát triển nền kinh tế số, qua đó từng bước tạo dựng và xác lập vị trí quốc gia trên bản đồ công nghệ toàn cầu.



Ảnh minh họa - Ảnh: Internet

Tại Châu Á, một số nước đã tập trung xây dựng trung tâm dữ liệu quốc gia để tạo nền tảng đẩy mạnh chuyển đổi số và đã đạt được những thành tựu quan trọng, như: Hàn Quốc, Nhật Bản, Singapore, Thái Lan, Ấn Độ, Trung Quốc… Để hoàn thành việc xây dựng, vận hành hiệu quả các trung tâm dữ liệu quốc gia cần bảo đảm những điều kiện như: Hoàn thiện quy định pháp luật về dữ liệu; Xây dựng trung tâm dữ liệu quốc gia quy mô lớn với nhiều trung tâm dễ quản lý tập trung, chia sẻ dữ liệu; Có tổ chức độc lập để xây dựng, vận hành, quản lý trung tâm dữ liệu quốc gia; Ban hành các tiêu chuẩn, quy chuẩn chung đối với quản lý, lưu trữ, khai thác dữ liệu; Có nguồn nhân lực chất lượng cao và chính sách đặc thù đãi ngộ phù hợp…

Có nhiều yếu tố ảnh hưởng đến chính sách dữ liệu trên thế giới như:

(1) Yếu tố văn hóa và xã hội: Mỗi quốc gia có một nền văn hóa và giá trị xã hội khác nhau, điều này ảnh hưởng đến cách họ nhìn nhận và đánh giá sự bảo vệ quyền riêng tư và bảo mật dữ liệu. Ví dụ, ở các quốc gia phương Tây, đặc biệt là ở Châu Âu, quyền riêng tư và dữ liệu cá nhân được coi trọng hơn, trong khi ở một số quốc gia khác, nhu cầu bảo vệ an ninh quốc gia có thể đặt lên hàng đầu. Điều này dẫn đến sự khác biệt trong các chính sách và quy định pháp luật về dữ liệu.

(2) Yếu tố kinh tế: Mức độ phát triển kinh tế ở mỗi quốc gia có thể ảnh hưởng đến khả năng đầu tư và triển khai các chính sách dữ liệu. Các quốc gia phát triển thường có điều kiện để xây dựng các hệ thống bảo mật mạnh mẽ và có đủ nguồn nhân lực để quản lý dữ liệu lớn và thực thi các luật bảo vệ quyền riêng tư. Trong khi đó, các quốc gia đang phát triển có thể thiếu nguồn lực để triển khai các biện pháp bảo vệ dữ liệu hiệu quả.

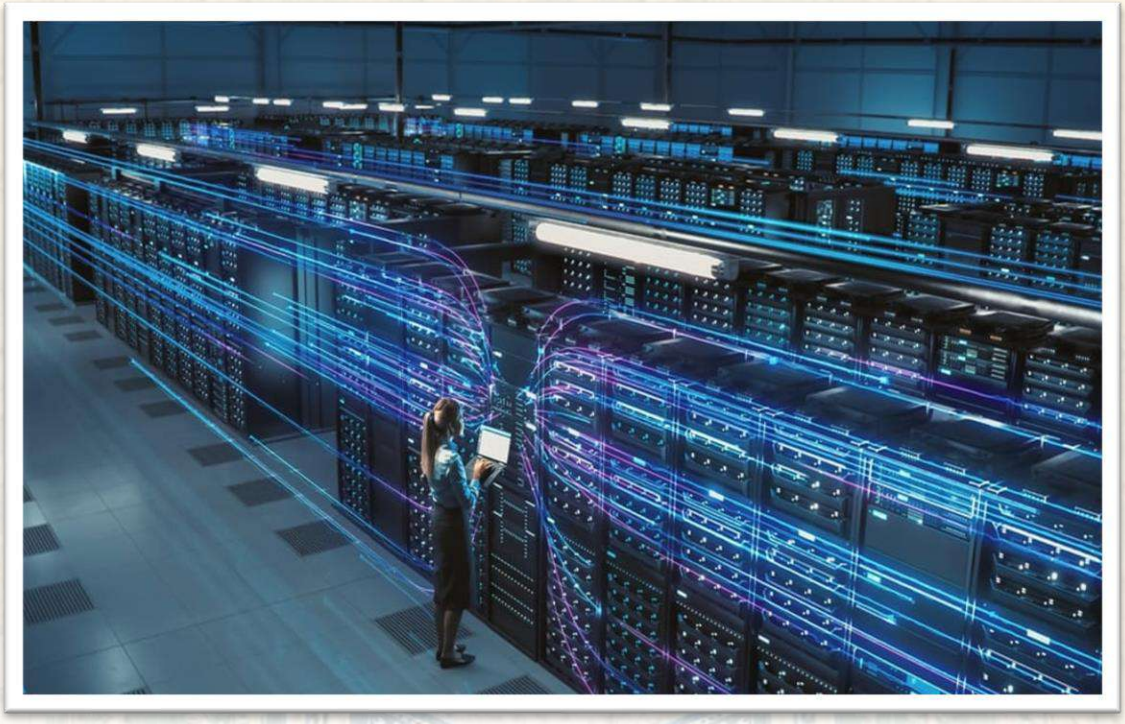
(3) Yếu tố chính trị: Chính trị quốc gia cũng ảnh hưởng đến việc xây dựng các chính sách về dữ liệu. Trong một số quốc gia, các chính phủ có thể muốn thu thập và giám sát dữ liệu để phục vụ mục đích an ninh quốc gia, trong khi các quốc gia khác lại đặc quyền tự do cá nhân lên hàng đầu. Chính trị quốc gia và các lợi ích chính trị có thể gây ảnh hưởng lớn đến các quy định và chính sách dữ liệu.

(4) Áp lực từ cách tổ chức quốc tế: Các tổ chức quốc tế như Liên hợp Quốc, OECD và EU, đặc biệt là thông qua GDPR, DGA đã đặt ra một tiêu chuẩn toàn cầu và dữ liệu. Các quốc gia khác thường xuyên bị áp lực phải thay đổi các quy định của mình để đáp ứng với các yêu cầu quốc tế, đặc biệt là khi họ tham gia vào các hiệp định thương mại quốc tế.

(5) Sự phát triển của công nghệ: Công nghệ không ngừng phát triển, đặc biệt là với sự ra đời của các công nghệ mới như AI, blockchain và các hệ thống dữ liệu phân tán. Những công nghệ này không chỉ giúp xử lý dữ liệu hiệu quả hơn mà còn mở ra những vấn đề pháp lý mới về dữ liệu và quyền riêng tư. Ví dụ, sự xuất hiện của AI và các hệ thống học máy khiến việc phân tích dữ liệu cá nhân trở nên mạnh mẽ hơn nhưng cũng đồng thời tạo ra các vấn đề liên quan đến việc sử dụng và lưu trữ dữ liệu cá nhân mà chưa có khung pháp lý rõ ràng.

Trung tâm dữ liệu siêu quy mô (hyperscale data center) ngày nay dã trở thành nền tảng không thể thiếu trong kỷ nguyên số hóa toàn cầu. Đây là những tổ hợp hạ tầng công nghệ cực lớn, nơi tập trung hàng chục nghìn đến hàng trăm nghìn máy chủ cùng hệ thống lưu trữ, thiết bị mạng và các hệ thống hỗ trợ, như điện, làm mát, bảo mật vật lý, kiểm soát cháy nổ và an ninh thông tin ở cấp độ cao nhất. Các trung tâm này vận hành liên tục 24/7, đáp ứng các yêu cầu khắt khe về độ tin cậy, an toàn và khả năng mở rộng

cho những nhu cầu xử lý, lưu trữ và truyền tải dữ liệu khổng lồ trong bối cảnh chuyển đổi số đang diễn ra mạnh mẽ ở mọi lĩnh vực.



Ảnh minh họa hyperscale data center - Ảnh: Internet

Vai trò của các trung tâm dữ liệu siêu quy mô vô cùng to lớn đối với nền kinh tế, an ninh quốc gia và đời sống xã hội. Chúng là nền tảng vận hành cho các dịch vụ điện toán đám mây, trí tuệ nhân tạo, phân tích dữ liệu lớn, thương mại điện tử, mạng xã hội, các hệ thống giao dịch tài chính, dịch vụ y tế từ xa và nhiều dịch vụ hiện đại khác. Sự phát triển và vận hành ổn định của các tập đoàn công nghệ hàng đầu như: Google, Facebook, Amazon, Microsoft Azure, Apple, Alibaba, Tencent, Netflix… đều dựa trên hệ sinh thái trung tâm dữ liệu siêu quy mô. Đặc biệt, trong bối cảnh an ninh mạng và chủ quyền dữ liệu ngày càng được coi trọng, các trung tâm dữ liệu này còn đóng vai trò dự phòng, bảo đảm an toàn thông tin cho Chính phủ, quốc phòng và các ngành kinh tế chiến lược của mỗi quốc gia.



Trung tâm dữ liệu dưới biển của Microsoft - Ảnh: Microsoft

Trên bình diện toàn cầu, số lượng các trung tâm dữ liệu siêu quy mô đã bùng nổ trong khoảng một thập kỷ trở lại đây. Theo số liệu của các tổ chức nghiên cứu uy tín như synergy research group và Statista, đến năm 2024, thế giới đã ghi nhận gần 900 trung tâm dữ liệu siêu quy mô, so với chỉ khoảng 300 trung tâm vào năm 2015. Sự phân bố các trung tâm này không đồng đều mà tập trung chủ yếu tại các quốc gia phát triển, nơi có chính sách hỗ trợ về đất đai, nguồn điện, công nghệ và an ninh. Hoa Kỳ hiện vẫn là quốc gia dẫn đầu thế giới về số lượng trung tâm dữ liệu siêu quy mô, chiếm hơn một nửa tổng số trung tâm trên toàn cầu. Các trung tâm dữ liệu lớn của Mỹ thường được đặt ở các bang như Nevada, Iowa, Oregon, North Carolina và Illinois nhờ ưu thế về chi phí, khí hậu và điều kiện vận hành thuận lợi. Các tập đoàn công nghệ như Amazon, Microsoft Azure, Google Cloud, Web Service, Meta, Switch và Apple liên tục đầu tư mở rộng hệ thống trung tâm dữ liệu để phục vụ nhu cầu tăng trưởng khổng lồ về lưu trữ và xử lý dữ liệu. Trung Quốc nổi lên là thị trường lớn thứ hai với tốc độ tăng trưởng cực nhanh nhờ

các trung tâm dữ liệu khổng lồ của China Telecom, Alibaba, Tencent và Baidu, chủ yếu đặt tại Nội Mông, Quảng Đông, Quý Châu, Bắc Kinh và Thượng Hải. Tận dụng lợi thế về nguồn điện giá rẻ và năng lượng sạch, Châu Âu cũng là khu vực phát triển mạnh với các trung tâm dữ liệu, với điểm nóng như Anh, Đức, Hà Lan và Ireland, nơi có thị trường dịch vụ tài chính lớn và hạ tầng số phát triển. Ngoài ra, ở nhiều quốc gia khác tại Châu Á như Ấn Độ, Singapore, Nhật Bản, Úc cũng đang đầu tư mạnh vào hạ tầng dữ liệu quy mô lớn để đáp ứng nhu cầu trong khu vực.

Sự xuất hiện của các trung tâm dữ liệu siêu quy mô không chỉ là kết quả của quá trình chuyển đổi số mà còn là chiến lược cạnh tranh dài hạn của các tập đoàn công nghệ lớn. Họ phát triển các trung tâm này nhằm đáp ứng nhu cầu tăng trưởng dữ liệu vượt bậc, giảm độ trễ khi truyền tải dữ liệu, nâng cao hiệu quả vận hành, giảm chi phí và đặc biệt là bảo đảm dự phòng, an ninh thông tin và chủ quyền dữ liệu của từng khu vực, quốc gia.

Nếu xét về quy mô cụ thể, China Telecom Data Center đặt tại Nội Mông, Trung Quốc hiện được xem là trung tâm dữ liệu lớn nhất thế giới với diện tích trên 1,3 triệu m^2. Trung tâm này sử dụng hàng trăm mW điện, tập trung xử lý và lưu trữ dữ liệu cho hàng loạt doanh nghiệp lớn và các dự án quốc gia của Trung Quốc. Địa điểm này cũng tận dụng tối đa nguồn điện giá rẻ từ thủy điện và điện gió ở Nội Mông, đồng thời được bảo vệ nghiêm ngặt về cả vật lý lẫn an ninh mạng theo các tiêu chuẩn quốc tế. Tại Mỹ, The Citadel Campus ở Nevada thuộc sở hữu của Switch có quy mô lên đến 1,2 triệu m^2, đây là trung tâm dữ liệu tư nhân lớn nhất Bắc Mỹ, được ví như là một *"pháo đài dữ liệu"* với nhiều lớp bảo vệ vật lý, hệ thống kiểm soát ra vào tự động, camera AI giám sát liên tục 24/7. The Citadel Campus cung cấp dịch vụ cho nhiều khách hàng, đồng thời được thiết kế theo mô hình *"campus"* giúp mở rộng dễ dàng trong tương lai mà không ảnh hưởng đến

hoạt động hiện tại. Một số trung tâm dữ liệu khác cũng rất nổi tiếng như Range International Information Group Data Center tại Bắc Kinh với diện tích khoảng 600.000 m^2; Lakeside Technology Center tại Chicago do Digital Realty quản lý với hơn 100.000 m^2, Tulip Data City ở Mumbai (Ấn Độ) là trung tâm dữ liệu lớn nhất Nam Á với diện tích 84.000 m^2 hay các trung tâm dữ liệu của Meta (Facebook), Google và Microsoft đặt tại Mỹ, mỗi trung tâm đều có diện tích từ hàng trăm nghìn mét vuông vận hành hàng trăm nghìn máy chủ và phục vụ cho các dịch vụ công nghệ toàn cầu.

Về mặt công nghệ, các trung tâm dữ liệu siêu quy mô luôn là nơi áp dụng những tiến bộ mới nhất, hiệu suất sử dụng năng lượng được tối ưu hoá bằng các giải pháp làm mát tiên tiến như làm mát bằng nước, khí tự nhiên hoặc thậm chí là công nghệ cooling bằng chất lỏng (liquid cooling). Nhiều trung tâm còn tái sử dụng nhiệt thải để phục vụ các dự án dân sinh hoặc các đô thị lân cận, góp phần tiết kiệm năng lượng và bảo vệ môi trường. Mặt khác, yếu tố bảo mật luôn được đặt lên hàng đầu với các lớp bảo vệ vật lý nghiêm ngặt, ứng dụng sinh trắc học, camera AI, hệ thống kiểm soát ra vào tự động và đội ngũ an ninh trực chiến 24/7. Bên cạnh đó, các khâu vận hành, giám sát sự cố và tối ưu tài nguyên được tự động hóa bởi các hệ thống trí tuệ nhân tạo, giúp giảm thiểu nhu cầu nhân lực trực tiếp, tăng tính chính xác và khả năng dự báo, phòng ngừa sự cố. Đáng chú ý, nhiều trung tâm dữ liệu siêu quy mô để đạt các tiêu chuẩn xanh, đã cam kết sử dụng hoàn toàn năng lượng tái tạo như điện gió, điện mặt trời nhằm giảm phát khí thải nhà kính và hướng tới phát triển bền vững trong dài hạn. Khả năng mở rộng cũng là một yếu tố quan trọng khi các trung tâm này thường được thiết kế dạng *"modular"* dễ dàng bổ sung thêm các khối trung tâm mới mà không phải làm gián đoạn hoạt động chung.



China Telecom Data Center tại Nội Mông là một trong những trung tâm dữ liệu lớn nhất trên thế giới thời điểm hiện tại - Ảnh: Total Telecom

Tuy nhiên, sự phát triển của các trung tâm dữ liệu siêu quy mô cũng kéo theo không ít thách thức. Điển hình nhất là các vấn đề tiêu thụ điện năng cực lớn có thể gây áp lực lên lưới điện địa phương và đòi hỏi nguồn năng lượng sạch để đảm bảo vận hành ổn định, thân thiện với môi trường. Ngoài ra, chi phí đầu tư ban đầu vô cùng lớn yêu cầu dòng vốn cực mạnh và công nghệ hiện đại hàng đầu thế giới. Bảo đảm an ninh thông tin, phòng chống tấn công mạng ngày càng tinh vi cũng là một vấn đề được các quốc gia đặc biệt quan tâm.

Bên cạnh các thách thức, các trung tâm dữ liệu siêu quy mô lại mang đến nhiều tác động tích cực cho nền kinh tế - xã hội. Chúng góp phần thúc đẩy phát triển kinh tế số, tạo ra hàng nghìn việc làm trực tiếp và gián tiếp, thu hút các dòng vốn đầu tư công nghệ cao. Sự phát triển của các trung tâm này cũng tạo động lực cho ngành năng lượng tái tạo, xây dựng hạ tầng viễn thông, logistics, đồng thời nâng cao năng lực quản lý, xử lý và phân

tích dữ liệu ở tầm quốc gia. Ngoài ra, các trung tâm này là bệ phóng quan trọng cho sự phát triển của các lĩnh vực mới như trí tuệ nhân tạo, Internet vạn vật, dịch vụ đám mây, fintech, Chính phủ điện tử và các thành phố thông minh.



Con người đang phải cạnh tranh trực tiếp với công nghệ - Ảnh: Internet

Nhìn chung, các trung tâm dữ liệu siêu quy mô chính là biểu tượng cho cuộc đua toàn cầu về công nghệ và hạ tầng số, là minh chứng cho việc dữ liệu đã trở thành nguồn tài nguyên chiến lược quan trọng bậc nhất trong thế kỷ XXI. Sự phát triển mạnh mẽ và bền vững của các trung tâm này không chỉ bảo đảm cho các doanh nghiệp công nghệ giữ vững vị thế cạnh tranh mà còn giúp mỗi quốc gia nâng cao năng lực bảo đảm an ninh mạng chủ quyền số và thúc đẩy đổi mới sáng tạo, phát triển kinh tế - xã hội một cách toàn diện. Đồng thời, với việc xây dựng và phát triển các trung tâm dữ liệu, nhiều nước trên thế giới đã có quy định pháp luật về dữ liệu (dữ liệu của cơ quan nhà nước, của tổ chức, doanh nghiệp và cá nhân), vận hành, khai thác sử dụng, dữ liệu và bảo vệ dữ liệu cá nhân. Cụ thể như sau:

1.2.1. Liên minh châu Âu

1.2.1.1. Quy định Bảo vệ Dữ liệu Chung (GDPR) và Đạo Luật dữ liệu Châu Âu (EU Data Act)

Liên minh châu Âu (EU) là một trong những khu vực tiên phong và có ảnh hưởng sâu rộng nhất trong lĩnh vực xây dựng khung pháp lý về bảo vệ dữ liệu tổ chức, doanh nghiệp và cá nhân. Với việc ban hành *"Quy định chung về bảo vệ dữ liệu"*, GDPR chính thức có hiệu lực từ ngày 25/5/2018, EU đã thiết lập một mô hình pháp lý toàn diện và thống nhất, được quốc tế ghi nhận như *"tiêu chuẩn vàng"*[3] trong bảo vệ quyền riêng tư và quản trị dữ liệu.

Cùng với sự phát triển của nền kinh tế dữ liệu, đến ngày 13/11/2024, Đạo Luật Dữ liệu châu Âu (EU Data Act) chính thức được Nghị viện và Hội đồng châu Âu thông qua và ban hành, với có hiệu lực vào ngày 11/01/2024 với những quy định mới về dữ liệu số so với GDPR (chỉ tập trung vào bảo vệ dữ liệu cá nhân) nhằm phát triển sức mạnh nền kinh tế dữ liệu của châu Âu và thúc đẩy sự cạnh tranh trong thị trường dữ liệu bằng cách giúp dữ liệu (đặc biệt là dữ liệu công nghiệp) dễ tiếp cận và sử dụng hơn, khuyến khích đổi mới, sáng tạo dựa trên tính khả dụng của dữ liệu[4]. Đặc biệt, Đạo luật Dữ liệu được xây dựng để bổ sung chứ không thay thế GDPR. Thật vậy, Khoản 5 Điều 1 Đạo luật này nêu rõ rằng nó *"không ảnh hưởng"* đến luật bảo vệ dữ liệu của EU và trong trường hợp có xung đột, GDPR sẽ được ưu tiên áp dụng.

Khác với cách tiếp cận phân tán, phi tập trung ở nhiều quốc gia, EU xây dựng hệ thống pháp luật bảo vệ dữ liệu theo mô hình *"omnibus"*, tức là điều chỉnh một cách bao trùm và hệ thống toàn bộ lĩnh vực này. Trọng tâm của

---

[3] Cortez, E. K. (2021), *Data Protection Around the World: Privacy Laws in Action,* T.M.C. Asser Press.

[4] European Commission (2025), *Data Act explained. Shaping Europe's digital future,* https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained, Truy cập ngày 14/7/2025.

Đạo luật dữ liệu châu Âu là cách tiếp cận dựa trên quyền con người, lấy con người làm trung tâm, trong đó dữ liệu cá nhân được nhìn nhận như một phần cấu thành của quyền bất khả xâm phạm về đời sống riêng tư và quyền kiểm soát thông tin cá nhân của mỗi công dân - điều đã được ghi nhận tại Điều 8 của Hiến chương về các quyền cơ bản của EU.



Trọng tâm của Đạo luật dữ liệu của Liên minh châu Âu là lấy con người làm trung tâm - Ảnh: Internet

Có thể thấy rằng, Đạo luật dữ liệu của EU là một phần trong chiến lược tổng thể của EU nhằm tạo ra một thị trường dữ liệu thống nhất và mạnh mẽ, thúc đẩy việc sử dụng dữ liệu trong nền kinh tế số, đồng thời bảo vệ quyền lợi của người dân và bảo đảm sự công bằng trong việc chia sẻ dữ liệu giữa các tổ chức, doanh nghiệp và Chính phủ. Được đề xuất vào năm 2022, Đạo luật dữ liệu là một bước tiến quan trọng trong xây dựng một ***"Châu Âu số"*** và hướng đến một nền kinh tế dữ liệu toàn cầu.

EU Data Act và GDPR được thiết kế không chỉ để áp dụng đối với các tổ chức và cá nhân trong liên minh, mà còn có phạm vi điều chỉnh mở rộng ra ngoài lãnh thổ, buộc mọi tổ chức trên thế giới khi xử lý dữ liệu của công dân EU đều phải tuân thủ quy định này. Cụ thể, *Điều 3(1)* (tức khoản 1 Điều 3) Đạo Luật dữ liệu châu Âu đề cập quy định này cũng được áp dụng đối với: ***(1)*** các nhà sản xuất sản phẩm và nhà cung cấp dịch vụ liên quan được đưa vào thị trường Liên minh châu Âu, bất kể họ có đặt trụ sở tại Liên minh hay không; ***(2)*** các bên cung cấp dữ liệu cho các bên nhận trong Liên minh, bất kể họ có đặt trụ sở tại Liên minh hay không; ***(3)*** các bên nhận dữ liệu tại Liên minh được cung cấp dữ liệu; ***(4)*** các cơ quan công quyền, Ủy ban châu Âu, Ngân hàng Trung ương châu Âu và các cơ quan của Liên minh khi yêu cầu bên nắm giữ dữ liệu cung cấp dữ liệu theo quy định tại Chương V. Nói cách khác, Đạo luật dữ liệu châu Âu có hiệu lực với mọi tổ chức nếu hoạt động xử lý liên quan đến cá nhân ở EU hoặc do đơn vị tại EU thực hiện, bất kể đơn vị đó ở đâu.

Ngoài ra, kế thừa khung pháp lý từ GDPR, Điều 5(1) Đạo luật dữ liệu ở châu Âu yêu cầu mỗi nước thành viên thành lập cơ quan bảo vệ dữ liệu độc lập (ví dụ như CNIL ở Pháp, BFDI ở Đức…), có thẩm quyền giám sát và xử phạt vi phạm nhằm bảo vệ các quyền và tự do cơ bản của cá nhân liên quan đến việc xử lý dữ liệu, đồng thời tạo điều kiện cho việc luân chuyển tự do dữ liệu cá nhân trong Liên minh. Đây là bước phát triển vượt bậc về tư duy pháp lý, đặt ra tiêu chuẩn bắt buộc để kiểm soát hoạt động tại các công ty công nghệ đa quốc gia, đặc biệt là các nền tảng số có quy mô toàn cầu như Facebook, Google hay Amazon...



Cơ quan bảo vệ dữ liệu của Chính phủ Pháp - Ảnh: Reuters

- Về mục tiêu chính sách

EU Data Act sẽ giúp đạt được các mục tiêu chính xác rộng hơn nhằm bảo đảm các doanh nghiệp EU trên tất cả các lĩnh vực có thể đổi mới và cạnh tranh trao quyền hiệu quả cho các cá nhân liên quan đến dữ liệu của họ và trang bị tốt hơn cho các doanh nghiệp và cơ quan khu vực công nghiệp cơ chế phù hợp để giải quyết những thách thức lớn về chính sách và xã hội, bao gồm các trường hợp khẩn cấp chung và các tình huống đặc biệt khác. Các doanh nghiệp sẽ có thể dễ dàng chuyển đổi dữ liệu của họ và các tài sản kỹ thuật số khác giữa các nhà cung cấp dịch vụ lưu trữ đám mây và các dịch vụ xử lý dữ liệu khác. Việc chia sẻ dữ liệu trong và giữa các lĩnh vực của nền kinh tế đòi hỏi một khuôn khổ các biện pháp và thủ tục pháp lý để nâng cao niềm tin và nâng cao hiệu quả việc tạo ra không gian dữ liệu chung của Châu Âu cho cho các lĩnh vực chiến lược của nền kinh tế và các lĩnh vực được công chúng quan tâm sẽ góp phần tạo ra thị trường nội bộ thực sự về dữ liệu

cho phép chia sẻ và sử dụng dữ liệu giữa các lĩnh vực. Do đó, quy định này góp phần vào các khuôn khổ quản trị và cơ sở hạ tầng này cũng như việc chia sẻ dữ liệu bên ngoài không gian dữ liệu.

Các mục tiêu cụ thể của Đạo luật dữ liệu có thể được nêu cụ thể như sau:

+ Tạo điều kiện thuận lợi cho người dùng, doanh nghiệp tiếp cận và sử dụng dữ liệu, đồng thời duy trì khuyến khích đầu tư vào các giải pháp tạo ra giá trị thông qua dữ liệu. Điều này bao gồm việc tăng cường sự chắc chắn về mặt pháp lý xung quanh việc chia sẻ dữ liệu được tạo ra khi sử dụng sản phẩm hoặc dịch vụ liên quan, cũng như các quy tắc vận hành để bảo đảm tính công bằng trong hợp đồng chia sẻ dữ liệu. Đề xuất làm rõ việc áp dụng các quyền liên quan theo Chỉ thị 96/9/EC về *bảo vệ pháp lý cơ sở dữ liệu* (Chỉ thị Cơ sở dữ liệu) theo các điều khoản của nó.

+ Cung cấp dữ liệu do doanh nghiệp nắm giữ cho các cơ quan khu vực công và các tổ chức Liên minh, các cơ quan hoặc cơ quan trong những tình huống nhất định khi có nhu cầu dữ liệu đặc biệt. Điều này chủ yếu liên quan đến các trường hợp khẩn cấp công cộng, nhưng cũng có các tình huống đặc biệt khác, trong đó việc chia sẻ dữ liệu bắt buộc giữa doanh nghiệp với Chính phủ là hợp lý nhằm hỗ trợ các chính sách mà dịch vụ công.

+ Tạo điều kiện chuyển đổi giữa các dịch vụ đám mây và biên. Việc tiếp cận các dịch vụ xử lý dữ liệu có tính cạnh tranh và tương tác là điều kiện tiên quyết cho một nền kinh tế dữ liệu phát triển mạnh mẽ, trong đó dữ liệu có thể được chia sẻ dễ dàng trong và giữa các hệ sinh thái ngành. Mức độ tin cậy vào các dịch vụ xử lý dữ liệu quyết định mức độ sử dụng các dịch vụ đó của người dùng trong các lĩnh vực của nền kinh tế.

+ Áp dụng các biện pháp bảo vệ chống lại việc truyền dữ liệu bất hợp pháp mà không có thông báo của nhà cung cấp dịch vụ đám mây. Điều này

là do đã có những lo ngại về việc các Chính phủ ngoài EU/Khu vực kinh tế Châu Âu (EEA) truy cập dữ liệu một cách bất hợp pháp. Những biện pháp bảo vệ như vậy sẽ nâng cao hơn nữa niềm tin vào các dịch vụ xử lý dữ liệu đang ngày càng củng cố nền kinh tế dữ liệu Châu Âu.

+ Cung cấp sự phát triển của các tiêu chuẩn về khả năng tương tác để dữ liệu được tái sử dụng giữa các ngành nhằm xóa bỏ các rào cản đối với việc chia sẻ dữ liệu trên các không gian dữ liệu chung của Châu Âu. Đề xuất này cũng hỗ trợ việc thiết lập các tiêu chuẩn cho "hợp đồng thông minh". Đây là các chương trình máy tính trên "sổ cái điện tử" thực hiện và giải quyết các giao dịch dựa trên các điều kiện được xác định trước. Họ có khả năng cung cấp cho người nắm giữ dữ liệu và người nhận dữ liệu sự đảm bảo rằng các điều kiện chia sẻ dữ liệu được tôn trọng.

- Tổng quan các nội dung lớn của Đạo luật Dữ liệu Châu Âu

Thứ nhất, chia sẻ dữ liệu giữa doanh nghiệp với người dùng và doanh nghiệp với doanh nghiệp. Theo quy định, các nhà sản xuất và nhà thiết kế phải thiết kế sản phẩm theo cách giúp dữ liệu có thể truy cập dễ dàng và họ phải minh bạch về dữ liệu nào sẽ có thể truy cập được cũng như cách truy cập chúng. Các quy định trong Chương này sẽ không ảnh hưởng đến khả năng nhà sản xuất truy cập và sử dụng dữ liệu từ sản phẩm hoặc dịch vụ liên quan mà họ cung cấp, khi đã được thỏa thuận với người dùng. Người giữ dữ liệu có nghĩa vụ cung cấp dữ liệu đó cho bên thứ ba theo yêu cầu của người dùng. Người dùng sẽ có quyền ủy quyền cho chủ sở hữu dữ liệu cấp quyền truy cập dữ liệu cho các nhà cung cấp dịch vụ bên thứ ba, chẳng hạn như nhà cung cấp dịch vụ hậu mãi. Các doanh nghiệp siêu nhỏ và nhỏ sẽ được miễn các nghĩa vụ này.

Thứ hai, nghĩa vụ cung cấp dữ liệu của chủ sở hữu dữ liệu. Theo luật của Liên minh, trong trường hợp chủ sở hữu dữ liệu có nghĩa vụ cung cấp dữ liệu cho người nhận dữ liệu như trong Chương 2 hoặc theo luật khác của Liên minh hoặc luật của quốc gia thành viên, khuôn khổ chung sẽ giải quyết các điều kiện mà theo đó dữ liệu được cung cấp và khoảng bồi thường cho việc cung cấp dữ liệu. Mọi điều kiện sẽ phải công bằng và không phân biệt đối xử, đồng thời mọi khoản bồi thường sẽ phải hợp lý. Bất kỳ khoản bồi thường nào dành cho các doanh nghiệp vừa và nhỏ sẽ không được vượt quá chi phí phát sinh để cung cấp dữ liệu, trừ khi có quy định khác trong luật pháp ngành. Cơ quan giải quyết tranh chấp được các quốc gia thành viên chứng nhận có thể hỗ trợ các bên khi không thống nhất được về khoản bồi thường hoặc điều kiện để đi đến thỏa thuận.

Thứ ba, điều khoản hợp đồng không công bằng liên quan đến truy cập dữ liệu và sử dụng giữa các doanh nghiệp. Nội dung này bảo đảm rằng các thỏa thuận hợp đồng về truy cập và sử dụng dữ liệu không lợi dụng sự mất cân bằng trong quyền đàm phán giữa các bên trong hợp đồng. Công cụ kiểm tra tính không công bằng bao gồm một điều khoản chung xác định tính không công bằng của điều khoản hợp đồng liên quan đến chia sẻ dữ liệu. Trong trường hợp quyền thương lượng không ngang bằng, công cụ đó sẽ bảo vệ bên hợp đồng yếu hơn nhằm tránh các hợp đồng không công bằng. Sự không công bằng như vậy cản trở việc sử dụng dữ liệu của cả hai bên trong hợp đồng. Cùng với đó các quy định bảo đảm phân bổ giá trị công bằng hơn trong nền kinh tế dữ liệu. Các điều khoản hợp đồng mẫu do Ủy ban khuyến nghị không thể hỗ trợ các bên thương mại ký kết hợp đồng dựa trên các điều khoản công bằng.

Thứ tư, cung cấp dữ liệu cho các cơ quan khu vực công, Ủy ban, Ngân hàng Trung ương Châu Âu và các cơ quan của Liên minh trên cơ sở một nhu cầu đặc biệt. Mục tiêu nội dung này là tạo ra một khuôn khổ hài hòa cho việc sử dụng dữ liệu của các cơ quan khu vực công và các tổ chức Liên minh, các cơ quan dữ liệu do doanh nghiệp nắm giữ trong các tình huống có nhu cầu đặc biệt về dữ liệu được yêu cầu.

Khuôn khổ này dựa trên nghĩa vụ cung cấp dữ liệu và sẽ chỉ áp dụng trong trường hợp khẩn cấp công cộng hoặc trong các tình huống mà cơ quan khu vực công có nhu cầu đặc biệt cần sử dụng một số dữ liệu nhất định nhưng dữ liệu đó không thể có được trên thị trường một cách kịp thời. Trong trường hợp có nhu cầu đặc biệt để ứng phó với tình trạng khẩn cấp công cộng, chẳng hạn như trường hợp khẩn cấp về sức khỏe cộng đồng hoặc các thảm họa lớn do thiên nhiên hoặc con người gây ra, dữ liệu sẽ được cung cấp miễn phí. Trong các trường hợp nhu cầu đặc biệt khác, bao gồm việc ngăn chặn hoặc hỗ trợ khôi phục sau tình trạng khẩn cấp công cộng, người nắm giữ dữ liệu cung cấp dữ liệu phải có quyền được bồi thường bao gồm các chi phí liên quan đến việc cung cấp dữ liệu liên quan. Để bảo đảm rằng quyền yêu cầu dữ liệu không bị lạm dụng và khu vực công vẫn chịu trách nhiệm về việc sử dụng dữ liệu đó, các yêu cầu về dữ liệu cần phải tương xứng, nêu rõ các mục đích cần đạt được và tôn trọng lợi ích của doanh nghiệp tạo ra dữ liệu. Các cơ quan có thẩm quyền sẽ bảo đảm tính minh bạch và công khai của tất cả các yêu cầu. Họ cũng sẽ xử lý mọi khiếu nại phát sinh.

Thứ năm, chuyển đổi giữa các dịch vụ xử lý dữ liệu. Nội dung này giới thiệu các quy định áp dụng đối với nhà cung cấp dịch vụ đám mây, biên và xử lý khác để cho phép chuyển đổi giữa các dịch vụ đó. Đạo luật không yêu cầu các tiêu chuẩn kỹ thuật hoặc giao diện cụ thể. Tuy nhiên, nó yêu cầu các

dịch vụ phải tương thích với các tiêu chuẩn Châu Âu hoặc các thông số kỹ thuật có khả năng tương tác mở (nếu có).

Thứ sáu, quy định về truy cập quốc tế bất hợp pháp và chuyển dữ liệu phi cá nhân, đề cập đến việc bên thứ ba truy cập bất hợp pháp vào dữ liệu phi cá nhân được lưu giữ trong Liên minh.

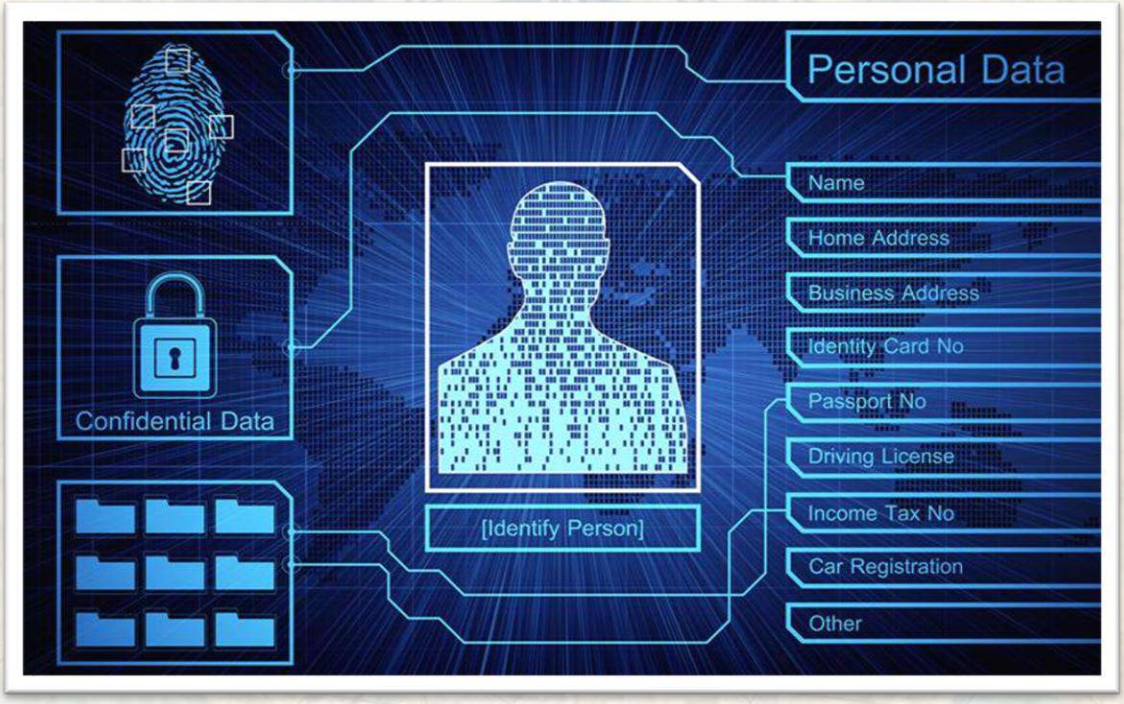
- Một số khái niệm

Một trong những đặc trưng nổi bật trong khung pháp lý của Liên minh châu Âu về dữ liệu là việc xác lập rõ ràng các khái niệm cốt lõi liên quan đến dữ liệu. *Điều 2 (1)* Đạo luật dữ liệu châu Âu đã xác định *"Dữ liệu là bất kỳ hình thức biểu hiện dưới dạng kỹ thuật số nào của hành vi, sự kiện, thông tin và bất kỳ tập hợp nào của các hành vi, sự kiện hoặc thông tin đó, bao gồm cả dưới dạng bản ghi âm thanh, hình ảnh hoặc ghi hình"*[5]. Đây là khái niệm có phạm vi rất rộng mang tính mở và định khung, phản ánh đầy đủ tính đa dạng của các loại dữ liệu, bao trùm cả dữ liệu cá nhân và dữ liệu phi cá nhân. Cách định nghĩa *"bất kỳ"* như trên cũng cho phép áp dụng cho nhiều công nghệ và hình thức lưu trữ mới trong tương lai, phù hợp với xu hướng chuyển đổi số liên tục của thế giới hiện đại. Không chỉ vậy, việc đưa *"compilation"* (tập hợp dữ liệu) vào khái niệm phản ánh thực tế là giá trị dữ liệu không chỉ ở từng phần tử riêng lẻ mà còn ở bộ dữ liệu tổng hợp.

Khác với GDPR có phạm vi áp dụng hẹp, chỉ giới hạn ở thuật ngữ *"dữ liệu cá nhân"* và không áp dụng cho dữ liệu của pháp nhân, tổ chức, trọng tâm của Đạo luật dữ liệu là dữ liệu được tạo ra từ "*sản phẩm, dịch vụ về dữ liệu"* thường được gọi là dữ liệu IoT hoặc dữ liệu công nghiệp (Điều 1 (2)). Sự mở rộng này tạo ra một thách thức lớn cho các doanh

[5] GDPR. Article 2 (1): "'data' means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording".

nghiệp trong việc phân biệt giữa các bộ dữ liệu cá nhân, phi cá nhân và hỗn hợp. Ví dụ, một luồng dữ liệu từ một chiếc xe được kết nối có thể chứa dữ liệu hiệu suất động cơ (là dữ liệu phi cá nhân), nhưng cũng có thể chứa dữ liệu về vị trí và hành vi lái xe của người dùng (là dữ liệu cá nhân theo GDPR). Việc phân loại sai dữ liệu mang lại rủi ro kép, đó là khi xử lý dữ liệu cá nhân như dữ liệu phi cá nhân sẽ vi phạm GDPR, trong khi hạn chế quyền truy cập vào dữ liệu phi cá nhân vì cho rằng đó là dữ liệu cá nhân thì sẽ có thể vi phạm Đạo luật Dữ liệu. Do đó, Đạo luật Dữ liệu buộc các tổ chức phải thay đổi cách quản trị dữ liệu, tập trung khả năng phân loại và quản lý dữ liệu theo cả hai quy định.



Minh họa về dữ liệu cá nhân - Ảnh: Báo Chính phủ

Về phân loại dữ liệu, cả GDPR và Đạo luật dữ liệu châu Âu đều không có điều khoản nào quy định riêng biệt về phân loại các nhóm dữ liệu số. Tuy nhiên, các văn bản này đều có các quy định gián tiếp liên quan đến mức độ nhạy cảm hoặc rủi ro của dữ liệu. Điển hình, GDPR đề cập đến một dạng

đặc biệt của dữ liệu cá nhân là *"dữ liệu nhạy cảm"*, được quy định cụ thể tại Điều 9 GDPR. Các loại dữ liệu này bao gồm: *Thông tin về chủng tộc hoặc nguồn gốc dân tộc, quan điểm chính trị, tín ngưỡng tôn giáo hoặc triết học, tư cách thành viên công đoàn, dữ liệu di truyền, dữ liệu sinh trắc học nhằm xác định danh tính cá nhân, thông tin sức khỏe, dữ liệu về đời sống tình dục hoặc khuynh hướng tình dục.* Việc xử lý các loại dữ liệu nhạy cảm này bị nghiêm cấm, trừ một số trường hợp ngoại lệ rất hạn chế, nhằm bảo vệ tối đa các giá trị nền tảng về tự do, phẩm giá và bình đẳng của cá nhân trong xã hội. Tương tự, *Điều 17* Đạo luật dữ liệu quy định việc chia sẻ dữ liệu với cơ quan khu vực công trong các tình huống khẩn cấp hoặc đặc biệt, thường gắn với dữ liệu *"quan trọng"* cho lợi ích công. Trong bối cảnh này, những dữ liệu đó có tầm quan trọng đối với kinh tế - xã hội *(Điều 27(2))*.



Những điều luật này góp phần phát triển kinh tế - xã hội có trật tự - Ảnh: Tạp chí Tài Chính

Trong quá trình xử lý dữ liệu, *"sự đồng ý"* của chủ thể dữ liệu (consent) là một khái niệm trung tâm và là một trong những cơ sở pháp lý quan trọng nhất theo Điều 6 và 7 GDPR. Mặc dù được xây dựng và ban hành sau GDPR, Đạo luật dữ liệu không thiết lập cơ chế đồng ý mới, mà viện dẫn trực tiếp sang GDPR để xác định cách thức và điều kiện hợp lệ của "sự đồng ý" đối với dữ liệu cá nhân. Đó là yêu cầu sự đồng ý phải được đưa ra một cách *tự nguyện, rõ ràng, cụ thể và có thông tin đầy đủ*; đồng thời, chủ thể dữ liệu có quyền rút lại sự đồng ý bất kỳ lúc nào mà không gây ảnh hưởng đến tính hợp pháp của việc xử lý trước đó. "Sự đồng ý" không được coi là hợp lệ nếu nó bị ràng buộc vào việc thực hiện một hợp đồng, trong khi dữ liệu được yêu cầu lại không cần thiết cho việc thực hiện hợp đồng đó, quy định điều này nhằm ngăn ngừa các hành vi ép buộc trá hình từ phía các tổ chức[6].



GDPR tạo không gian pháp lý mạnh mẽ - Ảnh : Internet

[6] Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide.* Springer International Publishing.p. 27-29

Về khái niệm đồng ý, ta phải lưu ý rằng "khi sự đồng ý được lấy thông qua phương tiện điện tử chỉ bằng một cú nhấp chuột, vuốt hoặc gõ phím, trên thực tế, chủ thể dữ liệu phải có thể rút lại sự đồng ý đó một cách dễ dàng như vậy". Khi sự đồng ý được thu thập thông qua việc sử dụng giao diện người dùng dành riêng cho dịch vụ (ví dụ: thông qua trang web, ứng dụng, tài khoản đăng nhập, giao diện của thiết bị IoT hoặc qua email), chắc chắn chủ thể dữ liệu phải có khả năng rút lại sự đồng ý thông qua cùng giao diện điện tử đó, vì việc chuyển sang giao diện khác chỉ vì lý do rút lại sự đồng ý sẽ đòi hỏi nhiều thao tác không cần thiết. Hơn nữa, chủ thể dữ liệu phải có khả năng rút lại sự đồng ý mà không bị thiệt hại. Điều này có nghĩa là, trong số những điều khác, bên kiểm soát phải tạo điều kiện cho việc rút lại sự đồng ý miễn phí hoặc không mất phí hạ thấp mức độ dịch vụ[7]. Bên cạnh đó, có thể tồn tại nguy cơ đến từ việc đơn giản hóa sự đồng ý thông qua các cú nhấp chuột và vuốt màn hình, do đó, cần đơn giản hóa việc rút lại sự đồng ý.

Ngoài ra, GDPR nêu rằng "trong trường hợp việc xử lý dữ liệu được dựa trên sự đồng ý của chủ thể dữ liệu, bên kiểm soát dữ liệu phải có khả năng chứng minh rằng chủ thể dữ liệu đã thực sự đưa ra sự đồng ý đối với hoạt động xử lý đó". Cụ thể, trong bối cảnh tuyên bố bằng văn bản về một vấn đề khác, các biện pháp bảo vệ phải đảm bảo rằng chủ thể dữ liệu nhận thức được thực tế là họ đã đồng ý và mức độ đồng ý được đưa ra. Theo Chỉ thị 93/13/EEC của Hội đồng, tuyên bố đồng ý do bên kiểm soát soạn thảo trước phải được cung cấp dưới dạng đơn giản và dễ tiếp cận, sử dụng ngôn ngữ rõ ràng, dễ hiểu và không được chứa các điều khoản không công bằng. Để có thể hiểu được sự đồng ý, chủ thể dữ liệu ít nhất phải biết danh tính của bên kiểm soát

[7] Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, adopted on 28 November 2017; as last Revised and Adopted on 10 April 2018, p. 21.

và mục đích xử lý dữ liệu cá nhân. Sự đồng ý không nên được coi là tự nguyện đưa ra nếu chủ thể dữ liệu không có sự lựa chọn thực sự hoặc tự do, hoặc không thể từ chối hoặc rút lại sự đồng ý mà không bị thiệt hại[8]. Theo hướng lập luận này, chúng ta có thể nhận thấy rằng ngưỡng để được thông báo về sự đồng ý được xem là "đã được thông tin" bị hạ thấp đáng kể. Điều này càng trở nên đáng lưu ý khi xét đến thực tế rằng một người dùng trung bình hầu như không hiểu mục đích xử lý dữ liệu, ngay cả khi những mục đích đó không được viết bằng thuật ngữ chuyên ngành, vì chúng thường mang tính kỹ thuật và phạm vi nghĩa rộng quá mức. Một thiếu sót khác là người dùng có thể mất quyền kiểm soát dữ liệu của mình sau khi đã đồng ý, vì người dùng không thể biết dữ liệu sau đó đã được cung cấp cho ai.

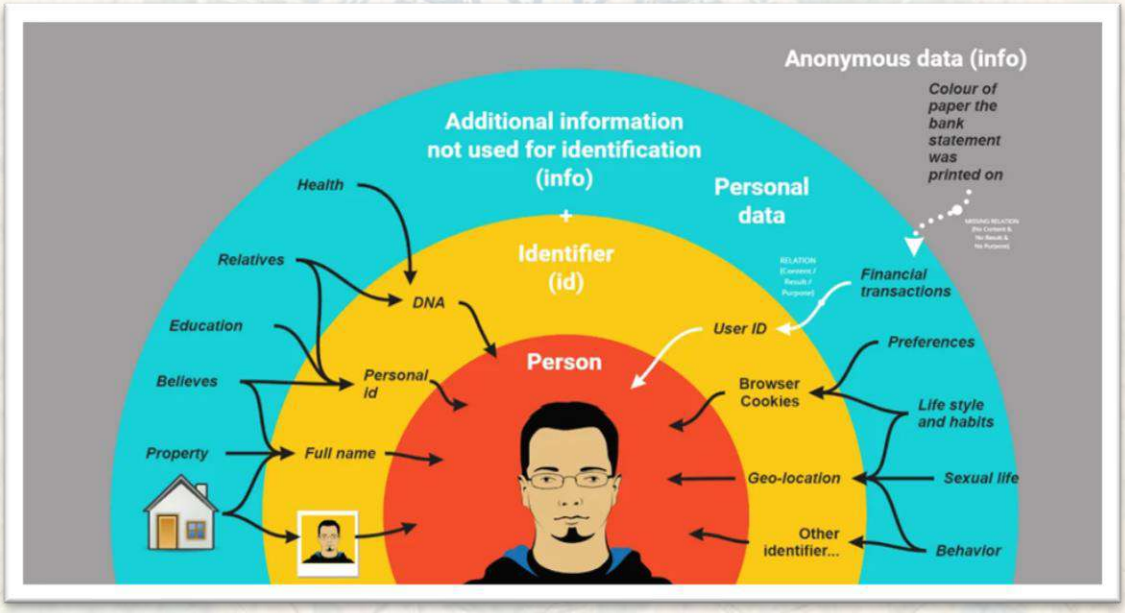


GDPR góp phần bảo vệ quyền riêng tư trên không gian mạng, điều chỉ có số ít quốc gia làm được - Ảnh: Internet

Tuy nhiên, GDPR quy định rằng "để đảm bảo sự đồng ý là tự nguyện, sự đồng ý không nên là một cơ sở pháp lý hợp lệ cho bất kỳ việc xử lý dữ

[8] GDPR., Recital 42 and Article 7.

liệu cá nhân trong một trường hợp cụ thể nào khi có sự mất cân bằng rõ ràng giữa chủ thể dữ liệu và bên kiểm soát dữ liệu, đặc biệt là khi bên kiểm soát là một cơ quan nhà nước. Sự đồng ý được cho là không được đưa ra một cách tự nguyện nếu không cho phép đưa ra sự đồng ý riêng biệt đối với từng hoạt động xử lý dữ liệu cá nhân khác nhau, mặc dù nó phù hợp trong từng trường hợp cụ thể. Hoặc nếu trong việc thực hiện ký kết hợp đồng, bao gồm cả việc cung cấp dịch vụ, nếu bên xử lý dữ liệu yêu cầu người dùng sự đồng ý nhưng sự đồng ý đó không cần thiết cho việc thực hiện hợp đồng thì sự đồng ý này không được coi là tự nguyện"[9]. Quy định này nhấn mạnh rằng sự đồng ý của người dùng phải là tự nguyện, có nhận thức đầy đủ, có quyền lựa chọn thật sự.



Các trường dữ liệu được định nghĩa trong GDPR - Ảnh: DPO Europe

Xét đến khía cạnh các khái niệm liên quan đến dữ liệu, GDPR xác định các vai trò chính bao gồm *"chủ thể dữ liệu"* (luôn là một cá nhân), *"bên kiểm soát"* (bên xác định mục đích và phương tiện xử lý) và *"bên xử lý"* (có

[9] GDPR., Recital 43.

vai trò thay cho bên kiểm soát xử lý dữ liệu). Trong khi đó, Đạo luật Dữ liệu đã giới thiệu các vai trò mới, như: *"người dùng"* (một cá nhân hoặc pháp nhân sở hữu, thuê hoặc cho thuê một sản phẩm được kết nối), *"bên sở hữu dữ liệu"* (thực thể có quyền hoặc nghĩa vụ cung cấp dữ liệu, thường là nhà sản xuất) và *"bên nhận dữ liệu"* (một bên thứ ba được cung cấp dữ liệu).

Khái niệm *"người dùng"* là một thuật ngữ mang tính cách mạng. Bằng cách bao gồm các pháp nhân (doanh nghiệp), Đạo luật Dữ liệu lần đầu tiên mở rộng các quyền về dữ liệu ra ngoài phạm vi cá nhân trong một quy định cấp liên minh của EU (Điều 2 (12)). Đây là cơ chế pháp lý cho phép khuôn khổ chia sẻ dữ liệu B2B (Business-to-Business) và có những tác động sâu sắc đến các mối quan hệ thương mại. Sự thay đổi từ "chủ thể dữ liệu" sang "người dùng" về cơ bản đã biến đổi bản chất của các quyền về dữ liệu từ một quyền không thể chuyển nhượng thành một quyền kinh tế và hợp đồng có thể chuyển nhượng. Điều này trao quyền cho các doanh nghiệp, đặc biệt là các doanh nghiệp vừa và nhỏ, trở thành những người tham gia tích cực vào nền kinh tế dữ liệu, thay vì chỉ là đối tượng thụ động của việc thu thập dữ liệu.

Điều đặc biệt đáng chú ý khác là thuật ngữ được sử dụng để phân loại các doanh nghiệp số[10]. Trong GDPR, các thuật ngữ như *"bên xử lý dữ liệu"* (processor) và *"bên kiểm soát dữ liệu"* (controller) được sử dụng cùng với các thuật ngữ khác. Chính bên kiểm soát dữ liệu là người quyết định mục đích và phương thức xử lý dữ liệu cá nhân, do đó chịu trách nhiệm cuối cùng và có trách nhiệm pháp lý đối với dữ liệu đã được xử lý[11]. Trong Quy định về Quyền riêng tư Điện tử, thuật ngữ "nhà cung cấp mạng và dịch vụ truyền

[10] Article 4 (8) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[11] GDPR., Article 24.

thông điện tử" được sử dụng. Trong Chỉ thị NIS, có sự phân biệt giữa "nhà điều hành các dịch vụ thiết yếu" và "nhà cung cấp dịch vụ kỹ thuật số", sự hợp tác giữa hai bên được khuyến khích[12] vì mục đích bảo mật, đặc biệt nếu hệ thống mạng và thông tin là trách nhiệm của cả hai bên[13]. Tuy nhiên, những sự phân biệt này có thể gây nhầm lẫn về việc phân bổ trách nhiệm, dẫn đến việc giảm bớt trách nhiệm, vì vai trò của các bên này không rõ ràng. Ngược lại, các bên này thường đảm nhiệm đồng thời nhiều vai trò. Ví dụ, các nhà cung cấp mạng lưới và dịch vụ truyền thông điện tử cũng có thể là nhà điều hành các dịch vụ thiết yếu khi họ cung cấp dịch vụ truy cập internet băng thông rộng và dịch vụ thoại, cả hai đều được coi là dịch vụ thiết yếu[14]. Sự nhầm lẫn này liên quan đến năng lực của các doanh nghiệp kỹ thuật số cũng có thể ảnh hưởng đến nghĩa vụ của họ trong việc xin sự đồng ý và đáp ứng các điều kiện cơ bản cho người dùng.

Không chỉ vậy, một khái niệm nổi bật khác trong khung GDPR là *"tính di động của dữ liệu"* (data portability), được quy định tại Điều 20. Quyền này cho phép cá nhân nhận lại dữ liệu mà họ đã cung cấp cho một tổ chức với định dạng có cấu trúc, phổ biến và có thể đọc được bằng máy, đồng thời có quyền chuyển dữ liệu đó đến một tổ chức khác mà không gặp cản trở từ phía tổ chức ban đầu. Quyền này góp phần nâng cao quyền kiểm soát dữ liệu cá nhân của người dùng và thúc đẩy tính cạnh tranh giữa các nhà cung cấp dịch vụ số[15].

---

[12] Recital 35 of the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[13] GDPR., Recital 44.

[14] Recital 18 of the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58EC.

[15] Sartor, G. (2018). *The right to data portability in the GDPR: Towards user-centric interoperability of digital services*. Computer Law & Security Review, 34(2), 193–203.

Bên cạnh đó, GDPR cũng quy định rõ nghĩa vụ thông báo vi phạm dữ liệu, yêu cầu các tổ chức phải thông báo cho cơ quan giám sát trong vòng 72 giờ kể từ khi phát hiện sự cố, trừ khi vi phạm đó không gây rủi ro cho quyền và tự do của cá nhân (Điều 33 GDPR). Việc minh định các khái niệm cốt lõi như vậy thể hiện cách tiếp cận của EU đặt quyền cá nhân làm trung tâm, đồng thời đảm bảo tính minh bạch, trách nhiệm giải trình và khả năng kiểm soát dữ liệu trong bối cảnh nền kinh tế số phát triển mạnh mẽ.

- Các nguyên tắc nền tảng



07 nguyên tác của GDPR - Ảnh: URM Consulting

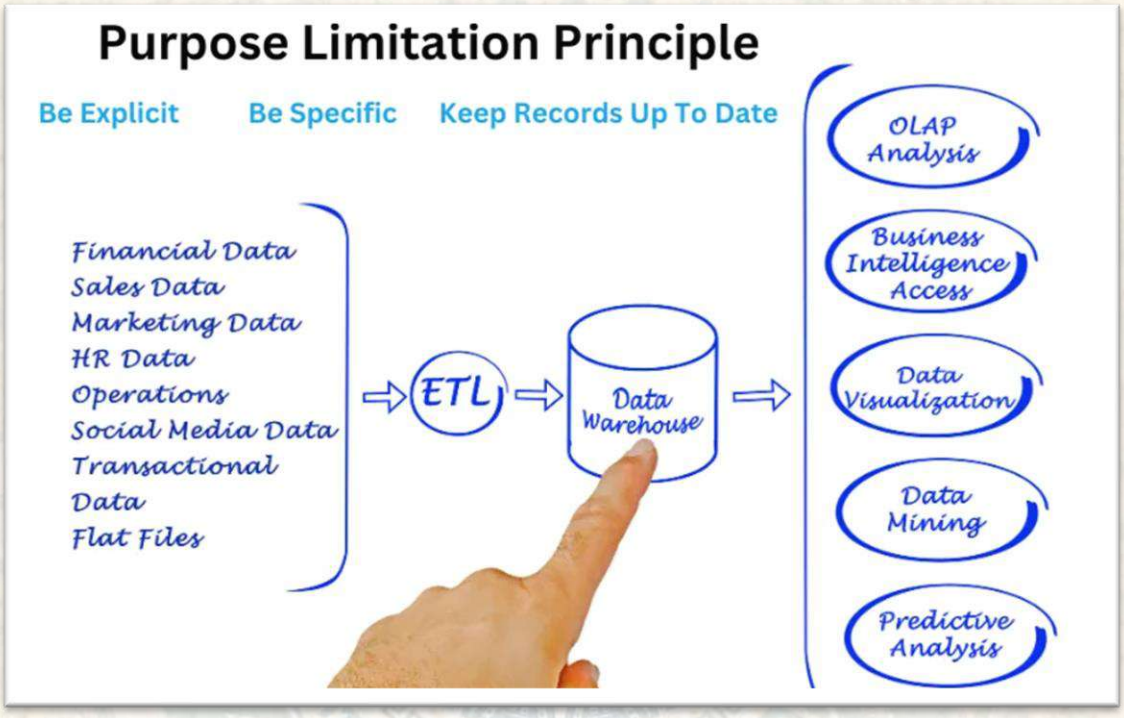
Trên cơ sở kế thừa GDPR, Đạo luật dữ liệu cũng xây dựng một hệ thống các nguyên tắc nền tảng, định hình cách thức xử lý dữ liệu cá nhân trong toàn bộ không gian số của EU. Các nguyên tắc này không chỉ mang tính pháp lý bắt buộc mà còn phản ánh triết lý phương châm *"lấy con người làm trung tâm"*, kết hợp các quy tắc hài hòa về quyền truy cập và sử dụng dữ liệu công bằng nhằm loại bỏ các rào cản đối với một thị trường dữ liệu năng động trong mô hình quản trị dữ liệu châu Âu, bên cạnh các nguyên tắc đã nêu trong GDPR, bao gồm:

(1) Nguyên tắc hợp pháp, công bằng và minh bạch (Lawfulness, Fairness and Transparency). Theo nguyên tắc này, dữ liệu cá nhân phải được xử lý một cách hợp pháp, công bằng và minh bạch đối với người dùng. Điều này có nghĩa là việc thu thập và sử dụng dữ liệu phải có cơ sở pháp lý rõ ràng, không được che giấu hoặc lừa dối... Để đảm bảo tính minh bạch, bên nắm giữ dữ liệu có nghĩa vụ cung cấp thông tin rõ ràng cho người dùng về loại dữ liệu, định dạng, khối lượng, cách lưu trữ và điều kiện truy cập trước khi ký hợp đồng (Điều 3).



Nguyên tắc hợp pháp, công bằng và minh bạch được nhiều luật học hỏi và phát triển - Ảnh: Internet

(2) Nguyên tắc giới hạn mục đích (Purpose Limitation): Dữ liệu cá nhân phải được thu thập cho các mục đích cụ thể, rõ ràng và hợp pháp và không được vượt quá giới hạn hoặc thực hiện các hành vi khác không phù hợp với các mục đích đó. Tức là cá nhân, tổ chức phải biết rõ tại sao mình thu thập dữ liệu và chỉ sử dụng cho mục đích đã nêu.



Ảnh minh họa nguyên tắc giới hạn mục đích - Ảnh: Formiti

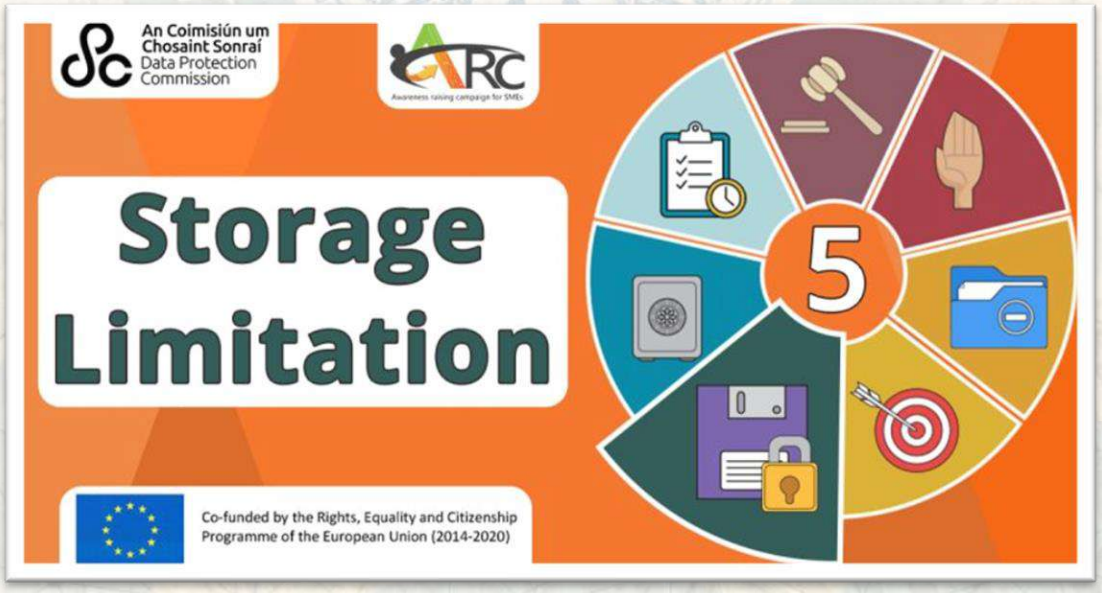
(3) Nguyên tắc chính xác (Accuracy): Dữ liệu cá nhân phải chính xác và, nếu cần, phải được cập nhật. Mọi bước đi hợp lý phải được thực hiện để đảm bảo rằng dữ liệu cá nhân không chính xác, sau khi xét đến các mục đích mà chúng được xử lý, sẽ bị xóa hoặc chỉnh sửa kịp thời.

(4) Nguyên tắc tối thiểu hóa dữ liệu (Data Minimisation): Đây là nguyên tắc do GDPR chỉ ra nhằm củng cố lớp bảo vệ vững chắc đối với dữ liệu cá nhân, đó là phải phù hợp, liên quan và chỉ giới hạn ở mức cần thiết cho các mục đích mà chúng được xử lý. Các cá nhân, tổ chức không thu thập nhiều dữ liệu hơn mức họ thực sự cần.



Ảnh minh họa - Ảnh: Cyberpilot

(5) Giới hạn lưu trữ (Storage Limitation): Dữ liệu cá nhân phải được lưu giữ dưới hình thức cho phép nhận dạng chủ thể dữ liệu không lâu hơn mức cần thiết cho các mục đích mà dữ liệu cá nhân được xử lý. Khi không còn cần thiết, dữ liệu phải được xóa an toàn hoặc ẩn danh.



Ảnh minh họa về giới hạn lưu trữ - Ảnh: Project ARC

(6) Toàn vẹn và bảo mật (Integrity and Confidentiality): Dữ liệu cá nhân phải được xử lý theo cách đảm bảo bảo mật dữ liệu cá nhân thích hợp,

bao gồm bảo vệ chống lại việc xử lý trái phép hoặc bất hợp pháp và chống lại việc mất mát, phá hủy hoặc thiệt hại ngẫu nhiên, bằng cách sử dụng các biện pháp kỹ thuật hoặc tổ chức phù hợp.



Tam giác CIA của giới bảo mật được cụ thể thành luật - Ảnh: LinkedIn

(7) Accountability (Trách nhiệm giải trình): Chủ thể xử lý dữ liệu phải chịu trách nhiệm và có khả năng chứng minh rằng mình tuân thủ tất cả các nguyên tắc trên. Điều này đòi hỏi các tổ chức phải có các chính sách, quy trình và hồ sơ tài liệu để chứng minh sự tuân thủ của họ.

Ngoài ra, so với GDPR, Đạo luật dữ liệu còn bổ sung thêm các nguyên tắc mới đối với các hành vi có liên quan đến dữ liệu dành cho các doanh nghiệp, tổ chức, đó là: ***(1)*** Tôn trọng quyền bảo vệ dữ liệu cá nhân (Mọi xử lý dữ liệu cá nhân theo Data Act vẫn phải tuân thủ đầy đủ GDPR, đặc biệt về sự đồng ý, tính hợp pháp của xử lý và quyền của chủ thể dữ liệu (Điều 1(5), Điều 6)); ***(2)*** Bảo vệ bí mật thương mại và an ninh (Được phép áp dụng biện pháp kỹ thuật hoặc tổ chức để bảo vệ bí mật thương mại và an ninh, nhưng không được dùng lý do này để phủ nhận quyền truy cập hợp pháp của

người dùng (Điều 4(3), 8(6)). Đặc biệt, EU Data Act đã để hiện một nguyên tắc mới trong quy định đối với cơ quan công quyền đó là cho phép các cơ quan này và Ủy ban, ECB hoặc cơ quan EU yêu cầu dữ liệu người dùng trong tình huống khẩn cấp, đặc biệt vì lợi ích công (Chương V).



Trách nhiệm phải giải trình được cụ thể trong luật - Ảnh: Internet

- Quyền và nghĩa vụ của cá nhân đối với dữ liệu

Đối với cá nhân, văn bản pháp luật có giá trị pháp lý cao và quy định cụ thể nhất vẫn là GDPR. Bên cạnh việc xây dựng các nguyên tắc nền tảng, GDPR thiết lập một khung pháp lý toàn diện và sâu rộng nhằm bảo vệ quyền và xác lập nghĩa vụ của cá nhân đối với dữ liệu. Một trong những điểm nổi bật nhất của GDPR là việc công nhận và bảo vệ một loạt các quyền của chủ thể dữ liệu, là người có dữ liệu bị thu thập và xử lý. Các quyền này bao gồm:



Các nguyên tắc của GDPR - Ảnh: ISCVietnam

(1) Quyền được biết (Right to be informed, Điều 13 và Điều 14): *"Khi dữ liệu cá nhân được thu thập từ người dữ liệu, người kiểm soát dữ liệu phải cung cấp cho người dữ liệu những thông tin sau: (a) danh tính và thông tin liên hệ của người kiểm soát dữ liệu; (b) mục đích của việc xử lý dữ liệu và cơ sở pháp lý cho việc xử lý đó; ..."*. Quyền được biết yêu cầu tổ chức phải thông báo rõ ràng và đầy đủ về việc thu thập và sử dụng dữ liệu cá nhân của người dùng, bao gồm việc cung cấp thông tin về tổ chức thu thập dữ liệu, mục đích thu thập dữ liệu, và cơ sở pháp lý cho hành động đó. Điều này đảm bảo sự minh bạch và công bằng trong việc xử lý dữ liệu cá nhân của các tổ chức.

(2) Quyền truy cập dữ liệu (Right of access, Điều 15): *"Người dữ liệu có quyền yêu cầu từ người kiểm soát dữ liệu xác nhận liệu dữ liệu cá nhân của mình có đang được xử lý hay không, và trong trường hợp có, quyền truy cập vào dữ liệu cá nhân và những thông tin sau: (a) mục đích của việc xử lý; (b) các loại dữ liệu cá nhân liên quan; (c) các bên nhận hoặc các nhóm nhận mà dữ liệu cá nhân đã được hoặc sẽ được tiết lộ; ..."*. Quyền truy cập dữ liệu

cho phép cá nhân yêu cầu tổ chức xác nhận việc xử lý dữ liệu của mình và yêu cầu cung cấp bản sao dữ liệu cá nhân mà tổ chức đang sở hữu. Điều này giúp cá nhân hiểu rõ cách dữ liệu của họ được sử dụng và đảm bảo quyền giám sát đối với thông tin cá nhân của mình. Đối với quyền truy cập, mặc dù có điểm tương đồng với GDPR nhưng EU Data Act đặc biệt nhấn mạnh quyền truy cập vào các dữ liệu không phải cá nhân mà cá nhân tạo ra trong quá trình sử dụng sản phẩm hoặc dịch vụ. Điều này giúp cá nhân có thể yêu cầu dữ liệu không phải cá nhân (như dữ liệu kỹ thuật hoặc dữ liệu liên quan đến việc sử dụng sản phẩm) được chia sẻ hoặc sử dụng bởi bên thứ ba.



Ảnh minh họa - Ảnh: Cedcoss

(3) Quyền xóa dữ liệu (Right to erasure, Điều 17): *"The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), and where there is no other legal ground for the processing; ..."*. Quyền xóa dữ liệu (hay "quyền được quên") cho phép cá nhân yêu cầu xóa bỏ dữ liệu cá nhân của họ khi không còn cần thiết hoặc khi họ rút lại sự đồng ý cho việc xử lý dữ liệu. Đây là một công cụ quan trọng để bảo vệ quyền riêng tư, đặc biệt trong thời đại số khi dữ liệu có thể được lưu trữ vĩnh viễn.

(4) Quyền phản đối (Right to object, Điều 21): *"The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject..."*. Quyền phản đối cho phép cá nhân ngừng việc xử lý dữ liệu cá nhân của họ trong các trường hợp cụ thể, đặc biệt khi dữ liệu được xử lý vì lợi ích hợp pháp của tổ chức. Điều này mang lại quyền kiểm soát cho cá nhân đối với việc sử dụng thông tin cá nhân của họ, nhất là trong các trường hợp dữ liệu được dùng cho các mục đích như quảng cáo hoặc phân tích.

(5) Quyền hạn chế xử lý (Right to restrict processing, Điều 18): *"The data subject shall have the right to obtain from the controller restriction of*

processing where one of the following applies: (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; ...". Quyền hạn chế xử lý cho phép cá nhân yêu cầu tổ chức ngừng xử lý dữ liệu trong khi tranh chấp về tính chính xác của dữ liệu hoặc khi dữ liệu không còn cần thiết nhưng chủ thể dữ liệu muốn giữ lại dữ liệu để phục vụ cho các yêu cầu pháp lý hoặc hợp pháp khác.

(6) Quyền chuyển dữ liệu (Right to data portability, Điều 20): *"The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or on a contract pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means".* Quyền chuyển dữ liệu giúp cá nhân dễ dàng di chuyển thông tin cá nhân của mình từ một tổ chức này sang tổ chức khác. Điều này đặc biệt hữu ích trong các dịch vụ trực tuyến khi người dùng muốn chuyển đổi giữa các dịch vụ mà không phải nhập lại dữ liệu. Mặc khác, nó yêu cầu các tổ chức cung cấp dữ liệu phải thực hiện các biện pháp bảo vệ hợp lý để đảm bảo quyền lợi của cá nhân, bao gồm bảo vệ quyền riêng tư và bảo mật của cá nhân khi chia sẻ dữ liệu.

Các quyền này là một bước tiến quan trọng trong việc bảo vệ quyền riêng tư của người dân trong bối cảnh công nghệ số ngày càng phát triển mạnh mẽ và việc thu thập, chia sẻ dữ liệu cá nhân trở thành một phần không

thể thiếu của các dịch vụ trực tuyến. GDPR không chỉ bảo vệ quyền lợi của cá nhân mà còn tạo ra một cơ chế giám sát và trách nhiệm rõ ràng đối với các tổ chức, đảm bảo rằng việc xử lý dữ liệu không gây tổn hại đến quyền lợi và tự do của người dân. Tuy nhiên, để các quyền này thực sự hiệu quả, cần có sự hợp tác chặt chẽ giữa các cơ quan quản lý và tổ chức, đồng thời các cá nhân cũng cần hiểu rõ quyền lợi của mình và chủ động bảo vệ dữ liệu cá nhân trong mọi tình huống.

Đồng thời, GDPR cũng đặt ra các nghĩa vụ pháp lý nhất định của cá nhân đối với dữ liệu trong quá trình bảo vệ và kiểm soát dữ liệu của mình. Cụ thể:

(1) Nghĩa vụ cung cấp thông tin chính xác và đầy đủ: Điều 5(1)(d) yêu cầu cá nhân phải cung cấp thông tin chính xác và đầy đủ khi liên quan đến dữ liệu cá nhân của mình. Nếu thông tin cung cấp không chính xác hoặc bị thay đổi, cá nhân có nghĩa vụ cập nhật và chỉnh sửa lại để đảm bảo tính chính xác của dữ liệu.

(2) Nghĩa vụ hợp tác khi tổ chức yêu cầu: Điều 12(3) và Điều 15 GDPR yêu cầu nếu tổ chức yêu cầu cá nhân cung cấp thông tin để thực hiện quyền truy cập hoặc các yêu cầu khác liên quan đến việc xử lý dữ liệu cá nhân (như quyền xóa dữ liệu, quyền chỉnh sửa…) với lý do chính đáng, đúng quy định pháp luật, cá nhân phải hợp tác để tổ chức thực hiện yêu cầu đó trong thời gian hợp lý. Nghĩa vụ hợp tác này giúp cá nhân dễ dàng thực thi quyền của mình và giúp tổ chức thực hiện các quyền đó một cách chính xác, minh bạch và hiệu quả.

(3) Nghĩa vụ thông báo khi quyền lợi bị vi phạm: Điều 82 GDPR yêu cầu tổ chức chịu trách nhiệm thông báo vi phạm dữ liệu cá nhân cho cơ quan giám sát và người bị ảnh hưởng, GDPR cũng yêu cầu cá nhân thông báo nếu

nhận thấy dữ liệu của mình bị xử lý trái phép hoặc có nguy cơ gây hại cho quyền lợi cá nhân. Việc quy định nghĩa vụ giúp cá nhân chủ động bảo vệ quyền lợi của mình và ngăn chặn vi phạm dữ liệu cá nhân. Tuy nhiên, một số cá nhân có thể lợi dụng quyền này để đưa ra khiếu nại không chính đáng.

(4) Nghĩa vụ xác nhận và duy trì sự đồng ý: Điều 7 GDPR yêu cầu cá nhân phải xác nhận sự đồng ý của mình đối với việc xử lý dữ liệu cá nhân và có quyền rút lại sự đồng ý bất kỳ lúc nào. Nếu việc xử lý dữ liệu cá nhân dựa trên sự đồng ý của cá nhân (như trong trường hợp các hình thức tiếp thị hoặc chia sẻ dữ liệu với bên thứ ba), cá nhân có nghĩa vụ cung cấp sự đồng ý rõ ràng và cụ thể.

(5) Nghĩa vụ sử dụng quyền đối với dữ liệu cá nhân của mình: GDPR cung cấp cho cá nhân nhiều quyền, bao gồm quyền truy cập, chỉnh sửa, xóa dữ liệu cá nhân của mình, quyền phản đối, hạn chế xử lý, và quyền chuyển dữ liệu (Điều 15 - 22). Cá nhân có nghĩa vụ sử dụng các quyền này khi cần thiết để bảo vệ quyền lợi của mình để đảm bảo dữ liệu cá nhân được xử lý một cách công bằng và minh bạch.

(6) Nghĩa vụ kiểm tra thông tin cá nhân trong các dịch vụ số: Để bảo vệ quyền lợi của mình, cá nhân cần thường xuyên kiểm tra các cài đặt và chính sách quyền riêng tư trong các dịch vụ mà mình sử dụng, từ đó đảm bảo rằng dữ liệu cá nhân của mình không bị lạm dụng hoặc tiết lộ mà không có sự đồng ý.

Trong khuôn khổ GDPR, quyền và nghĩa vụ của cá nhân đối với dữ liệu cá nhân không chỉ là những yếu tố pháp lý cơ bản, mà còn phản ánh nỗ lực bảo vệ quyền lợi và quyền con người trong môi trường số. Như đã phân tích, GDPR đảm bảo tính bao quát và phù hợp với thực tế số hóa khi đề ra các quyền giúp cá nhân kiểm soát và bảo vệ dữ liệu cá nhân của mình, đặc

biệt trong bối cảnh công nghệ ngày càng phát triển. Các quy định như "quyền được quên", quyền yêu cầu xóa hoặc quyền chuyển dữ liệu đã phản ánh sự tiến bộ trong việc bảo vệ quyền riêng tư và quyền kiểm soát dữ liệu của người dân. Mặc dù các quyền này đã được xây dựng sát với thực tiễn hiện nay, việc thực thi chúng vẫn gặp phải không ít khó khăn, đặc biệt là trong việc cá nhân phải chủ động thực hiện quyền lợi của mình. Cá nhân thường xuyên phải đối mặt với rào cản về nhận thức và thiếu sự hỗ trợ kịp thời từ các tổ chức hoặc cơ quan bảo vệ quyền lợi công dân khi có vi phạm xảy ra. Hơn nữa, mặc dù GDPR đã tạo ra một cơ chế bảo vệ dữ liệu mạnh mẽ trong phạm vi EU, nhưng các tổ chức ngoài EU đôi khi không hoàn toàn tuân thủ những quy định này, dẫn đến việc bảo vệ quyền lợi của cá nhân tại các quốc gia ngoài EU chưa được đảm bảo một cách đầy đủ. Điều này cho thấy GDPR vẫn còn một số hạn chế trong việc bảo vệ quyền của cá nhân, đặc biệt khi dữ liệu được xử lý xuyên biên giới hoặc trong môi trường số toàn cầu.



Chủ thể dữ liệu (cá nhân) có quyền và nghĩa vụ cụ thể - Ảnh: Internet

Tóm lại, mặc dù GDPR đã thiết lập một khuôn khổ pháp lý mạnh mẽ và toàn diện bảo vệ quyền lợi của cá nhân đối với dữ liệu, nhưng việc thực thi các quyền và nghĩa vụ của cá nhân vẫn cần được cải thiện để đảm bảo tính hiệu quả trong việc bảo vệ quyền riêng tư và quyền con người, đặc biệt trong bối cảnh toàn cầu hóa và sự phát triển không ngừng của công nghệ thông tin. Các cơ chế hỗ trợ và giám sát, cùng với việc tăng cường nhận thức cho cá nhân về quyền lợi của mình, là những yếu tố cần thiết để cải thiện việc thực thi GDPR trong tương lai.

- Quyền và nghĩa vụ của các "doanh nghiệp số"

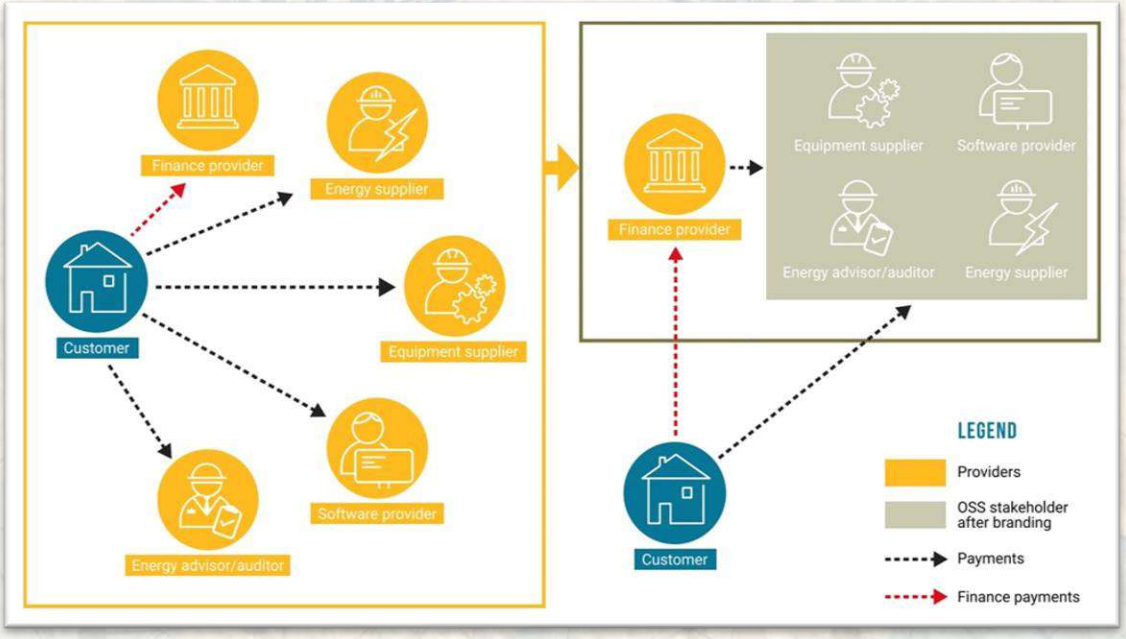
Trong bối cảnh bảo vệ dữ liệu cá nhân và thúc đẩy chia sẻ dữ liệu, cả GDPR và EU Data Act đều đặt ra các quy định rõ ràng về quyền và nghĩa vụ của tổ chức (pháp nhân) trong việc xử lý, bảo vệ và chia sẻ dữ liệu. Tuy cả hai văn bản này tập trung vào các đối tượng khác nhau, nhưng chúng đều hướng đến việc tạo ra một hệ sinh thái bảo vệ dữ liệu hiệu quả và minh bạch.



Hình minh họa doanh nghiệp số - Ảnh: Internet

Đối với GDPR, trọng tâm của GDPR là bảo vệ dữ liệu cá nhân, do đó, quy định đối với tổ chức trong văn bản này khá hạn chế. Mặc dù vậy, vẫn có

sự giao thoa giữa quyền và nghĩa vụ của tổ chức và cá nhân nhằm đảm bảo bao quát, đầy đủ các quyền riêng tư về dữ liệu của cá nhân. Theo đó, GDPR đã đặt ra các yêu cầu nghiêm ngặt đối với các tổ chức trong việc xử lý dữ liệu cá nhân, đảm bảo quyền bảo vệ thông tin của cá nhân, đồng thời cũng tạo ra quyền xử lý dữ liệu trong các phạm vi hợp pháp. Các tổ chức có quyền xử lý dữ liệu nhưng phải tuân thủ các nghĩa vụ bảo vệ quyền lợi cá nhân. Cụ thể, về quyền của tổ chức, *Điều 6 (1)* GDPR cho phép các tổ chức có quyền xử lý dữ liệu cá nhân khi có sự đồng ý hợp pháp từ người dùng hoặc khi việc xử lý là cần thiết cho mục đích thực hiện hợp đồng, nghĩa vụ pháp lý, hoặc lợi ích hợp pháp. Về nghĩa vụ, các tổ chức phải đảm bảo các biện pháp bảo mật thích hợp đối với dữ liệu cá nhân, bao gồm mã hóa và bảo vệ thông tin khỏi rủi ro vi phạm dữ liệu (Điều 32 (1)) và nghĩa vụ thông báo vi phạm dữ liệu (Điều 33 (1)).

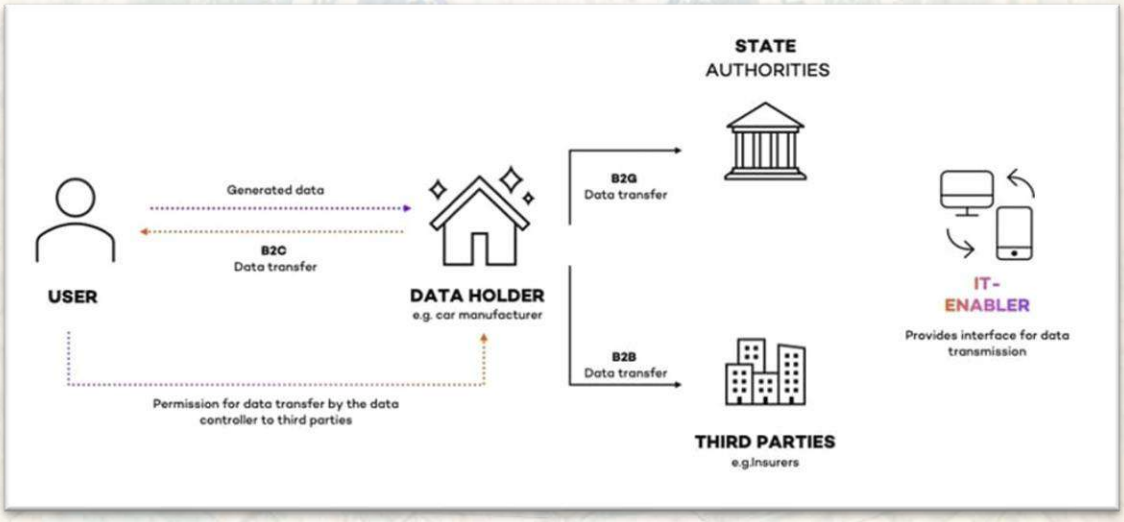


Cơ chế one-stop-shop của các nước - Ảnh: Consumers International

Một nội dung đáng chú ý khác là cơ chế *"một cửa"* (one - stop - shop mechanism), cho phép doanh nghiệp hoạt động tại nhiều quốc gia thành viên

EU chỉ cần làm việc với một Cơ quan bảo vệ dữ liệu quốc gia chủ quản tại nơi đặt trụ sở chính, thay vì phải tương tác với nhiều cơ quan khác nhau. Cơ chế này giúp đơn giản hóa quy trình hành chính, giảm trùng lặp thủ tục và bảo đảm hiệu quả trong quản lý nhà nước.

Về mặt chế tài, GDPR thiết lập khung xử phạt rất nghiêm khắc nhằm bảo đảm tính răn đe và hiệu lực thi hành. Tổ chức vi phạm các quy định về bảo vệ dữ liệu có thể bị phạt lên đến 20 triệu Euro hoặc 4% doanh thu toàn cầu, tùy theo mức nào cao hơn. Đây là một trong những mức xử phạt hành chính cao nhất được quy định trong pháp luật về dữ liệu trên thế giới hiện nay. Thực tiễn đã chứng kiến nhiều vụ việc sau xử lí với mức phạt nặng đối với các tập đoàn công nghệ lớn như Google, Meta (Facebook),... qua đó cho thấy tính "nghiêm khắc" trong việc bảo vệ dữ liệu cá nhân tại EU.



Tương tác của Chủ thể dữ liệu - Ảnh: Diconium

Ngược lại, EU Data Act tạo ra một khuôn khổ pháp lý cho việc chia sẻ và sử dụng dữ liệu, đặc biệt là dữ liệu không phải cá nhân, và thúc đẩy quyền truy cập dữ liệu giữa các bên, quy định cụ thể quyền và nghĩa vụ của các tổ chức trong việc chia sẻ và truy cập dữ liệu.

Về quyền của tổ chức trong EU Data Act, văn bản này cho phép các tổ chức trong phạm vi điều chỉnh được thực hiện các quyền sau:

(i) Quyền chia sẻ dữ liệu với bên thứ ba. Điều 4(1) quy định: *"Data holders shall be required to make data available to users and third parties in accordance with this Regulation, provided that such sharing complies with the conditions laid down in this Regulation"*. Các tổ chức sở hữu dữ liệu có quyền chia sẻ dữ liệu với người sử dụng và bên thứ ba trong phạm vi pháp lý, nhằm hỗ trợ việc phát triển dịch vụ hoặc sản phẩm mới.

(ii) Quyền truy cập dữ liệu từ sản phẩm và dịch vụ kết nối: Tương tự quyền truy cập dữ liệu tại *Điều 6 (1)* đối với cá nhân. Các tổ chức có quyền truy cập dữ liệu được tạo ra trong quá trình sử dụng sản phẩm kết nối hoặc dịch vụ và phải cung cấp dữ liệu đó một cách minh bạch và công bằng.

Về nghĩa vụ của Tổ chức trong EU Data Act, các tổ chức phải có nghĩa vụ bảo vệ quyền lợi cá nhân người sử dụng các sản phẩm, dịch vụ số. *Điều 5(2): "Các tổ chức phải đảm bảo rằng dữ liệu chia sẻ với bên thứ ba không vi phạm quyền riêng tư và bảo vệ dữ liệu cá nhân, tuân thủ các quy định bảo vệ dữ liệu liên quan*". Ngoài ra, các tổ chức có nghĩa vụ cung cấp dữ liệu cho các cơ quan có thẩm quyền:

"Điều 9(1): Tổ chức có nghĩa vụ cung cấp dữ liệu cho các cơ quan có thẩm quyền khi có yêu cầu hợp pháp, ví dụ như cung cấp dữ liệu phục vụ điều tra hoặc thực thi các nghĩa vụ pháp lý".

Từ các quy định trên, có thể thấy rằng cả GDPR và EU Data Act đều quy định các quyền và nghĩa vụ của tổ chức và đều bổ sung cho nhau trong việc thúc đẩy một môi trường dữ liệu an toàn và minh bạch. Tuy nhiên, mỗi văn bản này có mục tiêu và phạm vi áp dụng khác nhau.



Những điểm đáng chú ý của GDPR - Ảnh: Xorlogics

GDPR tập trung vào bảo vệ quyền lợi cá nhân, yêu cầu tổ chức phải bảo vệ dữ liệu cá nhân một cách nghiêm ngặt, đồng thời yêu cầu các tổ chức phải thực hiện các biện pháp bảo mật và thông báo vi phạm khi có sự cố xảy ra. Tổ chức có quyền xử lý dữ liệu cá nhân, nhưng chỉ trong những trường hợp hợp pháp và phải tuân thủ các nghĩa vụ bảo vệ quyền lợi cá nhân theo GDPR. Mặt khác, EU Data Act chủ yếu điều chỉnh việc chia sẻ dữ liệu trong môi trường kỹ thuật số, bảo đảm việc truy cập và sử dụng dữ liệu giữa các tổ chức, người sử dụng và bên thứ ba được thực hiện công bằng và minh bạch. Tuy không đi sâu vào bảo vệ dữ liệu cá nhân, EU Data Act yêu cầu tổ chức

phải bảo vệ dữ liệu không phải cá nhân và đảm bảo tuân thủ các quy định bảo vệ quyền riêng tư khi chia sẻ dữ liệu.

Một điểm mơ hồ khác phát sinh khi GDPR chỉ yêu cầu đảm bảo an ninh trong quá trình xử lý dữ liệu[16], trong khi Chỉ thị NIS hướng đến bảo mật mạng và hệ thống thông tin. Mơ hồ phát sinh khi doanh nghiệp kỹ thuật số phải tuân thủ cả hai văn bản, nhưng không rõ trách nhiệm chính yếu của họ là gì, chỉ bảo vệ dữ liệu (GDPR), hay bảo vệ toàn bộ hạ tầng mạng và thông tin (NIS)? Tuy nhiên, các văn bản sau này lại yêu cầu cả nhà khai thác dịch vụ thiết yếu và nhà cung cấp dịch vụ kỹ thuật số phải đảm bảo an ninh cho mạng và hệ thống thông tin[17].

Một lần nữa, câu hỏi liệu doanh nghiệp kỹ thuật số có liên quan hay không việc đã thực hiện các biện pháp thích hợp để giảm thiểu rủi ro và đã hoàn thành nghĩa vụ của mình về vấn đề này, điều này phụ thuộc vào năng lực và vai trò của họ, bị mờ nhạt do sự mơ hồ về vai trò mà họ có thể đảm nhận. Điều này đặc biệt đúng khi chỉ thị NIS nêu rằng "các yêu cầu bảo mật đối với nhà cung cấp dịch vụ kỹ thuật số nên nhẹ nhàng hơn"[18], và "các nhà cung cấp dịch vụ kỹ thuật số nên chịu sự giám sát hậu kiểm nhẹ và phản ứng dựa trên bản chất dịch vụ và hoạt động của họ"[19], theo đó các cơ quan có thẩm quyền, bên cạnh đó, "không có nghĩa vụ chung phải giám sát các nhà cung cấp dịch vụ kỹ thuật số"[20]. Sự miễn trừ này mang lại cho các nhà cung

[16] Article 32 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[17] Recital 52 of the preamble of the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[18] GDPR, Recital 49.

[19] GDPR, Recital 60.

[20] GDPR, Article 28.

cấp dịch vụ kỹ thuật số rất nhiều quyền tự do và do đó, góp phần vào sự mất cân bằng giữa người dùng và nhà cung cấp, do đó làm tăng thêm rủi ro cho quyền riêng tư Chỉ thị NIS còn tạo ra một lối thoát cho nhà cung cấp dịch vụ kỹ thuật số, bởi vì nó nêu rõ rằng đối với câu hỏi liệu nhà cung cấp đó có ý định cung cấp dịch vụ trong EU hay không, "việc chỉ có thể truy cập vào trang web của nhà cung cấp dịch vụ kỹ thuật số hoặc trung gian, hoặc địa chỉ email và các thông tin liên hệ khác, hoặc việc sử dụng ngôn ngữ thường được sử dụng ở quốc gia thứ ba nơi nhà cung cấp dịch vụ kỹ thuật số đặt trụ sở, là không đủ để xác định ý định đó"[21]. Có thể thấy rằng, các quy định đã mang lại cho các doanh nghiệp kỹ thuật số rất nhiều sự tự do thay vì tăng nghĩa vụ bảo vệ và an ninh tốt hơn cho quyền riêng tư của người dùng. Điều này bất chấp thực tế là chỉ thị này nhằm tôn trọng các quyền và nguyên tắc cơ bản, chẳng hạn như quyền tôn trọng đời sống riêng tư và thông tin liên lạc, và bảo vệ dữ liệu cá nhân[22].

Dựa trên phân tích ở phần này, có thể rút ra kết luận rằng, với sự thiếu nhất quán trong thuật ngữ được sử dụng trong các văn bản pháp luật được xem xét, vai trò và thẩm quyền của các doanh nghiệp số thường bị lu mờ, tạo điều kiện cho họ đóng vai kép nhằm né tránh trách nhiệm và nghĩa vụ pháp lý. Đây là một mối đe dọa trực tiếp đối với quyền riêng tư cá nhân. Bên cạnh đó, sự mất cân bằng giữa chủ thể dữ liệu và bên xử lý dữ liệu là một vấn đề nan giải chưa được các luật này giải quyết một cách đầy đủ, và chính điều đó có thể làm gia tăng nguy cơ xâm phạm quyền riêng tư. Do đó, những tác động tiêu cực mà sự mơ hồ và đơn giản hóa các khái niệm pháp lý gây ra đối với quyền riêng tư không nên bị xem nhẹ hay bỏ qua.

[21] GDPR., Recital 65.

[22] GDPR., Recital 75.

- Tác động của Đạo luật dữ liệu đối với nền kinh tế và xã hội

Đạo luật dữ liệu của EU có thể có những tác động sâu rộng đến nền kinh tế và xã hội, đặc biệt là trong việc thúc đẩy sự đổi mới sáng tạo và cải thiện hiệu quả trong các ngành công nghiệp số:

+ *Tăng trưởng kinh tế số:* Đạo luật Dữ liệu sẽ tạo ra cơ hội cho các doanh nghiệp trong việc phát triển các dịch vụ và sản phẩm mới dựa trên dữ liệu, từ đó thúc đẩy tăng trưởng kinh tế số.

+ *Cải thiện tính minh bạch và công bằng:* Việc chia sẻ dữ liệu công sẽ giúp tăng cường sự minh bạch và công bằng trong các hoạt động của chính phủ và doanh nghiệp, từ đó xây dựng lòng tin của người dân.

+ *Khuyến khích đổi mới sáng tạo:* Các doanh nghiệp và tổ chức có thể sử dụng dữ liệu mở để phát triển các giải pháp sáng tạo phục vụ cho nhu cầu của người dùng và xã hội.

Nhìn chung, Đạo luật Dữ liệu của Liên minh Châu Âu là một bước đi quan trọng trong việc xây dựng một thị trường dữ liệu thống nhất và công bằng tại EU. Với các quy định về quyền sở hữu, quyền truy cập và bảo mật dữ liệu, Đạo luật Dữ liệu không chỉ giúp thúc đẩy sự chia sẻ dữ liệu mà còn bảo vệ quyền lợi của người tiêu dùng và các tổ chức. Nó tạo ra một cơ hội lớn cho các doanh nghiệp và tổ chức phát triển các sản phẩm, dịch vụ và ứng dụng sáng tạo trên dữ liệu, đồng thời thúc đẩy nền kinh tế số và sự cạnh tranh lành mạnh trong khu vực.

1.2.1.2. Luật Quản trị dữ liệu (DGA)

Bên cạnh hai đạo luật phổ biến trên, EU còn xây dựng và ban hành Luật Quản trị dữ liệu (Data Governance Act - DGA), đây là một bước đi quan trọng của EU trong việc điều chỉnh và quản lý dữ liệu trong kỷ nguyên số, giúp tạo ra một khuôn khổ pháp lý hiệu quả và minh bạch cho việc chia

sẻ và sử dụng dữ liệu trên toàn khu vực. Được thông qua vào tháng 11/2020, DGA là một phần trong chiến lược tổng thể của EU nhằm phát triển một nền kinh tế dữ liệu, bảo đảm rằng dữ liệu được sử dụng một cách hợp lý, an toàn và có lợi cho cả cá nhân và tổ chức.

DGA là một phần trong chương trình "Châu Âu số" của EU nhằm thúc đẩy sự phát triển của dịch vụ và ứng dụng số, đồng thời bảo vệ quyền lợi của người tiêu dùng và bảo đảm sự minh bạch trong việc sử dụng dữ liệu. Đặc biệt, DGA còn nhằm mục đích xây dựng một cơ chế quản lý dữ liệu hợp lý, giúp các tổ chức, doanh nghiệp và công dân dễ dàng hơn trong việc truy cập, chia sẻ và sử dụng dữ liệu mà không vi phạm các quyền riêng tư.

- Mục tiêu và tầm quan trọng của Luật quản trị dữ liệu (DGA)

Mục tiêu chính của DGA là tạo ra một cơ chế pháp lý giúp cải thiện và thúc đẩy sự chia sẻ dữ liệu giữa các tổ chức, doanh nghiệp và các quốc gia trong EU, đồng thời bảo đảm tính bảo mật, quyền riêng tư và quyền lợi của người dùng. Cụ thể, DGA có những mục tiêu quan trọng như:

(1) Khuyến khích chia sẻ dữ liệu: DGA được xây dựng nhằm tạo ra một môi trường thuận lợi để các tổ chức, doanh nghiệp và Chính phủ chia sẻ dữ liệu một cách an toàn và có kiểm soát. Điều này giúp thúc đẩy sự phát triển của các dịch vụ và ứng dụng dựa trên dữ liệu, đặc biệt trong các lĩnh vực như: y tế, giao thông, môi trường và giáo dục.

(2) Bảo vệ quyền riêng tư: DGA bảo đảm rằng việc chia sẻ và sử dụng dữ liệu không xâm phạm quyền riêng tư của công dân. Điều này giúp duy trì sự tin tưởng của người dân đối với các hệ thống dữ liệu và công nghệ số.

(3) Tạo các cơ chế quản lý dữ liệu minh bạch: DGA yêu cầu các tổ chức phải có các quy trình rõ ràng và minh bạch trong việc thu thập, sử dụng

và chia sẻ dữ liệu. Điều này giúp người tiêu dùng và các tổ chức khác có thể theo dõi cách thức dữ liệu của mình được xử lý.

(4) Khuyến khích các sáng kiến hợp tác và đổi mới: DGA khuyến khích các sáng kiến hợp tác giữa các doanh nghiệp, chính phủ và các tổ chức nghiên cứu, từ đó thúc đẩy sự sáng tạo và đổi mới trong việc sử dụng dữ liệu.

- Các yếu tố nổi bật trong DGA

Luật quản trị dữ liệu của EU bao gồm nhiều điểm quan trọng giúp định hình cách thức quản lý và chia sẻ dữ liệu, bao gồm các quy định về quyền và nghĩa vụ của các tổ chức, cơ chế chia sẻ dữ liệu và các biện pháp bảo vệ quyền lợi của người dùng.

Thứ nhất, về các quyền và nghĩa vụ của các tổ chức.

DGA quy định các quyền và nghĩa vụ của các tổ chức khi tham gia vào việc chia sẻ và quản lý dữ liệu. Đó là các tổ chức sẽ có thể tham gia vào một cơ chế chia sẻ dữ liệu minh bạch và có kiểm soát nhưng cũng phải bảo đảm rằng họ tuân thủ các nguyên tắc bảo mật và quyền riêng tư của người dùng.

(1) Khuyến khích các tổ chức chia sẻ dữ liệu: Các tổ chức có thể chia sẻ dữ liệu của mình thông qua các nền tảng được tạo ra bởi EU nhưng phải tuân thủ các nguyên tắc bảo mật và yêu cầu pháp lý. Các tổ chức có thể hợp tác với nhau để tạo ra những dịch vụ hoặc sản phẩm mới dựa trên dữ liệu chia sẻ.

(2) Bảo vệ quyền lợi của người tiêu dùng: Các tổ chức phải bảo đảm rằng dữ liệu của người tiêu dùng không bị sử dụng trái phép hoặc không rõ ràng họ phải thông báo cho người dùng về cách thức dữ liệu của họ được thu thập, sử dụng và chia sẻ

Thứ hai, về các nền tảng chia sẻ dữ liệu.

DGA thiết lập các nền tảng chia sẻ dữ liệu trong khu vực EU, giúp kết nối các bên tham gia vào quá trình chia sẻ dữ liệu từ các doanh nghiệp, tổ chức công đến người dân. Các nền tảng này giúp thúc đẩy việc sử dụng dữ liệu trong các lĩnh vực y tế, môi trường và giao thông, đồng thời tạo ra một môi trường an toàn và có kiểm soát.

+ ***Nền tảng dữ liệu công cộng:*** Đây là những nền tảng cho phép các cơ quan công quyền và tổ chức phi lợi nhuận chia sẻ dữ liệu một cách minh bạch và có kiểm soát.

+ ***Nền tảng dữ liệu doanh nghiệp:*** DGA khuyến khích các doanh nghiệp chia sẻ dữ liệu với nhau trong các lĩnh vực như nghiên cứu, phát triển sản phẩm và dịch vụ, hoặc hợp tác trong các sáng kiến đổi mới.

Thứ ba, về các biện pháp bảo vệ quyền lợi của người tiêu dùng.

DGA chú trọng đến việc bảo vệ quyền lợi và quyền riêng tư của người dùng trong quá trình chia sẻ dữ liệu. Các công dân EU có quyền yêu cầu quyền truy cập, chỉnh sửa hoặc xóa dữ liệu của mình và các tổ chức phải bảo đảm rằng họ tuân thủ đầy đủ các yêu cầu này.

+ ***Quyền được biết và quyền được kiểm soát:*** Các công dân có quyền được thông báo về dữ liệu mà họ cung cấp cho các tổ chức và có quyền kiểm soát cách thức dữ liệu của mình được sử dụng.

+ ***Giới hạn quyền sử dụng dữ liệu:*** DGA quy định các giới hạn nghiêm ngặt với việc sử dụng dữ liệu cá nhân của người dùng, bảo đảm rằng dữ liệu không bị sử dụng sai mục đích hoặc bị lạm dụng.

- Tác động của DGA đối với nền kinh tế và xã hội

Luật Quản trị dữ liệu của EU không chỉ tạo ra một khung pháp lý cho việc quản lý dữ liệu, mà còn có tác động sâu rộng đến nền kinh tế và xã hội EU. DGA mở ra cơ hội lớn cho các doanh nghiệp và tổ chức nghiên cứu

trong việc phát triển các sản phẩm và dịch vụ mới, nhờ vào việc chia sẻ và khai thác dữ liệu một cách hiệu quả.

(1) Thúc đẩy đổi mới sáng tạo: Việc chia sẻ dữ liệu có thể giúp các doanh nghiệp và tổ chức nghiên cứu phát triển các công nghệ và sản phẩm mới, đặc biệt trong các lĩnh vực như y tế, giao thông và năng lượng.

(2) Tăng trưởng kinh tế: Với việc thúc đẩy, chia sẻ và sử dụng dữ liệu hiệu quả, DGA có thể đóng góp vào việc tăng trưởng kinh tế của EU, tạo ra cơ hội kinh doanh mới và các dịch vụ công cộng cải tiến.

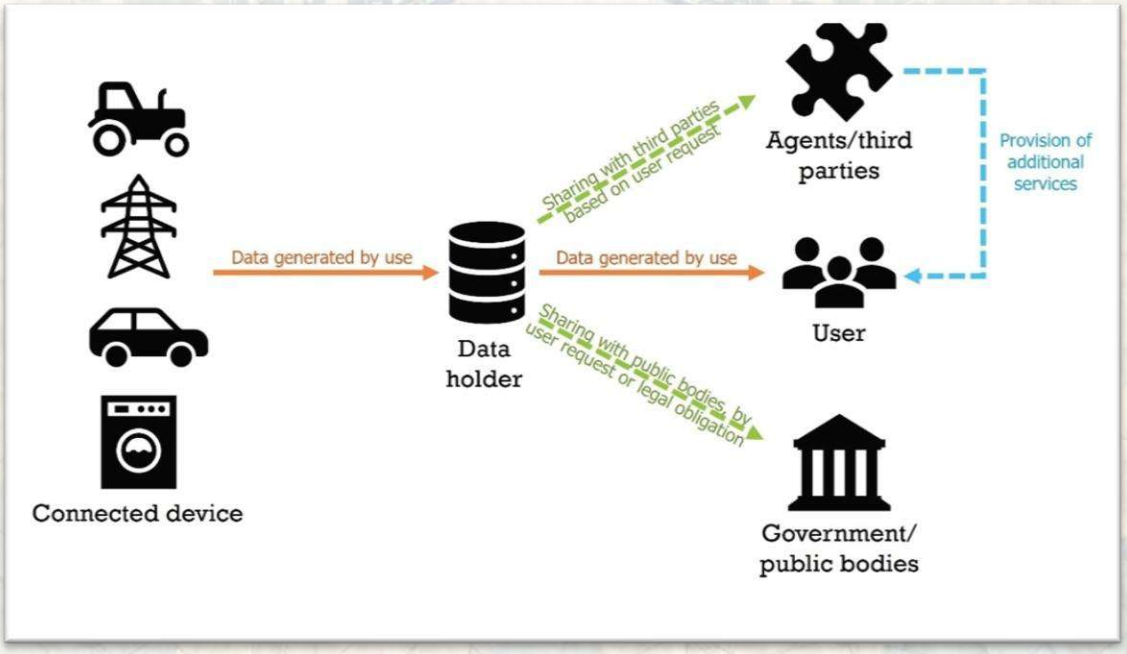
(3) Cải thiện chất lượng cuộc sống: Việc chia sẻ dữ liệu trong các lĩnh vực như chăm sóc sức khỏe, môi trường và giao thông có thể giúp cải thiện chất lượng cuộc sống của người dân, đồng thời giảm thiểu tác động tiêu cực đến môi trường và xã hội.

Nhìn chung, DGA của EU là một bước tiến quan trọng trong việc xây dựng một khuôn khổ pháp lý minh bạch và an toàn để quản lý dữ liệu trong kỷ nguyên số. DGA không chỉ bảo đảm quyền lợi và quyền riêng tư của công dân mà còn tạo cơ hội cho các doanh nghiệp và tổ chức hợp tác để phát triển các sản phẩm và dịch vụ mới. Với DGA, EU mong muốn chung là xây dựng một nền kinh tế dữ liệu mạnh mẽ, thúc đẩy sự đổi mới sáng tạo và phát triển bền vững trong khu vực.

1.2.1.3. Những điểm mạnh của mô hình pháp luật dữ liệu tại EU

Khung pháp lý DGA, GDPR, EU Data Act, Liên minh Châu Âu không chỉ đặt những tiêu chuẩn, mức độ bảo vệ rất cao cho quyền riêng tư và dữ liệu cá nhân, mà còn tạo ra một mô hình pháp luật mạnh mẽ, được coi là một trong những đạo luật *"hà khắc"* nhất thế giới. Mô hình pháp luật dữ liệu của EU, thể hiện qua GDPR, mang lại nhiều điểm mạnh vượt trội cả về phương diện lập pháp, hành pháp và ảnh hưởng sâu rộng với cả các quốc gia thành viên và bên ngoài Khối EU.

Thứ nhất, về tính hệ thống và đồng bộ, GDPR được xây dựng như một quy định có hiệu lực trực tiếp tại tất cả các quốc gia thành viên EU, thay thế cho hệ thống chỉ thị vốn bị phân tán trước đây. Điều này tạo ra một khuôn khổ thống nhất, đồng bộ trong việc bảo vệ dữ liệu cá nhân trên toàn khối, đồng thời nâng cao hiệu quả thực thi và giảm thiểu sự khác biệt giữa các hệ thống pháp luật quốc gia. Tương tự, EU Data Act cũng đóng vai trò quan trọng trong việc thúc đẩy sự chia sẻ dữ liệu công bằng và minh bạch trong các doanh nghiệp và các tổ chức. EU Data Act không chỉ giúp mở rộng quyền truy cập và chia sẻ dữ liệu mà còn tạo ra những quy định cụ thể về bảo mật dữ liệu, nhằm tạo ra một môi trường tin cậy và công bằng. Cùng với GDPR, EU Data Act giúp thiết lập một hệ thống pháp lý vững mạnh để hỗ trợ cả tổ chức và cá nhân trong việc xử lý và chia sẻ dữ liệu một cách hợp lý, bảo vệ quyền lợi của tất cả các bên liên quan.



Cơ chế hoạt động của Đạo luật Dữ liệu châu Âu - Ảnh: Transforma Insight

Thứ hai, tăng cường quyền năng thực chất cho cá nhân, tổ chức. GDPR đặt trọng tâm vào việc bảo vệ quyền lợi thực tế của cá nhân, bảo đảm cho

người dân quyền kiểm soát dữ liệu của mình một cách chủ động, minh bạch, buộc tổ chức phải chịu trách nhiệm về cách xử lý dữ liệu. Điều này tạo ra sự thay đổi căn bản trong cách tiếp cận quyền riêng tư dữ liệu, đó là từ quyền mang tính hình thức sang quyền có hiệu lực trong thực tiễn. Người dùng không chỉ được thông báo về việc dữ liệu của họ bị thu thập, mà còn có thể yêu cầu chỉnh sửa, xóa bỏ, hoặc ngăn chặn việc tiếp tục sử dụng dữ liệu không mong muốn. Tính chất quyền lực này của cá nhân không chỉ được duy trì trong GDPR mà còn được mở rộng trong EU Data Act, nơi cá nhân có quyền truy cập vào dữ liệu mà họ tạo ra qua việc sử dụng các sản phẩm kết nối hoặc dịch vụ. EU Data Act còn đảm bảo rằng các tổ chức không chỉ phải thông báo mà còn phải minh bạch và công bằng trong việc chia sẻ dữ liệu với người sử dụng, bảo vệ quyền lợi của người dân khi dữ liệu của họ được sử dụng cho mục đích khác ngoài nhu cầu ban đầu.



Luật bảo vệ dữ liệu Brazil (LGPD) kế thừa và phát triển nhiều quy định pháp luật dựa trên GDPR - Ảnh: Monitora

Thứ ba, tầm ảnh hưởng toàn cầu. Với cách tiếp cận toàn diện và có phạm vi ngoài lãnh thổ, GDPR đã trở thành một khuôn mẫu pháp lý ảnh hưởng rộng khắp trên toàn cầu. Nhiều quốc gia như Brazil (Luật bảo vệ dữ liệu cá nhân - LGPD), Nhật Bản (Đạo luật về bảo vệ thông tin cá nhân - APPI), Indonesia, Thổ Nhĩ Kỳ, Tanzania… đã ban hành hoặc sửa đổi pháp luật dữ liệu theo hướng tiệm cận với quy định của EU. Điều này thể hiện khả năng *"toàn cầu hóa"* và gia tăng ảnh hưởng, củng cố vai trò định hình trật tự pháp lý toàn cầu trong môi trường không gian mạng của EU mà không làm tổn hại đến quyền lợi công dân.

Thứ tư, nhờ chế tài và hệ thống nghĩa vụ chặt chẽ, GDPR và sau đó là EU Data Act đã tạo ra một thay đổi đáng kể trong hành vi của các tổ chức, đặc biệt là các doanh nghiệp về công nghệ. Với các cơ quan độc lập (như CNIL) cho phép EU thanh tra, xử phạt nghiêm khắc các vi phạm của các công ty công nghệ, điển hình, năm 2019, Google bị phạt 50 triệu EUR vì vi phạm GDPR trong quá trình người dùng cài đặt mới thiết bị Android[23]. Việc buộc các tập đoàn lớn phải minh bạch giúp cải thiện hệ thống kiểm soát nội bộ và tôn trọng quyền người dùng, góp phần hình thành văn hóa bảo vệ dữ liệu trong nền kinh tế số.

Thứ năm, khả năng thích ứng và đổi mới trong khuôn khổ pháp lý. GDPR và EU Data Act không chỉ là các đạo luật cứng nhắc mà còn được thiết kế để linh hoạt và thích ứng với sự phát triển nhanh chóng của công nghệ. Chúng cung cấp các nguyên tắc cơ bản và khung pháp lý, cho phép các quốc gia thành viên và tổ chức tự chủ trong việc triển khai, phù hợp với đặc thù địa phương và ngành nghề. Điều này giúp duy trì tính ổn định của

[23] Vietnamnet (2019). Google bị phạt 50 triệu Euro vì vi phạm luật bảo vệ dữ liệu của EU. https://vietnamnet.vn/google-bi-phat-50-trieu-eur-vi-vi-pham-luat-bao-ve-du-lieu-cua-eu-i27065.html

hệ thống pháp luật trong khi vẫn đảm bảo khả năng đổi mới và ứng phó kịp thời với các thách thức mới.



Google bị phạt vì vi phạm GDPR cho thấy đạo luật này có chế tài pháp lý rất chặt chẽ - Ảnh: Báo Hà Nội Mới

Thứ sáu, khuyến khích đổi mới và cạnh tranh trong nền kinh tế dữ liệu. EU Data Act đặc biệt chú trọng đến việc thúc đẩy đổi mới và cạnh tranh trong nền kinh tế dữ liệu[24]. Bằng cách giảm bớt các rào cản kỹ thuật và pháp lý trong việc chia sẻ và sử dụng dữ liệu, đạo luật này khuyến khích các doanh nghiệp sáng tạo và cạnh tranh công bằng. Điều này không chỉ mang lại lợi ích cho người tiêu dùng mà còn thúc đẩy sự phát triển của các ngành công nghiệp dựa trên dữ liệu, từ đó đóng góp vào sự tăng trưởng kinh tế bền vững của EU.

[24] Dupree, L. P., Javed, H., & Adeyemi, C. O. (2025), *The EU Data Act: Implications and preparation for businesses,* Finnegan, https://www.finnegan.com/en/insights/articles/the-eu-data-act-implications-and-preparation-for-businesses.html, truy cập ngày 14/7/2025.

1.2.1.4. Một số hạn chế và thách thức trong quá trình thực thi chính sách, pháp luật về dữ liệu tại EU

Mặc dù có nhiều ưu điểm, mô hình pháp luật dữ liệu của EU cũng tồn tại một số điểm hạn chế và đặt ra không ít thách thức trong thực tiễn triển khai. ***Thứ nhất,*** mặc dù GDPR và EU Data Act là một quy định có hiệu lực trực tiếp, việc thực thi vẫn gặp khó khăn do sự khác biệt trong cơ cấu pháp lý và hành chính giữa các quốc gia thành viên. Những quốc gia có cấu trúc liên bang hoặc đa ngôn ngữ như Bỉ, Đức… thường gặp khó khăn trong việc phối hợp giữa các cấp cơ quan bảo vệ dữ liệu (DPA), làm giảm hiệu quả thực thi thống nhất trong toàn EU. Mặc khác, ở một số nước thành viên (Hy Lạp, Italia) việc thực thi quyền của cá nhân bị trì hoãn do thủ tục hành chính - tư pháp tốn nhiều thời gian, khiến người dân phải đợi rất lâu để được bảo vệ hoặc đền bù khi quyền riêng tư bị xâm phạm. Ở Pháp, việc sửa đổi Luật 1978 liên tục để phù hợp GDPR mà không thay đổi cấu trúc khiến luật trở nên khó đọc, dễ gây nhầm lẫn và gánh nặng truyền thông thêm cho CNIL.



Cơ quan bảo vệ dữ liệu quốc gia của Pháp - Ảnh: Data Legal Drive

Thứ hai, các chi phí để xây dựng cơ cấu tổ chức đảm bảo tiêu chuẩn GDPR và EU Data Act khá cao là một trở ngại đáng kể đối với các doanh nghiệp nhỏ và vừa. Việc phải bổ nhiệm cán bộ DPO, xây dựng quy trình DPIA, cập nhật hệ thống bảo mật… đòi hỏi nguồn lực tài chính và nhân sự không nhỏ, đặc biệt tại các thị trường có nền kinh tế đang phát triển hoặc doanh nghiệp chưa sẵn sàng chuyển đổi số toàn diện.

Thứ ba, một số nhà nghiên cứu và tổ chức trong ngành công nghệ cho rằng GDPR có thể làm cản trở đổi mới sáng tạo, do những hạn chế trong việc thu thập, phân tích và tái sử dụng dữ liệu. Đặc biệt là đối với những công nghệ mới như trí tuệ nhân tạo, học máy, dữ liệu lớn… Khi các yêu cầu pháp lý trở nên quá nghiêm ngặt, doanh nghiệp có thể trở nên dè dặt trong nghiên cứu, thử nghiệm và triển khai các mô hình kinh doanh dựa trên dữ liệu. Các rào cản này có thể làm chậm quá trình phát triển của các công nghệ mới và ảnh hưởng đến khả năng cạnh tranh của EU trong thị trường toàn cầu.

Thứ tư, việc mở rộng hiệu lực ngoài lãnh thổ của GDPR cũng tạo ra các xung đột pháp lý quốc tế, nhất là trong các giao dịch dữ liệu xuyên biên giới. Điển hình là các vụ việc như tranh chấp giữa DPA Bỉ và Facebook Ireland, hay vụ SWIFT - một cơ quan viễn thông thuộc hệ thống tài chính toàn cầu có trụ sở tại Bỉ đã bị cáo buộc chuyển dữ liệu cho Cơ quan Tình báo trung ương Hoa Kỳ (CIA)[25], đã đặt ra vấn đề về chủ quyền pháp lý và tương thích luật giữa các hệ thống khác nhau. Điều này đòi hỏi cần có các hiệp định quốc tế hoặc cơ chế điều phối pháp luật để bảo đảm sự hài hòa và tôn trọng quyền chủ thể trong không gian số toàn cầu. Các cơ chế này cần được thiết lập để tạo ra

[25] Hà Nhi (2020), *Mỹ thừa nhận CIA theo dõi các giao dịch tài chính thông qua SWIFT,* Báo Nhân Dân, https://nhandan.vn/my-thua-nhan-cia-theo-doi-cac-giao-dich-tai-chinh-thong-qua-swift-post489020.html, truy cập ngày 15/07/2025.

một khung pháp lý thống nhất, đồng thời bảo vệ quyền lợi của người dân khi dữ liệu của họ được xử lý và chia sẻ xuyên biên giới, giúp giải quyết các xung đột pháp lý giữa các hệ thống pháp luật quốc gia.

Mặc dù GDPR và EU Data Act là một mô hình pháp lý mạnh mẽ và tiên phong trong bảo vệ quyền riêng tư và dữ liệu cá nhân, nhưng việc thực thi nó vẫn đối mặt với không ít thách thức. Những khó khăn liên quan đến sự khác biệt giữa các quốc gia thành viên, chi phí cao trong việc tuân thủ quy định, tác động đối với đổi mới sáng tạo và nghiên cứu công nghệ, cùng với các xung đột pháp lý quốc tế, đều là những vấn đề cần được giải quyết để nâng cao hiệu quả thực thi chính sách, pháp luật về dữ liệu. Việc phát triển các cơ chế hợp tác quốc tế và tạo ra sự hài hòa giữa các hệ thống pháp lý sẽ là yếu tố then chốt trong việc duy trì tính hiệu quả của GDPR trong bối cảnh toàn cầu hóa và chuyển đổi số hiện nay.

1.2.2. Hoa Kỳ

Pháp luật về bảo vệ thông tin cá nhân tại Hoa Kỳ liên quan đến việc thu thập và sử dụng dữ liệu của chính phủ và các doanh nghiệp tư nhân. Trái ngược với luật pháp châu Âu, áp dụng cách tiếp cận tổng quát đối với quyền riêng tư và bảo vệ dữ liệu, pháp luật về bảo vệ quyền riêng tư của Hoa Kỳ sử dụng cách tiếp cận theo ngành[26]. Nói cách khác, hầu hết các luật về quyền riêng tư của Hoa Kỳ đều điều chỉnh việc xử lý dữ liệu dựa trên bối cảnh sử dụng dữ liệu[27].

Nhìn chung, quy định về quyền riêng tư tại Hoa Kỳ có thể được mô tả là mang tính bối cảnh cao, theo ngành (ngân hàng, y tế, giáo dục…), bắt nguồn từ các điều khoản trong luật chung và quy chế riêng của từng liên

[26] Schwartz 2009, p. 905.

[27] Schwartz and Solove 2014, p. 879.

bang và tiểu bang[28], phần lớn dựa trên luật tư hoặc các thỏa thuận có tính ràng buộc rõ ràng sau đó được thực thi bởi luật liên bang hoặc tiểu bang[29]. Luật liên bang chủ yếu được thực hiện bởi Ủy ban Thương mại Liên bang (FTC), trong khi các Tổng chưởng lý (Viên chức tư pháp cao cấp của tiểu bang) cũng đóng vai trò tích cực trong việc bảo vệ quyền riêng tư của người dân. Các nguyên tắc về quyền riêng tư thông tin, cung cấp một bộ nguyên tắc tiêu chuẩn làm cơ sở cho nhiều luật về quyền riêng tư và bảo vệ dữ liệu, bao gồm cả luật ở Hoa Kỳ, EU và các nơi khác trên thế giới, lần đầu tiên được đặt ra vào năm 1973 bởi một ủy ban cố vấn của Bộ Y tế, Giáo dục và Phúc lợi Hoa Kỳ[30] và sau đó được ghi nhận trong Đạo luật Quyền riêng tư Hoa Kỳ năm 1974[31].



Pháp luật về bảo vệ thông tin cá nhân tại Hoa Kỳ đều có cách tiếp cận khác biệt so với các điều khoản của GDPR - Ảnh: Internet

[28] DeVries 2003, p. 285.

[29] Cate, 2011.

[30] Sec'y Advisory Comm. On Automated Personal Data Sys., U.S. Dept. of Health, Educ. & Welfare, Records, Computers, and the Rights of Citizens (1973), https://aspe.hhs.gov/report/records-computers-and-rights-citizens.

[31] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

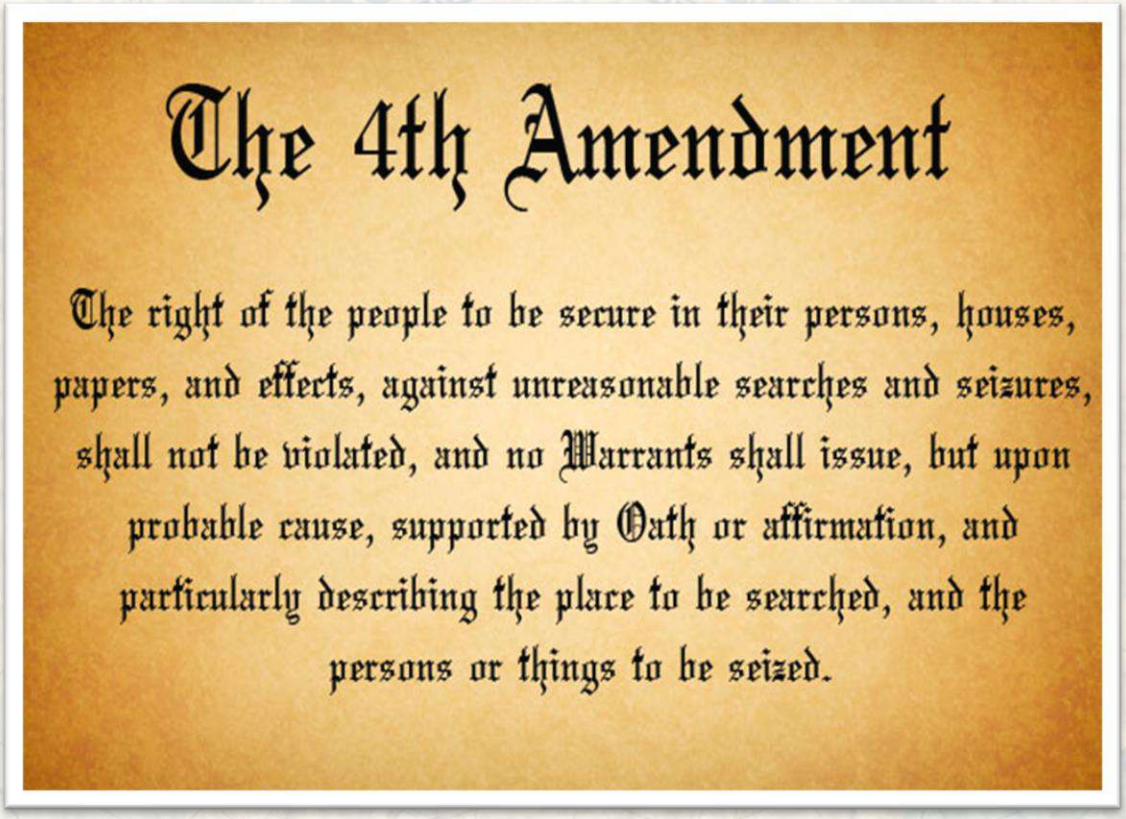
Trong những năm gần đây, một số luật quyền riêng tư mới của một số tiểu bang đã được thông qua, trong đó có luật ở tiểu bang California, Nevada và Maine. Đạo luật mở rộng nhất trong số này, Đạo luật Quyền riêng tư của Người tiêu dùng California năm 2018 (CCPA), cung cấp cho người tiêu dùng California các quyền truy cập, xóa bỏ và từ chối bán dữ liệu cá nhân của họ, cùng nhiều quyền khác, đồng thời áp đặt các nghĩa vụ bổ sung cho các doanh nghiệp thu thập và bán thông tin cá nhân. Với việc CCPA có hiệu lực vào ngày 01/01/2020, một số thành viên Quốc hội đã và đang nỗ lực thông qua luật riêng tư liên bang. Một số đề xuất lập pháp liên bang này sẽ hệ thống hóa các biện pháp bảo vệ quyền riêng tư của tiểu bang thành luật ở cấp liên bang, trong khi một số khác sẽ ưu tiên luật tiểu bang bằng cách thiết lập giới hạn trên hoặc dưới cho quyền riêng tư và bảo vệ dữ liệu tại Hoa Kỳ[32]. Tuy nhiên, tại thời điểm này, các thành viên Quốc hội vẫn chưa đạt được sự đồng thuận về những điều khoản và biện pháp bảo vệ quyền riêng tư mà một đạo luật liên bang mới về quyền riêng tư nên có[33].

1.2.2.1. Tu chính án thứ Tư (The Fourth Amendment)

Ranh giới của quyền riêng tư tại Hoa Kỳ được xác định một phần bởi Tu chính án thứ Tư của Hiến pháp Hoa Kỳ, bảo vệ cá nhân khỏi *"các cuộc khám xét và tịch thu vô lý"* của chính phủ[34]. Nếu chính quyền địa phương, tiểu bang hoặc liên bang tham gia vào việc thu thập và sử dụng dữ liệu, quyền Tu chính án thứ Tư của cá nhân có thể được áp dụng. Một khiếu nại về quyền riêng tư có liên quan đến Tu chính án thứ Tư, viện dẫn cái được gọi là tiêu chuẩn hợp lý và bài kiểm tra kỳ vọng về quyền riêng tư, bắt nguồn từ vụ kiện

[32] Chander, Kaminski, and McGeveran 2019, p. 37.
[33] Fazlioglu 2019, p. 5.
[34] U.S. Constitution, Amendment IV.

Katz kiện Hoa Kỳ. Trong quyết định của mình về vụ án, Tòa án Tối cao phán quyết rằng việc chính phủ nghe lén (không có lệnh) của một người đang gọi điện từ buồng điện thoại đã vượt quá kỳ vọng chủ quan của bị đơn về quyền riêng tư, điều này có thể được coi là hợp lý theo các chuẩn mực xã hội hiện hành[35]. Do đó, các khiếu nại về quyền riêng tư ở Hoa Kỳ thường được đánh giá theo tiêu chuẩn của một "bên thứ ba khách quan", một người có "cách nhìn nhận hợp lý"[36]. Trong một vụ án mang tính bước ngoặt gần đây của Tòa án Tối cao Hoa Kỳ, việc cảnh sát truy cập vào hồ sơ lịch sử trong điện thoại di động và vị trí thực tế của các cá nhân mà không có lệnh khám xét được coi là vi phạm Tu chính án thứ Tư[37].



Tu chính án thứ Tư - Ảnh: The Leventhal Film

[35] Trong ý kiến đồng thuận của mình, Thẩm phán Harlan giải thích rằng một kỳ vọng hợp lý về quyền riêng tư được xác định dựa trên cả kỳ vọng chủ quan và kỳ vọng khách quan về quyền riêng tư. (389 U.S. 347, 361 (1967)).

[36] Haynes v Alfred Knopf, 8 F. 3d. 1222 (1993).

[37] Carpenter v United States, 138 S. Ct. 2206 (2018).

Tòa án Tối cao Hoa Kỳ cũng đã bảo vệ quyền riêng tư của các cá nhân liên quan đến các vấn đề như kiểm soát sinh sản, các mối quan hệ đồng giới và phá thai, như một phần mờ nhạt của các quyền bắt nguồn hoặc ngụ ý theo Hiến pháp[38]. Những quyền này cũng được gọi là quyền riêng tư *"không được liệt kê"*[39] mà, thay vào đó, thường được gọi trong luật pháp châu Âu là các quyền cơ bản[40].

1.2.2.2. Luật chuyên ngành

Có lẽ đặc điểm đáng chú ý nhất của luật bảo vệ dữ liệu và quyền riêng tư của Hoa Kỳ là phạm vi điều chỉnh. Các quy định về quyền riêng tư của Hoa Kỳ chủ yếu mang tính định hướng theo ngành[41], tức là, nhiều quy định khác nhau được áp dụng cho các hoạt động xử lý dữ liệu của các cơ quan chính phủ và các công ty tư nhân[42]. Hơn nữa, các doanh nghiệp nằm trong các lĩnh vực khác nhau của nền kinh tế hoặc xử lý các loại dữ liệu khác nhau phải tuân theo các quy tắc khác nhau[43]. Do đó, luật theo ngành quy định mức

---

[38] Griswold V. Connecticut, 381 U.S. 479 (1965); *Lawrence V. Texas*, 539 U.S. 558 (2003); Roe v Wade, 410 U.S. 113 (1973).

[39] Helscher (1994). *Tài liệu đã dẫn*

[40] While privacy in Europe connotes respect for personal dignity, the meaning of privacy in the U.S is more inclined towards liberty from intervention by the state. Whitman 2004, pp. 1160 – 1163.

[41] Các ví dụ được xem xét ở phần khác trong nghiên cứu này bao gồm Đạo luật Báo cáo Tín dụng Công bằng (FCRA), Đạo luật Gramm-Leach-Bliley (GLBA), và Đạo luật Bảo vệ Quyền riêng tư trong Giao tiếp Điện tử (ECPA).

[42] Schwartz 2013, p. 1974. Tuy nhiên, một vấn đề đối với sự phân biệt này là ranh giới giữa hoạt động của chính phủ và hoạt động của khu vực tư nhân ngày càng trở nên mờ nhạt. Ví dụ, đã có báo cáo cho thấy 98% thông tin tình báo trong chương trình PRISM – một trong những chương trình giám sát quy mô lớn của Cơ quan An ninh Quốc gia Hoa Kỳ (NSA) được Edward Snowden tiết lộ – đến từ các công ty tư nhân như Yahoo, Google và Microsoft. Gellman B and Poitras L (2013) U.S., *British Intelligence Mining Data from Nine U.S Internet Companies in Broad Secret Program* https://www.washingtonpost.com/investigations/us-intelligence-miningdata-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497 story.html. Accessed 4 June 2018.

[43] Schwartz 2013, p. 1974. Ví dụ, việc phân phối các sản phẩm nghe nhìn đã được ghi hình sẵn được điều chỉnh bởi Đạo luật Bảo vệ Quyền riêng tư về Video (Video Privacy Protection Act – VPPA). Tuy nhiên, nếu video đó được phân phối qua hệ thống truyền hình cáp, thì Đạo luật Chính sách Truyền thông Cáp (Cable

độ bảo vệ cần thiết cho các hoạt động xử lý dữ liệu riêng biệt, từ giao dịch tài chính của người tiêu dùng đến thực thi pháp luật và lưu trữ hồ sơ y tế[44]. Về bản chất, luật theo ngành coi các mối đe dọa đối với quyền riêng tư và bảo vệ dữ liệu là đặc thù của ngành hoặc đối với một số loại ngành hoặc công nghệ xử lý dữ liệu nhất định[45].

Các loại thông tin phải chịu nghĩa vụ xử lý chặt chẽ hơn tại Hoa Kỳ "thường là thông tin được coi là có bản chất "riêng tư", chẳng hạn như thông tin sức khỏe cá nhân[46]. Các luật liên bang dành riêng cho từng lĩnh vực tại Hoa Kỳ điều chỉnh việc xử lý dữ liệu cá nhân bao gồm Đạo luật về khả năng chuyển giao và trách nhiệm giải trình về quyền riêng tư thông tin sức khỏe (HIPPA)[47], Đạo luật về quyền riêng tư và giáo dục gia đình (FERPA)[48], Đạo luật bảo vệ quyền riêng tư trực tuyến của trẻ em (COPPA)[49], Đạo luật Gramm-Leach-Bliley (GLBA),[50] Đạo luật Báo cáo Tín dụng Công bằng

---

Communications Policy Act) sẽ được áp dụng. Hơn nữa, trong một số trường hợp nhất định, cả hai đạo luật có thể đồng thời được áp dụng.

[44] Swire and Ahmad 2012, p. 32.

[45] Reidenberg 2000, p. 1318; Simitis 2010, p. 139. Cách tiếp cận theo ngành (sectoral approach) của Hoa Kỳ trong việc điều chỉnh quyền riêng tư hoàn toàn trái ngược với mô hình của Liên minh châu Âu (EU), nơi áp dụng các quy định tổng thể (omnibus regulations) nhằm thiết lập nghĩa vụ cho tất cả các lĩnh vực trong nền kinh tế, bao gồm cả khu vực tư nhân và khu vực công. Khuôn khổ bảo vệ dữ liệu toàn diện của EU được duy trì dựa trên "cách tiếp cận lấy quyền làm trung tâm" (rights-dominated approach), với mục tiêu đảm bảo rộng rãi và đáng tin cậy cho việc thu thập và sử dụng dữ liệu cá nhân. Hơn nữa, ở EU, số lượng các chỉ thị (directive) liên quan đến nhiều vấn đề khác nhau – chẳng hạn như tài liệu liên quan đến y tế, an sinh xã hội, các vấn đề sức khỏe, v.v. – đang ngày càng gia tăng.

[46] Gratton 2014, p. 165; Skinner-Thompson 2015, p. 159.

[47] U.S. Dep't of Health & Hum. Serv. (2017) Your rights under HIPPA https://www.hhs.gov/hipaa/ for-individuals/guidance-materials-for-consumers/index.html. Accessed 28 May 2018.

[48] U.S. Dep't of Educ. (2018) Family Educational Rights and Privacy Act https://www2.ed.gov/ policy/gen/guid/ fpco/ferpa/index.html? Accessed 28 May 2018.

[49] Fed. Trade Comm'n (2015) Complying with COPPA: Frequently asked questions https://www.ftc.gov/ti ps-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General%20Questions. Accessed 28 May 2018.

[50] Fed. Trade Comm'n (2002) How to comply with the privacy of consumer financial information rule of the Gramm-Leach-Bliley Act https://www.ftc.gov/tips-advice/business-center/gui dance/how-comply-privacy-consumer-financial-information-rule-gramm. Accessed 3 June 2018.

(FCRA)[51], Đạo luật Chính sách Truyền thông Cáp[52], Đạo luật Quyền riêng tư Truyền thông Điện tử[53], Đạo luật Gian lận và Lạm dụng Máy tính[54], Đạo luật Bảo vệ Quyền riêng tư Video[55], và Đạo luật Không Phân biệt Đối xử Thông tin Di truyền[56]. Do đó, luật bảo vệ dữ liệu và quyền riêng tư của Hoa Kỳ áp dụng cho các ngành công nghiệp, công nghệ và cách sử dụng dữ liệu cụ thể chứ không phải cho việc xử lý "dữ liệu cá nhân", theo định nghĩa rộng. Nói cách khác, việc xử lý dữ liệu tại Hoa Kỳ thực chất được quy định dựa trên bối cảnh sử dụng dữ liệu[57].



Đạo luật Gramm-Leach-Bliley - Ảnh: Safetica

[51] Fed. Trade Comm'n (2016) Fair Credit Reporting Act, 15 U.S.C. § 1681 https://www.ftc.gov/system/files/fcra_2016.pdf. Accessed 3 June 2018.

[52] Fed. Commc'n Comm'n (2015) Cable television https://www.fcc.gov/media/engineering/cabletelevision. Accessed 3 June 2018.

[53] U.S. Dep't of Just. (2013) Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22 https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285. Accessed 3 June 2018.

[54] Jarrett H and Bailie M (2015) Prosecuting Computer Crimes https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf. Accessed 3 June 2018.

[55] Comm. on the Judiciary, Subcomm. on Privacy, Tech. and the Law (2012) The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century https://www.judiciary.senate.gov/ imo/media/doc/CHRG-112shrg87342.pdf. Accessed 3 June 2018.

[56] U.S. Equal Employment Opportunity Comm'n (2008) The Genetic Information Nondiscrimination Act of 2008 https://www.eeoc.gov/laws/statutes/gina.cfm. Accessed 3 June 2018.

[57] Schwartz and Solove 2014, p. 879.

1.2.2.3. Hành vi xâm phạm quyền riêng tư

Các hành vi xâm phạm quyền riêng tư, vốn cung cấp các biện pháp bảo vệ cơ bản cho quyền riêng tư tại Hoa Kỳ, đã được hầu hết các tiểu bang áp dụng thông qua luật chung hoặc luật riêng ở từng tiểu bang, hoặc được thiết lập thông qua việc diễn giải hiến pháp tiểu bang[58]. Các hành vi xâm phạm quyền riêng tư bao gồm: Xâm phạm sự riêng tư[59], Tiết lộ công khai thông tin cá nhân[60], Chiếm đoạt[61], Đưa thông tin sai sự thật[62]. Các hành vi xâm phạm dân sự (tort law) này được pháp luật quy định nhằm bảo vệ 04 lợi ích khác nhau của cá nhân, tất cả đều xoay quanh "quyền được yên thân", như Samuel Warren và Louis Brandeis đã mô tả một cách nổi tiếng về quyền riêng tư trong một bài báo tổng quan luật năm 1890[63]. Khi pháp luật quy định một hành vi là "tort", điều đó có nghĩa là nạn nhân có quyền được pháp luật bảo vệ trước hành vi đó, và có thể yêu cầu bồi thường hoặc can thiệp hợp pháp nếu bị xâm hại. Tuy nhiên, khả năng áp dụng của các hành vi vi phạm quyền riêng tư (privacy torts) đã phần nào bị hạn chế bởi tiêu chuẩn về tính hợp lý trong luật án lệ của Hoa Kỳ, cũng như bởi Tu chính án thứ Nhất của Hiến pháp Hoa Kỳ[64]. Thật vậy, Tòa án Tối cao Hoa Kỳ đã bác bỏ

---

[58] Prosser 1960; Privacilla.org (2002) How U.S. state law quietly leads the way in privacy protection http://www.privacilla.org/releases/Torts_Report.html. Accessed 12 January 2017.

[59] Restatement (Second) of Torts § 652B (1977).

[60] Restatement (Second) of Torts § 652B (1977).

[61] Restatement (Second) of Torts § 652B (1977).

[62] Restatement (Second) of Torts § 652B (1977).

[63] Warren and Brandeis 1890.

[64] Có thể hiểu là: Mặc dù hệ thống luật Hoa Kỳ công nhận một số hành vi vi phạm quyền riêng tư có thể bị kiện dân sự (gọi là "privacy torts"), nhưng việc thực thi những quyền này không phải lúc nào cũng dễ dàng. Nguyên nhân là vì:

- Tiêu chuẩn về tính hợp lý (reasonableness standard): Tòa án sẽ xét xem hành vi bị cho là xâm phạm quyền riêng tư đó có thực sự "quá mức" hoặc "phi lý" đối với một người bình thường hay không. Nếu tòa thấy hành vi đó hợp lý trong hoàn cảnh xã hội cụ thể, thì có thể không coi đó là vi phạm.
- Tu chính án thứ Nhất (First Amendment): Đây là quy định bảo vệ quyền tự do ngôn luận, tự do báo chí ở Mỹ. Trong nhiều trường hợp, quyền tự do ngôn luận của một cá nhân hoặc tổ chức có thể được coi là quan trọng

các đạo luật của tiểu bang liên quan đến quyền riêng tư nếu những luật đó không yêu cầu rằng hành vi xâm phạm phải là cực kỳ xúc phạm hoặc phi lý[65]. Ví dụ, hành vi vi phạm quyền riêng tư thông qua việc công khai thông tin riêng tư chỉ bị coi là vi phạm khi thông tin được công bố là rất xúc phạm và không liên quan đến lợi ích chính đáng. Tương tự, trong hành vi xâm nhập vào không gian riêng tư, hành vi xâm nhập vào bí mật hay vấn đề riêng tư của cá nhân cũng phải gây xúc phạm nghiêm trọng đối với một người thì mới được coi là vi phạm.

Như vậy, ở Mỹ, quyền riêng tư không được bảo vệ một cách "tuyệt đối", mà chỉ được bảo vệ khi sự xâm phạm đó vượt qua ngưỡng chuẩn mực của xã hội, gây tổn hại nghiêm trọng, và không có lý do chính đáng. Chính vì vậy, nhiều vụ kiện vi phạm quyền riêng tư có thể không được tòa án chấp nhận, nếu không chứng minh được mức độ nghiêm trọng của hành vi xâm phạm.

1.2.2.4. Ủy ban Thương mại Liên bang

Việc xử lý thông tin cá nhân tại Hoa Kỳ cũng được Ủy ban Thương mại Liên bang (FTC) quản lý, đóng vai trò quan trọng trong việc bảo vệ quyền riêng tư của người tiêu dùng Hoa Kỳ[66]. Ủy ban thực hiện điều này chủ yếu thông qua quyền duy trì giám sát độc lập và thực hiện các hành động chống lại các hoạt động kinh doanh không công bằng và lừa đảo được quy định tại Mục 5 của Đạo luật Ủy ban Thương mại Liên bang[67]. FTC có thể cung cấp biện pháp khắc phục bằng lệnh cấm và áp dụng các hình phạt dân sự đối với các công ty có hành vi vi phạm quyền riêng tư của người tiêu dùng và hiện

---

hơn quyền riêng tư của người khác, đặc biệt nếu thông tin được công khai liên quan đến lợi ích công cộng. Điều này làm cho việc khởi kiện các hành vi xâm phạm quyền riêng tư trở nên khó khăn hơn".

[65] Cate 2001, p. 59.

[66] Hoofnagle 2016.

[67] 15 U.S.C § 45.

nay cơ quan này "quản lý việc thực thi các chính sách về quyền riêng tư"[68]. Mặc dù FTC đã thành công trong việc thay đổi hoạt động của các công ty lớn[69], nhưng cơ quan này cũng bị chỉ trích vì đã bỏ qua đối với các hoạt động bị chỉ trích rộng rãi gây ra lo ngại về quyền riêng tư, chẳng hạn như các hoạt động theo dõi trực tuyến của Facebook[70].

FTC là cơ quan thực thi chính đối với các luật liên bang về quyền riêng tư như GLBA, FCRA, và COPPA. Trong những năm gần đây, FTC cũng đã đóng vai trò tích cực hơn trong việc bảo vệ quyền riêng tư của người tiêu dùng thông qua các sắc lệnh đồng thuận (consent decrees), được ban hành trong các thỏa thuận giải quyết với các công ty bị cáo buộc vi phạm quyền riêng tư.

Logo Federal Trade Commission - Ảnh: Internet

[68] Solove and Hartzog 2014.

[69] In 2011, the FTC imposed a settlement order on Google requiring it to implement a privacy program because of its misrepresentations around the use of consumer information through its network, Google Buzz. Fed. Trade Comm'n (2011) *FTC charges deceptive privacy practices in Google's rollout of its Buzz social network,* https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout -its-buzz, truy cập ngày 15/07/2025.

[70] Rotenberg M (2012), *The reform of the EU data protection framework-building trust in a digital and global world,* https://epic.org/privacy/Rotenberg_EP_Testimony_10_10_12.pdf, truy cập ngày 15/07/2025.

Ví dụ, vào tháng 7 năm 2019, FTC đã áp dụng mức phạt 5 tỷ đô la đối với Facebook, mức phạt cao nhất mà một công ty từng phải chịu trong một vụ kiện về quyền riêng tư trên toàn thế giới. Hình phạt này được áp dụng do Facebook vi phạm sắc lệnh đồng thuận do FTC ban hành năm 2012, trong đó yêu cầu Facebook phải *"thông báo rõ ràng và nổi bật"* cho người tiêu dùng và phải có được *"sự đồng ý rõ ràng"* của họ trước khi chia sẻ thông tin[71]. Sau một năm điều tra, FTC phát hiện ra rằng Facebook đã lừa dối người dùng và làm suy yếu các tùy chọn quyền riêng tư của họ. Lệnh dàn xếp áp đặt các yêu cầu quyền riêng tư đáng kể đối với Facebook[72]. Vài tháng sau, vào đầu tháng 9/2019, FTC cũng đã giải quyết khiếu nại chống lại Google và công ty con YouTube về việc thu thập thông tin cá nhân bất hợp pháp từ trẻ em mà không có sự đồng ý của cha mẹ[73]. Như Chủ tịch FTC Joe Simons đã giải thích, YouTube vừa tự giới thiệu với các khách hàng doanh nghiệp là một nền tảng phổ biến dành cho trẻ em, vừa từ chối thừa nhận rằng các trang trên nền tảng của mình nhắm mục tiêu đến trẻ em để tránh phải tuân thủ

---

[71] Fed. Trade Comm'n (2012), *FTC approves final settlement with Facebook,* https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook, truy cập ngày 15/07/2025.

[72] Các yêu cầu này bao gồm việc buộc Facebook thành lập một ủy ban quyền riêng tư độc lập trong Hội đồng Quản trị, tách biệt với Giám đốc điều hành Mark Zuckerberg. Facebook cũng phải bổ nhiệm các cán bộ giám sát tuân thủ, những người sẽ chịu trách nhiệm nộp các bản chứng nhận hàng quý và hàng năm cho Ủy ban Thương mại Liên bang (FTC) liên quan đến việc tuân thủ sắc lệnh của công ty. Ngoài ra, sắc lệnh của FTC cũng tăng cường giám sát bên ngoài đối với Facebook thông qua một bên đánh giá độc lập, bên này cũng sẽ báo cáo trực tiếp cho ủy ban quyền riêng tư mới thành lập. Sắc lệnh còn yêu cầu Facebook phải tiến hành các "đánh giá quyền riêng tư" đối với mọi sản phẩm hoặc dịch vụ mới (hoặc được sửa đổi) trước khi triển khai. Một yêu cầu quan trọng khác là Facebook phải "tăng cường giám sát các ứng dụng bên thứ ba", trong đó có thể bao gồm cả việc chấm dứt hợp tác với các nhà phát triển ứng dụng không tuân thủ chính sách nền tảng của Facebook, hoặc không thể chứng minh lý do chính đáng khi yêu cầu truy cập dữ liệu người dùng. Fed. Trade Comm'n (2019) *FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook,* https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions, truy cập ngày 15/07/2025.

[73] Fed. Trade Comm'n (2019), *Google and YouTube will pay record $170 million for allegedviolations of children's privacy law,* https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations?utm_source=govdelivery, truy cập ngày 15/07/2025.

COPPA. Thỏa thuận giải quyết này bao gồm khoản tiền phạt 170 triệu đô la, cũng lập kỷ lục là khoản tiền phạt về quyền riêng tư lớn nhất đối với Google cũng như là hình phạt lớn nhất từng được đưa ra theo COPPA[74].

1.2.2.5. Hệ thống Cơ sở dữ liệu tại Hoa Kỳ

Hoa Kỳ có một số cơ sở dữ liệu quốc gia phục vụ nhiều chức năng khác nhau, từ an ninh và thực thi pháp luật đến phân tích thống kê và công khai. Cụ thể như sau:

- Hệ thống nhận dạng vân tay tự động tích hợp (IAFIS): Do FBI quản lý, hệ thống này chứa dữ liệu vẫn tay cho mục đích tội phạm và dân sự;

- Nhận dạng thế hệ tiếp theo (NGI): Cũng do FBI quản lý, đây là cơ sở dữ liệu nâng cao bao gồm dữ liệu sinh trắc học như dấu vân tay, dấu tay, quét mống mắt và nhận dạng khuôn mặt;

- Hệ thống chỉ số DNA kết hợp (CODIS): Cơ sở dữ liệu DNA được FBI sử dụng để điều tra tội phạm;

- Trung tâm Thông tin Tội phạm Quốc gia (NCIC);

- Cơ sở dữ liệu địa chỉ quốc gia (National Adddress Database) do Bộ Giao thông Vận tải Hoa Kỳ (USDOT) quản lý;

- Quản lý Cầu Quốc gia: Cơ sở dữ liệu chứa thông tin về tình trạng của các cây cầu ở Hoa Kỳ;

- Cơ sở dữ liệu dinh dưỡng quốc gia: Do USDA quản lý, nó cung cấp thông tin về hàm lượng dinh dưỡng trong thực phẩm;

- Hệ thống thông tin đăng ký quốc gia. Chứa thông tin về các địa điểm lịch sử được Sổ đăng ký địa điểm lịch sử quốc gia công nhận.

---

[74] Carson A (2019), *FTC touts historic YouTube settlement as 'game changer' for COPPA enforcement,* https://iapp.org/news/a/ftc-touts-historic-youtube-settlement-as-game-changer-for-coppa-enforcement/, truy cập ngày 15/07/2025.

Tại Hoa Kỳ, các hoạt động trao đổi và chia sẻ dữ liệu được điều chỉnh bởi một khuôn khổ phức tạp bao gồm luật liên bang, quy định của tiểu bang và các thỏa thuận quốc tế như:

- Chia sẻ dữ liệu của Chính phủ (Government Data Sharing): Chính phủ Hoa Kỳ có hướng dẫn chia sẻ dữ liệu giữa các cơ quan nhằm cải thiện hoạt động và dịch vụ công

- Liên đoàn dữ liệu Hoa Kỳ (U.S. Data Federation): Đơn giản hóa việc thu thập, kết hợp và trao đổi dữ liệu giữa các cơ quan Chính phủ bằng cách sử dụng các tái sử dụng các công cụ và quy trình lặp.

- Thỏa thuận trao đổi dữ liệu quốc tế (IDTAs): Hoa Kỳ tham gia vào các thỏa thuận quốc tế về chia sẻ dữ liệu, như Đạo luật làm rõ việc sử dụng dữ liệu ở nước ngoài hợp pháp (CLOUD), tạo điều kiện thuận lợi cho việc chia sẻ dữ liệu song phương đồng thời bảo đảm quyền riêng tư và bảo vệ quyền tự do dân sự.

1.2.3. Trung Quốc

1.2.3.1. Tổng quan về chính sách, pháp luật về dữ liệu tại Trung Quốc

Là một trong số quốc gia đông dân nhất trên thế giới, việc hoàn thiện pháp luật trên lĩnh vực dữ liệu luôn là vấn đề được các cấp, các ngành ở Trung Quốc hết sức quan tâm, chú trọng và đẩy mạnh. Năm 2020, trong thông báo "Ý kiến về việc xây dựng một hệ thống và cơ chế hoàn thiện hơn để phân bố các yếu tố theo định hướng thị trường", Chính phủ Trung quốc liệt kê dữ liệu là *"yếu tố sản xuất thứ năm"* sau đất đai, lao động, vốn và công nghệ. Để phát huy vai trò của dữ liệu, Ban chấp hành Trung ương Đảng Cộng sản Trung Quốc đã nhiều lần định hướng phát triển thị trường dữ liệu trong các tài liệu quan trọng như "Kế hoạch 4 năm lần thứ 14 (2021 - 2025)", "Thông báo về phương án tổng thể thí điểm cải cách toàn diện phân bổ thị

trường yếu tố sản xuất" (năm 2022). Theo đó, Trung Quốc đã thúc đẩy xây dựng hệ thống quản trị dữ liệu với ba trụ cột chính đó là: Bảo đảm an ninh dữ liệu, bảo vệ quyền lợi người dùng và giải phóng giá trị dữ liệu.

Xuất phát từ quan điểm trên, Trung Quốc đã đi từ một khung quy định phân mảnh (chỉ tập trung vào một số ngành nhất định như tài chính, viễn thông, y tế) sang một hệ thống ngày càng toàn diện về bảo vệ thông tin cá nhân và an ninh dữ liệu. Hiện nay, ba trụ cột chính của khung pháp lý về dữ liệu ở Trung Quốc là Luật An ninh mạng (CSL, 2017), Luật An ninh Dữ liệu (DSL, 2021) và Luật Bảo vệ Thông tin Cá nhân (PIPL, 2021). Theo DLA Piper, *"Trung Quốc không có một luật duy nhất toàn diện về dữ liệu, mà quy định phân tán qua nhiều đạo luật khác nhau... tuy nhiên hiện nay bộ ba CSL, DSL, PIPL là trụ cột chính của khung bảo vệ thông tin cá nhân"*[75]. Về mối quan hệ, CSL là nền tảng cơ bản về chủ quyền không gian mạng và thiết lập khung pháp lý tổng thể, DSL tập trung vào bảo vệ an ninh dữ liệu nói chung (cả cá nhân và tổ chức), và PIPL điều chỉnh việc xử lý thông tin cá nhân. DSL và PIPL đều có quyền lực ngoài lãnh thổ để bảo vệ dữ liệu và thông tin cá nhân được xử lý bởi hạ tầng được CSL bảo vệ[76]. Đồng thời, PIPL và CSL cũng bổ sung các quy định về xử lý thông tin cá nhân, chịu ảnh hưởng bởi mô hình GDPR nhưng có thêm điều khoản miễn trừ thông tin đã ẩn danh[77].

---

[75] DLA Piper (n.d.), *Data protection laws in China. Retrieved from DLA Piper Data Protection Laws of the World,* https://www.dlapiperdataprotection.com/index.html?c=CN#:~:text=There%20is%20 not%20a%20single, truy cập ngày 16/07/2025.

[76] PwC Indonesia (n.d.), *A comparison of cybersecurity regulations: China,* PwC, https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/china.html, truy cập ngày 16/07/2025.

[77] Lexonogy (n.d), *A Few Key Points of the China Personal Information Protection Law*, https://www.lexology.com/library/detail.aspx?g=2830ff2c-cbcd-4a56-8ff0-852a09086169#:~:text=information%20as%20,a%20natural%20person%20will%20not, truy cập ngày 16/07/2025.

Có thể khái quát hệ thống văn bản pháp luật về dữ liệu tại Trung Quốc như sau:

Về bảo đảm an ninh dữ liệu, Quốc hội nước Cộng hòa nhân dân Trung Hoa đã thông qua Luật An ninh Quốc gia, Luật An ninh mạng, Luật bảo mật dữ liệu và các quy định liên quan; thiết lập các cơ chế như phân loại, phân cấp dữ liệu và bảo vệ dữ liệu quan trọng; đánh giá bảo mật dữ liệu.

Về bảo vệ quyền của người dùng, đã thông qua Bộ luật Dân sự (sửa đổi), Luật Bảo vệ thông tin cá nhân; xây dựng các quy định bổ sung để làm rõ quy tắc xử lý thông tin cá nhân, cung cấp thông tin cá nhân xuyên biên giới, quy định quyền của cá nhân và nghĩa vụ của bên xử lý trong xử lý thông tin cá nhân.

Về giải phóng giá trị dữ liệu, gần đây nhiều địa phương cấp tỉnh, thành phố đã đưa ra các quy định về dữ liệu, xây dựng các quy tắc chia sẻ và mở dữ liệu công khai cũng như lưu thông giao dịch dữ liệu. Tuy nhiên, ở cấp trung ương vẫn còn thiếu một hệ thống pháp luật tổng thể để thúc đẩy việc giải phóng giá trị của các yếu tố dữ liệu. Hiện nay, hệ thống dữ liệu lớn tích hợp quốc gia của Trung Quốc là một sáng kiến chiến lược quan trọng nhằm thúc đẩy hiện đại hóa hệ thống quản trị quốc gia và năng lực quản trị.

Dưới đây là một số điểm chính về hệ thống: ***(1)*** Chức năng quản lý dữ liệu của Chính phủ đã được làm rõ và mỗi tỉnh (khu tự trị, đô thị trực thuộc Trung ương) chịu trách nhiệm thu thập, quản lý, chia sẻ, mở và bảo vệ an ninh dữ liệu của Chính phủ; ***(2)*** Hệ thống tài nguyên dữ liệu Chính phủ bước đầu đã được hình thành, bao gồm cơ sở dữ liệu cơ bản và cơ sở dữ liệu chuyên đề, nhằm hỗ trợ Chính phủ thực hiện nhiệm vụ của mình; ***(3)*** Cơ sở hạ tầng dữ liệu của Chính phủ đã được xây dựng, bao gồm nền tảng đám mây của Chính phủ, trung tâm chia sẽ dữ liệu...

Trung Quốc đã xây dựng danh mục dữ liệu quốc gia thống nhất, tiêu chuẩn dữ liệu quốc gia thống nhất, đồng thời cung cấp các dịch vụ dữ liệu hữu ích và hiệu quả cho các khu vực công - tư.

Cơ sở dữ liệu cơ bản quốc gia của Trung Quốc bao gồm: Cơ sở dữ liệu dân cư cơ bản, Cơ sở dữ liệu địa lý không gian, Cơ sở dữ liệu kinh tế vĩ mô, Cơ sở dữ liệu tổ chức và các đối tượng cơ bản khác dần được hoàn thiện, đồng thời nâng cao tính đầy đủ, tiêu chuẩn hóa và độ chính xác của dữ liệu.

Trung Quốc cũng từng bước hoàn thiện cơ chế chia sẻ và trao đổi dữ liệu của địa phương và trung ương, củng cố trách nhiệm chủ đạo của chính quyền cấp tỉnh trong việc chia sẻ và ứng dụng dữ liệu dựa trên nền tảng chia sẻ và trao đổi dữ liệu quốc gia. Bằng cách thiết lập cơ chế điều phối và chia sẻ dữ liệu của Chính phủ, cơ quan dữ liệu của Chính phủ làm rõ, chịu trách nhiệm xây dựng các kế hoạch và biện pháp chính sách phát triển dữ liệu lớn, đồng thời tổ chức và thực hiện việc thu thập, thu thập, quản trị, chia sẻ và bảo vệ an ninh dữ liệu.

Tính đến tháng 12/2022, 29 trong số 31 tỉnh (khu tự trị và thành phố) đã thành lập các cơ quan quản lý dữ liệu hoặc dịch vụ Chính phủ ở cấp sở, ban, ngành, và hơn 20 khu vực đã ban hành các văn bản quy hoạch liên quan đến chính quyền số hoặc chuyển đổi số.

Bên cạnh đó, Trung Quốc dang sử dụng hệ thống các quy tắc quản trị dữ liệu cụ thể, bao gồm: Bảo vệ an ninh dữ liệu, bảo vệ thông tin cá nhân, quản lý dữ liệu công khai và lưu thông giao dịch dữ liệu.

Về hệ thống bảo vệ an ninh dữ liệu. Thiết lập một hệ thống bảo vệ an ninh dữ liệu lấy Luật bảo mật dữ liệu làm nền tảng, đồng thời ban hành các quy định cụ thể như: Quy định quản lý bảo mật dữ liệu mạng (dự thảo), Quy định quản lý bảo mật dữ liệu ô tô (thử nghiệm)...

Về cơ chế cụ thể, đã thiết lập hệ thống quản lý phân loại, chấm điểm dữ liệu, xác định danh mục dữ liệu quan trọng cần bảo vệ: thiết lập cơ chế đánh giá, báo cáo, chia sẻ thông tin, giám sát và canh bảo sớm rủi ro bảo mật dữ liệu; thiết lập cơ chế ứng phó khẩn cấp về bảo mật dữ liệu...

Về hệ thống bảo vệ thông tin cá nhân, xây dựng một hệ thống pháp luật đa cấp, đa lĩnh vực để bảo vệ thông tin cá nhân với Luật Bảo vệ thông tin cá nhân là nền tảng.

Về hệ thống cụ thể, thiết lập một loạt các quy tắc xử lý thông tin cá nhân dựa trên cơ sở "đồng thuận"; thiết lập các quy tắc cho việc cung cấp thông tin cá nhân xuyên biên giới; làm rõ quyền của cá nhân trong hoạt động xử lý thông tin cá nhân, bao gồm quyền được biết, quyền quyết định, quyền hỏi, quyền sửa, quyền xóa...; làm rõ việc quản lý tuân thủ của bên xử lý thông tin cá nhân và nghĩa vụ của các bên liên quan để bảo đảm an toàn cho thông tin cá nhân.

Về hệ thống quản lý dữ liệu công khai, Luật Bảo mật dữ liệu đưa ra các yêu cầu về chất lượng dữ liệu do Chính phủ cung cấp, quy định nghĩa vụ của các cơ quan nhà nước trong việc bảo đảm an toàn dữ liệu của Chính phủ, giám sát việc xử lý của các bên được ủy thác... Bên cạnh đó, các địa phương đã ban hành quy định riêng để cụ thể hóa Luật Bảo mật dữ liệu.

Về hệ thống lưu thông giao dịch dữ liệu, Luật Bảo mật dữ liệu xác định bảo đảm luồng dữ liệu có trật tự và tự do theo quy định của pháp luật, yêu cầu "nhà nước thiết lập một hệ thống quản lý giao dịch dữ liệu lành mạnh"; quy định các tổ chức tham gia dịch vụ trung gian giao dịch dữ liệu phải thực hiện nghĩa vụ và trách nhiệm pháp lý tương ứng, phải yêu cầu nhà cung cấp dữ liệu giải thích nguồn dữ liệu, xác minh danh tính bên tham gia giao dịch, lưu giữ hồ sơ giao dịch.

Về mặt luật pháp địa phương, có quy định về dữ liệu của Đặc khu kinh tế Thâm Quyến, các biện pháp tạm thời để quản lý giao dịch dữ liệu của thành phố Thiên Tân quy định về đối tượng giao dịch, sàn giao dịch, an toàn giao dịch, giám sát và quản lý giao dịch...

Về cơ quan chuyên trách, tháng 3/2023, Trung Quốc đã thảo luận để thành lập Cục dữ liệu quốc gia. Cơ quan này chịu trách nhiệm điều phối và thúc đẩy việc xây dựng hệ thống dữ liệu cơ bản quốc gia, điều phối việc tích hợp, chia sẻ, phát triển và sử dụng tài nguyên dữ liệu.

Dựa trên các luận điểm đã nêu, có thể khái quát lại hệ thống pháp luật về dữ liệu tại Trung Quốc là một hệ thống đa tầng, toàn diện nhưng vẫn đang trong quá trình hoàn thiện. Điểm nổi bật là sự phân tầng rõ rệt, từ các luật cấp quốc gia như Luật An ninh mạng, Luật Bảo mật dữ liệu và Luật Bảo vệ thông tin cá nhân cho đến các quy định chi tiết ở cấp địa phương, cho thấy cách tiếp cận vấn đề dữ liệu một cách bao quát từ an ninh quốc gia, bảo vệ cá nhân đến quản lý thương mại. Hệ thống này thể hiện vai trò chủ đạo của Chính phủ và sự tập trung quyền lực trong việc quản lý, thu thập và bảo vệ dữ liệu, được minh chứng qua việc thành lập các cơ quan chuyên trách và xây dựng cơ sở dữ liệu quốc gia. Các văn bản này nhấn mạnh quan điểm *"dữ liệu là yếu tố then chốt cho an ninh quốc gia, lợi ích công cộng và phát triển kinh tế"*.

Bên cạnh đó, an ninh dữ liệu được đặt lên hàng đầu và là nền tảng của toàn bộ hệ thống, với các luật quan trọng như Luật An ninh mạng và Luật Bảo mật dữ liệu cho phép nhà nước kiểm soát chặt chẽ dữ liệu, đặc biệt là dữ liệu quan trọng. Cùng với đó, việc bảo vệ quyền cá nhân cũng có những bước tiến đáng kể với sự ra đời của Luật Bảo vệ thông tin cá nhân, làm rõ các quyền của người dùng và nghĩa vụ của bên xử lý dữ liệu. Tuy nhiên, sự cân bằng giữa kiểm soát của nhà nước và quyền riêng tư cá nhân vẫn là một

vấn đề phức tạp. Ngoài ra, Trung Quốc cũng đang nỗ lực thúc đẩy giá trị kinh tế của dữ liệu, mặc dù vẫn còn thiếu một hệ thống pháp luật tổng thể ở cấp trung ương. Việc thành lập Cục Dữ liệu Quốc gia được kỳ vọng sẽ giải quyết khoảng trống này.



Luật Bảo vệ Thông tin Cá nhân (PIPL) - Ảnh: Cookie Law info

Về nguồn của luật, hệ thống pháp luật dữ liệu Trung Quốc không chỉ giới hạn ở ba trụ cột mà còn dựa trên nhiều nguồn, như: Hiến pháp nước Cộng hòa nhân dân Trung Hoa (Điều 40 Hiến pháp 1982 - đảm bảo "tự do và bí mật thư tín" của công dân)[78]; Luật Hình sự (bổ sung tội xâm phạm thông tin cá nhân vào năm 2009, sửa đổi 2015 - mở rộng phạm vi đối tượng phạm tội ra bất kỳ ai và tăng hình phạt lên tối đa 7 năm tù)[79]; Bộ luật Dân sự mới (2021) có chương riêng về quyền riêng tư và bảo vệ thông tin cá nhân[80]. Luật CSL

[78] Government of the People's Republic of China. (2019, November 20). *Administrative Procedure Law of the People's Republic of China* [Article 40 on freedom and confidentiality of correspondence]. Retrieved from https://english.www.gov.cn/archive/lawsregulations/201911/20/content_WS5ed8856ec6d0b3f0e949913.html

[79] China Justice Observer (2023), *A look into cybercrime in China: Infringement of privacy as a crime,* https://www.chinajusticeobserver.com/a/-a-look-into-cybercrime-in-china, truy cập ngày 15/07/2025.

[80] Zhou, Q (2020), *New Chinese Civil Code Restates and Strengthens Chinese Data Privacy Laws,* China Law Vision, https://www.chinalawvision.com/2020/07/uncategorized/new-chinese-civil-code-restates-and-strengthens-chinese-data-privacy-laws/, truy cập ngày 15/07/2025.

(2017) nêu ví dụ về thông tin cá nhân như họ tên, ngày sinh, sinh trắc học, địa chỉ, số điện thoại[81]; Luật DSL (2021) đặt ra khung phân loại và bảo vệ dữ liệu dựa trên an ninh quốc gia[82]; và các quy định của các cơ quan, ban ngành như Luật Bảo vệ người tiêu dùng (sửa đổi 2013 - bắt buộc doanh nghiệp bảo vệ thông tin cá nhân khách hàng), các quy định của Bộ Công nghiệp và Công nghệ Thông tin (MIIT) đối với các nhà cung cấp dịch vụ Internet và viễn thông. Ngoài ra, Trung Quốc ban hành nhiều tiêu chuẩn kỹ thuật (chẳng hạn Tiêu chuẩn An ninh Công nghệ Thông tin GB/T 35273-2020 định nghĩa yêu cầu bảo vệ thông tin cá nhân) để hướng dẫn thực thi pháp luật về dữ liệu.

序号	标准编号	标准名称	代替标准号	实施日期
1.	GB/T 17901.1-2020	信息技术 安全技术 密钥管理 第1部分：框架	GB/T 17901.1-1999	2020-10-01
2.	GB/T 35273-2020	信息安全技术 个人信息安全规范	GB/T 35273-2017	2020-10-01
3.	GB/T 38540-2020	信息安全技术 安全电子签章密码技术规范		2020-10-01
4.	GB/T 38541-2020	信息安全技术 电子文件密码应用指南		2020-10-01
5.	GB/T 38542-2020	信息安全技术 基于生物特征识别的移动智能终端身份鉴别技术框架		2020-10-01
6.	GB/T 38556-2020	信息安全技术 动态口令密码应用技术规范		2020-10-01
7.	GB/T 38558-2020	信息安全技术 办公设备安全测试方法		2020-10-01
8.	GB/T 38561-2020	信息安全技术 网络安全管理支撑系统技术要求		2020-10-01

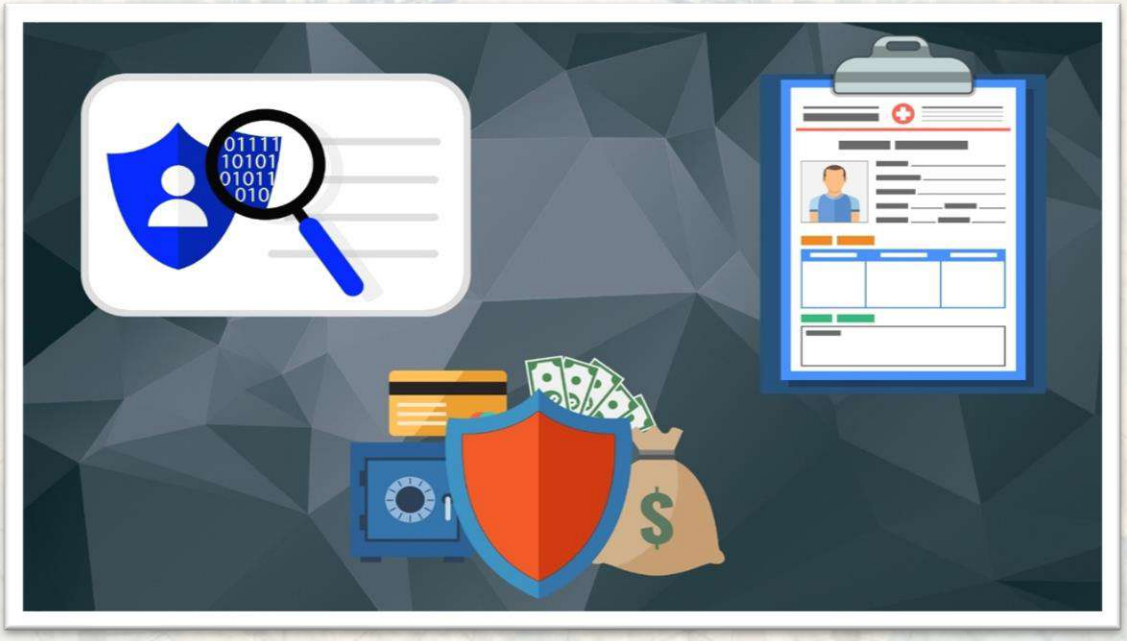
Tiêu chuẩn An ninh Công nghệ Thông tin GB/T 35273-2020 - Ảnh: 河南金盾信安

Đối với các khái niệm, Chính phủ Trung Quốc định nghĩa *"thông tin cá nhân"* tại Điều 4 PIPL tương tự GDPR của EU, đó là: "mọi thông tin liên quan đến một cá nhân tự nhiên đã xác định hoặc có thể xác định" và không bao gồm thông tin đã được ẩn danh. CSL (Điều 76) liệt kê cụ thể một số ví

[81] SECRSS (2021), *《网络安全法》 第七十六条第五项规定的“ 个人信息”如何理解？*, https://www.secrss.com/articles/27769, truy cập ngày 15/07/2025.

[82] Skadden Arps Slate Meagher & Flom LLP (2021), *China's new data security and personal information protection laws: What they mean for multinational companies*, https://www.skadden.com/insights/publications/2021/11/chinas-new-data-security-and-personal-information-protection-laws, truy cập ngày 15/07/2025.

dụ như họ tên, ngày sinh, số chứng minh nhân dân, sinh trắc học, địa chỉ, điện thoại. Một điểm quan trọng là Bộ luật Dân sự phân biệt khái niệm *"quyền riêng tư"* (mang tính chất cá nhân, như đời sống riêng tư) và *"thông tin cá nhân"* (có thể nhận dạng cá nhân) một cách rõ ràng: thông tin cá nhân nào thuộc nhóm "riêng tư" sẽ được điều khoản về quyền riêng tư điều chỉnh. Ngoài ra, một số văn bản còn đề cập khái niệm *"thông tin cá nhân nhạy cảm"* (Sensitive Personal Information - SPI), đây là một loại thông tin được bảo vệ nghiêm ngặt hơn. SPI được định nghĩa là thông tin mà nếu bị rò rỉ hoặc sử dụng bất hợp pháp có thể gây ra phân biệt đối xử hoặc tổn hại nghiêm trọng đến an toàn cá nhân hoặc tài sản[83]. Ví dụ, dữ liệu sinh trắc học (nhận dạng khuôn mặt, vân tay), tín ngưỡng tôn giáo, danh tính cụ thể, thông tin sức khỏe, tài khoản tài chính, theo dõi vị trí cá nhân, và thông tin của trẻ vị thành niên dưới 14 tuổi...



Thông tin cá nhân nhạy cảm phải được bảo vệ nghiêm ngặt - Ảnh: Captain Compliance

[83] Ren, Z., & Li, J. (n.d.). *China: Data protection laws and regulations. In International Comparative Legal Guide: Data Protection Laws and Regulations 2024*. Retrieved from https://iclg.com/practice-areas/data-protection-laws-and-regulations/china.

1.2.3.2. Các nguyên tắc và quy định chính

Về nguyên tắc, Chính phủ Trung Quốc đặt ra nhiều nguyên tắc xử lý dữ liệu tương tự các hệ thống khác trên thế giới, cụ thể:

- Tính hợp pháp và có mục đích rõ ràng: Dữ liệu chỉ được thu thập để phục vụ mục đích hợp pháp, cụ thể và không được xử lý vượt quá phạm vi cần thiết. Ví dụ, Bộ luật Dân sự nêu rõ việc xử lý thông tin cá nhân phải "hợp pháp, có lý do chính đáng, cần thiết và không vượt quá phạm vi cần thiết". PIPL cũng yêu cầu các doanh nghiệp thông báo rõ ràng chính sách quyền riêng tư với người dùng (nguyên tắc minh bạch).

- Sự đồng ý của chủ thể: Trong đa số trường hợp, việc thu thập và sử dụng thông tin cá nhân đòi hỏi sự đồng ý tự nguyện, rõ ràng của chủ thể dữ liệu. PIPL yêu cầu đồng ý từng trường hợp và quy định chặt chẽ với thông tin nhạy cảm (sinh trắc học, vị trí, y tế, tín ngưỡng…) phải công khai mục đích cụ thể và biện pháp bảo vệ đặc biệt. Tuy nhiên, luật cũng ghi nhận một số trường hợp ngoại lệ cho phép xử lý không cần đồng ý (ví dụ thực hiện hợp đồng, yêu cầu pháp luật, bảo vệ lợi ích cộng đồng…). Đặc biệt, ở Trung Quốc có sự mở rộng trong khái niệm đồng ý, đó là sự đồng ý riêng biệt (Separate Consent), đây là một yêu cầu nghiêm ngặt hơn so với "sự đồng ý rõ ràng" của GDPR trong nhiều tình huống[84].

- Nguyên tắc minh bạch: Các hoạt động thu thập thông tin, dữ liệu phải được thông báo trước hoặc tại thời điểm thu thập dữ liệu. Điều này bao gồm việc thông báo cho cá nhân về tên và thông tin liên hệ của tổ chức xử lý, mục

---

[84] ISACA (2022), *Demystifying China's Personal Information Protection Law,* ISACA Blog, https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/demystifying-chinas-personal-information-protection-law, truy cập ngày 15/07/2025.

đích, phương tiện và phạm vi xử lý, loại và thời gian lưu giữ thông tin cá nhân, và cách thức thực hiện quyền của họ[85].

- Nguyên tắc chính xác và cập nhật: Luật yêu cầu dữ liệu cá nhân phải được bảo đảm tính chính xác và thường xuyên cập nhật, song quy định này ít được nhấn mạnh ở Trung Quốc so với GDPR.

- Bảo mật dữ liệu: Tất cả các văn bản đều yêu cầu doanh nghiệp phải xây dựng hệ thống an ninh, kỹ thuật bảo vệ dữ liệu để phòng ngừa, ngăn chặn truy cập trái phép, sửa đổi, rò rỉ hoặc làm mất mát dữ liệu và các biện pháp bảo vệ dữ liệu phải được áp dụng đồng bộ trong toàn bộ quá trình xử lý dữ liệu. Ví dụ, Bộ luật Dân sự chỉ rõ các bên xử lý dữ liệu phải "thực hiện các biện pháp kỹ thuật và tổ chức cần thiết để bảo đảm an toàn thông tin cá nhân" và trong trường hợp vi phạm phải khắc phục kịp thời, thông báo cho cá nhân bị ảnh hưởng và cơ quan, tổ chức có liên quan.

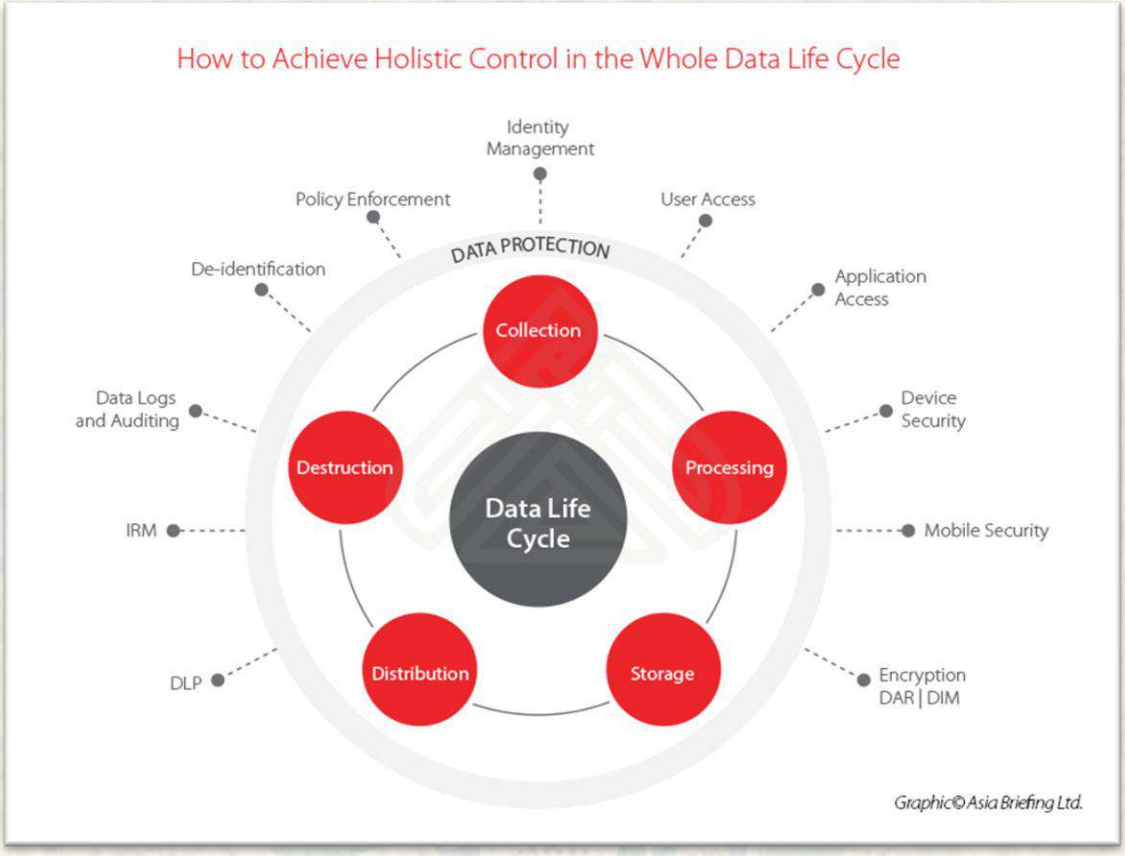
- Chuyển dữ liệu xuyên biên giới: Đối với dữ liệu nhạy cảm và dữ liệu quan trọng (theo DSL), việc chuyển ra nước ngoài phải tuân thủ quy định nghiêm ngặt như: phải thông qua đánh giá về mặt an ninh; xin phép cơ quan thẩm quyền, hoặc sử dụng hợp đồng chuẩn. Luật cấm cung cấp bất kỳ dữ liệu nào lưu trữ trong nước cho cơ quan nước ngoài mà không có phê duyệt của chính phủ. Với dữ liệu cá nhân không nhạy cảm, PIPL áp dụng cơ chế hợp đồng tiêu chuẩn (CN SCCs) cho chuyển dữ liệu ra nước ngoài (hiện đang được CAC ban hành).

- Quyền của chủ thể dữ liệu: PIPL cung cấp cho cá nhân nhiều quyền cơ bản tương tự GDPR, như: Truy cập và xin bản sao dữ liệu của mình mà tổ chức xử lý lưu giữ; yêu cầu sửa đổi nếu thông tin sai; yêu cầu thu hồi, xóa

---

[85] Future of Privacy Forum (n.d.), *China's new comprehensive data protection law: Context, stated objectives, & key provisions,* FPF Blog, https://fpf.org/blog/chinas-new-comprehensive-data-protection-law-context-stated-objectives-key-provisions/, truy cập ngày 15/07/2025.

hoặc hủy dữ liệu nếu việc xử lý vi phạm pháp luật hoặc thỏa thuận; quyền từ chối một số hình thức xử lý. Trong Bộ luật Dân sự, cá nhân còn được quyền yêu cầu chấm dứt hành vi xâm phạm, yêu cầu xin lỗi công khai hoặc bồi thường thiệt hại (cả tổn thất vật chất và tinh thần) khi quyền riêng tư cá nhân bị tổn hại[86].



Mô hình nội dung cốt lõi của luật dữ liệu - Ảnh: China Briefing

Nhìn chung, luật dữ liệu của Trung Quốc đang trong giai đoạn trưởng thành mạnh mẽ, từ hệ thống rời rạc tiến tới một khung toàn diện hơn với đầy đủ các cơ chế bảo vệ mang tính bao quát và chặt chẽ đối với thông tin cá nhân nói riêng và an ninh mạng nói chung. Với khung pháp

[86] Yang, S., & Blackmore, N (2020), *New Chinese Civil Code restates and strengthens Chinese data privacy laws,* China Law Vision, https://www.chinalawvision.com/2020/07/unca tegorized/new-chinese-civil-code-restates-and-strengthens-chinese-data-privacy-laws/, truy cập ngày 15/07/2025.

lý ngày càng được hoàn thiện, Chính phủ Trung Quốc cho thấy rõ sự ưu tiên trong bảo đảm an ninh quốc gia và phục vụ công tác quản lý nhà nước đối với dữ liệu.

Ví dụ, DSL quy định rõ *"dữ liệu cốt lõi"* ảnh hưởng đến an ninh quốc phòng, kinh tế vĩ mô, an ninh xã hội... phải được bảo mật ở mức tối đa. Các văn bản luật trao nhiều quyền cho nhà nước trong việc kiểm soát, thanh tra và phê duyệt các luồng dữ liệu, đặc biệt với dữ liệu quan trọng.

Bên cạnh đó, Luật PIPL công nhận tầm quan trọng của việc sử dụng dữ liệu để phát triển kinh tế, đảm bảo cân bằng giữa bảo vệ quyền riêng tư và "khuyến khích khai thác hợp lý dữ liệu". Nhà nước khuyến khích đầu tư, nghiên cứu - phát triển công nghệ dữ liệu để thúc đẩy ngành công nghiệp dữ liệu, bao gồm cả việc xây dựng hạ tầng lưu trữ dữ liệu trong nước. Tuy nhiên, việc triển khai khung pháp lý về dữ liệu này vẫn gặp nhiều khó khăn, thách thức và sự xung đột với một số quy chuẩn quốc tế về quyền riêng tư. Tạp chí New America đánh giá các quy định về dữ liệu và an ninh mạng ở Trung Quốc có nhiều giao thoa phức tạp (ví dụ, quyền xử lý dữ liệu dựa trên đồng ý được quy định trong CSL nhưng cho phép quy định pháp luật khác điều chỉnh như trong Luật Dân sự).

Ngoài ra, Ở Trung Quốc cũng đang thiếu cơ quan độc lập phụ trách quản lý về dữ liệu như DPA (Cơ quan bảo vệ dữ liệu) ở Châu Âu, nhiều cơ quan vẫn đang cùng thực hiện quản lý về dữ liệu như Cục Quản lý Không gian mạng Trung Quốc (CAC), Bộ Công an, Bộ Công nghiệp và Công nghệ Thông tin (MIIT)… dẫn đến sự chồng chéo và nguy cơ rò rỉ thông tin cá nhân người dân.

1.2.3.3. Ưu, nhược điểm của khung pháp luật về dữ liệu tại Trung Quốc

- Về ưu điểm

+ Tính toàn diện và quy định chi tiết của PIPL

Một trong những ưu điểm nổi bật của hệ thống pháp lý bảo vệ dữ liệu tại Trung Quốc là tính toàn diện và chi tiết trong các quy định bảo vệ quyền lợi người tiêu dùng. Luật Bảo vệ Thông tin Cá nhân (PIPL) được xây dựng với các nguyên tắc bảo vệ rõ ràng, giúp các cá nhân có quyền kiểm soát dữ liệu của mình trong môi trường số. Điều này không chỉ giúp tăng cường quyền riêng tư của công dân, mà còn khẳng định cam kết của Trung Quốc trong việc tham gia vào xu hướng toàn cầu về bảo vệ dữ liệu cá nhân. Cụ thể, PIPL bao gồm các điều khoản quan trọng như yêu cầu đồng ý rõ ràng của người dùng trước khi thu thập và xử lý dữ liệu, yêu cầu các tổ chức phải cung cấp quyền truy cập, quyền chỉnh sửa, quyền xóa bỏ và quyền chuyển giao dữ liệu cho cá nhân[87].

Bên cạnh đó, PIPL có những biện pháp bảo vệ dữ liệu xuyên biên giới, yêu cầu các công ty Trung Quốc phải tuân thủ những tiêu chuẩn bảo vệ dữ liệu khi chuyển dữ liệu ra ngoài lãnh thổ Trung Quốc, nhằm đảm bảo rằng dữ liệu của người dân Trung Quốc sẽ được bảo vệ thích hợp ngay cả khi bị chuyển đi quốc gia khác. Điều này đặc biệt quan trọng trong bối cảnh số hóa ngày càng gia tăng và dữ liệu cá nhân có thể dễ dàng bị chuyển giao toàn cầu. Các điều khoản này giúp tăng cường bảo mật dữ liệu và quyền kiểm soát của cá nhân, làm cho PIPL trở thành một khuôn khổ mạnh mẽ để bảo vệ quyền lợi người tiêu dùng trong môi trường số.

---

[87] Greenleaf, G (2021), *China's completed Personal Information Protection Law*: *Rights plus cyber-security,* UNSW Law Research Paper No. 21-63, http://classic.austlii.edu.au/au/journals/UNSWLRS/2021/91.pdf, truy cập ngày 15/07/2025.



Luật PIPL cung cấp các công cụ nhằm ngăn chặn việc đưa dữ liệu trong Trung Quốc ra nước ngoài - Ảnh: Jones Day

+ Sự phân loại và quản lý chặt chẽ dữ liệu trong DSL

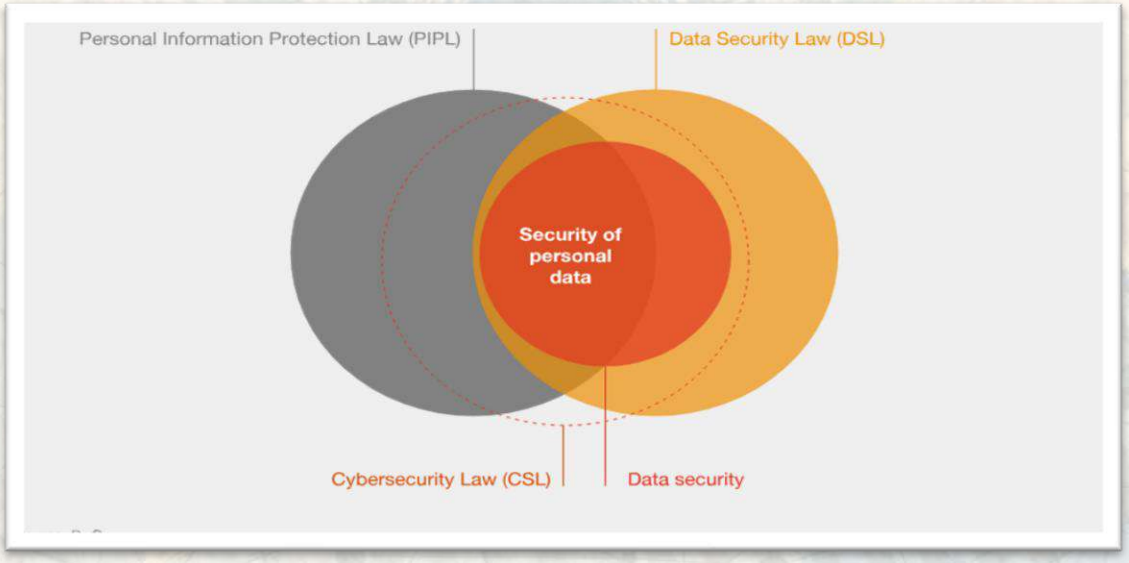
Cùng với PIPL, Luật An toàn Dữ liệu (DSL) cũng đóng vai trò quan trọng trong việc bảo vệ dữ liệu tại Trung Quốc. DSL không chỉ phân loại dữ liệu thành các nhóm như dữ liệu thông thường, dữ liệu quan trọng và dữ liệu cốt lõi, mà còn quy định cụ thể các biện pháp bảo vệ đối với từng nhóm dữ liệu. Điều này giúp các doanh nghiệp dễ dàng phân loại và tổ chức dữ liệu một cách hiệu quả, đồng thời xác định rõ ràng các biện pháp bảo vệ cần thiết cho mỗi loại dữ liệu. Việc phân loại dữ liệu không chỉ giúp đảm bảo bảo mật, mà còn giúp các tổ chức và doanh nghiệp dễ dàng thực thi các nghĩa vụ bảo vệ dữ liệu của mình, đồng thời tạo ra một hệ thống quản lý dữ liệu hiệu quả.

Một điểm đáng chú ý là sự hợp tác giữa các cơ quan nhà nước và các tổ chức, doanh nghiệp trong việc quản lý dữ liệu. Các cơ quan quản lý nhà nước có quyền giám sát việc thu thập, xử lý và lưu trữ dữ liệu của các tổ chức, từ đó đảm bảo tính minh bạch và tuân thủ pháp luật trong quản lý dữ liệu. Việc

này giúp tạo ra một hệ sinh thái dữ liệu mạnh mẽ, nơi các tổ chức và doanh nghiệp có thể tiếp cận dữ liệu một cách hợp pháp và bảo vệ quyền lợi người tiêu dùng, đồng thời không vi phạm các quy định về bảo mật và bảo vệ dữ liệu cá nhân.

+ Tăng cường các biện pháp bảo vệ thông qua chế tài nghiêm khắc

Một trong những ưu điểm quan trọng của PIPL và DSL là hệ thống chế tài nghiêm khắc đối với những vi phạm liên quan đến bảo vệ dữ liệu. Các biện pháp xử phạt mạnh mẽ không chỉ làm gia tăng tính nghiêm khắc của pháp luật mà còn đóng vai trò như một công cụ răn đe mạnh mẽ, thúc đẩy các tổ chức và cá nhân tuân thủ các quy định về bảo vệ dữ liệu. Theo PIPL, các tổ chức vi phạm có thể bị phạt tới 50 triệu nhân dân tệ hoặc 5% doanh thu hàng năm của công ty, điều này cho thấy mức độ nghiêm khắc của chính sách pháp luật Trung Quốc đối với vi phạm bảo vệ dữ liệu (Kerry, 2021). Các biện pháp phạt nghiêm ngặt này đã tạo ra một môi trường tuân thủ chặt chẽ, đồng thời khuyến khích các doanh nghiệp đầu tư vào công nghệ bảo mật và các giải pháp bảo vệ dữ liệu.



Phạm vi của PIPL và DSL - Ảnh: PwC

+ Tạo dựng môi trường pháp lý ổn định và có tính đồng bộ

Một ưu điểm nữa của PIPL và DSL là việc tạo ra một môi trường pháp lý ổn định và có tính đồng bộ, giúp Trung Quốc xây dựng một hệ thống bảo vệ dữ liệu thống nhất trên toàn quốc. Điều này rất quan trọng trong việc tạo dựng niềm tin đối với cả người tiêu dùng và các tổ chức kinh doanh trong nước và quốc tế. Với việc xác định rõ trách nhiệm của các tổ chức trong việc bảo vệ dữ liệu và quy định các biện pháp bảo vệ cụ thể đối với từng loại dữ liệu, Trung Quốc đã tạo ra một khung pháp lý ổn định cho việc quản lý và bảo vệ dữ liệu cá nhân.



Các quyền cơ bản được quy định tại PIPL - Ảnh: Captain Compliance

- Về nhược điểm

Mặc dù khung pháp luật về dữ liệu của Trung Quốc có những ưu điểm như phạm vi điều chỉnh toàn diện, phân loại dữ liệu rõ ràng và tạo dựng được môi trường quản lý nhất định, song vẫn tồn tại một số nhược điểm, hạn chế. Các nhược điểm này không chỉ tạo ra thách thức cho doanh nghiệp và cơ quan quản lý trong nước, mà còn cho thấy khoảng cách giữa khuôn khổ pháp lý Trung Quốc với các chuẩn mực quốc tế.

Thứ nhất, *khung pháp luật phức tạp, phân mảnh.* Hệ thống quy định pháp luật về dữ liệu ở Trung Quốc hết sức đồ sộ với nhiều lớp văn bản chồng chéo, dẫn đến tình trạng khó nắm bắt. Không có một bộ luật duy nhất điều chỉnh toàn diện dữ liệu; thay vào đó là *"một khung phức hợp bao gồm nhiều luật và quy định khác nhau"*[88]. Bên cạnh đó, hàng loạt văn bản dưới luật, tiêu chuẩn kỹ thuật và quy định ngành đã được ban hành nhằm cụ thể hóa các luật này. Chính điều này làm cho việc "điều hướng các quy định trở nên phức tạp, với nhiều phần chồng lấn" giữa CSL, DSL và PIPL [53]. Ví dụ, CSL đặt ra yêu cầu về an ninh mạng và bảo vệ thông tin rộng rãi, DSL điều chỉnh an ninh cho mọi loại dữ liệu (bao gồm cả dữ liệu không liên quan đến cá nhân), trong khi PIPL tập trung vào dữ liệu cá nhân - nhưng phạm vi của chúng giao thoa nhau đáng kể. Sự trùng lặp và đôi khi khác biệt trong phạm vi điều chỉnh và thuật ngữ giữa các văn bản này có thể gây lúng túng cho doanh nghiệp trong việc xác định nghĩa vụ tuân thủ. Thêm vào đó, nhiều cơ quan quản lý cùng tham gia ban hành quy định (CAC, Bộ Công an, MIIT,...) khiến khung pháp luật thiếu tính thống nhất. Mặc dù cách tiếp cận phân tán này giúp bao quát nhiều khía cạnh (như đã nêu ở phần ưu điểm), nó cũng dẫn tới tình trạng *"phân mảnh"* trong quản lý dữ liệu - các quy định rời rạc khó tạo thành một hệ thống mạch lạc. Hệ quả là doanh nghiệp phải tuân thủ đồng thời nhiều yêu cầu pháp lý khác nhau, có nguy cơ chồng chéo hoặc mâu thuẫn, làm tăng chi phí tuân thủ và rủi ro vi phạm do hiểu sai quy định.

Thứ hai, *một số khái niệm pháp lý còn mơ hồ - đặc biệt là "dữ liệu quan trọng".* Trung Quốc đã đưa ra các khái niệm phân loại dữ liệu nhằm quản lý rủi ro theo mức độ nhạy cảm (như *dữ liệu thông thường, dữ liệu*

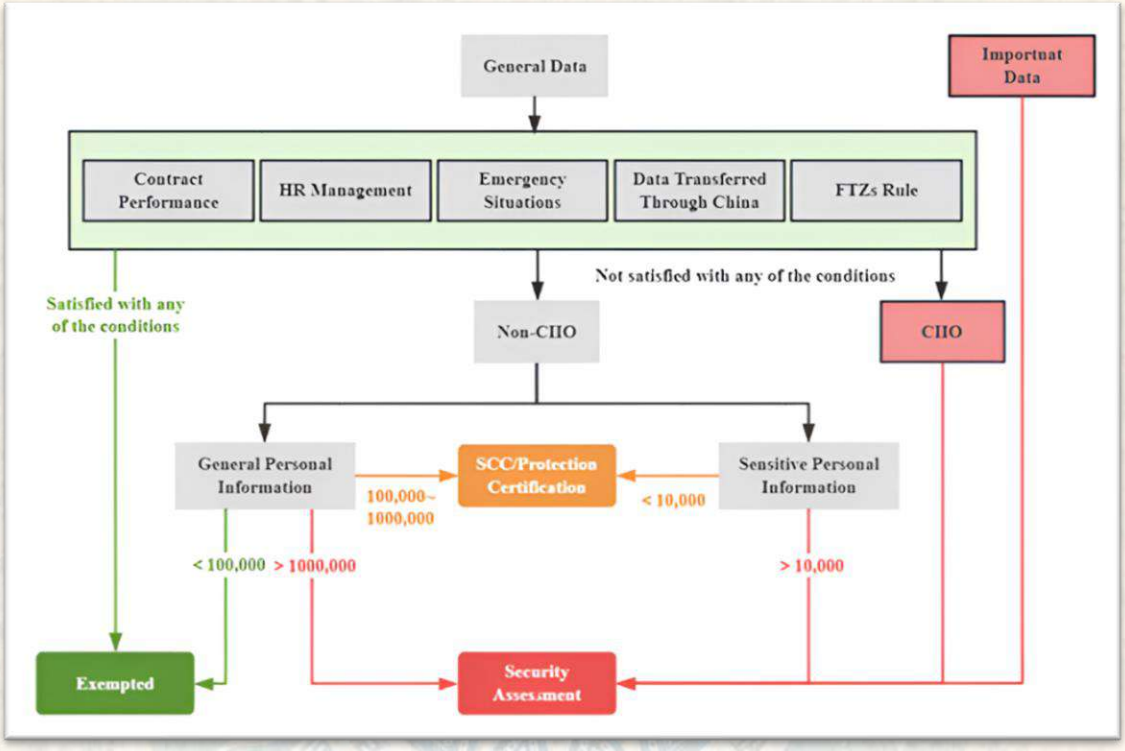
[88] DLA Piper, *Data Protection Laws of the World – People's Republic of China:* nhận định không có một luật duy nhất về bảo vệ dữ liệu cá nhân tại Trung Quốc, mà thay vào đó là "các quy định nằm trong một khung pháp luật phức hợp gồm nhiều luật và văn bản khác nhau".

quan trọng, dữ liệu cốt lõi theo DSL). Tuy nhiên, không phải mọi định nghĩa đều rõ ràng. Đáng chú ý, thuật ngữ *"dữ liệu quan trọng"* (important data) đến nay *vẫn chưa được luật định nghĩa cụ thể*, mới chỉ được mô tả một cách chung chung là dữ liệu mà nếu bị tiết lộ có thể ảnh hưởng đến an ninh quốc gia, trật tự công cộng, lợi ích kinh tế hoặc các ngành trọng yếu [45].

DSL trao cho các ngành và địa phương thẩm quyền xây dựng danh mục *"dữ liệu quan trọng"*, nhưng việc này dẫn đến cách hiểu không thống nhất và tạo sự mơ hồ, lo ngại cho các doanh nghiệp về phạm vi dữ liệu nào bị coi là quan trọng [120]. Các tổ chức phải đối mặt với rủi ro là nếu dữ liệu mình xử lý sau này bị xác định là "quan trọng", họ sẽ chịu nhiều nghĩa vụ nghiêm ngặt (ví dụ: bổ nhiệm cán bộ phụ trách an ninh dữ liệu, tiến hành đánh giá an ninh khi chuyển dữ liệu ra nước ngoài) và chế tài nặng nề nếu vi phạm. Hiện tại, doanh nghiệp phần lớn phải tự đánh giá hoặc tham vấn cơ quan quản lý để xác định dữ liệu của mình có "quan trọng" hay không - một tình trạng thiếu chắc chắn gây khó khăn cho kế hoạch kinh doanh. Đến những năm 2024 - 2025, các nhà làm luật Trung Quốc bước đầu có động thái giảm bớt sự bất định này.

Quy định về Thúc đẩy và Quản lý Dòng chảy Dữ liệu Ra ngoài (3/2024) cho phép doanh nghiệp "giả định dữ liệu của mình không phải là dữ liệu quan trọng, trừ khi dữ liệu đó nằm trong danh mục quan trọng được công bố hoặc họ được cơ quan chức năng thông báo là dữ liệu quan trọng" [120]. Cách tiếp cận *"ngầm định không quan trọng nếu chưa bị liệt kê"* này được cộng đồng doanh nghiệp hoan nghênh vì phần nào giảm bớt rủi ro tuân thủ. Dựa trên quy định mới, các cơ quan trung ương đang gấp rút xây dựng danh mục dữ liệu quan trọng theo từng ngành. Tuy nhiên, cho đến tháng 7/2025, những danh mục như vậy chưa đầy đủ và tính chất "quan trọng" của nhiều

loại dữ liệu vẫn còn phụ thuộc vào diễn giải của nhà chức trách. Sự thiếu rõ ràng trong định nghĩa thuật ngữ pháp lý cốt lõi này đi ngược lại ưu điểm *"phân loại rõ ràng"* của DSL, và đòi hỏi Trung Quốc phải tiếp tục hoàn thiện để khung pháp luật khả thi hơn trong thực tiễn.

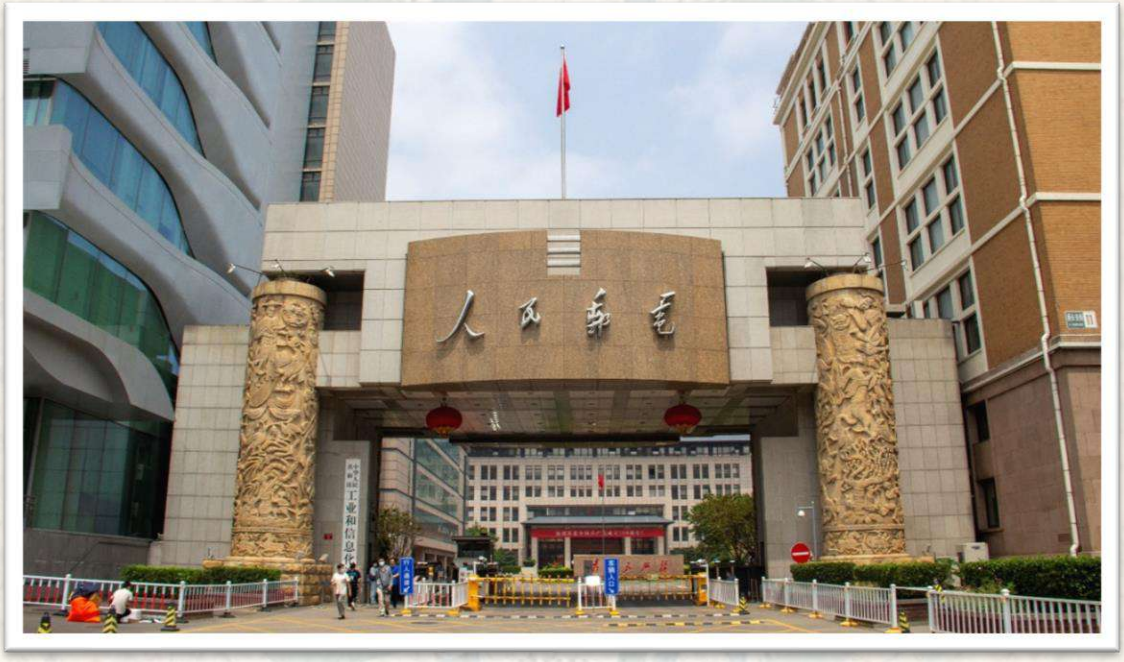


Mô hình của Quy định về Thúc đẩy và Quản lý Dòng chảy Dữ liệu Ra ngoài - Ảnh: Lexology

Thứ ba, *thiếu cơ quan giám sát độc lập về dữ liệu*. Khác với nhiều nước thiết lập cơ quan chuyên trách độc lập (như các Data Protection Authority ở châu Âu) để giám sát việc bảo vệ dữ liệu, Trung Quốc hiện *chưa có một cơ quan độc lập tương tự.* Thay vào đó, chức năng quản lý và thực thi được phân tán cho nhiều cơ quan nhà nước khác nhau, đứng đầu là *Cục Quản lý Không gian mạng Trung Quốc (CAC)* cùng các bộ ngành liên quan.

PIPL thiết lập mô hình phối hợp liên ngành, theo đó "các cơ quan hữu quan của Quốc vụ viện" cùng chia sẻ nhiệm vụ bảo vệ thông tin cá nhân. Cách tiếp cận "phối hợp" này trên thực tế không khắc phục được vấn đề phân mảnh

trong bộ máy quản lý [121]. Mỗi cơ quan có ưu tiên và lợi ích riêng, dẫn đến chồng chéo chức năng hoặc khoảng trống trách nhiệm trong một số trường hợp. Đơn cử, CAC chịu trách nhiệm chính về an ninh mạng và bảo vệ dữ liệu internet, Bộ Công an tập trung vào điều tra các vụ rò rỉ, gian lận dữ liệu, còn MIIT quản lý dữ liệu viễn thông - sự phối hợp liên tục và hiệu quả giữa các đơn vị này không phải lúc nào cũng được đảm bảo. Hơn nữa, do không có một *"Ủy ban bảo vệ dữ liệu"* độc lập ở trung ương, việc bảo vệ quyền riêng tư cá nhân có thể bị xếp sau các ưu tiên chính trị hoặc phát triển kinh tế.



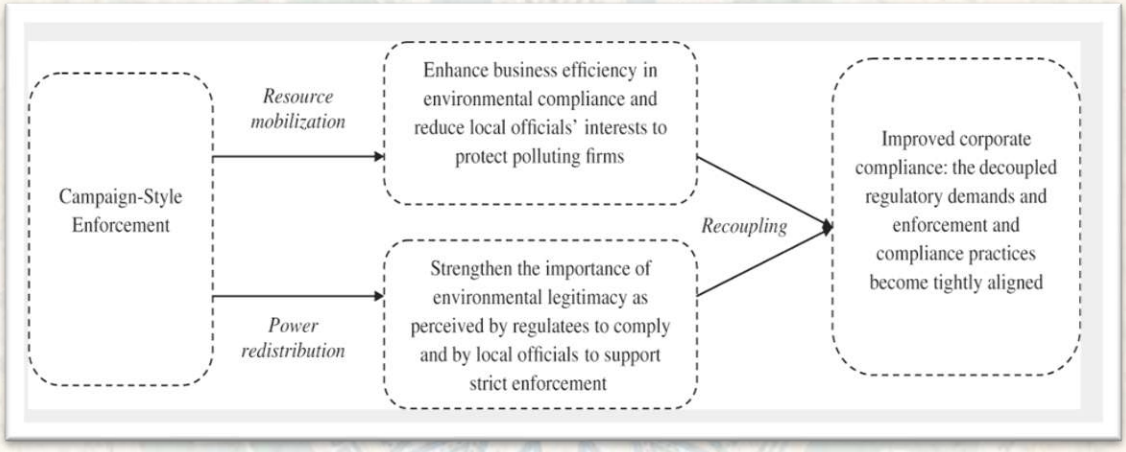
Trụ sở bộ Công nghiệp và Công nghệ thông tin của Trung Quốc (Ministry of Industry and Information Technology - MIIT) - Ảnh: Medium

Giới nghiên cứu cho rằng Trung Quốc *cần thành lập một cơ quan chuyên trách ở cấp quốc gia về bảo vệ dữ liệu cá nhân* - một mô hình "cơ quan chuyên môn hóa" - để đảm bảo thực thi nhất quán và cân bằng giữa bảo vệ quyền cá nhân với phát triển dữ liệu. Việc thiếu một thiết chế độc lập còn kéo theo lo ngại về tính minh bạch và trách nhiệm giải trình trong quá trình thực thi pháp luật. Hiện nay, CAC là một cơ quan thuộc hệ thống Đảng

- Nhà nước; mặc dù có quyền lực rất lớn trong quản lý dữ liệu, CAC lại thiếu các thuộc tính minh bạch, trách nhiệm giải trình như một cơ quan hành chính độc lập [105]. Thực tế này khiến doanh nghiệp và công chúng khó có kênh độc lập để khiếu nại hoặc giám sát các quyết định về dữ liệu. Nói cách khác, môi trường pháp lý tuy được củng cố bởi sự điều hành tập trung của nhà nước (mang lại ưu điểm "ổn định" bề ngoài), nhưng đồng thời lại thiếu vắng cơ chế kiểm tra, đối trọng độc lập để bảo đảm quyền lợi của các chủ thể dữ liệu được bảo vệ một cách khách quan, nhất quán.

Thứ tư, *công tác thực thi chủ yếu theo mô hình "chiến dịch", khó bền vững.* Một đặc thù trong quản lý của Trung Quốc là việc phát động những chiến dịch cao điểm theo từng đợt nhằm chấn chỉnh vi phạm pháp luật, và lĩnh vực dữ liệu cũng không ngoại lệ. Thay vì xây dựng cơ chế giám sát thường xuyên và lâu dài, các cơ quan Trung Quốc thường tiến hành các đợt cao điểm cưỡng chế tập trung trong thời gian ngắn (chẳng hạn, chiến dịch "Thanh lọc mạng" năm 2018 - 2019 truy quét hàng chục ngàn vụ vi phạm dữ liệu cá nhân). Cách làm này giúp đạt kết quả nhanh trong việc răn đe, xử phạt các hành vi sai phạm, nhưng lại *không tạo được nền tảng tuân thủ bền vững*. Nhiều doanh nghiệp có thể chỉ tăng cường tuân thủ trong thời gian chiến dịch diễn ra, sau đó mức độ tuân thủ lại giảm khi chiến dịch kết thúc. Hơn nữa, việc thực thi theo chiến dịch thường gắn với các mục tiêu chính trị hoặc sự kiện cụ thể, dẫn đến tính gián đoạn và khó dự đoán. Chẳng hạn, năm 2021 Trung Quốc bất ngờ mở cuộc điều tra an ninh mạng đối với tập đoàn gọi xe Didi ngay sau khi doanh nghiệp này IPO ở Mỹ, và một năm sau áp dụng mức phạt kỷ lục 1,2 tỷ USD vì vi phạm luật an ninh mạng, an toàn dữ liệu và bảo vệ thông tin cá nhân. Tuy nhiên, quyết định xử phạt không được công bố chi tiết, viện lý do an ninh quốc gia, khiến dư luận và các công ty

khác "không có hướng dẫn rõ ràng về cách tuân thủ" trong một môi trường pháp lý dữ liệu phức tạp, luôn biến động [105]. Đây chính là hệ quả của lối thực thi thiếu minh bạch và nhất quán: doanh nghiệp khó rút ra bài học cụ thể để tự điều chỉnh, trong khi người dân và giới học giả khó đánh giá được hiệu quả thực thi. Về tổng thể, mô hình *"cưỡng chế theo chiến dịch"* (campaign-style enforcement) được thúc đẩy từ trên xuống với các chỉ tiêu ngắn hạn, thưởng phạt rõ rệt, có thể huy động nhanh nguồn lực thực thi nhưng thường đi kèm những hạn chế cố hữu.



Cách thức vận hành của Mô hình Campaign - style enforcement - Ảnh: Wiley

Nghiên cứu chỉ ra rằng các chiến dịch hành pháp kiểu này thiếu tính cân bằng, thiếu quy trình pháp lý bài bản, thiếu tương xứng giữa vi phạm và chế tài, làm suy giảm tính dự báo và ổn định của pháp luật trong dài hạn. Do đó, dù trước mắt tạo ấn tượng về một môi trường pháp lý "ổn định" (với các đợt ra quân mạnh tay), về lâu dài cách làm này có thể *gây biến động và thiếu bền vững*, làm xói mòn lòng tin của doanh nghiệp vào hệ thống pháp luật.

Thứ năm, *áp lực tuân thủ gia tăng do cập nhật pháp lý nhanh và liên tục.* Khuôn khổ pháp luật về dữ liệu tại Trung Quốc đang phát triển với tốc độ rất nhanh. Chỉ trong vòng vài năm, hàng loạt văn bản quan trọng liên tiếp được ban hành, tạo ra *gánh nặng tuân thủ đáng kể cho doanh nghiệp*. Sau

khi CSL (2017), DSL và PIPL (2021) có hiệu lực, chính quyền Trung Quốc tiếp tục chi tiết hóa bằng nhiều quy định mới: chẳng hạn, *Biện pháp Đánh giá Bảo mật Dữ liệu Xuất cảnh* (có hiệu lực từ tháng 9/2022) yêu cầu doanh nghiệp xin cấp phép trước khi chuyển ra nước ngoài dữ liệu "quan trọng" hoặc dữ liệu cá nhân quy mô lớn; *Biện pháp Hợp đồng Mẫu về chuyển dữ liệu cá nhân ra nước ngoài* (có hiệu lực từ tháng 6/2023) đưa ra mẫu hợp đồng chuẩn và yêu cầu nộp hồ sơ lên CAC; *Quy định Quản lý An ninh Dữ liệu Mạng* (Network Data Security Regulations - NDSR, có hiệu lực từ 1/1/2025) bổ sung hàng loạt nghĩa vụ mới về bảo mật dữ liệu; cùng với đó là các hướng dẫn mới về đánh giá dữ liệu xuyên biên giới (ban hành 3/2024) và biện pháp kiểm toán tuân thủ bảo vệ thông tin cá nhân (có hiệu lực từ 1/5/2025) đòi hỏi doanh nghiệp định kỳ tự đánh giá và báo cáo việc tuân thủ PIPL. Chính phủ Trung Quốc vẫn đang *liên tục sửa đổi, bổ sung quy định* nhằm hoàn thiện khung pháp luật - *"các luật nền tảng đặt ra, nhưng vô số sửa đổi, hướng dẫn mới và cách thức thực thi biến đổi đòi hỏi doanh nghiệp không thể lơ là cập nhật"* [46]. Mặc dù điều này cho thấy nỗ lực kịp thời điều chỉnh chính sách trước công nghệ và rủi ro mới, nó cũng khiến môi trường pháp lý thiếu ổn định tương đối cho hoạt động kinh doanh. Nhiều doanh nghiệp, đặc biệt là doanh nghiệp vừa và nhỏ, gặp khó khăn trong việc theo dõi và tuân thủ tất cả các yêu cầu mới ban hành với tần suất dày đặc. Chẳng hạn, *Quy định An ninh Dữ liệu Mạng 2025* được công bố cuối tháng 9/2024 nhưng chỉ cho thời gian chuẩn bị vỏn vẹn 3 tháng trước khi áp dụng, buộc các công ty phải gấp rút đánh giá lại hệ thống dữ liệu của mình. Tương tự, *Biện pháp Kiểm toán Tuân thủ* yêu cầu những công ty xử lý lượng lớn dữ liệu cá nhân phải tiến hành kiểm toán định kỳ mỗi 2 năm và nộp kết quả cho cơ quan quản lý, tạo thêm chi phí tuân thủ mới. Việc pháp luật thay đổi liên

tục, "luôn trong trạng thái vận động" với các cập nhật thường xuyên, có thể dẫn tới tình trạng *"trì trệ"* trong khâu pháp lý cho doanh nghiệp khi họ phải đầu tư nguồn lực đáng kể cho việc điều chỉnh quy trình nội bộ, tập huấn nhân viên, thuê tư vấn pháp lý… gần như liên tục. Nếu không kịp thích ứng, doanh nghiệp đứng trước rủi ro vi phạm và bị phạt nặng theo chế tài nghiêm khắc của luật Trung Quốc. Áp lực tuân thủ gia tăng do cập nhật pháp luật nhanh và thường xuyên này phần nào làm giảm hiệu quả của ưu điểm *"môi trường pháp lý ổn định"* - bởi lẽ trên thực tế, các quy tắc vẫn đang thay đổi không ngừng. Điều này đặt ra nhu cầu về các cơ chế hỗ trợ tuân thủ (hướng dẫn thực thi rõ ràng, gia hạn thời gian áp dụng, phổ biến pháp luật sâu rộng hơn) để doanh nghiệp có thể theo kịp và thực thi đúng các quy định mới, qua đó mục tiêu bảo vệ dữ liệu của pháp luật được hiện thực hóa một cách bền vững.

1.2.4. Hàn Quốc

1.2.4.1. Tổng quan về chính sách, pháp luật về dữ liệu tại Hàn Quốc

Hàn Quốc là một trong những quốc gia tiên phong trong việc thúc đẩy chính sách dữ liệu mở và phát triển sáng kiến về dữ liệu số. Chính sách này không chỉ giúp cải thiện tính minh bạch của Chính phủ mà còn khuyến khích sự phát triển của các doanh nghiệp và dịch vụ dựa trên dữ liệu. Theo đó, khung pháp lý về bảo vệ dữ liệu tại Hàn Quốc được xây dựng trên một nền tảng đa tầng, phản ánh sự nhận thức sâu sắc về tầm quan trọng của quyền riêng tư trong kỷ nguyên số. Hệ thống này không chỉ giới hạn ở một đạo luật duy nhất mà bao gồm ba văn bản chính, mỗi văn bản quản lý một lĩnh vực dữ liệu cụ thể. Đạo luật Bảo vệ Thông tin Cá nhân (PIPA) đóng vai trò là đạo luật khung, áp dụng cho việc xử lý thông tin cá nhân của các bên kiểm soát dữ liệu trong cả khu vực công và tư. Cùng với PIPA, Đạo luật về Sử dụng và Bảo vệ Thông tin Tín dụng (CIA) điều chỉnh các vấn đề liên quan đến dữ

liệu tín dụng, trong khi Đạo luật về Bảo vệ và Sử dụng Thông tin Vị trí (LIA) tập trung vào dữ liệu vị trí cá nhân. Sự tồn tại của các đạo luật chuyên biệt này cho thấy một cách tiếp cận chi tiết, nhằm giải quyết các rủi ro riêng của từng loại dữ liệu. Bên cạnh đó, Đạo luật về Thúc đẩy Mạng lưới Thông tin và Truyền thông cũng cung cấp các quy định bổ sung, đặc biệt trong lĩnh vực thương mại điện tử và các hoạt động trực tuyến.

Đặc biệt, Luật dữ liệu Mở của Hàn Quốc, được gọi là Luật Khuyến khích cung cấp và sử dụng dữ liệu Công (Act on Promotion of the Provision and Use of Public Data), đã được Quốc hội Hàn Quốc thông qua vào ngày 30/7/2013 và có hiệu lực từ 30/7/2013. Luật dữ liệu Mở Hàn Quốc (Open Data Act) được ban hành nhằm tạo ra hệ thống mở cho dữ liệu công của Chính phủ và các tổ chức công, qua đó thúc đẩy sự phát triển của nền kinh tế số và giúp cải thiện hiệu quả hoạt động của các cơ quan nhà nước.

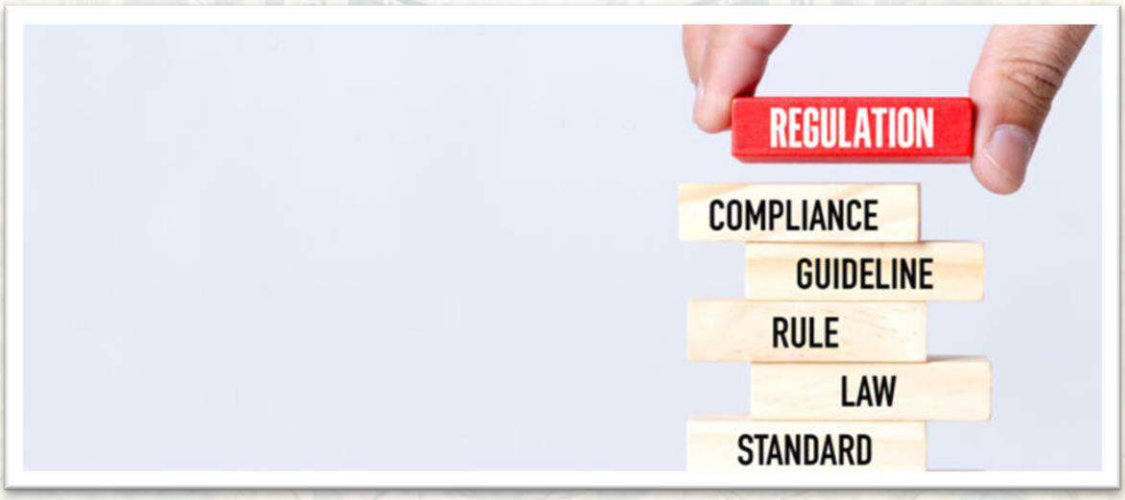
1.2.4.2. Đạo luật Bảo vệ thông tin cá nhân (PIPA) của Hàn Quốc

- Các sửa đổi quan trọng và nguyên tắc "Cùng hành vi - Cùng quy định" trong PIPA Hàn Quốc

Một trong những bước tiến quan trọng nhất trong lịch sử pháp lý dữ liệu của Hàn Quốc là các sửa đổi lớn đối với PIPA vào năm 2023, có hiệu lực từ ngày 15 tháng 9 năm 2023. Các sửa đổi này được xây dựng trên nguyên tắc cốt lõi là "cùng hành vi - cùng quy định" (same conduct - same regulation). Nguyên tắc này đã bãi bỏ các điều khoản đặc biệt trước đây chỉ áp dụng cho các Nhà cung cấp Dịch vụ Trực tuyến (OSP), đồng nghĩa với việc tất cả các bên kiểm soát dữ liệu cá nhân hiện phải tuân thủ một bộ quy tắc thống nhất, không phân biệt bản chất hoạt động của họ[89].

[89] Baker McKenzie (2024), *South Korea data privacy laws* 2024, https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/asia-pacific/south-korea/topics/whats-new, truy cập ngày 01/8/2025.

Việc xóa bỏ sự phân biệt giữa các OSP và các nhà kinh doanh truyền thống là một chiến lược pháp lý sâu sắc. Trong một nền kinh tế kỹ thuật số, ranh giới giữa các mô hình kinh doanh đã trở nên mờ nhạt, và việc duy trì các quy định phân mảnh sẽ tạo ra sự không công bằng. Bằng cách áp dụng một tiêu chuẩn chung, Hàn Quốc đang dịch chuyển khỏi mô hình quy định cũ, hướng tới một hệ thống toàn diện hơn, tương tự như Khuôn khổ Bảo vệ Dữ liệu Chung của Liên minh Châu Âu (GDPR). Điều này không chỉ tạo ra một sân chơi cạnh tranh bình đẳng giữa các công ty trong nước và quốc tế, mà còn giữa các công ty công nghệ và phi công nghệ, bởi tất cả đều phải đáp ứng cùng một mức độ tuân thủ nghiêm ngặt. Ủy ban Bảo vệ Thông tin Cá nhân (PIPC), cơ quan chịu trách nhiệm thực thi PIPA, đã tích cực làm việc để cụ thể hóa các sửa đổi này, với việc đề xuất Nghị định Thi hành vào tháng 4 năm 2024 để cung cấp các chi tiết phụ trợ cần thiết.



Ảnh minh họa - Ảnh: Internet

- Cơ quan thực thi

Như đã đề cập, Ủy ban Bảo vệ Thông tin Cá nhân (PIPC) là cơ quan quản lý và thực thi chính đối với PIPA. PIPC có nhiều trách nhiệm và quyền hạn, bao gồm: thiết lập và thực thi các chính sách bảo vệ dữ liệu; tiến hành

điều tra các vi phạm; ban hành lệnh khắc phục; xử lý khiếu nại và hợp tác với các tổ chức quốc tế.

- Pháp luật về dữ liệu đối với các tổ chức nước ngoài

PIPA có phạm vi áp dụng rộng, mở rộng ra ngoài lãnh thổ Hàn Quốc. Đạo luật này áp dụng cho các công ty nước ngoài cung cấp hàng hóa hoặc dịch vụ cho, hoặc giám sát hành vi của, các chủ thể dữ liệu Hàn Quốc. Điều này cho thấy một sự thay đổi đáng kể trong cách tiếp cận của PIPC, từ việc tập trung vào các thực thể trong nước sang việc khẳng định quyền hạn của mình trên phạm vi toàn cầu. Các vụ việc chống lại Alibaba.com Singapore (AliExpress) và Meta Platforms là những ví dụ điển hình. PIPC đã áp dụng các khoản phạt và lệnh khắc phục đối với các công ty này, gửi một thông điệp rõ ràng rằng các nhà điều hành nước ngoài cũng phải tuân thủ các yêu cầu pháp lý của PIPA khi họ hoạt động trong thị trường Hàn Quốc[90].



South Korea's Personal Information Protection Act PIPA - Ảnh: Pandectes

Việc PIPC tích cực thực thi luật pháp của mình chống lại các công ty toàn cầu không chỉ là một hành động đơn lẻ mà là một sự khẳng định quyền lực trong bối cảnh toàn cầu hóa. Bằng cách áp dụng các hình phạt và lệnh

[90] Personal Information Protection Commission (2023), *PIPC imposes corrective orders and recommendations on AliExpress*, https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=2602, truy cập ngày 01/8/2025.

khắc phục, PIPC đã cho thấy các doanh nghiệp nước ngoài không thể bỏ qua các quy định của Hàn Quốc. Điều này có thể dẫn đến việc các công ty quốc tế phải đầu tư đáng kể vào việc tuân thủ pháp luật Hàn Quốc, có khả năng tạo ra một "hiệu ứng Brussels" (Brussels effect), nơi các quy định nghiêm ngặt của một khu vực ảnh hưởng đến tiêu chuẩn toàn cầu. Để củng cố thêm việc thực thi này, PIPA cũng quy định rằng các doanh nghiệp nước ngoài không có địa chỉ hoặc văn phòng tại Hàn Quốc phải chỉ định một đại diện trong nước để xử lý các vấn đề về quyền riêng tư[91].

- Các khái niệm được đề cập

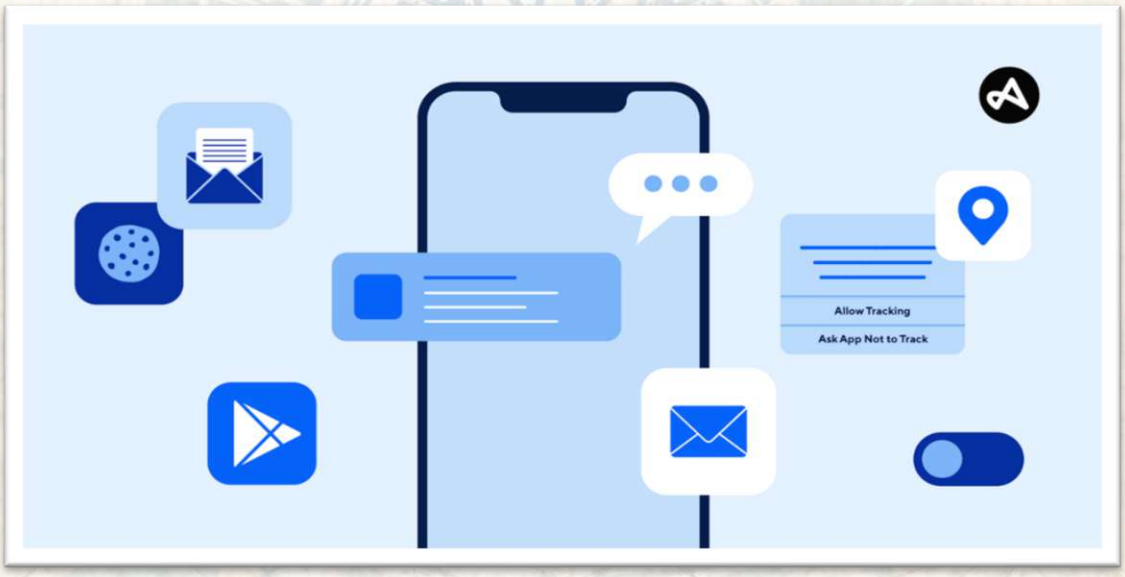
PIPA phân biệt rõ ràng giữa thông tin cá nhân thông thường và các loại dữ liệu có mức độ nhạy cảm cao hơn, đặt ra các quy tắc xử lý nghiêm ngặt hơn cho từng loại. Trong đó, khái niệm *"Thông tin nhận dạng duy nhất"* được đề cập, bao gồm số đăng ký cư trú (RRN), số bằng lái xe và số hộ chiếu. Trong số này, việc xử lý RRN bị kiểm soát chặt chẽ nhất. PIPA cấm xử lý RRN trừ khi có một đạo luật đặc biệt yêu cầu hoặc cho phép, hoặc khi việc đó là cần thiết để bảo vệ tính mạng, lợi ích cơ thể và tài sản của chủ thể dữ liệu. Điều này có nghĩa là ngay cả khi có sự đồng ý của chủ thể dữ liệu, việc xử lý RRN vẫn là bất hợp pháp nếu không có cơ sở pháp lý rõ ràng. Để đảm bảo an toàn, bên kiểm soát dữ liệu có nghĩa vụ mã hóa RRN để ngăn chặn việc mất mát, trộm cắp, hoặc rò rỉ.

- Các nguyên tắc cơ bản. PIPA quy định rằng việc xử lý thông tin cá nhân phải tuân thủ một số nguyên tắc cơ bản: dữ liệu phải được thu thập cho các mục đích cụ thể, hợp pháp, và chỉ giới hạn ở mức tối thiểu cần thiết để đạt được các mục đích đó. Cơ sở pháp lý phổ biến nhất để xử lý thông tin cá

[91] Global Referral Network (2025), *Personal Information Protection Act (PIPA) Updates – 2025*, https://globalreferral.group/personal-information-protection-act-pipa-updates-2025/, truy cập ngày 01/8/2025.

nhân là sự đồng ý rõ ràng của chủ thể dữ liệu, được gọi là phương pháp "chấp thuận tham gia" (opt-in). Khi xin sự đồng ý, bên kiểm soát dữ liệu phải thông báo cho chủ thể dữ liệu về các vấn đề sau: mục đích thu thập và sử dụng, các mục thông tin sẽ được thu thập, thời gian lưu giữ và sử dụng, và hậu quả của việc từ chối đồng ý[92].

Tuy nhiên, PIPA cũng đưa ra các trường hợp ngoại lệ quan trọng, cho phép xử lý dữ liệu mà không cần sự đồng ý, bao gồm: Khi có quy định đặc biệt trong một đạo luật khác; Khi cần thiết để thực hiện một thỏa thuận đã ký với chủ thể dữ liệu; Khi cần thiết để bảo vệ tính mạng, lợi ích cơ thể và tài sản khỏi nguy cơ cận kề; Khi cần thiết để đạt được lợi ích hợp pháp của bên kiểm soát dữ liệu, miễn là lợi ích đó rõ ràng cao hơn quyền của chủ thể dữ liệu.



Ảnh minh họa chấp thuận tham gia (opt-in) - Ảnh: Adjust

- Quy định về chuyển dữ liệu xuyên biên giới. Theo quy tắc chung, một bên kiểm soát dữ liệu không được cung cấp thông tin cá nhân cho bên thứ ba ở nước ngoài nếu không có sự đồng ý "chấp thuận tham gia" (opt-in) của

[92] Linklaters (2024), *Data Protected - Republic of Korea,* https://www.linklaters.com/insight s/data-protected/data-protected---republic-of-korea, truy cập ngày 01/8/2025.

chủ thể dữ liệu. PIPA yêu cầu phải thông báo rõ ràng cho chủ thể dữ liệu về bên nhận, quốc gia đích, mục đích sử dụng, và thời gian lưu giữ dữ liệu. Tuy nhiên, có một số trường hợp ngoại lệ cho phép chuyển giao xuyên biên giới mà không cần sự đồng ý, chẳng hạn như khi có quy định đặc biệt trong luật pháp, hiệp ước hoặc khi việc đó là cần thiết để thực hiện một thỏa thuận với chủ thể dữ liệu và đã được tiết lộ rõ ràng trong chính sách quyền riêng tư.

Việc PIPC thực thi quyết liệt các quy định này đã được thể hiện qua các vụ việc nổi bật. Vụ việc PIPC tạm đình chỉ hoạt động của ứng dụng AI DeepSeek vì chuyển dữ liệu người dùng Hàn Quốc sang Trung Quốc và Mỹ mà không có sự đồng ý, đã gửi một cảnh báo mạnh mẽ tới các công ty toàn cầu về tầm quan trọng của việc tuân thủ các quy tắc này[93]. Tương tự, PIPC đã phạt AliExpress vì không thông báo đầy đủ cho người dùng Hàn Quốc về việc chuyển giao dữ liệu xuyên biên giới và làm cho việc thực hiện quyền của họ trở nên khó khăn. Các vụ việc này cho thấy rằng việc thiếu minh bạch hoặc không có sự đồng ý rõ ràng về việc chuyển giao dữ liệu xuyên biên giới là một vi phạm nghiêm trọng và sẽ bị xử lý.

- *Hệ thống chế tài.* Việc không tuân thủ PIPA có thể dẫn đến một loạt các hình phạt, bao gồm phụ phí hành chính, phạt hành chính, lệnh khắc phục và chế tài hình sự. Mức phụ phí hành chính có thể lên tới 3% doanh thu trung bình hàng năm trong ba năm kinh doanh gần nhất đối với các vi phạm nghiêm trọng. Đối với các vi phạm hình sự, chẳng hạn như chuyển giao dữ liệu cá nhân cho bên thứ ba mà không có sự đồng ý, cả bên chuyển và bên nhận đều có thể phải chịu mức phạt tù lên đến 5 năm hoặc phạt tiền lên đến 50 triệu KRW.

---

[93] Quảng Ngãi TV (2025), *Deepseek chuyển thông tin người dùng Hàn Quốc ra nước ngoài,* https://quangngaitv.vn/deepseek-chuyen-thong-tin-nguoi-dung-han-quoc-ra-nuoc-ngoai-6502104.html, truy cập ngày 01/8/2025

- Đạo luật về Bảo vệ và Sử dụng thông tin vị trí. Bên cạnh PIPA, Đạo luật về Bảo vệ và Sử dụng thông tin vị trí (LIA) là khuôn khổ pháp lý chuyên biệt quản lý dữ liệu vị trí cá nhân. LIA do Ủy ban Truyền thông Hàn Quốc (KCC) quản lý và thực thi. Các sửa đổi năm 2022 của LIA là một sự thay đổi đáng chú ý. Các quy định đã chuyển đổi từ *hệ thống cấp phép* sang *hệ thống đăng ký* để hoạt động kinh doanh dữ liệu vị trí. Sự thay đổi này được đưa ra để đáp ứng sự tăng trưởng nhanh chóng của thị trường dịch vụ dựa trên vị trí (LBS), được thúc đẩy bởi sự phổ biến của mạng 5G và các ứng dụng IoT trong nhiều ngành công nghiệp. Việc giảm bớt gánh nặng hành chính cho các doanh nghiệp, đặc biệt là các startup, có thể thúc đẩy đổi mới, trong khi các yêu cầu mới về sự đồng ý đối với mục đích và thời gian lưu giữ, cùng với nghĩa vụ thiết lập một chính sách dữ liệu vị trí rõ ràng, vẫn đảm bảo quyền riêng tư không bị xâm phạm.

Nhìn chung, chính sách và pháp luật dữ liệu của Hàn Quốc đang tiếp cận các tiêu chuẩn toàn cầu như GDPR, với một cách tiếp cận chủ động và thích ứng với các công nghệ mới nổi. Việc tập trung vào AI, dữ liệu vị trí và các quy định về chuyển giao dữ liệu xuyên biên giới cho thấy sự nhạy bén của các nhà quản lý trong việc đối phó với những thách thức của kỷ nguyên số. Các thay đổi vẫn đang tiếp diễn, đặc biệt là việc thực thi quyền chuyển đổi dữ liệu và Đạo luật Khung AI, hứa hẹn sẽ định hình thêm nữa bối cảnh pháp lý trong những năm tới và củng cố vị thế của Hàn Quốc như một trong những quốc gia đi đầu về bảo vệ quyền riêng tư và dữ liệu.

1.2.4.3. Đạo luật Dữ liệu mở của Hàn Quốc

- Mục tiêu và tầm quan trọng của Luật dữ liệu Mở của Hàn Quốc

Luật Dữ liệu Mở của Hàn Quốc được xây dựng với các mục tiêu chính là:

+ Tăng cường minh bạch và trách nhiệm giải trình của Chính phủ: Chính phủ Hàn Quốc nhận thức rõ rằng việc cung cấp dữ liệu công khai

không chỉ giúp người dân và các tổ chức có quyền truy cập vào các thông tin quan trọng mà còn thúc đẩy sự tin tưởng của công chúng đối với các cơ quan nhà nước.

+ *Thúc đẩy đổi mới sáng tạo và phát triển kinh tế:* Việc mở rộng quyền truy cập vào dữ liệu công sẽ tạo ra cơ hội cho các doanh nghiệp, đặc biệt là các startup, trong việc phát triển các dịch vụ và ứng dụng dựa trên dữ liệu mở.

+ *Tạo điều kiện cho các sáng kiến hợp tác:* Hàn Quốc muốn khuyến khích các cơ quan Chính phủ, các doanh nghiệp và các tổ chức khác hợp tác để tận dụng dữ liệu mở trong việc phát triển các giải pháp sáng tạo phục vụ cho cộng đồng.

+ *Nâng cao sự tham gia của công dân:* Dữ liệu mở cũng giúp tăng cường sự tham gia của công dân trong các quá trình ra quyết định của Chính phủ, đồng thời tạo ra các cơ hội để công dân có thể giám sát và đóng góp vào việc quản lý các nguồn tài nguyên công.

- Các điểm nổi bật của Luật Dữ liệu mở Hàn Quốc

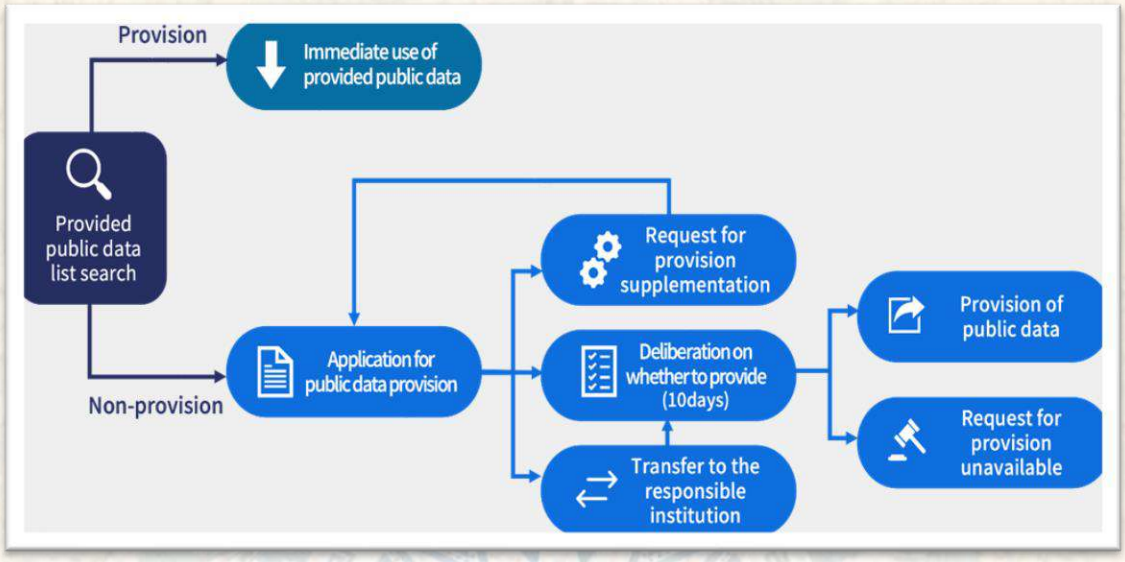
Luật Dữ liệu mở Hàn Quốc được thiết kế để tạo ra một cơ chế toàn diện cho việc quản lý, chia sẻ và sử dụng dữ liệu công. Một số điểm nổi bật trong luật này bao gồm:

Một là, *Cơ chế mở đối với dữ liệu công.*

Một trong những yếu tố quan trọng nhất của Luật Dữ liệu Mở là yêu cầu các cơ quan nhà nước và các tổ chức công phải công khai các dữ liệu mà họ thu thập được. Các cơ quan nhà nước sẽ phải chia sẻ các dữ liệu công này thông qua các nền tảng mở và dễ tiếp cận.

+ *Danh mục dữ liệu công:* Mỗi cơ quan nhà nước phải công khai danh mục các dữ liệu mà họ sở hữu và quản lý, cho phép người dân và các tổ chức có thể dễ dàng tiếp cận.

+ Dữ liệu mở có thể sử dụng lại: Dữ liệu mở không chỉ đơn thuần là dữ liệu có sẵn mà còn phải được cung cấp trong các định dạng dễ sử dụng, có thể tái sử dụng và dễ dàng phân tích.



Yêu cầu Dữ liệu mở của Chính phủ- Ảnh: Data.go.kr

Hai là, *Quản lý và bảo mật dữ liệu.*

Mặc dù Luật Dữ liệu Mở yêu cầu chia sẻ dữ liệu công khai, nhưng luật này cũng có các biện pháp bảo vệ để bảo đảm rằng thông tin cá nhân và dữ liệu nhạy cảm không bị lạm dụng. Các dữ liệu cá nhân sẽ được bảo vệ theo các quy định của Luật bảo vệ thông tin cá nhân, bảo đảm rằng dữ liệu mở không xâm phạm quyền riêng tư của công dân.

+ Kiểm soát và phân loại dữ liệu: Các cơ quan sẽ phải phân loại dữ liệu và chỉ công khai những dữ liệu không chứa thông tin cá nhân hoặc nhạy cảm.

+ Bảo đảm tính bảo mật: Các biện pháp bảo mật được yêu cầu đẻ ngăn ngừa các mối đe dọa và bảo mật và rò rỉ dữ liệu.

Ba là, *Khuyến khích sự tham gia của các tổ chức ngoài khu vực công.*

Một điểm quan trọng của Luật Dữ liệu Mở của Hàn Quốc là khuyến khích sự tham gia của các tổ chức ngoài khu vực công, bao gồm các doanh

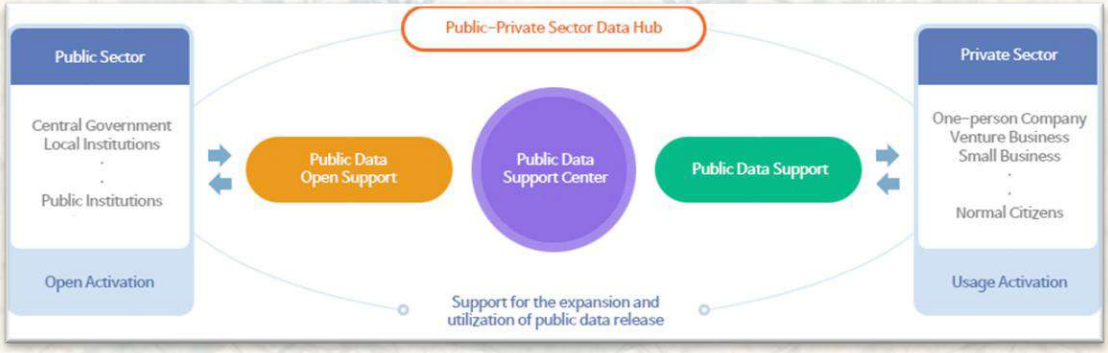
nghiệp, tổ chức nghiên cứu và các nhóm cộng đồng. Các tổ chức này có thể sử dụng dữ liệu mở để phát triển các ứng dụng, dịch vụ và sản phẩm mới.

+ *Hợp tác công - tư:* Luật khuyến khích các mô hình hợp tác giữa các cơ quan Chính phủ và các tổ chức tư nhân trong việc khai thác và sử dụng dữ liệu mở. Điều này có thể dẫn đến việc phát triển các công nghệ mới và các giải pháp sáng tạo cho các vấn đề xã hội.

+ *Đưa dữ liệu vào các ngành công nghiệp:* Dữ liệu mở có thể giúp các doanh nghiệp và ngành công nghiệp phát triển các sản phẩm và dịch vụ dựa trên dữ liệu, từ đó thúc đẩy sự sáng tạo và đổi mới.

Bốn là, *Các nền tảng dữ liệu mở.*

Hàn Quốc đã xây dựng các nền tảng dữ liệu mở chính thức, nơi công dân và các tổ chức dễ dàng truy cập vào dữ liệu công. Một trong các nền tảng quan trọng là Open Data Portal của Chính phủ Hàn Quốc, nơi cung cấp hơn 10 triệu bộ dữ liệu từ hơm 1.000 cơ quan và tổ chức công.



Mô hình OGD Portal của Hàn Quốc - Ảnh: 공공데이터포털

+ *Dễ dàng truy cập:* Các nền tảng này cho phép người dùng truy cập vào dữ liệu một cách dễ dàng và tiện lợi. Dữ liệu cung cấp trong các định dạng tiêu chuẩn, dễ dàng cho việc phân tích và sử dụng lại.

+ *Dữ liệu được cập nhật thường xuyên:* Các bộ dữ liệu được cập nhật liên tục, giúp bảo đảm tính chính xác và kịp thời của thông tin.

- Tác động của Luật Dữ liệu Mở đối với nền kinh tế và xã hội Hàn Quốc

Luật Dữ liệu Mở Hàn Quốc có tác động sâu rộng đến cả nền kinh tế và xã hội quốc gia. Một số tác động tích cực bao gồm:

+ *Thúc đẩy sự sáng tạo và đổi mới:* Các doanh nghiệp có thể sử dụng dữ liệu mở để phát triển các ứng dụng và dịch vụ mới, đồng thời giúp các startup và công ty nhỏ hơn tiếp cận các tài nguyên dữ liệu công.

+ *Tăng cường hiệu quả quản lý của Chính phủ:* Chính phủ có thể sử dụng dữ liệu mở để cải thiện việc ra quyết định và quản lý các dịch vụ công, từ đó nâng cao hiệu quả hoạt động của các cơ quan nhà nước.

+ *Cải thiện sự tham gia của công dân:* Công dân có thể dễ dàng truy cập vào các thông tin công khai và tham gia vào các quá trình ra quyết định của Chính phủ, từ đó nâng cao sự minh bạch và trách nhiệm giải trình.

1.2.5. Nhật Bản

Trong bối cảnh toàn cầu hóa và sự bùng nổ của công nghệ thông tin, việc quản lý và bảo vệ dữ liệu cá nhân đã trở thành một thách thức pháp lý và xã hội cấp bách. Tháng 6/2021, Nhật Bản công bố *"Chiến lược dữ liệu quốc gia"*, đây là chiến lược dữ liệu toàn diện đầu tiên của Nhật Bản, có mục đích là: Thông qua việc bảo đảm sự tin tưởng và lợi ích công cộng, xây dựng khung cấu trúc để sử dụng dữ liệu an toàn và hiệu quả; bảo đảm sự tiến bộ vào bản thân dữ liệu cũng như phương pháp tạo, lưu thông dữ liệu của Nhật Bản trên phạm vi toàn thế giới; xây dựng một xã hội mà thế giới có thể yên tâm lưu trữ dữ liệu tại Nhật Bản.

Để thực hiện chiến lược này, tháng 9/2021, Nhật Bản đã thành lập Cơ quan kỹ thuật số. Trong "Chiến lược dữ liệu quốc gia", Nhật Bản dự kiến kiến trúc quản trị dữ liệu gồm 7 tầng:

- Tầng 1 (cơ sở hạ tầng): 5G, Trung tâm dữ liệu; cơ sở hạ tầng máy tính và cơ sở hạ tầng khác hỗ trợ xã hội số;

- Tầng 2 (dữ liệu): Bắt đầu từ dữ liệu cơ bản của các hoạt động xã hội, xây dựng cấu trúc các dữ liệu cần thiết;

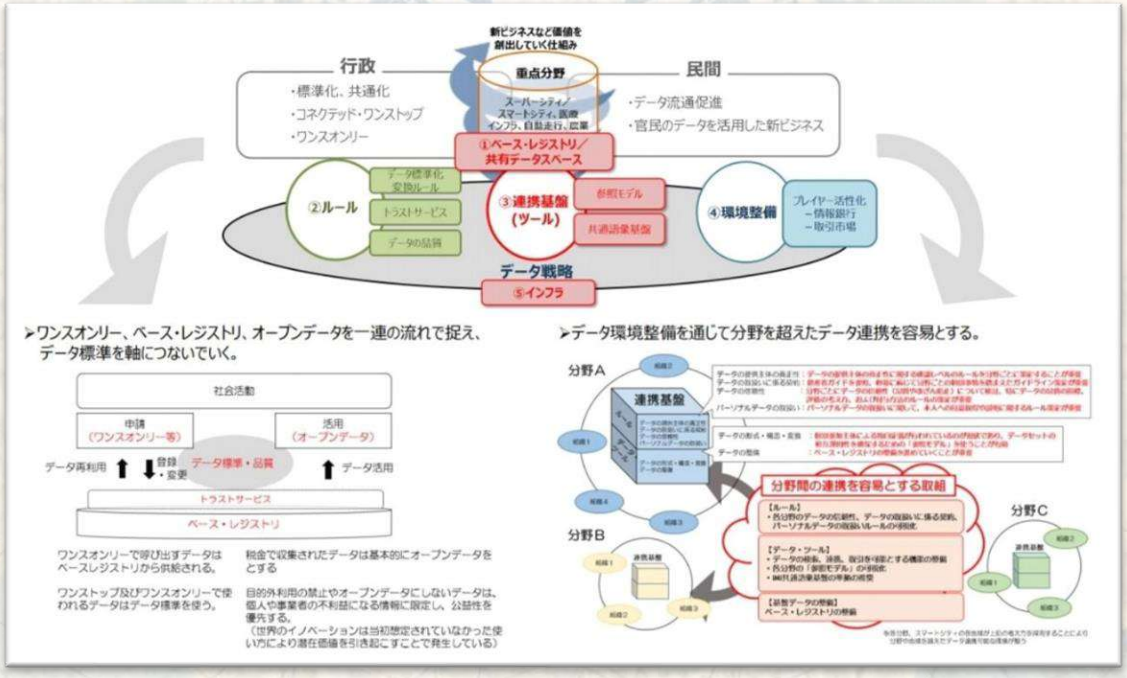
- Tầng 3 (nền tảng hợp tác): Trang bị các công cụ liên kết để tích hợp các dữ liệu một cách có hệ thống;

- Tầng 4 (môi trường sử dụng): Cung cấp môi trường thuận lợi cho các đối tượng khác nhau lưu trữ dữ liệu cá nhân thuận tiện và liên kết chúng với ngân hàng thông tin, thị trường giao dịch dữ liệu;

- Tầng 5 (quy tắc): Ngoài việc hoàn thiện các nguyên tắc cần thiết cho liên kết dữ liệu, còn cần hoàn thiện các quy tắc để các chủ thể an tâm sử dụng dữ liệu;

- Tầng 6 (tổ chức): Cải cách hành chính và công vụ;

- Tầng 7: chiến lược chính sách.

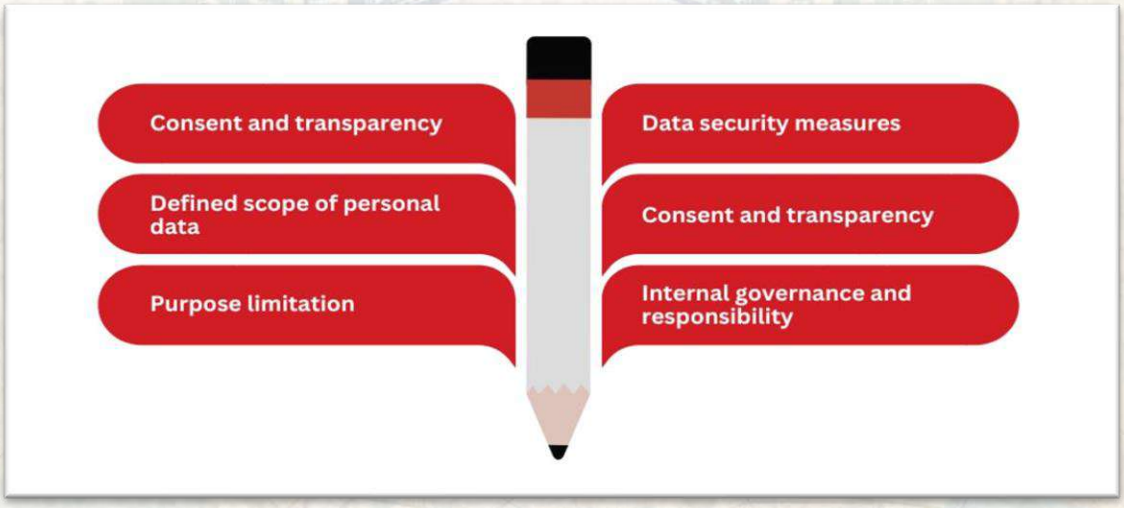


Mô tả cách thức vận hành Chiến lược dữ liệu quốc gia của Nhật Bản - Ảnh: ビジネス+IT

Lý do Nhật Bản triển khai các biện pháp thúc đẩy chuỗi công nghiệp dữ liệu vì nước này nhận thấy rằng họ có các vấn đề như hạ tầng kỹ thuật số

chưa hoàn thiện; thiếu dữ liệu cơ sở; chia sẻ dữ liệu không đầy đủ giữa Chính phủ, tư nhân và doanh nghiệp; hiểu biết về dữ liệu trong xã hội còn thấp và vấn đề về quyền riêng tư.

Xuất phát từ thực tiễn trên, Đạo luật Bảo vệ Thông tin Cá nhân Nhật Bản (APPI - Act on the Protection of Personal Information) ra đời như một phản ứng pháp lý trước những diễn biến này, với mục tiêu thiết lập một khuôn khổ toàn diện để điều chỉnh các vấn đề liên quan đến quyền riêng tư tại Nhật Bản[94]. Tinh thần cốt lõi của APPI là tạo ra sự cân bằng giữa việc bảo vệ quyền và lợi ích của cá nhân với việc thúc đẩy tính hữu dụng của thông tin cá nhân[95]. Điều này phản ánh quan điểm rằng dữ liệu không chỉ là đối tượng cần được bảo vệ mà còn là một nguồn lực quan trọng cho sự phát triển kinh tế và xã hội. Triết lý này đã định hình các quy định chi tiết của APPI, từ việc phân loại dữ liệu cho đến các cơ chế xử lý và chuyển giao, nhằm tạo ra một hệ thống pháp lý vừa nghiêm ngặt vừa linh hoạt.



Những Nguyên tắc được quy định trong Japan Data Protection Law (APPI) - Ảnh: Luvina Software JSC

[94] CookieFirst (2018), *APPI - Act on Protection of Personal Information - Japan,* CookieFirst, https://cookiefirst.com/act-on-protection-of-personal-information-appi-japan, Truy cập ngày 01/8/2025.

[95] Atsumi & Sakai (2020), *Amendments to the Act on the Protection of Personal Information,* https://www.aplawjapan.com/application/files/5816/3339/3524/Newsletter_AS_016.pdf, Truy cập ngày 28/7/2025

1.2.5.1. Tổng quan về APPI Nhật Bản

- Lịch sử hình thành và các lần sửa đổi quan trọng

APPI ban đầu được ban hành vào năm 2003 và có hiệu lực từ ngày 01/4/2004. Đạo luật này đánh dấu bước tiến đầu tiên của Nhật Bản trong việc thiết lập một khung pháp lý quốc gia về bảo vệ dữ liệu cá nhân[96]. Các thay đổi đáng chú ý đã được thực hiện trong lần sửa đổi năm 2017, có hiệu lực từ ngày 30/5/ 2017. Bản sửa đổi này đã bổ sung một chương riêng quy định về cơ quan bảo vệ dữ liệu, dẫn đến sự thành lập của Ủy ban Bảo vệ Thông tin Cá nhân (PPC), một cơ quan giám sát độc lập ở cấp trung ương[97].



Sự ra đời của Ủy ban Bảo vệ Thông tin Cá nhân Nhật Bản là điểm đáng chú ý nhất của APPI - Ảnh: Asahi

[96] Tạp chí Luật sư Việt Nam (2023), *Bảo vệ dữ liệu cá nhân trong hoạt động giao dịch thương mại điện tử: Kinh nghiệm của một số quốc gia trên thế giới và kiến nghị cho Việt Nam,* https://lsvn.vn/ba-o-ve-du-lie-u-ca-nhan-trong-hoa-t-do-ng-giao-di-ch-thuong-ma-i-die-n-tu-kinh-nghie-m-cu-a-mo-t-so-quo-c-gia-tren-the-gio-i-va-kie-n-nghi-cho-vie-t-nam-1686710508-a131590.html, truy cập ngày 28/7/2025.

[97] Trường Đại học Khoa học Xã hội và Nhân văn TP.HCM (2018), *Bảo vệ dữ liệu cá nhân theo pháp luật Nhật Bản và đề xuất đối với Việt Nam,* https://hcmussh.edu.vn/news/item/20595?, truy cập ngày 28/7/2025.

Tiếp theo, một bản sửa đổi lớn khác đã được Quốc hội Nhật Bản thông qua vào ngày 5/6/2020 và chính thức có hiệu lực từ ngày 01/4/2022. Bản sửa đổi này không chỉ tăng cường các quy định hiện hành mà còn hợp nhất đạo luật bảo vệ dữ liệu riêng cho khu vực công vào APPI, tạo ra một khuôn khổ pháp lý thống nhất hơn. Riêng luật bảo vệ dữ liệu cho chính quyền địa phương có hiệu lực sau ngày 01/4/2023.

- Cơ quan thực thi

Ủy ban Bảo vệ Thông tin Cá nhân (PPC) được thành lập như một cơ quan độc lập và trung lập, đóng vai trò then chốt trong việc giám sát và thực thi APPI. Nhiệm vụ chính của PPC là ban hành các hướng dẫn chi tiết để diễn giải và áp dụng Đạo luật, bao gồm các quy tắc chung về xử lý thông tin cá nhân, chuyển dữ liệu xuyên biên giới, và việc tạo, xử lý các loại dữ liệu mới.

Về quyền hạn, PPC có quyền yêu cầu doanh nghiệp nộp báo cáo, tiến hành kiểm tra tại chỗ và ban hành lệnh chấm dứt vi phạm. Tuy nhiên, một điểm đáng lưu ý là PPC hiện tại không có quyền trực tiếp áp dụng các khoản phạt hành chính hay hình phạt hình sự. Các chế tài tài chính hiện có chủ yếu là phạt tiền đối với việc không tuân thủ lệnh của PPC hoặc tiết lộ thông tin trái phép.

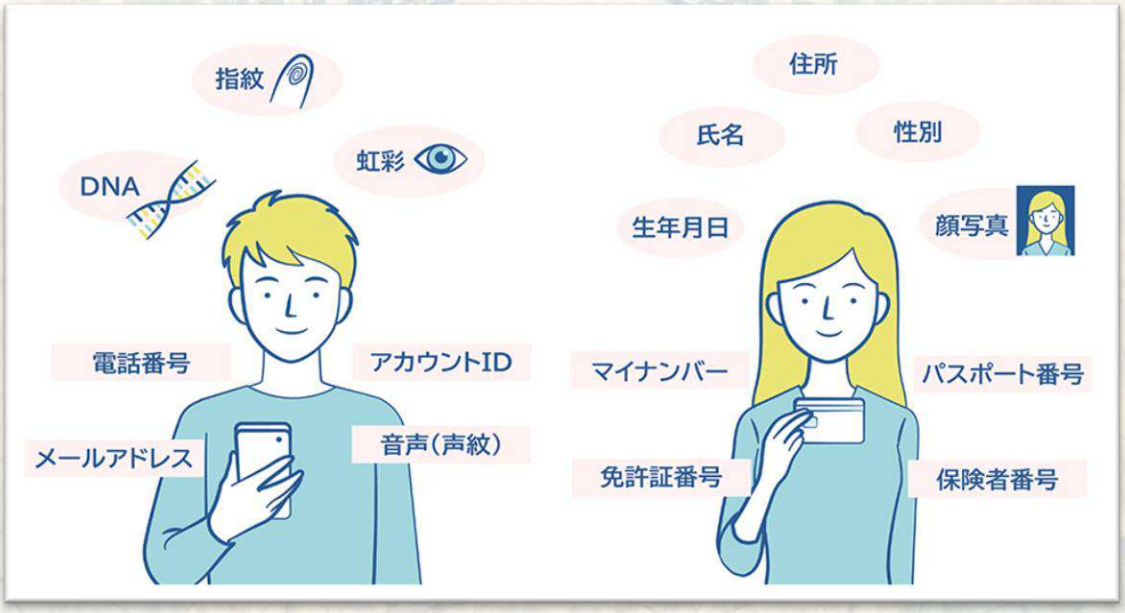
Sự thiếu vắng quyền áp dụng các khoản phạt hành chính trực tiếp là một đặc điểm của mô hình thực thi pháp luật của Nhật Bản, vốn thiên về hướng dẫn, khuyến nghị và khắc phục hơn là trừng phạt ngay lập tức. Tuy nhiên, điều này đang có dấu hiệu thay đổi. Theo DLA Piper, các cuộc thảo luận đang được tiến hành để sửa đổi APPI từ năm 2025 trở đi, với các chủ đề chính bao gồm việc giới thiệu một hệ thống phạt tiền hành chính bên cạnh các hình phạt hiện có. Sự thay đổi này cho thấy một bước ngoặt chiến lược, hướng tới việc tăng cường tính răn đe của luật pháp, hài hòa với các tiêu

chuẩn quốc tế như GDPR của Liên minh châu Âu, và cho phép phản ứng hiệu quả hơn trước các vụ vi phạm dữ liệu quy mô lớn.

1.2.5.2. Các khái niệm

Bên cạnh các khái niệm đã tồn tại trong GDPR, PIPL về dữ liệu cá nhân và dữ liệu nhạy cảm, APPI còn mở rộng nghiên cứu về các khái niệm mới, đó là thông tin được xử lý ẩn danh, thông tin đã được xử lý giả danh và thông tin có thể tham chiếu cá nhân. Cụ thể:

- Thông tin đã được xử lý ẩn danh: là dữ liệu về các cá nhân đã được loại bỏ hoàn toàn các yếu tố nhận dạng và không thể khôi phục lại thông tin cá nhân đã bị loại bỏ đó bằng các biện pháp thích hợp. Quy định này cho phép các doanh nghiệp sử dụng và tiết lộ loại thông tin này cho bên thứ ba mà không cần sự đồng ý của chủ thể dữ liệu, miễn là các yêu cầu về ẩn danh hóa được tuân thủ đầy đủ.



Minh họa cho APPI - Ảnh: 政府広報オンライン

Tuy nhiên, các tài liệu nghiên cứu chỉ ra rằng khái niệm này ít được sử dụng trong thực tế hơn so với dự kiến ban đầu. Yêu cầu nghiêm ngặt về việc không thể khôi phục dữ liệu đã ẩn danh hóa (khiến cho dữ liệu

không còn giá trị) đã tạo ra một rào cản lớn đối với việc sử dụng nó trong các hoạt động phân tích dữ liệu chuyên sâu. Sự khó khăn này đã thúc đẩy các nhà lập pháp tìm kiếm một giải pháp pháp lý linh hoạt hơn để cân bằng giữa bảo vệ dữ liệu và khả năng khai thác giá trị kinh tế của nó. Điều này dẫn trực tiếp đến việc giới thiệu một khái niệm mới trong APPI sửa đổi năm 2022.

- *Thông tin đã được xử lý giả danh:* Để giải quyết những hạn chế của thông tin đã được xử lý ẩn danh, bản sửa đổi APPI năm 2022 đã giới thiệu khái niệm thông tin đã được xử lý giả danh. Đây là thông tin đã được xử lý sao cho không thể sử dụng để xác định một cá nhân cụ thể, nhưng có thể được giải mã bằng cách tham chiếu đến các thông tin khác. Ví dụ điển hình là việc thay thế tên, địa chỉ bằng một chuỗi ký tự ngẫu nhiên. Điểm khác biệt quan trọng của loại dữ liệu này là doanh nghiệp có thể thay đổi mục đích sử dụng nó theo quyết định của mình mà không cần xin phép chủ thể dữ liệu. Điều này làm cho nó trở thành một công cụ hiệu quả cho các mục đích phân tích dữ liệu nội bộ, chẳng hạn như phân tích hành vi khách hàng, đặc biệt là trong các lĩnh vực như y tế và dược phẩm.

- *Thông tin có thể tham chiếu cá nhân:* APPI sửa đổi cũng định nghĩa một loại thông tin mới là thông tin có thể tham chiếu cá nhân. Khái niệm này bao gồm các dữ liệu như lịch sử duyệt web (thông qua cookie), tuổi, giới tính, lịch sử mua hàng hoặc dữ liệu vị trí. Bản thân loại thông tin này chưa được coi là thông tin cá nhân. Tuy nhiên, loại thông tin này bị quy định bởi APPI khi nó được chuyển cho bên thứ ba và bên nhận có khả năng xác định một cá nhân cụ thể bằng cách kết hợp nó với các thông tin khác mà họ đã có. Trong trường hợp này, bên nhận phải có được sự đồng ý trước của chủ thể dữ liệu. Yêu cầu này nhằm đảm bảo rằng các dữ liệu gián tiếp không được

lạm dụng để theo dõi hoặc xác định danh tính của người dùng mà không có sự cho phép của họ.

1.2.5.3. Các quy định về hoạt động có liên quan đến dữ liệu

- Quy định về thu thập và sử dụng dữ liệu, quy định về mục đích và yêu cầu đồng ý.

- Quy định về chuyển giao dữ liệu cho bên thứ ba. APPI quy định rằng việc chuyển giao dữ liệu cá nhân cho bên thứ ba yêu cầu sự đồng ý trước của cá nhân, trừ một số trường hợp ngoại lệ. Một trong những ngoại lệ đó là cơ chế "tùy chọn từ chối" (opt - out), cho phép doanh nghiệp mặc định tiết lộ thông tin cho bên thứ ba trừ khi cá nhân từ chối. Tuy nhiên, cơ chế này không áp dụng cho thông tin cá nhân nhạy cảm. Ngoài ra, APPI cũng cho phép "sử dụng chung" dữ liệu, chẳng hạn giữa các công ty trong cùng một tập đoàn. Trong trường hợp này, doanh nghiệp phải thông báo hoặc công khai cho chủ thể dữ liệu về các thông tin như các mục dữ liệu sẽ được sử dụng chung, phạm vi của những người sử dụng chung và mục đích sử dụng.

- Quy định về chuyển dữ liệu xuyên biên giới. Việc chuyển dữ liệu cá nhân ra nước ngoài cũng tuân theo các quy định nghiêm ngặt. Theo APPI, ngoài các yêu cầu chung cho việc chuyển dữ liệu cho bên thứ ba, cần có sự đồng ý trước của chủ thể dữ liệu có ghi rõ quốc gia nhận dữ liệu. Tuy nhiên, có một số trường hợp ngoại lệ, đó là: (1) Chuyển dữ liệu đến các quốc gia nằm trong danh sách "whitelist" theo quy tắc thi hành của APPI, được coi là có các tiêu chuẩn bảo vệ dữ liệu tương đương. Hiện tại, Vương quốc Anh và các nước Liên minh châu Âu nằm trong danh sách này dựa trên quyết định tương đương vào ngày 23/01/2019; (2) Chuyển dữ liệu cho bên thứ ba đã thiết lập các tiêu chuẩn bảo vệ quyền riêng tư tương đương với APPI[98]. Luật sửa

[98] Amazon Web Services (2019). *Quyền riêng tư dữ liệu tại Nhật Bản*. https://aws.amazon.com /vi/compliance/japan-data-privacy/. Truy cập ngày 28/8/2025.

đổi năm 2022 đã bổ sung một yêu cầu quan trọng: khi chuyển dữ liệu ra nước ngoài dựa trên sự đồng ý, doanh nghiệp phải cung cấp thông tin chi tiết về hệ thống luật bảo vệ dữ liệu của quốc gia nhận và các biện pháp bảo vệ dữ liệu mà bên nhận đang thực hiện.

- *Quy định về thông báo vi phạm dữ liệu.* Theo APPI sửa đổi, doanh nghiệp phải thông báo các sự cố vi phạm dữ liệu cho PPC và các chủ thể dữ liệu bị ảnh hưởng nếu sự cố đó có khả năng gây tổn hại đến quyền và lợi ích của các cá nhân. PPC đã đặt ra các ngưỡng cụ thể cho nghĩa vụ báo cáo, bao gồm: ***(1)*** Rò rỉ thông tin nhạy cảm; ***(2)*** Rò rỉ thông tin có thể gây thiệt hại tài chính; ***(3)*** Sự cố xảy ra không phải vì lý do khách quan; (4) Sự cố liên quan đến hơn 1000 chủ thể dữ liệu.

- *Quy định về chế tài.* Hệ thống chế tài của APPI bao gồm cả hình phạt tiền và hình phạt tù, áp dụng cho cả cá nhân và tổ chức. Điển hình như một số chế tài sau:

+ *Không nộp báo cáo hoặc cung cấp thông tin sai lệch:* Phạt tới 500,000 JPY.

+ *Không tuân thủ lệnh của PPC:* Phạt tới 1,000,000 JPY hoặc phạt tù tới một năm.

+ *Tiết lộ thông tin trái phép:* Phạt tới 500,000 JPY hoặc phạt tù tới một năm.

+ *Đối với tổ chức:* Nếu vi phạm được thực hiện bởi cán bộ hoặc quản lý, tổ chức có thể bị phạt tiền lên tới 100,000,000 JPY.

Tuy có những khác biệt, một điểm đáng chú ý là vào ngày 23/01/2019, EU đã thông qua quyết định về *"mức độ tương đương"* đối với Nhật Bản, cho phép tự do trao đổi dữ liệu cá nhân giữa hai nền kinh tế. Quyết định này là một minh chứng mạnh mẽ cho thấy hệ thống APPI được coi là đủ mạnh mẽ và tương đương với các biện pháp bảo vệ của GDPR.



APPI tạo hành lang pháp lý cho Nhật Bản giải quyết những vụ việc vi phạm an ninh dữ liệu - Ảnh: クローバーテック

1.2.5.4. So sánh giữa APPI và GDPR

Mặc dù APPI và GDPR đều có chung nội dung cốt lõi là bảo vệ dữ liệu trong khi thúc đẩy tính hữu dụng của nó, hai đạo luật này vẫn có những khác biệt đáng kể về phạm vi, yêu cầu và chế tài.

Về định nghĩa dữ liệu, GDPR có phạm vi rộng hơn, bao gồm các định danh trực tuyến và dữ liệu vị trí. Ngược lại, APPI đã phát triển một hệ thống phân loại chi tiết và phức tạp hơn với việc giới thiệu các khái niệm mới như thông tin đã được xử lý giả danh và thông tin có thể tham chiếu cá nhân, nhằm điều chỉnh các mức độ xử lý dữ liệu khác nhau.

Về quy tắc đồng ý, APPI có xu hướng tập trung hơn vào sự đồng ý rõ ràng của người dùng, đặc biệt đối với việc chia sẻ dữ liệu. Cả hai đạo luật cũng khác nhau về quy trình báo cáo vi phạm: GDPR yêu cầu báo cáo trong vòng 72 giờ, trong khi APPI chỉ yêu cầu báo cáo "kịp thời" mà không có một

khung thời gian cụ thể. Cuối cùng, một điểm khác biệt lớn là mức phạt tối đa của APPI thấp hơn đáng kể so với GDPR, đây là một trong những lý do thúc đẩy các cuộc thảo luận về việc sửa đổi APPI trong tương lai[99].



Minh họa APPI và GDPR - Ảnh: Endpoint

Có thể thấy rằng, chính sách, pháp luật về dữ liệu của Nhật Bản đang có xu hướng hội tụ với các chuẩn mực quốc tế, đặc biệt là GDPR. APPI không chỉ là một đạo luật tĩnh mà là một khuôn khổ pháp lý năng động, linh hoạt được điều chỉnh để đáp ứng các thách thức của bối cảnh công nghệ và kinh tế số. APPI còn thể hiện nỗ lực điều chỉnh chính sách nhằm cân bằng giữa việc bảo vệ quyền riêng tư và thúc đẩy kinh tế dữ liệu của Chính phủ Nhật Bản.

1.2.6. Bỉ

1.2.6.1. Tổng quan về pháp luật dữ liệu tại Bỉ

Thoạt nhìn, Vương quốc Bỉ khó có thể được coi là quốc gia đi đầu trong việc phát triển luật bảo vệ dữ liệu. Việc đưa quyền riêng tư thực sự vào Hiến pháp Bỉ mãi đến năm 1994 mới được thực hiện. Rõ ràng, điều đó không có nghĩa là dữ liệu cá nhân và quyền riêng tư trước đây không được bảo vệ. Các quy định trong luật quốc gia cùng với các điều khoản nhân quyền quốc tế đã

[99] Nihonium (2022), *APPI vs GDPR: Key Differences for SaaS - Simplifying Japan Entry*, https://nihonium.io/appi-vs-gdpr-key-differences-for-saas/, Truy cập ngày 28/7/2025.

được sử dụng làm cơ sở pháp lý. Chính áp lực quốc tế đã thúc đẩy Bỉ phải nhanh chóng bắt kịp khuôn khổ pháp lý quốc gia về quyền riêng tư và bảo vệ dữ liệu. Nguyên nhân trực tiếp là việc thành lập *"Khu vực Schengen"*, bãi bỏ các biện pháp kiểm soát biên giới nội bộ khối EU, làm gia tăng tội phạm xuyên biên giới, đòi hỏi phải chuyển giao dữ liệu xuyên biên giới nhiều hơn cho mục đích điều tra tội phạm. Kết quả là Luật Bảo vệ Dữ liệu Cá nhân năm 1992 (sau đây gọi là luật năm 1992)[100] toàn diện được ban hành, tiếp theo là một danh sách các sắc lệnh hoàng gia sửa đổi và thi hành luật.

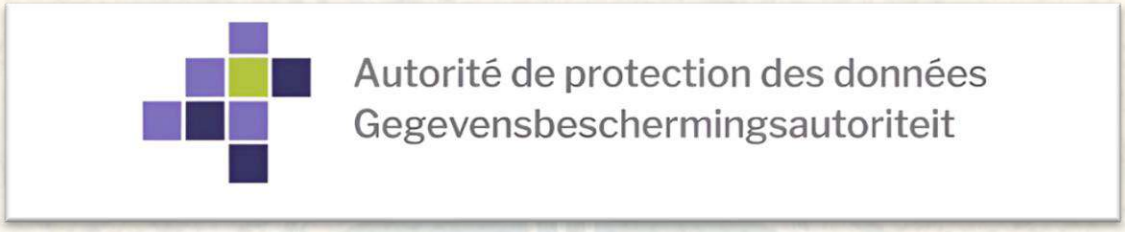
Tuy nhiên, sự thức tỉnh muộn màng này của các thể chế chính trị ở Bỉ đối với quyền riêng tư và bảo vệ dữ liệu hoàn toàn tương phản với vai trò nổi bật mà họ đã đảm nhận trong những năm gần đây. Đất nước này đã nhanh chóng phát triển từ một kẻ theo đuôi vào phút chót thành một nhà lãnh đạo được công nhận nhờ Ủy ban Quyền riêng tư chuyên trách - nay là Cơ quan Bảo vệ Dữ liệu (sau này gọi là DPA), đó là việc thành lập một vị trí đặc biệt trong chính phủ về quyền riêng tư.

Người ta nghĩ rằng sự chuyển đổi này sẽ giúp Bỉ trở thành quốc gia tiên phong trong việc triển khai khuôn khổ pháp lý bảo vệ dữ liệu mới của EU. Thế nhưng, chính phủ Bỉ đã mất khá nhiều thời gian để ban hành các đạo luật thực thi cụ thể đối với GDPR và Chỉ thị về bảo vệ dữ liệu trong lĩnh vực thực thi pháp luật. Ngày 5/9/2018 - vài tháng sau khi thời hạn triển khai kết thúc, một đạo luật khung mở rộng đã được công bố, bao gồm các quy định về GDPR, các Chỉ thị liên quan về bảo vệ dữ liệu trong thực thi pháp luật, cũng như các quy định cụ thể hơn về bảo vệ dữ liệu do các cơ quan tình báo và an ninh xử lý (sau đây gọi là Đạo luật Khung)[101]. Trước đó, một phần

[100] Act on the Protection of the Private Life concerning the Processing of Personal Data, B.S.18.03.1993.

[101] Act on the Protection of Natural Persons concerning the Processing of Personal Data, B.S.05.09.2018.

đáng kể của GDPR (bao gồm việc thành lập DPA) đã được thực hiện trong một đạo luật riêng được thông qua vào ngày 03/02/2017[102] để có hiệu lực vào ngày GDPR có hiệu lực. Mục đích của đạo luật này là cải tổ Ủy ban Bảo vệ Quyền riêng tư Bỉ thành một DPA.



Cơ quan Bảo vệ Dữ liệu Bỉ - Ảnh: PPC Land

Bên cạnh hai đạo luật thực thi kể trên, với việc Bỉ ủng hộ học thuyết nhất nguyên, về mặt kỹ thuật, GDPR không cần phải được chuyển đổi thành luật quốc gia. Tuy nhiên, vì GDPR không phải là một quy định theo nghĩa truyền thống, một số điều khoản cần được triển khai trên phạm vi quốc gia vì chúng cho phép nhà lập pháp quốc gia có một biên độ diễn giải khá rộng. Tuy nhiên, cần lưu ý rằng, như Ủy ban Quyền riêng tư Bỉ đã công bố trong văn bản giới thiệu *"Kế hoạch 13 bước"* chủ động triển khai GDPR, rằng các bên xử lý và kiểm soát dữ liệu vốn đã tuân thủ luật năm 1992 có thể sử dụng khuôn khổ hiện có đó làm điểm xuất phát để tuân thủ GDPR.

1.2.6.2. Bối cảnh bảo vệ dữ liệu ở Bỉ trước GDPR

Việc các luật thực thi GDPR và Chỉ thị về bảo vệ dữ liệu cho mục đích thực thi pháp luật của Bỉ được ban hành sau khi thời hạn chuyển đổi đã hết là điều mâu thuẫn với lập trường rõ ràng mà chính phủ nước này và Ủy ban Quyền riêng tư (nay là DPA) đã đưa ra trong những năm qua gần đây. Mặc dù là quốc gia đầu tiên dành một vị trí đặc biệt trong chính phủ cho lĩnh vực quyền riêng tư và tiên phong trong việc xử phạt vi phạm trên lĩnh vực này

[102] Act on the Protection of Natural Persons concerning the Processing of Personal Data, B.S.05.09.2018.

(vụ việc Facebook vi phạm quyền riêng tư ở Bỉ), việc chuyển đổi khuôn khổ pháp lý mới của EU về bảo vệ dữ liệu tại Bỉ diễn ra khá chậm chạp. Điều này gợi nhớ đến việc ban hành luật bảo vệ dữ liệu toàn diện đầu tiên - luật năm 1992 tại quốc gia này.



Trước đây, Hiến pháp Bỉ không đề cập đến khái niệm "bảo vệ dữ liệu" hay "bảo vệ thông tin" - Ảnh: Internet

Trước đó, Hiến pháp Bỉ năm 1831 không bao gồm quyền riêng tư. Tuy nhiên, Hiến pháp này có quy định quyền bảo vệ nhà ở[103] liên quan đến việc khám xét và tịch thu cho mục đích thực thi pháp luật. Điều 226 ban đầu chỉ bảo vệ tính bảo mật của thư từ. Cả hai đều có thể được coi là bảo vệ các khía cạnh của cái mà chúng ta gọi là quyền riêng tư ngày nay,

[103] Article 10 in the original version, Article 15 in the current version of the Constitution: Consolidated Constitution of 17.02.1994, B.S. 17.02.1994.

nhưng quyền chung về đời sống riêng tư không được hiến pháp bảo vệ cho đến năm 1994[104]. Trước thời điểm đó, việc bảo vệ quyền riêng tư được thực hiện bằng cách dựa vào hiệu lực của Điều 8 Công ước ECHR kết hợp với các ngành luật cụ thể như luật hình sự, luật dân sự và luật lao động, bao gồm các điều khoản bảo vệ quyền riêng tư trong các bộ luật tương ứng khác. Ngoại trừ các hành vi pháp lý cụ thể như luật liên quan đến sổ đăng ký dân số quốc gia hoặc sắc lệnh hoàng gia về cơ sở dữ liệu dành cho nhân viên chính phủ[105], thuật ngữ "bảo vệ dữ liệu" không được đề cập trong luật pháp nước Bỉ trước năm 1992.

1.2.6.3. Đạo luật Bảo vệ Dữ liệu năm 1992

Bất chấp những nỗ lực xây dựng luật quốc gia đầu tiên về bảo vệ dữ liệu cá nhân vào những năm 70 của Thế kỉ XIX, các đề xuất này đã vấp phải sự phản đối chính trị và không bao giờ được thực hiện[106]. Do đó, việc ban hành luật chung năm 1992 về bảo vệ dữ liệu cá nhân[107] khá muộn; mặc dù cần lưu ý rằng danh sách các luật cụ thể hơn và các sắc lệnh hoàng gia bao gồm bảo vệ dữ liệu trong một số lĩnh vực[108] đã đóng vai trò tiền thân cho luật toàn diện năm 1992. Tuy nhiên, việc thông qua luật bảo vệ dữ liệu chung đầu tiên của Bỉ muộn màng cùng với việc phê chuẩn muộn Công ước về bảo vệ dữ liệu của Hội đồng Châu Âu vào năm 1993 đã cho thấy một môi trường ban đầu không thuận lợi cho việc bảo vệ dữ liệu cá nhân tại quốc gia này, trong khi áp lực quốc tế buộc Bỉ phải thực hiện các bước đi pháp lý cần thiết là rất lớn[109]. Xét cho cùng, việc Bỉ phê chuẩn Công ước gốc của Hội đồng

[104] Current Article 29 of the Constitution.

[105] De Hert and Gutwirth 2013, pp. 28 and 44.

[106] De Hert 2003, pp. 42–43.

[107] De Hert 2003, pp. 42–43.

[108] Act on the Protection of the Private Life concerning the Processing of Personal Data, B.S.18.03.1993.

[109] Act on the Protection of the Private Life concerning the Processing of Personal Data, B.S. 18.03.1993.

châu Âu về bảo vệ dữ liệu đã diễn ra song song với thời điểm Công ước Thi hành Schengen năm 1990 bắt đầu có hiệu lực. Các quốc gia EU thành lập "Khu vực Schengen" đã đồng ý mỗi nước thông qua một luật bảo vệ dữ liệu trước khi phê chuẩn Công ước thực hiện Schengen. Khi ấy, điều này gây thêm áp lực cho chính phủ, đó là phải soạn thảo một đề xuất lập pháp cuối cùng và nó đã dẫn đến luật năm 1992[110]. Khi Chỉ thị 95/46 của EU được thông qua chỉ hai năm sau khi ban hành luật dữ liệu tại Bỉ, chính phủ đã điều chỉnh chính sách của mình khi cần thiết thông qua các sắc lệnh hoàng gia[111]. Cuối cùng, vào năm 1998, luật năm 1992 đã trải qua một lượng lớn các sửa đổi do việc thực hiện đầy đủ Chỉ thị 95/46[112]. Dựa trên những nỗ lực này nhằm đưa luật quốc gia Bỉ phù hợp với Chỉ thị 95/46, việc EU cải tổ khung pháp lý về bảo vệ dữ liệu thông qua GDPR có thể sẽ không nên gây quá nhiều lo ngại ở cấp độ lập pháp.

- Quốc vụ khanh Bảo vệ Quyền riêng tư

Vào năm 2014, chính phủ Bỉ là chính phủ đầu tiên ở châu Âu giới thiệu một chức vụ đặc biệt trong chính phủ liên bang: một Quốc vụ khanh (Secretary of State) phụ trách quyền riêng tư, đấu tranh chống gian lận xã hội và Biển Bắc, trực thuộc Bộ trưởng Bộ Các vấn đề Xã hội và Y tế Công cộng. Điều này có nghĩa là một trong những trách nhiệm của ông là xây dựng pháp luật về bảo vệ quyền riêng tư cá nhân. Kể từ năm 2016, một cựu thành viên Nghị viện châu Âu, ông Philippe De Backer, đảm nhận chức vụ này. Nhiệm vụ của ông được xác định một cách đơn giản nhưng rộng rãi là "phụ trách lập pháp về bảo vệ quyền riêng tư", và nội dung này được đưa vào danh mục công tác của ông khi ông trở thành Bộ trưởng

[110] De Hert and Gutwirth 2013, p. 35.
[111] De Hert and Gutwirth 2013, p. 36.
[112] De Hert 2003, p. 43.

Liên bang phụ trách Chương trình Kỹ thuật số, Viễn thông và Dịch vụ Bưu chính vào năm 2018[113].

So với các quốc gia khác, việc có một danh mục chính phủ riêng dành riêng cho chính sách quyền riêng tư là một điều đặc biệt. Ưu điểm chính của nó là đảm bảo rằng chủ đề bao trùm chính sách này nhận được sự quan tâm thích đáng trong quá trình ra quyết định của các đạo luật hoặc chính sách khác, thay vì chỉ là một vấn đề bên lề. Ngoài ra, chức năng của Bộ trưởng Ngoại giao cũng giúp làm nổi bật một cuộc tranh luận, đặc biệt là trong những tháng trước khi GDPR có hiệu lực, giúp nâng cao nhận thức của người dân và trấn an các công ty rằng chính phủ công nhận các khoản đầu tư của họ là tuân thủ.

- Cơ quan bảo vệ dữ liệu

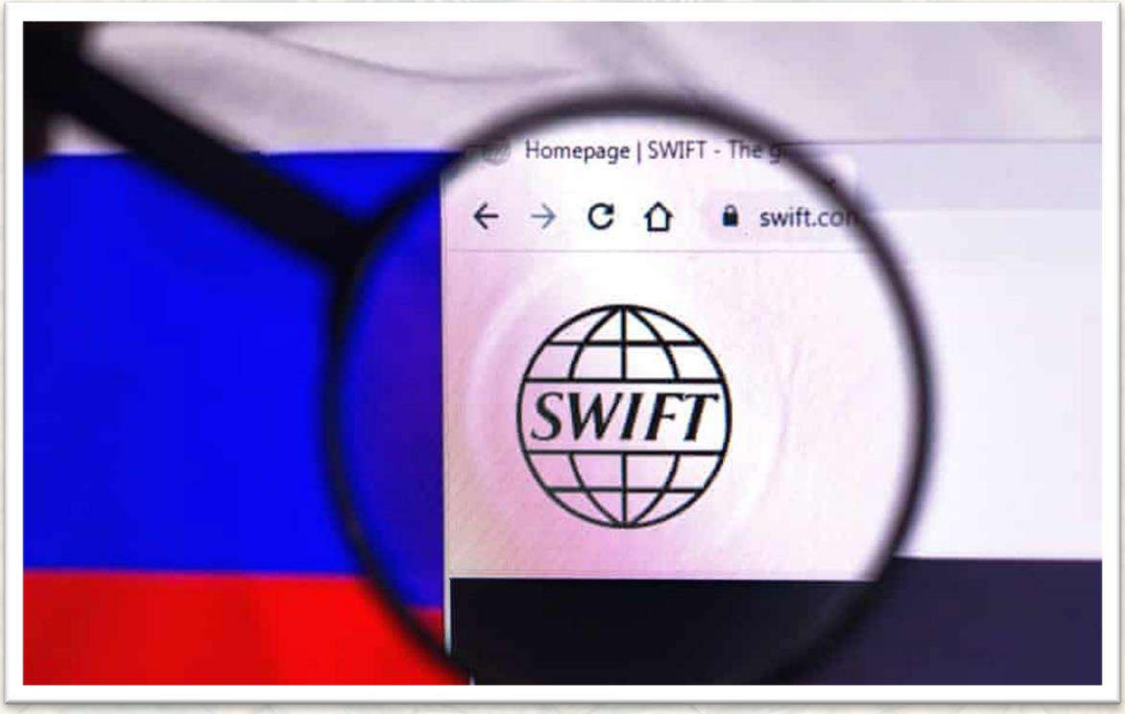
Thường được gọi là Ủy ban Bảo mật, Ủy ban Bảo vệ Quyền riêng tư đã được cải tổ kể từ ngày 25/5/2018 thành DPA[114]. Việc thay đổi tên nghe có vẻ tầm thường nhưng phù hợp với vai trò của cơ quan giám sát và xử phạt hơn là một cơ quan tư vấn đơn thuần. Tuy nhiên, cần lưu ý rằng ngay cả trước khi cải cách, Ủy ban Bảo mật Bỉ đã có vai trò nổi bật trong các vấn đề bảo vệ dữ liệu thu hút sự chú ý của quốc tế. Điển hình, vụ chuyển dữ liệu tin nhắn tài chính giữa SWIFT và các cơ quan chức năng Hoa Kỳ năm 2007, vụ kiện chống lại Facebook...

Theo luật năm 1992, Ủy ban bảo vệ quyền riêng tư Bỉ có thẩm quyền rộng hơn so với phạm vi của GDPR. Ví dụ, GDPR loại trừ các hoạt động nằm ngoài phạm vi Luật Cộng đồng như xử lý dữ liệu cho mục đích phòng ngừa, điều tra, truy tố tội phạm hình sự và thi hành án. Do đó, Hội đồng Nhà

[113] Royal Decree establishing certain ministerial competences, B.S. 10.02.2015.

[114] Royal Decree establishing certain ministerial competences, B.S. 10.02.2015.

nước (Conseil d'État) đã nhấn mạnh trong ý kiến của mình về Đạo luật gần đây thành lập Cơ quan Bảo vệ Dữ liệu rằng cần phải làm rõ thẩm quyền (lãnh thổ) của DPA sẽ là gì[115]. Vị Quốc vụ khanh được đề cập ở trên đã làm rõ rằng thẩm quyền của Cơ quan Bảo vệ Dữ liệu (DPA) sẽ được mở rộng hơn nữa để bao phủ cả các lĩnh vực bổ sung. Liên quan đến việc xử lý dữ liệu mà được điều chỉnh bởi các đạo luật khác ngoài luật thực thi GDPR, Khoản 1 Điều 4 của Đạo luật thành lập DPA quy định rằng DPA có thẩm quyền đối với tất cả các văn bản pháp luật có chứa các quy định liên quan đến bảo vệ hoạt động xử lý dữ liệu.



Vụ việc của SWIFT là một trong những vụ việc điển hình do Ủy ban Bảo mật Bỉ giải quyết - Ảnh: VOV.vn

Trong đề xuất lập pháp ban đầu, cơ quan DPA quyết định các vụ án và xác định hậu quả được gọi là *"cơ quan tư pháp hành chính"*. Công thức

[115] See Chambre, 2648/001, Travaux Préparatoires, Proposed Act establishing the Data Protection Authority, 23.08.2017, pp. 103–133.

như vậy đã gây ra sự nhầm lẫn và khiến Hội đồng Nhà nước nghi ngờ về bản chất tư pháp của cơ quan này[116]. Một mặt, đề xuất lập pháp sử dụng các thuật ngữ như thẩm phán, hình phạt và sổ đăng ký, thường được sử dụng trong bối cảnh tư pháp. Mặt khác, đề xuất nêu rằng cơ quan này có thể áp dụng các khoản tiền phạt hành chính, dẫn đến giả định rằng đó là một cơ quan hành chính. Tuy nhiên, theo lập luận của GDPR, Hội đồng Nhà nước kết luận rằng cơ quan DPA đang được đề cập được cho là một cơ quan hành chính. Theo khuyến nghị của Hội đồng Nhà nước (Council of State) nhằm làm rõ vấn đề, đạo luật được thông qua hiện đã quy định tại Điều 32 về cơ quan giải quyết tranh chấp hành chính. Tất cả các thuật ngữ gây nhầm lẫn trước đó đều bị loại bỏ.

Việc xếp loại cơ quan giải quyết tranh chấp này như một cơ quan hành chính đã dẫn đến một hệ quả đáng chú ý khác. Hội đồng Nhà nước dẫn chiếu đến án lệ Schrems năm 2015 của Tòa án Công lý Liên minh Châu Âu (CJEU) để chỉ ra rằng nếu cơ quan giải quyết tranh chấp không phải là một cơ quan tư pháp, thì nó sẽ không thể gửi yêu cầu giải thích sơ bộ lên Tòa án Công lý EU theo Điều 267 của Hiệp ước về hoạt động của EU (TFEU). Trong trường hợp này, Khoản 65 của Phán quyết Schrems[117] có thể gợi ý một quy trình khác để xử lý nếu DPA nghi ngờ tính hợp lệ của quyết định về mức độ bảo vệ tương đương của Ủy ban Châu Âu. Tuy nhiên, đạo luật được thông qua về việc thành lập DPA dường như chưa khắc phục được tình trạng này.

[116] Council of State, Opinion 61.267/2/AG, 27.06.2017, on the Proposed Act establishing the Data Protection Authority, pp. 43–47.

[117] CJEU 6.10.2015, C-362/14, Schrems.



Tòa án Công lý Liên minh Châu Âu (CJEU) - Ảnh: ELENA

1.2.6.4. Các vấn đề mới liên quan đến GDPR

Đạo luật Khung của Bỉ thực hiện GDPR đã được công bố vào tháng 9/2018, bao gồm cả việc thực hiện Chỉ thị về bảo vệ dữ liệu cho mục đích thực thi pháp luật[118]. Việc Hội đồng Bộ trưởng liên bang phê duyệt vào tháng 5/2018 đã công bố những điểm chính của luật thực thi cũng như sự lựa chọn của chính phủ đối với Đạo luật Khung thay vì một loạt các sửa đổi riêng lẻ trong các luật cụ thể. Theo GDPR, những điểm chính của Đạo luật Khung là trách nhiệm giải trình, tính minh bạch và tăng cường giám sát của DPA. Theo quan điểm cuối cùng đó, một luật mới đã được ban hành vào ngày 03/12/2017, cải tổ Ủy ban Quyền riêng tư Bỉ thành DPA.

Trong ý kiến của Hội đồng Nhà nước đối với dự thảo văn bản của đạo luật, hai điểm quan trọng đã được nêu ra. *Điểm đầu tiên* liên quan đến bản chất giám sát của DPA - tư pháp hoặc hành chính - đã được đề cập trong

[118] Act on the Protection of Natural Persons concerning the Processing of Personal Data, B.S. 05.09.2018.

tiểu mục trước. *Điểm thứ hai* do Hội đồng Nhà nước nêu ra liên quan đến cấu trúc liên bang của Bỉ và đặt ra vấn đề về việc tăng cường các cơ quan giám sát trong các lĩnh vực thẩm quyền khác nhau. Do đó, tiểu mục này tập trung làm rõ luận điểm sau (liên quan đến sự lựa chọn ban hành Đạo luật Khung trong việc thực thi GDPR), trước khi đặt ra hai vấn đề tiếp theo liên quan đến việc thực thi GDPR tại Bỉ: Cơ sở pháp lý của các hoạt động xử lý dữ liệu; Việc thực hiện quyền bảo vệ dữ liệu trực tuyến. Cuối cùng, tiểu mục này đề cập đến việc Bỉ thực hiện các điều khoản GDPR cụ thể, vốn đã tạo đủ khoảng trống cho cơ quan lập pháp quốc gia để mở rộng phạm vi áp dụng.

- Cấu trúc liên bang của Bỉ

Là một trong những quốc gia thành viên nhỏ hơn của Liên minh châu Âu, Vương quốc Bỉ thường thu hút sự chú ý do có cấu trúc liên bang phức tạp, kết hợp giữa cơ quan lập pháp liên bang và các cơ quan lập pháp ở cấp cộng đồng và vùng. Mặc dù việc bảo vệ dữ liệu cá nhân thuộc thẩm quyền lập pháp của chính phủ liên bang, nhưng việc EU giới thiệu khuôn khổ pháp lý mới về bảo vệ dữ liệu cũng có tác động đến cấp chính quyền vùng, cụ thể là các chính phủ Flemish (Vùng nói tiếng Hà Lan) và Walloon (Vùng nói tiếng Pháp). Các sắc lệnh của Flemish và Walloon, vốn được ban hành dựa trên Luật năm 1992 và có viện dẫn đến các điều khoản của luật này, đều cần được sửa đổi để phù hợp với việc thực thi GDPR. Trong khi đó, chính phủ Flemish đã chủ động thực hiện các bước điều chỉnh sắc lệnh của mình cho phù hợp với GDPR, thậm chí trước cả khi Đạo luật Khung của Bỉ được hoàn thiện[119].

[119] Council of State, Opinion 62.834/3 on the proposed decree by the Flemish Community and the Flemish Region concerning the amendments to the decrees based on Regulation (EU) 2016/679, 19.02.2018.



Phân vùng phương ngữ tại Bỉ - Ảnh: Internet

Tuy nhiên, đây không phải là điểm tranh cãi duy nhất liên quan đến GDPR. Khi chính phủ liên bang đệ trình luật đề xuất về việc thành lập DPA, thực chất là cải cách Ủy ban Quyền riêng tư hiện hành theo GDPR đến Hội đồng Nhà nước để xin tư vấn, một câu hỏi về quyền tự chủ của các cộng đồng và khu vực đã trở thành tâm điểm chú ý, cụ thể là liệu việc chính phủ liên bang thành lập cơ quan có xâm phạm thẩm quyền của các cộng đồng và khu vực hay không[120]. Kể từ năm 2010, một cơ quan giám sát của vùng Flemish đã đi vào hoạt động nhằm giám sát hoạt động lưu chuyển dữ liệu

[120] Council of State, Opinion 61.267/2/AG, 27.06.2017, on the Proposed Act establishing the Data Protection Authority, pp. 30–37.

hành chính điện tử[121]. Đạo luật được đề xuất thiết lập một cơ quan bảo vệ dữ liệu có thẩm quyền đối với tất cả các chủ thể khai thác, xử lý dữ liệu bất kể lĩnh vực được xử lý hoặc cơ quan nhà nước có liên quan, ngay cả khi các chủ thể nằm trong phạm vi của các cộng đồng và vũng lãnh thổ.



Đạo luật Bảo vệ dữ liệu của Bỉ được hoàn thiện từ trước khi GDPR ra đời

Dựa trên án lệ của Tòa án Hiến pháp liên quan đến Điều 22 của Hiến pháp Bỉ (quy định về quyền tôn trọng đời sống riêng tư), Hội đồng Nhà nước nhấn mạnh rằng chính phủ liên bang có thẩm quyền đối với các quy định chung về quyền đời sống riêng tư. Trong khi đó, các cộng đồng và vùng lãnh thổ có thể quy định quyền đời sống riêng tư trong các lĩnh vực thuộc thẩm quyền của mình, nhưng phải tuân theo các quy tắc liên bang. Theo các quy tắc cụ thể này, các cộng đồng và khu vực có thể thành lập các cơ quan giám sát cụ thể, nhưng chính phủ liên bang vẫn có thẩm quyền thành lập một cơ quan giám sát các quy tắc chung. Tóm lại, Hội

[121] Flemish Decree on electronic administrative data traffic, B.S. 29.10.2008.

đồng Nhà nước cho rằng trong trường hợp tồn tại các cơ quan giám sát ở nhiều cấp độ khác nhau, một thỏa thuận hợp tác cần được thiết lập càng sớm càng tốt nhằm đảm bảo sự phối hợp hiệu quả và nhất quán giữa các cấp chính quyền[122].

- Cơ sở pháp lý của hoạt động xử lý dữ liệu

Việc ban hành GDPR đã khiến Cơ quan Bảo vệ Dữ liệu (DPA) của Bỉ sớm trình bày một kế hoạch từng bước[123], chủ yếu thông báo cho các công ty - bên xử lý dữ liệu và bên kiểm soát dữ liệu về các nghĩa vụ mới của họ và cách họ nên bắt đầu chuẩn bị để tuân thủ. Ngay cả trước khi luật thực thi của Bỉ được ban hành, GDPR đã có hiệu lực trực tiếp, nghĩa là bên xử lý dữ liệu và bên kiểm soát dữ liệu có nguy cơ chịu hậu quả nếu không tuân thủ các quy định của GDPR.

Cơ quan DPA của Bỉ thừa nhận thực tế là theo luật năm 1992, nhiều công ty và tổ chức chưa xác định cơ sở pháp lý cho các hoạt động xử lý dữ liệu của họ. Mặc dù điều này không gây ra hậu quả nghiêm trọng theo luật năm 1992, nhưng nó lại tạo ra sự khác biệt theo GDPR vì quyền của công dân liên quan có thể thay đổi tùy thuộc vào cơ sở pháp lý của hoạt động xử lý dữ liệu cụ thể[124]. Các loại căn cứ pháp lý vẫn giữ nguyên (sự đồng ý của chủ thể dữ liệu hoặc ngoại lệ dựa trên sự cần thiết của hoạt động xử lý), nhưng hệ quả pháp lý đối với trách nhiệm giải trình (accountability) của bên xử lý hoặc kiểm soát dữ liệu là khác nhau. Khi sự đồng ý là căn cứ pháp lý cho hoạt động xử lý dữ liệu, DPA Bỉ thừa nhận rằng cách quy định về "sự đồng ý" và "sự đồng ý rõ ràng" trong GDPR là chưa rõ ràng. Tuy vậy, DPA

---

[122] Council of State, Opinion 61.267/2/AG, 27.06.2017, on the Proposed Act establishing the Data Protection Authority, p. 37.

[123] Belgian Privacy Commission 2016 GDPR, Prepare yourself in 13 steps. https://www.gegevensbeschermingsautoriteit.be/bereid-je-voor-13-stappen. Accessed 6 May 2019.

[124] GDPR.

đưa ra khuyến nghị mạnh mẽ đối với các bên kiểm soát dữ liệu rằng họ nên thiết lập một chuỗi kiểm toán để chứng minh rằng sự đồng ý đã được chủ thể dữ liệu đưa ra một cách hợp pháp.

Điều này có nghĩa là các tổ chức phải lưu giữ được bằng chứng rõ ràng về quá trình thu thập sự đồng ý, như thời điểm, hình thức và nội dung đồng ý, nhằm đáp ứng yêu cầu minh bạch và trách nhiệm giải trình theo quy định của GDPR.



Báo cáo thường niên của cơ quan DPA nước Bỉ - Ảnh: Lydian

- Thực hiện Quyền bảo vệ dữ liệu trực tuyến

Cơ quan Bảo vệ Dữ liệu Bỉ (DPA) đã chỉ ra một cách chính đáng rằng, nhìn chung, quyền của công dân theo GDPR không có nhiều thay đổi so với Luật năm 1992, ngoại trừ một số cải tiến quan trọng. Đồng thời, DPA hoan nghênh quyền chuyển dữ liệu mới nhưng cũng chỉ ra rằng nhiều công ty và tổ chức đã tự mình áp dụng quyền này trước khi GDPR có hiệu lực. Tuy nhiên, các công ty và tổ chức này được khuyến khích sửa đổi hệ thống hiện tại, ít nhất phải đảm bảo rằng thủ tục thực hiện quyền chuyển dữ liệu là hoàn toàn số hóa.

Tương tự, DPA cũng đưa ra khuyến nghị đối với các thủ tục yêu cầu truy cập dữ liệu cá nhân. Ngoài các thời hạn mới theo GDPR, quy định còn áp đặt nghĩa vụ cung cấp thêm thông tin cho người dùng, điều này có thể đòi hỏi các khoản đầu tư đáng kể, chẳng hạn như thiết lập hệ thống giúp người dân có thể truy cập dữ liệu của họ trực tuyến. Do đó, các công ty và tổ chức được đề cập được khuyến khích tiến hành phân tích chi phí - lợi ích của một quy trình trực tuyến[125]. Xét đến các quy định pháp luật về ngôn ngữ tại Bỉ (một quốc gia đa ngôn ngữ)[126], các công ty và tổ chức hoạt động trên lãnh thổ nước này phải đối mặt với những khoản đầu tư bổ sung nhằm bảo đảm rằng thông tin và thủ tục trực tuyến của họ có sẵn ít nhất bằng hai ngôn ngữ chính thức.



Một số mô tả về cơ quan DPA của Bỉ - Ảnh: Lydian

Đạo luật Khung của Bỉ quy định các biện pháp khắc phục đối với các hành vi vi phạm có thể xảy ra trong quá trình xử lý dữ liệu. Một vụ việc có

[125] GDPR.

[126] With Article 4 of the Constitution as the legal basis.

thể được đưa ra tòa án không chỉ bởi chủ thể dữ liệu mà còn bởi DPA hoặc một cơ quan hoặc tổ chức đại diện cho chủ thể dữ liệu. Cơ quan hoặc tổ chức đó phải hoạt động trong lĩnh vực bảo vệ dữ liệu trong ít nhất 03 năm[127].

- Giải thích trong Luật thi hành của Bỉ

Vì GDPR để lại nhiều không gian cho các quốc gia thành viên EU mở rộng phạm vi của các điều khoản cụ thể, nên tiểu mục này sẽ đề cập đến một số trường hợp mà nhà lập pháp Bỉ đã đưa ra lựa chọn tăng cường bảo vệ đối với các điểm cụ thể và chỉ định các điều khoản về các điểm khác. Điển hình, độ tuổi tối thiểu để đồng ý xử lý dữ liệu là 16 tuổi theo GDPR. Mọi trẻ em dưới độ tuổi này đều cần sự cho phép của cha mẹ hoặc người có trách nhiệm nuôi dưỡng. Tuy nhiên, các quốc gia thành viên được phép hạ thấp ngưỡng này miễn là không thấp hơn 13 tuổi. Quốc vụ Khanh phụ trách bảo vệ quyền riêng tư đã làm rõ trong các tài liệu chuẩn bị (travaux préparatoires) rằng việc lựa chọn độ tuổi tối thiểu là 13 được đưa ra theo ý kiến của Ủy viên Quyền Trẻ em, Hội đồng Thanh niên và các Bộ trưởng Cộng đồng có thẩm quyền[128]. Văn bản của GDPR đã cho phép các quốc gia thành viên có nhiều quyền hạn đáng kể trong việc cho phép xử lý dữ liệu nhạy cảm. Theo đó, Đạo luật Khung của Bỉ có một số ngoại lệ đối với quy tắc chung là không được xử lý dữ liệu nhạy cảm.

Các cơ quan công quyền cụ thể được phép xử lý dữ liệu nhạy cảm cho mục đích thực hiện nhiệm vụ của họ. Điều này bao gồm việc xử lý dữ liệu liên quan đến chủng tộc và sắc tộc, quan điểm chính trị và tôn giáo, tư cách thành viên công đoàn, dữ liệu di truyền, dữ liệu sức khỏe, sở thích tình dục và dữ liệu liên quan đến tiền án hình sự của các cơ quan tình báo cho mục

[127] See Article 220 of the Act on the Protection of Natural Persons concerning the Processing of Personal Data.
[128] Chambre, 3126/003, Travaux Préparatoires, Proposed Act on the Protection of Natural Persons concerning the Processing of Personal Data, 06.07.2018, p. 5.

đích cấp phép an ninh[129]. Trong travaux préparatoires, điều khoản này được làm rõ bằng cách nhấn mạnh những rủi ro "cực đoan hóa" có thể được phát hiện khi cho phép sử dụng dữ liệu về quan điểm chính trị hoặc tôn giáo và rủi ro mắc bệnh tâm thần có thể xuất hiện thông qua xử lý dữ liệu sức khỏe[130]. Ba loại tổ chức có thể xử lý dữ liệu nhạy cảm một cách hợp pháp bao gồm: Các tổ chức nhằm mục đích bảo vệ nhân quyền, Tổ chức bảo vệ trẻ em và các tổ chức được thành lập nhằm mục đích hỗ trợ khắc phục tội phạm tình dục[131]. Do đó, ngoại lệ cho phép xử lý dữ liệu cá nhân nhạy cảm vì lý do lợi ích công cộng đáng kể của Điểm g, Khoản 2 Điều 9 của GDPR đã được nhà lập pháp Bỉ diễn giải một cách đầy đủ mà không làm phương hại đến yêu cầu về lợi ích công cộng đáng kể. Tuy nhiên, travaux préparatoires làm rõ rằng danh sách các tổ chức tự nó là không đủ. Các yêu cầu bổ sung bao gồm tính tương xứng của dữ liệu với mục đích xử lý dữ liệu, bản chất của quyền bảo vệ dữ liệu phải được tôn trọng và các biện pháp cụ thể phải được thực hiện để bảo vệ quyền và lợi ích cơ bản của những người liên quan.

Dữ liệu nhạy cảm cũng có thể được xử lý bởi Cơ quan Điều phối Phân tích Mối đe dọa Bỉ (OCAD, Orgaan voor de Coördinatie en de Analyse van de Dreiging). Nhiệm vụ của OCAD bao gồm phân tích và đánh giá các mối đe dọa tiềm ẩn đối với an ninh quốc gia và công dân dựa trên thông tin nhận được từ một số dịch vụ hỗ trợ quốc gia. Xét đến việc khuôn khổ pháp lý về các cơ quan tình báo và an ninh, cũng như OCAD quy định các cơ chế giám

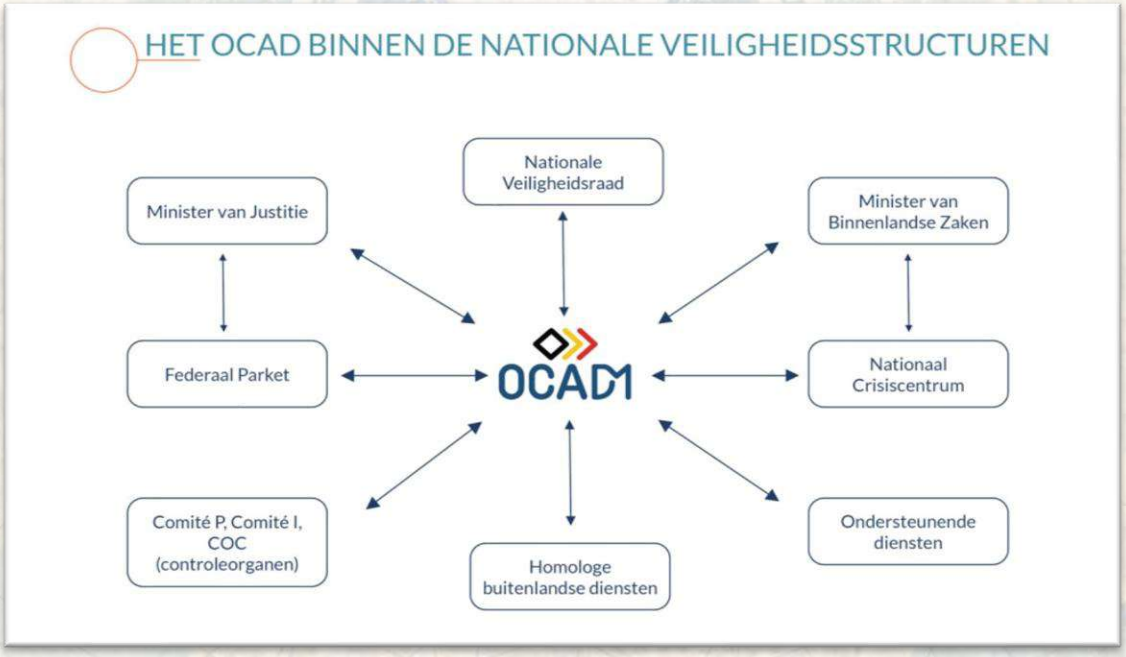
[129] Chambre, 3126/003, Travaux Préparatoires, Proposed Act on the Protection of Natural Persons concerning the Processing of Personal Data, 06.07.2018, p. 5.

[130] Chambre, 3126/003, Travaux Préparatoires, Proposed Act on the Protection of Natural Persons concerning the Processing of Personal Data, 06.07.2018, pp. 53–54.

[131] Chambre, 3126/003, Travaux Préparatoires, Proposed Act on the Protection of Natural Persons concerning the Processing of Personal Data, 06.07.2018, p. 5 and Article 8 §1 of the Act on the Protection of Natural Persons concerning the Processing of Personal Data.

sát chặt chẽ, các ngoại lệ đối với lệnh cấm chung về xử lý dữ liệu nhạy cảm rõ ràng đã bị thay thế bởi nhiệm vụ của cơ quan này[132].

Việc chỉ định một cán bộ bảo vệ dữ liệu là bắt buộc đối với tất cả các dịch vụ của chính phủ liên bang. Nghĩa vụ này được quy định tại Điều 21 của Đạo luật Khung. Tuy nhiên, điều khoản tương ứng trong GDPR (Điều 37) cho phép các quốc gia thành viên xác định các đơn vị kiểm soát hoặc xử lý dữ liệu khác, những đơn vị nên chỉ định một cán bộ bảo vệ dữ liệu. Nhà lập pháp Bỉ đã chủ động lựa chọn áp dụng yêu cầu này cho tất cả các công ty tư nhân xử lý dữ liệu cá nhân thay mặt cho các dịch vụ của chính phủ và tất cả các công ty tư nhân nhận dữ liệu cá nhân từ các dịch vụ của chính phủ. Ý kiến của DPA Bỉ về Đạo luật Khung được đề xuất đã thúc đẩy nhà lập pháp giới hạn nghĩa vụ bổ nhiệm, chỉ đối với việc xử lý dữ liệu có rủi ro cao[133].



Hình minh họa nội dung chính của OCAD - Ảnh: OCDA

[132] Chambre, 3126/001, Travaux Préparatoires, Proposed Act on the Protection of Natural Persons concerning the Processing of Personal Data, 11.06.2018, pp. 20–21.

[133] Chambre, 3126/001, Travaux Préparatoires, Proposed Act on the Protection of Natural Persons concerning the Processing of Personal Data, 11.06.2018, pp. 46–47.

1.2.7. Thổ Nhĩ Kỳ

1.2.7.1. Tổng quan về Luật Bảo vệ Dữ liệu của Thổ Nhĩ Kỳ

- Tổng quan

Sự phát triển của dữ liệu quy mô lớn là một trong những yếu tố quan trọng nhất đang định hình xã hội ngày nay. Hệ quả của xu hướng này trong lĩnh vực pháp lý là sự cần thiết phải bảo vệ quyền riêng tư trước những hành vi như phân tích hồ sơ, việc thu thập dữ liệu trái phép... Các quốc gia không thể làm ngơ trước xu hướng này; do đó, nhiều nơi đã phát triển các quy định để bảo vệ dữ liệu cá nhân. Một trong những đạo luật tiên tiến và chi tiết về vấn đề này được soạn thảo bởi Liên minh Châu Âu cũng đã thu hút sự chú ý tại Thổ Nhĩ Kỳ. Là quốc gia ứng cử viên trong hơn 30 năm, Thổ Nhĩ Kỳ có nhiều lý do để đưa luật bảo vệ dữ liệu của mình phù hợp với các tiêu chuẩn của EU.



Thổ Nhĩ Kỳ là một trong những quốc gia tiên phong về luật dữ liệu
- Ảnh: GRC World Forum

Thổ Nhĩ Kỳ cũng đã ban hành một đạo luật bảo vệ dữ liệu mới, cụ thể là Luật số 6698 về Bảo vệ Dữ liệu Cá nhân (DPL)[134] vào năm 2016 và thành

[134] Kisisel Verilerin Korunması Kanunu, [Law on the Protection of Personal Data] OJ no. 29677, 24 March 2016.

lập một cơ quan để giám sát việc bảo vệ dữ liệu cá nhân, gọi là Cơ quan Bảo vệ Dữ liệu (DPA) vào cùng năm đó. DPL là kết quả của những cuộc thảo luận lâu dài và các dự thảo luật. Trước khi DPL có hiệu lực, đã có nhiều nỗ lực để thông qua các đạo luật bảo vệ dữ liệu. Những chuẩn bị đầu tiên bắt đầu từ năm 1995 với sự thành lập ủy ban đầu tiên để chuẩn bị dự thảo bộ luật về bảo vệ dữ liệu cá nhân. Từ đầu những năm 2000, nhiều dự thảo khác đã được chuẩn bị, nhưng không có dự thảo nào được thông qua. Dự thảo cuối cùng của DPL được chuẩn bị nhanh chóng và được bỏ phiếu thông qua tại Quốc hội vào năm 2016 và có hiệu lực trong cùng năm đó[135].

- Luật Bảo vệ Dữ liệu tại Thổ Nhĩ Kỳ

Mặc dù một bộ luật cụ thể về bảo vệ dữ liệu khá mới, các quy định và án lệ của Thổ Nhĩ Kỳ liên quan đến quyền bảo vệ dữ liệu và quyền riêng tư là rất rộng lớn. Dưới đây, trước tiên sẽ là giới thiệu về các quy định bảo vệ dữ liệu của Thổ Nhĩ Kỳ, sau đó là án lệ có liên quan.

Luật chính về bảo vệ dữ liệu của Thổ Nhĩ Kỳ là Luật Bảo vệ Dữ liệu Cá nhân (DPL). Luật này có hiệu lực từ ngày 07/10/2016[136] và được xây dựng dựa trên Chỉ thị 95/46/EC về Bảo vệ Cá nhân liên quan đến Việc Xử lý Dữ liệu Cá nhân và Tự do Di chuyển Dữ liệu[137] (Chỉ thị 95/46/EC), vốn có hiệu lực trước khi GDPR ra đời. Do thiếu các quy định cụ thể về bảo vệ dữ liệu cho đến năm 2016, một loạt các quy định và bộ luật khác nhau đã

---

[135] See Küzeci 2018, pp. 311–314.

[136] Tuy nhiên, một số điều khoản trong Luật Bảo vệ Dữ liệu Cá nhân (DPL) chỉ có hiệu lực sau sáu tháng kể từ ngày luật được công bố trên Công báo Chính thức. Các điều khoản này bao gồm: chuyển dữ liệu (Điều 8), chuyển dữ liệu ra nước ngoài (Điều 9), quyền của chủ thể dữ liệu (Điều 11), thủ tục khiếu nại đối với bên kiểm soát dữ liệu (Điều 13), thủ tục khiếu nại lên Cơ quan Bảo vệ Dữ liệu (Điều 14), quy trình kiểm tra của Cơ quan Bảo vệ Dữ liệu (Điều 15), đăng ký bên kiểm soát dữ liệu (Điều 16), các hành vi phạm tội (Điều 17), và các chế tài xử phạt (Điều 18).

[137] Chỉ thị 95/46/EC của Nghị viện Châu Âu và Hội đồng ngày 24 tháng 10 năm 1995 về việc bảo vệ các cá nhân liên quan đến việc xử lý dữ liệu cá nhân và về tự do lưu chuyển dữ liệu đó, (1995) Công báo Liên minh Châu Âu (OJ) L 281.

bao gồm các điều khoản liên quan đến việc bảo vệ dữ liệu cá nhân[138]. Bên cạnh các quy định này, các Điều 23 - 25 trong Bộ Luật Dân sự Thổ Nhĩ Kỳ (TCC)[139] cũng áp dụng đối với việc bảo vệ dữ liệu cá nhân trong phạm vi bảo vệ quyền lợi cá nhân. Mặt khác, với sự cải cách trong Bộ Luật Hình sự Thổ Nhĩ Kỳ (TPC)[140] vào năm 2005, các tội phạm liên quan đến việc ghi nhận dữ liệu cá nhân, chia sẻ hoặc thu thập dữ liệu cá nhân trái phép, và không hủy bỏ dữ liệu cá nhân đã được đưa vào luật hình sự.

DPL cũng đặc biệt tham chiếu đến các quy định này. Trước khi DPL có hiệu lực, một bước quan trọng khác là việc công nhận quyền bảo vệ dữ liệu trong Hiến pháp Thổ Nhĩ Kỳ. Sau cuộc trưng cầu dân ý năm 2010, một đoạn mới đã được thêm vào Điều 20 của Hiến pháp Thổ Nhĩ Kỳ về quyền riêng tư. Đoạn này đưa ra một quyền chung về bảo vệ dữ liệu và quy định rằng việc xử lý dữ liệu chỉ có thể thực hiện khi có sự đồng ý rõ ràng của chủ thể dữ liệu hoặc theo quy định của pháp luật.

Sau khi DPL được thông qua, các quy định bổ sung cũng đã được thông qua. Các quy định này bao gồm: Quy định về việc xóa, hủy hoại hoặc ẩn danh dữ liệu cá nhân[141], và Quy định về Tổ chức và Hoạt động của Cơ quan Bảo vệ Dữ liệu, Quy định về Sổ đăng ký Các tổ chức Xử lý Dữ liệu, Quy định về Chuyên gia Bảo vệ Dữ liệu, Quy định về Tổ chức Cơ quan Bảo vệ Dữ liệu, Quy định về Việc Thúc đẩy Các Chủ Sở Hữu Lao Động trong Cơ

---

[138] Một số ví dụ bao gồm: Luật Điều chỉnh Thương mại Điện tử ("ETL") - Elektronik Ticaretin Düzenlenmesi Hakkında Kanun, Công báo số 29166, ngày 5 tháng 11 năm 2014; Luật Truyền thông Điện tử ("ECL") - Elektronik Haberleşme Kanunu, Công báo số 27050 (bản phụ), ngày 10 tháng 11 năm 2008; Luật Ngân hàng - Bankacılık Kanunu, Công báo số 25983 (bản phụ), ngày 1 tháng 11 năm 2005; Quy định về Quyền của Bệnh nhân - Hasta Hakları Yönetmeliği, Công báo số 23420, ngày 1 tháng 8 năm 1998.

[139] Türk Medeni Kanunu, OJ no. 24607, 08 December 2001 (entered into force 1 January 2002).

[140] Türk Ceza Kanunu, OJ no. 25611, 12 October 2004 (entered into force 1 April 2005).

[141] Kisisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, OJ no. 30224, 28 October 2017 (entered into force 1 January 2018).

quan Bảo vệ Dữ liệu, Quy định về Trưởng phòng Kỷ luật của Cơ quan Bảo vệ Dữ liệu, và Quy định về Dữ liệu Sức Khỏe Cá Nhân.



Một số nội dung trong luật bảo vệ dữ liệu Thổ Nhĩ Kỳ -
Ảnh: Turkish Law Services in Istanbul

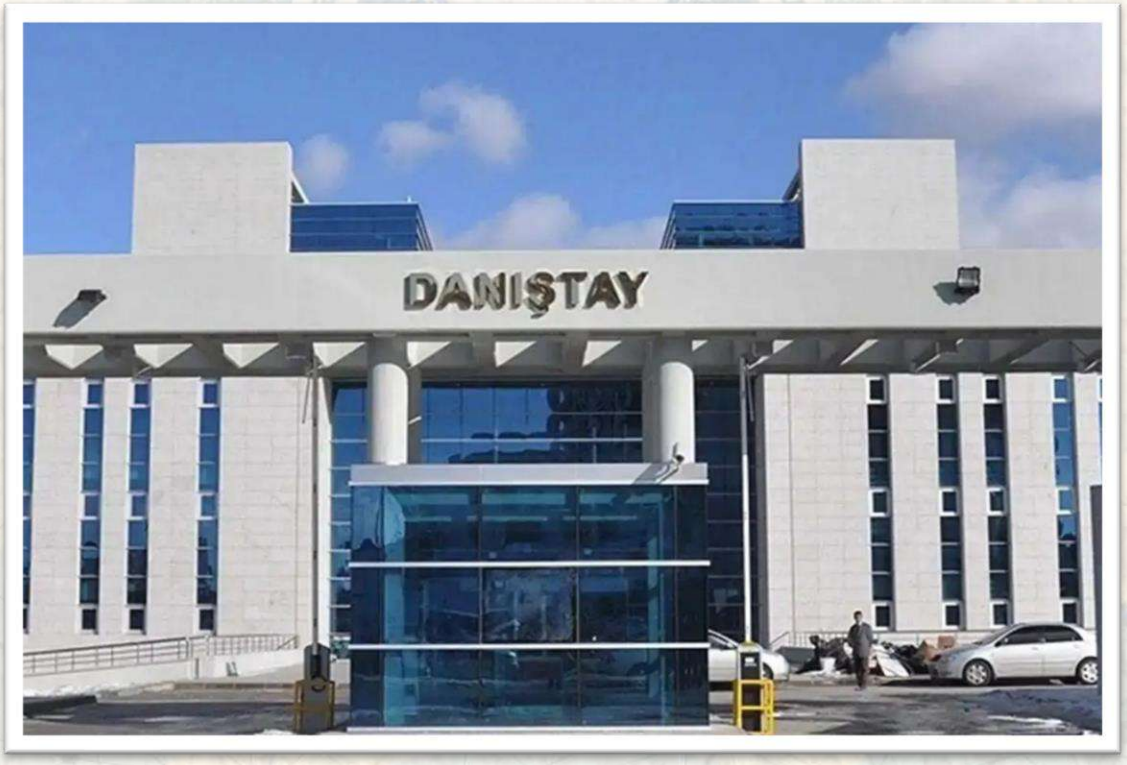
Ở cấp quốc tế, Thổ Nhĩ Kỳ là thành viên của Công ước 1981 về Bảo vệ Các Cá Nhân liên quan đến Xử lý Tự động Dữ liệu Cá nhân ("Công ước 1981"), được ký kết vào năm 1981, nhưng chỉ được phê chuẩn 35 năm sau vào năm 2016. Thổ Nhĩ Kỳ cũng đã phê chuẩn Nghị định bổ sung cho Công ước 1981 vào năm 2016 nhưng chưa phê chuẩn Nghị định bổ sung năm 2018. Mặt khác, Thổ Nhĩ Kỳ là thành viên của Công ước Châu Âu về Quyền con người và Tự do cơ bản từ năm 1949.

- Án lệ

+ Tính hợp hiến của các quy định liên quan đến dữ liệu cá nhân

Trong khoảng thời gian giữa việc thông qua Điều 20 của Hiến pháp và việc thông qua DPL, các tòa án Thổ Nhĩ Kỳ đã xử lý tính hợp hiến và hợp

pháp của một số luật và quy định về dữ liệu cá nhân. Ví dụ, Hội đồng Nhà nước (Danıştay), tòa án cao cấp về các vấn đề hành chính, đã xem xét tính hợp hiến của một điều khoản trong Luật Bảo hiểm Y tế Công cộng ("PHIL") yêu cầu tất cả các cơ sở y tế cung cấp dữ liệu thu được từ bệnh nhân cho Cơ quan Bảo hiểm Xã hội (SSI) và cho phép Bộ Lao động và Bảo hiểm Xã hội quyết định phạm vi pháp lý của việc chia sẻ dữ liệu. Tòa án Hiến pháp (CC) đã kết luận rằng việc xử lý dữ liệu bởi SSI trong trường hợp này là bắt buộc để tiến hành các dịch vụ y tế. Tuy nhiên, Tòa án Hiến pháp (CC) đã hủy bỏ phần của điều khoản nói trên trao quyền cho Bộ Lao động và Xã hội với lý do rằng quyền lập các quy định liên quan đến bảo vệ dữ liệu chỉ thuộc về các cơ quan lập pháp theo Điều 20 của Hiến pháp; do đó, các cơ quan chính phủ không có quyền này[142].



Hội đồng Nhà nước (Danıştay) Thổ Nhĩ Kỳ - Ảnh: Ilketv.com.tr

[142] E. 2014/74, K. 2014/201, 25.12.2014, OJ no. 29364, 23.05.2015.

Nghị định - Luật số 663[143] về Tổ chức và Quyền hạn của Bộ Y tế và Các Cơ quan Liên quan đã quy định rằng SSI được quyền thu thập toàn bộ dữ liệu sức khỏe cá nhân từ các cơ sở y tế công và tư. Tòa án Hiến pháp đã hủy bỏ điều khoản này vì lý do rằng các quyền và tự do cơ bản, cũng như quyền chính trị, không thể bị hạn chế hoặc điều chỉnh bằng nghị định - luật[144]. Một điều khoản rất giống đã được tái triển khai với một dự luật tổng hợp nhằm lách quyết định của CC; tuy nhiên, điều khoản này cũng đã bị thách thức. Lần này, Tòa án Hiến pháp kết luận rằng sự can thiệp vào quyền bảo vệ dữ liệu là không tương xứng, đặc biệt là khi điều khoản bị thách thức quy định việc thu thập, xử lý và chia sẻ dữ liệu sức khỏe "bằng mọi phương tiện". Với lý do tương tự, CC đã hủy bỏ các điều khoản trong các Nghị định - Luật khác trao quyền cho nhân viên hải quan và Viện Văn hóa, Tôn giáo và Lịch sử Atatürk (Atatürk Kültür, Dil ve Tarih Yüksek Kurumu)[145] yêu cầu bất kỳ dữ liệu hoặc thông tin nào trong phạm vi của họ.

Cuối cùng, một số điều khoản về hình phạt liên quan đến tội phạm bảo vệ dữ liệu đã bị thách thức trước Tòa án Hiến pháp. Ví dụ, Điều 136 của Bộ Luật Hình sự (TPC) đã bị thách thức do thiếu sự rõ ràng về định nghĩa của thuật ngữ "dữ liệu cá nhân". Tòa án kết luận rằng thuật ngữ "dữ liệu cá nhân" đã được định nghĩa rõ ràng trong nhiều quyết định của tòa án, vì vậy các điều khoản liên quan của TPC tuân thủ nguyên tắc hợp pháp trong các tội phạm[146]. Hơn nữa, một số điều khoản trong DPL cũng đã được đưa ra trước Tòa án Hiến pháp (CC). Tòa án Hiến pháp không coi các điều khoản này là vi phạm hiến pháp.

---

[143] Sa˘ glık Alanında Bazı Düzenlemeler Hakkında Kanun Hükmünde Kararname, OJ no. 28103 bis.,2 November 2011.

[144] E. 2011/150, K. 2013/30, 14 February 2013, OJ no. 28688, 26 June 2013.

[145] E. 2011/141, K. 2013/10, 10 January 2013, OJ no. 28865, 28 December 2013

[146] E. 2015/32, K. 2015/102, 12 November 2015, OJ no. 29550, 2 December 2015.



Viện Văn hóa, Tôn giáo và Lịch sử Atatürk - Ảnh: TOKI Haber

+ Án lệ Thổ Nhĩ Kỳ cũng đã công nhận quyền được quên.

Trong một khiếu nại hiến pháp liên quan đến việc không gỡ bỏ một bản tin đã được đăng tải trên Internet suốt mười bốn năm, Tòa án Hiến pháp khẳng định rằng mặc dù quyền được quên chưa được quy định rõ trong bất kỳ văn bản luật nào, nhưng "đây là một trong những nghĩa vụ tích cực của Nhà nước nhằm bảo vệ quyền tự định đoạt cá nhân". Tuy nhiên, Tòa cũng đã bác bỏ các khiếu nại hiến pháp tương tự với lý do thời gian trôi qua chưa đủ lâu để biện minh cho việc thực hiện quyền được quên[147]. Đại Hội đồng của Tòa Phúc thẩm (Yargıtay) - tòa án tối cao chuyên trách các vụ việc dân sự và hình sự - cũng đã công nhận quyền được quên trong một vụ án, trong đó tên đầy đủ của nạn nhân trong một vụ án hình sự trước đó được nêu rõ trong bản án và sau này tiếp tục xuất hiện trong các cuốn sách đề cập đến vụ việc đó.

[147] 0Asli Alp ve ¸ Sükrü Alp, No. 2014/18260, 4 October 2017; Asım Bayar ve Veysel Bayar, No. 2014/4141, 4 October 2017; G.D (2), No. 2014/1808, 4 October 2017; Gözde Yi˘ git, No. 2017/16026,5 October 2017; Fahri Göncü, No. 2014/17943, 5 October 2017.



Trụ sở Tòa phúc thẩm của Thổ Nhĩ Kỳ - Ảnh: Eden Hukuk & Arabuluculuk

1.2.7.2. Sự tương tác giữa GDPR và chính sách pháp luật của Thổ Nhĩ Kỳ

Vì DPL (Luật Bảo vệ Dữ liệu Cá nhân của Thổ Nhĩ Kỳ) được xây dựng dựa trên Chỉ thị 95/46/EC, nên nó có nền tảng tương tự như GDPR. Tuy nhiên, GDPR có các quy định tiên tiến hơn về bảo vệ dữ liệu và duy trì an ninh dữ liệu. Cả hai hệ thống sẽ được đánh giá dưới đây về các khía cạnh như phạm vi áp dụng, nguyên tắc và ngoại lệ, cùng với quyền, nghĩa vụ và biện pháp khắc phục.

- Phạm vi áp dụng và các điều khoản

Cả DPL và GDPR đều đưa ra các quy định liên quan đến bảo vệ dữ liệu cá nhân. Định nghĩa về dữ liệu trong DPL và GDPR cũng rất giống nhau. DPL có phạm vi rộng hơn về việc thông tin nào sẽ được xem là dữ liệu. Theo đó, *"bất kỳ thông tin nào có thể gán cho hoặc liên kết với một cá nhân"* là dữ liệu cá nhân. Giống như GDPR, DPL chỉ áp dụng cho dữ liệu của các cá nhân, trong khi các pháp nhân không nằm trong phạm vi áp dụng.

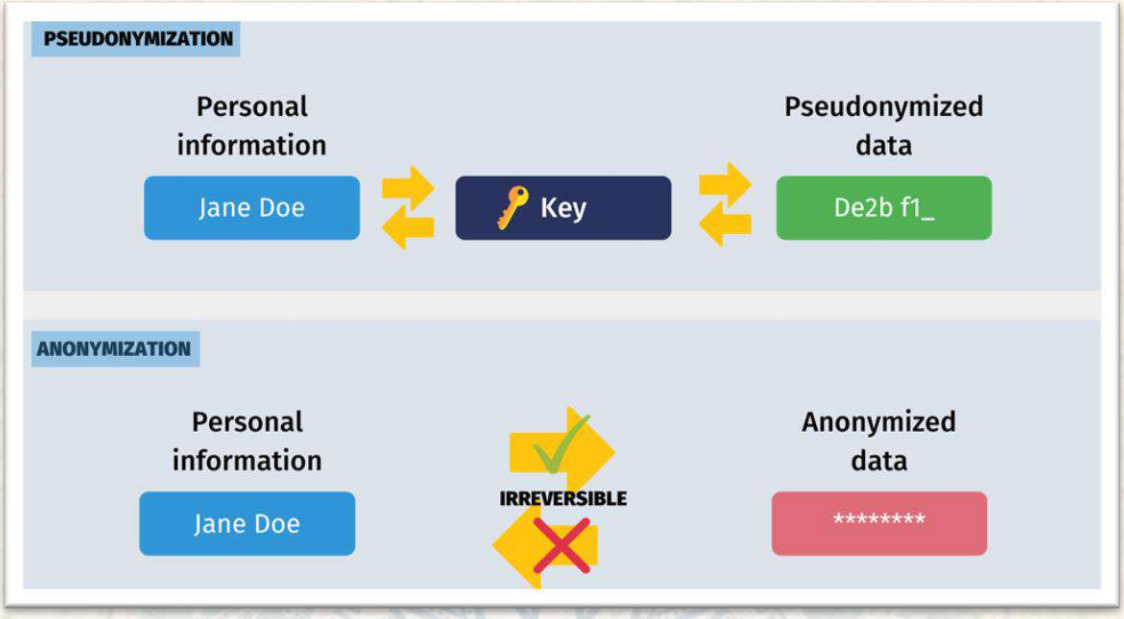
DPL áp dụng đối với việc xử lý dữ liệu cá nhân. Các hoạt động được liệt kê như là xử lý bao gồm: "thu thập, ghi nhận, lưu trữ, giữ, thay đổi,

sắp xếp, tiết lộ, chuyển nhượng, tiếp nhận, cung cấp, phân loại hoặc khóa" (Điều 3(1)/e). Danh sách này không đầy đủ như trong GDPR, nơi liệt kê các phương pháp xử lý dữ liệu là "thu thập, ghi nhận, tổ chức, cấu trúc, lưu trữ, điều chỉnh hoặc thay đổi, truy xuất, tham vấn, sử dụng, tiết lộ qua truyền tải, phân phối hoặc cung cấp theo bất kỳ cách nào khác, căn chỉnh hoặc kết hợp, hạn chế, xóa bỏ hoặc hủy diệt" (Điều 4(2)). Giống như GDPR, DPL cũng thừa nhận các phương thức xử lý dữ liệu không tự động bên cạnh các phương thức tự động trong trường hợp chúng là một phần của hệ thống hồ sơ.

Cả hai DPL và GDPR đều áp dụng đối với bất kỳ loại dữ liệu cá nhân nào, ngoại trừ dữ liệu đã được ẩn danh, nhưng DPL không có quy định cụ thể về dữ liệu đã được mã hóa (pseudonymized). *Về dữ liệu nhạy cảm,* Điều 6 DPL định nghĩa dữ liệu nhạy cảm là "dữ liệu liên quan đến chủng tộc, nguồn gốc dân tộc, quan điểm chính trị, niềm tin triết học, tôn giáo, tín ngưỡng hoặc các tín ngưỡng khác, ngoại hình, tư cách thành viên các hiệp hội, tổ chức hay công đoàn, sức khỏe, đời sống tình dục, án tù hoặc các biện pháp an ninh cũng như dữ liệu sinh trắc học và di truyền". Định nghĩa này gần như giống hệt trong GDPR, ngoại trừ việc DPL không bao gồm "hướng tính" (sexual orientation). Hơn nữa, theo Điều 9(1) GDPR, dữ liệu sinh trắc học và di truyền được coi là dữ liệu nhạy cảm khi "được xử lý nhằm mục đích xác định một cách duy nhất một cá nhân". Sự khác biệt này không tồn tại trong DPL.

DPL cũng phân biệt giữa người kiểm soát dữ liệu và người xử lý dữ liệu. Người xử lý dữ liệu là "cá nhân hoặc pháp nhân xử lý dữ liệu cá nhân thay mặt người kiểm soát dữ liệu theo quyền hạn mà họ đã được cấp". Mặt khác, người kiểm soát dữ liệu là "cá nhân hoặc pháp nhân có quyền quyết

định mục đích và phương thức xử lý dữ liệu, và vận hành và quản lý một hệ thống đăng ký dữ liệu" (Điều 3(1)/1, tức điểm 1, khoản 1, Điều 3).



GDPR phát triển cả nội dung về dữ liệu được mã hóa - Ảnh: DPM

Việc chuyển dữ liệu cho bên thứ ba được phép thực hiện khi có sự đồng ý rõ ràng của chủ thể dữ liệu. Thêm vào đó, các điều kiện tại Điều 5(2) và Điều 6(3) cũng phải được đáp ứng. Đối với việc chuyển dữ liệu ra ngoài quốc gia, sự đồng ý rõ ràng của chủ thể dữ liệu lại một lần nữa là cần thiết. Ngoài ra, Điều 9 DPL chỉ cho phép chuyển dữ liệu sang "các quốc gia được chấp nhận". Trong trường hợp không có sự chấp nhận này, người kiểm soát dữ liệu tại Thổ Nhĩ Kỳ và quốc gia thứ ba cần cung cấp bảo lãnh bằng văn bản và DPA phải phê duyệt việc chuyển dữ liệu. Theo Điều 9(4) DPL, khi ra quyết định này, DPA sẽ xem xét các thỏa thuận quốc tế mà Thổ Nhĩ Kỳ đã phê chuẩn, tính đối ứng trong việc chuyển dữ liệu giữa Thổ Nhĩ Kỳ và quốc gia thứ ba, mục đích và thời gian xử lý dữ liệu, các quy định và thực tiễn bảo vệ dữ liệu của quốc gia thứ ba, và các biện pháp an toàn mà người kiểm soát dữ liệu cung cấp. DPA vẫn chưa quyết định quốc gia thứ ba nào được chấp nhận, tuy nhiên, đã công bố các tiêu chí cần thiết để đánh giá. Theo đó, DPA

sẽ đánh giá các tiêu chí được quy định tại Điều 9(4) cùng với việc thành lập một cơ quan bảo vệ dữ liệu độc lập, các công ước quốc tế về bảo vệ dữ liệu mà quốc gia thứ ba là bên tham gia, các tổ chức khu vực hoặc quốc tế mà quốc gia thứ ba là thành viên, và khối lượng thương mại với quốc gia thứ ba. Trong trường hợp không có quốc gia thứ ba được chấp nhận, DPA đã kết luận trong một quyết định rằng việc sử dụng email doanh nghiệp qua nền tảng Google sẽ dẫn đến việc chuyển dữ liệu quốc tế sang một quốc gia thứ ba và do đó việc sử dụng này phải tuân theo các tiêu chí được quy định trong Điều 9 DPL. Theo GDPR, các quốc gia được quy định tại Điều 45 và Điều 46 có các yêu cầu rộng hơn và chi tiết hơn về việc bảo vệ dữ liệu. Trong hệ thống GDPR, Thổ Nhĩ Kỳ không được liệt kê là một trong các quốc gia cung cấp mức độ bảo vệ đầy đủ.

- Nguyên tắc và ngoại lệ

Trong Điều 4, DPL công nhận các nguyên tắc sau: "xử lý hợp pháp và công bằng", "xử lý chính xác và thực tế", "xử lý cho mục đích cụ thể, rõ ràng và hợp pháp", "xử lý phù hợp với mục đích, cũng như xử lý có giới hạn và tỉ lệ", và "lưu trữ chỉ trong thời gian quy định bởi luật hoặc cần thiết cho mục đích xử lý". Các nguyên tắc "minh bạch", "an ninh phù hợp", và "trách nhiệm giải trình" trong Điều 5(1)/a, 5(1)/f, và 5(2) của GDPR không được nhắc đến rõ ràng trong DPL. Tuy nhiên, những nguyên tắc này, cùng với các tiêu chí được quy định trong Điều 5(2) và Điều 6(2) và (3), xác định phạm vi mà trong đó việc xử lý dữ liệu được phép thực hiện.

Điều 5 DPL quy định rằng việc xử lý dữ liệu chỉ có thể thực hiện khi có sự đồng ý rõ ràng của chủ thể dữ liệu. Sự đồng ý phải "cụ thể đối với nội dung, dựa trên thông tin và được đưa ra một cách tự nguyện" theo Điều 3(1)/a DPL. GDPR phân biệt sự đồng ý đối với dữ liệu cá nhân và dữ liệu

nhạy cảm. Ngược lại, DPL yêu cầu sự đồng ý rõ ràng đối với cả hai loại dữ liệu này trong Điều 5(1) và Điều 6(2). GDPR quy định sự đồng ý của người chưa đủ tuổi; tuy nhiên, DPL không có quy định cụ thể về sự đồng ý của người chưa đủ tuổi. Các vấn đề liên quan đến người chưa đủ tuổi sẽ được giải quyết theo Bộ Luật Dân sự Thổ Nhĩ Kỳ (TCC).

Điều kiện để xử lý dữ liệu mà không cần sự đồng ý rõ ràng của chủ thể dữ liệu được quy định tại Điều 5(2) DPL. Các nguyên tắc này, dựa trên Chỉ thị 95/46/EC, tương tự như trong GDPR.

Khác biệt, DPL cũng công nhận việc tiết lộ dữ liệu trước đó bởi chủ thể dữ liệu như một ngoại lệ đối với yêu cầu về sự đồng ý rõ ràng (Điều 5(2)/d). Mối quan hệ giữa các điều kiện này với yêu cầu về sự đồng ý rõ ràng đang được tranh luận. Xu hướng hiện tại trong học thuật là không tìm kiếm một thứ bậc giữa yêu cầu về sự đồng ý rõ ràng và các điều kiện khác[148]. Một cách giải thích khác là trao cho thẩm phán quyền tự quyết định liệu việc xử lý dữ liệu mà không có sự đồng ý rõ ràng có hợp pháp hay không, ngay cả khi các điều kiện được đề cập đã được đáp ứng.

Về ngoại lệ đối với sự đồng ý đối với việc xử lý dữ liệu nhạy cảm, DPL phân biệt giữa dữ liệu nhạy cảm liên quan đến sức khỏe và đời sống tình dục và các loại dữ liệu nhạy cảm khác. Không có sự đồng ý rõ ràng, dữ liệu sức khỏe và đời sống tình dục chỉ có thể được xử lý bởi các cơ quan và tổ chức có thẩm quyền, hoặc những người có nghĩa vụ bảo mật, vì mục đích bảo vệ sức khỏe cộng đồng, y tế phòng ngừa, thực hiện dịch vụ chẩn đoán y tế, điều trị và chăm sóc, lập kế hoạch dịch vụ y tế và tài chính của chúng theo Điều 6(3) DPL. Mặt khác, các loại dữ liệu nhạy cảm khác có thể được xử lý mà không cần sự đồng ý rõ ràng nếu được quy định trong luật. Trong mọi trường

[148] Dülger 2019, p. 26; Yüceda˘ g 2017, p. 773.

hợp, các điều kiện cần thiết theo Điều 5 cũng phải được đáp ứng đối với việc xử lý dữ liệu nhạy cảm. GDPR, ngược lại, có một bộ ngoại lệ khác đối với việc xử lý dữ liệu nhạy cảm. Ở đây, việc tiết lộ rõ ràng dữ liệu bởi chủ thể dữ liệu là một ngoại lệ đối với yêu cầu về sự đồng ý rõ ràng (Điều 9(2)/e).

Các trường hợp mà DPL không áp dụng tương tự như trong Chỉ thị 95/46/EC. Chỉ thị 95/46/EC không áp dụng cho các vấn đề an ninh công cộng, quốc phòng hoặc luật hình sự. Theo Chỉ thị 95/46/EC, DPL có một ngoại lệ tương tự nhưng rộng hơn trong Điều 28. DPL không áp dụng cho việc xử lý dữ liệu cho mục đích gia đình, cho thống kê miễn là dữ liệu được ẩn danh với thống kê công cộng, cho nghệ thuật, lịch sử, văn học hoặc cho việc xử lý được thực hiện trong phạm vi tự do ngôn luận (Điều 28(1)/a, b, c). Ngoài ra, DPL cũng không áp dụng cho việc xử lý dữ liệu của các cơ quan công quyền cho mục đích quốc phòng, an ninh quốc gia, an ninh công cộng, chính sách công hoặc an ninh kinh tế, hoặc do các cơ quan tư pháp thực hiện (Điều 28(1)/c và d).

Mặt khác, nghĩa vụ thông báo và đăng ký vào sổ đăng ký của người xử lý dữ liệu không áp dụng trong trường hợp xử lý dữ liệu cần thiết để ngăn ngừa hoặc điều tra tội phạm, dữ liệu đã được tiết lộ bởi chủ thể dữ liệu, việc xử lý dữ liệu được thực hiện bởi các cơ quan công quyền và cần thiết cho công tác kiểm toán hoặc kỷ luật, và trong các trường hợp mà việc xử lý dữ liệu là cần thiết cho mục đích thuế hoặc kinh tế.

- Quyền, nghĩa vụ và biện pháp bảo đảm

Quyền của chủ thể dữ liệu và nghĩa vụ của người kiểm soát dữ liệu trong DPL có bản chất tương tự như trong GDPR. Tuy nhiên, các quy định trong GDPR chi tiết hơn. DPL công nhận quyền thông tin, quyền truy cập, quyền chỉnh sửa, quyền xóa bỏ, quyền chuyển dữ liệu, quyền phản đối và

quyền đền bù. DPL không quy định quyền *"quyền được quên"* như trong Điều 17 của GDPR, nhưng công nhận quyền xóa bỏ ít chi tiết hơn phù hợp với Chỉ thị 95/46/EC.

Về quyền phản đối, DPL chỉ công nhận quyền này khi việc xử lý dẫn đến một kết quả không có lợi cho chủ thể dữ liệu. Cách diễn đạt trong quy định có vẻ mở và có thể được giải thích khác nhau, so với cách diễn đạt trong Điều 21 GDPR.

Về nghĩa vụ của người kiểm soát dữ liệu, DPL có ít quy định toàn diện hơn so với GDPR. Ví dụ, DPL không đưa ra nghĩa vụ chung về việc ghi chép, cũng không có quy định cụ thể về các cơ chế bảo vệ dữ liệu theo thiết kế hoặc theo mặc định. Điều 12 DPL liệt kê các nghĩa vụ chung của người kiểm soát dữ liệu về bảo mật dữ liệu. Những nghĩa vụ này bao gồm: "thực hiện tất cả các biện pháp kỹ thuật và hành chính để đảm bảo bảo mật dữ liệu, tiến hành kiểm tra cần thiết, tránh tiết lộ dữ liệu cá nhân đã thu thập và thông báo ngay cho DPA trong trường hợp dữ liệu cá nhân bị thu thập trái phép bởi bên thứ ba." Người kiểm soát dữ liệu có trách nhiệm liên đới với người xử lý dữ liệu theo Điều 12(2) DPL. Trong trường hợp vi phạm dữ liệu, người kiểm soát dữ liệu có nghĩa vụ thông báo cho DPA càng sớm càng tốt. DPA, với sự tham chiếu rõ ràng đến GDPR, đã kết luận rằng thời gian thông báo vi phạm dữ liệu là 72 giờ.

Người kiểm soát dữ liệu phải đăng ký trong Sổ đăng ký Người kiểm soát Dữ liệu. DPA cũng đã triển khai Hệ thống Thông tin về Sổ đăng ký Người kiểm soát Dữ liệu (VERBIS), một cơ sở dữ liệu trực tuyến nhằm tạo điều kiện thuận lợi cho việc ghi chép đăng ký. DPA đã công bố các thời hạn đăng ký vào VERBIS như sau: 01.10.2018 - 30.09.2019 đối với các cá nhân hoặc pháp nhân có hơn 50 nhân viên hoặc doanh thu trên TRY 25,000,000,

và các tổ chức đăng ký ở nước ngoài; 01.01.2019 - 31.03.2020 đối với các cá nhân và pháp nhân có ít hơn 50 nhân viên hoặc doanh thu dưới TRY 25,000,000, nhưng xử lý dữ liệu nhạy cảm; 01.04.2019 - 30.06.2020 đối với các tổ chức công. Tuy nhiên, thời hạn đối với các cá nhân hoặc pháp nhân có hơn 50 nhân viên hoặc doanh thu trên TRY 25,000,000, và các tổ chức đăng ký ở nước ngoài đã được kéo dài đến 31/12/2019.



Hệ thống Thông tin về Sổ đăng ký Người kiểm soát Dữ liệu (VERBIS) - Ảnh: Kurt Gürler Partners

Trong một quyết định trước đó, DPA đã tuyên bố rằng những người xử lý sử dụng hệ thống xử lý không tự động, công chứng viên, các hiệp hội, quỹ và công đoàn chỉ xử lý dữ liệu cá nhân liên quan đến nhân viên, thành viên và người đóng góp trong lĩnh vực hoạt động của họ, các đảng chính trị, luật sư, kế toán độc lập và kế toán công chứng viên được miễn nghĩa vụ đăng ký. Ngoài ra, DPA cũng miễn trừ các nhân viên hải quan, môi giới, và các cá nhân hoặc pháp nhân có ít hơn 50 nhân viên hoặc doanh thu dưới TRY 25,000,000 nếu họ không xử lý dữ liệu nhạy cảm khỏi nghĩa vụ đăng ký.

Các điểm mới quan trọng khác của GDPR là việc bổ nhiệm Cán bộ Bảo vệ Dữ liệu (DPO) và yêu cầu thực hiện Đánh giá Tác động Bảo vệ Dữ liệu. Những tổ chức này không được quy định trong DPL.

Điều 13 DPL cung cấp quy trình khiếu nại cho chủ thể dữ liệu: họ có thể gửi khiếu nại bằng văn bản đến người kiểm soát dữ liệu và phải nhận được phản hồi trong vòng 30 ngày. Trong trường hợp phản hồi tiêu cực hoặc không thỏa đáng, chủ thể dữ liệu có thể gửi khiếu nại tiếp theo tới DPA. DPA cũng có thể thực hiện chức năng kiểm tra vi phạm dữ liệu mà không cần có khiếu nại trước.

DPL quy định *ba loại biện pháp khắc phục:* hình phạt hành chính, hình phạt hình sự và bồi thường. Phạt hành chính được áp dụng nếu người kiểm soát dữ liệu không tuân thủ nghĩa vụ minh bạch hoặc các yêu cầu liên quan đến sổ đăng ký người kiểm soát dữ liệu, vi phạm bảo mật dữ liệu, hoặc không tuân theo các quyết định của DPA. Các mức phạt hành chính dao động từ TRY 5,000 đến TRY 1,000,000 tùy theo mức độ vi phạm. Có thể áp dụng nhiều khoản phạt cho mỗi vi phạm. Ngoài các khoản phạt hành chính, một cuộc điều tra kỷ luật cũng có thể được thực hiện nếu vi phạm xảy ra do cán bộ nhà nước.

Về hình phạt hình sự, DPL tham chiếu đến các Điều 135 - 138 của Bộ Luật Hình sự (TPC). Điều 135 quy định án tù từ một đến ba năm trong trường hợp ghi nhận dữ liệu cá nhân. Điều 136 quy định án tù từ hai đến bốn năm trong trường hợp thu thập và tiết lộ dữ liệu cá nhân trái phép. Và Điều 138 quy định án tù từ một đến hai năm đối với việc không hủy dữ liệu cá nhân.

Cuối cùng, chủ thể dữ liệu cũng có quyền theo Điều 23 - 25 TCC để ngừng các hành vi xâm phạm quyền nhân thân. Theo đó, chủ thể dữ liệu có quyền yêu cầu ngừng xâm phạm, ngừng xâm phạm có thể xảy ra trong tương

lai, tuyên bố xâm phạm, yêu cầu bồi thường vật chất hoặc phi vật chất, hoặc yêu cầu chuyển nhượng lợi nhuận thu được từ việc xâm phạm. GDPR cũng có nhiều biện pháp khắc phục khác nhau. Tùy thuộc vào mức độ nghiêm trọng của vi phạm, GDPR bao gồm các khoản phạt hành chính rất cao theo Điều 83. Quyền yêu cầu bồi thường phụ thuộc vào luật của quốc gia thành viên theo Điều 82 GDPR. Các hình phạt hình sự có thể áp dụng theo luật quốc gia thành viên theo Điều 84 GDPR.

1.2.7.3. Các vấn đề nổi bật

Mặc dù Thổ Nhĩ Kỳ đã thông qua những luật và quy định quan trọng về bảo vệ dữ liệu cá nhân, nhưng vẫn còn một số trở ngại trong việc đảm bảo các tiêu chuẩn bảo vệ cao. Một trong những thách thức lớn nhất là việc sử dụng dữ liệu cá nhân một cách thường xuyên cả bởi các cơ quan công quyền và các công ty tư nhân. Cơ quan Bảo vệ Dữ liệu (DPA), mặt khác, đã nỗ lực ngăn chặn việc sử dụng dữ liệu cá nhân, đặc biệt là trong khu vực tư nhân. Các hoạt động và quyết định liên quan của DPA là một bước phát triển tích cực. Tuy nhiên, tính độc lập của DPA cũng là một vấn đề đáng lo ngại. Một số khía cạnh quan trọng của các vấn đề này sẽ được phản ánh dưới đây.

- Việc sử dụng dữ liệu cá nhân thường xuyên

Việc số hóa các dịch vụ công đã tạo thêm một lớp vấn đề nữa. Ví dụ, nhiều cơ quan nhà nước cung cấp dịch vụ tài liệu trực tuyến qua một cổng gọi là e-State. Dịch vụ này đã được cung cấp cho công dân Thổ Nhĩ Kỳ từ năm 2008. Người dân có thể lấy các thông tin như hộ khẩu, sổ đăng ký dân sự, hồ sơ tội phạm và sức khỏe; họ cũng có thể thanh toán nợ thuế hoặc khoản vay sinh viên, hoặc theo dõi các tài liệu tòa án trực tuyến qua cổng này. Cũng có các cổng dịch vụ trực tuyến khác do các cơ quan công quyền vận hành. Ví dụ, *MERNIS* là cơ sở dữ liệu chứa hồ sơ sổ đăng ký dân sự; cơ

sở dữ liệu *UYAP* được sử dụng bởi nhân viên pháp lý, luật sư và công dân để quản lý các tranh chấp pháp lý và hồ sơ pháp lý; cuối cùng, *e-Nabız* là cơ sở dữ liệu chứa hồ sơ y tế và cho phép công dân lấy lịch hẹn bác sĩ và các yêu cầu liên quan đến y tế khác.

Từ khi bắt đầu số hóa các dịch vụ công, việc lưu trữ dữ liệu trực tuyến đã dấy lên câu hỏi về mức độ bảo mật dữ liệu mà nhà nước cung cấp. Không may, vào năm 2016, một vụ vi phạm bảo mật đã xảy ra liên quan đến một nền tảng khác lưu trữ dữ liệu cá nhân của cử tri và đã lộ ra rằng dữ liệu của các cử tri có quyền bầu cử từ năm 2010 đã bị hack và bị rò rỉ trên Internet. Thông tin bị hack gồm có số Chứng minh nhân dân, tên, họ, địa chỉ đăng ký, ngày sinh, tên cha mẹ của gần 50 triệu công dân Thổ Nhĩ Kỳ.

Không chỉ các cơ quan công quyền, mà cả các cá nhân tư nhân cũng thường xuyên sử dụng dữ liệu cá nhân. Một vấn đề gây tranh cãi trong thực tế là việc các công ty tư nhân sử dụng dữ liệu cá nhân như một phương pháp xác minh danh tính hoặc kiểm tra an ninh. Ví dụ, các ngân hàng cũng như các công ty GSM đều sao chép thẻ căn cước của một người, thậm chí sao chép các hóa đơn đã thanh toán trước đó hoặc biên lai thẻ tín dụng trong một số hoạt động của họ. Báo cáo SSC 2013 cho biết các công ty GSM lưu trữ bản sao thẻ căn cước của khoảng 68 triệu người ở Thổ Nhĩ Kỳ. Một ví dụ khác là các công ty vận chuyển tư nhân theo quyết định của BTK về "Các Biện pháp An ninh liên quan đến Giao hàng Bưu kiện" ban hành vào năm 2016. Theo đó, các công ty vận chuyển có nghĩa vụ lưu trữ thông tin tên, địa chỉ và số Chứng minh nhân dân của cả người gửi và người nhận. Thông tin này cần phải được lưu trữ trong cơ sở dữ liệu của các công ty vận chuyển trong hai năm. Tương tự, các công ty cũng yêu cầu người tiêu dùng cung cấp số Chứng minh nhân dân trong các hợp đồng từ xa để có thể cung cấp thông

tin này cho việc vận chuyển. Do số chứng minh nhân dân chỉ có thể được cấp một lần và không thể thay đổi theo Điều 46 của Luật Dịch vụ Đăng ký Dân sự, Việc sử dụng số chứng minh nhân dân một cách thường xuyên khiến thông tin này dễ bị lạm dụng và gian lận. Các cuộc gọi quảng cáo trái phép và tin nhắn SMS từ các công ty cũng là một vấn đề đáng lo ngại.

Mặc dù đã có những vấn đề tiêu cực, nhưng chính sách bảo vệ dữ liệu của Thổ Nhĩ Kỳ đã được cải thiện sau khi thông qua DPL và thành lập DPA. Cả các cơ quan công và các tổ chức tư nhân đều đang xem xét lại các chính sách bảo mật của họ và việc bảo vệ dữ liệu đã nhận được sự quan tâm và tầm quan trọng cần thiết. Hy vọng rằng việc áp dụng nhất quán DPL sẽ thay đổi triển vọng về bảo vệ dữ liệu và quyền riêng tư tại Thổ Nhĩ Kỳ.

- Hoạt động của DPA

Vai trò của Cơ quan Bảo vệ Dữ liệu (DPA) như một cơ quan giám sát việc bảo vệ dữ liệu cá nhân trong thực tế là một sự phát triển được hoan nghênh. Kể từ khi được thành lập với DPL, DPA không chỉ xử lý các khiếu nại từ các chủ thể dữ liệu về các vi phạm liên quan đến dữ liệu cá nhân, mà còn công khai các quyết định này qua trang web của mình. DPA cũng đóng vai trò tích cực trong việc chia sẻ kiến thức về luật bảo vệ dữ liệu, bao gồm việc công bố các hướng dẫn khác nhau về các chủ đề trong luật bảo vệ dữ liệu. DPA cũng xuất bản một tạp chí định kỳ mang tên ***"Kişisel Verileri Koruma Dergisi"*** (Tạp chí Luật Bảo vệ Dữ liệu) và tổ chức các hội nghị thường xuyên.

Vai trò quan trọng nhất mà DPA đảm nhận là đưa ra quyết định đối với các khiếu nại của chủ thể dữ liệu. DPA công bố các quyết định của mình nếu vi phạm đó xảy ra thường xuyên trong thực tế, theo Điều 15(6) DPL. Do đó, DPA đã công bố nhiều quyết định trên trang web của mình kể từ khi được

thành lập. Mặc dù các quyết định này chỉ có giá trị pháp lý đối với các chủ thể dữ liệu đã làm khiếu nại và đối với cá nhân hoặc pháp nhân đã gây ra vi phạm, chúng vẫn là một ví dụ quan trọng trong thực tiễn để đảm bảo tuân thủ, do đó chúng là tài sản quý giá trong việc bảo vệ dữ liệu cá nhân.



Hình ảnh Tạp chí Luật Bảo vệ Dữ liệu - Ảnh: Kişisel Verileri Koruma Dergisi

Các khiếu nại mà DPA đã xử lý liên quan đến một loạt các vi phạm dữ liệu. Chúng có thể được nhóm lại như sau:

+ ***Tiết lộ dữ liệu cá nhân trái phép:*** Quyết định đầu tiên của DPA đã xác định một vi phạm dữ liệu từ các trang web cung cấp dịch vụ danh bạ điện thoại, nơi mọi người có thể truy cập tên của người khác thông qua số điện thoại hoặc ngược lại. Trong một quyết định tiếp theo, DPA đã quyết định rằng các công ty cung cấp dịch vụ qua quầy và bàn cần phải tổ chức cấu trúc nội bộ của mình sao cho ngăn chặn người thứ ba thu thập dữ liệu cá nhân của các chủ thể dữ liệu, để họ không thể nghe, thấy, học hỏi hoặc thu thập dữ liệu cá nhân khi chủ thể dữ liệu tiết lộ chúng. DPA đã phạt một hiệu thuốc vì tiết lộ dữ liệu sức khỏe của khách hàng cho một người thứ ba do

thiếu sự đồng ý rõ ràng và phạt một luật sư số tiền TRY 50.000 vì gửi nhầm tin nhắn chứa dữ liệu cá nhân cho một khách hàng khác. DPA đã cảnh báo một công ty kinh doanh trực tuyến qua trang web của mình và đã cung cấp dữ liệu của khách hàng cho các khách hàng đã đăng ký khác.

+ ***Biện pháp bảo vệ cho bảo vệ đầy đủ:*** Một quyết định của DPA đã thiết lập các biện pháp cần thiết mà người kiểm soát dữ liệu phải thực hiện khi xử lý dữ liệu nhạy cảm. Các biện pháp quan trọng nhất trong đó bao gồm quy trình ổn định và bền vững, đào tạo nhân viên, các thỏa thuận bảo mật, lưu trữ mã hóa và ghi chép an toàn để...

- Những thay đổi trong tổ chức và quyền hạn của DPA

Cấu trúc tổ chức của DPA cũng đã thay đổi. Do đó, giờ đây DPA chịu sự quản lý của Bộ Tư pháp theo Sắc lệnh Tổng thống số 1. Nghị định - Luật số 703 đã giới thiệu một số thay đổi đối với DPL về tổ chức của DPA. Theo hệ thống mới, bốn trong số chín thành viên được bầu bởi Tổng thống, trong khi năm thành viên còn lại được bầu bởi Quốc hội. Thêm vào đó, DPA không còn gửi báo cáo hàng năm cho Văn phòng Thủ tướng mà sẽ gửi cho Chủ tịch và Ủy ban Kiểm tra Nhân quyền trong Quốc hội.

Trước khi thay đổi này, DPL yêu cầu các thành viên của DPA phải có ít nhất 10 năm kinh nghiệm làm việc trong khu vực công hoặc tư nhân, cũng như trong các tổ chức phi chính phủ hoặc các tổ chức quốc tế. Điều kiện này sẽ không còn yêu cầu nữa. Hơn nữa, Điều 21(3)/d của Luật quy định rằng "các thành viên được bổ nhiệm vào công việc phải đồng ý và cần chú ý đảm bảo có các thành viên có kinh nghiệm trong lĩnh vực này" cũng bị bãi bỏ. Theo Điều 21(5) DPA, việc lựa chọn thành viên bởi Quốc hội được bắt đầu bằng các đề xuất từ các nhóm chính trị hoặc đại diện, sau đó là cuộc bỏ phiếu kín trong Đại hội đồng Quốc hội. Quy trình về việc lựa chọn thành viên bởi

Tổng thống, mặt khác, không được quy định trong DPL. Thêm nữa, từ giờ trở đi, Tổng thống sẽ quyết định về bất kỳ cuộc điều tra nào đối với các thành viên của DPA theo Điều 21(11) DPL.

Những thay đổi này dấy lên câu hỏi về tính độc lập của DPA. Mối liên hệ của DPA với tổ chức nhà nước đã đặt ra nghi ngờ về phương thức làm việc của DPA và hiệu quả của các biện pháp bảo vệ cho bảo vệ dữ liệu cá nhân. Ví dụ, Tổng thống là người duy nhất khởi xướng các cuộc điều tra đối với các thành viên của DPA. Mặt khác, việc không công khai tất cả các quyết định của DPA cũng làm suy yếu tính minh bạch của nó. Câu hỏi về tính độc lập này cũng đã được nêu trong các báo cáo tiến độ về Thổ Nhĩ Kỳ. Không thể quên rằng Tòa án Công lý của Liên minh Châu Âu đã từng giải quyết vấn đề về "tính độc lập" và có quan điểm tiêu cực về sự kiểm soát của nhà nước hoặc chính phủ đối với các cơ quan bảo vệ dữ liệu quốc gia.

- Sự hài hòa của Thổ Nhĩ Kỳ với EU và GDPR

Ngoài việc GDPR áp dụng gián tiếp, Thổ Nhĩ Kỳ cũng có thể thông qua một đạo luật mới dựa trên GDPR để đảm bảo sự hài hòa với luật EU, với tư cách là quốc gia ứng cử viên gia nhập EU. Thổ Nhĩ Kỳ đã nộp đơn xin trở thành quốc gia ứng cử viên vào năm 1987, được phê duyệt vào năm 1999, và các cuộc đàm phán gia nhập bắt đầu từ năm 2005. Việc đóng một số chương trong đàm phán đã bị trì hoãn trừ khi Thổ Nhĩ Kỳ công nhận Síp là bên ký kết của Thỏa thuận Ankara. Tuy nhiên, các cuộc đàm phán gia nhập hiện nay đang bị đóng băng.

Việc ứng cử của Thổ Nhĩ Kỳ cũng đã đưa việc điều chỉnh luật bảo vệ dữ liệu vào các vấn đề đàm phán. Nhu cầu của Thổ Nhĩ Kỳ để điều chỉnh luật bảo vệ dữ liệu theo các tiêu chuẩn của EU trong lĩnh vực Tư pháp và Nội vụ đã được nêu ra lần đầu tiên một cách ngắn gọn trong báo cáo tiến độ

năm 1998. Nhu cầu soạn thảo một đạo luật riêng biệt về bảo vệ dữ liệu sau đó đã được thể hiện trong Tài liệu Quan hệ Đối tác Gia nhập năm 2003, trong đó nói rằng việc hài hòa hóa trong lĩnh vực này là một trong những mục tiêu ngắn hạn. Trong Chương trình Quốc gia năm 2003, thời gian để soạn thảo các đạo luật cần thiết được lên kế hoạch hoàn thành vào năm 2004. Cho đến khi DPL được thông qua, việc thiếu một quy định đặc biệt về bảo vệ dữ liệu cá nhân gần như đã được đề cập trong mọi báo cáo tiến độ. Tuy nhiên, công việc này chỉ được hoàn thành vào năm 2016, khi mà EU đã có những tiến bộ về bảo vệ dữ liệu và đang chuẩn bị tiếp nhận các quy định tiên tiến hơn. Việc không xem xét GDPR trong quá trình soạn thảo DPL là một cơ hội bị bỏ lỡ đối với Thổ Nhĩ Kỳ.

Yêu cầu về các quy định bảo vệ dữ liệu hài hòa với hệ thống EU có hai yếu tố: *Thứ nhất,* các quy tắc bảo vệ dữ liệu cá nhân phải tuân thủ các tiêu chuẩn của EU và *thứ hai,* cần có sự thực hành tương tự về xử lý dữ liệu bởi các cơ quan cảnh sát và tư pháp để đảm bảo hợp tác trong các vấn đề tư pháp và cảnh sát. Thực tế, Báo cáo Tiến độ 2016 chỉ ra rằng việc Thổ Nhĩ Kỳ thông qua Luật Bảo vệ Dữ liệu Cá nhân không đạt được mức độ tương đương với Luật pháp Chung của EU do các ngoại lệ rộng rãi áp dụng đối với việc xử lý dữ liệu và những lo ngại về tính độc lập của DPA. Báo cáo Tiến độ 2018 cũng chỉ ra rằng Thổ Nhĩ Kỳ cần tiến bộ về luật bảo vệ dữ liệu để điều chỉnh luật lệ với các tiêu chuẩn của châu Âu và bắt đầu các cuộc đàm phán với các hoạt động của Europol. Báo cáo tiến độ mới nhất vào năm 2019 nhấn mạnh rằng Thổ Nhĩ Kỳ cần phải hài hòa hóa luật bảo vệ dữ liệu với GDPR và Chỉ thị EU 2016/680. Báo cáo này cũng đề cập đến các lo ngại về quyền hạn của DPA và việc bảo vệ dữ liệu cá nhân trong thực thi pháp luật.



Trụ sở cơ quan europool - Ảnh: European Union

Liên minh Châu Âu đang thảo luận về việc mở đàm phán một thỏa thuận về việc trao đổi dữ liệu để chống lại tội phạm nghiêm trọng và khủng bố. Trong một nghị quyết gần đây về các cuộc đàm phán với Thổ Nhĩ Kỳ về việc trao đổi dữ liệu cá nhân giữa Europol và Thổ Nhĩ Kỳ, Nghị viện Châu Âu đã nhấn mạnh rằng việc chuyển giao dữ liệu sang Thổ Nhĩ Kỳ có nhiều rủi ro và yêu cầu thỏa thuận trong tương lai phải có các quy định cụ thể về việc lưu trữ dữ liệu cá nhân.

Mặc dù tương lai của nó hiện nay còn chưa chắc chắn, các cuộc đàm phán về thỏa thuận này dự kiến sẽ có tác động tích cực đối với việc phát triển các quy định về bảo vệ dữ liệu cá nhân tại Thổ Nhĩ Kỳ. Là một quốc gia ứng cử viên gia nhập EU, việc thông qua các quy định hài hòa với GDPR chắc chắn sẽ là một trong những chính sách trong chương trình hài hòa hóa của Thổ Nhĩ Kỳ trong tương lai.

Như vậy, nhu cầu bảo vệ đầy đủ dữ liệu cá nhân là một trong những vấn đề quan trọng nhất của xã hội số. Việc EU thông qua GDPR đã tạo ra một bước tiến quan trọng để xây dựng một thị trường duy nhất, nơi các chủ thể được bảo vệ đầy đủ về dữ liệu cá nhân của mình. Theo bước EU, Thổ Nhĩ Kỳ cũng đã có tiến bộ trong việc bảo vệ dữ liệu cá nhân và quyền riêng tư bằng cách thông qua DPL; tuy nhiên, việc hài hòa hóa hơn nữa yêu cầu một cách tiếp cận thận trọng hơn đối với việc xử lý dữ liệu. Đặc biệt, như chương này đã chỉ ra, việc sử dụng dữ liệu cá nhân thường xuyên trong thực tế cần phải giảm bớt và DPA cần phải độc lập hơn. Tuy nhiên, chương này cũng đưa ra rằng các luật và quy định hiện tại cũng như án lệ cung cấp một mức độ bảo vệ tương đương và việc hài hòa hóa trong tương lai sẽ không gặp quá nhiều khó khăn. Tương lai sẽ cho thấy các bước đi tiếp theo của Thổ Nhĩ Kỳ để thu hẹp khoảng cách giữa DPL và GDPR.

1.2.8. Liên bang Nga

Tại Liên bang Nga, hiện nay có một số đạo luật liên quan đến thông tin, công nghệ thông tin, dữ liệu cá nhân đang được áp dụng như Luật Liên bang Nga về thông tin, công nghệ thông tin và bảo vệ thông tin; Luật Liên bang Nga về dữ liệu cá nhân. Theo quy định của Luật Liên bang Nga về thông tin, công nghệ thông tin và bảo vệ thông tin, thông tin được xác định là tin tức, dữ liệu, bất kể hình thức trình bày nào của chúng. Đạo Luật này thiết lập các quy định cụ thể liên quan đến thông tin, công nghệ thông tin và bảo vệ thông tin như xác định thông tin được chia thành thông tin có sẵn công khai và thông tin bị hạn chế quyền truy cập. Luật của Nga cũng xác định cụ thể về chủ sở hữu thông tin, quyền và nghĩa vụ của chủ sở hữu thông tin; quyền tiếp cận thông tin; hoạt động của nhà cung cấp dịch vụ lưu trữ, nhà điều hành hệ thống tìm kiếm phân phối thông tin trang tổng hợp tin tức; việc

phổ biến thông tin trên mạng xã hội; hạn chế quyền truy cập thông tin; trách nhiệm của cơ quan nhà nước, chính quyền địa phương trong việc thực hiện cung cấp thông tin, tài liệu theo yêu cầu của công dân.

Hệ thống thông tin theo pháp luật của Nga được xác định bao gồm: ***(1)*** Hệ thống thông tin nhà nước, hệ thống thông tin liên bang và hệ thống thông tin khu vực được tạo ra dựa trên cơ sở Luật liên bang, luật của các đơn vị cấu thành Liên bang Nga, trên cơ sở thẩm quyền của các cơ quan này. Theo đó, danh sách các loại thông tin được cung cấp bắt buộc được quy định theo Luật Liên bang; ***(2)*** Hệ thống thông tin thành phố được tạo ra trên cơ sở quyết định của các cơ quan chính quyền địa phương; ***(3)*** các hệ thống thông tin khác[149].

Luật Liên bang về dữ liệu cá nhân (Luật số 152 - FZ), còn được gọi là Luật bảo vệ dữ liệu của Nga, là văn bản pháp luật điều chỉnh việc thu thập, xử lý, lưu trữ và chuyển giao dữ liệu cá nhân tại quốc gia này. Luật này được ban hành lần đầu vào năm 2006 và đã trải qua nhiều lần sửa đổi, bổ sung, gần nhất là vào tháng 2/2023. Luật số 152 - FZ áp dụng rộng rãi cho bất kỳ cá nhân, tổ chức nào xử lý dữ liệu cá nhân của công dân nước Nga, bất kể họ ở trong hay ngoài nước. Thật vậy, Luật Dữ liệu cá nhân của Liên bang Nga điều chỉnh việc xử lý dữ liệu cá nhân của các nhà khai thác trong lãnh thổ Liên bang Nga và các nhà khai thác ở nước ngoài liên quan đến dữ liệu cá nhân của công dân Nga nếu dữ liệu này được thu thập trong lãnh thổ Nga hoặc liên quan đến cung cấp hàng hóa, dịch vụ cho công dân Nga hoặc giám sát hành vi của họ trong nước Nga. Luật được áp dụng cho mọi dữ liệu cá nhân bao gồm thông tin về danh tính như tên, địa

[149] Russian Federation (2006), *Federal Law No. 149-FZ of July 27, 2006*, on Information, Information Technologies and Protection of Information, [Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации"].

chỉ, ngày sinh, số hộ chiếu và thông tin cá nhân khác cũng như thông tin về sức khỏe và tài chính.



Luật Liên bang Nga về thông tin, công nghệ thông tin và bảo vệ thông tin - Ảnh: Лезги Газет

Mở rộng phạm vi nghiên cứu và tìm hiểu, khi đề cập đến nước Nga chúng ta có thể nhận thấy chính sách bảo mật về an toàn thông tin ở quốc gia này cũng được chú trọng xây dựng một cách chặt chẽ. Ngày 1/5/2022, Tổng thống Nga đã ký Sắc lệnh số 250 về *"các biện pháp bổ sung để đảm bảo an ninh thông tin của Liên bang Nga"*. Đáng chú ý, Sắc lệnh này có hiệu lực từ ngày công bố, có nghĩa là ngay lập tức các yêu cầu được đặt ra trong pháp lệnh cần phải được tuân thủ[150].

[150] Nam Trần (2022), *Một số điểm quan trọng trong Sắc lệnh mới của Nga về tăng cường an toàn thông tin*, https://antoanthongtin.vn/tin/mot-so-diem-quan-trong-trong-sac-lenh-moi-cua-nga-ve-tang-cuong-an-toan-thong-tin, truy cập ngày 8/8/2025.



Minh họa Luật số 152-FZ - Ảnh: мнение

Những tổ chức chịu sự điều chỉnh của Sắc lệnh này cần phải thực hiện một số biện pháp nhằm tăng cường mức độ an toàn của tài nguyên thông tin, bao gồm: Cơ quan hành pháp liên bang; các cơ quan hành pháp cao nhất của quyền lực nhà nước của các chủ thể cấu thành của Liên bang Nga; Quỹ Nhà nước; Các tập đoàn nhà nước và các công ty nhà nước do Liên bang Nga thành lập trên cơ sở luật liên bang (ví dụ Rosatom, Gazprom, rusHydro, Russian Railways và các công ty khác); Doanh nghiệp chiến lược và công ty cổ phần chiến lược; Các pháp nhân là đối tượng của các cơ sở hạ tầng thông tin quan trọng; các tổ chức "xương sống" của nền kinh tế Nga.



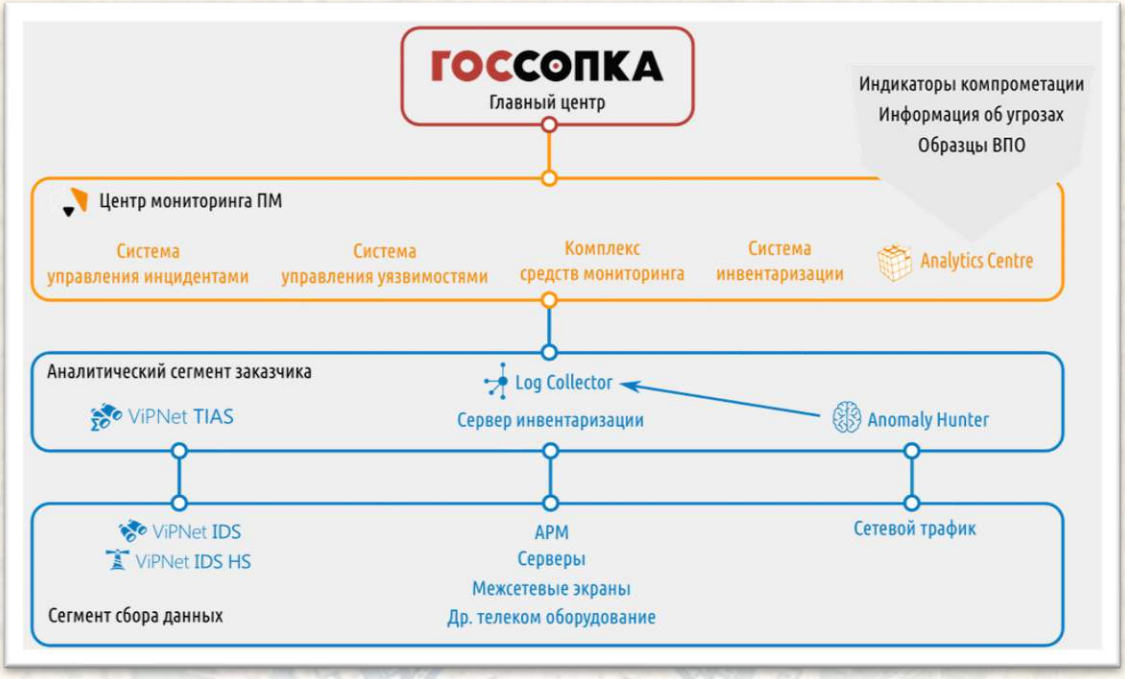
Những tác động của Sắc lệnh số 250 - Ảnh: Телеком биржа

Theo yêu cầu được nêu trong Sắc lệnh số 250, các tổ chức trên cần phải thực hiện:

+ ***Xây dựng đơn vị riêng trực thuộc tổ chức của mình có trách nhiệm bảo đảm an toàn thông tin:*** Giao một cán bộ cấp phó đứng đầu đơn vị bảo đảm an toàn thông tin; Xác định rõ trách nhiệm của người đứng đầu tổ chức trong việc đảm bảo an toàn thông tin. Để chuẩn bị cho điều này, Chính phủ Liên bang Nga đã chỉ đạo xây dựng các quy định tiêu chuẩn về cấp phó phụ trách và cơ cấu tổ chức của đơn vị đảm bảo an toàn thông tin, trong đó cần lưu ý với những người làm trực tiếp công tác bảo đảm an toàn thông tin cần đáp ứng các yêu cầu bổ sung về trình độ theo Điều 12 Sắc lệnh số 235 ngày 21/12/2017 của các trung tâm ứng cứu, khắc phục sự cố máy tính (FSTEC) Liên bang Nga.

+ ***Tiến hành kiểm kê các hợp đồng với nhà thầu cung cấp dịch vụ bảo mật thông tin,*** chỉ có những nhà thầu được FSTEC Liên bang Nga cấp phép mới được tham gia các dịch vụ đảm bảo an toàn thông tin với các thông tin

liên quan đến bí mật nhà nước Nga. Yêu cầu này cũng cần được tính đến khi đưa ra các quyết định tiếp theo về việc thu hút nhà thầu. Danh sách các tổ chức doanh nghiệp được cơ quan FSTEC Liên bang Nga cấp phép, được đăng tải thông tin công khai trên trang web chính thức của cơ quan này.



Phương thức kết nối theo GosSOPKA - Ảnh: ООО КриптоСвязь

+ Chỉ những trung tâm được công nhận của hệ thống nhà nước về phát hiện ngăn chặn và loại bỏ hậu quả của các cuộc tấn công máy tính (GosSOPKA) mới có thể tham gia vào các hoạt động phát hiện, ngăn chặn và loại bỏ hậu quả của các cuộc tấn công máy tính và ứng phó với các sự cố máy tính. Do đó, các tổ chức cần phải chủ động kết nối với một trung tâm GosSOPKA đã được công nhận để phối hợp trong việc theo dõi, giám sát, khắc phục sự cố liên quan đến các cuộc tấn công trên hệ thống máy tính của tổ chức mình. Hiện tại, yêu cầu này chưa bắt buộc, tuy nhiên, về lâu dài các tổ chức cần tính toán xây dựng lộ trình phối hợp với các trung tâm nói trên tùy theo mức độ của hệ thống thông tin mình đang quản lý hoặc theo quy định của từng bộ ngành, trong lĩnh vực hoạt động của mình.

+ Các tổ chức cần đảm bảo giám sát liên tục và thực hiện đầy đủ các khuyến cáo (cả về chính sách quản lý và giải pháp kỹ thuật) để bảo đảm an ninh, an toàn thông tin do cơ quan FSB Liên bang Nga và FSTEC của Nga gửi tới. Ngoài ra, các tổ chức cần chuẩn bị cung cấp các quyền truy cập (bao gồm các truy cập từ xa) cho cơ quan FSB Liên bang Nga vào các nguồn thông tin để giám sát an ninh. Dựa trên kết quả giám sát đó, các tổ chức phải tuân thủ các hướng dẫn của FSB Nga (nếu có).

Như vậy, theo sắc lệnh mới này của Tổng thống Liên Bang Nga, tất cả các tổ chức thuộc danh mục tổ chức quan trọng phải có trách nhiệm tổ chức thực hiện việc đảm bảo an toàn thông tin đối với hệ thống công nghệ thông tin của mình, đồng thời, phân định trách nhiệm cụ thể của lãnh đạo các cấp trong tổ chức của mình liên quan đến việc bảo đảm an ninh an toàn thông tin cho hệ thống.

Trong tương lai, Chính phủ Liên bang Nga sẽ đưa ra các yêu cầu về đảm bảo an toàn thông tin cho hệ thống công nghệ thông tin vào các văn bản hành chính liên quan đến thực thi công vụ của Liên bang Nga. Bên cạnh đó, các tổ chức thuộc danh mục tổ chức quan trọng cần nhanh chóng tiến hành đánh giá an ninh, kiểm kê các thiết bị bảo mật thông tin và lập kế hoạch chuyển đổi sang sử dụng chủ yếu các thiết bị, giải pháp được phát triển trong nước.

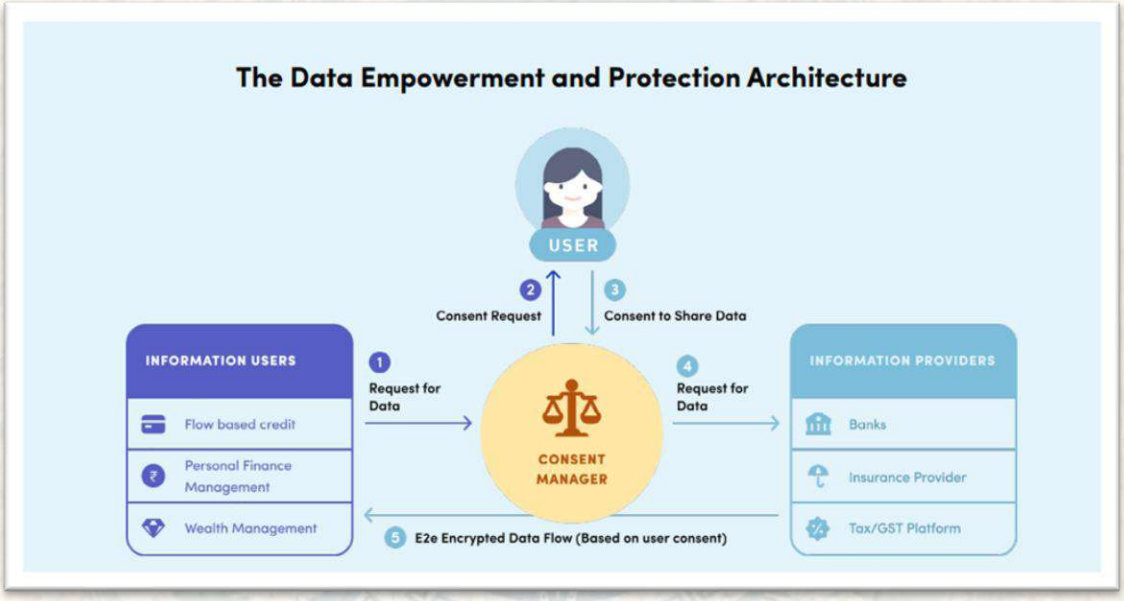
1.2.9. Ấn Độ

Chính sách quản trị dữ liệu của Ấn Độ tập trung vào từng loại dữ liệu, đã xây dựng khung quản trị cho dữ liệu cá nhân, dữ liệu phi cá nhân và dữ liệu của Chính phủ.

Về dữ liệu cá nhân, "Quy tắc công nghệ thông tin" thông qua năm 2011 là khuôn khổ cơ bản điều chỉnh dữ liệu cá nhân nhạy cảm. Dự thảo "Luật bảo vệ dữ liệu cá nhân" năm 2019 chú ý nhiều đến nội địa hóa dữ liệu; đề

xuất quy định chặt chẽ đối với luồng dữ liệu xuyên biên giới và trao cho chính phủ Ấn Độ quyền lấy dữ liệu người dùng từ các công ty (nỗ lực nhằm áp đặt các quy định chặt chẽ hơn đối với các Bigtech).

Để cho phép chia sẻ dữ liệu cá nhân thuận lợi, Ấn Độ đã đề xuất "Khung kiến trúc trao quyền và bảo vệ dữ liệu" (DEPA). Tháng 8/2022, Ấn Độ rút lại dự thảo năm 2019 và công bố bản dự thảo "Luật bảo vệ dữ liệu cá nhân" mới năm 2022.



Khung kiến trúc trao quyền và bảo vệ dữ liệu - Ảnh:niti.gov.in

Dự thảo năm 2022 được kỳ vọng là sẽ thiết lập cơ chế luồng dữ liệu xuyên biên giới tự do hơn, khung thông báo và chấp thuận đơn giản hơn, cơ quan giám sát, bảo vệ dữ liệu toàn diện hơn và khung bảo vệ dữ liệu cá nhân chặt chẽ hơn…

Về dữ liệu phi cá nhân, Ấn Độ không chỉ nỗ lực chia sẻ dữ liệu trong nền kinh tế và xã hội mà còn xây dựng các quy tắc để thúc đẩy lưu thông và sử dụng dữ liệu do Chính phủ nắm giữ. Năm 2019, Bộ điện tử và Công nghệ thông tin đã triệu tập Ủy ban Gorpalakrishnan để đưa ra các ý tưởng về cách quản lý dữ liệu phi cá nhân ở Ấn Độ.

Tháng 12/2020, Ủy ban Gorpalakrishnan công bố báo cáo về *"Khung quản trị đối với dữ liệu khi cá nhân"* để tham khảo ý kiến cộng đồng. Ủy ban Gorpalakrishnan định nghĩa dữ liệu phi cá nhân này dữ liệu không liên quan đến một cá nhân và dữ liệu từng là dữ liệu cá nhân nhưng được ẩn danh để không xác định danh tính của một cá nhân. Ủy ban cũng khuyến nghị thành lập một cơ quan dữ liệu phi cá nhân để hoạt động tách biệt với cơ quan bảo vệ dữ liệu.

Về dữ liệu của Chính phủ, tháng 03/2022, Ấn Độ công bố "Chính sách tiếp cận và chia sẻ dữ liệu quốc gia" nhằm mục đích chia sẻ dữ liệu phi cá nhân và không nhạy cảm cho chính phủ nắm giữ vì lợi ích công cộng.

Chính sách quy định cho phép Chính phủ cung cấp dữ liệu ở định dạng có thể đọc được bằng mấy và con người thông qua việc phát triển nền tảng dữ liệu mở. Để thúc đẩy việc sử dụng dữ liệu cho Chính phủ quản lý, tháng 2/2022, Bộ Điện tử và Công nghệ thông tin công bố dự thảo *"Chính sách về khả năng truy cập và sử dụng dữ liệu"* của Ấn Độ năm 2022, quy định rằng Chính phủ có thể đặt giá bán dữ liệu mà họ nắm giữ, điều này đã gặp nhiều chỉ trích.



Chính sách tiếp cận và chia sẻ dữ liệu quốc gia của Ấn Độ - Ảnh: Secure Privacy

Do đó, tháng 5/2022, Bộ Điện tử và Công nghệ thông tin công bố dự thảo "Chính sách của quản lý dữ liệu quốc gia" có cấu trúc tương tự như dự thảo ban hành vào tháng 2 nhưng đã loại bỏ các điều khoản cấp phép về định giá dữ liệu gây tranh cãi. Dự thảo đặt ra việc xây dựng kho lưu trữ dữ liệu lớn và thành lập Văn phòng quản lý dữ liệu Ấn Độ (IDMO), chịu trách nhiệm xây dựng quy tắc thu thập, lưu trữ dữ liệu và quản lý nền tảng tập dữ liệu.

Ngoài ra, Ấn Độ cũng đề xuất một khung pháp lý kỹ thuật cho việc sử dụng dữ liệu cá nhân, cụ thể là dự thảo *"Kiến trúc trao quyền và bảo vệ dữ liệu"* do Viện nghiên cứu chuyển đổi quốc gia ban hành vào tháng 8 năm 2020 nhằm mục đích cung cấp cho bên xử lý dữ liệu phương pháp kiểm soát đối với dữ liệu cá nhân, thúc đẩy chia sẻ dữ liệu thống nhất giữa các bên xử lý dữ liệu.

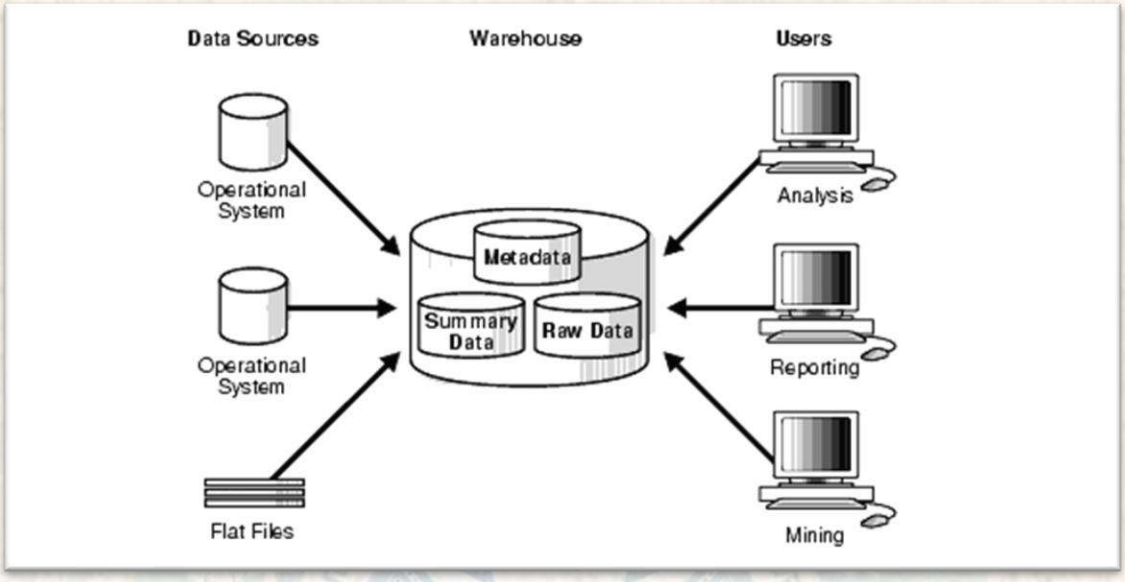
1.2.10. Đan Mạch

Để nâng cao hiệu quả chia sẻ dữ liệu giữa các cơ quan Chính phủ và các cộng đồng doanh nghiệp, Đan Mạch đã xây dựng chương trình *"Dữ liệu cơ bản"*. Chương trình đã xây dựng các "cơ sở dữ liệu cơ bản" và hệ thống "Phân phối dữ liệu tập trung" để đáp ứng các dịch vụ công cũng như các hoạt động khác của Chính phủ, đồng thời cung cấp dịch vụ dữ liệu cho các doanh nghiệp khác.

Các "cơ sở dữ liệu cơ bản" đóng vai trò như "cơ sở dữ liệu quốc gia" mà Đan Mạch đã triển khai, bao gồm: ***(1)*** Cơ sở dữ liệu về con người; ***(2)*** Cơ sở dữ liệu về pháp nhân; ***(3)*** Cơ sở dữ liệu tài sản; ***(4)*** Cơ sở dữ liệu địa chính; ***(5)*** Cơ sở dữ liệu địa chỉ; ***(6)*** Cơ sở dữ liệu địa lý, bản đồ.

Đối với việc trao đổi các dữ liệu đặc thù giữa các cơ quan Chính phủ vẫn được tiến hành thông qua các kênh kết nối trực tiếp, Đan Mạch không triển khai các hệ thống tập trung để đáp ứng trao đổi dữ liệu giữa các bộ

ngành. Tuy nhiên, Đan Mạch có các công ty tư nhân cung cấp các nền tảng tích hợp dữ liệu, trao đổi dữ liệu dưới hình thức các dịch vụ đám mây, cho phép các cơ quan chính phủ thực hiện trao đổi thông tin.



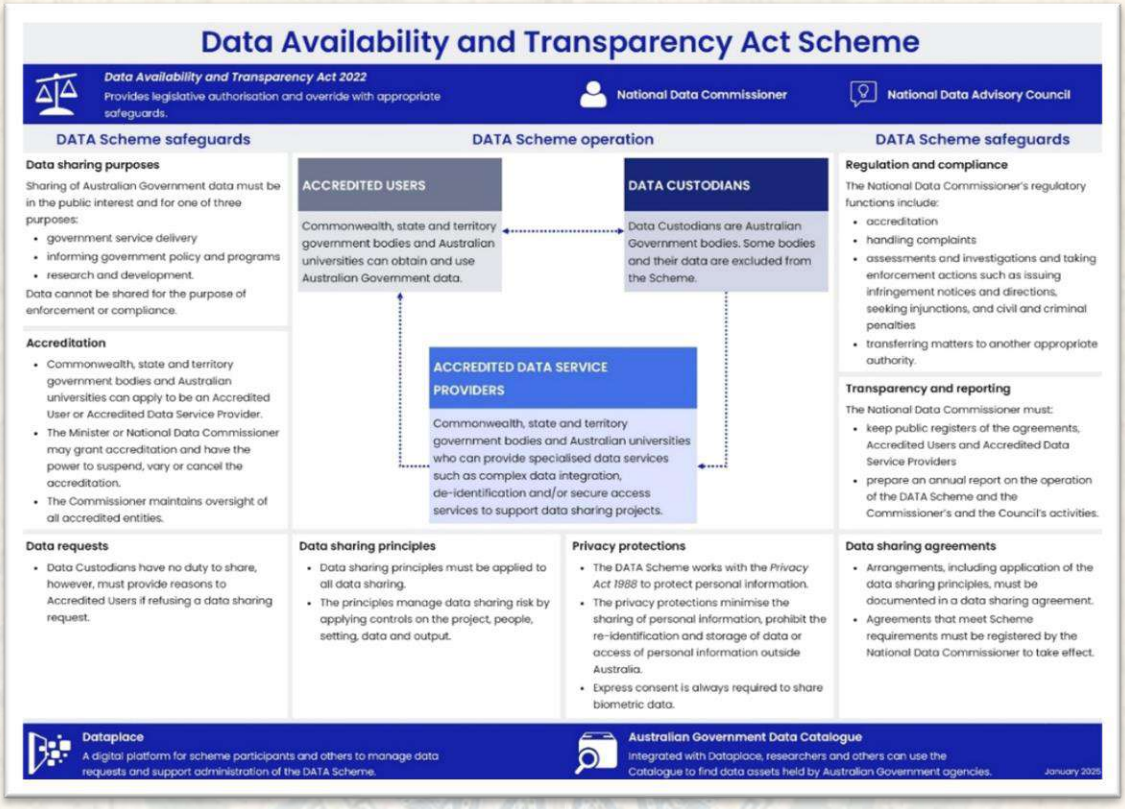
Mô hình Grundlæggende data của Đan Mạch - Ảnh: Astera Software

1.2.11. Úc

"Đạo luật minh bạch và sẵn có dữ liệu 2022" (Data Availability and Transparency Act 2022 - DAT Act) của Úc đã thiết lập một chương trình thực hành mới, tốt nhất để chia sẻ dữ liệu của Chính phủ Úc - Lược đồ DATA. Lược đồ DATA được củng cố bởi các biện pháp bảo vệ mạnh mẽ mà các quy trình nhất quán, hiệu quả. Nó tập trung vào việc tăng tính sẵn có và sử dụng dữ liệu của Chính phủ Úc để cung cấp các dịch vụ của Chính phủ một cách đơn giản, hiệu quả, thể hiện sự tôn trọng và thông báo các chính sách, chương trình tốt hơn của Chính phủ và hỗ trợ nghiên cứu, phát triển hàng đầu thế giới.

Dữ liệu có thể được chia sẻ: Dữ liệu của Chính phủ bao gồm tất cả các dữ liệu được thu thập, tạo ra hoặc nắm giữ hợp pháp bởi một cơ quan Khối thịnh vượng chung hoặc thay mặt cho cơ quan đó. Dữ liệu có thể bao gồm

một loạt các chủ đề, từ dữ liệu liên quan đến thời tiết, dữ liệu cá nhân và doanh nghiệp, thông qua các phong trào vận chuyển hàng hóa, giao thông và sản lượng công nông nghiệp.



Đạo luật minh bạch và sẵn có dữ liệu 2022 - Ảnh: datacommissioner.gov.au

Những người tham gia vào Lược đồ DATA bao gồm: Người giám sát dữ liệu; Người dùng được công nhận; Các nhà cung cấp dịch vụ dữ liệu được công nhận trong các cơ quan Chính phủ Khối thịnh vượng chung kiểm soát dữ liệu khu vực công; các cơ quan Chính phủ Tiểu bang và vùng lãnh thổ và các Trường đại học Úc. Các thực thể phải đăng ký để được công nhận là người dùng dữ liệu hoặc nhà cung cấp dịch vụ dữ liệu.

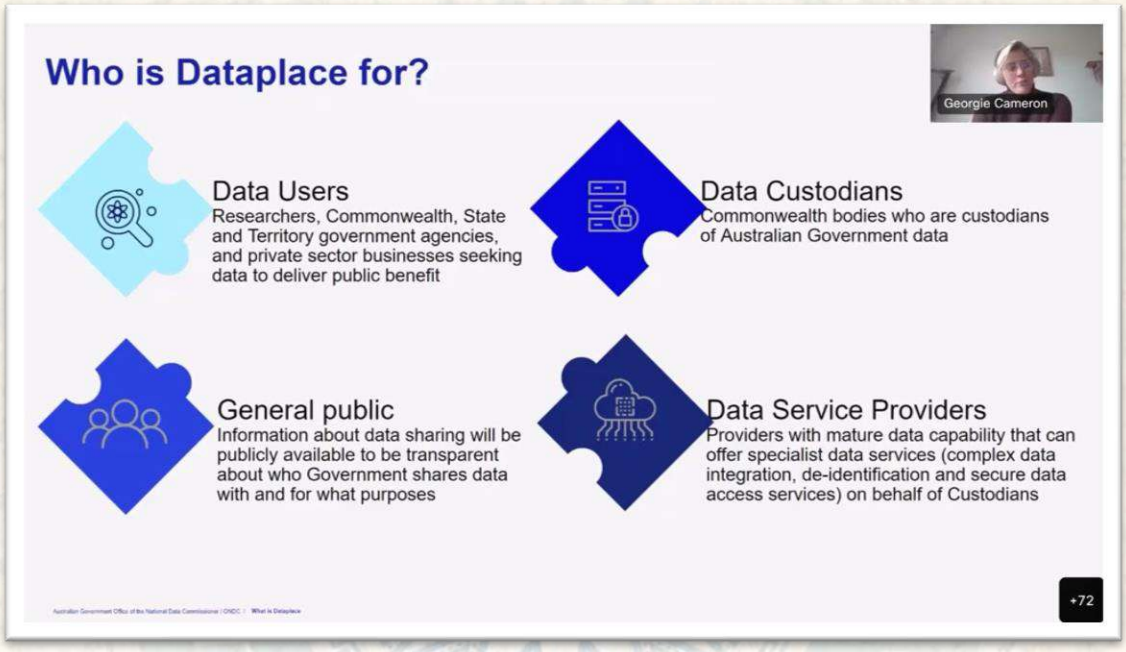
Lược đồ DATA hoạt động theo cách: Người dùng được công nhận có thể yêu cầu dữ liệu của Chính phủ Úc từ người giám sát dữ liệu. Nhà cung cấp dịch vụ dữ liệu được công nhận có thể được sử dụng dữ liệu để cung cấp dịch vụ dữ liệu để hỗ trợ dự án chia sẻ dữ liệu.

"Dataplace" là nền tảng kỹ thuật số của Chính phủ cho những người tham gia Lược đồ DATA và những người khác để quản lý các yêu cầu dữ liệu, xây dựng thỏa thuận chia sẻ và giám sát các hoạt động chia sẻ dữ liệu của chính mình nên tháng này tập hợp những người muốn truy cập vào dữ liệu của Chính phủ Úc (chẳng hạn như các nhà nghiên cứu, những người làm việc về chính sách công và cung cấp dịch vụ công) với các cơ quan Khối thịnh vượng chung là người giám sát dữ liệu. Nền tảng này cũng được Ủy viên Dữ liệu quốc gia sử dụng để điều chỉnh Lược đồ DATA.

Dataplace giúp các cơ quan cộng tác với nhau dễ dàng hơn trong yêu cầu dữ liệu, đặc biệt là khi có thể có nhiều người giám sát một tập dữ liệu hoặc khi không biết dữ liệu nào có sẵn, tìm ở đâu, ai nắm giữ dữ liệu. Văn phòng Ủy ban Dữ liệu quốc gia đang phát triển *Danh mục dữ liệu của Chính phủ Úc*. Danh mục này sẽ đóng vai trò là điểm trung tâm để tạo điều kiện thuận lợi cho việc khám phá, sử dụng và tái sử dụng dữ liệu do Chính phủ nắm giữ. Danh mục sẽ tăng tính minh bạch của việc nắm giữ dữ liệu do Chính phủ nắm giữ, giảm trùng lặp, cho phép tái sử dụng và chia sẻ dữ liệu nhiều hơn. Danh mục sẽ dựa trên cơ sở dữ liệu của các cơ quan Chính phủ theo kế hoạch của *Chương trình thí điểm kiểm kê dữ liệu (DIPP)* cũng như các nguồn dữ liệu mở và các nguồn dữ liệu khác để giúp người dùng tìm thấy dữ liệu của Chính phủ Úc. Một thách thức chính đối với người quản lý dữ liệu là cung cấp dữ liệu với tiện ích tối đa cho người dùng nhưng vẫn duy trì tính bảo mật của thông tin.

"Khung năm Yếu tố an toàn (Five Safes Framework)" là một tập các nguyên tắc cung cấp cách tiếp cận đa chiều để quản lý rủi ro tiết lộ thông tin. Mỗi yếu tố an toàn đề cập đến một khía cạnh độc lập nhưng có liên quan đến rủi ro bị tiết lộ. Khung đặt ra các câu hỏi cụ thể để giúp đánh giá và mô tả

từng khía cạnh rủi ro (hoặc an toàn) một cách định tính. Điều này cho phép người quản lý dữ liệu đặt các biện pháp kiểm soát thích hợp, không chỉ trên chính dữ liệu mà còn về cách thức truy cập dữ liệu. Khung này được thiết kế để tạo điều kiện phát hành dữ liệu an toàn và ngăn chặn được chia sẻ dữ liệu quá mức được cho phép.



Dataplace của Chính phủ Úc - Ảnh: Internet

Các yếu tố an toàn được đánh giá độc lập, nhưng cũng được xem xét một cách tổng thể. Chúng có thể được coi là một loạt các đòn bẩy hoặc kiểm soát có thể điều chỉnh để quản lý rủi ro hiệu quả và tối đa hóa tính hữu ích của việc phát hành dữ liệu. Mức độ mà mỗi yếu tố an toàn được kiểm soát là rất quan trọng để đánh giá rủi ro tiết lộ. Khung này đã được ABS, một cơ quan Chính phủ Úc khác cũng như các tổ chức thống kê quốc gia như Văn phòng Thống kê quốc gia (Anh) và Thống kê New Zealand áp dụng.

1.2.12. Các quốc gia Đông Nam Á (ASEAN)

Trong khu vực Đông Nam Á, các quốc gia ASEAN đang ngày càng nhận thức rõ tầm quan trọng của việc xây dựng một khuôn khổ pháp luật dữ

liệu mạnh mẽ, không chỉ để bảo vệ quyền riêng tư cá nhân mà còn nhằm tạo nền tảng cho sự phát triển kinh tế số, thúc đẩy đổi mới sáng tạo và tăng cường hợp tác khu vực. Dù trình độ phát triển và mức độ hoàn thiện của chính sách dữ liệu còn khác nhau, nhưng điểm chung nổi bật là xu hướng hội nhập với các chuẩn mực quốc tế, đồng thời phản ánh những đặc thù chính trị - kinh tế - văn hóa riêng của từng nước.

- Singapore



Luật bảo vệ dữ liệu cá nhân (PDPA) của Singapore - Ảnh: PCPD

Singapore là hình mẫu tiên phong trong khu vực với ***Luật bảo vệ dữ liệu cá nhân (PDPA)*** được ban hành vào ngày 15/10/2012 và liên tục được cập nhật để theo kịp thực tiễn công nghệ, gần nhất là Đạo luật sửa đổi Luật bảo vệ dữ liệu cá nhân năm 2020. PDPA được xây dựng với mục tiêu kép: một mặt, bảo vệ quyền riêng tư của cá nhân, mặt khác cho phép các tổ chức thu thập, sử dụng hoặc chuyển giao dữ liệu cá nhân cho những mục đích hợp pháp và hợp lý, qua đó cân bằng giữa lợi ích cá nhân và nhu cầu hoạt động của doanh nghiệp. Bên cạnh đó, Đạo luật này nhấn mạnh tầm quan trọng của

việc ngăn chặn sự lạm dụng dữ liệu, duy trì niềm tin của cá nhân vào các tổ chức kiểm soát thông tin của họ, đồng thời góp phần củng cố vị thế của Singapore như một trung tâm dữ liệu và tài chính tin cậy trong khu vực và trên thế giới.

Về phạm vi điều chỉnh, PDPA bao trùm mọi "dữ liệu cá nhân" - được định nghĩa là *"dữ liệu về một cá nhân có thể nhận dạng được, bất kể dưới dạng điện tử hay phi điện tử"*[151]. Tuy nhiên, PDPA loại trừ một số trường hợp nhất định. Cụ thể, PDPA không áp dụng đối với: ***(i)*** cá nhân tự xử lý dữ liệu cho mục đích cá nhân hoặc gia đình; ***(ii)*** dữ liệu được cá nhân xử lý với tư cách là nhân viên của một tổ chức; ***(iii)*** các cơ quan nhà nước khi thu thập, sử dụng, tiết lộ dữ liệu phục vụ chức năng công; ***(iv)*** thông tin liên hệ công vụ[152]. Ngoài ra, Đạo luật này có hiệu lực ngoài lãnh thổ, nghĩa là nó áp dụng cho các tổ chức thu thập, sử dụng hoặc chuyển giao dữ liệu cá nhân tại Singapore, bất kể tổ chức đó có trụ sở thực tế hay được đăng ký là một công ty tại Singapore hay không.

Về cơ quan thực thi, Chính phủ Singapore đã thành lập Ủy ban Bảo vệ dữ liệu cá nhân (PDPC) là Cơ quan chuyên trách độc lập có quyền điều tra, ra quyết định xử phạt, hướng dẫn doanh nghiệp tuân thủ các quy định và thúc đẩy chuyển đổi số an toàn. PDPC trực thuộc Bộ Thông tin và Truyền thông Singapore và nằm trong cơ cấu của Cơ quan Phát triển Truyền thông (IMDA). Với sứ mệnh đề ra, PDPC đóng vai trò cơ quan đầu mối về bảo vệ dữ liệu, đại diện chính phủ Singapore trong các vấn đề quốc tế liên quan,

---

[151] ICLG (2025), *Data protection laws and regulations 2025: Singapore*. International Comparative Legal Guides. https://iclg.com/practice-areas/data-protection-laws-and-regulations/singapore, Truy cập ngày 01/8/2025

[152] PDPC (2023), *PDPA Overview*, https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act#:~:text=The%20PDPA%C2%A0recognises%20both%20the%20need,for%20legitimate%20and% %20purposes, Truy cập ngày 01/8/2025.

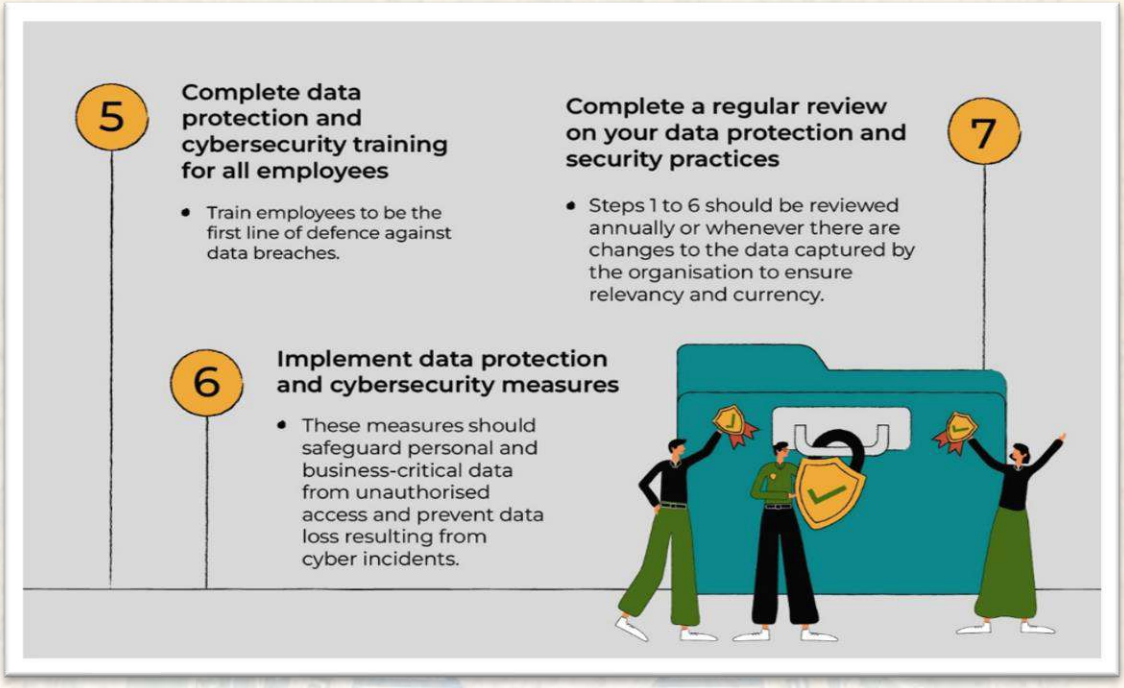
đồng thời đảm bảo thực thi hiệu quả PDPA nhằm thúc đẩy môi trường tin cậy giữa doanh nghiệp và người tiêu dùng.



Logo Cơ quan Phát triển Truyền thông Singapore - Ảnh: AsiaOne

Chức năng của PDPC bao gồm xây dựng chính sách, hướng dẫn thực hiện các quy định liên quan đến bảo vệ dữ liệu cá nhân để hỗ trợ các tổ chức tuân thủ hiệu quả PDPA. PDPC còn ban hành các Hướng dẫn tư vấn giải thích chi tiết các khái niệm và nghĩa vụ trong PDPA, cũng như tổ chức các chương trình đào tạo, nâng cao nhận thức cho doanh nghiệp và cộng đồng. Trên phương diện tố tụng, PDPC có quyền thanh tra, điều tra các vụ việc vi phạm; đưa ra quyết định hoặc mệnh lệnh buộc tổ chức vi phạm phải khắc phục hoặc tuân thủ đúng luật; phối hợp với các cơ quan quản lý chuyên ngành khác để giám sát việc bảo vệ dữ liệu trong các lĩnh vực đã có quy định riêng. PDPC cũng quản lý hệ thống *Danh sách không nhận cuộc gọi* - danh sách cho phép người dân đăng ký số điện thoại để không bị nhận tin nhắn, cuộc gọi tiếp thị không mong muốn và xử lý các vi phạm liên quan. Nhìn

chung, PDPC là *hạt nhân* đảm bảo PDPA được thực thi nghiêm ngặt, đồng thời thúc đẩy văn hóa bảo vệ dữ liệu trong xã hội Singapore.



Chương trình thiết yếu về bảo vệ dữ liệu Singapore - Ảnh: IMDA

Không chỉ vậy, theo PDPC, mỗi tổ chức bắt buộc phải chỉ định một hoặc nhiều DPO (Cán bộ bảo vệ dữ liệu) chịu trách nhiệm đảm bảo tổ chức tuân thủ Đạo luật. Một tổ chức có thể chỉ định một người hoặc một nhóm người làm DPO. Sau khi được chỉ định, DPO có thể ủy quyền một số trách nhiệm nhất định, bao gồm cho những người không phải là nhân viên của tổ chức. Thông tin liên hệ kinh doanh của DPO phải được công khai. Việc không chỉ định DPO có thể dẫn đến một cuộc điều tra sơ bộ của PDPC. Nếu một tổ chức hoặc cá nhân không hợp tác, điều này sẽ cấu thành một hành vi vi phạm pháp luật. Theo đó, một cá nhân có thể bị phạt tới 10.000 SGD hoặc phạt tù không quá 12 tháng, hoặc cả hai. Một tổ chức có thể bị phạt tới 100.000 SGD[153].

[153] DLA Piper (2025), *Data Protection Laws of the World: Singapore*. DLA Piper. https://dlapiperdataprotection.com, Truy cập ngày 01/8/2025

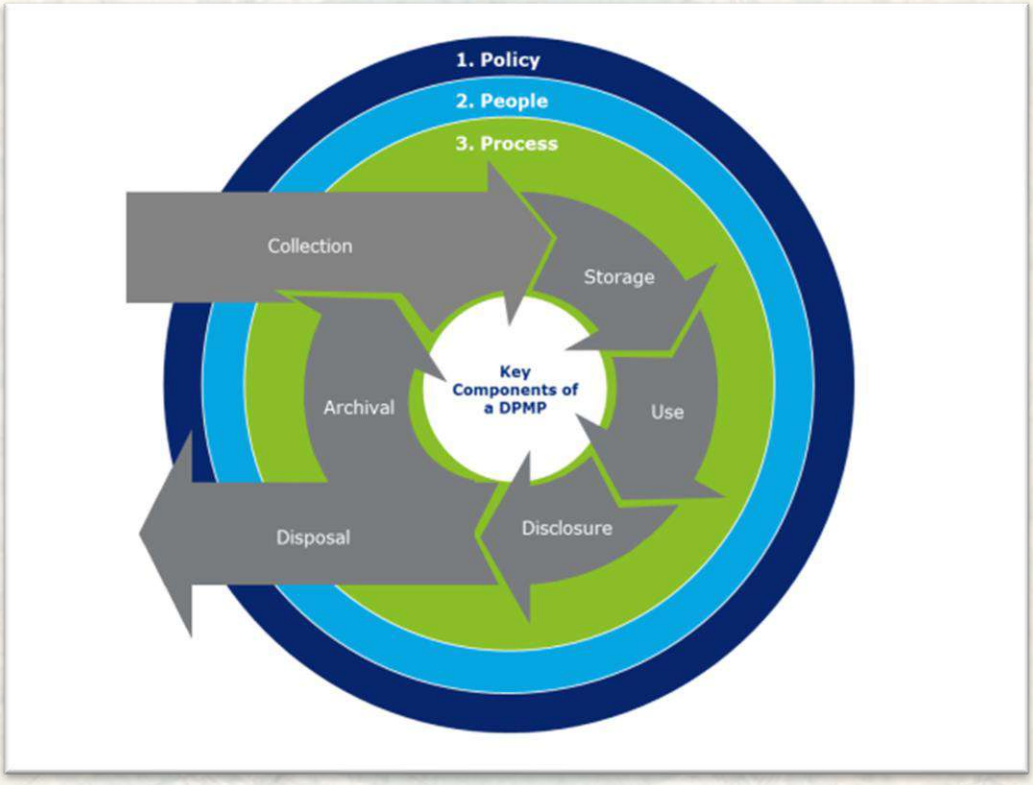


Tòa nhà quốc hội Singapore - Ảnh: Trade Brains

Về định nghĩa, PDPA Singapore không có định nghĩa về dữ liệu cá nhân nhạy cảm trong Đạo luật. Tuy nhiên, các hướng dẫn không ràng buộc từ PDPC cho thấy tính nhạy cảm của dữ liệu là một yếu tố cần xem xét khi thực hiện các chính sách và thủ tục để đảm bảo mức độ bảo mật phù hợp cho dữ liệu cá nhân. Ngoài ra, các hướng dẫn này cũng quy định rằng, trong tính toán các khoản phạt tài chính cho các vi phạm Đạo luật, PDPC sẽ xem xét liệu tổ chức đang kinh doanh xử lý khối lượng lớn dữ liệu cá nhân nhạy cảm, mà việc tiết lộ có thể gây ra thiệt hại, tổn thương hoặc khó khăn đặc biệt cho một cá nhân (như dữ liệu y tế hoặc tài chính), nhưng lại không thiết lập các biện pháp bảo vệ đầy đủ tương xứng với thiệt hại có thể gây ra..

Các nghĩa vụ bảo vệ dữ liệu theo PDPA không áp dụng cho khu vực công, khu vực này phải tuân thủ các quy tắc riêng theo Hướng dẫn của Chính phủ 8 ("IM8") và Đạo luật khu vực công. Theo hướng dẫn của PDPC, có *11*

nghĩa vụ chính bao quát toàn bộ vòng đời dữ liệu, từ lúc thu thập đến sử dụng, lưu trữ, chia sẻ và hủy dữ liệu, bao gồm: "Trách nhiệm giải trình; Nghĩa vụ thông báo; Nghĩa vụ xin sự đồng ý; Giới hạn mục đích; Đảm bảo độ chính xác; Bảo mật dữ liệu; Giới hạn lưu giữ; Giới hạn chuyển giao; Tiếp cận và chỉnh sửa dữ liệu; Thông báo vi phạm dữ liệu; Chuyển đổi dữ liệu"[154]. Quy định cụ thể về các nghĩa vụ này khá tương đồng với các nghĩa vụ bảo vệ dữ liệu của GDPR.



Minh họa về một DPMP (Chính sách, Con người, Quy trình), với Vòng đời Dữ liệu (Từ Thu thập đến Lưu trữ/Xử lý) trong PDPC - Ảnh: pdpc.gov.sg

Một điểm cần lưu ý rằng các nghĩa vụ trên không tuyệt đối trong mọi trường hợp, PDPA vẫn có quy định một số ngoại lệ cụ thể. Chẳng hạn, một số tình huống thu thập, sử dụng dữ liệu không cần xin đồng ý nếu rơi vào

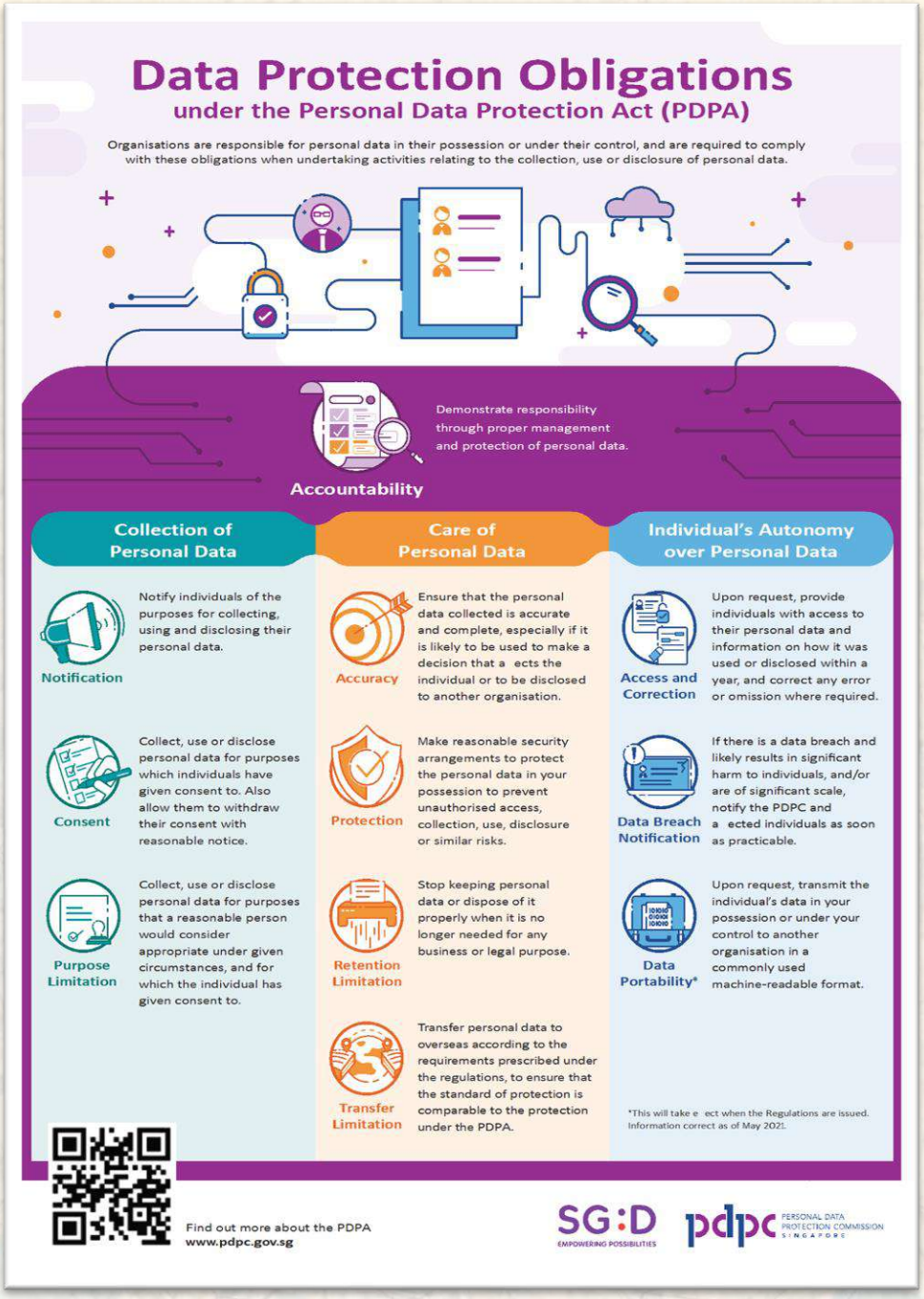
[154] SPW (2023), The EU's GDPR vs Singapore's PDPA. SPW. https://spwcircular.com/blog/the-eus-gdpr-vs-singapores-pdpa/. Truy cập ngày 01/8/2025

trường hợp ngoại lệ cho phép (ví dụ: để xử lý trong tình huống khẩn cấp đe dọa tính mạng, phục vụ điều tra tội phạm, vì lợi ích công cộng, cho lợi ích chính đáng của doanh nghiệp… được quy định trong luật)[155]. Tuy nhiên, nguyên tắc chung là mọi hoạt động xử lý dữ liệu đều phải đáp ứng tiêu chuẩn "hợp lý" - tức là điều mà một người bình thường nhìn nhận là phù hợp, cần thiết trong hoàn cảnh nhất định. Triết lý "hợp lý và trách nhiệm" chi phối PDPA, đảm bảo rằng dù có ngoại lệ, các tổ chức vẫn phải cân nhắc cẩn trọng và chịu trách nhiệm giải trình cho mỗi quyết định xử lý dữ liệu của mình.

Một điểm đáng chú ý khác là PDPA Singapore không áp dụng cho thông tin liên hệ kinh doanh nếu thông tin đó chỉ được cung cấp cho mục đích kinh doanh. Tuy nhiên, Đạo luật vẫn điều chỉnh thông tin liên hệ kinh doanh được các cá nhân cung cấp chỉ với tư cách cá nhân của họ. Khi mục đích cung cấp thông tin liên hệ kinh doanh là hỗn hợp (tức là cho cả mục đích kinh doanh và cá nhân), trường hợp này không nằm trong phạm vi điều chỉnh của Đạo luật.

Về quyền của chủ thể dữ liệu, PDPA xác lập một số quyền nhất định cho chủ thể dữ liệu nhằm đảm bảo họ có thể kiểm soát thông tin cá nhân của mình. Mặc dù các quyền theo PDPA có phần hạn chế hơn so với các chế độ bảo vệ dữ liệu nghiêm ngặt như GDPR của EU, chúng đóng vai trò quan trọng trong việc bảo đảm sự công bằng và minh bạch.

[155] Pang, C. K., Ng, J. J., & Koh, B. J. M (2022*), Consent and Personal Data: Charting the Differences between the PDPA and GDPR*. SMU Lexicon, https://smulexicon.com/2022/02/06/consent-and-personal-data-charting-the-differences-between-the-pdpa-and-gdpr/, truy cập ngày 01/8/2025.



Inforgraphic về PDPA và PDPC của Chính phủ Singapore - Ảnh: PDPC

Các quyền chính về dữ liệu theo pháp luật Singapore bao gồm: "Quyền được thông tin; Quyền tiếp cận dữ liệu; Quyền đính chính dữ liệu; Quyền rút lại sự đồng ý; Quyền hạn chế nhận quảng cáo; Quyền chuyển giao dữ liệu". Bên cạnh những quyền trên, điểm khác biệt đáng lưu ý là PDPA không trao cho cá nhân một số quyền mở rộng như trong GDPR. Không có quyền yêu

cầu xóa dữ liệu cá nhân ("quyền được lãng quên") trong PDPA - tổ chức không bắt buộc phải xóa dữ liệu trừ phi chính họ thấy không còn cần thiết hoặc cá nhân rút lại sự đồng ý[156]. Cũng không có quyền riêng yêu cầu hạn chế hoặc phản đối việc xử lý dữ liệu cho các mục đích cụ thể (ngoài việc rút lại sự đồng ý như đã nêu. Pháp luật Singapore cũng chưa đề cập đến quyền phản đối quyết định tự động (automated decision-making) hay yêu cầu được giải thích thuật toán; cá nhân nếu không muốn bị quyết định hoàn toàn tự động (ví dụ bởi AI) thì biện pháp chính vẫn là rút lại sự đồng ý hoặc không cung cấp dữ liệu cho mục đích đó. Ngoài ra, PDPA không phân loại "dữ liệu nhạy cảm" thành một hạng mục đặc biệt với chế độ bảo vệ cao hơn (như cách GDPR quy định dữ liệu về sức khỏe, sinh trắc học, tư tưởng... là nhạy cảm cần điều kiện xử lý chặt chẽ hơn). Tất cả dữ liệu cá nhân dưới PDPA về nguyên tắc đều được đối xử như nhau. Mặc dù vậy, trên thực tế PDPC có lưu ý rằng các loại dữ liệu như tài chính, y tế, thông tin trẻ em... có mức độ nhạy cảm cao, do đó tổ chức nên áp dụng biện pháp bảo vệ tăng cường và cơ quan quản lý có thể xem xét yếu tố này như tình tiết tăng nặng khi xử phạt vi phạm

Đối với quy định về chuyển giao dữ liệu xuyên biên giới, theo Điều 26 PDPA, một tổ chức không được chuyển bất kỳ dữ liệu cá nhân nào ra ngoài lãnh thổ Singapore trừ khi đáp ứng các yêu cầu được pháp luật hoặc quy định đề ra nhằm đảm bảo bên nhận ở nước ngoài cung cấp mức độ bảo vệ tương đương với PDPA[157]. Nói cách khác, trước khi chuyển dữ liệu cho một công ty hoặc máy chủ đặt tại nước khác, tổ chức Singapore phải đánh

[156] ICLG (2025), *Data protection laws and regulations 2025: Singapore,* International Comparative Legal Guides, https://iclg.com/practice-areas/data-protection-laws-and-regulations/singapore, Truy cập ngày 01/8/2025.
[157] ICLG (2025), *Data protection laws and regulations 2025: Singapore,* International Comparative Legal Guides. https://iclg.com/practice-areas/data-protection-laws-and-regulations/singapore, Truy cập ngày 01/8/2025.

giá và đảm bảo rằng dữ liệu đó sẽ tiếp tục được bảo vệ không kém tiêu chuẩn nội địa.



Thỏa thuận bảo vệ dữ liệu là cách thức mà các doanh nghiệp Singapore sử dụng để thực hiện các nghĩa vụ đối với chuyển giao dữ liệu xuyên biên giới - Ảnh: Privacy Ninja

Trên thực tế, để tuân thủ nghĩa vụ này, các doanh nghiệp thường sử dụng những biện pháp như: ký kết thỏa thuận bảo vệ dữ liệu với bên nhận (Data Transfer Agreement) lồng ghép các điều khoản bảo mật yêu cầu bên nhận tuân thủ chuẩn PDPA; áp dụng các điều khoản hợp đồng mẫu do PDPC gợi ý; hoặc chuyển dữ liệu cho các tổ chức đã đạt được chứng nhận bảo vệ dữ liệu tin cậy. PDPA hiện không duy trì một danh sách sẵn các "quốc gia đáp ứng tiêu chuẩn tương đương". Thay vào đó, trách nhiệm chứng minh thuộc về tổ chức chuyển dữ liệu, phải chủ động đánh giá và ràng buộc bên nhận tuân thủ các biện pháp bảo vệ cần thiết. PDPC có thẩm quyền đưa ra

miễn trừ cho yêu cầu này trong một số trường hợp, nhưng nhìn chung nguyên tắc "bảo vệ tương đương" luôn được áp dụng.

Quy định chặt chẽ về chuyển dữ liệu qua biên giới của Singapore nhằm ngăn chặn hiện tượng "di cư dữ liệu" đến các nước có luật lỏng lẻo để trục lợi. Điều này cũng góp phần xây dựng lòng tin của người dân và đối tác quốc tế, rằng dữ liệu cá nhân tại Singapore sẽ không bị tuồn ra nước ngoài và sử dụng một cách vô tội vạ. Tóm lại, dù dữ liệu "xuất khẩu" sang đâu, chiếc "áo giáp" PDPA vẫn phải đồng hành cùng nó, đảm bảo quyền riêng tư được bảo vệ xuyên biên giới.

Về trách nhiệm pháp lý và chế tài xử phạt, hệ thống thực thi và chế tài của PDPA được thiết kế nhằm đảm bảo tuân thủ nghiêm túc từ phía các tổ chức, đồng thời tạo sự răn đe cần thiết. Cơ quan PDPC được trao quyền hạn rộng rãi để giám sát và xử lý vi phạm. Cụ thể, PDPC có thể tiến hành điều tra khi nhận được khiếu nại hoặc có dấu hiệu vi phạm; yêu cầu tổ chức cung cấp thông tin, tài liệu phục vụ điều tra. Nếu phát hiện vi phạm PDPA, PDPC có thể ban hành các mệnh lệnh hành chính buộc tổ chức phải chấn chỉnh hành vi. Ví dụ, PDPC có thể yêu cầu một công ty ngưng thu thập hoặc xóa bỏ dữ liệu đã thu thập không đúng quy định, cải thiện biện pháp bảo mật, hoặc dừng chuyển dữ liệu ra nước ngoài nếu không đảm bảo an toàn. Đặc biệt, PDPC có quyền áp dụng chế tài tài chính (hình phạt tiền) đối với các vi phạm nghiêm trọng. Theo luật gốc trước đây, mức phạt tối đa mà PDPC có thể áp dụng cho mỗi vi phạm là 1 triệu đô la Singapore (SGD). Tuy nhiên, sau sửa đổi năm 2020, trần phạt tiền đã được tăng lên đáng kể nhằm tạo sức răn đe cao hơn. Cụ thể, kể từ ngày 1/10/2022, PDPC có quyền phạt tới 10% doanh thu hàng năm tại Singapore của tổ chức vi phạm (đối với các tổ chức có doanh thu nội địa trên 10 triệu SGD), hoặc 1 triệu SGD, lấy

mức nào cao hơn[158]. Như vậy, với các doanh nghiệp lớn, mức phạt có thể vượt mốc 1 triệu và tỷ lệ thuận với quy mô tài chính của họ. Việc nâng trần xử phạt này đặt PDPA tiệm cận hơn với các khung pháp lý quốc tế. Đây là động thái khẳng định cam kết của Singapore trong việc tăng cường hiệu lực thực thi, khiến việc vi phạm dữ liệu trở thành rủi ro tài chính - pháp lý lớn cho các tổ chức.

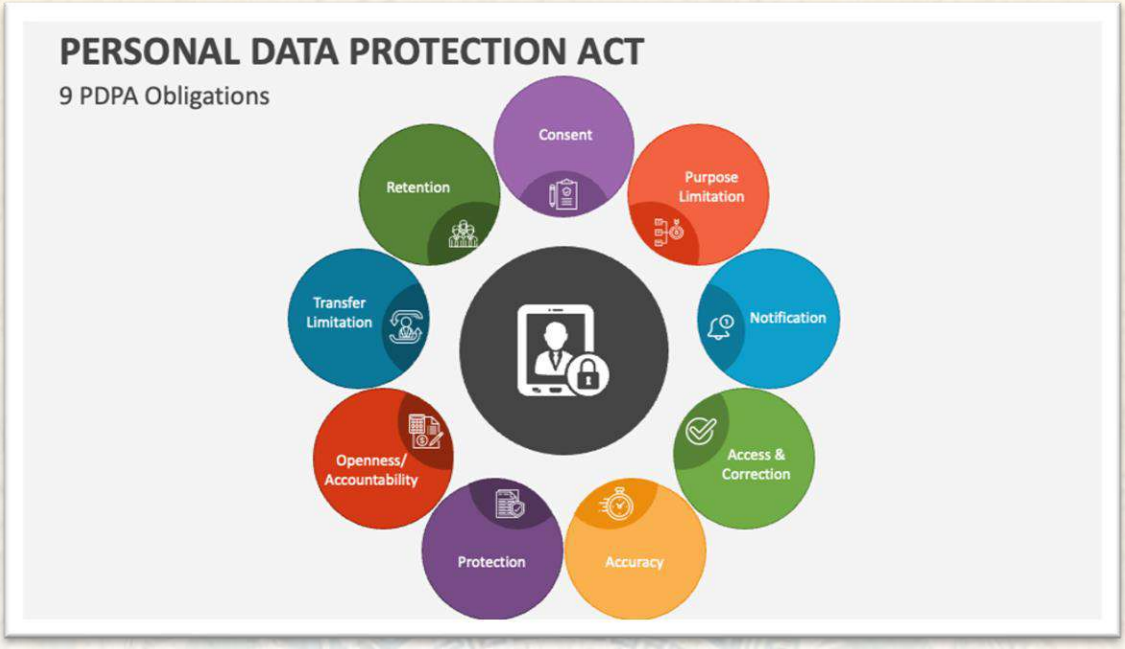
Song song với chế tài hành chính, PDPA còn mở ra cơ chế khiếu kiện dân sự cho cá nhân. Theo PDPA (mục 48O, sửa đổi 2020), bất kỳ người nào chịu tổn thất hoặc thiệt hại do một hành vi vi phạm PDPA của tổ chức đều có quyền khởi kiện đòi bồi thường trước tòa án[159]. Đáng chú ý, Tòa án cấp cao Singapore đã diễn giải rằng "tổn thất" bao gồm cả thiệt hại về tinh thần, tâm lý, chứ không chỉ thiệt hại vật chất hữu hình[160]. Điều này có nghĩa là nếu một cá nhân bị căng thẳng, lo lắng do dữ liệu riêng tư của mình bị lộ hoặc sử dụng sai, họ có thể yêu cầu tòa buộc tổ chức vi phạm bồi thường cho sự đau khổ về tinh thần đó. Cơ chế quyền tư pháp này bổ sung cho vai trò của PDPC, tạo thêm một tầng bảo vệ lợi ích cho cá nhân và áp lực trách nhiệm cho tổ chức. Bên cạnh đó, các quyết định của PDPC cũng có thể được kháng nghị lên Ủy ban Phúc thẩm về Bảo vệ Dữ liệu Cá nhân, và sau đó có thể đưa ra Tòa án để xem xét tư pháp, đảm bảo tính khách quan và đúng pháp luật trong quá trình thực thi.

---

[158] Báo Đại biểu Nhân dân (2022), *Khung pháp lý bảo vệ dữ liệu cá nhân*. Báo Đại biểu Nhân dân. https://daibieunhandan.vn/khung-phap-ly-bao-ve-du-lieu-ca-nhan-10294680.html, Truy cập ngày 01/8/2025.

[159] Osborne Clarke (2023), *Private right of action under Singapore's Personal Data Protection Act,* Osborne Clarke, https://www.osborneclarke.com/insights/private-right-action-under-singapores-personal-data-protection-act, Truy cập ngày 01/8/2025.

[160] Dentons Rodyk (2022), *In cases of PDPA breaches, individuals can now claim for emotional distress against organisations,* Dentons Rodyk, https://dentons.rodyk.com/en/insights/alerts/2022/october/4/in-cases-of-pdpa-breaches-individuals-can-now-claim-for-emotional-distress-against-organisations, Truy cập ngày 01/8/2025.



09 Nghĩa vụ theo PDPA - Ảnh: Collidu

Ngoài các vi phạm hành chính, PDPA còn quy định một số hành vi phạm tội hình sự. Thí dụ: cố ý tiếp thị tới số điện thoại trong danh sách DNC; tiết lộ dữ liệu cá nhân của người khác một cách trái phép, gian dối hoặc gây tổn hại; hoặc cản trở điều tra của PDPC (như hủy chứng cứ, cung cấp thông tin sai lệch) đều có thể bị truy cứu trách nhiệm hình sự. Các trường hợp này có thể dẫn đến phạt tiền hình sự, thậm chí phạt tù, tùy mức độ nghiêm trọng và quy định cụ thể trong luật.

Hiệu lực của khung thực thi PDPA được minh chứng qua nhiều vụ việc thực tế. Một trường hợp tiêu biểu là sự cố rò rỉ dữ liệu y tế của hệ thống bệnh viện SingHealth năm 2018 - vụ vi phạm dữ liệu lớn nhất lịch sử Singapore, ảnh hưởng thông tin của khoảng 1,5 triệu bệnh nhân. Trong vụ việc này, PDPC đã điều tra kỹ lưỡng và quyết định phạt hai đơn vị liên quan là Cơ quan Hệ thống Thông tin Y tế Tích hợp (IHiS) 750.000 SGD và Tập đoàn Y tế SingHealth 250.000 SGD, tổng cộng 1 triệu SGD (mức phạt kịch trần theo luật cũ). Quyết định này không chỉ trừng phạt thích đáng đơn vị vi phạm mà

còn phát đi thông điệp mạnh mẽ về trách nhiệm bảo mật thông tin y tế. Bên cạnh đó, PDPC cũng tích cực xử lý nhiều vụ vi phạm khác: chỉ riêng năm 2019, cơ quan này đã điều tra 185 trường hợp liên quan đến vi phạm dữ liệu và ban hành 58 quyết định xử lý; trong đó 39 tổ chức bị áp dụng phạt tiền với tổng số tiền phạt lên tới 1,7 triệu SGD[161].

Về ưu điểm, nhìn chung, khung pháp luật bảo vệ dữ liệu cá nhân của Singapore (PDPA) được đánh giá là một hệ thống tiên tiến và cân bằng, phản ánh sự dung hòa giữa nhu cầu phát triển kinh tế số và việc bảo vệ quyền riêng tư cá nhân. PDPA thể hiện rõ triết lý cân bằng lợi ích, ngay từ mục tiêu đề ra, luật đã nhấn mạnh việc bảo vệ dữ liệu cá nhân phải song hành với việc đáp ứng các mục đích sử dụng hợp lý của tổ chức, điều này giúp Singapore duy trì được môi trường pháp lý thân thiện với đổi mới và kinh doanh hơn so với những mô hình quá thiên về bảo hộ một chiều. Thực tế, PDPA thường được nhìn nhận khá linh hoạt hơn GDPR nhờ tập trung vào các nguyên tắc chung và trách nhiệm giải trình thay vì những thủ tục cứng nhắc, phức tạp[162]. Điều này giúp giảm gánh nặng tuân thủ cho doanh nghiệp vừa và nhỏ, tạo lợi thế cạnh tranh cho Singapore trong thu hút đầu tư và phát triển kinh tế số, đồng thời vẫn đảm bảo mức độ bảo vệ cơ bản cho người dùng.

Các sửa đổi PDPA năm 2020 đã khiến khung pháp luật Singapore tiệm cận hơn với thông lệ quốc tế, cho thấy nỗ lực cập nhật không ngừng của chính phủ Singapore. Chẳng hạn, việc bổ sung nghĩa vụ thông báo vi phạm dữ liệu bắt buộc và quyền chuyển dữ liệu đã đưa Singapore ngang hàng với

---

[161] Bộ Khoa học và Công nghệ (2020), *Singapore sửa luật bảo vệ dữ liệu, cho phép đáp ứng nghiên cứu, kinh doanh số,* Bộ Khoa học và Công nghệ, https://most.gov.vn/singapore-sua-luat-bao-ve-du-lieu-cho-phep-dap-ung-nghien-cuu-kinh-doanh-so-197145422.htm, Truy cập ngày 01/8/2025.

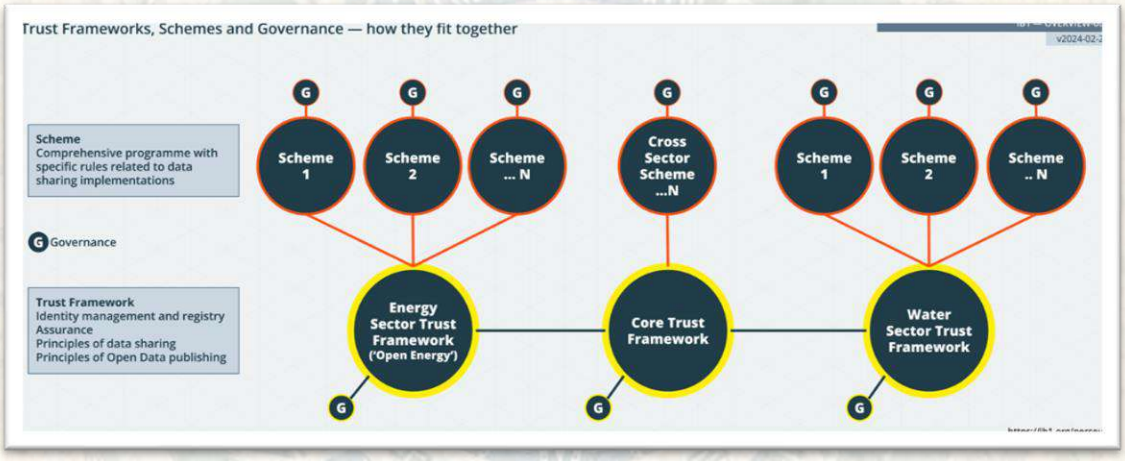
[162] Personal Data Protection Commission Singapore (2020), *Navigating the Road Ahead,* Personal Data Protection Commission Singapore, https://www.pdpc.gov.sg/-/media/Files/PDPC/DPO-Connect/November-20/Navigating-the-Road-Ahead.html, Truy cập ngày 01/8/2025.

xu hướng toàn cầu về tăng cường trách nhiệm giải trình của tổ chức và trao thêm quyền cho cá nhân. Cùng với đó, PDPA mới cũng giới thiệu các căn cứ pháp lý thay thế cho sự đồng ý như lợi ích hợp pháp của doanh nghiệp hoặc mục đích cải tiến sản phẩm/dịch vụ tương tự cách GDPR có các cơ sở xử lý khác ngoài sự đồng ý. Điều này cho phép doanh nghiệp tại Singapore chủ động trong việc xử lý dữ liệu phục vụ đổi mới, nghiên cứu mà không cần xin sự đồng ý cho mọi trường hợp, miễn là đáp ứng các điều kiện an toàn nhất định. Chẳng hạn, một công ty có thể phân tích dữ liệu khách hàng sẵn có để cải tiến dịch vụ hoặc phục vụ nghiên cứu R&D (nghiên cứu phát triển) mà không phải xin lại từng cá nhân, với điều kiện phải đánh giá rủi ro và đảm bảo việc sử dụng đó là hợp lý, có lợi ích vượt trội so với tác động bất lợi tới người dùng. Những điều chỉnh này vừa tạo dư địa cho đổi mới sáng tạo, vừa duy trì các biện pháp bảo vệ, cho thấy Singapore đã học hỏi từ kinh nghiệm quốc tế để hoàn thiện luật. Hơn nữa, việc nâng khung phạt tiền lên đến 10% doanh thu chứng tỏ Singapore sẵn sàng đi cùng xu thế quốc tế về chế tài răn đe mạnh đối với vi phạm dữ liệu. Tất cả những yếu tố trên cho thấy PDPA là một khung pháp luật năng động, có khả năng thích ứng; Singapore đã và đang tích cực điều chỉnh luật cho "hợp thời đại" trong nền kinh tế số.

Bên cạnh các ưu điểm, so với một số chuẩn mực quốc tế hàng đầu, PDPA cũng có *những hạn chế nhất định*. ***Thứ nhất,*** quyền của chủ thể dữ liệu trong PDPA còn hạn chế hơn đáng kể so với GDPR. Như đã phân tích, người dùng Singapore không có quyền yêu cầu xóa bỏ dữ liệu cá nhân của mình trong tay doanh nghiệp, cũng như không có quyền hạn chế hay phản đối việc xử lý dữ liệu vì lý do cá nhân đặc biệt nào; quyền phản đối trực tiếp duy nhất chính là rút lại sự đồng ý. Hệ quả là mức độ kiểm soát của cá

nhân đối với dữ liệu của họ dưới PDPA còn yếu hơn, khó đảm bảo các nguyên tắc như "quyền được lãng quên" hay "tính di động của dữ liệu" mà thông lệ quốc tế rất coi trọng. ***Thứ hai,*** PDPA thiếu vắng khái niệm và cơ chế bảo vệ đặc thù cho dữ liệu nhạy cảm. Không có danh mục các loại thông tin nhạy cảm được luật định kèm theo yêu cầu chặt chẽ hơn khi xử lý, trong khi đó, GDPR và nhiều quốc gia khác có quy định riêng cho dữ liệu nhạy cảm. Việc này có thể khiến một số loại dữ liệu dễ bị tổn hại do không được "ưu tiên" bảo vệ về mặt pháp lý. Mặc dù PDPC có hướng dẫn nội bộ khuyến nghị doanh nghiệp cẩn trọng hơn với dữ liệu nhạy cảm nhưng tính ràng buộc pháp lý không cao gây ảnh hưởng đến mức độ tin cậy quốc tế. ***Thứ ba,*** mô hình dựa nhiều vào sự đồng ý của PDPA tuy phù hợp với văn hóa Á Châu do đề cao đồng thuận, nhưng trong bối cảnh dữ liệu lớn và trí tuệ nhân tạo, việc yêu cầu nhiều sự đồng ý cho mọi trường hợp sử dụng dữ liệu có thể trở nên hình thức hóa và kém hiệu quả. Nhận ra điều đó, Singapore đã bổ sung các ngoại lệ mới cho yêu cầu đồng ý (như "lợi ích chính đáng" và "cải tiến kinh doanh" trong đạo luật sửa đổi 2020). Tuy nhiên, mặt trái là các ngoại lệ này nếu không được định nghĩa và hướng dẫn rõ ràng có thể bị doanh nghiệp lạm dụng để mở rộng mục đích xử lý ngoài tầm mục đích hợp pháp. Một số ý kiến lo ngại rằng phạm vi các ngoại lệ này khá rộng và mơ hồ. Dù PDPC đã yêu cầu đi kèm các biện pháp bảo vệ như bắt buộc doanh nghiệp đánh giá rủi ro và lợi ích trước khi viện dẫn ngoại lệ, cũng như cá nhân vẫn có quyền "*opt - out*" (chọn không tham gia) ngay cả sau khi bị đưa vào ngoại lệ. ***Thứ tư,*** xét về mức độ quốc tế hóa, PDPA hiện chưa được EU công nhận đạt mức độ bảo vệ tương đương (tức Singapore chưa nằm trong danh sách các nước được EU trao quyết định "công nhận tương đương"). Điều này có nghĩa là các doanh nghiệp

Singapore hợp tác với thị trường EU vẫn phải áp dụng thêm các biện pháp đáp ứng GDPR khi xử lý dữ liệu công dân EU, làm tăng các chi phí tuân thủ. So với một số quốc gia tiên tiến khác (như Nhật Bản, Hàn Quốc) đã đạt thoả thuận công nhận tương đương với EU, Singapore có phần chậm hơn trong cuộc đua này, một phần do PDPA chưa đáp ứng đầy đủ các tiêu chí nghiêm ngặt của GDPR như đã nêu trên. Tuy nhiên, Singapore cũng đang tích cực tham gia các diễn đàn, khuôn khổ khu vực như APEC CBPR, và việc PDPC đại diện chính phủ trong các vấn đề bảo vệ dữ liệu quốc tế cho thấy nỗ lực hòa nhập thông lệ chung.



Khung đánh giá tin cậy dữ liệu - Ảnh: Icebreaker One

Có thể thấy rằng trong pháp luật về dữ liệu tại Singapore, các quyền của cá nhân được bảo vệ chặt chẽ, trong khi doanh nghiệp được khuyến khích sử dụng dữ liệu theo cách có trách nhiệm thông qua các sáng kiến như khung đánh giá tin cậy dữ liệu (Data Trust Framework). Ngoài ra, Singapore cũng đi đầu trong việc phát triển chính sách quản trị dữ liệu xuyên biên giới, tạo điều kiện cho nền kinh tế số khu vực phát triển thông suốt và hài hòa, tương lai có thể trở thành "trạm trung chuyển dữ liệu" trong khu vực ASEAN. Với các cải cách gần đây, Singapore tiếp tục củng cố vị trí của mình như một quốc gia coi trọng bảo vệ dữ liệu, song hành cùng mục tiêu trở thành trung

tâm dữ liệu và sáng tạo của thế giới. Các nhà nghiên cứu và hoạch định chính sách có thể xem PDPA như một minh chứng cho cách tiếp cận kết hợp giữa mô hình châu Âu và châu Á - đề cao trách nhiệm giải trình và sự đồng thuận xã hội, qua đó rút ra những bài học phù hợp cho việc xây dựng luật bảo vệ dữ liệu tại quốc gia mình.

- Malaysia

Ở Malaysia, đạo luật đầu tiên về dữ liệu được ban hành là ***Luật Bảo vệ dữ liệu cá nhân (PDPA 2010)***, đã được Quốc hội Malaysia thông qua vào ngày 02/6/2010 và có hiệu lực từ ngày 15/11/2013 - Đây là một trong những đạo luật đầu tiên tại khu vực nhằm điều chỉnh việc xử lý thông tin cá nhân trong lĩnh vực thương mại. Trong tiến trình xây dựng, bổ sung và hoàn thiện chính sách, pháp luật về dữ liệu, đối với PDPA, Ủy viên bảo vệ dữ liệu cá nhân thuộc Bộ Truyền thông và Đa phương tiện Malaysia đã ban hành *"Văn bản tham vấn công chúng số 01/2020"* - Rà soát Đạo luật bảo vệ dữ liệu cá nhân 2010 (PC01/2020) đề ngày 14/02/2020 nhằm lấy ý kiến và bình luận của công chúng về 22 vấn đề được nêu trong PC01/2020. Qua quá trình rà soát ý kiến, Cục bảo vệ dữ liệu cá nhân (PDP Department) cho biết, trong số 22 vấn đề, có 5 vấn đề đã được đưa vào danh sách rút gọn làm các sửa đổi chủ chốt đề xuất đối với PDPA[163]. Các sửa đổi đối với PDPA, tức đạo luật bảo vệ dữ liệu cá nhân (sửa đổi) năm 2024 (gọi là "Đạo luật sửa đổi"), lần đầu được trình dưới dạng dự luật tại Nghị viện Malaysia vào tháng 7/2024 và sau đó lần lượt được Dewan Rakyat (Hạ viện) và Dewan Negara (Thượng viện) thông qua vào các ngày 16 và 31/7/2024. Dự luật này đã được Hoàng gia phê chuẩn và được đăng Công

[163] Hall Booth Smith (2024), *Malaysia's 2024 data privacy reform,* Hall Booth Smith, https://hallboothsmith.com/malaysia-2024-data-privacy-reform/, Truy cập ngày 01/8/2025.

báo thành luật vào ngày 17/10/2024 nhằm hiện đại hóa khuôn khổ pháp lý, đưa luật dữ liệu Malaysia tiệm cận hơn với các chuẩn mực quốc tế như GDPR và các nước ASEAN khác[164].



Malaysia là một trong những nước đầu tiên tại khu vực ASEAN ban hành khung pháp lý cho dữ liệu - Ảnh: Chooi & Company

Ngày 19/12/2024, Bộ trưởng Kỹ thuật số đã ấn định ba mốc thời điểm mà các điều khoản của Đạo luật Sửa đổi sẽ có hiệu lực. Theo đó, các điều khoản không đặt ra nghĩa vụ mới đối với người sử dụng dữ liệu/người kiểm soát dữ liệu (tức các Điều 7, 11, 13 và 14 của Đạo luật Sửa đổi) đã có hiệu lực từ ngày 01/01/2025; các điều khoản đưa ra các yêu cầu mới như bổ nhiệm cán bộ bảo vệ dữ liệu (DPO), thông báo vi phạm dữ liệu và quyền di

[164] International Association of Privacy Professionals (IAPP) (2024), *Malaysia's PDPA Amendments: Delivering Enhanced Data Governance and Transparency*. International Association of Privacy Professionals (IAPP), https://iapp.org/news/a/malaysia-s-pdpa-amendments-delivering-enhanced-data-governance-and-transparency/, Truy cập ngày 01/8/2025.

chuyển dữ liệu (tức các Điều 6 và 9 của Đạo luật Sửa đổi) sẽ có hiệu lực từ ngày 01/06/2025. Các sửa đổi còn lại theo Đạo luật Sửa đổi sẽ có hiệu lực từ ngày 01/4/2025. Bên cạnh đó, Bộ trưởng Kỹ thuật số, ông Gobind Singh Deo, công bố kế hoạch ban hành và/hoặc xây dựng bảy (07) bộ hướng dẫn theo PDPA, gồm: ***(i)*** Hướng dẫn Thông báo Vi phạm Dữ liệu; ***(ii)*** Hướng dẫn Cán bộ Bảo vệ Dữ liệu; ***(iii)*** Hướng dẫn Di chuyển Dữ liệu; ***(iv)*** Hướng dẫn Chuyển giao Dữ liệu Xuyên biên giới; ***(v)*** Hướng dẫn Đánh giá Tác động Bảo vệ Dữ liệu; ***(vi)*** Hướng dẫn Quyền riêng tư theo Thiết kế; và ***(vii)*** Hướng dẫn Ra quyết định Tự động[165].

Về phạm vi áp dụng, PDPA áp dụng đối với mọi cá nhân và tổ chức xử lý dữ liệu cá nhân cho mục đích thương mại tại Malaysia. Luật bảo vệ bất kỳ thông tin nào về cá nhân còn sống có thể được xác định danh tính (dù trực tiếp hay gián tiếp) trong bối cảnh giao dịch thương mại. Điều này bao gồm cả dữ liệu được xử lý bằng phương thức tự động hoặc phi tự động. Thông tin cá nhân được bảo vệ có thể là tên, địa chỉ, số định danh, thông tin sức khỏe, email, hình ảnh, video, hồ sơ cá nhân... miễn là có thể xác định một cá nhân từ những dữ liệu đó[166]. Tuy nhiên, dữ liệu cá nhân do cá nhân xử lý cho mục đích cá nhân, gia đình hoặc sinh hoạt riêng không nằm trong phạm vi điều chỉnh của PDPA. Về không gian lãnh thổ, PDPA chủ yếu điều chỉnh các thực thể có hiện diện tại Malaysia. Tuy nhiên, luật có hiệu lực ngoài lãnh thổ hạn chế: nếu một tổ chức đặt tại nước ngoài nhưng sử dụng thiết bị tại Malaysia để xử lý dữ liệu cá nhân (ví dụ sử dụng máy chủ đặt tại Malaysia), tổ chức đó cũng phải tuân thủ PDPA. Ngược lại, dữ liệu chỉ truyền qua Malaysia (transit) thì không thuộc phạm vi luật.

---

[165] DLA Piper (2025), *DLA Piper Global Data Protection Laws of the World - Malaysia,* https://www.dlapiperdataprotection.com/index.html?t=law&c=MY, Truy cập ngày 01/8/2025.

[166] Linklaters (2024), *Data Protected – Malaysia,* Linklaters, https://www.linklaters.com/en-us/insights/data-protected/data-protected---malaysia, Truy cập ngày 01/8/2025.

Về nghĩa vụ đối với các bên liên quan, Luật PDPA đặt ra các nghĩa vụ pháp lý nghiêm ngặt đối với các tổ chức, cá nhân được coi là "bên kiểm soát dữ liệu" (trong PDPA 2010 dùng thuật ngữ data user, nay sửa đổi 2024 thống nhất dùng data controller)[167]. Bên kiểm soát dữ liệu là đơn vị quyết định mục đích và phương thức xử lý dữ liệu cá nhân, có trách nhiệm tuân thủ mọi quy định của PDPA. Từ 2024, một số nghĩa vụ cũng mở rộng trực tiếp đến bên xử lý dữ liệu (data processor - đơn vị xử lý dữ liệu thay mặt cho bên kiểm soát). Cụ thể, nền tảng của PDPA 2010 là *07 Nguyên tắc Bảo vệ Dữ liệu Cá nhân,* bao gồm: Nguyên tắc chung; Nguyên tắc thông báo và lựa chọn; Nguyên tắc chuyển giao; Nguyên tắc bảo mật; Nguyên tắc lưu trữ; Nguyên tắc toàn vẹn dữ liệu và Nguyên tắc truy cập. Về mặt nội dung, các nguyên tắc này khá giống GDPR và PDPA Singapore, tuy nhiên, PDPA yêu cầu một số biện pháp tuân thủ bổ sung, chẳng hạn: đăng ký dữ liệu đối với một số ngành nghề nhất định phải đăng ký như một "data user" chính thức với Ủy viên PDPC; hợp đồng với bên xử lý - bên kiểm soát phải đảm bảo hợp đồng với bên xử lý dữ liệu có điều khoản bảo vệ dữ liệu phù hợp; ác tổ chức cần lưu trữ hồ sơ về hoạt động xử lý, đặc biệt là hồ sơ các trường hợp chuyển dữ liệu ra nước ngoài, vi phạm dữ liệu và biện pháp khắc phục. Gần đây, Malaysia cũng xây dựng hướng dẫn về đánh giá tác động bảo vệ dữ liệu và bảo vệ dữ liệu theo thiết kế để khuyến khích tổ chức chủ động tuân thủ ngay từ giai đoạn triển khai hệ thống. Những hướng dẫn này không bắt buộc theo luật nhưng thể hiện thông lệ tốt phù hợp với xu hướng quốc tế.

---

[167] Amita Haylock & Justin Lai (2025), *From legislative reform to practical guidance: key amendments to Malaysia's PDPA and the launch of cross-border transfer guidelines,* Mayer Brown, https://www.mayerbrown.com/en/insights/publications/2025/07/from-legislative-reform-to-practical-guidance-key-amendments-to-malaysias-pdpa-and-the-launch-of-cross-border-transfer-guidelines, Truy cập ngày 01/8/2025.

Không chỉ vậy, PDPA Malaysia quy định khá cụ thể về nghĩa vụ đảm bảo an ninh và thông báo vi phạm. Thật vậy, ngoài việc duy trì biện pháp bảo mật phòng ngừa, PDPA (sửa đổi 2024) bổ sung nghĩa vụ thông báo sự cố vi phạm dữ liệu cá nhân. Cụ thể, nếu xảy ra vi phạm dữ liệu (mất mát, rò rỉ, truy cập trái phép vào dữ liệu cá nhân), bên kiểm soát phải thông báo cho Ủy viên Bảo vệ Dữ liệu trong vòng 72 giờ kể từ khi phát hiện sự cố hoặc sớm nhất có thể[168]. Đồng thời, nếu vi phạm có khả năng gây tổn hại đáng kể cho chủ thể dữ liệu, bên kiểm soát còn phải thông báo cho các cá nhân bị ảnh hưởng một cách kịp thời, không trì hoãn bất hợp lý. Quy định thông báo vi phạm này giúp Malaysia đồng bộ với chuẩn mực GDPR về ứng phó sự cố bảo mật. Để hỗ trợ tuân thủ, cơ quan PDPC Malaysia đã ban hành Hướng dẫn về thông báo vi phạm nêu rõ quy trình, biểu mẫu báo cáo và ngưỡng đánh giá ảnh hưởng để xác định trường hợp phải thông báo.



Logo Cục bảo vệ dữ liệu cá nhân - Ảnh: pdp.gov.my

[168] Personal Data Protection Commissioner Malaysia (2010), *Personal Data Protection Act 2010,* Personal Data Protection Commissioner Malaysia, https://www.pdp.gov.my/ppdpv1/en/akta/pdp-act-2010-en/, Truy cập ngày 01/8/2025.

Đồng thời, PDPA Malaysia bắt buộc mỗi tổ chức phải chỉ định nhân sự phụ trách bảo vệ dữ liệu cá nhân (DPO) để thực thi các quy định của đạo luật. DPO có nhiệm vụ giám sát việc tuân thủ PDPA trong tổ chức, thúc đẩy văn hóa bảo vệ dữ liệu và làm đầu mối làm việc với cơ quan quản lý. Mọi quy mô doanh nghiệp đều phải có DPO - từ tập đoàn đa quốc gia đến doanh nghiệp nhỏ tại Malaysia đều không được miễn trừ. Việc bổ nhiệm DPO phải được thông báo lên Văn phòng Ủy viên Bảo vệ Dữ liệu (PDPC) và tiêu chuẩn năng lực và trách nhiệm cụ thể của DPO được hướng dẫn chi tiết trong các tài liệu do PDPC ban hành. Đặc biệt, PDPC sẽ được cố vấn bởi một Ủy ban cố vấn bảo vệ dữ liệu cá nhân do Bộ trưởng bổ nhiệm. Ủy ban này bao gồm một chủ tịch, 03 thành viên từ khu vực công, và ít nhất 07, nhưng không quá 11 thành viên khác. Nhiệm kỳ của các thành viên trong Ủy ban không vượt quá 03 năm, tuy nhiên, họ có thể được bổ nhiệm cho hai nhiệm kỳ liên tiếp.



Mối quan hệ của nhân sự phụ trách bảo vệ dữ liệu cá nhân - Ảnh: Cloud9 Data Solutions

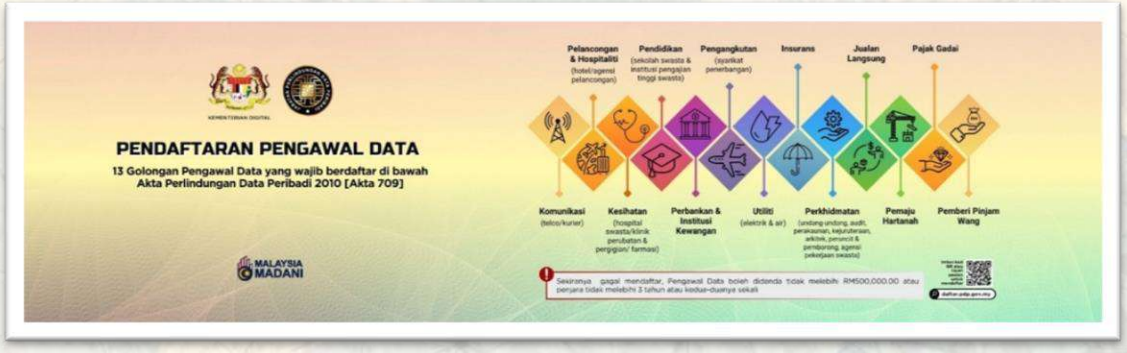
Về các quyền đối với dữ liệu, tương tự như PDPA Singapore, PDPA Malaysia trao cho chủ thể dữ liệu (cá nhân mà dữ liệu đó liên quan) các quyền nhất định nhằm đảm bảo họ có thể kiểm soát và bảo vệ thông tin cá nhân của mình. Bên cạnh các quyền cơ bản giống với quy định tại Singapore, sửa đổi PDPA 2024 bổ sung quyền về tính di động dữ. Theo đó, chủ thể dữ liệu có quyền yêu cầu bên kiểm soát chuyển trực tiếp dữ liệu cá nhân của mình cho một bên kiểm soát khác theo định dạng dữ liệu phổ biến, nếu điều này khả thi về mặt kỹ thuật. Đây là một điểm tương đồng với GDPR (vốn có quyền dữ liệu di động), thể hiện bước tiến mới của Malaysia trong việc trao thêm quyền kiểm soát dữ liệu cho cá nhân.

Về quy định chuyển giao dữ liệu xuyên biên giới, việc chuyển dữ liệu cá nhân ra ngoài Malaysia được PDPA kiểm soát nhằm đảm bảo dữ liệu tiếp tục được bảo vệ khi được chuyển đi. Theo Luật gốc 2010, việc chuyển dữ liệu xuyên biên giới chỉ được phép đến những nước nằm trong ***"danh sách trắng"*** do Bộ trưởng phê duyệt (các nước có luật bảo vệ dữ liệu tương đương Malaysia) hoặc trong các tình huống ngoại lệ vì lợi ích công cộng. Tuy nhiên, danh sách trắng này trên thực tế chưa từng được ban hành đầy đủ, gây khó khăn cho hoạt động chuyển dữ liệu quốc tế của doanh nghiệp. Nhận thấy hạn chế đó, sửa đổi 2024 đã bãi bỏ chế độ danh sách trắng cứng nhắc, thay thế bằng cơ chế mềm dẻo hơn, kết hợp đánh giá rủi ro và điều kiện bảo đảm thích hợp.

Về điều kiện chuyển dữ liệu xuyên biên giới, PDPA (theo hướng dẫn mới) còn yêu cầu các nghĩa vụ chung khi chuyển dữ liệu, đó là: thông báo cho chủ thể dữ liệu về việc dữ liệu của họ sẽ được chuyển ra nước ngoài (nêu rõ quốc gia đích và mục đích); đảm bảo hợp đồng với bên nhận có điều khoản bảo vệ dữ liệu phù hợp; sử dụng phương tiện truyền chuyển an toàn; và lưu hồ sơ mỗi lần chuyển (gồm bên nhận, quốc gia, loại dữ liệu, mục đích và căn

cứ pháp lý áp dụng như TIA, consent, hợp đồng…). Việc tăng cường kiểm soát chuyển dữ liệu xuyên biên giới này cho thấy Malaysia quyết tâm đáp ứng các chuẩn mực bảo mật quốc tế, tạo dựng niềm tin cho người dùng trong nước và nâng cao uy tín để thúc đẩy hợp tác dữ liệu với các quốc gia khác.

Cơ quan chịu trách nhiệm thực thi PDPA là Văn phòng Ủy viên Bảo vệ Dữ liệu Cá nhân Malaysia (Personal Data Protection Commissioner - PDPC), thuộc Bộ Truyền thông và Kỹ thuật số Malaysia. Ủy viên PDPC có thẩm quyền giám sát, thanh tra việc tuân thủ PDPA của các tổ chức, tiếp nhận và giải quyết khiếu nại của công dân, cũng như tiến hành điều tra và xử lý vi phạm. Lần sửa đổi 2024 đã tăng cường quyền hạn cho PDPC, cho phép cơ quan này chủ động tiến hành các cuộc kiểm toán định kỳ tại tổ chức để kiểm tra việc tuân thủ luật. PDPC cũng ban hành nhiều hướng dẫn, tiêu chuẩn để hỗ trợ doanh nghiệp tuân thủ và có thể đưa ra khuyến nghị chính sách về bảo vệ dữ liệu. Điển hình như các tiêu chuẩn thể hiện yêu cầu tối thiểu của Ủy ban đối với việc xử lý dữ liệu cá nhân, bao gồm: Tiêu chuẩn an ninh cho dữ liệu cá nhân được xử lý bằng phương tiện điện tử; Tiêu chuẩn an ninh cho dữ liệu cá nhân được xử lý bằng phương tiện phi điện tử; Tiêu chuẩn lưu trữ cho dữ liệu cá nhân được xử lý bằng cả hai phương tiện; Tiêu chuẩn toàn vẹn dữ liệu cho dữ liệu cá nhân được xử lý bằng cả hai phương tiện.



Văn phòng Ủy viên Bảo vệ Dữ liệu Cá nhân Malaysia và các quy định nổi bật - Ảnh: Jabatan Perlindungan Data Peribadi

Chế tài xử phạt dưới PDPA mang tính hình sự và hành chính. Vi phạm các quy định quan trọng của PDPA được xác định là tội hình sự, xử lý thông qua truy tố hoặc phạt tiền do cơ quan có thẩm quyền áp dụng. Sửa đổi 2024 đã tăng nặng mức phạt để nâng cao tính răn đe: mức phạt tiền tối đa tăng từ 300.000 MYR lên 1.000.000 MYR (tương đương khoảng 236.000 USD) và mức phạt tù tối đa tăng từ 2 năm lên 3 năm tù giam[169]. Những mức phạt này áp dụng cho các vi phạm nghiêm trọng, chẳng hạn vi phạm các nguyên tắc bảo vệ dữ liệu, xử lý dữ liệu nhạy cảm trái phép, không tuân thủ lệnh của Ủy viên, hoặc tiếp tục xử lý sau khi chủ thể đã rút sự đồng ý. Trên thực tế, PDPC thường sử dụng cơ chế phạt tiền hành chính đối với các vi phạm ít nghiêm trọng: cơ quan có thể đưa ra đề nghị phạt hành chính và nếu tổ chức vi phạm nộp phạt đúng hạn, có thể tránh truy tố hình sự. Điểm đáng chú ý là PDPA không thiết lập quyền khởi kiện dân sự cho cá nhân bị xâm phạm dữ liệu. Điều này khác với GDPR (cho phép cá nhân kiện đòi bồi thường). Tại Malaysia, việc xử lý hoàn toàn do cơ quan nhà nước tiến hành. Tuy nhiên, cá nhân có thể dựa trên các luật dân sự chung (như luật về xâm phạm quyền riêng tư hoặc hợp đồng) để khởi kiện nếu hội đủ yếu tố, dù PDPA không trao quyền này trực tiếp.

Nhìn chung, hệ thống pháp luật dữ liệu cá nhân của Malaysia hiện nay có nhiều nét tương đồng với các chuẩn mực quốc tế. Tuy nhiên, GDPA của Malaysia hiện chưa áp dụng cho khu vực công và vẫn đang trong quá trình sửa đổi nhằm nâng cao tính tương thích với GDPR của Châu Âu và cập nhật theo thực tiễn công nghệ. Những cải cách này không chỉ giúp bảo vệ quyền

[169] Pavla Jonette (2024), *Malaysia's PDPA amendments: Delivering enhanced data governance and transparency,* IAPP News, https://iapp.org/news/a/malaysia-s-pdpa-amendments-delivering-enhanced-data-governance-and-transparency#:~:text=Mandatory%20breach%20notification,becoming%20aware%20of%20the%20breach, Truy cập ngày 01/8/2025.

riêng tư của người dân Malaysia tốt hơn mà còn tạo thuận lợi cho doanh nghiệp hội nhập, khi luật trở nên tương thích với khung pháp lý toàn cầu.

- Thái lan

Thái Lan có bước tiến quan trọng khi thông qua ***Luật bảo vệ dữ liệu cá nhân (PDPA Thailand)*** vào năm 2019 và chính thức có hiệu lực từ năm 2022. Sau thời gian chuẩn bị kỹ lưỡng, luật này được đánh giá là một bản sao khá gần của GDPR, với đầy đủ các quy định về thu thập, xử lý, lưu trữ, chuyển giao dữ liệu cá nhân và các quyền cơ bản của chủ thể dữ liệu. Thái Lan thiết lập Văn phòng Ủy ban bảo vệ dữ liệu để hướng dẫn và xử lý vi phạm, đây là bước đi quyết liệt của quốc gia này nhằm tăng cường niềm tin số, thu hút đầu tư và nâng cao vị thế trong khu vực. Thái Lan cũng đang xây dựng các quy định chi tiết hơn về dữ liệu nhạy cảm, dữ liệu xuyên biên giới và giám sát AI trong thu thập dữ liệu.



Luật bảo vệ dữ liệu cá nhân Thái Lan - Ảnh: Internet

- Indonesia

Indonesia, quốc gia đông dân nhất khu vực và có tốc độ số hóa bùng nổ, chỉ vừa thông qua ***Luật Bảo vệ Dữ liệu Cá nhân (PDP Law)*** vào năm 2022. Đây là bộ luật đầu tiên điều chỉnh toàn diện việc xử lý dữ liệu cá nhân trong cả lĩnh vực công lẫn tư. Đạo luật này quy định chi tiết trách nhiệm của người kiểm soát và xử lý dữ liệu, yêu cầu sự chấp thuận minh bạch và rõ ràng từ người dùng, đồng thời thiết lập nghĩa vụ báo cáo khi có

vi phạm. Hiện tại, chính phủ Indonesia đang xúc tiến thành lập Ủy ban Bảo vệ Dữ liệu Cá nhân quốc gia, dự kiến sẽ đóng vai trò tương tự như các cơ quan bảo vệ dữ liệu tại châu Âu và Hàn Quốc. Đây được xem là một bước tiến mang tính quyết định, nhằm củng cố lòng tin của công chúng vào hệ sinh thái số, đồng thời kiến tạo một môi trường pháp lý thuận lợi để thu hút đầu tư vào lĩnh vực công nghệ.



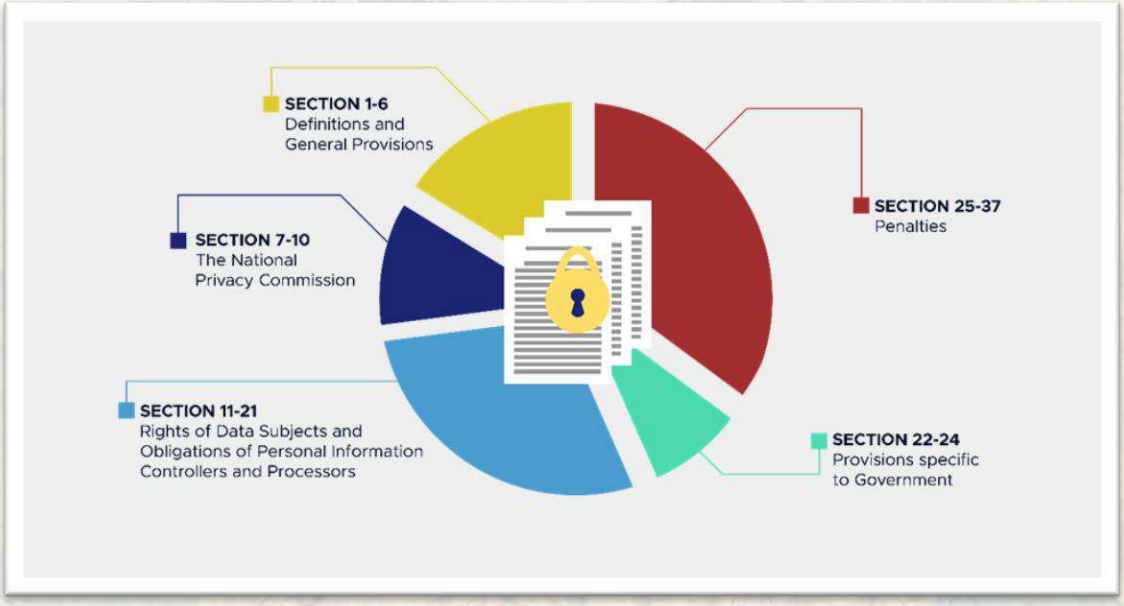
Đạo luật bảo vệ dữ liệu Indoneisa - Ảnh: PT. REFIKA ADITAMA

- Philippines

Philippines là một trong những quốc gia tiên phong ở khu vực Đông Nam Á có luật riêng về dữ liệu - ***Đạo luật quyền riêng tư dữ liệu năm 2012.*** Văn bản pháp lý này thiết lập một khuôn khổ pháp lý vững chắc để bảo vệ

thông tin cá nhân trong kỷ nguyên số. Cơ quan giám sát chính là Ủy ban Bảo vệ dữ liệu quốc gia (NPC), có quyền ban hành các quy định bổ sung, tiến hành điều tra, xử lý các hành vi vi phạm và khuyến khích một văn hóa dữ liệu có trách nhiệm trong cả khu vực doanh nghiệp lẫn chính phủ. Philippines đi đầu trong việc thúc đẩy nhận thức cộng đồng về quyền dữ liệu và xây dựng Bộ quy tắc đạo đức cho việc thu thập, sử dụng dữ liệu của các cơ quan nhà nước và tổ chức tư nhân.

Ở các quốc gia còn lại như Campuchia, Lào, Myanmar và Brunei, khuôn khổ pháp lý về dữ liệu cá nhân đang ở nhiều giai đoạn phát triển khác nhau. Campuchia và Lào đang trong quá trình soạn thảo các dự luật tương tự, trong khi Myanmar chịu tác động lớn từ bất ổn chính trị, khiến tiến trình này diễn ra chậm hơn.



Mô hình luật dữ liệu của Philippines - Ảnh: National Privacy Commission

Về tổng thể, bức tranh chính sách pháp luật dữ liệu ở ASEAN đang chuyển động mạnh mẽ theo hướng đồng bộ, minh bạch và lấy con người làm trung tâm. Mặc dù xuất phát điểm và mức độ hoàn thiện khác nhau, các quốc gia trên đều hướng tới mục tiêu xây dựng niềm tin kỹ thuật số, bảo vệ quyền

công dân trên môi trường không gian mạng, đồng thời khai thác hiệu quả dữ liệu để phát triển kinh tế, đổi mới sáng tạo và nâng cao năng lực quản trị của nhà nước trong kỷ nguyên số.

1.2.13. Một số quốc gia khác

Bên cạnh các quốc gia và khu vực đã phân tích, nhiều quốc gia khác cũng đã ban hành văn bản luật về bảo vệ dữ liệu để thích ứng với sự phát triển của công nghệ thông tin và nền kinh tế số. Các đạo luật này không chỉ giúp bảo vệ quyền lợi của người dân mà còn thúc đẩy sự phát triển của các dịch vụ và ứng dụng sáng tạo dựa trên dữ liệu trong các quốc gia và khu vực, cụ thể như:

- ***Đức:*** Chính sách pháp luật về dữ liệu tại Đức được xây dựng trên hai nền tảng chính: Quy định chung về Bảo vệ Dữ liệu (GDPR) của Liên minh Châu Âu và Luật Bảo vệ Dữ liệu Liên bang (BDSG). Cả hai luật này đều hoạt động song song để tạo ra một khuôn khổ pháp lý chặt chẽ nhằm bảo vệ quyền riêng tư và dữ liệu cá nhân của người dân. Việc thực thi pháp luật về dữ liệu tại Đức được giám sát bởi một hệ thống các cơ quan, bao gồm Ủy viên Liên bang về Bảo vệ Dữ liệu và Tự do Thông tin (BfDI) và các cơ quan giám sát cấp bang. Các cơ quan này chịu trách nhiệm điều tra các khiếu nại, áp dụng các biện pháp trừng phạt, và đảm bảo các tổ chức tuân thủ cả GDPR và BDSG.

- ***Canada:*** Personal Information Protection and Electronic Documents Act - ***Đạo luật Bảo vệ Thông tin Cá nhân và Tài liệu Điện tử (PIPEDA)*** được coi là một trong những đạo luật quan trọng trong việc bảo vệ quyền riêng tư và dữ liệu cá nhân. PIPEDA áp dụng cho các tổ chức kinh doanh trong khu vực tư nhân, yêu cầu các tổ chức phải thu thập, sử dụng và tiết lộ thông tin cá nhân một cách hợp pháp, minh bạch và có sự đồng thuận của chủ thể dữ liệu. Các cá nhân có quyền truy cập và yêu

cầu chỉnh sửa thông tin cá nhân của mình, đồng thời các tổ chức cần phải thực hiện các biện pháp bảo mật phù hợp để bảo vệ thông tin khỏi bị truy cập trái phép hoặc lạm dụng. PIPEDA cũng yêu cầu các tổ chức phải thông báo cho người dùng khi có sự cố bảo mật nghiêm trọng ảnh hưởng đến dữ liệu cá nhân của họ[170].

- Brazil: Brazil ban hành ***Lei Geral de Proteção de Dados (LGPD)*** vào năm 2020, được thiết kế để bảo vệ quyền riêng tư và dữ liệu cá nhân của người dân. LGPD được xem như là một phiên bản tương tự của Quy định chung về bảo vệ dữ liệu (GDPR) của Liên minh Châu Âu. LGPD yêu cầu các tổ chức phải có sự đồng thuận rõ ràng từ người dùng trước khi thu thập hoặc xử lý dữ liệu cá nhân. Hơn nữa, người dùng có quyền truy cập vào dữ liệu của mình, yêu cầu chỉnh sửa hoặc xóa dữ liệu khi không còn cần thiết. LGPD cũng yêu cầu các tổ chức phải chỉ định một người chịu trách nhiệm bảo vệ dữ liệu và công bố chính sách bảo mật thông tin rõ ràng với công chúng[171].

- Chile: Chính sách bảo vệ dữ liệu tại Chile được điều chỉnh bởi ***Đạo luật Bảo vệ Cuộc sống Cá nhân*** (Ley de Protección de la Vida Privada - Law 19.496), có hiệu lực từ năm 1999. Đạo luật này yêu cầu các tổ chức phải bảo vệ thông tin cá nhân của công dân và chỉ được thu thập và sử dụng dữ liệu khi có sự đồng thuận từ chủ thể dữ liệu. Các cá nhân có quyền yêu cầu truy cập, sửa đổi hoặc xóa dữ liệu của mình. Chính phủ Chile cũng đã thực hiện các bước để cải thiện khả năng tuân thủ các nguyên tắc bảo mật, trong đó có việc thành lập Cơ quan Bảo vệ Dữ liệu Cá nhân vào năm 2004[172].

---

[170] Cavoukian, A (2012), *PIPEDA: Protecting Personal Information in a Digital Age,* Toronto: Ontario Publishing.

[171] Mendonça, R (2020), *The Brazilian Data Protection Act: LGPD and Implications,* Rio de Janeiro: Legal Insights.

[172] López, M., & Salazar, F (2018), *The Chilean Data Protection Act: Policy and Legal Considerations,* Santiago: Chilean Government.

- Mexico: Mexico đã ban hành ***Đạo luật Bảo vệ Dữ liệu Cá nhân trong Tay Các Tổ chức Tư nhân*** (Ley Federal de Protección de Datos Personales en Posesión de los Particulares - LFPDPPP) vào năm 2010. Đạo luật này yêu cầu các tổ chức tư nhân phải bảo vệ dữ liệu cá nhân của khách hàng và chỉ được thu thập thông tin khi có sự đồng thuận của chủ thể dữ liệu. Các cá nhân có quyền yêu cầu truy cập, sửa đổi hoặc xóa dữ liệu cá nhân của mình, đồng thời các tổ chức phải thông báo cho người dùng về các mục đích và phương thức thu thập thông tin. LFPDPPP cũng đặt ra các yêu cầu nghiêm ngặt đối với việc chia sẻ và chuyển nhượng dữ liệu cá nhân giữa các tổ chức, đặc biệt trong các trường hợp vượt qua biên giới quốc gia[173].

- Nigeria: Nigeria đã ban hành ***Quy định Bảo vệ Dữ liệu Nigeria*** (Nigeria Data Protection Regulation - VDPR) vào năm 2019, nhằm mục đích bảo vệ thông tin cá nhân của người dân. VDPR yêu cầu các tổ chức phải thu thập và xử lý dữ liệu cá nhân một cách minh bạch, hợp pháp và có sự đồng thuận của chủ thể dữ liệu. Các cá nhân có quyền yêu cầu truy cập, sửa đổi hoặc xóa dữ liệu của mình. VDPR cũng yêu cầu các tổ chức phải thực hiện các biện pháp bảo vệ dữ liệu nhằm ngăn ngừa việc sử dụng sai mục đích hoặc truy cập trái phép vào thông tin cá nhâ[174].

- South Africa: Cộng hòa Nam Phi đã ban hành ***Đạo luật Bảo vệ Thông tin Cá nhân*** - Protection of Personal Infomation Act (POPIA) vào năm 2020, với mục tiêu bảo vệ quyền riêng tư của công dân trong bối cảnh sự phát triển mạnh mẽ của công nghệ thông tin và truyền thông. POPIA yêu cầu các tổ chức phải thu thập và xử lý dữ liệu cá nhân một cách hợp pháp và bảo mật.

---

[173] Sánchez, R (2019), *Mexico's Federal Data Protection Law: Key Legal Aspects,* Mexico City: Legal Institute Press.

[174] Nigerian Data Protection Bureau (2019), *Nigeria Data Protection Regulation (VDPR)*, Lagos: Nigerian Data Bureau.

Các tổ chức phải đảm bảo rằng dữ liệu cá nhân chỉ được sử dụng cho mục đích đã được xác định trước và có sự đồng thuận của người dùng. POPIA cũng quy định rõ quyền của các cá nhân trong việc yêu cầu truy cập, sửa đổi hoặc xóa dữ liệu cá nhân của mình[175].

- Israel: Israel có ***Đạo luật Bảo vệ Quyền riêng tư*** (Protection of Privacy Law), yêu cầu các tổ chức phải thực hiện các biện pháp bảo vệ dữ liệu cá nhân của công dân. Đạo luật này quy định các tổ chức phải đảm bảo rằng việc thu thập và xử lý dữ liệu cá nhân chỉ được thực hiện khi có sự đồng thuận của người dùng và cho mục đích hợp pháp. Các cá nhân có quyền yêu cầu truy cập và chỉnh sửa thông tin của mình, đồng thời các tổ chức phải bảo mật thông tin cá nhân để ngăn ngừa các vi phạm bảo mậ[176].

- Argentina: Argentina đã ban hành ***Đạo luật Bảo vệ Dữ liệu Cá nhân*** (Ley de Protección de Datos Personales) vào năm 2000 và sửa đổi vào các năm sau đó. Đạo luật yêu cầu các tổ chức phải tuân thủ các nguyên tắc bảo vệ dữ liệu cá nhân, bao gồm sự đồng thuận của chủ thể dữ liệu, quyền truy cập và sửa đổi thông tin cá nhân, và bảo mật thông tin. Argentina cũng cam kết tuân thủ các quy định quốc tế về bảo vệ dữ liệu, đặc biệt là trong mối quan hệ với các quốc gia trong Liên minh Châu Âu[177].

- United Kingdom (Vương quốc Anh): Sau khi Vương quốc Anh rời Liên minh Châu Âu, ***Đạo luật Bảo vệ Dữ liệu 2018*** (DPA 2018) đã được ban hành, tuân thủ các nguyên tắc của GDPR. DPA 2018 quy định rõ quyền của các cá nhân đối với dữ liệu của họ, bao gồm quyền truy cập, sửa đổi và xóa dữ liệu cá nhân. Các tổ chức phải thực hiện các biện pháp bảo vệ dữ liệu,

---

[175] Schreuder, H (2020), *The POPIA and Its Impact on Data Protection in South Africa,* Cape Town: South African Press.

[176] Ben-Shahar, O (2020), *Israel's Privacy Protection: Legal and Regulatory Approaches,* Tel Aviv University Press.

[177] Figueroa, E (2018), *Argentina's Personal Data Protection Law: A Legal Overview,* Buenos Aires: Legal Press.

đồng thời thông báo cho người dùng về cách thức và mục đích thu thập dữ liệu cá nhân[178].

- New Zealand: Privacy Act 2020 - New Zealand ban hành ***Đạo luật Bảo vệ Quyền riêng tư 2020***, yêu cầu các tổ chức phải thông báo cho người dân khi thu thập, sử dụng hoặc bảo vệ dữ liệu cá nhân. Đạo luật này cung cấp quyền cho các cá nhân yêu cầu truy cập và chỉnh sửa thông tin cá nhân của mình, đồng thời yêu cầu các tổ chức phải bảo vệ dữ liệu cá nhân để ngăn ngừa vi phạm bảo mật[179].

- United Arab Emirates (UAE): Federal Decree-Law No. 45/2021 on Personal Data Protection - ***Đạo luật bảo vệ dữ liệu cá nhân***, nhằm bảo vệ quyền riêng tư của công dân và cư dân tại UAE. Đạo luật này yêu cầu các tổ chức phải thực hiện các biện pháp bảo vệ dữ liệu và chỉ thu thập dữ liệu khi có sự đồng thuận của người dân. UAE cũng yêu cầu các tổ chức phải thông báo cho người dân về các mục đích và phương thức thu thập dữ liệu cá nhân[180].

1.2.14. So sánh các mô hình chính sách pháp luật về dữ liệu và bài học kinh nghiệm cho Việt Nam

1.2.14.1. Điểm tương đồng trong chính sách, pháp luật về dữ liệu của các quốc gia

Mỗi quốc gia đều có những điều kiện chính trị, kinh tế, văn hóa, xã hội riêng biệt, tuy nhiên trong quá trình xây dựng chính sách, pháp luật về dữ liệu, các quốc gia đã thể hiện một số điểm tương đồng rõ rệt. Những điểm chung này phản ánh xu thế hội tụ trong tư duy quản lý dữ liệu của các

---

[178] Hague, D (2020), *The Data Protection Act 2018 and its Impact in the UK,* Oxford University Press.

[179] Privacy Commissioner (2020), *New Zealand Privacy Act 2020: A Detailed Review,* Wellington: New Zealand Government Publishing.

[180] Al-Suwaidi, R (2021), *UAE Federal Decree-Law No. 45/2021 on Personal Data Protection,* Dubai: UAE Government Publishing.

quốc gia, đồng thời góp phần hình thành một hành lang pháp lý thống nhất, nhằm bảo vệ an ninh, an toàn thông tin và quyền riêng tư cá nhân trong kỷ nguyên số.

Thứ nhất, các quốc gia đều xây dựng khung pháp lý cơ bản về bảo vệ dữ liệu cá nhân. Một điểm tương đồng nổi bật giữa các quốc gia là sự chú trọng đến bảo vệ quyền riêng tư đối với dữ liệu cá nhân, điều này vốn được xem là quyền con người cần được bảo vệ trong thời đại số. Mặc dù có nhiều cách tiếp cận khác nhau, nhìn chung các nước đều đưa ra định nghĩa rõ ràng về khái niệm dữ liệu cá nhân và thiết lập các nguyên tắc trong việc xử lý loại dữ liệu này. Liên minh châu Âu với GDPR là một trong những hệ thống pháp lý nghiêm ngặt và toàn diện nhất. Theo đó, các tổ chức phải có căn cứ pháp lý rõ ràng và có biện pháp bảo vệ khi xử lý dữ liệu cá nhân, đồng thời phải minh bạch, đảm bảo tính chính xác và bảo mật. Tương tự, Luật bảo vệ dữ liệu cá nhân của Nhật Bản (APPI), Luật Bảo mật thông tin cá nhân của Hàn Quốc (PIPA) cũng yêu cầu các tổ chức, doanh nghiệp minh bạch trong việc thu thập, sử dụng và cung cấp dữ liệu cá nhân. Tại Hoa Kỳ, một số khu vực cũng luật liên bang thống nhất về dữ liệu cá nhân, như nhiều bang có luật riêng như California với (CCPA và CPRA) cũng đã ban hành các luật nhằm bảo vệ quyền riêng tư tương tự GDPR.

Thứ hai, các quốc gia có sự tương đồng trong việc thiết lập và trao các quyền cho chủ thể dữ liệu. Hầu hết các đạo luật về dữ liệu đều trao quyền cho chủ thể dữ liệu. Những quyền phổ biến là: Quyền được biết; quyền truy cập dữ liệu; quyền yêu cầu sửa đổi hoặc xóa dữ liệu; quyền phản đối xử lý dữ liệu; quyền chuyển giao dữ liệu. Những quyền này được thể hiện rõ trong GDPR, APPI của Nhật Bản, PIPA của Hàn Quốc, và CCPA của California. Mục tiêu của các quy định này là nhằm tăng cường tính minh bạch và sự

kiểm soát của người dân đối với dữ liệu cá nhân của họ, đồng thời tạo ra một môi trường pháp lý công bằng giữa người tiêu dùng và doanh nghiệp. Ngay cả các nước đang phát triển như Ấn Độ hay Brazil cũng đã bắt đầu tiếp cận theo hướng này. Đạo luật Bảo vệ dữ liệu cá nhân của Brazil (LGPD) có nhiều điểm tương đồng với GDPR, bao gồm quyền truy cập, chỉnh sửa, xóa bỏ dữ liệu và phản đối xử lý.

Thứ ba, một điểm chung khác trong pháp luật dữ liệu giữa các quốc gia là việc yêu cầu các tổ chức, doanh nghiệp phải chịu trách nhiệm khi thu thập và xử lý dữ liệu. Chẳng hạn, GDPR quy định doanh nghiệp phải thông báo vi phạm dữ liệu trong vòng 72 giờ sau khi phát hiện. APPI của Nhật Bản cũng yêu cầu các tổ chức áp dụng biện pháp quản lý nội bộ, đào tạo nhân viên và thiết lập quy trình ứng phó sự cố.

Thứ tư, quản lý chặt chẽ việc chuyển giao dữ liệu ra ngoài phạm vi lãnh thổ của quốc gia và thành lập cơ quan quản lý về dữ liệu. Hầu hết các quốc gia đều có quy định kiểm soát việc chuyển giao dữ liệu ra nước ngoài nhằm bảo đảm dữ liệu công dân không bị xâm phạm hoặc rơi vào tay các bên không đáng tin cậy. Để bảo đảm cho pháp luật về dữ liệu được thực thi một cách hiệu quả thì các quốc gia đã thành lập các cơ quan chuyên môn có chức năng giám sát và thi hành pháp luật về dữ liệu.

Thứ năm, xây dựng các cơ chế giải quyết tranh chấp và khiếu nại. Một trong những điểm quan trọng trong chính sách bảo vệ dữ liệu là việc thiết lập các cơ chế giải quyết tranh chấp và khiếu nại. Các quốc gia thường xuyên yêu cầu phải có những cơ quan độc lập có quyền tiếp nhận và xử lý khiếu nại của cá nhân khi quyền riêng tư của họ bị vi phạm. Cơ chế này không chỉ giúp bảo vệ quyền lợi của chủ thể dữ liệu mà còn đóng vai trò quan trọng trong việc duy trì niềm tin của công chúng vào hệ thống

bảo vệ dữ liệu của quốc gia. Ví dụ, trong khuôn khổ GDPR của Liên minh Châu Âu, Cơ quan bảo vệ dữ liệu quốc gia có quyền thụ lý khiếu nại từ người dân và ra quyết định xử phạt đối với tổ chức vi phạm. Cơ chế giải quyết tranh chấp này thường yêu cầu các tổ chức phải cung cấp các thông tin minh bạch về quyền lợi của người tiêu dùng, bao gồm các quyền yêu cầu sửa đổi, xóa dữ liệu, hoặc yêu cầu tổ chức ngừng xử lý dữ liệu cá nhân. Điều này tạo ra một môi trường pháp lý công bằng, nơi mọi hành vi xử lý dữ liệu đều phải tuân theo các quy định nghiêm ngặt về bảo vệ quyền lợi cá nhân.

Thứ sáu, tính bảo vệ dữ liệu tại nguồn (Privacy by Design). Privacy by Design, hay tính bảo vệ dữ liệu tại nguồn, là một nguyên tắc quan trọng trong chính sách bảo vệ dữ liệu cá nhân. Nguyên tắc này yêu cầu các tổ chức, doanh nghiệp phải áp dụng các biện pháp bảo vệ dữ liệu ngay từ khi bắt đầu thiết kế các sản phẩm, dịch vụ và quy trình xử lý dữ liệu. Thay vì chỉ áp dụng các biện pháp bảo vệ sau khi dữ liệu đã được thu thập, các tổ chức phải tích hợp các biện pháp bảo vệ quyền riêng tư ngay từ giai đoạn đầu của quá trình phát triển.

Điều này có nghĩa là trong suốt quá trình thiết kế sản phẩm hoặc dịch vụ, các tổ chức cần phải xem xét các yếu tố như mức độ bảo mật của dữ liệu, cách thức thu thập dữ liệu, và việc xử lý dữ liệu đó sau khi thu thập. Chẳng hạn, khi thiết kế một ứng dụng di động, các nhà phát triển phải xác định từ đầu các biện pháp bảo vệ quyền riêng tư, chẳng hạn như việc yêu cầu người dùng đồng ý trước khi thu thập dữ liệu, hoặc mã hóa dữ liệu cá nhân trong suốt quá trình xử lý. Việc bảo vệ dữ liệu không phải là một yếu tố phụ, mà phải được tích hợp trực tiếp vào quy trình thiết kế và phát triển sản phẩm.

Thứ bảy, phạm vi ảnh hưởng toàn cầu của các quy định bảo vệ dữ liệu. Có thể thấy rằng, các quốc gia xác định phạm vi ảnh hưởng của các quy định bảo vệ dữ liệu không chỉ giới hạn trong lãnh thổ của quốc gia mà còn ảnh hưởng đến các tổ chức, doanh nghiệp ở nước ngoài. Ví dụ, theo GDPR của Liên minh Châu Âu, các tổ chức ở ngoài EU nếu thu thập, xử lý hoặc lưu trữ dữ liệu cá nhân của công dân EU cũng phải tuân thủ các quy định này. Điều này tạo ra một khung pháp lý đồng nhất và có tính toàn cầu, giúp đảm bảo rằng các tổ chức ở mọi quốc gia đều có trách nhiệm bảo vệ dữ liệu cá nhân của người dân, không phân biệt quốc tịch.

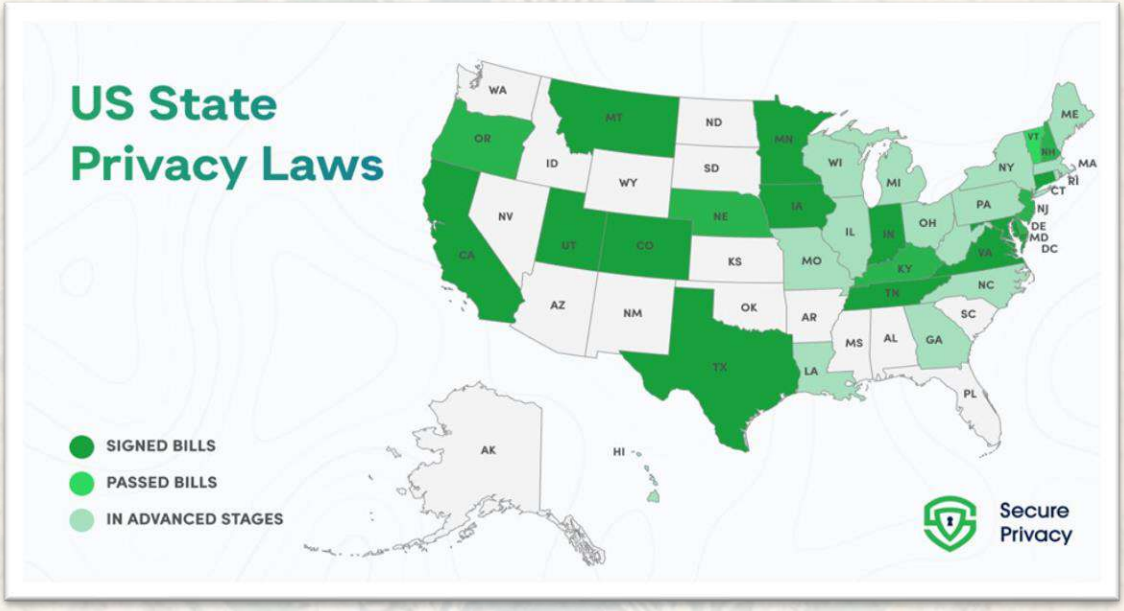
Tương tự, các quốc gia khác như Brazil với Đạo luật Bảo vệ Dữ liệu Cá nhân (LGPD) cũng yêu cầu các tổ chức xử lý dữ liệu của công dân Brazil phải tuân thủ các quy định bảo vệ quyền riêng tư, ngay cả khi tổ chức đó không đặt trụ sở tại Brazil. Điều này phản ánh sự chuyển động toàn cầu trong việc bảo vệ quyền riêng tư và bảo mật dữ liệu, khuyến khích các quốc gia hợp tác với nhau để xây dựng các quy định và chuẩn mực quốc tế về bảo vệ dữ liệu.

Những điểm chung này không chỉ phản ánh xu thế toàn cầu về bảo vệ dữ liệu cá nhân, mà còn thúc đẩy sự hợp tác và minh bạch trong việc bảo vệ quyền lợi của người dân trong kỷ nguyên số. Các quốc gia đều đang hướng đến việc xây dựng các khung pháp lý nghiêm ngặt và toàn diện, nhằm bảo vệ thông tin cá nhân của công dân, đồng thời tạo ra một môi trường pháp lý công bằng và đáng tin cậy.

1.2.14.2. Sự tương tác giữa GDPR và pháp luật Hoa Kỳ

Có một số điểm chung và khác biệt đáng chú ý giữa khuôn khổ quyền riêng tư và bảo vệ dữ liệu của Liên minh Châu Âu và Hoa Kỳ. Về sự chồng chéo, luật về quyền riêng tư ở cả hai khu vực pháp lý đều bắt nguồn từ *"Bộ*

nguyên tắc Thực hành thông tin công bằng" (FIP), được một ủy ban cố vấn ban hành lần đầu tiên vào năm 1973 của Bộ Y tế, Giáo dục và Phúc lợi Hoa Kỳ. Tổ chức Hợp tác và Phát triển Kinh tế đã cung cấp các hướng dẫn tương tự vào năm 1980, được cập nhật vào năm 2013. FIP đã ảnh hưởng đến cả luật pháp của EU và Hoa Kỳ, bao gồm Chỉ thị bảo vệ dữ liệu và GDPR tại EU, và Đạo luật về quyền riêng tư, Đạo luật báo cáo tín dụng công bằng và Đạo luật bảo vệ quyền riêng tư trực tuyến của trẻ em tại Hoa Kỳ, cũng như các thỏa thuận về quyền riêng tư quốc tế.



Biểu đồ luật riêng tư tại các bang của Hoa Kỳ - Ảnh: Secury Privacy

Tuy nhiên, các nguyên tắc của luật riêng tư EU và Hoa Kỳ lại khác nhau nhiều hơn là trùng lặp. Ví dụ, theo luật EU, *"luôn cần có cơ sở pháp lý và mục đích hợp pháp trước khi dữ liệu cá nhân được xử lý"*. Ngược lại, tại Hoa Kỳ, dữ liệu thương mại thường có thể được xử lý *"trừ khi có quy định pháp lý nào đó ngăn cấm"*. Do đó, mặc dù luật EU không cho phép xử lý dữ liệu mà không có lý do chính đáng, nhưng việc xử lý dữ liệu tại Hoa Kỳ được mặc định cho phép trừ khi nó gây ra thiệt hại pháp lý hoặc bị luật pháp hạn chế.

- Quyền được lãng quên

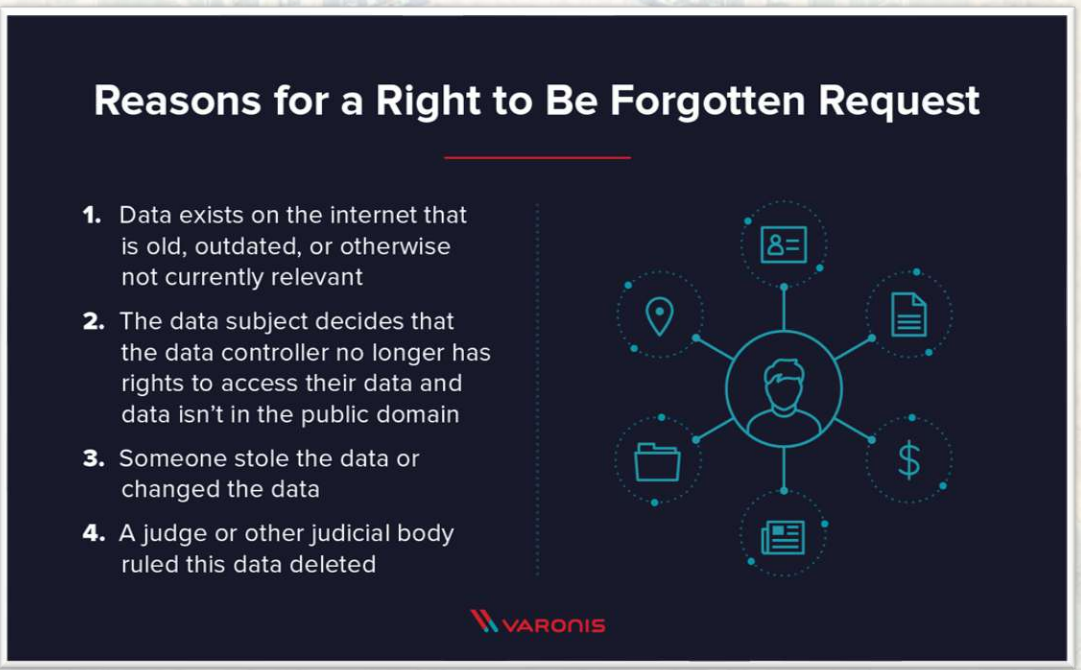
Một vấn đề then chốt về sự không tương thích giữa luật bảo vệ dữ liệu và quyền riêng tư của EU và Hoa Kỳ là quyền được lãng quên. Các ranh giới của quyền được lãng quên, khả năng áp dụng của nó đối với các công cụ tìm kiếm và ảnh hưởng của nó đối với các giá trị khác, chẳng hạn như quyền tự do ngôn luận và quyền tiếp cận thông tin, là những chủ đề được thảo luận quan trọng trong suốt quá trình soạn thảo GDPR. Thật vậy, xung đột tiềm tàng giữa quyền được lãng quên và các giá trị tự do ngôn luận và tự do báo chí được Tu chính án thứ nhất bảo vệ là một trong những vấn đề quan trọng nhất trong các cuộc thảo luận liên quan đến việc áp dụng luật EU đối với các nhà xuất bản và nền tảng công nghệ của Hoa Kỳ. Do một trong những mục tiêu của GDPR là tăng cường quyền được lãng quên, việc thực thi các yêu cầu xóa đối với các công ty Hoa Kỳ có thể vẫn là một vấn đề gây tranh cãi trong giao diện của luật bảo mật của EU và Hoa Kỳ.

Quyền được lãng quên đã được thiết lập trong Chỉ thị Bảo vệ Dữ liệu năm 1995 và cho phép người dùng yêu cầu "sửa chữa, xóa hoặc chặn dữ liệu" khi dữ liệu đó không đầy đủ, không chính xác hoặc không nhất quán với chỉ thị và trong trường hợp việc xử lý dữ liệu không tuân thủ luật pháp. Quyền này đã được Tòa án Công lý của Liên minh Châu Âu (CJEU) diễn giải bao gồm quyền yêu cầu xóa dữ liệu *"không đầy đủ, không liên quan hoặc không còn liên quan hoặc quá mức"*. Điều 17 của GDPR củng cố cách diễn giải này bằng cách cung cấp quyền rộng hơn cho chủ thể dữ liệu không chỉ yêu cầu xóa dữ liệu cá nhân mà còn ngăn chặn việc sử dụng và phổ biến thêm dữ liệu đó. GDPR sẽ cho phép các cá nhân rút lại sự đồng ý của họ cho phép bộ điều khiển dữ liệu xử lý dữ liệu của họ. Quyền này tạo ra thêm trách nhiệm cho bộ điều khiển dữ liệu trong việc công khai một số thông tin nhất

định, chẳng hạn như *"thực hiện các bước hợp lý, bao gồm các biện pháp kỹ thuật"* để thông báo cho các bộ điều khiển khác về yêu cầu xóa của cá nhân.

- *RTBF (Quyền được quên) và Tu chính án thứ nhất*

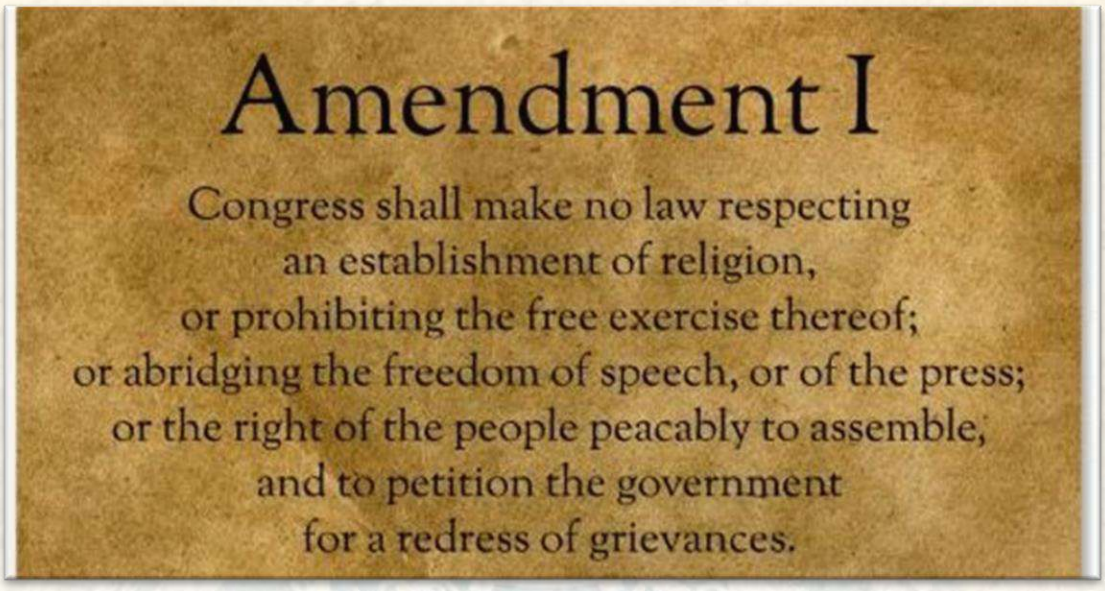
Tu chính án thứ nhất của Hiến pháp Hoa Kỳ là nguồn xung đột chính trong luật pháp Hoa Kỳ liên quan đến quyền xóa bỏ thông tin của GDPR. Về mặt lịch sử, Tu chính án thứ nhất đã đóng một vai trò quan trọng trong việc xác định ranh giới của luật riêng tư Hoa Kỳ. Vì nó hạn chế việc thực thi quyền lực của chính phủ - ngăn chặn chính phủ hạn chế dòng chảy thông tin - Tu chính án thứ nhất thường cản trở các luật nhằm bảo vệ quyền riêng tư trong chừng mực chúng được hiểu là của chính phủ hành động ngăn cản báo chí hoặc ngôn luận. Nếu tòa án cho rằng luật hoặc hành động do chính phủ thực hiện hạn chế việc truyền đạt thông tin, thì hành động đó có thể bị coi là vi hiến.



Dẫn giải về quyền được quên - Ảnh: Varonis

Do đó, các khiếu nại về quyền riêng tư tại Hoa Kỳ thường bị Tu chính án thứ nhất, vốn có vị trí vững chắc trong luật chung, qua mặt. Các luật hạn

chế một số cách sử dụng dữ liệu nhất định cũng đã bị thách thức bởi Tu chính án thứ nhất. Ví dụ, trong trường hợp Sorrell kiện IMS Health, Tòa án Tối cao đã xem xét một đạo luật của tiểu bang Vermont cấm việc bán, cấp phép hoặc trao đổi thông tin nhận dạng người kê đơn cho mục đích tiếp thị hoặc quảng cáo cũng như việc sử dụng thông tin này bởi các nhà sản xuất dược phẩm. Sau khi xác định rằng các hoạt động xử lý dữ liệu này về cơ bản là một hình thức *"hỗ trợ tiếp thị dược phẩm"*, Tòa án đã giải thích đạo luật này là quy định của chính phủ về quyền tự do ngôn luận được bảo vệ, đưa nó vào sự giám sát tư pháp chặt chẽ hơn và coi đó là hành vi vi hiến đối với Tu chính án thứ nhất. Ngay cả lời nói thái quá hoặc gây tổn hại về mặt cảm xúc hoặc danh tiếng cũng có thể được bảo vệ theo Hiến pháp theo Tu chính án thứ nhất. Thật vậy, những lo ngại của người nghe và người xem bị xúc phạm đã bị tòa án Hoa Kỳ bác bỏ ngay lập tức. Ví dụ, trong vụ Cohen kiện California, việc công khai thể hiện lời lẽ tục tĩu chống quân đội được xác định là được Tu chính án thứ nhất bảo vệ. Tòa án phán quyết rằng nếu một người cảm thấy khó chịu về một số điều nhất định, họ có thể *"quay mặt đi"* hoặc chấp nhận lời nói đó như một điều kiện thiết yếu của tự do. Lời nói gây tổn thương tinh thần cho người khác cũng được Tu chính án thứ nhất bảo vệ đặc biệt trong vụ Snyder kiện Phelps. Hơn nữa, việc Tu chính án thứ nhất bảo vệ quyền tự do ngôn luận trung thực cũng có thể lấn át các khiếu nại về tổn hại danh tiếng. Như Tòa án đã lập luận trong vụ Bartnicki kiện Vopper, *"trừ những trường hợp ngoại lệ, tổn hại danh tiếng không thể biện minh cho việc cấm đoán tự do ngôn luận trung thực"*. Những trường hợp ngoại lệ này cực kỳ hạn hẹp. Do đó, nguy cơ hậu quả tiêu cực phát sinh từ việc công bố hoặc phổ biến thông tin trung thực đã không vượt qua được Tu chính án thứ nhất.



Tu chính án thứ nhất - Ảnh: Reference.vn

Các tòa án đã giữ nguyên rằng *"nỗi sợ rằng mọi người sẽ đưa ra quyết định tồi tệ nếu được cung cấp thông tin trung thực"* không biện minh cho những hạn chế dựa trên nội dung về ngôn luận. Xung đột tiềm tàng này giữa quyền được lãng quên và quyền tự do ngôn luận cũng đã được Tòa án Công lý Châu Âu xử lý gần đây trong phán quyết rằng cơ quan bảo vệ dữ liệu của Pháp CNIL không thể buộc Google phải tôn trọng quyền yêu cầu xóa bỏ trên các tên miền công cụ tìm kiếm của mình trên toàn thế giới. Như Giám đốc điều hành Diễn đàn Tương lai về Quyền riêng tư Jules Polonetsky đã lưu ý, mặc dù tòa án phán quyết rằng luật pháp Châu Âu không buộc các công cụ tìm kiếm phải xóa bỏ trên toàn cầu khi quyền được lãng quên được khẳng định, nhưng tòa án vẫn để chỗ cho các cơ quan bảo vệ dữ liệu theo đuổi việc xóa bỏ trên toàn cầu như vậy *"nếu sự cân bằng về quyền riêng tư đòi hỏi điều đó trong một trường hợp cụ thể"*. Với những động lực này, sự tương tác giữa quyền xóa bỏ và các giá trị được bảo vệ bởi Tu chính án thứ nhất vẫn là một lĩnh vực mà cách tiếp cận của EU và Hoa Kỳ đối với quyền riêng tư và bảo vệ dữ liệu vẫn chưa được hòa giải.

1.2.14.3. Điểm khác trong chính sách pháp luật về dữ liệu giữa Trung Quốc và Liên minh châu Âu

Cả Luật Bảo vệ Thông tin Cá nhân của Trung Quốc (PIPL) và Quy định Bảo vệ Dữ liệu Chung (GDPR) của Liên minh châu Âu đều hướng tới mục tiêu bảo vệ quyền riêng tư của cá nhân và kiểm soát việc xử lý dữ liệu cá nhân. Tuy nhiên, giữa hai hệ thống pháp lý này tồn tại một số sự khác biệt về phạm vi, các nguyên tắc áp dụng, quyền của chủ thể dữ liệu, các cơ chế thực thi và biện pháp khắc phục.

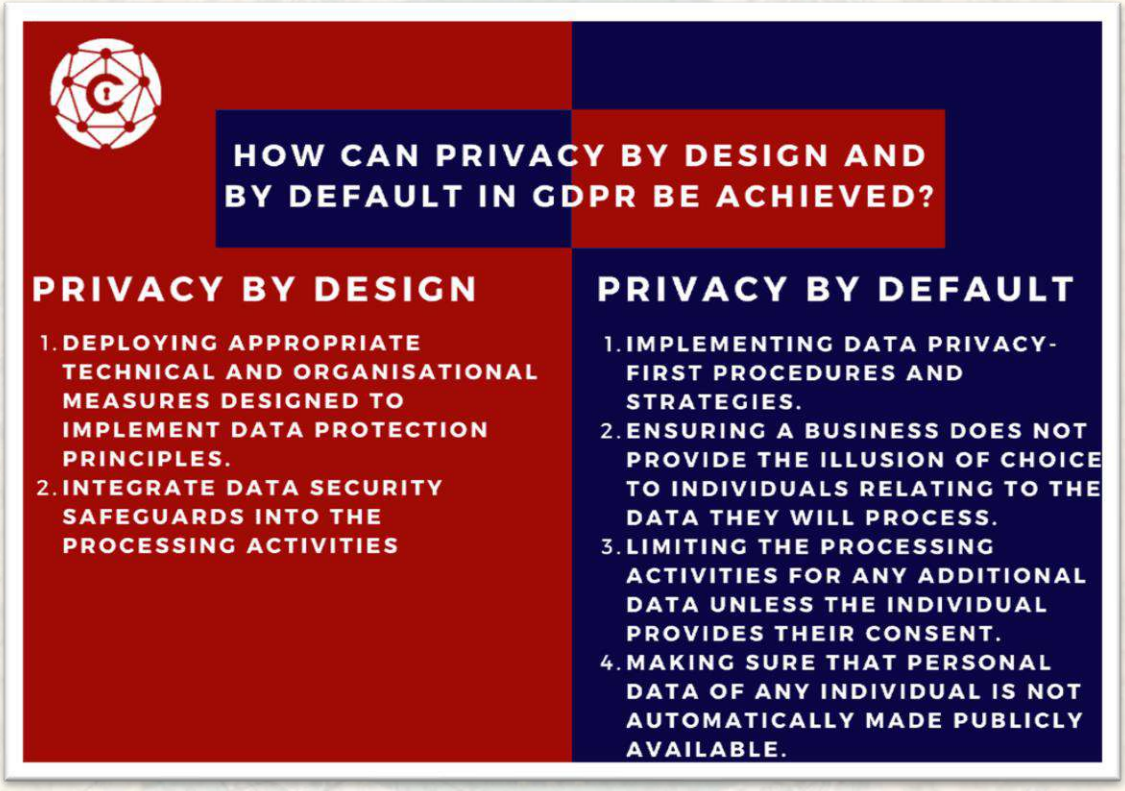


Cả Trung Quốc và Liên minh Châu Âu đều có luật các luật quy định về bảo vệ dữ liệu PIPL và GDPR - Ảnh: Gnovis Journal

- Phạm vi và nguyên tắc cơ bản

GDPR có phạm vi áp dụng toàn cầu, bao gồm tất cả các tổ chức xử lý dữ liệu của công dân EU hoặc theo dõi hành vi của họ, bất kể tổ chức đó có trụ sở trong EU hay không. Điều này giúp bảo vệ dữ liệu cá nhân của công dân EU ngay cả khi dữ liệu được xử lý ngoài EU. Ngược lại, PIPL chỉ áp dụng đối với các tổ chức trong lãnh thổ Trung Quốc hoặc các tổ chức ngoài

Trung Quốc nếu họ xử lý dữ liệu cá nhân của công dân Trung Quốc hoặc cung cấp dịch vụ cho họ. Cả hai hệ thống đều công nhận các nguyên tắc cơ bản như tính hợp pháp, minh bạch và mục đích rõ ràng trong việc xử lý dữ liệu, nhưng GDPR bao gồm các nguyên tắc bổ sung như "Privacy by Design" và "Privacy by Default", yêu cầu bảo vệ quyền riêng tư phải được tích hợp ngay từ đầu trong thiết kế hệ thống và quy trình xử lý dữ liệu, điều này không có trong PIPL.

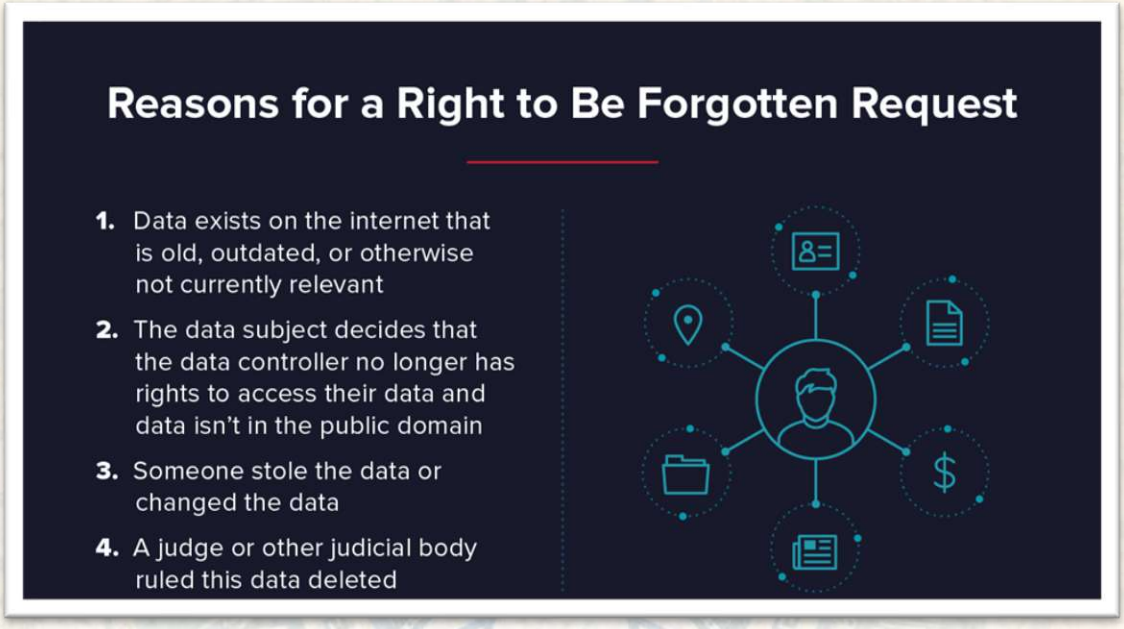


Các nguyên tắc "Privacy by Design" và "Privacy by Default" của GDPR - Ảnh: Cyphere

- Quyền của chủ thể dữ liệu

Cả hai đạo luật đều công nhận quyền của chủ thể dữ liệu đối với dữ liệu cá nhân của họ, bao gồm quyền truy cập, quyền chỉnh sửa, quyền xóa bỏ, quyền chuyển giao dữ liệu và quyền phản đối. Tuy nhiên, GDPR có những quy định chi tiết và cụ thể hơn về quyền "quyền được quên", cho phép cá

nhân yêu cầu xóa bỏ dữ liệu của họ khỏi các hệ thống của tổ chức. PIPL cũng công nhận quyền xóa dữ liệu nhưng không quy định chi tiết như trong GDPR và không có quyền "quyền được quên". Thêm vào đó, PIPL đặc biệt chú trọng đến việc xử lý dữ liệu nhạy cảm, yêu cầu sự đồng ý rõ ràng từ chủ thể dữ liệu và đặt ra các điều kiện nghiêm ngặt hơn đối với loại dữ liệu này.



Lý giải về quyền được quên của GDPR - Ảnh: Varonis

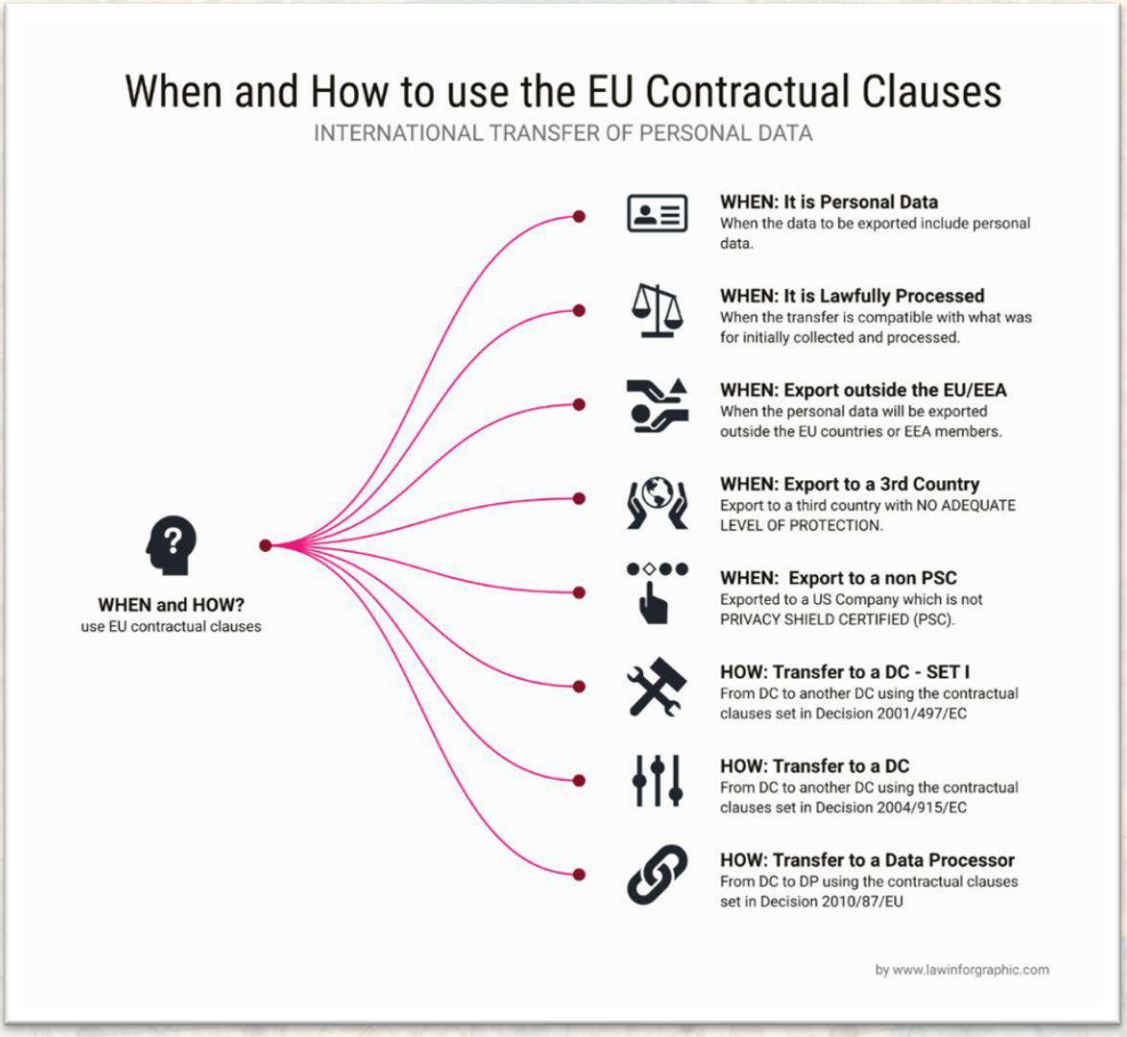
- Sự đồng ý và cơ sở pháp lý xử lý dữ liệu

Cả GDPR và PIPL đều yêu cầu sự đồng ý của chủ thể dữ liệu để xử lý dữ liệu cá nhân. Tuy nhiên, GDPR yêu cầu sự đồng ý phải rõ ràng, tự nguyện và có thể rút lại, đồng thời cung cấp các cơ sở pháp lý rộng hơn cho việc xử lý dữ liệu, bao gồm hợp đồng và lợi ích hợp pháp. PIPL yêu cầu sự đồng ý rõ ràng đối với cả dữ liệu cá nhân và dữ liệu nhạy cảm, nhưng ít cơ sở pháp lý linh hoạt hơn. Đặc biệt, GDPR có quy định chi tiết về sự đồng ý của trẻ em, trong khi PIPL không đề cập cụ thể về sự đồng ý của trẻ em.

- Chuyển giao dữ liệu quốc tế

GDPR có các quy định nghiêm ngặt về việc chuyển giao dữ liệu ra ngoài EU, yêu cầu các quốc gia hoặc tổ chức nhận dữ liệu phải có mức độ bảo vệ

dữ liệu tương đương EU, hoặc phải có các biện pháp bảo vệ như *"Standard Contractual Clauses"* (SCCs). Bên cạnh đó, PIPL cũng quy định việc chuyển giao dữ liệu ra ngoài Trung Quốc, nhưng yêu cầu phải có sự phê duyệt từ cơ quan chức năng của Trung Quốc và các công ty phải chứng minh rằng quốc gia tiếp nhận có biện pháp bảo vệ dữ liệu tương đương. Điều này cho thấy GDPR có cơ chế chi tiết và rõ ràng hơn trong việc điều chỉnh chuyển giao dữ liệu quốc tế.

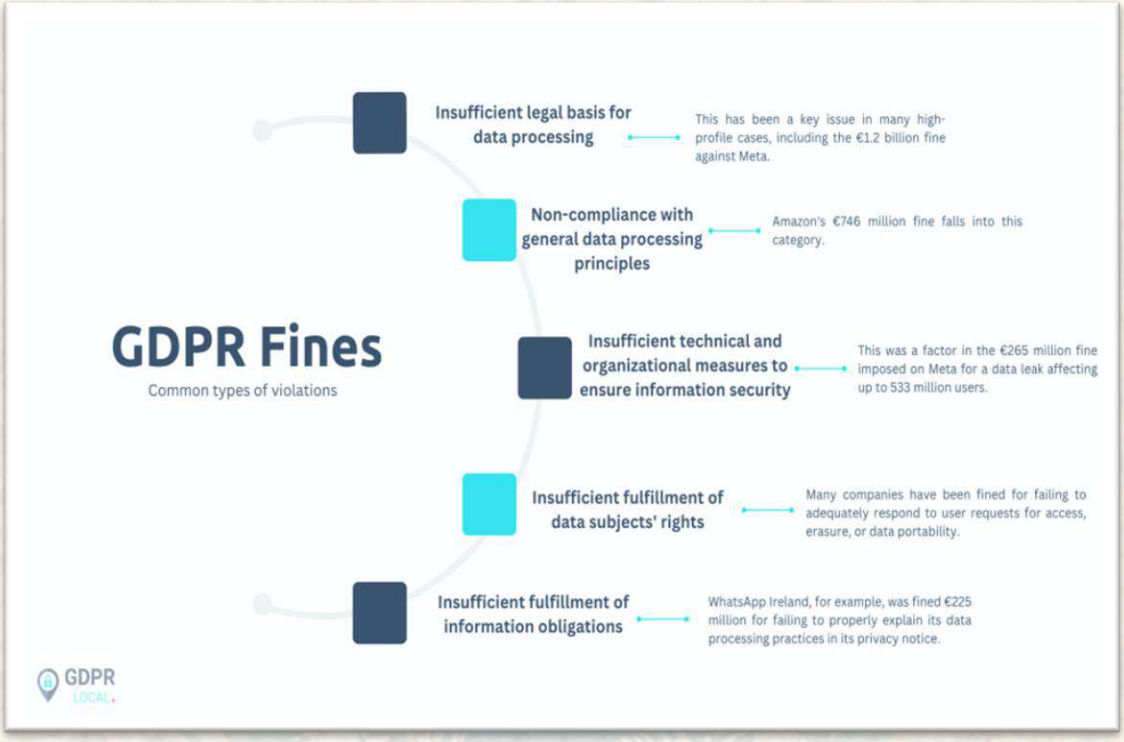


Lý giải về Standard Contractual Clauses (SCCs) - Ảnh: Lawinfographic

- Chế tài và biện pháp khắc phục

GDPR quy định các hình phạt hành chính nghiêm khắc, có thể lên tới 4% doanh thu toàn cầu hoặc 20 triệu Euro, tùy theo điều kiện nào cao hơn.

Các biện pháp khắc phục trong GDPR bao gồm yêu cầu tổ chức sửa chữa vi phạm và thực hiện các biện pháp bảo vệ dữ liệu bổ sung. PIPL cũng quy định các hình phạt hành chính và hình sự, nhưng mức phạt có thể thấp hơn và có sự linh hoạt hơn tùy vào mức độ vi phạm. Thêm vào đó, PIPL cũng quy định hình phạt hình sự đối với những vi phạm nghiêm trọng, chẳng hạn như việc bán hoặc cung cấp dữ liệu cá nhân trái phép.



Các hình phạt được quy định tại GDPR - Ảnh: GDPR Local

- Tính độc lập của cơ quan giám sát

GDPR yêu cầu mỗi quốc gia thành viên EU có cơ quan giám sát độc lập để thực thi các quy định bảo vệ dữ liệu và có quyền phạt các tổ chức vi phạm. Các cơ quan này hoạt động dưới sự giám sát của Ủy ban Bảo vệ Dữ liệu Châu Âu (EDPB). PIPL có cơ quan giám sát là Cục Quản lý Bảo vệ Dữ liệu Cá nhân Trung Quốc, nhưng tính độc lập của cơ quan này vẫn còn nhiều vấn đề cần cải thiện, đặc biệt trong việc thực thi và giám sát các quy định bảo vệ dữ liệu tại Trung Quốc.

1.2.14.4. Bài học kinh nghiệm cho Việt Nam trong xây dựng chính sách pháp luật về dữ liệu

Trong bối cảnh chuyển đổi số và sự phát triển nhanh chóng của công nghệ, việc xây dựng chính sách pháp luật về dữ liệu đã trở thành một yếu tố cốt lõi đối với các quốc gia trên toàn thế giới, trong đó có Việt Nam. Chính sách dữ liệu không chỉ đảm bảo bảo vệ quyền riêng tư và an ninh quốc gia mà còn tạo ra nền tảng vững chắc để phát triển nền kinh tế số và hội nhập quốc tế. Qua việc nghiên cứu và phân tích các mô hình pháp lý của những quốc gia điển hình, nhóm tác giả rút ra một số bài học kinh nghiệm quý báu, từ đó xây dựng một hệ thống pháp luật về dữ liệu phù hợp, linh hoạt và bền vững tại Việt Nam. Cụ thể như sau:

Một là, xây dựng khung pháp lý toàn diện và linh hoạt. Việc xây dựng một khung pháp lý toàn diện là bước đi đầu tiên và vô cùng quan trọng trong quá trình phát triển chính sách dữ liệu tại Việt Nam. Khung pháp lý này không chỉ cần bảo vệ các nguyên tắc cơ bản liên quan đến dữ liệu, mà còn phải có khả năng linh hoạt và thích ứng nhanh chóng với sự phát triển không ngừng của công nghệ. Đặc biệt trong bối cảnh chuyển đổi số đang diễn ra mạnh mẽ và sự phát triển nhanh chóng của các công nghệ tiên tiến như trí tuệ nhân tạo (AI) và chuỗi khối (blockchain), việc đảm bảo các quy định bảo vệ dữ liệu được cập nhật và điều chỉnh thường xuyên là điều hết sức cần thiết.

Để đạt được điều này, Việt Nam cần áp dụng nguyên lý *"Điều tiết động"* (Dynamic Regulation), tức là xây dựng một cơ chế linh hoạt cho phép các quy định trong Luật Dữ liệu 2024 được đánh giá và điều chỉnh định kỳ. Điều này sẽ giúp đảm bảo rằng khung pháp lý luôn đồng hành với sự tiến bộ của công nghệ, không bị tụt lại phía sau trong bối cảnh những thay đổi công nghệ diễn ra liên tục và nhanh chóng. Thực tế, các quy định pháp lý về dữ

liệu cần được xây dựng sao cho có thể thay đổi và thích ứng kịp thời với các yêu cầu mới, nhất là khi các công nghệ như AI và blockchain đang ngày càng trở nên phổ biến và ứng dụng rộng rãi.



Hoàn thiện hành lang pháp lý, tạo nền tảng cho phát triển kinh tế số, xã hội số - Ảnh: Báo Điện tử Chính phủ

Khung pháp lý phải đảm bảo tính linh hoạt, không chỉ đáp ứng được nhu cầu bảo vệ dữ liệu trong hiện tại mà còn có thể điều chỉnh phù hợp với những công nghệ mới nổi trong tương lai. Cụ thể, đối với công nghệ blockchain, cần phải có quy định rõ ràng về việc bảo vệ dữ liệu trong môi trường phi tập trung, nơi mà dữ liệu không được lưu trữ tại một điểm cố định mà phân tán trên nhiều mạng lưới. Tương tự, trong lĩnh vực trí tuệ nhân tạo, khung pháp lý cần đảm bảo rằng việc thu thập và xử lý dữ liệu phục vụ cho các ứng dụng AI phải tôn trọng quyền riêng tư của cá nhân và không làm tổn hại đến quyền lợi của người dân.

Với một khung pháp lý như vậy, Việt Nam sẽ có thể bảo vệ quyền lợi của công dân trong môi trường số hóa, đồng thời tạo điều kiện thuận lợi cho

sự phát triển mạnh mẽ của các ngành công nghiệp số, hướng đến một nền kinh tế số hội nhập và phát triển bền vững trong tương lai.

Hai là, tăng cường quản lý và giám sát từ cấp trung ương. Một bài học quan trọng mà Việt Nam cần rút ra trong việc xây dựng chính sách bảo vệ dữ liệu là sự cần thiết thành lập một cơ quan quản lý dữ liệu quốc gia mạnh mẽ. Có thể tính toán xây dựng cơ cấu một đơn vị cấp Cục trực thuộc Bộ Công an phụ trách lĩnh vực dữ liệu này bên cạnh Trung tâm dữ liệu quốc gia. Cơ quan này không chỉ cần có quyền lực giám sát mà còn phải có khả năng thực thi các quy định bảo vệ dữ liệu một cách nghiêm ngặt, đảm bảo rằng mọi hành vi thu thập, xử lý và chia sẻ dữ liệu đều được giám sát và kiểm soát chặt chẽ. Điều này giúp bảo vệ quyền lợi và dữ liệu cá nhân của công dân khỏi những vi phạm, đồng thời duy trì sự tin tưởng của xã hội đối với các tổ chức và doanh nghiệp trong việc xử lý dữ liệu.



Chỉ thị số 26/CT-TTg ngày 20/10/2023 của Thủ tướng Chính phủ về việc chấn chỉnh, tăng cường công tác thanh tra, kiểm tra, giám sát hoạt động công vụ - Ảnh: Báo Điện tử Chính phủ

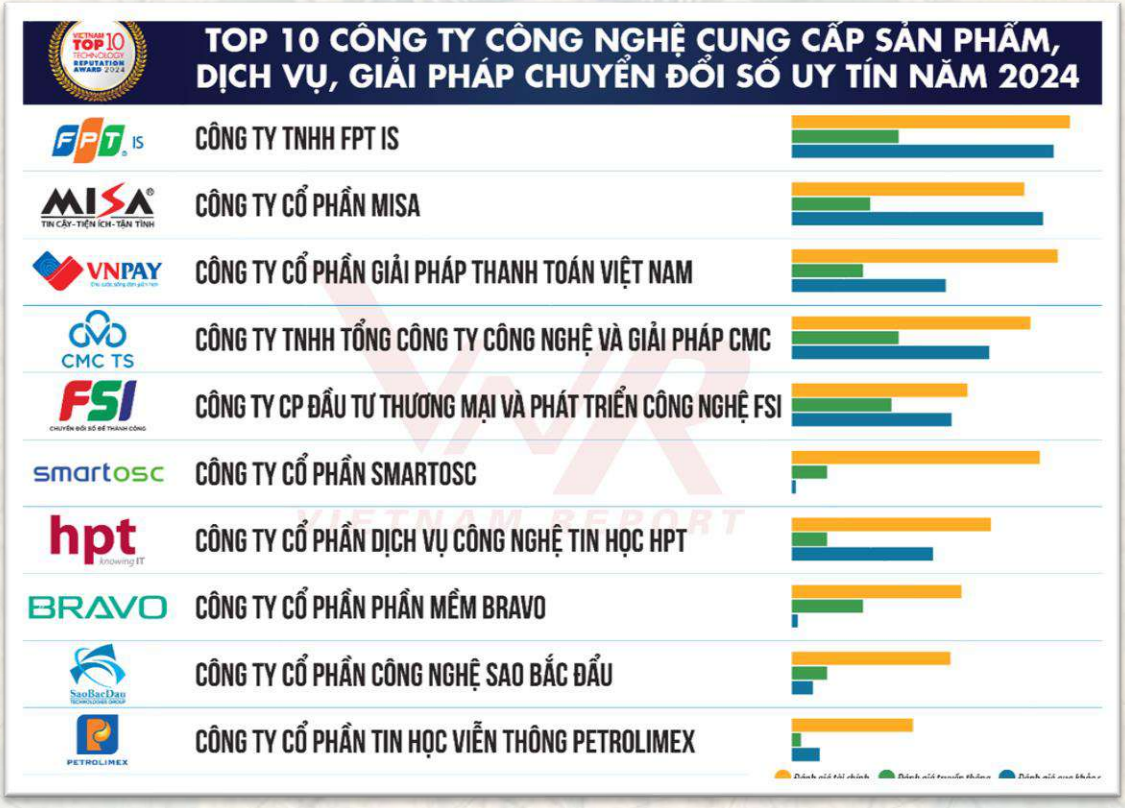
Cơ quan quản lý dữ liệu quốc gia cần hoạt động độc lập, có thẩm quyền rõ ràng trong việc giám sát các quy định bảo vệ dữ liệu và thực thi các biện pháp xử lý khi có vi phạm. Một mô hình đáng tham khảo là việc thành lập một cơ quan giám sát tương tự như Ủy ban Bảo vệ Dữ liệu Cá nhân (PDPC) ở Singapore, với nhiệm vụ giám sát và xử lý các vi phạm liên quan đến bảo vệ dữ liệu cá nhân. Cơ quan này sẽ chịu trách nhiệm đảm bảo tính minh bạch và công bằng trong việc áp dụng các quy định, tạo ra một môi trường bảo vệ dữ liệu hiệu quả và dễ tiếp cận đối với người dân và các tổ chức.

Để hoạt động hiệu quả, cơ quan quản lý cần có khả năng kiểm tra, thanh tra các tổ chức và doanh nghiệp trong việc tuân thủ các quy định bảo vệ dữ liệu. Điều này không chỉ giúp phát hiện kịp thời các vi phạm mà còn nâng cao ý thức và trách nhiệm của các tổ chức trong việc bảo vệ dữ liệu cá nhân. Việc giám sát và kiểm soát chặt chẽ sẽ đảm bảo rằng mọi tổ chức đều thực hiện đúng quy định về bảo mật và quyền riêng tư, đồng thời tạo ra sự công bằng trong việc bảo vệ quyền lợi cá nhân trong môi trường số hóa.

Ba là, cân bằng giữa bảo vệ quyền riêng tư và an ninh quốc gia. Việc xây dựng chính sách bảo vệ dữ liệu cân bằng giữa việc bảo vệ quyền riêng tư của công dân và bảo đảm an ninh quốc gia là thách thức đối với tất cả các quốc gia, trong đó có Việt Nam. Trong bối cảnh này, Việt Nam cần xây dựng hành lang pháp lý hài hòa, triệt tiêu xung đột giữa bảo đảm an ninh - quốc phòng và bảo vệ quyền lợi của cá nhân, tạo cơ chế để bảo vệ an ninh quốc gia cũng bao hàm bảo vệ quyền lợi cá nhân. Các quy định về bảo vệ dữ liệu phải đảm bảo tính minh bạch và rõ ràng, đồng thời tạo cơ chế minh bạch để không xâm phạm quyền riêng tư của công dân. Một bài học từ các quốc gia phát triển là việc kết hợp bảo vệ quyền riêng tư song song với yêu cầu minh bạch, tạo điều kiện cho người dân và doanh nghiệp hiểu rõ quyền lợi và nghĩa

vụ của mình. Các quy định phải dễ hiểu và dễ tiếp cận, từ đó tạo ra một môi trường an toàn mà không gây mâu thuẫn giữa việc bảo vệ quyền lợi cá nhân và an ninh quốc gia.

Việt Nam cũng cần thực hiện lưu trữ dữ liệu dựa hoàn toàn trên cơ sở hạ tầng trong hệ thống cơ quan nhà nước, nhằm đảm bảo an toàn thông tin công dân và đặc biệt là các bí mật nhà nước, tránh phụ thuộc vào các công nghệ của các doanh nghiệp tư nhân. Tuy nhiên, chính sách này cần phải được triển khai một cách hợp lý, tránh gây trở ngại cho quá trình hội nhập quốc tế và phát triển kinh tế số.



Top 10 Công ty Công nghệ uy tín năm 2024 - Ảnh: Vietnam Report

Bốn là, khuyến khích đổi mới và tạo điều kiện cho doanh nghiệp nhỏ và vừa. Một yếu tố quan trọng trong việc xây dựng chính sách dữ liệu là việc hỗ trợ các doanh nghiệp nhỏ và vừa (SMEs) có thể tiếp cận dữ liệu một cách an toàn và hiệu quả. Các SMEs, vốn là động lực của nền kinh tế Việt Nam,

cần được khuyến khích và tạo điều kiện để phát triển các dịch vụ đổi mới sáng tạo mà không gặp phải các khó khăn trong việc tuân thủ các quy định bảo vệ dữ liệu.

Việt Nam cần đơn giản hóa các quy định liên quan đến bảo vệ dữ liệu cho các doanh nghiệp nhỏ và vừa, giúp họ dễ dàng tuân thủ mà không gặp phải các rào cản lớn. Điều này có thể được thực hiện thông qua việc cung cấp các công cụ và nền tảng hỗ trợ, giúp các doanh nghiệp quản lý dữ liệu và bảo mật một cách hiệu quả. Việc tạo ra các công cụ này không chỉ giúp SMEs tiết kiệm chi phí mà còn thúc đẩy sự phát triển bền vững của các doanh nghiệp trong môi trường số.



Hội nghị đẩy mạnh chương trình hỗ trợ doanh nghiệp nhỏ và vừa chuyển đổi số năm 2022 - Ảnh: Báo Quân đội nhân dân

Bên cạnh đó, chính sách cần khuyến khích sự đổi mới sáng tạo, đặc biệt là trong các lĩnh vực công nghệ như AI, blockchain và fintech. Quyền chuyển giao dữ liệu sẽ là một yếu tố quan trọng, giúp các công ty có thể phát triển các dịch vụ cá nhân hóa dựa trên dữ liệu, đồng thời bảo vệ quyền lợi của người dùng và thúc đẩy sự đổi mới trong các ngành công nghiệp này.

Năm là, minh bạch trong quản trị dữ liệu. Một yếu tố thiết yếu khác là việc yêu cầu các tổ chức và doanh nghiệp thực hiện quản trị dữ liệu một cách minh bạch. Việc công khai các chính sách bảo mật, thông báo rõ ràng về mục đích sử dụng dữ liệu và quyền lợi của cá nhân khi tham gia vào các hoạt động thu thập dữ liệu là vô cùng quan trọng. Minh bạch trong việc quản lý dữ liệu sẽ không chỉ giúp bảo vệ quyền lợi của người dân mà còn tạo ra môi trường tin cậy cho các doanh nghiệp hoạt động trong lĩnh vực dữ liệu.

Các tổ chức cần phải minh bạch về cách thức thu thập, sử dụng và chia sẻ dữ liệu cá nhân. Điều này không chỉ giúp người dùng hiểu rõ về cách thức dữ liệu của họ được xử lý mà còn nâng cao sự tin tưởng đối với các tổ chức, đặc biệt là trong bối cảnh người dân ngày càng quan tâm hơn đến vấn đề bảo mật thông tin cá nhân.

Ngoài ra, các doanh nghiệp cần đảm bảo rằng họ có sự đồng ý rõ ràng từ phía người dùng trước khi thu thập và xử lý dữ liệu cá nhân. Quy trình này không chỉ giúp bảo vệ quyền lợi của người dùng mà còn làm tăng cường sự tin tưởng của họ đối với các tổ chức và doanh nghiệp, qua đó tạo ra một môi trường giao dịch an toàn và minh bạch.

Sáu là, hợp tác quốc tế và hội nhập toàn cầu. Trong thời đại số hóa toàn cầu, bảo vệ dữ liệu cá nhân không thể chỉ giới hạn trong phạm vi quốc gia mà cần phải có sự hợp tác quốc tế để đảm bảo tính toàn vẹn và an toàn của dữ liệu khi trao đổi qua biên giới. Điều này càng trở nên quan trọng khi các công ty, tổ chức và doanh nghiệp có hoạt động quốc tế, và dữ liệu cá nhân có thể được chuyển giao qua nhiều quốc gia.

Việt Nam cần đảm bảo rằng các quy định bảo vệ dữ liệu của mình tương thích với các tiêu chuẩn quốc tế như GDPR (Châu Âu), APEC CBPR (Châu Á-Thái Bình Dương) nhằm thu hút đầu tư quốc tế và tạo điều kiện cho các

doanh nghiệp Việt Nam mở rộng ra thị trường toàn cầu. Hợp tác quốc tế sẽ giúp Việt Nam không chỉ bảo vệ dữ liệu cá nhân của công dân mà còn tạo điều kiện thuận lợi cho các doanh nghiệp trong nước khi giao dịch với các đối tác quốc tế.



Ủy viên Bộ Chính trị, Thủ tướng Chính phủ Phạm Minh Chính tiếp Tổng thư ký Liên hợp quốc Antonio Guterres trong chuyến thăm chính thức Việt Nam nhân dịp kỷ niệm 45 năm Việt Nam tham gia Liên hợp quốc - Ảnh: TTXVN

Bên cạnh đó, Việt Nam cần xây dựng các cơ chế đối thoại song phương với các quốc gia khác để giải quyết các vấn đề pháp lý và quy định liên quan đến bảo vệ dữ liệu. Việc này sẽ tạo ra một môi trường hợp tác an toàn và hiệu quả trong trao đổi dữ liệu, đồng thời giúp tránh những xung đột pháp lý có thể phát sinh trong quá trình hợp tác quốc tế.

Từ các bài học trên, Việt Nam có thể xây dựng một chính sách dữ liệu toàn diện và linh hoạt, đáp ứng yêu cầu bảo vệ quyền lợi của công dân trong bối cảnh kỷ nguyên số. Việc thành lập một cơ quan giám sát mạnh mẽ, xây dựng các quy định minh bạch, hỗ trợ các doanh nghiệp nhỏ và vừa, và thúc

đẩy hợp tác quốc tế là những yếu tố quan trọng giúp Việt Nam xây dựng một hệ thống dữ liệu an toàn và hiệu quả, đồng thời tạo điều kiện cho sự phát triển của nền kinh tế số.

1.3. SỰ CẦN THIẾT XÂY DỰNG VÀ HOÀN THIỆN PHÁP LUẬT VỀ DỮ LIỆU Ở VIỆT NAM

1.3.1. Bối cảnh trong nước và quốc tế

1.3.1.1. Xu hướng toàn cầu về xây dựng và ban hành chính sách pháp luật về dữ liệu

Trong hai thập niên qua, dữ liệu đã chuyển mình từ một loại tài nguyên *"thứ yếu"* của hoạt động trực tuyến để trở thành nền tảng cốt lõi vận hành nền kinh tế số, hệ sinh thái tri thức và các chức năng chủ chốt của nhà nước hiện đại. Vì vậy, các quốc gia bước vào một chu kỳ lập pháp mới, trong đó *"chính sách pháp luật về dữ liệu"* không chỉ là khuôn khổ bảo vệ quyền riêng tư hay an ninh mạng, mà còn là kiến thiết thể chế phù hợp nhằm điều tiết dòng chảy dữ liệu xuyên biên giới, bảo đảm tiêu chuẩn quốc tế, tạo lập thị trường dữ liệu và duy trì tính bền vững của hạ tầng số.

Dữ liệu lúc này trở thành một nguồn tài nguyên như điện, nước, đồng thời là một hình thái tư bản, là đầu vào của trí tuệ nhân tạo và là *"yếu tố kết nối"* các chuỗi giá trị xuyên biên giới.

Dưới góc độ thực tiễn, thế giới trực tuyến hôm nay đã đạt độ bao phủ chưa từng có. Liên minh Viễn thông Quốc tế (ITU) ước tính năm 2024 có khoảng 5,4 - 5,5 tỷ người dùng Internet, tương đương xấp xỉ 67 - 68% dân số toàn cầu, cho thấy *"xã hội dữ liệu"* đã trở thành trạng thái phổ biến chứ không còn là ngoại lệ[181]. Ở đầu kia của chuỗi, dung lượng dữ liệu tạo ra và

[181] Liên minh Viễn thông Quốc tế (2024), *Thực tế và Con số 2024*, https://www.itu.int/itu-d/reports/statistics/2024 /11/10/ff24-internet-use/, truy cập ngày 20/7/2025.

sao chép toàn cầu năm 2025 được IDC ước tính chạm mốc 142 zettabyte, gấp nhiều lần so với một thập niên trước và tiếp tục tăng theo cấp số nhân[182].



Dữ liệu đóng vai trò ngày càng quan trọng - Ảnh: Cục Thông tin, Thống kê

Không chỉ lượng dữ liệu tăng bùng nổ, mà cả độ *"kết nối"* của nó cũng sâu rộng. Theo UNCTAD, thương mại điện tử quy mô 27 nghìn tỷ USD (ước tính đến 2022, bao phủ 43 nền kinh tế đại diện 3/4 GDP thế giới) và bùng nổ thiết bị Internet vạn vật dự kiến đạt 39 tỷ đơn vị vào 2029 là hai động lực đẩy nhu cầu quản trị dữ liệu lên mức thể chế. Sự tăng trưởng kết nối chuyển hóa thành tăng trưởng dữ liệu. Các báo cáo định lượng nhiều năm liền dự báo *"datasphere"* toàn cầu tăng theo cấp số nhân, IDC từng dự phóng từ 45 zettabyte năm 2019 lên 175 zettabyte vào năm 2025; các ước tính mới tiếp tục củng cố quỹ đạo này dù phương pháp luận khác nhau. Dù những con số khác biệt về chi tiết, bức tranh nhất quán là dữ liệu trở thành tài nguyên phổ

[182] UNCTAD (2024), *Data Protection and Privacy Legislation Worldwide,* https://unctad.org/page/data-protection-and-privacy-legislation-worldwide, truy cập ngày 02/8/2025.

quát, mọi ngành, mọi quốc gia đều lệ thuộc vào chuỗi giá trị dữ liệu - từ thu thập, khai thác, lưu trữ, chia sẻ đến phân tích.

Dòng chảy dữ liệu xuyên biên giới, hay *"chuyển dữ liệu quốc tế"*, đã trở thành mạch máu của thương mại số. Nhiều nghiên cứu kinh tế lượng chỉ ra đóng góp đáng kể của luồng dữ liệu đối với GDP toàn cầu; chẳng hạn, một phân tích kinh điển đã ước tính các dòng dữ liệu xuyên biên tạo ra khoảng 2,3 - 2,8 nghìn tỷ USD giá trị vào năm 2014, tương đương cỡ vài phần trăm GDP toàn cầu khi đó. Ý nghĩa của chỉ dấu này không nằm ở con số tuyệt đối, mà ở kết luận rằng dữ liệu giờ đây đứng ngang hàng, thậm chí vượt, các dòng chảy truyền thống như hàng hóa, dịch vụ hay vốn về khả năng tạo giá trị gia tăng.



Dòng chảy dữ liệu xuyên biên giới - Ảnh: McKinsey

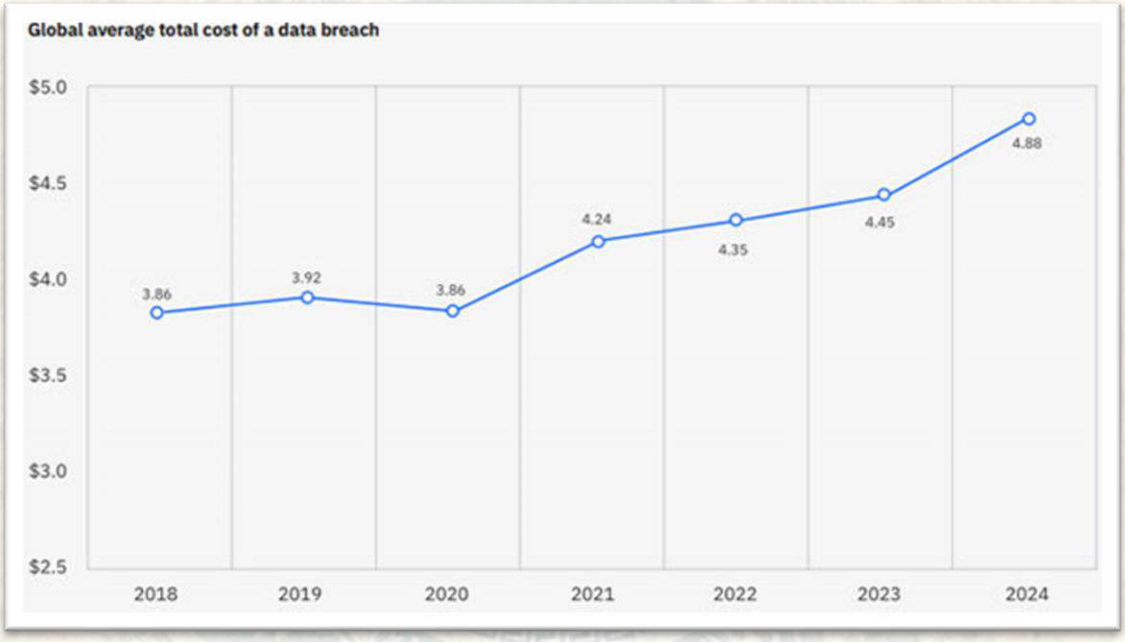
Bên cạnh quy mô, cấu trúc tiêu dùng dữ liệu cũng thay đổi. Với sự dịch chuyển lên 4G/5G, lưu lượng dữ liệu di động bình quân đã tăng mạnh, đạt

gần 13 GB mỗi kết nối trong năm 2023 theo một khảo sát công nghiệp lớn. Cùng lúc, thương mại điện tử doanh nghiệp - doanh nghiệp và doanh nghiệp - người tiêu dùng tăng nhanh, từ dữ liệu mới từ 43 nền kinh tế cho thấy doanh số thương mại điện tử doanh nghiệp tăng gần 60% giai đoạn 2016 - 2022, đạt khoảng 27 nghìn tỷ USD. Dưới bề mặt mỗi giao dịch là những gói dữ liệu về hành vi người dùng, chuỗi cung ứng, định danh thanh toán - những thực thể pháp lý chưa được *"định danh"* rõ ràng nếu thiếu khung luật.

Nếu dữ liệu là hạ tầng mềm của tăng trưởng, thì sự tin cậy là *"chất kết dính"* của hạ tầng ấy. Theo đó, chính sách - pháp luật về dữ liệu xuất hiện như một yêu cầu tất yếu. ***Thứ nhất,*** đó là tất yếu từ góc độ thị trường. Không có một chuẩn mực chung về quyền riêng tư, bảo mật, tính toàn vẹn và khả chuyển dữ liệu, các giao dịch trên môi trường điện tử sẽ đối mặt với rủi ro lừa đảo và chi phí giao dịch cao. Tổ chức Hợp tác và Phát triển Kinh tế (OECD) khái quát luận đề *"Data Free Flow with Trust"* (DFFT) như sau: "Phải vừa bảo đảm lưu thông dữ liệu qua biên giới để thúc đẩy thương mại số, vừa bảo đảm dữ liệu được bảo vệ đầy đủ khi vượt biên". Nói cách khác, lưu thông nhưng thiếu tin cậy sẽ đổ vỡ, còn bảo vệ mà không có lưu thông sẽ triệt tiêu động lực đổi mới. Pháp luật dữ liệu được thiết kế để giải quyết bài toán đó.

Thứ hai, sự tất yếu xuất phát từ rủi ro hệ thống ngày càng lớn. Chi phí sự cố rò rỉ dữ liệu leo thang trở thành *"tín hiệu giá"* thúc ép các chủ thể, trong đó có nhà nước, nội luật hóa các tiêu chuẩn quản trị rủi ro. Báo cáo *"Cost of a Data Breach 2024"* về lĩnh vực an ninh mạng ghi nhận chi phí trung bình một vụ lộ lọt dữ liệu toàn cầu tăng lên khoảng 4,88 triệu USD; có ngành còn cao hơn mức bình quân đáng kể. Đằng sau con số là thực tế: thời gian phát hiện - khắc phục kéo dài, gián đoạn vận hành, yêu cầu bồi thường,

phạt vi phạm, tổn thất uy tín. Với các hệ thống dựa nhiều vào trí tuệ nhân tạo, một lớp rủi ro mới xuất hiện - *"shadow AI"*, truy cập không kiểm soát vào mô hình, và chuỗi cung ứng thuật toán - khiến chi phí tổn thất có thể gia tăng. Các phép đo gần đây cho thấy tác nhân xấu đã tận dụng AI để tăng tốc lừa đảo, giả mạo, tăng bề mặt tấn công. Khi rủi ro lan tỏa như thế, luật dữ liệu trở thành công cụ ràng buộc trách nhiệm, chuẩn hóa kiểm soát truy cập, nghĩa vụ thông báo sự cố và quản trị vòng đời dữ liệu.



Thông kê thiệt hại trung bình của một vụ lộ, lọt dữ liệu năm 2024 - Ảnh: IBM

Thứ ba, xuất phát từ quyền con người trong kỷ nguyên số. Quyền riêng tư, quyền được bảo vệ dữ liệu cá nhân, quyền tiếp cận và sửa dữ liệu, quyền di chuyển dữ liệu giữa các dịch vụ… không còn là khái niệm đạo đức mơ hồ mà đã trở thành nội dung pháp lý cứng. Sự lan tỏa của bộ khung quyền riêng tư hiện đại thể hiện trong thống kê toàn cầu. Qua theo dõi của UNCTAD, khoảng gần 80% các quốc gia đã có luật hoặc quy định về bảo vệ dữ liệu và quyền riêng tư, với mức độ bao phủ khác nhau giữa các khu vực. Tỷ lệ này gia tăng đều đặn cùng với quá trình số hóa xã hội. Con số không nói lên chất

lượng từng đạo luật, nhưng cho thấy xu thế *"phổ cập hóa"* của ý niệm: dữ liệu cá nhân không thể bị đối xử như một loại hàng hóa vô chủ.

Thứ tư, xuất phát từ sự cạnh tranh và đổi mới. Dữ liệu vừa là tài sản công cục bộ, vừa là tài sản tư (chi phí thu thập, xử lý, phân loại) và còn là rào cản gia nhập nếu bị tích lũy độc quyền. Pháp luật về chia sẻ dữ liệu, khả năng tương tác, tính khả chuyển và chống độc quyền dữ liệu hình thành để điều tiết hai mặt này, đó là khuyến khích lưu thông có chủ đích giữa khu vực công - tư và giữa các nền tảng, nhưng ngăn ngừa lạm dụng vị thế dữ liệu để bóp méo cạnh tranh. OECD trong các văn bản gần đây nhấn mạnh những điểm giao cắt giữa quản trị dữ liệu và quản trị AI, như quyền riêng tư, minh bạch, trách nhiệm giải trình, và các kỹ thuật tăng cường quyền riêng tư như học liên kết, mã hóa đồng hình hay MPC đóng vai trò hạ tầng, trong khi các thiết kế luật định tạo động lực áp dụng chúng ở quy mô toàn ngành.

Thứ năm, xuất phát từ địa chính trị của dữ liệu trong giai đoạn hiện nay. Dữ liệu vừa là tài sản kinh tế vừa là *"nguồn lực chiến lược"*, có thể bị khai thác trong lĩnh vực tình báo kinh tế, hướng lái đường lối chính sách, hoặc gây gián đoạn chuỗi cung ứng. Các chính phủ vì vậy có xu hướng xác lập *"chủ quyền dữ liệu"* ở những lĩnh vực quan trọng, như dữ liệu nhạy cảm công dân, hạ tầng trọng yếu, bản đồ quân sự, hệ thống nhận dạng, sinh trắc học, y tế, tài chính...

Những xu hướng trên đòi hỏi lưu trữ nội địa hay kiểm soát chuyển dữ liệu quốc tế phải đảm bảo yếu tố an ninh, an toàn dữ liệu. Song vẫn kèm theo rủi ro cô lập dữ liệu làm giảm hiệu quả kinh tế, ngăn cản hội nhập thị trường số, và khiến doanh nghiệp phải đối mặt với gánh nặng chi phí lớn để tuân thủ các quy định phức tạp của mỗi quốc gia. Các phân tích chính sách gần đây của OECD cho thấy một phổ mô hình quản trị luồng dữ liệu, từ "mở" có điều

kiện đến hạn chế có chọn lọc; bài toán tối ưu nằm ở thiết kế cơ chế *"mở đáng tin cậy"*, Đặt ra các tiêu chuẩn bảo vệ thật chặt chẽ để các nước, tổ chức và cá nhân yên tâm khi trao đổi thông tin, dữ liệu với nhau trên phạm vi quốc tế.

Thứ sáu, xuất phát từ hiệu quả của chính phủ số và dữ liệu vì lợi ích công. Dữ liệu công, dữ liệu nghiên cứu, dữ liệu môi trường, và siêu dữ liệu là nền tảng cho hoạch định chính sách dựa trên bằng chứng, quản trị rủi ro, và cá nhân hóa dịch vụ công. Trong quản trị AI, các tổ chức quốc tế nhấn mạnh vai trò của nhà nước như người tạo lập, quản lý và chia sẻ dữ liệu phục vụ mô hình AI an toàn và hữu ích; việc thiếu khung pháp lý về chia sẻ dữ liệu công sẽ chặn đứng tác động bên ngoài tích cực của dữ liệu. Khuyến nghị gần đây đề xuất các tiêu chí cho chia sẻ dữ liệu giữa cơ quan nhà nước và giữa nhà nước với doanh nghiệp, gắn với quyền riêng tư, mục đích sử dụng, và trách nhiệm giải trình.



Nhà nước đóng vai trò quan trọng trong tạo lập, quản lý và chia sẻ dữ liệu bằng trí tuệ nhân tạo - Ảnh: Internet

Nhìn từ sự vận động của kinh tế số, có thể rút ra bốn trụ cột nội dung phổ quát của luật dữ liệu hiện đại. ***Một là,*** bảo vệ dữ liệu cá nhân, xác lập các

nguyên tắc thu thập, xử lý, lưu giữ, chuyển giao dựa trên mục đích, bảo mật ngay từ thiết kế, minh bạch và quyền của chủ thể dữ liệu. ***Hai là,*** quản trị dữ liệu phi cá nhân có giá trị kinh tế - xã hội, đó là chia sẻ dữ liệu công, dữ liệu nghiên cứu, và dữ liệu doanh nghiệp - doanh nghiệp trong khuôn khổ hợp đồng công bằng, thúc đẩy đổi mới và cạnh tranh. ***Ba là,*** an ninh dữ liệu, tiêu chuẩn kỹ thuật và nghĩa vụ pháp lý về kiểm soát truy cập, mã hóa, phân quyền, quản trị nhà cung cấp, thông báo sự cố, thử nghiệm xâm nhập, và phục hồi sau thảm họa. ***Bốn là,*** liên quan đến việc chuyển dữ liệu qua biên giới, bao gồm các nội dung như: cơ chế công nhận tương đương, các nghĩa vụ ràng buộc, tiêu chuẩn hóa điều khoản hợp đồng, đánh giá tác động của việc chuyển dữ liệu và mô hình "dòng chảy dữ liệu tin cậy". Tùy theo từng hệ thống pháp luật, các nội dung này có thể được quy định trong luật khung, luật chuyên ngành hoặc phân tán trong nhiều văn bản dưới luật khác nhau.



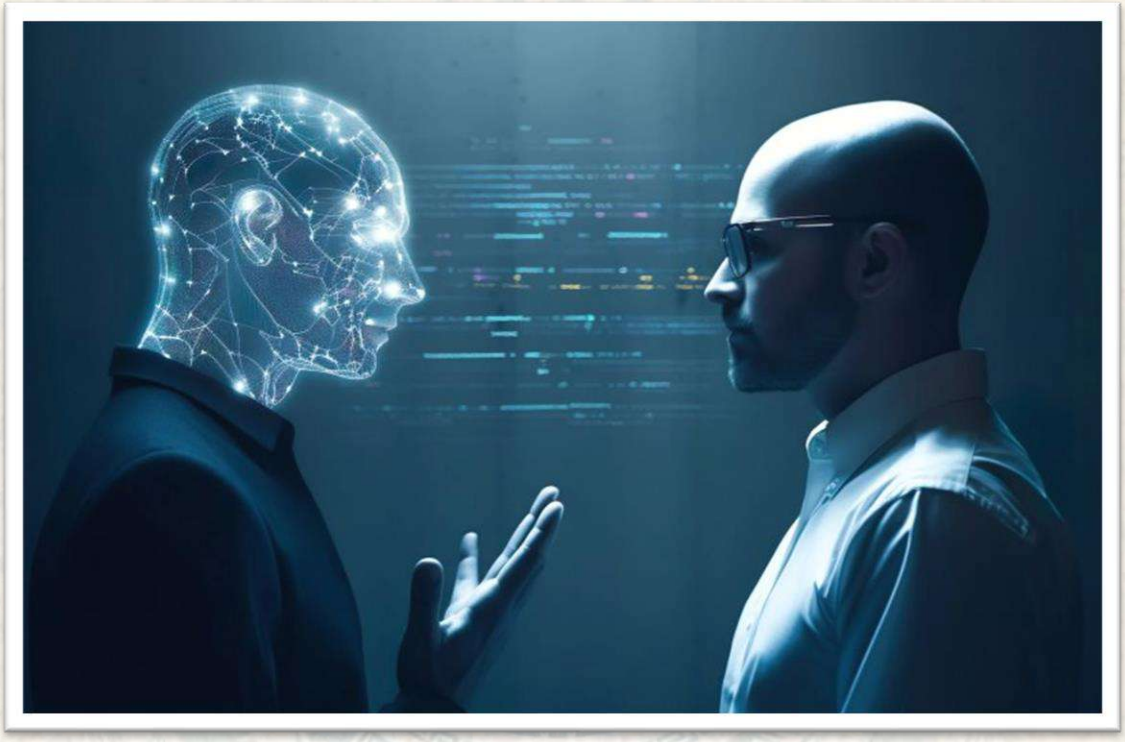
Nền kinh tế số có tác động lớn đến chuỗi giá trị xuyên quốc gia - Ảnh: Internet

Động lực kinh tế cho sự hình thành luật dữ liệu có thể thấy rõ ở nơi luồng dữ liệu dày đặc nhất, đó là các hành lang số xuyên Đại Tây Dương và

khu vực có độ mở thương mại số cao. Một phân tích về nền kinh tế số xuyên Đại Tây Dương nhấn mạnh rằng các luồng dữ liệu giữa hai bờ chiếm hơn một nửa luồng dữ liệu của châu Âu và khoảng một nửa của Hoa Kỳ, hỗ trợ mối quan hệ kinh tế quy mô hàng nghìn tỷ USD; hơn 90% doanh nghiệp hoạt động tại một bờ có trao đổi dữ liệu với bờ kia. Không có khuôn khổ pháp lý tối thiểu về chuyển dữ liệu, chuỗi giá trị xuyên biên sẽ tắc nghẽn.

Ở chiều ngược lại, những thiệt hại kinh tế do sự cố dữ liệu đặt ra chi phí cơ hội rất lớn nếu không có luật. Khi chi phí trung bình một vụ vi phạm tiệm cận 5 triệu USD và những vụ việc đặc thù (như phần mềm độc hại, lừa đảo qua thư điện tử, đánh cắp thông tin cá nhân) có chi phí cao hơn nữa, doanh nghiệp và nhà đầu tư đối diện rủi ro mà họ khó tự xử lý nếu không có nghĩa vụ pháp lý rõ ràng. Trong thời gian ngắn hạn, việc để thị trường tự điều chỉnh cũng có thể thúc đẩy doanh nghiệp đầu tư vào an ninh thông tin. Tuy nhiên, thực tế cho thấy động lực này thường không đạt mức tối ưu vì tồn tại tác động tiêu cực ra bên ngoài, như thiệt hại do rò rỉ dữ liệu thường ảnh hưởng đến bên thứ ba (như khách hàng, đối tác), trong khi lợi ích của việc phòng ngừa lại chủ yếu thuộc về doanh nghiệp. Điều này tạo ra *"khoảng cách đầu tư an ninh"*. Luật dữ liệu, với cơ chế chế tài và nghĩa vụ thông báo sự cố, được thiết kế để thu hẹp khoảng trống đó. Một khía cạnh ngày càng được chú ý là trí tuệ nhân tạo. Trí tuệ nhân tạo phụ thuộc vào dữ liệu cả về lượng và chất, đồng thời tạo ra rủi ro mới cho quyền riêng tư, thiên lệch, và an toàn hệ thống. Các tổ chức quốc tế ghi nhận mức gia tăng đột biến các *"sự cố AI"* trong giai đoạn bùng nổ mô hình tạo sinh, phản ánh sự đan cài giữa dữ liệu huấn luyện, dữ liệu suy luận và môi trường triển khai. Trong bối cảnh ấy, nhiều báo cáo nhấn mạnh nhu cầu điều phối giữa khung quyền riêng tư và khung quản trị AI, thay vì phát triển hai đường ray rời rạc. Luật dữ liệu hiện

đại vì thế không thể chỉ là bảo vệ dữ liệu cá nhân; nó phải trở thành *"hợp đồng xã hội dữ liệu - AI"*, xác lập nguyên tắc dùng dữ liệu công bằng, minh bạch, giải thích được, và chịu trách nhiệm, đồng thời thúc đẩy các công nghệ tăng cường quyền riêng tư và các hình thức chia sẻ dữ liệu an toàn để vẫn bảo toàn năng lực đổi mới.



Trí tuệ nhân tạo có thể mang nhiều thách thức, rủi ro về dữ liệu riêng tư - Ảnh: Kiểm toán Nhà nước

Không thể bỏ qua yếu tố môi trường và tính bền vững khi bàn về dữ liệu. Sự phình to của trung tâm dữ liệu, chuỗi cung ứng phần cứng, và tiêu thụ năng lượng - nước làm dấy lên câu hỏi về *"dấu chân môi trường"* của nền kinh tế dữ liệu. Ấn phẩm kinh tế số gần đây nhấn mạnh thách thức cân bằng giữa tăng trưởng số và mục tiêu bền vững, chỉ ra cả tác động tích cực (tối ưu hóa năng lượng nhờ phân tích dữ liệu) và tiêu cực (tiêu thụ tài nguyên, phát thải gián tiếp). Từ góc độ lập pháp, điều này dịch thành yêu cầu công khai chỉ số bền vững của hạ tầng dữ liệu và lồng ghép mục tiêu môi trường vào chính sách

khuyến khích - ví dụ điều kiện ưu đãi cho trung tâm dữ liệu gắn với hiệu suất năng lượng, tái sử dụng nhiệt thải, hay tiêu chuẩn nước làm mát.

Bối cảnh chính sách hiện nay có thể tóm lược bằng ba xu hướng hội tụ. ***Thứ nhất*** là *"phổ cập hóa"* luật bảo vệ dữ liệu cá nhân. Tỷ lệ các quốc gia có luật hoặc quy định về quyền riêng tư - bảo vệ dữ liệu tiến dần đến ngưỡng phổ quát, bất chấp mức độ chín muồi khác nhau. Sự phổ cập không chỉ do áp lực xã hội, mà còn do động lực thương mại: muốn tham gia chuỗi giá trị số toàn cầu, một nền kinh tế buộc phải chứng minh mức bảo vệ tối thiểu tương thích với đối tác. ***Thứ hai*** là *"thiết kế tin cậy"* cho chuyển dữ liệu quốc tế. Cốt lõi của xu hướng này là xây dựng cơ chế đánh giá tương đương, hợp đồng chuẩn, nghĩa vụ ràng buộc và phương tiện kỹ thuật để giảm rủi ro khi dữ liệu vượt biên, từ đó đạt "lưu thông có tin cậy". ***Thứ ba*** là *"điều tiết theo rủi ro"* trong kỷ nguyên AI: phân tầng nghĩa vụ theo mức rủi ro của hệ thống và mục đích xử lý, kết nối liền mạch giữa khung dữ liệu và khung AI để tránh "song trùng" nhưng cũng không để "vùng xám" pháp lý.

Một câu hỏi trọng yếu là làm thế nào viết luật dữ liệu để vừa thúc đẩy đổi mới vừa bảo vệ quyền. Câu trả lời nằm ở tư duy "dữ liệu như một hệ sinh thái", trong đó quyền và nghĩa vụ được phân bổ theo vai trò: người kiểm soát, người xử lý, nhà cung cấp hạ tầng, và chủ thể dữ liệu. Luật cần thiết lập nghĩa vụ gắn với mục tiêu, không gắn với công nghệ cụ thể, để đủ linh hoạt trước biến động nhanh của kỹ thuật. Ví dụ, thay vì yêu cầu "mã hóa theo tiêu chuẩn X", luật nên đặt mục tiêu "bảo đảm bí mật và tính toàn vẹn ở mức Y" và công nhận danh mục biện pháp tương đương (mã hóa khóa quản lý an toàn, kiểm soát truy cập dựa trên thuộc tính, phân tách môi trường xử lý, ẩn danh hay giả danh mạnh, kiểm toán truy cập). Quan điểm dựa trên mục tiêu giảm nguy cơ "tụt hậu công nghệ" của văn bản pháp luật.

Ở tầng thực thi, kinh nghiệm quốc tế gợi ý bốn then chốt giúp luật dữ liệu không trở thành *"giấy trắng mực đen"*. ***Một là*** kiến trúc thể chế: cơ quan giám sát độc lập, có thẩm quyền điều tra, phạt, ban hành hướng dẫn, và tham gia hợp tác quốc tế. ***Hai là*** năng lực thực thi: đầu tư vào nhân lực điều tra số, công cụ giám sát tuân thủ, và cơ chế xử phạt có tính răn đe tương xứng với quy mô kinh doanh dựa trên dữ liệu. ***Ba là*** hạ tầng "định danh và chuẩn hóa": từ định nghĩa dữ liệu nhạy cảm, tiêu chuẩn giao tiếp lập trình, đến định dạng siêu dữ liệu phục vụ kiểm soát mục đích sử dụng, truy vết và khả chuyển. ***Bốn là*** cơ chế hợp tác xuyên biên giới, bởi phần lớn tranh chấp và vi phạm đều mang tính xuyên biên giới; nguyên tắc "một cửa" phối hợp giữa cơ quan đồng đẳng các nước và cơ chế trợ giúp pháp lý lẫn nhau trở thành điều kiện tiên quyết.



Việc xây dựng luật dữ liệu ở các quốc gia gặp nhiều khó khăn, thách thức - Ảnh: Trần Cường

Có thể đặt vấn đề ngược lại: nếu không có luật dữ liệu, điều gì sẽ xảy ra? ***Thứ nhất,*** chi phí giao dịch tăng vọt do bất định pháp lý. Doanh nghiệp toàn

cầu phải tự đàm phán hàng nghìn điều khoản hợp đồng thiếu chuẩn mực, làm chậm giao dịch số và kìm hãm đổi mới. ***Thứ hai,*** "chủ nghĩa cát cứ dữ liệu": mỗi tổ chức tự xây "thành lũy" dữ liệu, từ chối chia sẻ vì sợ rủi ro pháp lý, kéo theo mất mát phúc lợi xã hội từ dữ liệu công và dữ liệu nghiên cứu. ***Thứ ba,*** gia tăng rủi ro hệ thống: không có chuẩn bắt buộc về thông báo sự cố, kiểm soát truy cập, hay thử nghiệm xâm nhập, hệ sinh thái dữ liệu dễ biến thành *"khu dân cư không có mã bưu chính"*, nơi kẻ xấu di chuyển không bị truy dấu. Các số liệu về chi phí vi phạm dữ liệu và gia tăng tấn công lợi dụng AI là lời cảnh báo thực chứng rằng chi phí *"không có luật"* rất hữu hình.



Cơ chế thử nghiệm có kiểm soát (sandbox) - Ảnh: Thư viện pháp luật

Một phản biện thường gặp là luật dữ liệu có thể "đóng khung" đổi mới. Điều này đúng nếu luật bị thiết kế theo tư duy cấm đoán hoặc "đóng băng" kỹ thuật. Nhưng luật dữ liệu không nhất thiết phải như vậy. Ngược lại, luật tốt tạo ra "thị trường tin cậy": xác lập quyền, nghĩa vụ và cơ chế trách nhiệm để các bên yên tâm đầu tư dài hạn. Về mặt vi mô, doanh nghiệp có thể hoạch định kiểm soát nội bộ, đầu tư bảo mật, và thiết kế sản phẩm *"privacy by design"* rõ ràng. Về mặt vĩ mô, các nền kinh tế có thể thiết lập cơ chế công

nhận tương đương, thí điểm cơ chế thử nghiệm có kiểm soát, và chuẩn hóa kỹ thuật để giảm chi phí tuân thủ. Khi OECD nêu rõ chủ trương thúc đẩy *"lưu thông có tin cậy"*, điều được giả định ở đó là một thị trường dữ liệu mở - nhưng có luật.

Trong thực tiễn, thế giới đang hội tụ về vài loại chính sách dữ liệu, dù mỗi nơi có sắc thái riêng. Có loại nhấn mạnh quyền cá nhân và trách nhiệm doanh nghiệp, đặt ra nguyên tắc xử lý toàn cục kèm cơ chế chuyển dữ liệu có điều kiện; có loại thiên về quản lý nhà nước và an ninh, thiết lập rào cản vững chãi với dữ liệu được coi là nhạy cảm; có loại phân mảnh theo lĩnh vực với rổ quy định chuyên ngành. Bất kể khác biệt, đều có những điểm gặp nhau: không ai phủ nhận quyền tối thiểu của chủ thể dữ liệu; không ai phủ nhận trách nhiệm thông báo và khắc phục khi vi phạm; không ai phủ nhận tầm quan trọng của tính tương thích kỹ thuật và công nhận lẫn nhau để thương mại số diễn ra.

Tuy nhiên, sự hội tụ đó diễn ra trong bối cảnh phân mảnh thể chế ngày càng hiện hữu. Khi mỗi khu vực xây khung pháp lý với *"từ điển"* riêng, doanh nghiệp đa quốc gia đối diện ma trận tuân thủ. Chiến lược vượt ma trận gồm ba lớp: "*thiết kế vì toàn cầu ngay từ đầu"* trong kiến trúc dữ liệu; "địa phương hóa tối thiểu cần thiết" bằng cách phân loại dữ liệu và áp dụng biện pháp tăng cường (giả danh, phân tách khóa, khoá vùng); và *"đồng quản trị"* với mạng lưới nhà cung cấp và đối tác. Ở cấp quốc gia, chính sách khôn ngoan là tham gia tích cực các diễn đàn đa phương để hình thành "cửa sổ" công nhận tương đương và thỏa thuận song/đa phương về chuyển dữ liệu, thay vì đơn độc.

Một khía cạnh khác thường bị bỏ quên là *"kinh tế học cùng với sự tin cậy"*. Tin cậy không tự nhiên sinh ra; nó là sản phẩm của thể chế. Khi người

dùng tin rằng dữ liệu của họ được bảo vệ, họ tham gia nhiều hơn vào nền kinh tế số; khi doanh nghiệp tin rằng đối tác chịu trách nhiệm, họ chia sẻ dữ liệu để tối ưu chuỗi cung ứng; khi chính phủ tin rằng doanh nghiệp tuân thủ, họ mở dữ liệu công có giá trị để cộng sinh. Nhiều minh chứng cho mối liên hệ giữa tin cậy và hiệu quả thị trường xuất hiện trong các phân tích về thương mại số và luồng dữ liệu. Luật dữ liệu, do đó, chính là chính sách công tạo dựng vốn xã hội dưới dạng tin cậy số - một loại tài sản vô hình nhưng đo đếm được qua chỉ số tham gia thương mại số, năng suất, và mức độ đổi mới.



Các công ty đa quốc gia gặp nhiều khó khăn về pháp lý có liên quan đến dữ liệu - Ảnh: Báo Công an nhân dân

Song hành với thiết kế thể chế là thiết kế kỹ thuật. *"Tuân thủ theo mặc định"* (compliance by default) không thể đạt được nếu hệ thống dữ liệu không được xây dựng theo mô hình tối thiểu hóa, phân quyền, ghi vết và xác minh. Luật đặt mục tiêu, kỹ thuật hiện thực hóa mục tiêu. Các công nghệ tăng cường quyền riêng tư (PETs) - như học liên kết, vi sai riêng tư, mã hóa

đồng hình, tính toán đa bên an toàn - dịch hóa yêu cầu pháp lý thành vận hành an toàn ở cấp hệ thống. Khi báo cáo chính sách đề cập thẳng đến vai trò của PETs trong chia sẻ dữ liệu và quản trị AI, đó không chỉ là "*lời kêu gọi công nghệ*" mà là sự thừa nhận rằng luật dữ liệu và kỹ thuật là hai nửa của cùng một đồng xu.



Công nghệ tăng cường quyền riêng tư (PET) - Ảnh: Marketing AI

Để đánh giá hiệu quả, một chủ thể dữ liệu cần sử dụng các chỉ báo. Một số chỉ báo đề xuất gồm: tỷ lệ doanh nghiệp có chương trình quản trị dữ liệu và quyền riêng tư đạt chuẩn; thời gian trung vị phát hiện - khắc phục sự cố; tỷ lệ áp dụng PETs; khối lượng dữ liệu công mở sử dụng lại; số lượng - giá trị giao dịch dữ liệu B2B theo khung tiêu chuẩn; số vụ công nhận tương đương chuyển dữ liệu; và mức phạt - mức tuân thủ theo ngành. Khi các báo cáo cho thấy trung bình chi phí vi phạm đang tăng, kèm sự gia tăng các sự cố liên quan AI, điều đó là lời nhắc rằng chỉ báo rủi ro - chứ không phải ý chí - sẽ *"điều chỉnh"* luật dữ liệu tiến hóa theo hướng thực chất.

Tuy nhiên chúng ta cũng cần lưu ý đến tính bao trùm. Khoảng cách số - 2,6 tỷ người còn ngoại tuyến vào năm 2024 là một nhắc nhở lớn rằng luật dữ liệu không thể trở thành rào cản gia nhập của doanh nghiệp siêu nhỏ, nhỏ và vừa (MSME) hay nhóm dễ bị tổn thương. Luật tốt phải tối giản gánh nặng tuân thủ với chủ thể rủi ro thấp và cung cấp công cụ thực thi phù hợp năng lực. Trách nhiệm của nhà nước là hỗ trợ khu vực tư xây dựng năng lực, cung cấp mẫu điều khoản chuẩn, và thiết kế hạ tầng dùng chung (chẳng hạn dịch vụ ủy thác dữ liệu, kho khóa mã hóa, cơ chế nhận dạng điện tử) để giảm chi phí biên tuân thủ.



Trách nhiệm của Nhà nước thiết kế hạ tầng kỹ thuật dùng chung - Ảnh: Bộ Khoa học và Công nghệ

Từ góc nhìn thương mại, một đường hướng đang nổi là *"chuyển dữ liệu có điều kiện"* kết hợp với thỏa thuận công nhận tương đương và hợp đồng chuẩn. Sự phối hợp đa phương được thúc đẩy bởi các tổ chức như OECD, vốn đặt trọng tâm vào hài hòa hóa khái niệm và phương pháp đánh giá rủi ro, tránh "đánh đố" doanh nghiệp khi phải diễn giải các thuật ngữ cốt lõi

(mục đích phù hợp, tối thiểu hóa, tính cần thiết, lợi ích hợp pháp, tác động đến quyền). Báo cáo chuyên đề về luồng dữ liệu của OECD phác thảo các cách tiếp cận trong nước đối với kiểm soát chuyển dữ liệu và yêu cầu lưu trữ cục bộ, đồng thời cảnh báo chi phí thặng dư đối với người tiêu dùng - doanh nghiệp nếu thiết kế rào cản thiếu cân nhắc.

Nhìn rộng hơn, luật dữ liệu phản chiếu sự trưởng thành của *"trật tự thông tin"* quốc tế. Ở thế kỷ XX, luật thương mại hàng hóa - dịch vụ và luật đầu tư định hình toàn cầu hóa; ở thế kỷ XXI, luật dữ liệu - cùng với luật AI - đang vẽ đường biên mới của hội nhập. Khi các tổ chức đa phương nói đến "dòng chảy dữ liệu tự do có tin cậy", đó là tuyên ngôn chính trị - pháp lý rằng hội nhập số chỉ bền vững nếu quyền và an ninh được bảo đảm. Để biến tuyên ngôn thành hiện thực, cần các cơ chế thực thi xuyên biên, từ hợp tác giữa cơ quan bảo vệ dữ liệu, cơ quan cạnh tranh, đến hợp tác kỹ thuật về tiêu chuẩn và thử nghiệm.

Những dữ liệu minh họa sau đây nhấn mạnh tầm quan trọng của pháp lý có liên quan đến dữ liệu: năm 2024, có 5,5 tỷ người trực tuyến; thương mại điện tử doanh nghiệp đạt khoảng 27 nghìn tỷ USD năm 2022; luồng dữ liệu xuyên biên giới đã tạo ra giá trị hàng nghìn tỷ USD ngay từ giữa thập niên 2010; lưu lượng dữ liệu di động bình quân gần 13 GB/kết nối; chi phí vi phạm dữ liệu trung bình tiến sát 5 triệu USD và chịu ảnh hưởng gia tăng bởi sự cố liên quan AI; và khoảng gần 80% quốc gia đã có khung luật hoặc quy định về bảo vệ dữ liệu. Mỗi chỉ báo là một *"lý do"* của luật dữ liệu: để thị trường số hoạt động trơn tru, để rủi ro được nội bộ hóa đúng chỗ, để quyền con người được tôn trọng, và để hội nhập diễn ra có tin cậy.

Tóm lại, có thể khẳng định rằng luật dữ liệu là tất yếu lịch sử của quá trình số hóa toàn cầu. Nó không phải *"vành đai an toàn"* lắp thêm cho cỗ xe

số, mà là phần khung chịu lực, cho phép xe chạy nhanh hơn mà không văng khỏi đường. Ở nơi dữ liệu là đầu vào của sản xuất tri thức, luật dữ liệu là công cụ phân bổ quyền lợi - nghĩa vụ; ở nơi dữ liệu là tài sản chiến lược, luật dữ liệu là hàng rào an ninh mềm; ở nơi dữ liệu là mạch máu thương mại số, luật dữ liệu là hệ tuần hoàn bảo đảm lưu thông có tin cậy; ở nơi dữ liệu là tiếng nói cá nhân, luật dữ liệu là tấm khiên bảo vệ phẩm giá con người.



Một hệ thống pháp lý về dữ liệu vững chắc sẽ tạo nên những thành tựu đáng kể - Ảnh: Tạp chí Pháp lý

Vì thế, khi các quốc gia xây dựng và ban hành chính sách - pháp luật về dữ liệu, họ không chỉ làm công việc "theo kịp công nghệ". Họ đang viết nên những quy tắc nền tảng của kỷ nguyên thông tin, nơi tăng trưởng, quyền và an ninh phải được tối ưu cùng lúc. Con đường phía trước đòi hỏi một cách tiếp cận dựa trên rủi ro, dựa trên bằng chứng, trung lập công nghệ, và lấy tin cậy làm thước đo. Cần sự gắn kết giữa luật dữ liệu và luật AI; cần đầu tư thể

chế và kỹ thuật để biến chuẩn mực thành vận hành; cần hợp tác đa phương để "nối cầu" giữa các hệ hình pháp lý; và cần một tầm nhìn coi dữ liệu không chỉ là "dầu mỏ mới", mà là hạ tầng mềm của một xã hội cởi mở, an toàn và thịnh vượng.

Nếu phải tóm gọn toàn bộ xu hướng toàn cầu trong một mệnh đề, đó là: mọi hệ thống pháp luật đang đi tới một điểm cân bằng động, ở đó quyền riêng tư và an ninh được mở rộng chứ không thu hẹp, còn lưu thông dữ liệu được bảo đảm nhờ tin cậy chứ không phải bất chấp tin cậy. Và chính tại điểm cân bằng đó, nhà nước, doanh nghiệp và công dân cùng trở thành đồng tác giả của *"hợp đồng xã hội dữ liệu"* cho thời đại mới.

1.3.1.2. Bối cảnh trong nước

- Yêu cầu từ định hướng chuyển đổi số và kinh tế số

Trong bối cảnh chuyển đổi số sâu rộng và hội nhập quốc tế mạnh mẽ, Việt Nam đang đối mặt với những cơ hội và thách thức lớn trong việc xây dựng một nền kinh tế số bền vững. Chính phủ Việt Nam đã nhận thức rõ tầm quan trọng của chuyển đổi số, coi đây là yếu tố quyết định để phát triển trong kỷ nguyên số. Chương trình Chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030 (Quyết định số 749/QĐ-TTg ngày 03/6/2020) khẳng định rõ rằng dữ liệu chính là *"tài nguyên mới"*, đóng vai trò then chốt trong việc xây dựng Chính phủ số, kinh tế số và xã hội số.

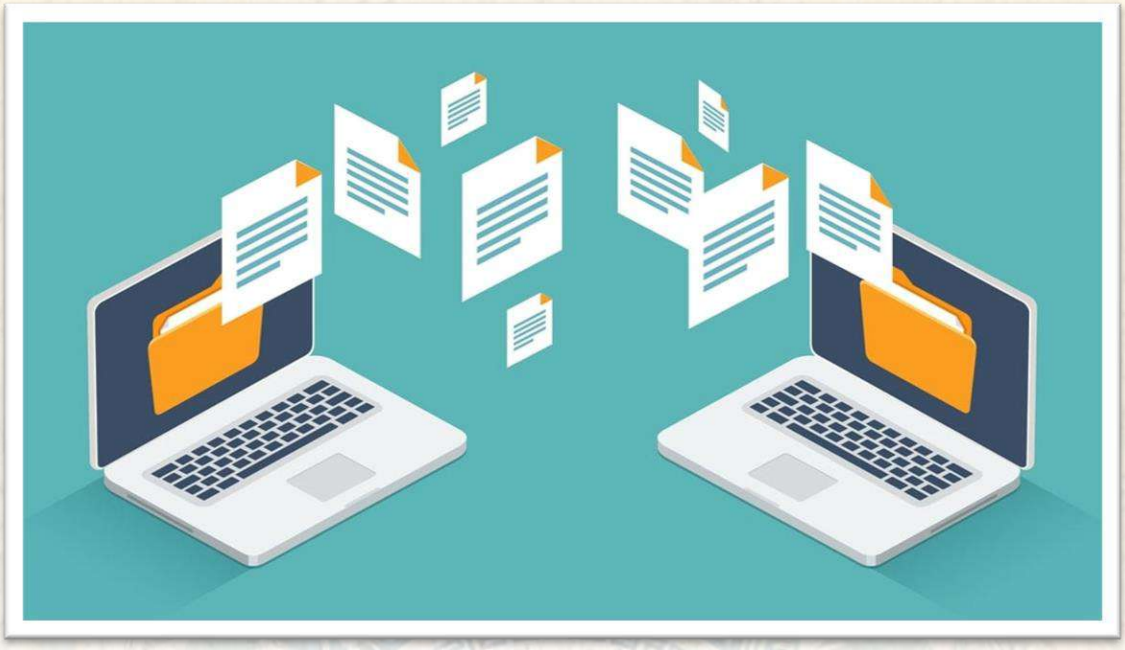
Trong chiến lược chuyển đổi số, Việt Nam đặt ra mục tiêu quan trọng là hoàn thiện cơ sở dữ liệu quốc gia, xây dựng hạ tầng số tích hợp và đảm bảo kết nối, chia sẻ dữ liệu giữa các cơ quan nhà nước, doanh nghiệp và người dân. Đây là một bước đi quan trọng trong việc xây dựng một hệ sinh thái dữ liệu có tính đồng bộ và khả năng tương tác cao. Cùng với đó, kinh tế số dự báo sẽ đóng góp hơn 20% vào GDP của đất nước vào năm 2025, mở

ra triển vọng lớn cho nền kinh tế số, với các ứng dụng mạnh mẽ trong các lĩnh vực như thanh toán điện tử, giao dịch trực tuyến, chăm sóc sức khỏe và giáo dục qua nền tảng số.



Hội nghị tổng kết năm 2024 và triển khai nhiệm vụ năm 2025 đặt mục tiêu kinh tế số sẽ chiếm 30 - 35% GDP vào năm 2030, khi đó Việt Nam sẽ lọt Top 30 toàn cầu - Ảnh: VGP/TH

Tuy nhiên, để thực hiện thành công các mục tiêu trên, một điều kiện tiên quyết không thể thiếu là phải có một hành lang pháp lý rõ ràng, minh bạch và khả thi để điều chỉnh việc thu thập, xử lý và chia sẻ dữ liệu, đặc biệt là trong bối cảnh quyền riêng tư của công dân ngày càng trở thành vấn đề quan trọng. Dữ liệu tại Việt Nam hiện nay còn mang tính phân mảnh, thiếu tính kết nối liên thông và tiêu chuẩn hóa giữa các cơ quan, ngành nghề khác nhau. Các dữ liệu này phần lớn chưa được quản lý một cách đồng bộ, và người dân còn thiếu quyền kiểm soát hoặc thông tin đầy đủ về dữ liệu cá nhân của mình, dẫn đến những mối lo ngại về bảo mật và quyền riêng tư.



Dữ liệu tại Việt Nam hiện nay còn mang tính phân mảnh, thiếu tính kết nối liên thông và tiêu chuẩn hóa - Ảnh: Smart Industry

Bên cạnh đó, nhiều doanh nghiệp và tổ chức vẫn chưa tuân thủ các nguyên tắc cơ bản về bảo mật dữ liệu, không có cơ chế minh bạch về việc thu thập và sử dụng dữ liệu cá nhân, cũng như thiếu cơ chế bảo vệ quyền riêng tư của người dùng. Những bất cập này đã tạo ra một lỗ hổng lớn trong công tác quản lý và bảo vệ dữ liệu, làm gia tăng rủi ro cho cả cá nhân và tổ chức trong việc đảm bảo quyền lợi hợp pháp của mình trong môi trường số.

- Rủi ro về an ninh dữ liệu và vi phạm quyền riêng tư

Trong những năm gần đây, tình trạng rò rỉ và lạm dụng dữ liệu cá nhân tại Việt Nam ngày càng phổ biến, làm dấy lên những lo ngại sâu sắc về an ninh mạng và vi phạm quyền riêng tư. Một ví dụ điển hình là vụ việc rò rỉ 17GB dữ liệu cá nhân của khách hàng ngân hàng vào năm 2023, bao gồm các thông tin như căn cước công dân, số tài khoản ngân hàng, email và địa chỉ thường trú (theo Báo Tuổi Trẻ). Ngoài ra, các vụ lừa đảo công nghệ cao qua điện thoại và mạng xã hội cũng đã lợi dụng dữ liệu cá nhân bị đánh cắp

để giả danh cơ quan nhà nước, gây thiệt hại tài sản lên đến hàng trăm tỷ đồng mỗi năm.

Không chỉ có vậy, nhiều ứng dụng di động và sàn thương mại điện tử không tuân thủ các nguyên tắc thu thập dữ liệu như yêu cầu minh bạch, mục đích cụ thể, và xin ý kiến đồng thuận từ người sử dụng. Hậu quả là người dùng thường không được thông báo về cách thức dữ liệu của họ sẽ được sử dụng hoặc không có lựa chọn từ chối, dẫn đến việc khai thác dữ liệu cá nhân sai mục đích hoặc bị rò rỉ ra ngoài biên giới quốc gia.

Trước bối cảnh đó, việc Quốc hội khóa XV thông qua Luật Dữ liệu năm 2024 (dự kiến có hiệu lực từ ngày 01/7/2025) và việc Bộ Công an tiếp tục hoàn thiện dự thảo Luật Bảo vệ dữ liệu cá nhân là bước đi chiến lược nhằm thiết lập lại trật tự pháp lý đối với tài nguyên dữ liệu số và quyền riêng tư số tại Việt Nam. Hai đạo luật này sẽ không chỉ là công cụ pháp lý giúp bảo vệ quyền con người trong môi trường số mà còn góp phần bảo vệ chủ quyền dữ liệu quốc gia trước các nguy cơ xuyên biên giới.



Tình trạng rò rỉ và lạm dụng dữ liệu cá nhân tại Việt Nam ngày càng phổ biến - Ảnh: Kaspersky

- Hành lang pháp lý còn rời rạc và chưa theo kịp quốc tế

Trước năm 2024, Việt Nam chưa có một đạo luật thống nhất và toàn diện điều chỉnh về dữ liệu và bảo vệ dữ liệu cá nhân. Các quy định pháp lý hiện tại chủ yếu được phân tán trong nhiều văn bản khác nhau, mỗi văn bản chỉ điều chỉnh một khía cạnh riêng lẻ, thiếu tính hệ thống và liên thông. Điều này gây khó khăn trong việc xây dựng một hệ thống pháp lý toàn diện, hiện đại và đáp ứng được yêu cầu quản lý dữ liệu trong nền kinh tế số hiện đại.

Cụ thể, Luật Giao dịch điện tử năm 2005, dù đã được sửa đổi vào năm 2023, vẫn chỉ tập trung vào cơ chế pháp lý cho các giao dịch điện tử, chữ ký số và giao dịch giữa các bên, chưa mở rộng phạm vi điều chỉnh đến các vấn đề quan trọng như quyền sở hữu dữ liệu, dữ liệu như tài sản số hay các vấn đề liên quan đến quản trị dữ liệu trong nền kinh tế số. Luật An ninh mạng năm 2018, mặc dù có quy định về bảo vệ dữ liệu cá nhân, nhưng chủ yếu tập trung vào mục tiêu an ninh quốc gia và chưa thiết lập được cơ chế bảo vệ quyền riêng tư của công dân trong không gian số. Mặc dù Nghị định số 13/2023/NĐ-CP đã bước đầu thiết lập các quy định cụ thể về bảo vệ dữ liệu cá nhân, nhưng do là văn bản dưới luật, các quy định này vẫn thiếu tính ràng buộc mạnh mẽ và chưa tạo ra cơ chế giám sát độc lập để thực thi quyền riêng tư cá nhân một cách hiệu quả.

Với những thách thức đó, việc ban hành Luật Dữ liệu năm 2024 là bước đi quan trọng để xây dựng một hệ thống pháp lý đầy đủ, thống nhất và toàn diện, đáp ứng yêu cầu quản lý và bảo vệ dữ liệu cá nhân trong môi trường số. Đạo luật này sẽ giúp phân loại rõ các loại dữ liệu, xác định quyền sở hữu và trách nhiệm pháp lý của các chủ thể liên quan, qua đó tạo nền tảng pháp lý cho việc xây dựng thị trường dữ liệu và đảm bảo quyền lợi của công dân trong kỷ nguyên số.

Việc hoàn thiện các cơ chế chia sẻ, khai thác và chuyển giao dữ liệu xuyên biên giới, cùng với việc thiết lập hệ thống Trung tâm Dữ liệu quốc gia và các hạ tầng dữ liệu chuyên ngành, sẽ không chỉ bảo đảm an toàn, bảo mật mà còn thúc đẩy sự phát triển bền vững của nền kinh tế số và bảo vệ chủ quyền dữ liệu quốc gia trong bối cảnh toàn cầu hóa.

Việc xây dựng và hoàn thiện pháp luật về dữ liệu ở Việt Nam không chỉ là yêu cầu cấp thiết trong bối cảnh chuyển đổi số mà còn là yếu tố then chốt để bảo đảm quyền lợi hợp pháp của người dân, đồng thời bảo vệ an ninh quốc gia trong thời đại số. Trước những thách thức và rủi ro ngày càng gia tăng từ việc quản lý và bảo vệ dữ liệu, việc thông qua Luật Dữ liệu và Luật Bảo vệ dữ liệu cá nhân là bước đi chiến lược không thể thiếu. Những đạo luật này sẽ tạo dựng hành lang pháp lý vững chắc, giúp Việt Nam vừa theo kịp xu thế phát triển toàn cầu, vừa bảo vệ được quyền riêng tư của công dân trong môi trường số, đồng thời khẳng định chủ quyền dữ liệu quốc gia.

Cùng với đó, việc triển khai các quy định rõ ràng, minh bạch và đồng bộ về quản trị dữ liệu không chỉ là yêu cầu cấp bách mà còn là điều kiện tiên quyết để xây dựng một nền tảng số bền vững, bảo vệ lợi ích quốc gia trong kỷ nguyên số. Việc thực hiện những bước đi này sẽ không chỉ giúp tạo ra môi trường số an toàn, bảo mật mà còn mở ra cơ hội phát triển mạnh mẽ cho nền kinh tế dữ liệu, góp phần vào sự thịnh vượng chung của xã hội. Thực tế đã chỉ ra rằng nếu không có khung pháp lý phù hợp, việc quản lý và bảo vệ dữ liệu sẽ trở thành một thách thức lớn, đe dọa đến sự phát triển bền vững của đất nước. Chính vì thế, việc xây dựng và hoàn thiện pháp luật về dữ liệu không chỉ là một nhiệm vụ cấp thiết mà còn là trách nhiệm lớn lao đối với tương lai của nền kinh tế số Việt Nam.

1.3.2. Cơ sở chính trị

Trong những năm qua, Đảng, Nhà nước đã có nhiều chủ trương, giải pháp đẩy mạnh ứng dụng khoa học, công nghệ phục vụ công cuộc chuyển đổi số quốc gia, xây dựng Chính phủ điện tử, Chính phủ số, kinh tế số, xã hội số như:

Một là, Điều 62 Hiến pháp năm 2013 quy định: ***(1)*** Phát triển khoa học và công nghệ là quốc sách hàng đầu, giữ vai trò then chốt trong sự nghiệp phát triển kinh tế - xã hội của đất nước; ***(2)*** Nhà nước ưu tiên đầu tư và khuyến khích tổ chức, cá nhân đầu tư nghiên cứu, phát triển, chuyển giao, ứng dụng có hiệu quả thành tựu khoa học và công nghệ; bảo đảm quyền nghiên cứu khoa học và công nghệ; bảo hộ quyền sở hữu trí tuệ; ***(3)*** Nhà nước tạo điều kiện để mọi người tham gia và được thụ hưởng lợi ích từ các hoạt động khoa học và công nghệ. Có thể thấy rằng, Điều 62 Hiến pháp năm 2013 đã khẳng định khoa học và công nghệ cũng là một trong những quốc sách hàng đầu, giữ vai trò then chốt trong sự nghiệp phát triển kinh tế - xã hội của đất nước.

Thật vậy, trong kỷ nguyên số, dữ liệu đã trở thành nguồn *"năng lượng mới"* - nguồn nhiên liệu thiết yếu cho mọi nghiên cứu và ứng dụng khoa học - công nghệ, từ trí tuệ nhân tạo đến Internet vạn vật kết nối. Khi Hiến pháp đặt khoa học - công nghệ là quốc sách hàng đầu, điều này hàm chứa yêu cầu phải xây dựng nền tảng dữ liệu vững chắc để thúc đẩy nghiên cứu và đổi mới sáng tạo. Nếu không có các quy định chặt chẽ về quản lý, chia sẻ và bảo vệ dữ liệu, thì các luận cứ và kết quả nghiên cứu sẽ thiếu tính minh bạch, đồng bộ và khó bảo vệ quyền lợi của chủ thể tạo lập dữ liệu.

Với vai trò là văn bản pháp lý cao nhất, thể hiện tinh thần xây dựng xã hội công bằng, dân chủ, văn minh, Hiến pháp năm 2013 đặt ra các định hướng, nguyên tắc cụ thể để bảo vệ quyền riêng tư và dữ liệu cá nhân của

công dân. Đối với nguyên tắc "ưu tiên đầu tư và bảo hộ quyền sở hữu trí tuệ", Luật Dữ liệu phải quy định cơ chế bảo vệ "tài sản dữ liệu", bao gồm cả dữ liệu đào tạo mô hình, dữ liệu chuyên ngành y tế, giáo dục... Nhà nước cần ban hành chính sách ưu đãi về kinh phí, hạ tầng thu thập, lưu trữ, xử lý và chia sẻ dữ liệu, đồng thời bảo vệ người tạo lập dữ liệu trước nguy cơ khai thác trái phép hoặc sao chép không bản quyền. Bên cạnh đó, nguyên tắc "mọi người tham gia và được thụ hưởng lợi ích từ hoạt động khoa học - công nghệ" đòi hỏi dữ liệu công và dữ liệu mở phải được xác định rõ phạm vi, mô hình chia sẻ và cơ chế giám sát. Chỉ khi đó, cá nhân, doanh nghiệp, nhất là các doanh nghiệp vừa và nhỏ mới có thể tiếp cận nguồn thông tin quan trọng để khởi nghiệp, nghiên cứu và phát triển sản phẩm dịch vụ mới. Luật Dữ liệu phải làm rõ khái niệm, nguyên tắc "mở - chung - bảo mật", đồng thời quy định cơ chế phối hợp giữa cơ quan nhà nước và tổ chức tư nhân để phân phối lợi ích một cách công bằng và minh bạch.



Dữ liệu là đối tượng bảo vệ chính của Luật dữ liệu - Ảnh: Internet

Để hiện thực hóa các định hướng trên, Quốc hội, Chính phủ cần tạo hành lang pháp lý cho "quốc sách" trong kỷ nguyên số, đó là một khung quản lý chuyên biệt, đầy đủ và thống nhất. Chính sách pháp luật về dữ liệu cần làm rõ các nguyên tắc quản lý dữ liệu (từ thu thập, lưu trữ đến xử lý và chia sẻ) nhằm đảm bảo dữ liệu được tổ chức, hệ thống hóa theo chuẩn mực quốc gia, giúp nhà nước và doanh nghiệp khai thác, ứng dụng một cách có kiểm soát, hiệu quả. Nhờ đó, nguồn dữ liệu khổng lồ sẽ thực sự trở thành động lực thúc đẩy nghiên cứu khoa học - công nghệ, nâng cao năng suất lao động và sức cạnh tranh của nền kinh tế. Ngoài ra, các nguyên tắc này góp phần đảm bảo quyền và lợi ích hợp pháp của các chủ thể dữ liệu. Dữ liệu không còn đơn thuần là việc tập hợp số liệu, mà mang giá trị kinh tế - xã hội to lớn, tương tự như tài sản trí tuệ. Hiến pháp yêu cầu Nhà nước bảo hộ quyền sở hữu trí tuệ; vì vậy, Luật Dữ liệu cần quy định rõ trách nhiệm bảo vệ quyền và lợi ích của những người tạo lập, sở hữu, chia sẻ dữ liệu. Cơ chế bản quyền, sở hữu công nghiệp cho dữ liệu như dữ liệu nghiên cứu chuyên ngành, dữ liệu đào tạo mô hình AI, sẽ khuyến khích tổ chức, cá nhân đầu tư cho việc thu thập, xử lý, gán nhãn và cập nhật dữ liệu. Đồng thời, luật cũng cần thiết lập cơ chế chia sẻ lợi ích, bảo đảm những đóng góp của chủ thể dữ liệu được thừa nhận xứng đáng, ngăn ngừa tình trạng sử dụng dữ liệu trái phép. Thêm vào đó, Hiến pháp thúc đẩy dân chủ và minh bạch trong khoa học - công nghệ. Khái niệm "mọi người tham gia và được thụ hưởng lợi ích từ các hoạt động khoa học - công nghệ" chỉ có thể hiện thực khi dữ liệu công được mở rộng và duy trì.

Luật Dữ liệu sẽ định nghĩa nguyên tắc "mở - chung - bảo mật," quy định rõ ràng dữ liệu công nào được công bố, dữ liệu cá nhân nào được bảo vệ, cũng như quy trình yêu cầu, cung cấp và giám sát. Nhờ đó, các start-up,

doanh nghiệp vừa và nhỏ… sẽ có cơ hội khai phá ý tưởng, tạo ra sản phẩm mới dựa trên nền dữ liệu phong phú; đồng thời, người dân cũng có thể theo dõi, giám sát hoạt động của cơ quan nhà nước, nâng cao tính minh bạch và trách nhiệm giải trình.



Chia sẻ lợi ích là cơ chế chỉ mới vừa được định nghĩa trong Luật Dữ liệu - Ảnh: Date communication

Như vậy, Hiến pháp không chỉ là văn bản pháp lý định hướng về quản lý dữ liệu, cần có Luật Dữ liệu làm công cụ hiện thực hóa nguyên tắc hiến định về khoa học - công nghệ, tạo nên hành lang pháp lý toàn diện, hiện đại, phù hợp với xu thế quốc tế và đáp ứng yêu cầu phát triển kinh tế - xã hội. Luật Dữ liệu sẽ mang đến một nền tảng vững chắc cho chuyển đổi số, thúc đẩy sáng tạo, bảo vệ quyền lợi mọi chủ thể và nâng cao dân chủ, minh bạch trong quản trị và ứng dụng khoa học - công nghệ.



Dữ liệu vừa là mục tiêu, vừa là động lực thúc đẩy các hoạt động nghiên cứu khoa học, công nghệ - Ảnh: Vecteezy

Hai là, Nghị quyết số 23-NQ/TW ngày 22/3/2018 của Bộ Chính trị về *"định hướng xây dựng chính sách phát triển công nghiệp quốc gia đến năm 2030, tầm nhìn đến năm 2045"* đã xác định chính sách khoa học và công nghệ cho phát triển công nghiệp: "Khuyến khích đầu tư, phát triển xây dựng các trung tâm dữ liệu lớn; đẩy mạnh phát triển khoa học phân tích, quản lý và xử lý dữ liệu lớn nhằm tạo ra các sản phẩm, tri thức mới"[183].



Nền công nghiệp nước nhà cần có những cú "huýt" mạnh mẽ - Ảnh: NIG

[183] Bộ Chính trị (2018), *Nghị quyết số 23-NQ/TW về định hướng xây dựng chính sách phát triển công nghiệp quốc gia đến năm 2030, tầm nhìn đến năm 2045*, Hà Nội.

Qua nghiên cứu nội dung, có thể thấy Nghị quyết 23-NQ/TW không chỉ dừng lại ở việc nhấn mạnh tầm quan trọng của dữ liệu lớn như một "nguồn nguyên liệu" mà còn đặt ra yêu cầu phải thiết kế toàn diện cả hệ thống hạ tầng và năng lực chuyển hóa dữ liệu thành sản phẩm, tri thức mới có giá trị khoa học. ***Trước hết,*** việc xác định các trung tâm dữ liệu lớn như "nhà máy" công nghiệp số nghĩa là Nhà nước và doanh nghiệp phải cùng nhau đầu tư xây dựng cơ sở vật chất: từ trung tâm lưu trữ đạt chuẩn quốc tế với khả năng chịu tải cao, chống sụp đổ khi khối lượng dữ liệu tăng đột biến, đến hệ thống đường truyền, kết nối liên vùng nhằm đảm bảo luồng dữ liệu được truyền tải liên tục, bảo đảm chất lượng và an toàn. Sự đầu tư này không chỉ mang tính kỹ thuật mà còn là cam kết chiến lược, bởi chỉ khi có hạ tầng đủ mạnh, dữ liệu mới trở thành công cụ hữu hiệu để tự động hóa sản xuất, quản lý chuỗi cung ứng, và phát triển các dịch vụ số phục vụ đời sống.



Thị trường Việt Nam chưa có nhiều "sản phẩm tri thức" chất lượng cao, kéo theo nhiều khu vực kinh tế thiếu động lực sáng tạo - Ảnh: CMLABS

Thứ hai, Nghị quyết tập trung phát triển năng lực khoa học phân tích, quản lý và xử lý dữ liệu lớn tức là chú trọng vào việc xây dựng nguồn nhân lực chất lượng cao và hệ sinh thái đổi mới sáng tạo. Điều này bao gồm đào tạo chuyên sâu về toán học tính toán, khoa học dữ liệu, trí tuệ nhân tạo và học máy; đồng thời khuyến khích các viện nghiên cứu, doanh nghiệp công nghệ phát triển các giải pháp phân tích dự báo, tối ưu hóa quy trình sản xuất và ra quyết định tự động. Khi dữ liệu được xử lý, phân tích và trực quan hóa hiệu quả, kết quả là các "sản phẩm tri thức". Chẳng hạn hệ thống cảnh báo sớm thiên tai, mô hình dự báo thị trường nông sản hay nền tảng y tế thông minh sẽ ra đời, thúc đẩy năng suất và tạo ra đột phá công nghệ...



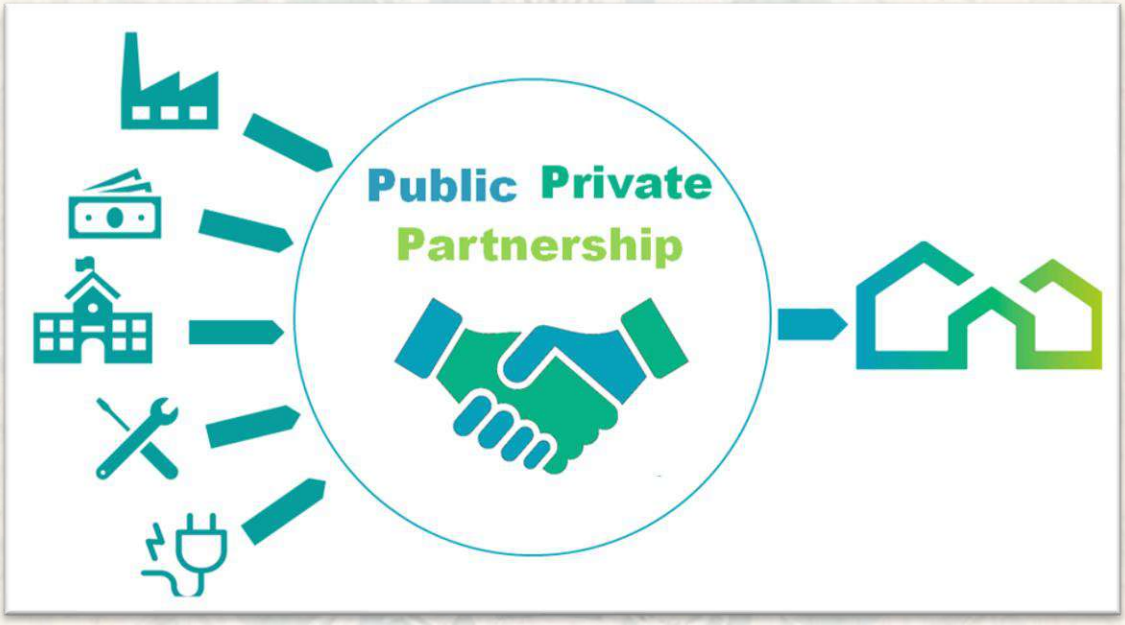
Dữ liệu tác động sâu sắc đến kết quả của các "kì lân công nghệ" nước nhà - Ảnh: NYC Data Science Academy

Thứ ba, Nghị quyết này đã mở ra cơ hội cho việc xây dựng khung pháp lý chuyên ngành về dữ liệu và bảo vệ dữ liệu cá nhân. Bởi khi hạ tầng và năng lực phân tích đã được đặt nền móng, bước tiếp theo là phải có các quy định rõ ràng về quyền sở hữu dữ liệu, trách nhiệm chia sẻ và nguyên tắc bảo mật để khuyến khích doanh nghiệp, tổ chức sẵn sàng chia sẻ dữ liệu một cách an toàn. Chính từ định hướng chiến lược của Nghị quyết 23 mà sau này Luật Dữ liệu và Luật Bảo vệ dữ liệu cá nhân mới được hình thành, đảm bảo vừa phát huy được giá trị của dữ liệu lớn trong công nghiệp, vừa bảo vệ quyền lợi và thông tin cá nhân của công dân, tạo nên một hệ sinh thái dữ liệu công bằng, minh bạch và bền vững.

Để chuyển chủ trương nâng cấp cơ sở hạ tầng, nhân lực trong Nghị quyết 23 thành hiện thực, cần phải có Luật Dữ liệu đóng vai trò như một "khung xương sống" pháp lý, trước hết bằng cách quy định chi tiết nguyên tắc quản trị dữ liệu: xác định rõ ai là chủ thể có quyền thu thập, ai sở hữu và ai được phép chia sẻ, từ đó phân định trách nhiệm và quyền lợi giữa cơ quan nhà nước, doanh nghiệp và cá nhân. Tiếp đó, luật cần ban hành các tiêu chuẩn kỹ thuật cho "trung tâm dữ liệu lớn". Ví dụ: hệ số sẵn sàng (uptime), khả năng mở rộng (scalability), tiêu chí an toàn thông tin (tham khảo ISO/IEC 27001) và yêu cầu về kết nối toàn quốc nhằm đảm bảo tính liên tục, thông suốt, ổn định của mạng dữ liệu quốc gia. Bên cạnh đó, Luật Dữ liệu phải thiết lập cơ chế đầu tư bền vững thông qua các chính sách ưu đãi như giảm thuế, hỗ trợ lãi suất cho vay, cơ chế đối tác công - tư (PPP) và cam kết ngân sách trung hạn, dài hạn giúp các trung tâm dữ liệu yên tâm huy động nguồn lực, vận hành lâu dài.

Ngoài ra, để thực thi mục tiêu "tạo ra sản phẩm, tri thức mới" mà Nghị quyết 23 đề ra, luật cần đưa ra hướng dẫn về chia sẻ "dữ liệu đầu ra" của các

trung tâm: định nghĩa rõ từng cấp độ dữ liệu (mở, hạn chế, nhạy cảm), quy trình xin phép và tiêu chí đánh giá mức độ rủi ro khi chia sẻ, đồng thời bảo đảm cơ chế chia sẻ lợi ích công bằng cho đơn vị cung cấp dữ liệu. Nhờ đó, các viện nghiên cứu, doanh nghiệp công nghệ và start-up sẽ có hành lang pháp lý vững chắc để khai thác, tích hợp và sáng tạo trên nền tảng dữ liệu khổng lồ, thúc đẩy các ứng dụng trí tuệ nhân tạo, phân tích dự báo và giải pháp tự động hóa, qua đó nâng cao năng suất, chất lượng sản phẩm, dịch vụ và sức cạnh tranh của toàn ngành công nghiệp.



Cơ chế đối tác công - tư (PPP) chính là cụ thể hóa của Nghị quyết 68 về phát triển mạnh mẽ khu vực kinh tế tư nhân - Ảnh: iPleaders

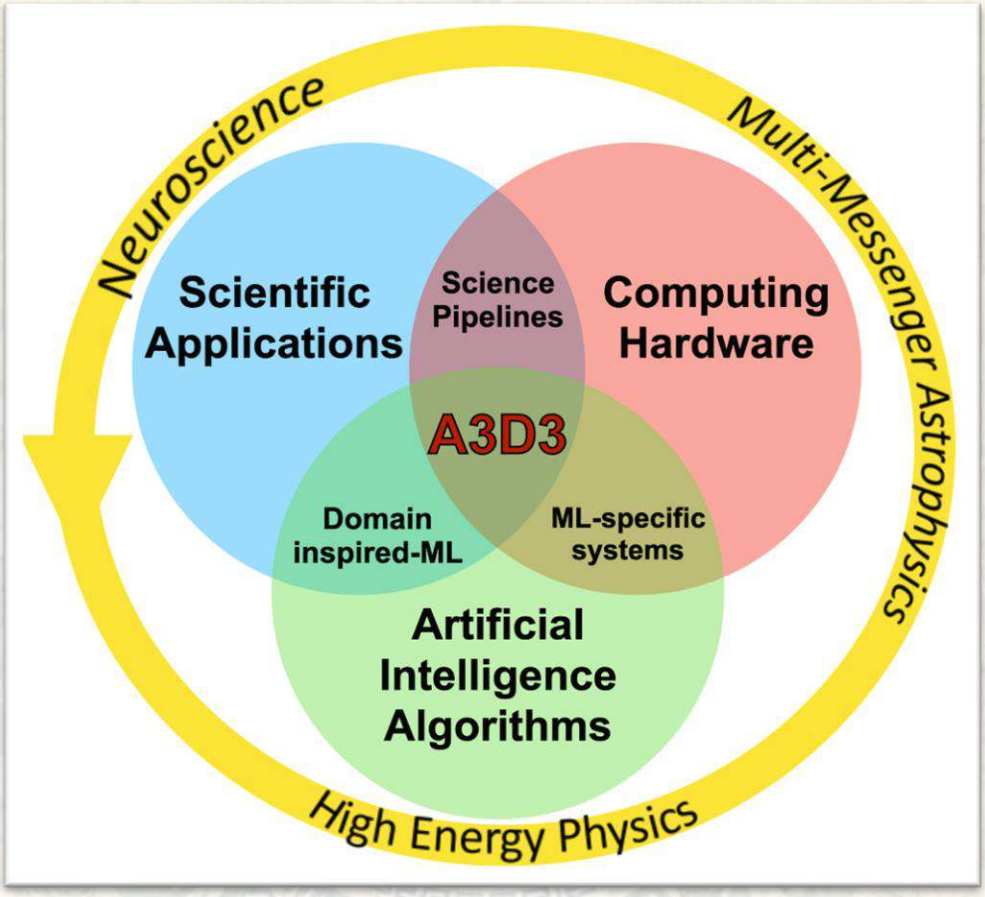
Trong khi đó, Luật Bảo vệ dữ liệu cá nhân được xây dựng dựa trên nguyên tắc bảo đảm quyền con người, phù hợp với quy định tại Hiến pháp năm 2013 về quyền bí mật đời tư và nguyên tắc Nhà nước "tạo điều kiện để mọi người tham gia và được thụ hưởng lợi ích từ hoạt động khoa học - công nghệ". Khi khuyến khích thu thập và xử lý dữ liệu quy mô lớn, Nghị quyết 23 cũng cảnh báo nguy cơ xâm phạm quyền riêng tư, do đó Luật Bảo vệ dữ liệu cá nhân thực hiện ba chức năng chính: đầu tiên là định nghĩa và phân loại dữ

liệu cá nhân, tách biệt khỏi dữ liệu công nghiệp, để xác định rõ phạm vi điều chỉnh; thứ hai là quy định nguyên tắc thu thập, xử lý và lưu trữ dữ liệu - gồm nguyên tắc tự nguyện, minh bạch mục đích và giới hạn xử lý - bảo đảm mọi hành vi xử lý đều dựa trên sự đồng thuận của chủ thể và có biện pháp bảo mật phù hợp; cuối cùng là thiết lập cơ chế giám sát, xử lý vi phạm với đầy đủ chế tài hành chính, trách nhiệm dân sự và khả năng bồi thường thiệt hại. Thông qua cơ quan giám sát độc lập về bảo vệ dữ liệu cá nhân, người dân có kênh khiếu nại, tố cáo và yêu cầu bồi thường khi quyền riêng tư bị xâm phạm, nhờ đó tạo dựng niềm tin để họ chủ động cung cấp dữ liệu, góp phần duy trì nguồn nguyên liệu dữ liệu dồi dào cho công nghiệp số.

Tóm lại, Nghị quyết số 23-NQ/TW ngày 22/3/2018 của Bộ Chính trị đã khẳng định dữ liệu lớn là một trong những trụ cột chiến lược của công nghiệp hóa, hiện đại hóa, đặt ra yêu cầu không chỉ xây dựng hạ tầng vật lý mà còn phải phát triển đồng bộ năng lực chuyển hóa dữ liệu thành sản phẩm, tri thức mới. Tuy nhiên, khi hạ tầng và quy mô thu thập, lưu trữ, xử lý dữ liệu ngày càng mở rộng, nguy cơ xâm phạm quyền cá nhân cũng tăng cao. Trên cơ sở đó, sự ra đời hai văn bản luật gồm Luật Dữ liệu và Luật Bảo vệ dữ liệu cá nhân vừa đáp ứng yêu cầu phát triển hạ tầng và năng lực xử lý dữ liệu lớn, như Nghị quyết 23 đã xác định, vừa bảo vệ các giá trị nhân văn, đảm bảo quyền con người không bị xem nhẹ trong cuộc Cách mạng công nghiệp 4.0. Nhờ đó, Việt Nam có thể hình thành một hệ sinh thái dữ liệu mạnh mẽ, minh bạch và bền vững, tạo đà cho quá trình chuyển đổi số quốc gia, nâng cao năng suất, chất lượng sản phẩm, dịch vụ và sức cạnh tranh của nền kinh tế trong kỷ nguyên vươn mình.

Ba là, Nghị quyết số 52-NQ/TW ngày 27/9/2019 của Bộ Chính trị về *"một số chủ trương, chính sách chủ động tham gia cuộc Cách mạng công*

nghiệp lần thứ Tư" xác định "Xây dựng và phát triển đồng bộ hạ tầng dữ liệu quốc gia. Hình thành hệ thống trung tâm dữ liệu quốc gia, các trung tâm dữ liệu vùng và địa phương kết nối đồng bộ và thống nhất".



Mô hình A3D3 thể hiện mối quan hệ mật thiết giữa cơ sở hạ tầng dữ liệu với các ứng dụng khoa học công nghệ và các thuật toán trí tuệ nhân tạo - Ảnh: Internet

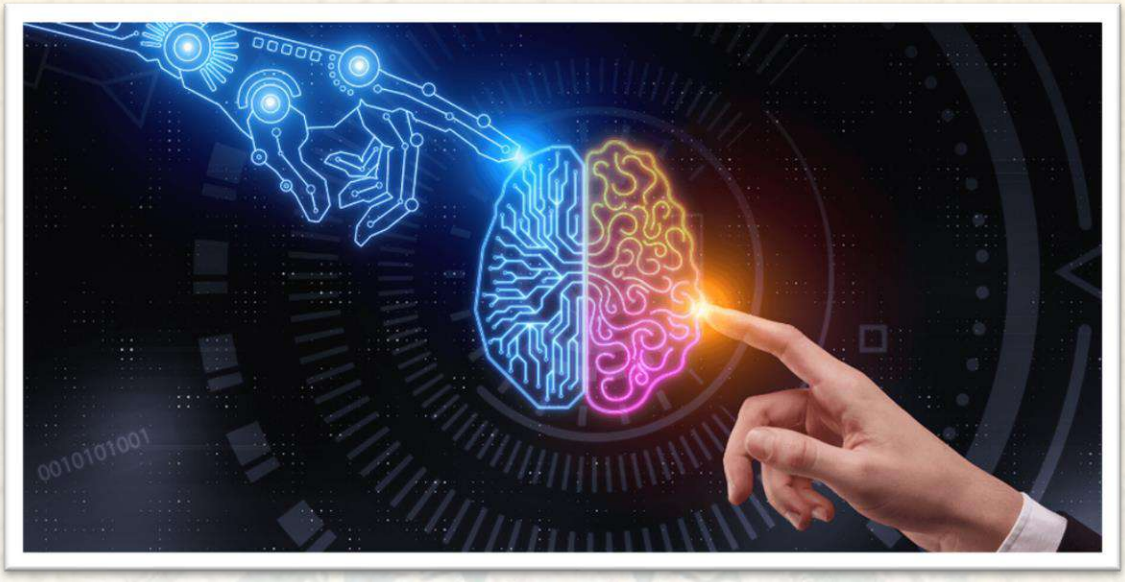
Có thể thấy Nghị quyết số 52-NQ/TW như một mục tiêu cấp thiết để Việt Nam chủ động tham gia Cuộc Cách mạng công nghiệp lần thứ tư. Để hiện thực hóa chủ trương này, Luật Dữ liệu cần được xây dựng nhằm thể chế hóa ba nhóm nội dung chính: ***(1)*** Quản trị dữ liệu, đó là quy định rõ thẩm quyền thu thập, sở hữu và chia sẻ giữa các cấp chính quyền, giữa bộ, ngành giữa nhà nước và doanh nghiệp tư nhân; ***(2)*** Tiêu chuẩn kỹ thuật định nghĩa khái niệm "trung tâm dữ liệu lớn", quy định hệ số sẵn sàng, khả năng mở

rộng, các chỉ tiêu an toàn thông tin và yêu cầu kết nối liên vùng để đảm bảo một hạ tầng dữ liệu an toàn, thống nhất và tương thích quốc tế; ***(3)*** Cơ chế đầu tư bền vững, thiết lập chính sách ưu đãi thuế, hỗ trợ lãi suất vay vốn, cơ chế đối tác (PPP) và cam kết nguồn lực ngân sách trung hạn, giúp các dự án Trung tâm dữ liệu quốc gia và vùng vận hành ổn định, đồng thời linh hoạt thích ứng với những tiến bộ công nghệ như trí tuệ nhân tạo, blockchain và điện toán đám mây.

Song song với việc phát triển hạ tầng, Luật Bảo vệ dữ liệu cá nhân cần được ban hành để cân bằng giữa khai thác dữ liệu quy mô lớn và bảo vệ quyền riêng tư công dân. Bên cạnh định nghĩa dữ liệu cá nhân và phân biệt rõ với dữ liệu tổ chức nhằm xác định phạm vi điều chỉnh; Quy định nguyên tắc thu thập, xử lý, lưu trữ, bắt buộc có sự đồng thuận của chủ thể, minh bạch mục đích, giới hạn xử lý và sử dụng biện pháp kỹ thuật bảo mật, mã hóa, phân quyền truy cập; Thiết lập cơ chế giám sát và chế tài bao gồm khiếu nại, tố cáo, xử phạt hành chính và bồi thường thiệt hại khi quyền riêng tư bị xâm phạm. Nhờ đó, cá nhân và doanh nghiệp có thể yên tâm chia sẻ và sử dụng dữ liệu trong khuôn khổ pháp luật.

Sự đồng bộ giữa Luật Dữ liệu và Luật Bảo vệ dữ liệu cá nhân không chỉ hiện thực hóa tinh thần Nghị quyết 52-NQ/TW mà còn kiến tạo một hệ sinh thái dữ liệu mạnh mẽ, minh bạch, bền vững, vừa thúc đẩy đổi mới sáng tạo, nâng cao năng suất và sức cạnh tranh của nền kinh tế, vừa đảm bảo tính nhân văn và quyền con người trong kỷ nguyên số.

Bốn là, Quyết định số 2289/QĐ-TTg 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 giao Bộ Công an thực hiện nhiệm vụ "Xây dựng, vận hành Trung tâm dữ liệu quốc gia. Nâng cao nhận thức của các tổ chức, doanh nghiệp và người dân về bảo vệ dữ liệu cá nhân, quản trị dữ liệu".



Chuyển đổi số là mục tiêu chiến lược trong con đường xây dựng xã hội chủ nghĩa tại Việt Nam - Ảnh: Agliedrop

Quyết định số 2289 đã xác lập rõ ràng dữ liệu và hạ tầng dữ liệu là một trụ cột chiến lược của Nhà nước trong thời đại số, Chính phủ đã giao Bộ Công an hai nhiệm vụ then chốt: ***(i)*** xây dựng, vận hành Trung tâm dữ liệu quốc gia; và ***(ii)*** nâng cao nhận thức của các tổ chức, doanh nghiệp cùng người dân về bảo vệ dữ liệu cá nhân và quản trị dữ liệu. Tinh thần và nội dung giao nhiệm vụ này không chỉ là mệnh lệnh hành chính về đầu tư hạ tầng kỹ thuật mà còn là tuyên bố chính trị về vị thế của dữ liệu trong chiến lược phát triển quốc gia, tức là dữ liệu được coi là tài nguyên quốc gia, là yếu tố then chốt để thực hiện chuyển đổi số, phát triển kinh tế số và bảo đảm an ninh - quốc phòng trong môi trường số.

Về mặt chính trị, quyết định này chính là bước thể chế hóa từ Nghị quyết 52-NQ/TW đã đề cập, theo đó Bộ Chính trị đã xác định hạ tầng dữ liệu đồng bộ là trụ cột chiến lược của Cách mạng 4.0, đòi hỏi phải "hình thành hệ thống Trung tâm dữ liệu quốc gia, các trung tâm dữ liệu vùng và địa phương kết nối đồng bộ và thống nhất". Từ góc độ phân tích chính sách,

Quyết định 2289 đặt ra ít nhất 03 mệnh đề nền tảng dẫn tới sự cần thiết phải ban hành các văn bản pháp luật chuyên ngành về dữ liệu.



Ảnh: Báo Công an nhân dân

- Khi dữ liệu trở thành hạ tầng chiến lược, cần một hành lang pháp lý rõ ràng để xác lập *"ai có quyền gì, ai chịu trách nhiệm gì"* trong vận hành hạ tầng đó, bao gồm cơ chế điều phối liên ngành, thẩm quyền quản lý trung tâm dữ liệu quốc gia, mối quan hệ giữa cơ quan nhà nước và các chủ thể tư nhân

tham gia cung cấp dịch vụ hạ tầng. Nếu thiếu pháp luật cụ thể, nguy cơ chồng chéo trách nhiệm, xung đột quyền hạn và lúng túng trong quản lý sẽ làm suy giảm hiệu quả đầu tư và tiềm ẩn rủi ro về an ninh, gián đoạn dịch vụ công.



Chống tư tưởng "cua cậy càng, cá cậy vây" trong hoạt động chuyển đổi số - Ảnh: Internet

- Quyết định nhấn mạnh khía cạnh an ninh và bảo vệ dữ liệu cá nhân; đây là tín hiệu cho thấy dữ liệu không chỉ là tài nguyên kinh tế mà còn liên quan trực tiếp tới an ninh quốc gia và quyền con người. Việc giao trực tiếp cho Bộ Công an, là lực lượng chủ quản về an ninh mạng, làm đầu mối xây dựng và vận hành Trung tâm dữ liệu quốc gia đồng thời cũng khẳng định dữ liệu được coi là tài sản chiến lược quốc gia, cần bảo đảm tối đa về bảo mật, sẵn sàng phục vụ mọi bộ, ngành và địa phương. Đồng thời, khi khối lượng dữ liệu cá nhân được thu thập, xử lý và lưu trữ ngày càng lớn, bao gồm dữ liệu y tế, giáo dục, dân cư. Do đó, Quyết định 2289 đã đặt ra đặc biệt nhiệm

vụ "nâng cao nhận thức" để tạo tiền đề chính trị và xã hội cho việc ban hành Luật Bảo vệ dữ liệu cá nhân. Luật này sẽ quy định rõ phạm vi và mục đích thu thập dữ liệu cá nhân, nguyên tắc "minh bạch - đồng thuận", các biện pháp kỹ thuật bảo mật, mã hóa, phân quyền truy cập cũng như chế tài xử lý vi phạm và bồi thường thiệt hại, nhằm bảo vệ quyền riêng tư và củng cố niềm tin của người dân, tổ chức trong môi trường số hóa.

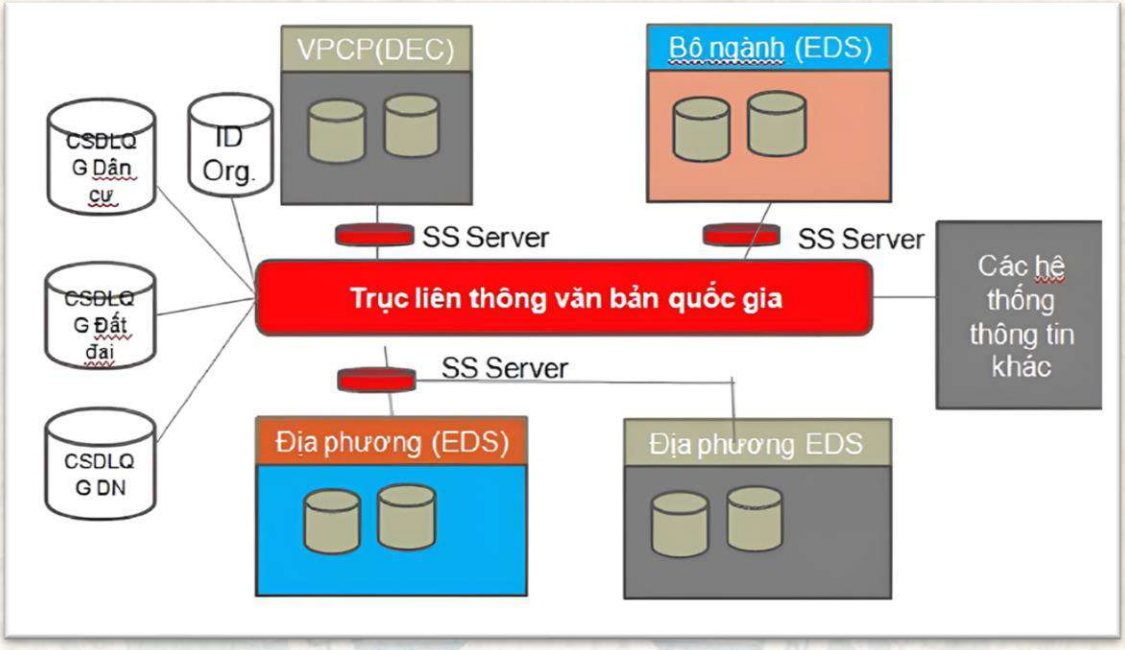
Hơn nữa, Quyết định 2289 còn gắn kết chặt chẽ chiến lược chuyển đổi số với an ninh mạg, từ đó dẫn đến nhu cầu phải có khuôn khổ pháp luật trong đó Luật Dữ liệu quy định nguyên tắc quản trị, chia sẻ và tiêu chuẩn kỹ thuật cho Trung tâm dữ liệu quốc gia, bảo đảm dữ liệu được thu thập, lưu trữ và sử dụng một cách an toàn, đồng bộ và hiệu quả. Nhờ vậy, sự đồng bộ giữa Luật Dữ liệu và Luật Bảo vệ dữ liệu cá nhân không chỉ thể hiện tinh thần nghị quyết và quyết định của Đảng, Chính phủ mà còn kiến tạo một hệ sinh thái dữ liệu mạnh mẽ, minh bạch và bền vững, đáp ứng yêu cầu chuyển đổi số toàn diện của quốc gia[184].

Năm là, Nghị quyết số 76/NQ-CP ngày 15/7/2021 của Chính phủ ban hành *"Chương trình tổng thể cải cách hành chính nhà nước giai đoạn 2021 -2030"* đã xác định xây dựng, phát triển hệ thống dữ liệu phục vụ triển khai Chính phủ điện tử hướng tới Chính phủ số tại bộ, ngành, địa phương.

Có thể thấy rằng mục tiêu của chương trình theo Nghị quyết số 76/NQ-CP ngày 15/7/2021 của Chính phủ là nâng cao hiệu lực, hiệu quả quản lý nhà nước, đồng thời phục vụ tốt hơn nhu cầu của người dân và doanh nghiệp. Các mục tiêu đến năm 2025 và 2030 đều nhấn mạnh việc hoàn thiện thể chế hành chính, thúc đẩy ứng dụng mạnh mẽ công nghệ thông tin và chuyển đổi số; xây

[184] Thủ tướng Chính phủ (2020), *Quyết định số 2289/QĐ-TTg ngày 31/12/2020 về ban hành Chiến lược quốc gia về Cách mạng công nghiệp lần thứ tư đến năm 2030,* Hà Nội.

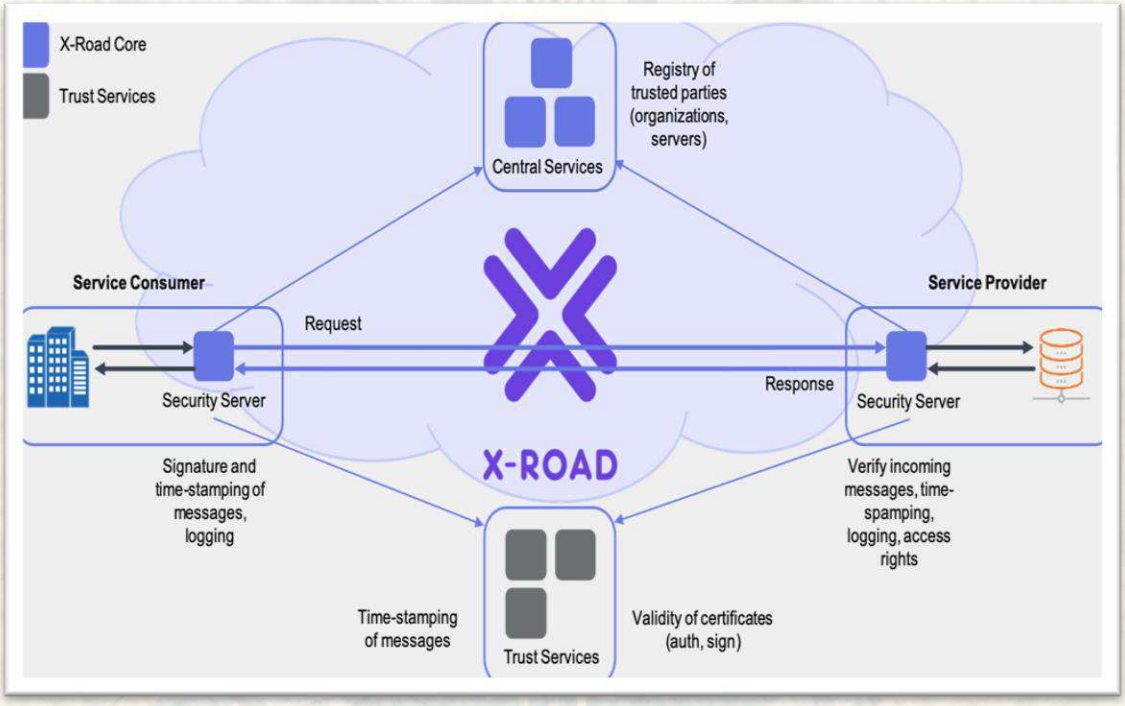
dựng và phát triển hệ thống dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành phục vụ quản lý nhà nước, cung cấp dịch vụ công trực tuyến; đồng thời tăng cường kết nối, chia sẻ dữ liệu giữa các bộ, ngành, địa phương để cải cách thủ tục hành chính và hỗ trợ ra quyết định chính sách dựa trên dữ liệu.



Mô hình trục liên thông văn bản quốc gia - Ảnh: Trang tin Chính phủ điện tử

Các nội dung của Nghị quyết 76 đều có mối liên hệ trực tiếp đến dữ liệu được thể hiện rõ qua ba phương diện chính. ***Thứ nhất,*** về phát triển và kết nối cơ sở dữ liệu quốc gia, Nghị quyết yêu cầu tối thiểu 80% các hệ thống thông tin của bộ, ngành, địa phương liên quan đến người dân và doanh nghiệp phải được kết nối, chia sẻ dữ liệu thông qua *Trục liên thông quốc gia*; dữ liệu được số hóa và tái sử dụng cho dịch vụ công. Đây không chỉ là chỉ tiêu kỹ thuật, mà còn là giải pháp chiến lược để khắc phục tình trạng dữ liệu phân tán, khó truy cập, gây lãng phí nguồn lực và cản trở cải cách hành chính. Việc dữ liệu được số hóa và tái sử dụng cho dịch vụ công giúp giảm thiểu trùng lặp thông tin, tiết kiệm thời gian xử lý và nâng cao chất lượng phục vụ công dân, doanh nghiệp. Đồng thời, phải hoàn thiện kết nối Cổng Dịch vụ công quốc gia với

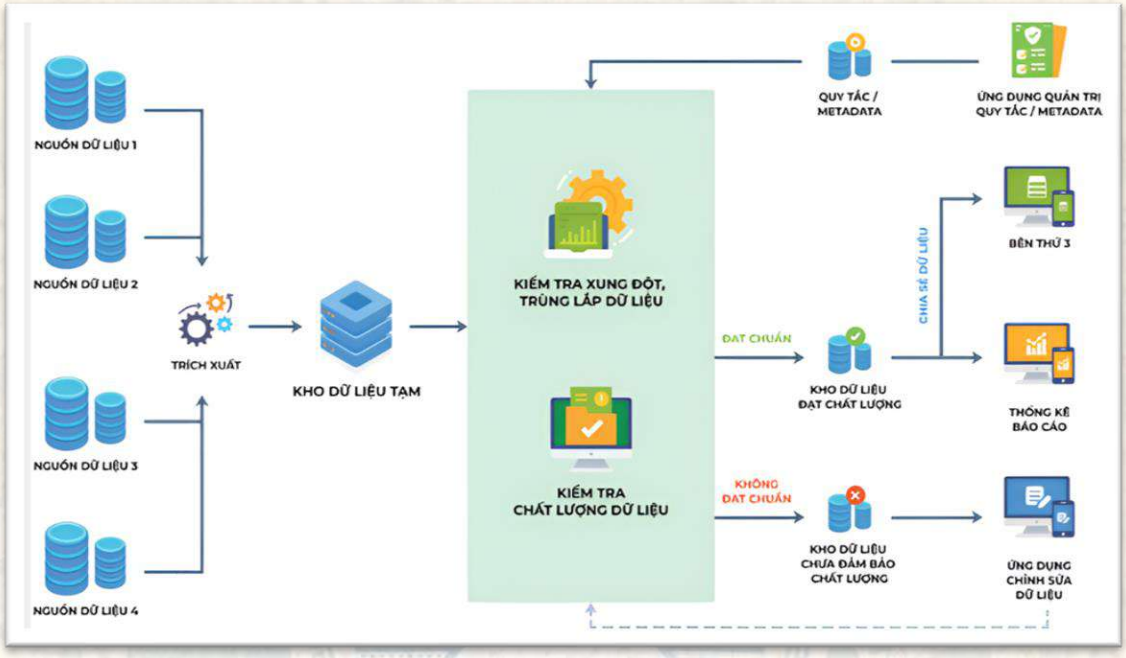
các cơ sở dữ liệu quốc gia và chuyên ngành để đảm bảo khả năng tích hợp, đồng bộ thông tin. Đây cũng là là bước quan trọng để tạo ra một hệ sinh thái dịch vụ công trực tuyến thống nhất. Khi các hệ thống này được đồng bộ, người dân chỉ cần cung cấp thông tin một lần và có thể thực hiện nhiều thủ tục khác nhau mà không phải lặp lại việc kê khai. Điều này phù hợp với xu hướng quản trị hiện đại mà Liên minh châu Âu và nhiều quốc gia OECD đã triển khai thành công, như Estonia với nền tảng X-Road, cho phép chia sẻ dữ liệu an toàn và tức thời giữa các cơ quan nhà nước.



Cách vận hành nền tảng X-Road của Estonia - Ảnh: API Conference

Thứ hai, về mở dữ liệu và phát triển dịch vụ dữ liệu, Nghị quyết yêu cầu mở dữ liệu của cơ quan nhà nước theo quy định pháp luật để phục vụ phát triển kinh tế số, xã hội số, đồng thời xây dựng kho dữ liệu dùng chung để cung cấp hợp pháp cho các cơ quan hành chính, doanh nghiệp và người dân. Chính sách mở dữ liệu mà Nghị quyết 76 đề cập là một trong những trụ cột của chính phủ minh bạch, thúc đẩy đổi mới sáng tạo và phát triển kinh tế

số. Khi dữ liệu của cơ quan nhà nước được mở theo quy định pháp luật, các doanh nghiệp, tổ chức xã hội và cá nhân có thể khai thác để tạo ra các sản phẩm, dịch vụ mới, từ ứng dụng giao thông thông minh, phân tích thị trường, đến các nền tảng học tập trực tuyến cá nhân hóa.



Quy trình xử lý dữ liệu của Kho dữ liệu dùng chung thành phố Đà Nẵng - Ảnh: Bộ Khoa học và Công nghệ

Việc xây dựng kho dữ liệu dùng chung giúp các cơ quan hành chính khai thác thông tin một cách hợp pháp, thống nhất, đồng thời giảm chi phí thu thập và xử lý dữ liệu riêng lẻ. Ở góc độ kinh tế, kho dữ liệu này có thể trở thành hạ tầng dữ liệu quốc gia, thúc đẩy hình thành thị trường dữ liệu - một xu thế đang phát triển mạnh tại các nước như Singapore (GovTech Data.gov.sg) hay Hàn Quốc (K-Data). Tại Việt Nam, khi kho dữ liệu dùng chung được vận hành rộng rãi, nó sẽ là nền tảng quan trọng để triển khai các dịch vụ dữ liệu thương mại, dịch vụ phân tích và dịch vụ trung gian dữ liệu theo quy định của Luật Dữ liệu 2024, từ đó tạo động lực cho cả khu vực công và khu vực tư nhân cùng phát triển.

Theo Tài liệu giới thiệu Luật Dữ liệu năm 2024 của Bộ Công an, Nghị quyết 76/NQ-CP là một trong những cơ sở chính trị quan trọng cho việc xây dựng Luật Dữ liệu. Mối liên hệ này thể hiện ở bốn khía cạnh. ***(1)*** Nghị quyết 76 đặt ra yêu cầu đồng bộ hạ tầng thông tin và dữ liệu để triển khai Chính phủ điện tử và Chính phủ số, đòi hỏi phải có một đạo luật thống nhất về thu thập, quản trị, chia sẻ, bảo vệ và khai thác dữ liệu. ***(2)*** Thực trạng phân mảnh dữ liệu trước khi có Luật Dữ liệu với nhiều cơ sở dữ liệu quốc gia và chuyên ngành rời rạc, thiếu chuẩn kết nối, đòi hỏi cơ chế pháp lý để tích hợp dữ liệu vào Cơ sở dữ liệu tổng hợp quốc gia, phù hợp tinh thần "kết nối, chia sẻ thông tin" của Nghị quyết 76. ***(3)*** Yêu cầu của Nghị quyết 76 về áp dụng công nghệ mới trong quản trị được cụ thể hóa trong Luật Dữ liệu 2024 thông qua các nguyên tắc và cơ chế xử lý, phân tích dữ liệu, hình thành thị trường dữ liệu. Bốn là, mục tiêu cải cách thủ tục hành chính của Nghị quyết 76, đặc biệt là "khai báo thông tin một cửa", được hiện thực hóa qua quy định của Luật Dữ liệu về kết nối và chia sẻ dữ liệu dùng chung, giúp giảm giấy tờ, tiết kiệm thời gian cho người dân và doanh nghiệp.

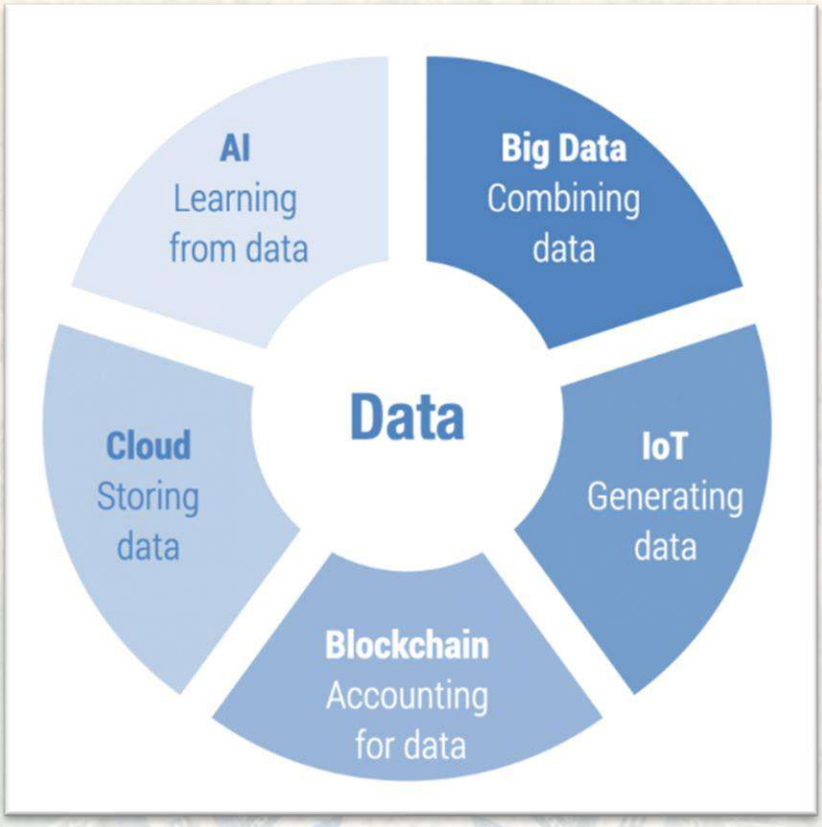
Như vậy, Nghị quyết 76/NQ-CP không chỉ đặt ra định hướng chiến lược cho cải cách hành chính giai đoạn 2021-2030 mà còn đóng vai trò nền móng chính trị quan trọng cho sự hình thành khung pháp lý chuyên biệt về dữ liệu. Luật Dữ liệu 2024 là bước hiện thực hóa mục tiêu này, tạo hạ tầng pháp lý đồng bộ cho cải cách hành chính, thống nhất quản lý dữ liệu trên phạm vi toàn quốc, thúc đẩy phát triển kinh tế số, xã hội số và Chính phủ số, đồng thời đảm bảo việc kết nối, chia sẻ, khai thác dữ liệu an toàn, hiệu quả, bảo vệ quyền lợi của người dân.

Sáu là, Nghị quyết số 29-NQ/TW ngày 17/11/2022 Hội nghị lần thứ sáu Ban Chấp hành Trung ương Đảng khóa XIII về *"tiếp tục đẩy mạnh công*

nghiệp hóa, hiện đại hóa đất nước đến năm 2030, tầm nhìn đến năm 2045" xác định ưu tiên nguồn lực và có cơ chế, chính sách khuyến khích đủ mạnh để phát triển những lĩnh vực ưu tiên; trong đó có phát triển công nghệ số (ưu tiên phát triển trí tuệ nhân tạo, dữ liệu lớn, chuỗi khối, điện toán đám mây, internet kết nối vạn vật, thiết bị điện tử - viễn thông, thiết kế và sản xuất chíp bán dẫn).

Nghị quyết số 29-NQ/TW ngày 17/11/2022 của Hội nghị lần thứ sáu Ban Chấp hành Trung ương Đảng khóa XIII đã xác định rõ định hướng chiến lược: ưu tiên nguồn lực, thiết lập cơ chế và chính sách đủ mạnh nhằm thúc đẩy phát triển các lĩnh vực công nghệ then chốt, trong đó đặc biệt nhấn mạnh vai trò của công nghệ số, bao gồm: trí tuệ nhân tạo (AI), dữ liệu lớn (Big Data), chuỗi khối (Blockchain), điện toán đám mây (Cloud Computing), Internet vạn vật (IoT), thiết bị điện tử - viễn thông, cũng như thiết kế và sản xuất chip bán dẫn. Điều này phản ánh nhận thức của Chính phủ về vai trò đột phá của công nghệ trong tối ưu hóa quy trình quản trị và cung cấp dịch vụ công. Big Data cho phép xử lý và phân tích khối lượng dữ liệu khổng lồ từ nhiều nguồn để dự báo, lập kế hoạch chính sách dựa trên bằng chứng. AI có thể hỗ trợ tự động hóa xử lý hồ sơ, phát hiện gian lận, hoặc cung cấp trợ lý ảo giải đáp thắc mắc cho người dân 24/7. Cloud Computing giúp giảm chi phí đầu tư hạ tầng công nghệ thông tin, tăng khả năng mở rộng và bảo đảm tính linh hoạt. Blockchain có thể được ứng dụng để đảm bảo tính bảo mật, minh bạch và truy vết dữ liệu, đặc biệt trong các giao dịch hành chính, đất đai, hoặc đấu thầu các dự án công. Điểm quan trọng là các công nghệ này khi triển khai trong quản trị sẽ thay đổi cách thức vận hành của bộ máy hành chính, từ cơ chế phản ứng sang cơ chế chủ động dự báo và ra quyết định nhanh hơn, chính xác hơn. Đây là tiền đề để hiện thực hóa mô hình Chính

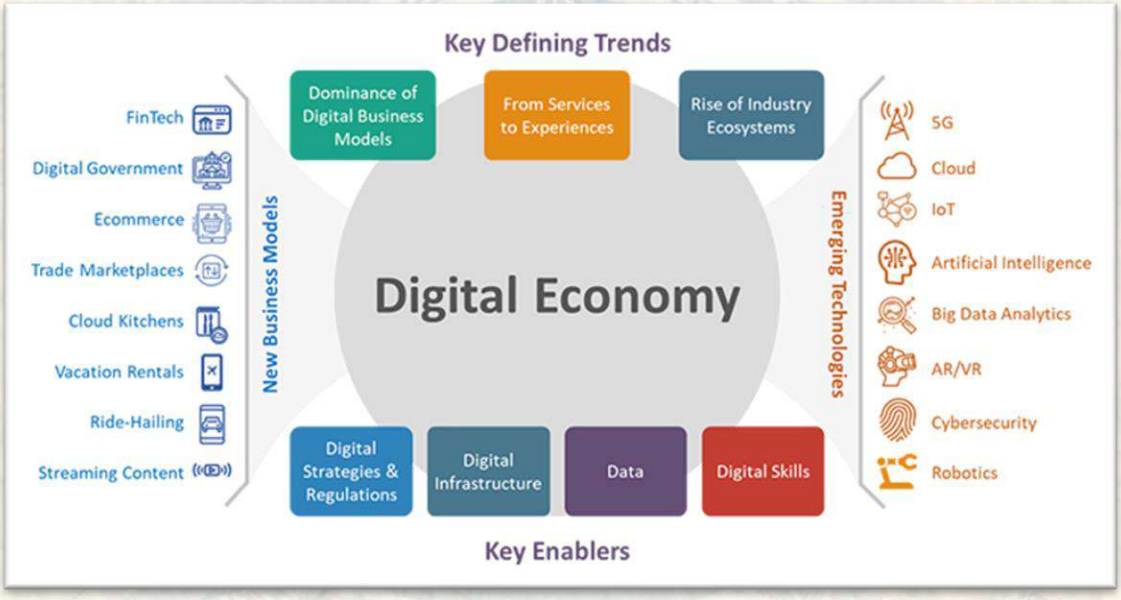
phủ số, khẳng định rằng công nghệ dữ liệu không chỉ là công cụ hỗ trợ mà là trụ cột của sự phát triển trong kỷ nguyên số.



Mối tương quan giữa dữ liệu và các công nghệ - Ảnh: dFarminc

Việc Nghị quyết đưa dữ liệu lớn và các công nghệ số có liên quan vào danh mục các lĩnh vực được ưu tiên phát triển, cho thấy dữ liệu đã và đang trở thành nguồn tài nguyên chiến lược, giữ vai trò trung tâm trong mô hình tăng trưởng mới của nền kinh tế tri thức. Tuy nhiên, để những lĩnh vực này phát triển bền vững, điều kiện tiên quyết là phải xây dựng hệ thống hành lang pháp lý đầy đủ, nhất quán, minh bạch, trong đó bao gồm Luật Dữ liệu nhằm thiết lập cơ chế thu thập, lưu trữ, khai thác, chia sẻ và liên thông dữ liệu một cách có kiểm soát và hợp pháp, cũng như Luật Bảo vệ dữ liệu cá nhân nhằm đảm bảo dữ liệu cá nhân không bị lạm dụng, xâm phạm, trở thành đối tượng bị khai thác trái phép trong quá trình phát triển các công nghệ mới như AI hay Big Data.

Nghị quyết 29-NQ/TW cũng cho thấy rằng nếu không có luật hóa chặt chẽ và theo kịp tốc độ công nghệ, Việt Nam có thể sẽ phải đối mặt với hệ lụy nghiêm trọng như rủi ro về an ninh mạng, xâm phạm quyền riêng tư cá nhân, và mất kiểm soát trong lưu thông, sử dụng dữ liệu xuyên biên giới. Việc xây dựng khung pháp lý và chính sách phù hợpkhông chỉ là hành động mang tính thủ tục, mà còn là một đòi hỏi chính trị cấp thiết, mang tính thời đại thể hiện năng lực hoạch định chiến lược của Đảng và Nhà nước trong việc định hướng phát triển khoa học công nghệ gắn với bảo vệ quyền con người và chủ quyền dữ liệu quốc gia. Do đó. việc xây dựng và ban hành chính sách, pháp luật về dữ liệu ở Việt Nam là hết sức cần thiết nhằm cụ thể hóa chủ trương của Đảng.



Dẫn giải về kinh tế số - Ảnh: Huawei

Như vậy, có thể khẳng định rằng Nghị quyết số 29-NQ/TW không chỉ là căn cứ chính trị quan trọng thúc đẩy quá trình xây dựng và ban hành Luật Dữ liệu và Luật Bảo vệ dữ liệu cá nhân, mà còn phản ánh tầm nhìn chiến lược của Đảng trong việc tạo dựng hạ tầng thể chế cho quá trình công nghiệp hóa, hiện đại hóa đất nước gắn liền với sự phát triển của nền kinh tế số, kinh tế dữ liệu, và xã hội số.

Bảy là, Nghị quyết số 81/2023/QH15 ngày 09/01/2023 của Quốc hội về Quy hoạch tổng thể quốc gia thời kỳ 2021 - 2030, tầm nhìn đến năm 2050 đã xác định "đưa Việt Nam trở thành một trong những trung tâm dữ liệu khu vực. Xây dựng các trung tâm dữ liệu gắn với các vùng động lực, cực tăng trưởng, hành lang kinh tế; phát triển các cụm trung tâm dữ liệu quốc gia tại khu vực phía Bắc và khu vực phía Nam".



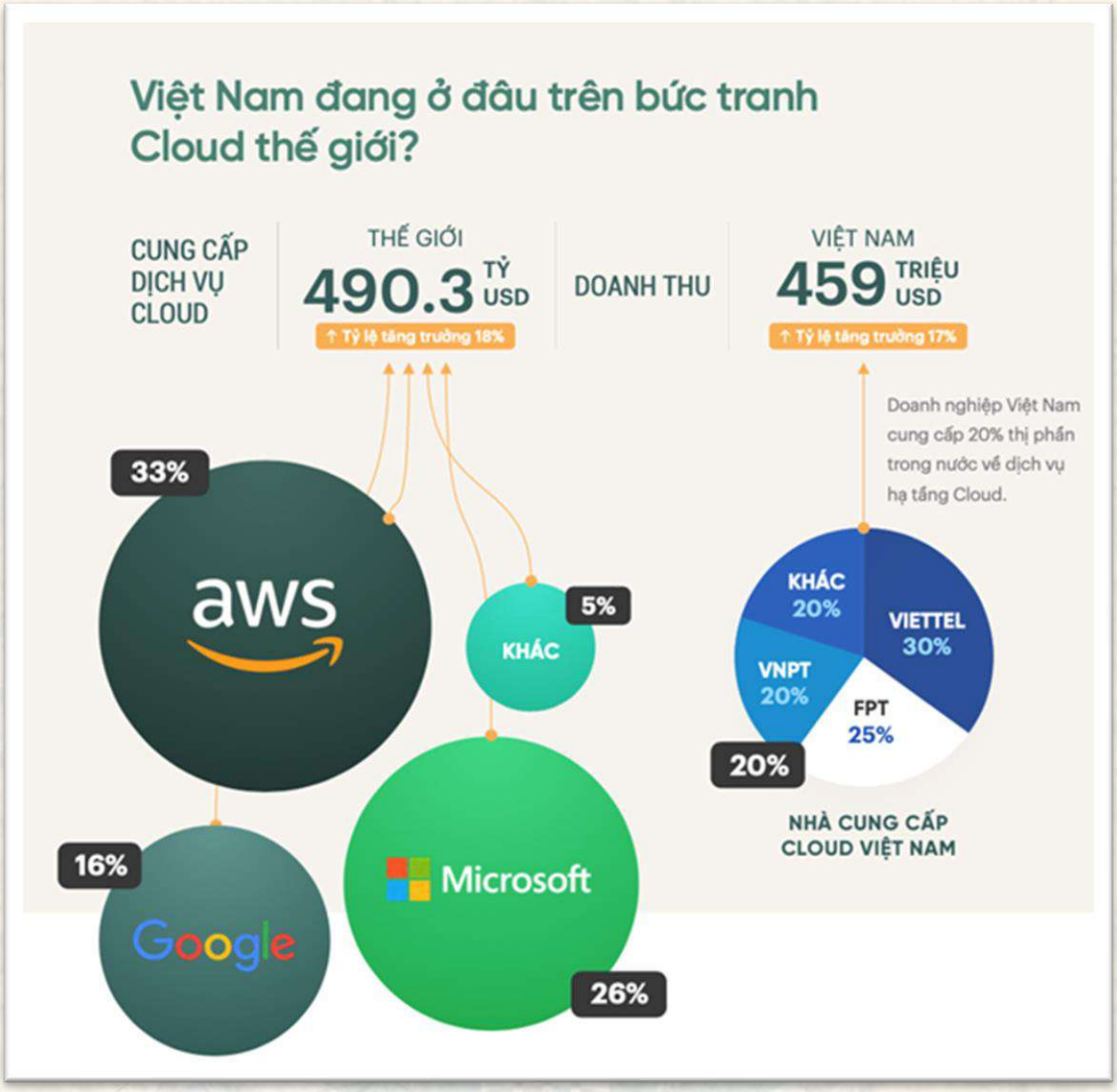
Trung tâm dữ liệu quốc gia tại nước ta phải được xây dựng trên hạ tầng công nghệ hiện đại - Ảnh: VnEconomy

Ta có thể thấy rõ định hướng chiến lược trong phát triển hạ tầng công nghệ số quốc gia, cụ thể là mục tiêu đưa Việt Nam trở thành một trong những trung tâm dữ liệu của khu vực. Nghị quyết nhấn mạnh việc xây dựng các trung tâm dữ liệu gắn với các vùng động lực phát triển, cực tăng trưởng, hành lang kinh tế, cùng với phát triển các cụm trung tâm dữ liệu quốc gia tại khu vực phía Bắc và phía Nam. Đây là một bước đi thể hiện quyết tâm chính trị ở cấp cao nhất nhằm đưa dữ liệu trở thành hạ tầng chiến lược của nền kinh tế số, đồng thời khẳng định vai trò trung tâm dữ liệu như một thành tố

chủ chốt trong tiến trình công nghiệp hóa, hiện đại hóa và chuyển đổi số quốc gia. Về mục tiêu đưa Việt Nam trở thành "trung tâm dữ liệu khu vực", việc đưa mục tiêu này vào Quy hoạch tổng thể quốc gia không chỉ là lựa chọn tức thời, nó thể hiện bước chuyển mình mạnh mẽ, phát triển không chỉ trên lĩnh vực công nghiệp, dịch vụ. Khi một mục tiêu đã được "cắm mốc" trong quy hoạch quốc gia, các bộ, ngành, địa phương buộc phải ưu tiên bố trí nguồn lực, không gian phát triển và cơ chế phối hợp để hiện thực hóa. Từ đây phát sinh nhu cầu thể chế hóa bằng một khung pháp luật chuyên biệt về dữ liệu nhằm biến định hướng quy hoạch thành các quy tắc vận hành cụ thể, có tính ràng buộc. Với cách tiếp cận gắn trung tâm dữ liệu với các vùng động lực, cực tăng trưởng và hành lang kinh tế hàm ý một cấu trúc không gian hạ tầng ở quy mô lớn, nơi tập trung nguồn điện ổn định, kết nối cáp quang trục, điểm trao đổi Internet, lao động kỹ thuật cao và dịch vụ hỗ trợ. Để cấu trúc đó vận hành hiệu quả, cần có khung pháp lý chi tiết quy định rõ: ***(i)*** quy chuẩn kỹ thuật tối thiểu cho trung tâm dữ liệu (bao gồm độ an toàn, khả năng hoạt động liên tục và phục hồi khi có sự cố.); ***(ii)*** Thủ tục hành chính (quy định riêng về đất đai, môi trường, và năng lượng, phù hợp với đặc thù của trung tâm dữ liệu); ***(iii)*** cơ chế phối hợp hiệu quả giữa các bộ, ngành liên quan để tránh chồng chéo hoặc tắc nghẽn. Không có khung pháp lý thống nhất, quy hoạch sẽ bị "nghẽn thể chế" ở khâu thực thi.

Mặt khác, khi Việt Nam hướng tới vai trò trung tâm dữ liệu khu vực, lưu lượng dữ liệu xuyên biên giới sẽ gia tăng, kéo theo yêu cầu pháp lý về chủ quyền và an ninh dữ liệu. Theo đó, cần có khung pháp lý cần làm rõ tiêu chí, điều kiện và quy trình chuyển đổi, xử lý dữ liệu xuyên biên giới; cơ chế đánh giá tác động an ninh quốc gia; trách nhiệm của nhà cung cấp dịch vụ trung tâm dữ liệu và đám mây cũng như chế tài tương xứng. Cách tiếp cận

này vừa giữ vững an ninh quốc gia, vừa bảo đảm dòng chảy dữ liệu phục vụ thương mại và đổi mới.



Bước tranh tổng thể về thị trường cloud tại Việt Nam và trên thế giới - Ảnh: Báo Khánh Hòa

Với mục tiêu hình thành "cụm trung tâm dữ liệu quốc gia ở miền Bắc và miền Nam" đòi hỏi dữ liệu của Nhà nước và doanh nghiệp tư nhân phải liên thông và dùng chung theo những nguyên tắc thống nhất. Vì vậy, pháp luật về dữ liệu cần: ***(i)*** phân loại dữ liệu (cốt lõi, quan trọng, mở…) gắn với mức bảo vệ tương ứng; ***(ii)*** quy định nghĩa vụ kết nối và chia sẻ qua nền tảng điều phối dữ liệu để chấm dứt tình trạng "cát cứ dữ liệu"; ***(iii)*** đặt chuẩn dữ

liệu và dữ liệu lớn chung để bảo đảm chất lượng, khả năng tương tác và truy xuất nguồn gốc; ***(iv)*** thiết kế cơ chế phí khai thác dữ liệu công để tối ưu hiệu quả đầu tư công và khuyến khích tái sử dụng



Trung tướng Nguyễn Minh Chính phát biểu tại tọa đàm "Góp ý dự thảo Luật Bảo vệ dữ liệu cá nhân" ngày 23/4/2025 - Ảnh: Báo Sài Gòn Giải Phóng

Về mặt chính trị, định hướng này thể hiện sự nhất quán trong chủ trương của Đảng và Nhà nước về việc coi dữ liệu là tài nguyên mới, tài sản chiến lược, có giá trị không thua kém các nguồn lực truyền thống như đất đai, tài chính hay nhân lực. Trong bối cảnh cạnh tranh chiến lược về dữ liệu và công nghệ số ngày càng gia tăng, việc xác lập vị thế của Việt Nam như một trung tâm dữ liệu khu vực không chỉ nhằm thu hút đầu tư, nâng cao năng lực tính toán và lưu trữ phục vụ điều hành quốc gia, mà còn tạo ra giá trị gia tăng từ nền kinh tế dữ liệu. Tuy nhiên, việc phát triển hệ thống trung tâm dữ liệu ở quy mô lớn và phân bố theo vùng động lực cũng kéo theo yêu cầu cấp thiết phải có khung pháp lý đầy đủ, chặt chẽ và minh bạch để điều chỉnh toàn diện

các hoạt động liên quan đến thu thập, xử lý, chia sẻ, khai thác, liên kết và lưu trữ dữ liệu.

Như vậy, Nghị quyết 81/2023/QH15 đặt ra mệnh lệnh chính trị xây dựng hạ tầng dữ liệu quy mô quốc gia với mục tiêu trung tâm khu vực, để mục tiêu này khả thi, Việt Nam cần một khung chính sách, pháp luật đồng bộ bao quát từ phân loại, quản lý, bảo vệ, điều phối, chia sẻ, khai thác dữ liệu đến dữ liệu xuyên biên giới và thị trường dịch vụ dữ liệu. Luật Dữ liệu 2024 và các văn bản dưới luật chính là bước cụ thể hóa, vừa thu hút đầu tư và phát triển hạ tầng, vừa giữ vững an ninh dữ liệu và lợi ích quốc gia.

Tám là, Công văn số 7455-CV/VPTW ngày 31/7/2023 của Văn phòng Trung ương Đảng thông báo kết luận của Bộ Chính trị về Đề án Trung tâm dữ liệu quốc gia, theo đó Bộ Chính trị đồng ý chủ trương xây dựng Trung tâm dữ liệu quốc gia và giao Đảng đoàn Quốc hội phối hợp lãnh đạo, chỉ đạo rà soát, sửa đổi, bổ sung, xây dựng các văn bản quy phạm pháp luật có liên quan theo thẩm quyền. Có thể thấy rằng, Công văn 7455-CV/VPTW là văn bản chỉ đạo trực tiếp của Bộ Chính trị, thể hiện quan điểm thống nhất của Đảng Cộng sản Việt Nam về việc cần thiết triển khai Trung tâm dữ liệu quốc gia. Chỉ đạo này chính là *"cơ sở chính trị"* quan trọng để đưa Luật Dữ liệu vào chương trình xây dựng pháp luật. Nó còn đặt nền tảng chính trị-mang tính định hướng cao nhất cho quá trình soạn thảo, sửa đổi các quy định liên quan đến dữ liệu và bảo vệ dữ liệu cá nhân.

Không chỉ vậy, việc Bộ Chính trị đồng ý chủ trương xây dựng Trung tâm dữ liệu quốc gia cho thấy Bộ Chính trị xác định hạ tầng dữ liệu là một "công trình chiến lược" mang tầm quốc gia, tương đương với các hạ tầng giao thông, năng lượng. Do đó, đây không chỉ là nội dung chuyên môn công nghệ thông tin, mà là công cụ then chốt để quản trị, điều hành và phát triển

kinh tế - xã hội. Sự đồng ý này còn mang một ý nghĩa chính trị quan trọng, chính là một chủ trương ở cấp cao nhất của Đảng buộc phải được ưu tiên đưa vào Nghị quyết của Quốc hội, Chương trình của Chính phủ, từ đó "đòn bẩy" để các bộ, ngành và địa phương triển khai đồng bộ.



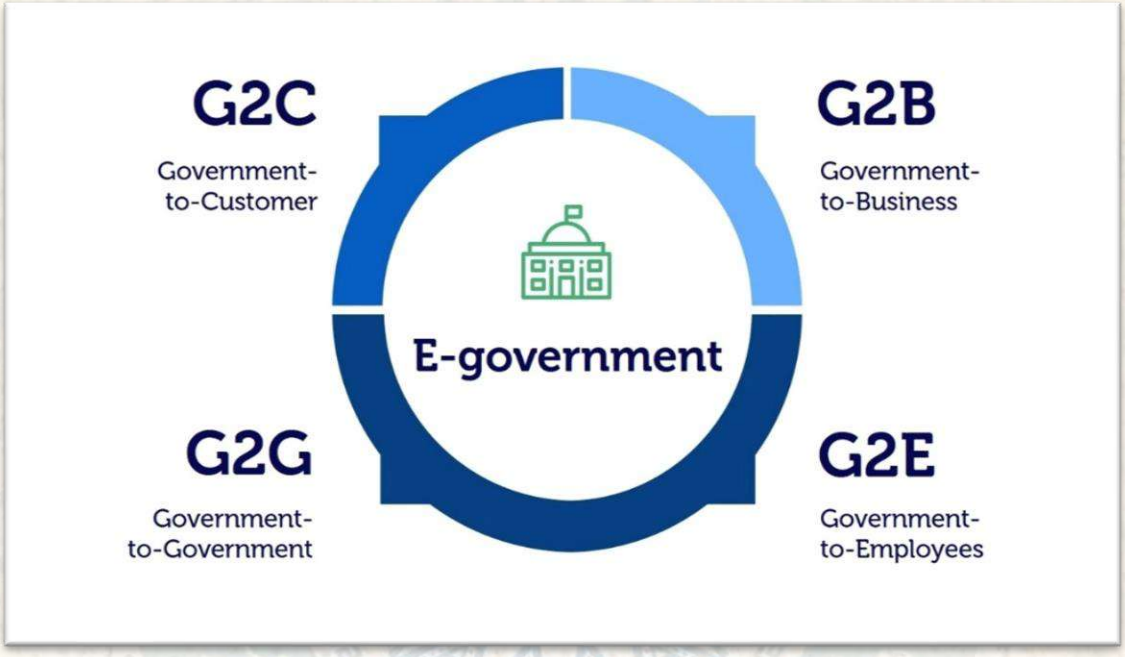
Trung tâm dữ liệu là "khung xương" của chính phủ số - Ảnh: FPT IS

Ngoài ra, trong bối cảnh chuyển đổi số quốc gia, sự ra đời của Công văn số 7455 không chỉ là một văn bản pháp lý thuần túy mà còn thể hiện sự nhất quán, tính định hướng chiến lược và cam kết chính trị mạnh mẽ của Đảng và Nhà nước Việt Nam. Về tính nhất quán, Công văn số 7455 nhất quán với các Nghị quyết chiến lược trước đó như: Nghị quyết 52-NQ/TW ngày 27/9/2019 về chủ trương, chính sách chủ động tham gia Cuộc Cách mạng Công nghiệp

lần thứ tư đã khẳng định: "Xây dựng và phát triển đồng bộ hạ tầng dữ liệu quốc gia; hình thành hệ thống trung tâm dữ liệu quốc gia, các trung tâm dữ liệu vùng và địa phương kết nối đồng bộ và thống nhất" (Điểm 1, Mục II). Đây là nền tảng luận lý cho việc coi dữ liệu như một công trình hạ tầng chiến lược, tương đương với giao thông, năng lượng, và viễn thông; Nghị quyết 81/2023/QH15 ngày 09/01/2023 về Quy hoạch tổng thể quốc gia giai đoạn 2021-2030, tầm nhìn đến 2050 xác định rõ mục tiêu: "Đưa Việt Nam trở thành một trong những trung tâm dữ liệu khu vực; xây dựng các trung tâm dữ liệu gắn với các vùng động lực, cực tăng trưởng, hành lang kinh tế" (Mục II, Điều 3). Nghị quyết này đã cụ thể hóa tầm nhìn dài hạn, tạo đầu bài cho việc ban hành Luật Dữ liệu, đảm bảo hành lang pháp lý tương xứng với yêu cầu phát triển hạ tầng dữ liệu toàn diện. Bên cạnh đó, công văn này còn là tiền đề cho khung chính trị - pháp lý ban hành bởi sự liên kết chặt chẽ giữa văn bản chỉ đạo chiến lược (Đảng), quy hoạch tổng thể (Quốc hội), chiến lược quốc gia (Thủ tướng) và khung hướng dẫn kỹ thuật (bộ, ngành) đã tạo ra một môi trường chính trị - pháp lý đồng bộ, bảo đảm Luật Dữ liệu không chỉ ra đời nhanh chóng mà còn mang tính khả thi và bền vững.

Bên cạnh đó, Chính phủ, Thủ tướng Chính phủ cũng đã ban hành nhiều quyết định có tính định hướng quan trọng về phát triển dữ liệu, hoàn thiện cơ sở hạ tầng thông tin trong chuyển đổi số ở nước ta như: Chiến lược dữ liệu quốc gia quy định tại Quyết định số 142/QĐ-TTg ngày 02/02/2024 của Thủ tướng Chính phủ, Đề án xây dựng Trung tâm dữ liệu quốc gia quy định tại Nghị quyết số 175/NQ-CP ngày 30/10/2023 của Chính phủ, Quy hoạch hạ tầng thông tin và truyền thông thời kỳ 2021 - 2030, tầm nhìn đến năm 2050 quy định tại Quyết định số 36/QĐ-TTg ngày 11/01/2024 của Thủ tướng Chính phủ. Đây là những cơ sở chính trị - pháp lý quan trọng, thể hiện rõ

định hướng và cam kết của Chính phủ trong việc xây dựng, phát triển hệ sinh thái dữ liệu và nền kinh tế số tại Việt Nam. Những văn bản này không chỉ phản ánh tầm nhìn dài hạn của quốc gia về phát triển dữ liệu, mà còn đặt ra những yêu cầu cấp bách về hoàn thiện khung pháp luật điều chỉnh dữ liệu một cách thống nhất, toàn diện và hiện đại.



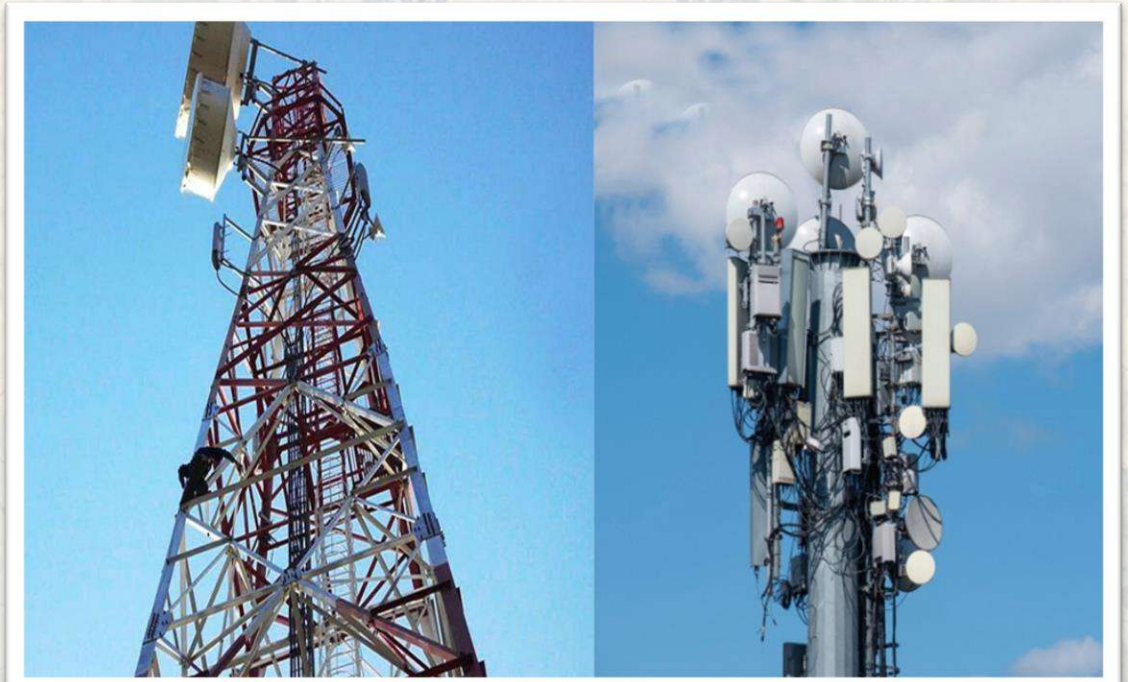
Chính phủ điện tử đối với từng loại chủ thể - Ảnh: RMIT Việt Nam

Về Chiến lược dữ liệu quốc gia đến năm 2030, tầm nhìn đến năm 2050 (Quyết định số 142/QĐ-TTg ngày 02/02/2024). Chiến lược này xác lập rõ dữ liệu là tài nguyên mới, là nền tảng để thúc đẩy chuyển đổi số, phát triển kinh tế số, xã hội số và chính phủ số. Chiến lược yêu cầu xây dựng hệ sinh thái dữ liệu quốc gia, trong đó bao gồm: Xây dựng khung pháp lý về dữ liệu và bảo vệ dữ liệu cá nhân; Phát triển thị trường dữ liệu, thúc đẩy chia sẻ và mở dữ liệu giữa các cơ quan nhà nước và khu vực tư nhân; Bảo đảm an toàn, an ninh dữ liệu, nhất là dữ liệu công dân.

Đây là minh chứng rõ ràng về mặt chính trị - hành pháp rằng việc ban hành Luật Dữ liệu và Luật Bảo vệ dữ liệu cá nhân là điều kiện tiên quyết để

triển khai đồng bộ chiến lược dữ liệu quốc gia. Không thể xây dựng một hệ sinh thái dữ liệu hiệu quả nếu thiếu hành lang pháp lý minh bạch, toàn diện và có tính cưỡng chế cao.

Đối với Đề án xây dựng Trung tâm dữ liệu quốc gia (Nghị quyết số 175/NQ-CP ngày 30/10/2023). Đề án này định hướng thành lập một Trung tâm dữ liệu quy mô quốc gia làm hạ tầng số cốt lõi để lưu trữ, xử lý, phân tích và chia sẻ dữ liệu dùng chung giữa các cơ quan nhà nước, phục vụ phát triển Chính phủ số. Đề án nhấn mạnh: ***(i)*** Trung tâm dữ liệu quốc gia sẽ xử lý dữ liệu nhạy cảm, dữ liệu cá nhân quy mô lớn; ***(ii)*** Phải bảo đảm tuân thủ nguyên tắc bảo vệ quyền riêng tư, an toàn thông tin và chủ quyền dữ liệu quốc gia. Trong bối cảnh này, sự vắng mặt của một đạo luật về dữ liệu và bảo vệ dữ liệu cá nhân sẽ tạo ra khoảng trống pháp lý nguy hiểm, khiến quá trình thu thập - xử lý - sử dụng dữ liệu dễ bị lạm dụng hoặc rò rỉ, ảnh hưởng đến quyền công dân và an ninh quốc gia.



Kế hoạch thực hiện Quy hoạch hạ tầng thông tin và truyền thông thời kỳ 2021 - 2030, tầm nhìn đến năm 2050 - Ảnh: bacgiang.gov.vn

Về Quyết định số 36/QĐ-TTg ngày 11/01/2024 về Quy hoạch hạ tầng thông tin và truyền thông đến năm 2030, tầm nhìn 2050. Quy hoạch xác định rõ việc phát triển đồng bộ hạ tầng số, trung tâm dữ liệu, mạng viễn thông và điện toán đám mây để phục vụ chiến lược chuyển đổi số. Trong đó, xây dựng hành lang pháp lý về quản lý dữ liệu là một trong những yếu tố then chốt, đồng hành với đầu tư công nghệ và hạ tầng kỹ thuật. Đây là dấu hiệu thể hiện rằng phát triển hạ tầng dữ liệu không thể tách rời khỏi xây dựng thể chế, và rằng hạ tầng số chỉ thực sự hiệu quả khi có luật pháp bảo vệ quyền lợi của người dân, doanh nghiệp và Nhà nước.

Tóm lại, ba văn bản nêu trên chính là cơ sở chính trị rõ ràng và nhất quán, khẳng định vai trò thiết yếu và cấp bách của việc ban hành Luật Dữ liệu và Luật Bảo vệ dữ liệu cá nhân tại Việt Nam. Chúng chứng minh rằng việc xây dựng chính sách pháp luật không đơn thuần là đáp ứng yêu cầu kỹ thuật - công nghệ, mà còn là một nhiệm vụ chính trị quan trọng nhằm bảo đảm an ninh dữ liệu, chủ quyền số, bảo vệ quyền riêng tư của công dân và thúc đẩy kinh tế số, chính phủ số và xã hội số phát triển theo đúng định hướng của Đảng và Nhà nước.

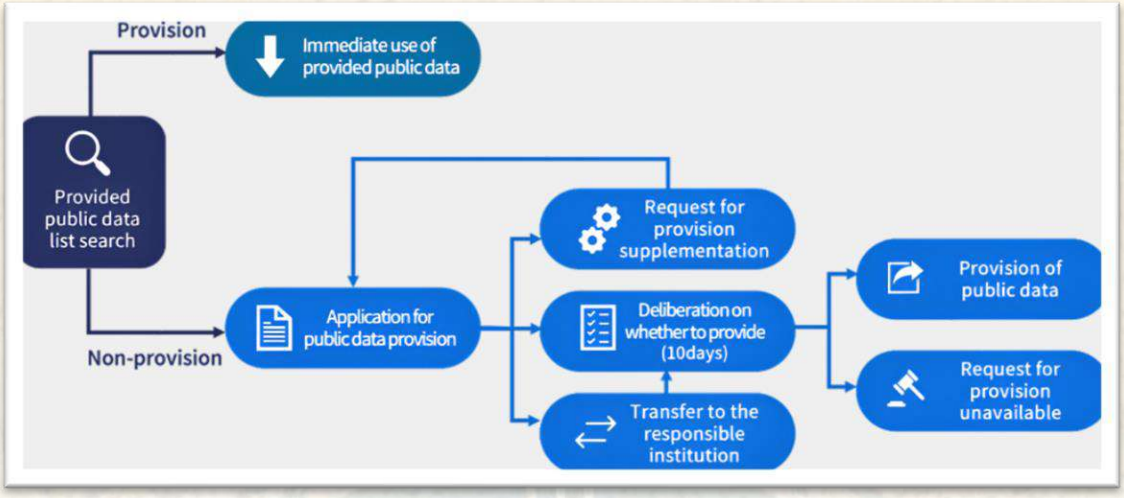
Do đó, trong bối cảnh chuyển đổi số đang diễn ra sâu rộng trên tất cả các lĩnh vực của đời sống xã hội, việc hoàn thiện hệ thống pháp luật, đặc biệt là ban hành các đạo luật chuyên ngành về dữ liệu như Luật Dữ liệu và Luật Bảo vệ dữ liệu cá nhân, là một yêu cầu cấp bách và mang tính thời sự. Đây không chỉ là vấn đề kỹ thuật pháp lý, mà còn là một định hướng chính trị quan trọng, thể hiện sự chủ động, quyết liệt của Nhà nước trong việc thể chế hóa các chủ trương, chính sách lớn của Đảng và Chính phủ về phát triển kinh tế số, xã hội số và Chính phủ số. Việc xây dựng và hoàn thiện khung pháp luật về dữ liệu sẽ tạo hành lang pháp lý vững chắc cho các hoạt động thu

thập, chia sẻ, kết nối, khai thác, sử dụng và bảo vệ dữ liệu, đồng thời đảm bảo quyền và lợi ích hợp pháp của tổ chức, cá nhân trong không gian số. Đây cũng là điều kiện tiên quyết để thúc đẩy ứng dụng dữ liệu trong quản lý nhà nước, nâng cao hiệu quả hoạt động của các cơ quan công quyền, hỗ trợ ra quyết định kịp thời, chính xác và dựa trên bằng chứng, qua đó góp phần nâng cao năng lực quản trị quốc gia. Mặt khác, việc ban hành chính sách pháp luật phù hợp về dữ liệu sẽ tạo môi trường thuận lợi để phát triển các mô hình kinh doanh dựa trên dữ liệu, thu hút đầu tư trong lĩnh vực công nghệ số, đồng thời khuyến khích người dân, doanh nghiệp tích cực tham gia, đóng góp vào quá trình phát triển kinh tế - xã hội dựa trên nền tảng số. Trong dài hạn, đây chính là bước đi chiến lược để đảm bảo mọi người dân đều có cơ hội bình đẳng trong việc tiếp cận, sử dụng và thụ hưởng các thành quả do chuyển đổi số mang lại, hướng tới một xã hội số an toàn, nhân văn, lấy người dân làm trung tâm, chủ thể, mục tiêu và động lực của sự phát triển.

1.3.3. Cơ sở thực tiễn

Hiện nay, nhiều nước trên thế giới đã có quy định về dữ liệu, vận hành, khai thác, sử dụng dữ liệu (dữ liệu của cơ quan nhà nước, của tổ chức, doanh nghiệp, cá nhân) như: Luật Dữ liệu mở (Hàn Quốc); Luật Quản trị dữ liệu và Luật Dữ liệu của Châu Âu áp dụng chung cho 27 nước thành viên… Qua đó, tạo cơ chế, chính sách để ứng dụng dữ liệu vào hoạt động quản lý nhà nước, phát triển kinh tế - xã hội.

Ở nước ta, quán triệt, triển khai các chủ trương, chính sách của Đảng, Nhà nước về phát triển khoa học, công nghệ, nhất là những vấn đề liên quan đến xây dựng, tạo lập, kết nối, chia sẻ dữ liệu, điều này đã đạt được một số kết quả tích cực như:



Mô hình vận hành Luật Dữ liệu mở tại Hàn Quốc - Ảnh: data.go.kr

Một là, bước đầu hình thành 07 cơ sở dữ liệu quốc gia. Các cơ sở dữ liệu này bao gồm: ***(1) Cơ sở dữ liệu quốc gia về dân cư:*** Đây là cơ sở dữ liệu cốt lõi, chứa thông tin cơ bản của tất cả công dân Việt Nam. Dữ liệu này được thu thập và quản lý bởi Bộ Công an, bao gồm các thông tin như họ tên, ngày sinh, giới tính, nơi đăng ký thường trú, quan hệ gia đình,... Việc triển khai cơ sở dữ liệu này giúp đơn giản hóa các thủ tục hành chính, thay thế sổ hộ khẩu giấy, và là nền tảng cho việc xác thực thông tin cá nhân trên môi trường số; ***(2) Cơ sở dữ liệu quốc gia về đăng ký doanh nghiệp,*** cơ sở dữ liệu này cung cấp thông tin đầy đủ và chính xác về các doanh nghiệp đang hoạt động tại Việt Nam, từ tên, địa chỉ, ngành nghề kinh doanh, vốn điều lệ, đến thông tin về người đại diện pháp luật. cơ sở dữ liệu này do Bộ Kế hoạch và Đầu tư quản lý, giúp các cơ quan nhà nước, doanh nghiệp và người dân dễ dàng tra cứu, kiểm tra tính pháp lý của doanh nghiệp; ***(3) Cơ sở dữ liệu quốc gia về bảo hiểm*** do Bảo hiểm xã hội Việt Nam quản lý, nó chứa thông tin về người tham gia bảo hiểm xã hội, bảo hiểm y tế, bảo hiểm thất nghiệp. Mục tiêu là số hóa sổ bảo hiểm và thẻ bảo hiểm y tế, tạo điều kiện thuận lợi cho việc khám chữa bệnh và giải quyết các chế độ bảo hiểm một cách nhanh chóng, chính xác; ***(4) Cơ sở dữ liệu hộ tịch điện tử,*** cở dữ liệu này chứa thông tin

về các sự kiện hộ tịch của công dân như khai sinh, kết hôn, khai tử. Nó giúp quản lý thông tin hộ tịch một cách tập trung, tránh tình trạng khai báo trùng lặp hoặc sai sót, đồng thời là cơ sở để liên thông dữ liệu với cơ sở dữ liệu quốc gia về dân cư; ***(5) Cơ sở dữ liệu quốc gia về đất đai,*** cơ sở dữ liệu này gắn liền với đất đai và tài sản gắn liền với đất trên phạm vi cả nước do Bộ Tài nguyên và Môi trường quản lý, cung cấp thông tin về vị trí, diện tích, mục đích sử dụng, chủ sở hữu của từng thửa đất. Việc hoàn thiện cơ sở dữ liệu này là rất quan trọng để quản lý hiệu quả tài nguyên đất đai, giải quyết các tranh chấp và hỗ trợ phát triển kinh tế; ***(6) Cơ sở dữ liệu quốc gia về tài chính***, cơ sở dữ liệu này do Bộ Tài chính quản lý, tổng hợp các thông tin về thu chi ngân sách nhà nước, thuế, hải quan, và các hoạt động tài chính công khác. Nó giúp nâng cao hiệu quả quản lý ngân sách, đảm bảo tính minh bạch và chống thất thoát; ***(7) Cơ sở dữ liệu quốc gia về cán bộ, công chức, viên chức*** chứa thông tin chi tiết về đội ngũ cán bộ, công chức, viên chức trong hệ thống hành chính nhà nước, bao gồm quá trình công tác, đào tạo, khen thưởng, kỷ luật. Mục tiêu là số hóa hồ sơ nhân sự, giúp công tác quản lý, đánh giá và quy hoạch cán bộ trở nên khách quan và hiệu quả hơn.

Việc xây dựng thành công các cơ sở dữ liệu quốc gia mang ý nghĩa chiến lược rất quan trọng. 07 cơ sở dữ liệu về quốc gia đã đặt nền móng cho chuyển đổi số quốc gia, ở đó, thông tin được chuẩn hóa, có cấu trúc, có chủ thể chịu trách nhiệm, đủ điều kiện tái sử dụng trong toàn hệ thống hành chính. Khi có định danh thống nhất và danh mục dùng chung, các hệ thống ngành dọc có điểm tựa để đồng bộ hóa, giảm sai lệch định danh và giảm trùng lặp khi thu thập dữ liệu. Khi các cơ sở dữ liệu được liên thông, người dân sẽ không phải cung cấp lại nhiều lần các thông tin đã có, giúp chuyển đổi cách người dân tương tác với bộ máy hành chính, từ mô hình "người dân

phải chạy" sang "dữ liệu phải chạy", giúp giảm thiểu giấy tờ, rút ngắn thời gian làm thủ tục hành chính, đồng thời tăng tính minh bạch và công bằng trong mọi quyết định góp phần nâng cao hiệu quả quản lý nhà nước, các cơ quan chức năng có cái nhìn tổng thể, đưa ra các quyết định chính sách kịp thời và hiệu quả hơn.

Bên cạnh đó, các cơ sở dữ liệu còn nâng cao chất lượng dữ liệu và khả năng tổng hợp, phân tích, dự đoán và hoạch định chính sách. Khi có một nguồn dữ liệu tập trung, chính xác và theo thời gian thực cho phép các nhà hoạch định chính sách đưa ra các quyết định kịp thời và chính xác hơn, dựa trên dữ liệu thực tế thay vì phán đoán. Đồng thời, các cơ quan chức năng có thể giám sát, đánh giá hiệu quả công việc và chống gian lận, thất thoát một cách hiệu quả hơn. Hơn nữa, khi dữ liệu tập trung, cơ quan chủ quản có thể quản trị dữ liệu với quy trình, tiêu chí chất lượng (đầy đủ, chính xác, nhất quán, kịp thời). Điều này nâng độ tin cậy của số liệu nhà nước, giảm rủi ro ban hành chính sách dựa vào dữ liệu nhiễu.

Không chỉ vậy, cơ sở dữ liệu quốc gia là *"hạ tầng mềm"* cho nhiều ứng dụng số góp phần thúc đẩy phát triển nền kinh tế số. Dữ liệu được coi là một tài nguyên quý giá trong kỷ nguyên số. Việc xây dựng và khai thác các cơ sở dữ liệu quốc gia tạo điều kiện cho các doanh nghiệp phát triển các dịch vụ số sáng tạo, thúc đẩy ngành công nghệ thông tin và tạo ra một thị trường tiềm năng lớn cho các sản phẩm, dịch vụ số. Ví dụ, dựa trên dữ liệu giao thông và dân cư, các công ty có thể phát triển các ứng dụng bản đồ thông minh và dịch vụ vận tải hiệu quả. Ngoài ra, một số ứng dụng như xác thực danh tính, định danh số, thanh toán, trợ cấp có mục tiêu, dự báo dân số lao động, quy hoạch đô thị, y tế, giáo dục số. Một khi bộ dữ liệu lõi vận hành ổn định, chi phí cho mỗi dịch vụ dữ liệu mới giảm mạnh.

Hai là, một số cơ sở dữ liệu quốc gia đã có sự kết nối liên thông, chia sẻ dữ liệu góp phần cải cách, đơn giản hóa thủ tục hành chính cho người dân. Khi dữ liệu được liên thông, nguyên tắc "một lần khai báo" bắt đầu được áp dụng: thông tin mà người dân hoặc doanh nghiệp đã cung cấp cho một cơ quan sẽ được các cơ quan khác khai thác trực tiếp từ hệ thống, thay vì yêu cầu cung cấp lại dưới dạng hồ sơ giấy. Điều này giúp giảm đáng kể số lượng giấy tờ phải nộp, rút ngắn thời gian xử lý thủ tục và hạn chế sai sót do nhập liệu thủ công. Bên cạnh đó, việc chia sẻ dữ liệu giữa các cơ sở dữ liệu quốc gia còn hỗ trợ các cơ quan hành chính đưa ra quyết định nhanh chóng và chính xác hơn, bởi thông tin được trích xuất trực tiếp từ nguồn chính thức, luôn được cập nhật và đồng bộ. Ví dụ, kết nối giữa Cơ sở dữ liệu quốc gia về dân cư với các hệ thống đăng ký, cấp giấy tờ hoặc giải quyết chế độ bảo hiểm xã hội đã cho phép xác thực thông tin cá nhân trong vài giây, thay vì phải kiểm tra thủ công qua nhiều khâu. Tác động cải cách thủ tục hành chính từ liên thông dữ liệu không chỉ thể hiện ở việc giảm chi phí và thời gian cho người dân, doanh nghiệp, mà còn nâng cao tính minh bạch, hạn chế tình trạng yêu cầu cung cấp lại hoặc làm phát sinh thủ tục không cần thiết. Đây là bước tiến quan trọng để hướng tới mô hình Chính phủ số phục vụ, trong đó dữ liệu trở thành công cụ trung tâm để nâng cao hiệu quả và chất lượng quản lý nhà nước.

Ba là, hạ tầng công nghệ xây dựng các trung tâm dữ liệu bước đầu được quan tâm đầu tư hơn. Có thể thấy sự quan tâm thể hiện ở một số khía cạnh sau: Chính phủ đã có những định hướng và đưa ra các cột mốc tiến độ cụ thể trong xây dựng hạ tầng phục vụ chuyển đổi số quốc gia như phê duyệt Nghị quyết số 175/NQ-CP ngày 30/10/2023 về Đề án Trung tâm dữ liệu quốc gia; Chỉ thị số 32/CT-TTg ngày 4/9/2024 ấn định mốc đưa trung tâm dữ liệu quốc gia vào hoạt động vào Quý IV/2025. Đây là dấu hiệu cho thấy việc đầu tư

hạ tầng công nghệ dữ liệu đã không còn là ý tưởng trên giấy mà đã hoàn toàn chuyển sang giai đoạn triển khai có thời hạn. Không chỉ vậy, nhà nước còn bảo đảm nguồn lực phục vụ công tác xây dựng các hạ tầng công nghệ. Các ngân hàng như HDBank đã hưởng ứng chủ trương của Chính phủ bằng cách triển khai các gói tín dụng ưu đãi lên tới 20.000 tỷ đồng dành riêng cho các doanh nghiệp đầu tư vào lĩnh vực hạ tầng và công nghệ số[185]. Mặc dù đây là nguồn vốn từ khu vực tư nhân, nó phản ánh sự đồng lòng và tạo ra một môi trường tài chính thuận lợi để triển khai các dự án hạ tầng số ở quy mô lớn, bao gồm cả các dự án liên quan đến dữ liệu nhà nước. Thêm vào đó, dưới sự chỉ đạo của các bộ ban ngành, Việt Nam đang đẩy mạnh triển khai mạng 5G, được coi là một trong những hạ tầng số cốt lõi, để đáp ứng nhu cầu bùng nổ dữ liệu. Việc việc phát triển hạ tầng băng thông rộng trên toàn quốc được xem là một phần quan trọng của khoản đầu tư lớn vào hạ tầng số để tạo nền tảng cho kinh tế số.

Bên cạnh các kết quả đạt được, vẫn còn tồn tại một số hạn chế sau:

Thứ nhất, một số bộ, ngành không có hoặc chưa đầy đủ hạ tầng để triển khai các hệ thống công nghệ thông tin cốt lõi phục vụ cho các công tác nghiệp vụ. Có thể thấy rằng, một khoảng trống quan trọng tồn tại trong tiến trình chuyển đổi số và xây dựng hạ tầng dữ liệu quốc gia. Hạ tầng công nghệ thông tin cốt lõi ở đây không chỉ bao gồm máy chủ, thiết bị lưu trữ và đường truyền, mà còn là một hệ thống đồng bộ gồm trung tâm dữ liệu đạt chuẩn, nền tảng tích hợp - chia sẻ dữ liệu theo kiến trúc Chính phủ số, hệ thống định danh và xác thực điện tử thống nhất, cơ chế quản trị dữ liệu tập trung và các lớp bảo mật đa tầng. Trong thực tế, nhiều cơ quan hiện vẫn vận hành trên hạ tầng phân tán, thiết bị đã lỗi thời, thiếu cơ chế dự phòng

[185] https://vnexpress.net/hdbank-danh-goi-vay-20-000-ty-cho-doanh-nghiep-so-4886536.html

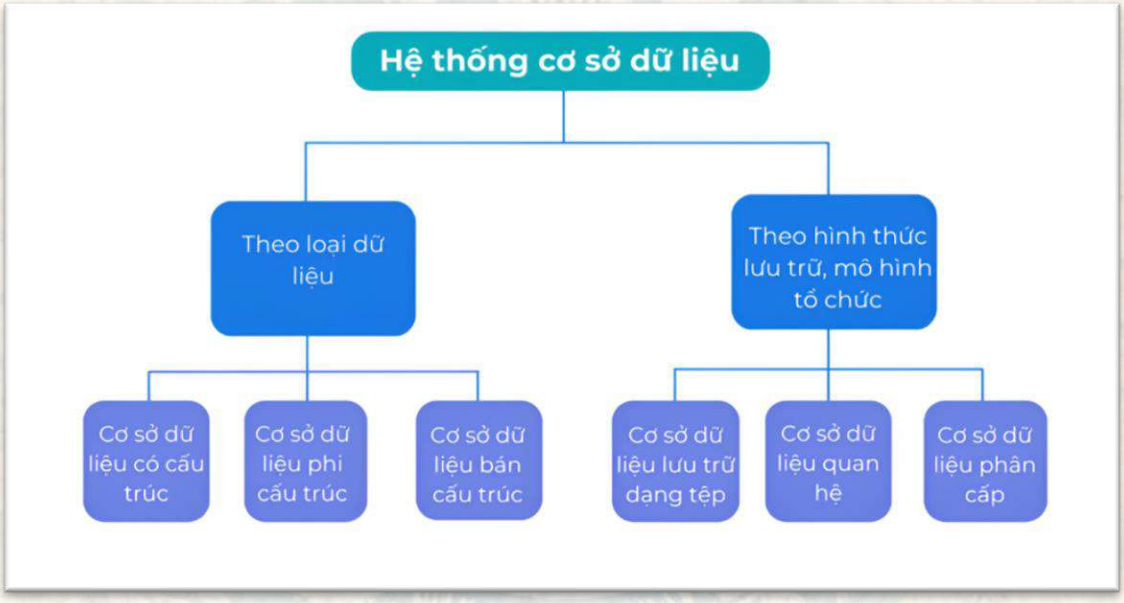
và khả năng khôi phục sau thảm họa. Một số nơi chưa có nền tảng tích hợp dữ liệu (Integration Platform) và không áp dụng chuẩn giao tiếp lập trình ứng dụng (API) an toàn, dẫn tới các hệ thống thông tin hoạt động rời rạc, không thể chia sẻ dữ liệu thời gian thực. Thậm chí, nhiều hệ thống còn phụ thuộc vào giải pháp của nhà thầu mà cơ quan không nắm toàn quyền kiểm soát kỹ thuật, gây rủi ro về bảo mật và quyền sở hữu dữ liệu.

Việc thiếu hoặc chưa đầy đủ hạ tầng công nghệ thông tin cốt lõi khiến các hoạt động nghiệp vụ như xử lý hồ sơ điện tử, kết nối liên thông dữ liệu, phân tích và khai thác dữ liệu phục vụ ra quyết định... gặp nhiều hạn chế. Ví dụ, nếu không có nền tảng chia sẻ dữ liệu bảo mật, việc thực hiện nguyên tắc "một lần khai báo" sẽ không khả thi, buộc người dân và doanh nghiệp phải cung cấp lại thông tin cho nhiều cơ quan khác nhau. Ngoài ra, thiếu hạ tầng bảo mật đồng bộ sẽ làm gia tăng nguy cơ rò rỉ hoặc bị tấn công vào dữ liệu quan trọng của Nhà nước.



Chuẩn bị sẵn sàng các điều kiện về hạ tầng công nghệ thông tin tại Thanh Hóa - Ảnh: Báo Điện tử Thanh Hóa

Nguyên nhân chủ yếu xuất phát từ đầu tư rời rạc, theo dự án đơn lẻ thay vì tuân thủ một kiến trúc tổng thể; hạn chế về ngân sách dành cho hạ tầng số; và năng lực kỹ thuật, nhân sự của một số đơn vị chưa đáp ứng yêu cầu thiết kế, vận hành hệ thống phức tạp. Điều này đặt ra yêu cầu cần chuẩn hóa và hợp nhất hạ tầng công nghệ thông tin ở tầm quốc gia, gắn với triển khai Cơ sở dữ liệu tổng hợp quốc gia và Trung tâm dữ liệu quốc gia theo Luật Dữ liệu 2024, đồng thời áp dụng các tiêu chuẩn - quy chuẩn kỹ thuật thống nhất để bảo đảm khả năng kết nối, chia sẻ và khai thác dữ liệu an toàn, hiệu quả.



Cơ sở dữ liệu cần phải được thu thập, phân loại theo quy chuẩn chung, có thể tương tự với hình minh họa - Ảnh: MISA AMIS

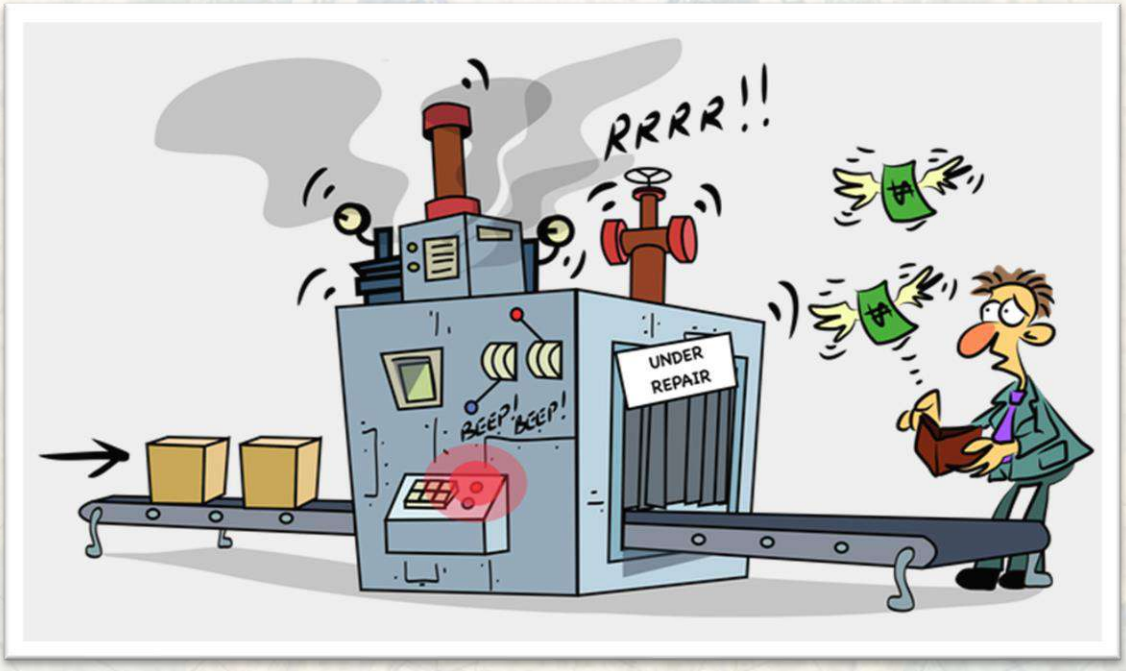
Thứ hai, nhiều cơ sở dữ liệu được thu thập, lưu trữ trùng lặp, chồng chéo, chưa thống nhất về danh mục dữ liệu dùng chung gây khó khăn khi kết nối, chia sẻ, khai thác dữ liệu. Trước hết, tình trạng thu thập và lưu trữ trùng lặp xảy ra khi các bộ, ngành, địa phương triển khai hệ thống thông tin và cơ sở dữ liệu chuyên ngành theo cách độc lập, không dựa trên kiến trúc tổng thể Chính phủ điện tử hoặc Chính phủ số và chưa tuân thủ nghiêm các danh mục dữ liệu chuẩn hóa ở tầm quốc gia. Ví dụ, thông tin về doanh nghiệp có thể vừa

lưu ở cơ sở dữ liệu đăng ký kinh doanh của Bộ Kế hoạch và Đầu tư, vừa lưu ở hệ thống quản lý thuế của Bộ Tài chính, lại vừa xuất hiện trong cơ sở dữ liệu ngành khác như bảo hiểm xã hội hay hải quan. Việc này dẫn đến nhiều *"bản sao"* của cùng một loại dữ liệu, nhưng mỗi bản có thể khác nhau về cấu trúc, định dạng, thậm chí giá trị, khiến đối chiếu, đồng bộ trở nên phức tạp.

Ngoài ra, chồng chéo dữ liệu phản ánh việc nhiều cơ quan cùng thu thập thông tin về cùng một đối tượng hoặc sự kiện mà không có sự phân công, điều phối rõ ràng. Điều này không chỉ lãng phí nguồn lực thu thập và lưu trữ, mà còn tạo ra rủi ro sai lệch và mâu thuẫn dữ liệu khi cơ quan này cập nhật nhưng cơ quan khác không cập nhật kịp thời. Trong nhiều trường hợp, các bộ, ngành còn đặt ra biểu mẫu riêng, yêu cầu doanh nghiệp hoặc người dân cung cấp lại thông tin vốn đã có ở cơ quan khác, làm gia tăng gánh nặng hành chính và chi phí tuân thủ.

Nguyên nhân sâu xa là thiếu một danh mục dữ liệu dùng chung thống nhất và cơ chế bắt buộc tuân thủ. Danh mục dữ liệu dùng chung không chỉ liệt kê tên trường dữ liệu mà còn phải quy định rõ định nghĩa, tiêu chuẩn mã hóa, định dạng, đơn vị đo lường, phương thức cập nhật, quyền truy cập và mức độ bảo mật. Hiện nay, danh mục này chưa được ban hành hoặc áp dụng đồng bộ ở tất cả các cấp, dẫn đến mỗi cơ quan sử dụng một *"phiên bản"* dữ liệu riêng. Hệ quả là việc kết nối, chia sẻ và khai thác dữ liệu bị cản trở. Các nền tảng tích hợp, chia sẻ dữ liệu khi triển khai thường phải xây dựng nhiều bộ chuyển đổi để đồng bộ dữ liệu từ các nguồn khác nhau, tốn kém thời gian và chi phí. Quan trọng hơn, dữ liệu không thống nhất sẽ làm giảm độ tin cậy của phân tích và ra quyết định dựa trên dữ liệu, đặc biệt trong các lĩnh vực đòi hỏi phản ứng nhanh như phòng chống dịch bệnh, an ninh trật tự hay quản lý thị trường.

Thứ ba, các trung tâm dữ liệu đầu tư thiếu đồng bộ, không đồng nhất về tiêu chuẩn, quy chuẩn kỹ thuật, không thường xuyên được kiểm tra, bảo trì, nâng cấp dẫn đến nguy cơ không bảo đảm an ninh, an toàn hệ thống. Điều này phản ánh một thực trạng đáng lo ngại trong phát triển hạ tầng dữ liệu của Việt Nam, đặc biệt trong bối cảnh Nghị quyết 81/2023/QH15 đã đặt mục tiêu hình thành cụm trung tâm dữ liệu quốc gia và đưa Việt Nam trở thành trung tâm dữ liệu của khu vực. Trước hết, thiếu đồng bộ thể hiện ở việc mỗi bộ, ngành, địa phương tự đầu tư trung tâm dữ liệu theo nhu cầu riêng, sử dụng thiết bị, phần mềm và công nghệ khác nhau, không dựa trên một kiến trúc và lộ trình chung ở cấp quốc gia. Điều này dẫn đến tình trạng *"mảnh ghép rời rạc"* thay vì một hệ thống hạ tầng thống nhất, khó đạt khả năng mở rộng và liên thông dữ liệu hiệu quả.



Hạ tầng công nghệ không được bảo trì sẽ gây lãng phí ngân sách

Tiếp theo, không đồng nhất về tiêu chuẩn, quy chuẩn kỹ thuật là vấn đề cốt lõi cản trở việc tích hợp và chia sẻ dữ liệu an toàn. Một số trung tâm dữ liệu chưa đáp ứng các tiêu chuẩn quốc tế như TIA-942, ISO/IEC 27001 hay

ISO/IEC 20000, trong khi tiêu chuẩn quốc gia về thiết kế, vận hành và an toàn thông tin chưa được áp dụng đồng bộ. Hậu quả là chất lượng dịch vụ, độ tin cậy, tính sẵn sàng và khả năng phòng chống sự cố của các trung tâm dữ liệu không đồng đều, gây rủi ro khi cần kết nối và vận hành các ứng dụng, dịch vụ liên thông ở quy mô quốc gia.

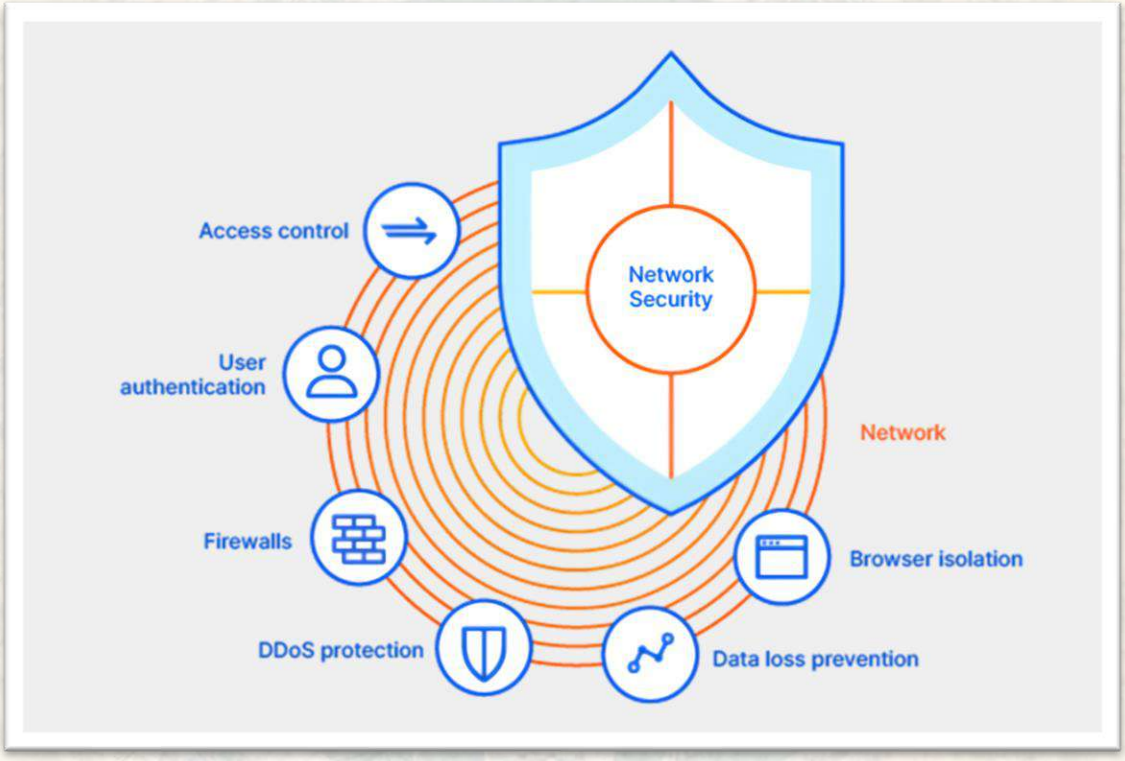
Ngoài ra, không thường xuyên được kiểm tra, bảo trì, nâng cấp là nguyên nhân khiến nhiều trung tâm dữ liệu dần lạc hậu so với tốc độ phát triển công nghệ. Hệ thống làm mát, nguồn điện dự phòng, tường lửa và thiết bị bảo mật nếu không được kiểm tra định kỳ sẽ suy giảm hiệu năng và khả năng chống chịu trước sự cố. Thực tế cho thấy, một số trung tâm dữ liệu ở địa phương vẫn sử dụng phần cứng đã vận hành trên 7 - 10 năm, không còn được nhà sản xuất hỗ trợ, hoặc phần mềm quản trị chưa được cập nhật bản vá bảo mật mới nhất, làm tăng nguy cơ bị tấn công mạng và mất dữ liệu.

Hệ quả của các tồn tại này là nguy cơ mất an ninh, an toàn hệ thống ở mức cao. Một trung tâm dữ liệu không đạt chuẩn và không được bảo trì định kỳ dễ trở thành *"điểm yếu"* cho toàn bộ mạng lưới hạ tầng dữ liệu quốc gia, có thể dẫn tới rò rỉ thông tin, gián đoạn dịch vụ công trực tuyến hoặc mất dữ liệu quan trọng. Trong bối cảnh Luật Dữ liệu 2024 yêu cầu tích hợp, chia sẻ và bảo đảm an toàn dữ liệu ở quy mô toàn quốc, việc duy trì các trung tâm dữ liệu không đạt chuẩn sẽ là rào cản lớn. Do đó, để khắc phục, cần ban hành và áp dụng thống nhất bộ tiêu chuẩn, quy chuẩn kỹ thuật cho trung tâm dữ liệu, gắn với cơ chế bắt buộc kiểm định định kỳ, bảo trì, nâng cấp theo chu kỳ. Đồng thời, nên ưu tiên mô hình tập trung hoặc cụm trung tâm dữ liệu liên vùng, bảo đảm đồng bộ về công nghệ, tối ưu chi phí và nâng cao khả năng bảo vệ dữ liệu quốc gia.

Bốn là, một số bộ, ngành, địa phương thuê dịch vụ hạ tầng công nghệ thông tin tiềm ẩn nhiều rủi ro về an ninh an toàn thông tin do chưa thực sự quản lý, kiểm soát được dữ liệu nhà nước trên hạ tầng của doanh nghiệp. Thực tế, việc thuê dịch vụ hạ tầng công nghệ thông tin (như máy chủ vật lý, máy chủ ảo, dịch vụ lưu trữ đám mây, hạ tầng mạng…) từ các doanh nghiệp cung cấp dịch vụ số giúp các cơ quan nhà nước giảm chi phí đầu tư ban đầu, tận dụng công nghệ hiện đại và mở rộng quy mô nhanh chóng khi có nhu cầu. Đây là giải pháp được nhiều đơn vị áp dụng trong bối cảnh ngân sách hạn chế và yêu cầu triển khai nhanh các hệ thống dịch vụ công trực tuyến. Tuy nhiên, hình thức này tiềm ẩn rủi ro lớn về an ninh, an toàn thông tin nếu không được thiết kế và quản lý chặt chẽ. Khi dữ liệu nhà nước bao gồm dữ liệu cá nhân, dữ liệu nhạy cảm hoặc dữ liệu quan trọng được lưu trữ, xử lý trên hạ tầng của doanh nghiệp, cơ quan nhà nước không nắm toàn quyền kiểm soát vật lý và kỹ thuật đối với hạ tầng đó. Điều này dẫn tới các nguy cơ: Rò rỉ hoặc bị truy cập trái phép nếu nhà cung cấp dịch vụ không đảm bảo chuẩn bảo mật hoặc bị tấn công; Phụ thuộc công nghệ và dữ liệu vào nhà cung cấp, khó chuyển đổi hoặc thu hồi dữ liệu khi hợp đồng kết thúc; Rủi ro từ quản trị nội bộ của doanh nghiệp, như nhân viên có thể truy cập trái phép vào dữ liệu nếu không có cơ chế phân quyền và giám sát chặt chẽ; Nguy cơ pháp lý quốc tế nếu dữ liệu được lưu trữ ở máy chủ đặt ngoài lãnh thổ Việt Nam, có thể chịu tác động từ luật pháp nước sở tại và ảnh hưởng đến chủ quyền dữ liệu quốc gia.

Một ví dụ thực tế có thể xảy ra là một số địa phương triển khai dịch vụ công trực tuyến trên nền tảng thuê ngoài nhưng không quy định rõ yêu cầu về tiêu chuẩn an toàn thông tin, vị trí lưu trữ dữ liệu hoặc cơ chế sao lưu, phục hồi. Kết quả là khi nhà cung cấp gặp sự cố hoặc bị tấn công mạng, hệ

thống bị gián đoạn, dữ liệu khó khôi phục đầy đủ và nhanh chóng. Nguyên nhân chủ yếu xuất phát từ thiếu khung pháp lý và tiêu chuẩn kỹ thuật ràng buộc khi thuê dịch vụ hạ tầng công nghệ thông tin cho dữ liệu nhà nước. Hợp đồng thuê thường chỉ tập trung vào yếu tố chi phí và tính năng kỹ thuật, chưa quy định đầy đủ các điều khoản về an toàn thông tin, quyền kiểm tra - giám sát của cơ quan nhà nước, hay yêu cầu tuân thủ tiêu chuẩn bảo mật quốc tế và quốc gia.

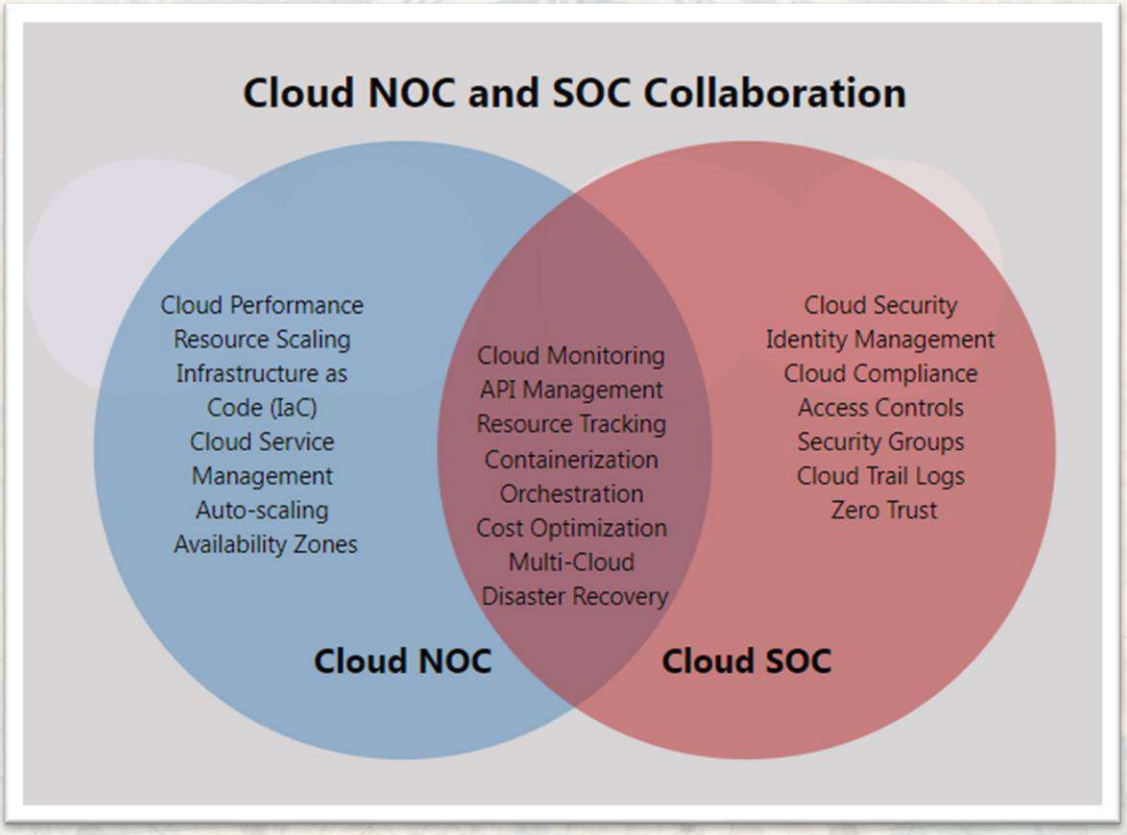


Một số tiêu chuẩn về an toàn kết nối - Ảnh: Cloudflare

Năm là, nhân lực vận hành, quản trị các hệ thống thông tin vừa thiếu, vừa yếu. Trước hết, "thiếu" ở đây bao hàm cả số lượng và cơ cấu chuyên môn. Nhiều bộ, ngành, địa phương chưa hình thành đầy đủ các vị trí chuyên trách về quản trị dữ liệu, kiến trúc hệ thống, bảo mật, vận hành hạ tầng trung tâm dữ liệu hay nền tảng tích hợp - chia sẻ. Thay vào đó, một số cán bộ kiêm nhiệm công việc lĩnh vực công nghệ thông tin, dẫn tới việc vận hành chủ yếu theo hướng "chữa cháy", thiếu tầm nhìn dài hạn và khả năng tối ưu hóa hệ

thống. Ở cấp trung tâm dữ liệu hoặc Cơ sở dữ liệu quốc gia, số lượng nhân sự được đào tạo bài bản về quản trị dữ liệu, quản trị cơ sở dữ liệu, an toàn thông tin hay giám sát vận hành (NOC/SOC) còn rất hạn chế.

Tiếp đến, "yếu" thể hiện ở khoảng trống về kỹ năng và kinh nghiệm chuyên sâu. Hệ quả của tình trạng thiếu và yếu nhân lực là khó đảm bảo vận hành ổn định, an toàn, liên tục cho các hệ thống thông tin quan trọng; khó đáp ứng yêu cầu tích hợp, chia sẻ dữ liệu với các cơ quan khác; và hạn chế khả năng phân tích, khai thác dữ liệu để hỗ trợ ra quyết định chính sách. Điều này cũng khiến việc triển khai Luật Dữ liệu 2024 - vốn đòi hỏi chuẩn hóa, liên thông, bảo mật và khai thác hiệu quả dữ liệu - gặp nhiều thách thức.



Cơ chế giám sát vận hành NOC và SOC - Ảnh: Internet

Sáu là, các cơ sở dữ liệu quốc gia theo Quyết định số 714/QĐ-TTg ngày 22/5/2015 của Thủ tướng Chính phủ chưa được xây dựng đầy đủ. Trong

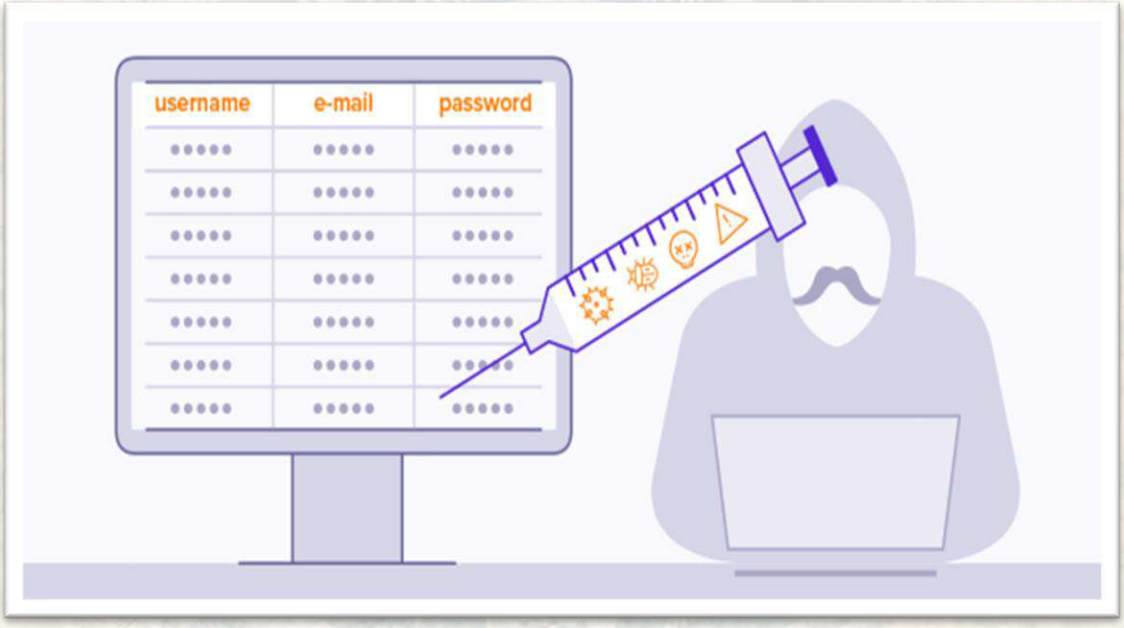
số các cơ sở dữ liệu, tiêu biểu là cơ sở dữ liệu quốc gia về dân cư và cơ sở dữ liệu đăng ký doanh nghiệp tương đối đảm bảo, số có sở dữ liệu còn lại đang ở tình trạng chưa hoàn thành toàn bộ hạng mục hoặc chưa vận hành đồng bộ trên phạm vi toàn quốc, thiếu chuẩn kết nối - chia sẻ dữ liệu liên thông với các hệ thống chuyên ngành và địa phương, chưa số hóa và làm sạch dữ liệu đầy đủ, dẫn đến dữ liệu thiếu độ chính xác và kịp thời, chưa ban hành hoặc chưa áp dụng đồng bộ tiêu chuẩn, quy chuẩn kỹ thuật để bảo đảm khả năng tích hợp vào hạ tầng dữ liệu quốc gia và thiếu cơ chế cập nhật dữ liệu theo thời gian thực hoặc gần thời gian thực, khiến thông tin bị chậm so với thực tế.



Lực lượng Công an Thủ đô tăng cường thu thập, hướng dẫn, kết nối phát triển dữ liệu để phục vụ nhân dân - Ảnh: Báo Công an nhân dân

Bảy là, nhiều hệ thống thông tin còn lỗ hổng bảo mật, không đủ điều kiện kết nối, chia sẻ dữ liệu với hệ thống thông tin của các cơ quan, tổ chức khác. Lỗ hổng bảo mật có thể tồn tại ở nhiều tầng: từ hạ tầng vật lý (máy

chủ, lưu trữ, thiết bị mạng) cho tới tầng ứng dụng và quản trị. Nhiều hệ thống chưa được thiết kế theo mô hình an toàn ngay từ đầu, thiếu cơ chế phân tách vùng tin cậy, chưa mã hóa toàn bộ dữ liệu nhạy cảm ở trạng thái lưu trữ và truyền dẫn, hoặc chưa có cơ chế giám sát - ghi vết truy cập theo thời gian thực. Điều này dẫn tới nguy cơ bị khai thác bởi các cuộc tấn công mạng như SQL injection, cross-site scripting, tấn công từ chối dịch vụ (DDoS), hay tấn công chiến quyền kiểm soát. Năm 2023, tổng cộng 13.900 vụ tấn công mạng nhắm vào các tổ chức tại Việt Nam, trong đó chính phủ và hệ thống trọng yếu là mục tiêu hàng đầu[186].



SQL injection nhằm mục đích thu thập khối lượng lớn dữ liệu quan trọng, nhạy cảm - Ảnh: Avast

Tám là, khó khăn trong việc khai thác, liên thông, cung cấp kịp thời dữ liệu để phục vụ giải quyết thủ tục hành chính, dịch vụ công liên thông, phân tích thống kê, đưa ra các chỉ tiêu, chỉ số phục vụ chỉ đạo điều hành của Chính phủ...

[186] Trung tâm Khoa học Công nghệ và Truyền thông Nghệ An (2023), *Năm 2023: Số vụ tấn công mạng nhắm vào các hệ thống tại Việt Nam tăng 9,5%*, Báo điện tử antoanthongtin.vn, https://naict.tttt.nghean.gov.vn/attt/nam-2023-so-vu-tan-cong-mang-nham-vao-cac-he-thong-tai-viet-nam-tang-9-5-571.html, Truy cập ngày 02/08/2025.



Người dân đang thao tác trên dịch vụ hành chính công - Ảnh: VTA

Việc xây dựng cơ sở dữ liệu tập trung đã trở thành xu thế tất yếu và là yêu cầu quan trọng của nhiều quốc gia trên thế giới, như Đan Mạch, Nhật Bản, Trung Quốc, và Hàn Quốc, nơi các hệ thống dữ liệu quốc gia đã được phát triển và vận hành hiệu quả. Trong bối cảnh đó, việc định hướng xây dựng và phát triển Cơ sở dữ liệu tổng hợp quốc gia tại Việt Nam không chỉ là một mục tiêu chiến lược mà còn là yếu tố then chốt trong quá trình chuyển đổi số, nhằm thúc đẩy sự phát triển của Chính phủ số, kinh tế số, và xã hội số. Cơ sở dữ liệu tổng hợp quốc gia sẽ trở thành nền tảng vững chắc cho việc kết nối, chia sẻ và sử dụng dữ liệu, từ đó tạo ra các mô hình ứng dụng phân tích dữ liệu chuyên sâu, mang lại những giá trị mới cho nền kinh tế - xã hội. Điều này không chỉ giúp Việt Nam xây dựng được một hệ thống dữ liệu tin cậy, ổn định và có khả năng liên thông mà còn tạo ra những nền tảng kết nối dữ liệu giữa các cơ quan nhà nước, doanh nghiệp và người dân. Hệ thống dữ liệu này sẽ là công cụ quan trọng để triển khai các giải pháp kết nối, chia sẻ và sử dụng lại

dữ liệu, phát triển các sản phẩm dịch vụ mới, từ đó tạo động lực mới cho sự phát triển của nền kinh tế - xã hội trong giai đoạn chuyển đổi số.

Bên cạnh đó, việc đầu tư vào Cơ sở dữ liệu tổng hợp quốc gia sẽ mang lại hiệu quả kinh tế rõ rệt. So với việc đầu tư cho các hệ thống dữ liệu riêng biệt, một cơ sở dữ liệu tập trung sẽ tiết kiệm chi phí đáng kể và nâng cao hiệu quả sử dụng dữ liệu. Thêm vào đó, cơ sở dữ liệu này sẽ giúp các bộ, ngành và địa phương có thể khai thác chung thông tin mà không cần phải xây dựng các kênh kết nối riêng biệt, từ đó giảm thiểu sự trùng lặp và tăng cường tính hiệu quả trong công tác quản lý.

Tuy nhiên, dù các quy định hiện hành đã đề cập đến cơ sở dữ liệu quốc gia và chuyên ngành, nhưng hệ thống pháp lý về dữ liệu của Việt Nam vẫn còn thiếu sự đồng bộ và rõ ràng. Các văn bản pháp lý hiện nay, như Luật Giao dịch điện tử, Luật An ninh mạng, và Luật An toàn thông tin mạng, mặc dù đã đưa ra các quy định liên quan đến dữ liệu, nhưng chưa đủ đầy đủ, thiếu tính hệ thống và chưa đáp ứng yêu cầu quản lý dữ liệu trong thời kỳ chuyển đổi số. Qua phân tích, thống kê tại các văn bản luật nêu trên thì các luật này đã quy định về các cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành với các nội dung và thành tố như: Trường thông tin có trong cơ sở dữ liệu (có cơ sở dữ liệu đã quy định rõ các trường thông tin, có cơ sở dữ liệu có quy định nhưng chưa cụ thể các trường thông tin và có cơ sở dữ liệu không quy định các trường thông tin); mô tả, định nghĩa về cơ sở dữ liệu (có cơ sở dữ liệu đã được nêu rõ mô tả, định nghĩa cụ thể, có cơ sở dữ liệu có quy định nhưng chưa cụ thể và có cơ sở dữ liệu không được định nghĩa); hình thức khai thác, chia sẻ (có cơ sở dữ liệu đã được quy định cụ thể về hình thức khai thác, chia sẻ dữ liệu, có cơ sở dữ liệu có quy định nhưng chưa cụ thể về hình thức khai thác, chia sẻ và có cơ sở dữ liệu không quy định).



Đồng chí Nguyễn Mạnh Hùng, Nguyên Bộ trưởng Bộ Thông tin và Truyền thông (cũ) phát biểu tại Hội thảo và Triển lãm quốc tế về an toàn, an ninh mạng Việt Nam 2019 - Ảnh: vietnamplus.vn

Trong các luật đã rà soát, chỉ có một số luật có quy định về trách nhiệm của cơ quan chủ quản cơ sở dữ liệu trong việc xây dựng, thu thập, quản lý, vận hành, kết nối, chia sẻ, khai thác, sử dụng thông tin trong cơ sở dữ liệu. Tuy nhiên, tất cả các luật đều: ***(1)*** Không quy định cụ thể, thống nhất về việc xử lý, quản trị dữ liệu (như việc thu thập, số hóa, bảo đảm chất lượng, lưu trữ dữ liệu…); ***(2)*** Chưa quy định về nền tảng phát triển, ứng dụng công nghệ cao trong xử lý dữ liệu; ***(3)*** Chưa quy định việc tạo lập cơ sở dữ liệu được tổng hợp từ các cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành phục vụ công tác chỉ đạo điều hành, hoạch định đường lối, chính sách, phát triển kinh tế - xã hội, cải cách thủ tục hành chính, dịch vụ công, bảo đảm lợi ích của tổ chức, cá nhân; ***(4)*** Chưa quy định sản phẩm, dịch vụ liên quan đến dữ liệu đang phát triển trên thế giới như sàn giao dịch dữ liệu, dịch vụ trung gian dữ

liệu, dịch vụ phân tích, tổng hợp dữ liệu… Trong khi đó, việc thiết lập thị trường dữ liệu, xây dựng và phát triển các sản phẩm, dịch vụ liên quan đến dữ liệu hiện nay lại có vai trò rất quan trọng, nó được xem là yếu tố đột phá để từng bước tạo lập và thúc đẩy mở thị trường dữ liệu, lấy thị trường dữ liệu làm động lực phát triển dữ liệu và kích thích, thúc đẩy chuyển đổi số các ngành, các lĩnh vực, tăng năng lực cạnh tranh, bảo đảm cho tiến trình chuyển đổi số ở nước ta.

Việc thiếu một hệ thống pháp lý vững chắc về dữ liệu cũng dẫn đến những khoảng trống trong việc quản lý dữ liệu, bảo vệ quyền lợi người dân, và đáp ứng nhu cầu của nền kinh tế số.

Trong bối cảnh đó, Nghị quyết số 175/NQ-CP ngày 30/10/2023 của Chính phủ phê duyệt Đề án Trung tâm dữ liệu quốc gia đã xác định đến Quý IV năm 2025 Trung tâm dữ liệu quốc gia sẽ đi vào hoạt động, là nơi lưu trữ, tổng hợp, phân tích, điều phối dữ liệu, cung cấp hạ tầng cho các bộ, ngành, địa phương. Do đó, việc ban hành Luật Dữ liệu năm 2024 là bước đi chiến lược hết sức quan trọng, cần thiết, cấp thiết, nhằm lấp đầy các khoảng trống pháp lý và tạo ra hành lang pháp lý rõ ràng, hiện đại cho việc quản lý, bảo vệ và sử dụng dữ liệu. Văn bản luật này sẽ không chỉ giúp đảm bảo tính minh bạch, công khai trong việc quản lý dữ liệu mà còn tạo nền tảng vững chắc cho việc phát triển các sản phẩm, dịch vụ dữ liệu, thúc đẩy quá trình chuyển đổi số của các ngành, lĩnh vực, từ đó tăng cường năng lực cạnh tranh và phát triển bền vững của nền kinh tế.

Cùng với Luật Bảo vệ dữ liệu cá nhân, Luật Dữ liệu sẽ giúp Việt Nam xây dựng một hệ sinh thái số an toàn, hiệu quả, bảo vệ quyền lợi của công dân trong môi trường số, đồng thời đảm bảo chủ quyền dữ liệu quốc gia trước các nguy cơ từ việc trao đổi dữ liệu xuyên biên giới. Thực tế, khi nền

kinh tế số phát triển mạnh mẽ, việc kiểm soát và khai thác dữ liệu đúng cách sẽ là yếu tố quan trọng để Việt Nam có thể hội nhập sâu rộng vào nền kinh tế toàn cầu, góp phần vào sự phát triển bền vững trong tương lai.



Luật Dữ liệu: Nền tảng cho Chuyển đổi số Quốc gia -

Ảnh: Trang thông tin điện tử Công an tỉnh Lai Châu

1.4. QUAN ĐIỂM, MỤC TIÊU VÀ ĐỊNH HƯỚNG CHÍNH SÁCH XÂY DỰNG, HOÀN THIỆN PHÁP LUẬT VỀ DỮ LIỆU TẠI VIỆT NAM

1.4.1. Quan điểm chỉ đạo

Trong bối cảnh chuyển đổi số đang trở thành xu thế tất yếu trên toàn cầu, dữ liệu đã và đang khẳng định vai trò là nguồn lực chiến lược của mỗi quốc gia, sánh ngang với các nguồn tài nguyên truyền thống. Việc xây dựng và ban hành Luật Dữ liệu không chỉ đáp ứng yêu cầu quản lý nhà nước trong thời đại số, mà còn hiện thực hóa các chủ trương, đường lối của Đảng và chính sách của Nhà nước về phát triển kinh tế số, xã hội số, Chính phủ số.



Thủ tướng Chính phủ Phạm Minh Chính, Chủ tịch Ủy ban Quốc gia về chuyển đổi số nhấn mạnh, Chính phủ quyết tâm theo đuổi cuộc cách mạng chuyển đổi số một cách sâu rộng - Ảnh: VOV.vn

Để bảo đảm quá trình xây dựng luật có cơ sở chính trị, pháp lý vững chắc và định hướng thống nhất, cần quán triệt đầy đủ các quan điểm chỉ đạo xuyên

suốt. Những quan điểm này vừa kế thừa, cụ thể hóa đường lối, chính sách của Đảng, vừa phản ánh kinh nghiệm rút ra từ thực tiễn quản lý dữ liệu thời gian qua, đồng thời bảo đảm sự tương thích với chuẩn mực quốc tế và phù hợp với điều kiện của Việt Nam. Đây là kim chỉ nam để toàn bộ nội dung của Luật Dữ liệu 2024 đạt được mục tiêu quản trị dữ liệu hiệu quả, an toàn, đồng bộ, phục vụ phát triển bền vững và bảo vệ lợi ích quốc gia. Cụ thể như sau:

Một là, quán triệt và cụ thể hóa quan điểm, chủ trương, chính sách của Đảng về xây dựng, hoàn thiện hệ thống pháp luật về dữ liệu; phù hợp với tiến trình hội nhập, mở rộng giao lưu và hợp tác quốc tế; phục vụ sự nghiệp phát triển kinh tế, văn hóa, xã hội và bảo đảm quốc phòng, an ninh, trật tự, an toàn xã hội. Quan điểm trên thể hiện yêu cầu kết hợp chặt chẽ giữa cơ sở chính trị, kỹ thuật lập pháp và mục tiêu phát triển đất nước. *Về chính trị - pháp lý,* mọi chính sách, quy phạm liên quan đến dữ liệu phải xuất phát từ đường lối của Đảng về công nghiệp hóa, hiện đại hóa, chuyển đổi số, chính phủ số và kinh tế số, đồng thời chuyển hóa thành các nguyên tắc pháp lý khả thi như coi dữ liệu là tài nguyên đặc biệt, phân loại dữ liệu gắn với mức độ bảo vệ, bảo đảm quyền của chủ thể dữ liệu và trách nhiệm giải trình của tổ chức quản lý. *Về hội nhập*, khung pháp luật cần tương thích với chuẩn mực quốc tế về quản trị và an toàn dữ liệu, có cơ chế chuyển dữ liệu xuyên biên giới dựa trên phân loại và đánh giá rủi ro, khuyến khích hợp tác, công nhận chứng chỉ và thử nghiệm công nghệ mới nhưng vẫn giữ vững chủ quyền dữ liệu quốc gia. *Về phát triển kinh tế - xã hội*, pháp luật dữ liệu phải mở đường cho thị trường dữ liệu, định danh chủ thể quyền, xác lập địa vị pháp lý của sản phẩm - dịch vụ dữ liệu, thúc đẩy mở dữ liệu có chọn lọc để nuôi dưỡng đổi mới sáng tạo, đồng thời nâng cao chất lượng dịch vụ công, giảm chi phí tuân thủ thông qua nguyên tắc "một

lần khai báo" và chuẩn hóa danh mục dữ liệu dùng chung. Song song, pháp luật phải bảo đảm an ninh dữ liệu gắn với an ninh quốc gia thông qua các biện pháp phân vùng, mã hóa, kiểm định, ứng cứu sự cố và chế tài đủ mạnh, bảo vệ dữ liệu cốt lõi và dữ liệu quan trọng, đồng thời cân bằng giữa yêu cầu mở và an toàn thông qua cơ chế đánh giá tác động và tham vấn xã hội. Quan điểm này tạo nền tảng để xây dựng một khung pháp luật thống nhất, vừa thúc đẩy phát triển, hội nhập, vừa bảo vệ lợi ích quốc gia và quyền lợi hợp pháp của các chủ thể dữ liệu.



Hình mô tả khung quản trị dữ liệu - Ảnh: FPT IS

Hai là, bảo đảm phù hợp với chủ trương của Đảng, Nhà nước về chuyển đổi số quốc gia, góp phần xây dựng Chính phủ điện tử, Chính phủ số, xã hội số. Quan điểm này đặt ra yêu cầu pháp luật về dữ liệu phải trở thành nền tảng pháp lý trực tiếp cho quá trình số hóa toàn diện hoạt động quản lý nhà nước và đời sống xã hội. Trọng tâm không chỉ dừng ở quản lý và bảo vệ dữ liệu, mà còn tạo môi trường pháp lý để dữ liệu được vận hành như một nguồn lực phát triển. Điều này đòi hỏi hệ thống pháp luật phải định hình rõ mô hình tổ chức, quản trị và khai thác dữ liệu trên quy mô

quốc gia; bảo đảm các cơ sở dữ liệu được tích hợp vào hạ tầng số dùng chung, phục vụ đồng thời cho điều hành, cung cấp dịch vụ công và thúc đẩy đổi mới sáng tạo. Bên cạnh đó, cần thiết lập cơ chế pháp lý để dữ liệu được kết nối liền mạch giữa các nền tảng số của Chính phủ và doanh nghiệp, tạo hệ sinh thái dữ liệu liên thông, an toàn, phục vụ cả quản lý nhà nước và nhu cầu xã hội. Với cách tiếp cận này, pháp luật về dữ liệu sẽ không chỉ hỗ trợ thực thi chiến lược chuyển đổi số, mà còn góp phần hình thành một môi trường số đồng bộ, tin cậy và bền vững.



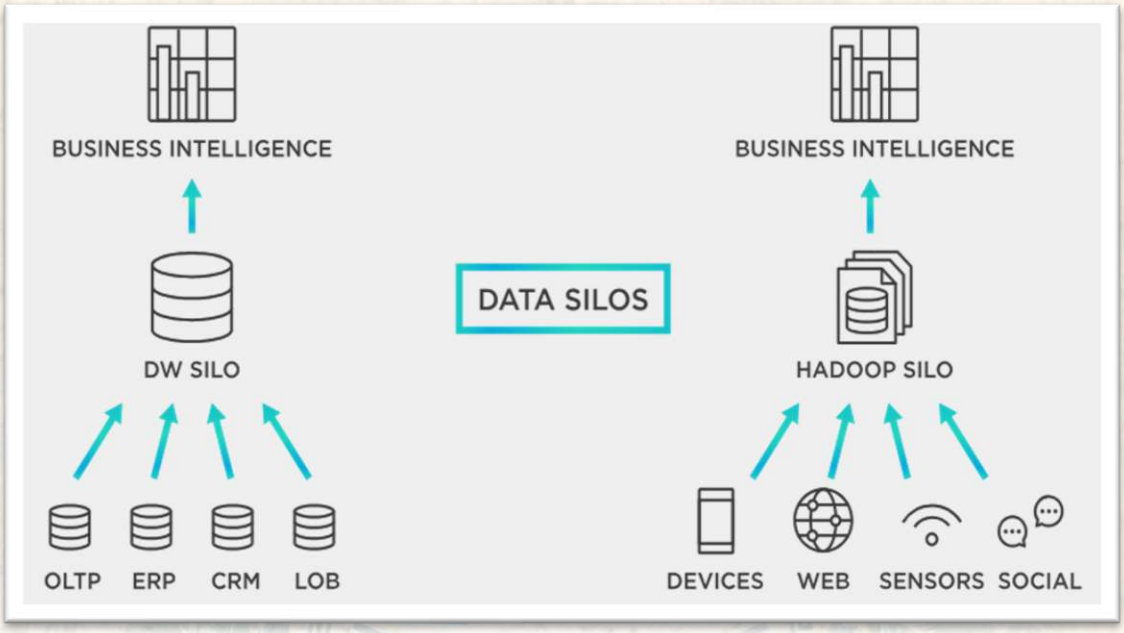
Phó Cục trưởng Cục Thuế Vũ Mạnh Cường phát biểu tại Lễ ký kết quy chế phối hợp trao đổi thông tin - Ảnh: PV

Ba là, việc xây dựng dự án Luật được tiến hành trên cơ sở tổng kết thực tiễn trong những năm qua; khắc phục những tồn tại, bất cập, hạn chế; thực hiện thống nhất, đồng bộ, sử dụng hiệu quả thông tin trong các cơ sở dữ liệu, phục vụ công tác quản lý nhà nước và phát triển kinh tế - xã hội, góp phần

phòng ngừa, đấu tranh chống tội phạm và các vi phạm pháp luật. Quan điểm này thể hiện rõ yêu cầu lập pháp dựa trên nền tảng thực tiễn, lấy thực tiễn làm căn cứ định hình giải pháp pháp lý. Trước hết, việc tổng kết thực tiễn xây dựng và vận hành các cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành trong những năm qua là bước quan trọng để đánh giá những thành tựu đã đạt được, như việc hình thành một số cơ sở dữ liệu trọng yếu và bước đầu triển khai kết nối, chia sẻ dữ liệu phục vụ cải cách thủ tục hành chính. Đồng thời, quá trình này giúp nhận diện rõ những tồn tại như dữ liệu còn phân tán, trùng lặp, thiếu chuẩn hóa; hạ tầng lưu trữ và xử lý chưa đồng bộ; nhân lực quản trị dữ liệu còn hạn chế; hay cơ chế phối hợp, chia sẻ thông tin giữa các cơ quan chưa hiệu quả.

Trên cơ sở đánh giá đó, dự án Luật cần đề xuất các giải pháp khắc phục mang tính hệ thống, bảo đảm thống nhất và đồng bộ trong quản lý dữ liệu trên phạm vi toàn quốc. Điều này bao gồm việc chuẩn hóa danh mục dữ liệu dùng chung, quy định cấu trúc và định dạng thống nhất, thiết lập các tiêu chuẩn - quy chuẩn kỹ thuật bắt buộc cho lưu trữ, kết nối, chia sẻ và bảo mật dữ liệu. Bên cạnh đó, Luật cần thiết kế cơ chế bắt buộc liên thông giữa các hệ thống thông tin của bộ, ngành, địa phương, tránh tình trạng "độc quyền dữ liệu" hay "data silo" gây cản trở khai thác hiệu quả. Việc sử dụng dữ liệu một cách hiệu quả không chỉ phục vụ cho công tác quản lý nhà nước và hoạch định chính sách phát triển kinh tế - xã hội, mà còn đóng vai trò then chốt trong bảo đảm quốc phòng, an ninh và trật tự, an toàn xã hội. Một khung pháp luật đầy đủ sẽ cho phép khai thác dữ liệu để phòng ngừa, phát hiện, điều tra và xử lý kịp thời các hành vi vi phạm pháp luật, đồng thời hỗ trợ phân tích dự báo, nhận diện rủi ro an ninh phi truyền thống. Đặc biệt, Luật cần quy định rõ thẩm quyền, trách nhiệm và giới hạn trong việc tiếp cận, sử

dụng dữ liệu cho mục đích an ninh, bảo đảm vừa đáp ứng yêu cầu bảo vệ Tổ quốc, vừa giữ vững nguyên tắc bảo vệ quyền con người, quyền riêng tư và quyền bảo vệ dữ liệu cá nhân.



Không chỉ các cơ quan nhà nước, data silo cũng là vấn đề đang gặp phải ở nhiều doanh nghiệp - Ảnh: DEHA Digital Solution

Với cách tiếp cận này, dự án Luật Dữ liệu sẽ trở thành công cụ pháp lý mang tính thực tiễn và chiến lược, vừa khắc phục triệt để các điểm nghẽn hiện nay, vừa tạo lập một hệ thống quản trị dữ liệu thống nhất, an toàn, minh bạch và hiệu quả, phục vụ đồng thời cho phát triển, hội nhập và bảo vệ lợi ích quốc gia.

Bốn là, tạo cơ sở pháp lý đầy đủ cho việc khai thác, vận hành Cơ sở dữ liệu tổng hợp quốc gia và phát triển Trung tâm dữ liệu quốc gia; bảo đảm sự đồng bộ, thống nhất trong hệ thống pháp luật. Trước hết, Cơ sở dữ liệu tổng hợp quốc gia và Trung tâm dữ liệu quốc gia là hai cấu phần hạ tầng số chiến lược, giữ vai trò *"trục xương sống"* trong quản trị, chia sẻ và khai thác dữ liệu trên phạm vi toàn quốc. Để các thiết chế này phát huy tối đa giá trị, cần một khung pháp lý quy định rõ ràng về mục tiêu, phạm vi dữ liệu được tích

hợp, nguyên tắc quản trị, cơ chế kết nối - chia sẻ, trách nhiệm của các cơ quan cung cấp và khai thác dữ liệu, cùng các chuẩn mực kỹ thuật bảo đảm tính tương thích và liên thông.

Bên cạnh đó, pháp luật phải xác lập các yêu cầu bắt buộc về an toàn thông tin và bảo mật, phân định rạch ròi giữa dữ liệu cốt lõi, dữ liệu quan trọng và dữ liệu mở để áp dụng các mức bảo vệ và chế độ khai thác phù hợp. Việc phát triển Trung tâm dữ liệu quốc gia cũng đòi hỏi quy định cụ thể về tiêu chuẩn hạ tầng, công nghệ dự phòng, khả năng mở rộng, phương án ứng cứu khi có sự cố, cũng như cơ chế phối hợp vận hành giữa các trung tâm dữ liệu vùng và trung tâm dữ liệu của các bộ, ngành, địa phương.

Quan điểm này còn đặt ra yêu cầu bảo đảm sự đồng bộ, thống nhất trong hệ thống pháp luật. Nghĩa là các quy định về dữ liệu phải ăn khớp với các luật và văn bản pháp luật khác liên quan như Luật An ninh mạng, Luật Bảo vệ dữ liệu cá nhân, Luật Giao dịch điện tử, Luật Công nghệ thông tin..., tránh mâu thuẫn, chồng chéo, hoặc để khoảng trống pháp lý. Chỉ khi hệ thống pháp luật về dữ liệu được thiết kế đồng bộ và nhất quán, Cơ sở dữ liệu tổng hợp quốc gia và Trung tâm dữ liệu quốc gia mới có thể vận hành như một hạ tầng chiến lược, bảo đảm cho sự phát triển của chính phủ số, kinh tế số, xã hội số, đồng thời giữ vững an ninh, chủ quyền dữ liệu quốc gia.

Năm là, tham khảo có chọn lọc pháp luật về quản lý dữ liệu của một số nước, phù hợp với điều kiện thực tiễn Việt Nam. Trên thế giới, nhiều quốc gia và khu vực đã xây dựng hệ thống pháp luật về dữ liệu tương đối hoàn chỉnh, tiêu biểu như Quy định bảo vệ dữ liệu chung của Liên minh châu Âu (GDPR), Luật quản trị dữ liệu của Singapore, Đạo luật bảo vệ thông tin cá nhân của Nhật Bản hay chính sách quản lý dữ liệu mở của Hoa Kỳ. Việc tham khảo các mô hình này giúp Việt Nam tiếp cận sớm những nguyên tắc

và thông lệ tiên tiến như quản trị dữ liệu theo vòng đời, phân loại dữ liệu gắn với cơ chế bảo vệ, bảo đảm quyền của chủ thể dữ liệu, thiết lập chế tài xử lý vi phạm nghiêm khắc, cũng như khuyến khích khai thác dữ liệu phục vụ đổi mới sáng tạo và tăng trưởng kinh tế.

Tuy nhiên, yếu tố *"có chọn lọc"* giữ vai trò quyết định, bởi điều kiện chính trị, pháp lý, trình độ phát triển kinh tế - xã hội, năng lực công nghệ và văn hóa pháp lý của Việt Nam có nhiều khác biệt so với các nước phát triển. Điều này đòi hỏi quá trình tiếp thu phải gắn với việc đánh giá mức độ phù hợp, điều chỉnh quy định cho tương thích với chiến lược phát triển đất nước, định hướng chuyển đổi số quốc gia, và yêu cầu bảo đảm an ninh, chủ quyền dữ liệu. Chẳng hạn, một số cơ chế chuyển dữ liệu xuyên biên giới theo mô hình mở của EU hoặc Mỹ cần được Việt Nam điều chỉnh theo hướng bảo lưu dữ liệu cốt lõi trong lãnh thổ, đồng thời thiết lập các điều kiện và thủ tục kiểm soát phù hợp với yêu cầu an ninh quốc gia.

Như vậy, việc tham khảo pháp luật quốc tế không chỉ giúp Việt Nam rút ngắn thời gian hoàn thiện khung pháp lý về dữ liệu mà còn tránh được những sai sót đã xảy ra ở các nước đi trước, đồng thời tạo nền tảng để hệ thống pháp luật trong nước vừa mang tính hội nhập, vừa phản ánh đúng nhu cầu, đặc thù và ưu tiên chiến lược của quốc gia.

1.4.2. Mục đích

Hiện nay, dữ liệu trở thành nguồn lực chiến lược của quốc gia, việc ban hành Luật Dữ liệu không chỉ là yêu cầu tất yếu để đáp ứng tiến trình chuyển đổi số, mà còn là giải pháp quan trọng nhằm hoàn thiện thể chế, bảo đảm quản trị dữ liệu đồng bộ, an toàn và hiệu quả. Mục đích của việc xây dựng luật được xác định trên cả phương diện quản lý nhà nước và phát triển kinh tế - xã hội, với trọng tâm là thiết lập nền tảng pháp lý cho hạ tầng dữ liệu

quốc gia, thúc đẩy kết nối - chia sẻ - khai thác dữ liệu phục vụ cải cách hành chính, phát triển Chính phủ số, kinh tế số, xã hội số, đồng thời bảo đảm an ninh, chủ quyền dữ liệu. Những mục tiêu này vừa phản ánh định hướng chiến lược của Đảng và Nhà nước, vừa đáp ứng nhu cầu thực tiễn của đời sống kinh tế - xã hội và yêu cầu hội nhập quốc tế trong kỷ nguyên số. Cụ thể:

Một là, tạo sự thống nhất, đồng bộ, sử dụng hiệu quả dữ liệu phục vụ công tác quản lý nhà nước và phát triển kinh tế - xã hội. Trước hết, Luật Dữ liệu cần điều chỉnh toàn diện các hoạt động xử lý, quản trị và điều phối dữ liệu, bao gồm từ khâu thu thập, số hóa, phân loại, lưu trữ, bảo vệ, đến khai thác và tiêu hủy dữ liệu khi hết thời hạn. Việc điều chỉnh này không chỉ nhằm thiết lập chuẩn mực kỹ thuật, bảo đảm tính thống nhất và đồng bộ trong toàn bộ hệ thống dữ liệu quốc gia, mà còn giúp xác định rõ trách nhiệm quản lý nhà nước về dữ liệu giữa các cơ quan trung ương và địa phương, tránh chồng chéo hoặc bỏ trống chức năng. Đây là nền tảng để hình thành cơ chế điều phối thống nhất, bảo đảm mọi dòng chảy dữ liệu được kiểm soát, kết nối và sử dụng đúng mục đích.

Một trụ cột quan trọng được xác lập trong Luật là Cơ sở dữ liệu tổng hợp quốc gia, tập hợp dữ liệu từ các cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành và các nguồn dữ liệu khác. Cơ sở dữ liệu này sẽ là nguồn dữ liệu trung tâm phục vụ vận hành Chính phủ số, thúc đẩy kinh tế số và hình thành xã hội số. Nó phải được thiết kế theo hướng tin cậy, ổn định, an toàn, có khả năng mở rộng và tích hợp với hạ tầng dữ liệu khu vực, quốc tế.

Trên cơ sở đó, Luật cần quy định cơ chế kết nối, chia sẻ và tái sử dụng dữ liệu giữa các cơ quan nhà nước, đồng thời tạo điều kiện cho doanh nghiệp và người dân khai thác dữ liệu theo phạm vi pháp luật cho phép. Khi dữ liệu được lưu thông một cách hợp pháp và hiệu quả, sẽ mở ra khả năng phát triển

các mô hình và ứng dụng phân tích dữ liệu chuyên sâu như trí tuệ nhân tạo, học máy, phân tích dự báo, hỗ trợ ra quyết định chính sách, hay xây dựng các sản phẩm và dịch vụ dữ liệu giá trị gia tăng.



Nhà nước cần thể hiện rõ vai trò của mình trong công cuộc chuyển đổi số ở nước ta - Ảnh: Tạp chí Quản lý Nhà nước

Ngoài ra, để đáp ứng yêu cầu của giai đoạn chuyển đổi số, Luật cần tính đến việc thiết lập các chuẩn kỹ thuật và quy chuẩn bảo mật áp dụng thống nhất cho toàn bộ hạ tầng dữ liệu, bảo đảm tính tương thích, khả năng liên thông và an ninh, an toàn thông tin. Cùng với đó là cơ chế giám sát, đánh giá chất lượng dữ liệu, bảo đảm dữ liệu phục vụ quản lý nhà nước và phát triển kinh tế - xã hội luôn đạt độ chính xác, đầy đủ và cập nhật.

Hai là, phục vụ phát triển Chính phủ số và cải cách, cắt giảm thủ tục hành chính. Trọng tâm trước hết là cung cấp hạ tầng kỹ thuật và pháp lý cho việc xây dựng, vận hành và mở rộng các cơ sở dữ liệu quốc gia, bảo đảm các hệ thống này không tồn tại rời rạc mà được tích hợp đồng bộ, liên thông hiệu quả trên phạm vi toàn quốc. Việc thiết lập cơ chế liên thông dữ liệu giữa các

bộ, ngành, địa phương sẽ giúp loại bỏ tình trạng *"cát cứ dữ liệu"* - khi mỗi cơ quan giữ dữ liệu riêng, không chia sẻ - và thay vào đó hình thành một mạng lưới dữ liệu thống nhất, có thể truy xuất và sử dụng lại theo nguyên tắc *"một lần khai báo"*.



Thủ tướng nhấn mạnh cần cắt giảm, đơn giản hóa tối đa các quy định kinh doanh, thủ tục hành chính - Ảnh: Đoàn Nhạn

Nguyên tắc này đặc biệt quan trọng trong cải cách thủ tục hành chính, vì nó cho phép người dân và doanh nghiệp chỉ cần cung cấp thông tin một lần duy nhất, cơ quan nhà nước sẽ chủ động khai thác thông tin đó từ nguồn dữ liệu đã có. Hệ quả là thời gian xử lý hồ sơ được rút ngắn, chi phí tuân thủ giảm đáng kể, hạn chế tối đa việc yêu cầu giấy tờ trùng lặp. Cùng với đó, quy trình làm việc của cơ quan nhà nước sẽ minh bạch hơn, hạn chế các khâu trung gian không cần thiết, từ đó nâng cao mức độ hài lòng và niềm tin của xã hội đối với bộ máy hành chính.

Không chỉ dừng lại ở việc cải cách thủ tục, hệ thống dữ liệu quốc gia liên thông và chuẩn hóa còn trở thành công cụ chiến lược trong chỉ đạo, điều

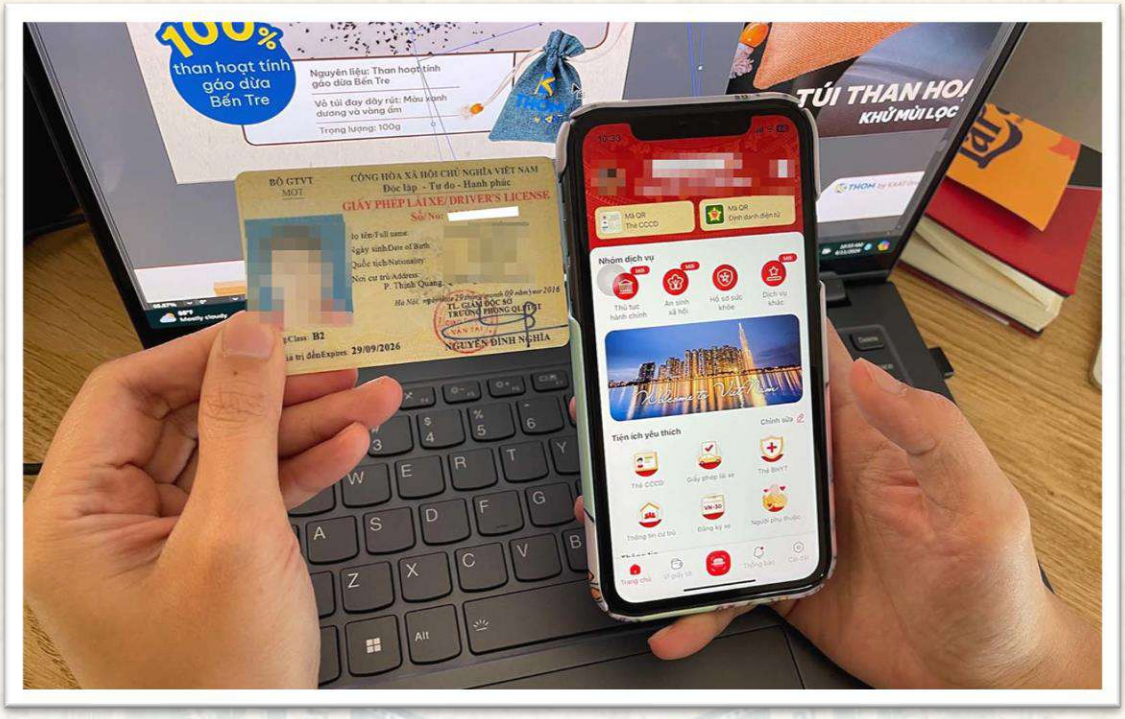
hành và hoạch định chính sách. Khi dữ liệu từ các cơ sở dữ liệu quốc gia, chuyên ngành và địa phương được thu thập, chuẩn hóa và cập nhật liên tục, Chính phủ và các cơ quan quản lý sẽ có trong tay nguồn thông tin chính xác, kịp thời và đầy đủ để thực hiện phân tích, dự báo, đánh giá tác động chính sách và ra quyết định dựa trên bằng chứng (evidence - based policymaking). Điều này đặc biệt cần thiết trong bối cảnh nền kinh tế - xã hội biến động nhanh, các vấn đề an ninh phi truyền thống, thiên tai, dịch bệnh hay biến đổi khí hậu đòi hỏi khả năng phản ứng nhanh, quyết định đúng và kịp thời.

Để đạt được mục tiêu đó, Luật Dữ liệu cần quy định rõ trách nhiệm và phân công nhiệm vụ cụ thể cho từng bộ, ngành, địa phương trong toàn bộ vòng đời dữ liệu - từ xây dựng, vận hành, cập nhật, kết nối đến khai thác. Việc phân công phải đi kèm cơ chế giám sát và đánh giá thường xuyên, nhằm bảo đảm dữ liệu được quản lý một cách kịp thời, thống nhất và hiệu quả, tránh tình trạng *"mạnh ai nấy làm"* hoặc để khoảng trống trách nhiệm.

Ngoài ra, Luật cũng cần xác lập các chuẩn kỹ thuật, quy chuẩn bảo mật và quy trình nghiệp vụ thống nhất cho các hoạt động chia sẻ và khai thác dữ liệu, bảo đảm tính tương thích giữa các hệ thống và an toàn thông tin trong mọi khâu vận hành. Đây là điều kiện cần để dữ liệu thực sự trở thành nguồn lực chiến lược cho Chính phủ số, đồng thời góp phần hình thành môi trường hành chính minh bạch, hiện đại, lấy người dân và doanh nghiệp làm trung tâm phục vụ.

Như vậy, mục tiêu *"phục vụ phát triển Chính phủ số và cải cách, cắt giảm thủ tục hành chính"* trong Luật Dữ liệu không chỉ mang tính kỹ thuật đơn thuần, mà còn là bước đột phá trong đổi mới phương thức quản trị công. Nó giúp Nhà nước chuyển từ mô hình quản lý truyền thống sang mô hình quản trị dựa trên dữ liệu, nơi mà thông tin được khai thác tối đa giá trị để

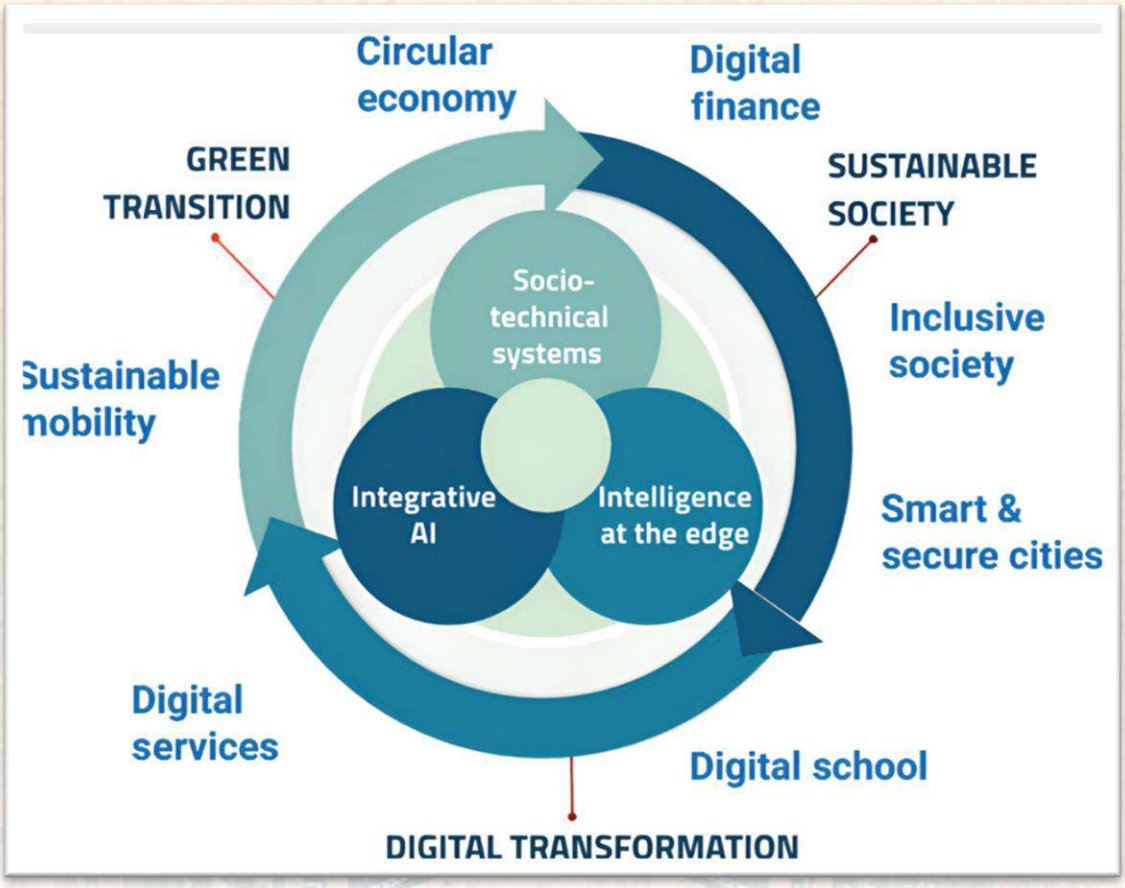
vừa nâng cao hiệu quả điều hành, vừa cải thiện trải nghiệm của người dân và doanh nghiệp trong mọi tương tác với bộ máy hành chính.



Ứng dụng VNeID là thành công đầu tiên của công cuộc chuyển đổi số -Ảnh: Tạp chí Tài chính

Ba là, phát triển kinh tế - xã hội.

Khi các quy định pháp luật về thu thập, quản trị, chia sẻ và khai thác dữ liệu được xác lập rõ ràng, dữ liệu sẽ trở thành một loại tài sản có giá trị thương mại, có thể giao dịch, mua bán, hoặc cung cấp như một dịch vụ. Điều này sẽ tạo điều kiện cho các sản phẩm và dịch vụ dựa trên dữ liệu - từ dịch vụ phân tích dữ liệu lớn, trí tuệ nhân tạo (AI), nền tảng thương mại điện tử, đến các ứng dụng cá nhân hóa - phát triển mạnh mẽ hơn. Kết quả là các giao dịch thương mại trên môi trường số sẽ được diễn ra thường xuyên, liên tục, nhưng vẫn bảo đảm các tiêu chí an toàn, bảo mật và minh bạch, củng cố niềm tin của người dùng và nhà đầu tư.



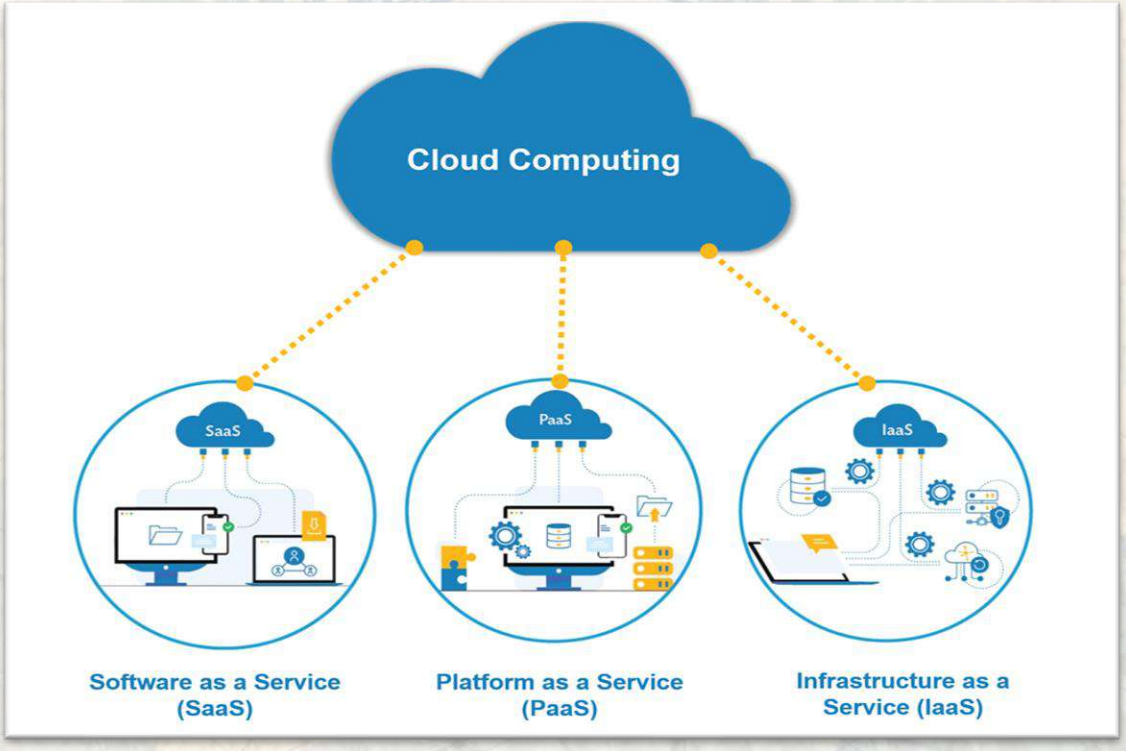
Mô hình chuyển đổi số - Ảnh: ResearchGate

Song song với việc hình thành thị trường dữ liệu, Luật Dữ liệu cũng hướng tới việc xây dựng và từng bước mở rộng kho dữ liệu tổng hợp quốc gia cùng kho dữ liệu mở. Kho dữ liệu tổng hợp sẽ đóng vai trò là hạ tầng cốt lõi, tập hợp dữ liệu từ nhiều nguồn khác nhau - từ cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành cho đến nguồn dữ liệu từ doanh nghiệp - để cung cấp cho các cơ quan nhà nước và các chủ thể có nhu cầu khai thác hợp pháp. Kho dữ liệu mở, ngược lại, sẽ cho phép người dân, doanh nghiệp và tổ chức xã hội tiếp cận dữ liệu miễn phí hoặc với chi phí hợp lý, nhằm phục vụ nghiên cứu, sáng tạo và phát triển các ngành nghề, lĩnh vực kinh doanh mới.

Cơ chế này sẽ khơi thông nguồn lực dữ liệu trong toàn xã hội, biến dữ liệu thành nguyên liệu đầu vào cho đổi mới sáng tạo, khởi nghiệp công nghệ, và chuyển đổi số trong mọi lĩnh vực - từ sản xuất, thương mại, logistics đến

y tế, giáo dục và quản lý đô thị thông minh. Về dài hạn, việc khai thác hiệu quả kho dữ liệu tổng hợp và kho dữ liệu mở sẽ góp phần thúc đẩy tăng trưởng của kinh tế số, gia tăng năng suất lao động, đồng thời hỗ trợ xây dựng một xã hội số toàn diện, nơi dữ liệu phục vụ không chỉ cho phát triển kinh tế mà còn cho nâng cao chất lượng sống của người dân.

Bốn là, phát triển Trung tâm dữ liệu quốc gia. Khi đi vào hoạt động, Trung tâm dữ liệu quốc gia không chỉ là nơi tập trung lưu trữ, quản lý và vận hành các cơ sở dữ liệu quốc gia một cách an toàn, bảo mật và ổn định, mà còn là điểm kết nối liên thông dữ liệu giữa các bộ, ngành, địa phương và các hệ thống dữ liệu chuyên ngành. Đây sẽ là điều kiện tiên quyết để khai thác tối đa giá trị của dữ liệu, hỗ trợ hiệu quả cho công tác quản lý nhà nước, hoạch định chính sách, cũng như cung cấp các dịch vụ công trực tuyến chất lượng cao.



Điện toán đám mây (Cloud Computing) là mấu chốt để phát triển Chính phủ số - Ảnh: Development Asia

Sự hiện diện của Trung tâm dữ liệu quốc gia cũng sẽ thúc đẩy việc khai thác, phân tích và ứng dụng dữ liệu trong mọi lĩnh vực của đời sống kinh tế - xã hội. Với khả năng tích hợp công nghệ tiên tiến như điện toán đám mây (Cloud Computing), phân tích dữ liệu lớn (Big Data Analytics) và trí tuệ nhân tạo (AI), trung tâm sẽ cung cấp hạ tầng mạnh mẽ cho các ứng dụng thông minh, từ quản lý đô thị, giám sát môi trường đến quản trị sản xuất và dịch vụ.

Qua đó, dữ liệu sẽ thực sự trở thành nguồn tài nguyên chiến lược, góp phần nâng cao năng suất lao động, thúc đẩy đổi mới sáng tạo và cải thiện chất lượng sống của người dân. Về mặt chiến lược, Trung tâm dữ liệu quốc gia sẽ là bước đi then chốt để nâng tầm vị thế của Việt Nam trong lĩnh vực kinh tế số, giúp nước ta theo kịp và từng bước cạnh tranh với các quốc gia đi đầu về công nghệ và quản trị dữ liệu. Đây cũng là nền tảng để Việt Nam hội nhập sâu rộng hơn vào nền kinh tế số toàn cầu, thu hút đầu tư nước ngoài, đặc biệt là từ các doanh nghiệp công nghệ và tập đoàn dữ liệu lớn. Đồng thời, trung tâm sẽ bảo đảm an ninh, an toàn và chủ quyền dữ liệu quốc gia, ngăn chặn nguy cơ phụ thuộc vào hạ tầng và dịch vụ dữ liệu từ bên ngoài.

Như vậy, việc phát triển Trung tâm dữ liệu quốc gia không chỉ nhằm phục vụ cho nhu cầu lưu trữ và quản trị dữ liệu, mà còn là bước đi chiến lược để hiện thực hóa các mục tiêu phát triển kinh tế - xã hội, nâng cao năng lực cạnh tranh và bảo đảm an ninh dữ liệu của Việt Nam trong kỷ nguyên số.

1.4.3. Định hướng chính sách xây dựng, hoàn thiện pháp luật về dữ liệu tại Việt Nam

Định hướng chính sách xây dựng, hoàn thiện pháp luật về dữ liệu tại Việt Nam được hình thành trên cơ sở quán triệt chủ trương, đường lối của

Đảng, chính sách của Nhà nước về chuyển đổi số, phát triển kinh tế số và xây dựng Chính phủ số. Mục tiêu trọng tâm là tạo ra một khung pháp lý đồng bộ, thống nhất và hiện đại, đủ khả năng điều chỉnh toàn diện các hoạt động liên quan đến thu thập, xử lý, quản trị, điều phối, chia sẻ, khai thác và bảo vệ dữ liệu trong mọi lĩnh vực của đời sống kinh tế - xã hội. Do đó, các chính sách về xây dựng, hoàn thiện pháp luật về dữ liệu cần bảo đảm các yêu cầu sau:

Thứ nhất, pháp luật về dữ liệu cần bảo đảm sự thống nhất với hệ thống pháp luật hiện hành và phù hợp với cam kết quốc tế mà Việt Nam tham gia. Pháp luật về dữ liệu không thể tồn tại độc lập mà cần hòa nhập vào khung pháp luật tổng thể của quốc gia. Điều này đòi hỏi phải tiến hành rà soát toàn bộ các văn bản pháp luật liên quan, xác định những điểm giao thoa, bổ sung và những xung đột trong các điều khoản trong các văn bản luật khác như Luật An ninh mạng, Luật Bảo vệ bí mật nhà nước, Luật Giao dịch điện tử (sửa đổi), Luật Công nghệ thông tin, đồng thời đáp ứng các tiêu chuẩn quốc tế về quản trị và bảo vệ dữ liệu. Trong bối cảnh toàn cầu hóa và hội nhập số, Việt Nam tham gia nhiều cam kết quốc tế, hiệp định thương mại tự do (FTA), và khuôn khổ hợp tác số như CPTPP, EVFTA, RCEP…

Các cam kết này thường có điều khoản liên quan đến luân chuyển dữ liệu xuyên biên giới, bảo vệ quyền riêng tư, và an ninh mạng. Các nguyên tắc và tiêu chuẩn quốc tế mà các luật gia cần quan tâm đã kể đến như: OECD Privacy Guidelines, APEC Privacy Framework, Nguyên tắc DFFT của G20, các tiêu chuẩn kỹ thuật như ISO 37120, ISO 8000… Việc bảo đảm thống nhất với pháp luật hiện hành và phù hợp cam kết quốc tế không chỉ là yêu cầu pháp lý mà còn là nền tảng chiến lược để pháp luật về dữ liệu có tính ổn định, khả thi và thích ứng lâu dài. Đây là điều kiện tiên quyết để biến dữ liệu

thành nguồn lực thực sự, hỗ trợ cải cách hành chính, phát triển kinh tế số, và bảo vệ an ninh quốc gia.

Thứ hai, định hướng chính sách phải hướng tới tối đa hóa giá trị của dữ liệu như một nguồn lực phát triển. Trên tinh thần xác định dữ liệu như một nguồn tài nguyên mới hay *"tài sản quốc gia"*, việc khai thác dữ liệu không chỉ phục vụ cho mục tiêu quản lý nhà nước mà còn biến dữ liệu thành nguyên liệu cho đổi mới sáng tạo, phát triển sản phẩm, dịch vụ mới và hình thành thị trường dữ liệu tại Việt Nam trong tương lai. Điều này đồng nghĩa với việc dữ liệu phải được nhìn nhận như một loại tài sản có giá trị kinh tế, có thể được định giá, giao dịch và đầu tư khai thác. Một thị trường dữ liệu đúng nghĩa không chỉ dừng ở khâu thu thập và lưu trữ, mà còn bao gồm: Nền tảng giao dịch dữ liệu (là nơi dữ liệu được chào bán, cho thuê hoặc cấp phép sử dụng.); Cơ chế định giá dữ liệu dựa trên độ hiếm, độ chính xác, mức độ cập nhật và giá trị ứng dụng; Cơ chế pháp lý bảo vệ quyền lợi của các chủ thể dữ liệu, ngăn ngừa rủi ro xâm phạm và bảo đảm tuân thủ các quy định về bảo mật, quyền riêng tư. Cần xác lập rõ cơ chế tiếp cận, khai thác và sử dụng dữ liệu mở, dữ liệu dùng chung. Trong đó, dữ liệu mở công khai cho mọi tổ chức, cá nhân khai thác miễn phí hoặc với chi phí rất thấp, nhằm thúc đẩy sáng tạo và dịch vụ cộng đồng; dữ liệu dùng chung là dữ liệu chia sẻ giữa các cơ quan nhà nước, hoặc giữa nhà nước với các tổ chức, doanh nghiệp, có quy định rõ về phạm vi, mục đích và quyền khai thác; và dữ liệu hạn chế, dữ liệu mật yêu cầu kiểm soát nghiêm ngặt, chỉ cung cấp trong điều kiện và phạm vi được phép. Việc phân loại và thiết lập cơ chế tiếp cận rõ ràng sẽ giúp tối ưu hóa giá trị khai thác mà vẫn đảm bảo an ninh, an toàn đối với dữ liệu và các chủ thể có liên quan.



"Dữ liệu của bạn là vàng của tôi" - Ảnh: SimpleSolve

Thứ ba, pháp luật về dữ liệu phải đáp ứng yêu cầu phát triển hạ tầng dữ liệu quốc gia. Hạ tầng dữ liệu quốc gia được hiểu là tập hợp các thành phần kỹ thuật, công nghệ, nền tảng và cơ sở pháp lý cho việc thu thập, lưu trữ, kết nối, chia sẻ và khai thác dữ liệu trên phạm vi toàn quốc. Trong định hướng này, bốn cấu phần cốt lõi được xác định gồm: ***(1)*** Cơ sở dữ liệu tổng hợp quốc gia (trung tâm tích hợp dữ liệu từ các cơ sở dữ liệu quốc gia, các cơ sở dữ liệu chuyên ngành và các nguồn dữ liệu khác đóng vai trò "kho dữ liệu trục" của quốc gia; ***(2)*** Các cơ sở dữ liệu chuyên ngành phục vụ quản lý lĩnh vực cụ thể như y tế, giáo dục, giao thông, dân cư, đất đai...; ***(3)*** Các trung tâm dữ liệu đạt chuẩn đóng vai trò là hạ tầng lưu trữ, xử lý dữ liệu tập trung, bảo đảm năng lực tính toán, lưu trữ và bảo mật theo chuẩn quốc gia và quốc tế; ***(4)*** Nền tảng chia sẻ và tích hợp dữ liệu là lớp hạ tầng số cho phép các cơ quan, tổ chức trao đổi, khai thác dữ liệu an toàn, nhanh chóng và có kiểm soát.

Về yêu cầu tiêu chuẩn kỹ thuật vận hành, một hạ tầng dữ liệu quốc gia hiệu quả cần được thiết kế và vận hành theo bộ tiêu chuẩn kỹ thuật thống

nhất để bảo đảm tính tương thích giữa các hệ thống, cho phép kết nối và trao đổi dữ liệu liên ngành, liên vùng; đáp ứng yêu cầu an ninh, an toàn thông tin. Dữ liệu phải được mã hóa, kiểm soát truy cập, dự báo rủ ro và có các biện pháp phòng chống nguy cơ tấn công mạng từ tội phạm sử dụng công nghệ cao. Trong đó, pháp luật về dữ liệu sẽ là nền tảng điều phối và quản lý thống nhất hạ tầng dữ liệu quốc gia, do đó, cần quy định rõ trách nhiệm đầu tư, quản lý và vận hành các thành phần hạ tầng, cơ chế phối hợp giữa Nhà nước, doanh nghiệp và các bên liên quan trong khai thác và phát triển hạ tầng, tiêu chí, tiêu chuẩn kỹ thuật, quy chuẩn an toàn bắt buộc, cơ chế bảo đảm tài chính, phí dịch vụ, chính sách ưu đãi để khuyến khích đầu tư và duy trì hạ tầng.

Thứ tư, định hướng xây dựng luật phải coi trọng yếu tố bảo đảm an ninh và chủ quyền dữ liệu quốc gia trên không gian mạng.



Chủ quyền không gian mạng trong từng đạo luật về an ninh mạng - Ảnh: Thales

Xuất phát từ việc dữ liệu ngày nay không chỉ là tài nguyên kinh tế mà còn là tài sản chiến lược liên quan trực tiếp đến an ninh quốc gia và chủ

quyền số. Thêm vào đó, trong giai đoạn hiện nay, lượng dữ liệu được lưu trữ, xử lý và truyền đưa xuyên biên giới ngày càng lớn, kéo theo nguy cơ bị khai thác trái phép, tấn công mạng hoặc phụ thuộc hạ tầng số nước ngoài. Nhiều văn kiện quan trọng của Đảng và Nhà nước, như Nghị quyết số 29-NQ/TW (2022) và Nghị quyết số 81/2023/QH15, đều nhấn mạnh yêu cầu bảo đảm chủ quyền dữ liệu như một yếu tố cấu thành an ninh quốc gia trong kỷ nguyên số. Về nội dung, định hướng đề ra một số nội dung trọng tâm sau: ***(i)*** Phân loại dữ liệu, xác định rõ dữ liệu cốt lõi, dữ liệu quan trọng và dữ liệu nhạy cảm; mỗi nhóm có chế độ bảo vệ, lưu trữ và xử lý riêng; ***(ii)*** Quy định điều kiện lưu trữ, xử lý, truyền đưa ra nước ngoài, chỉ cho phép xuất dữ liệu khi đáp ứng yêu cầu an toàn, có hợp đồng ràng buộc pháp lý và được cơ quan có thẩm quyền phê duyệt đối với các nhóm dữ liệu trọng yếu; ***(iii)*** Thiết lập cơ chế giám sát, cảnh báo, ứng phó sự cố, tổ chức hệ thống theo dõi an toàn dữ liệu quốc gia, phát hiện sớm các dấu hiệu xâm nhập, rò rỉ hoặc phá hoại; ban hành quy trình ứng phó nhanh và khôi phục dữ liệu. Bảo vệ quyền và lợi ích hợp pháp của cá nhân, tổ chức, trong đó, tập trung bảo đảm tính minh bạch trong thu thập và xử lý dữ liệu, bảo vệ quyền riêng tư và quyền kiểm soát dữ liệu của chủ thể dữ liệu. Các chủ thể được giao trách nhiệm, có nghĩa vụ bảo đảm an ninh, an toàn dữ liệu cần chú ý nghiên cứu, xây dựng các quy định bảo vệ dữ liệu phải đủ chặt để bảo đảm an ninh, nhưng không được gây cản trở dòng chảy dữ liệu phục vụ thương mại, nghiên cứu và đổi mới sáng tạo. Ngoài ra, cần tăng cường phối hợp liên ngành, đảm bảo sự tham gia của nhiều cơ quan trong và ngoài nhà nước.

Thứ năm, cần tiếp thu có chọn lọc các bài học kinh nghiệm quốc tế về quản lý và khai thác dữ liệu, đồng thời vận dụng linh hoạt để phù hợp với điều kiện thực tiễn Việt Nam.



Mô hình quốc gia thông minh của Singapore - Ảnh: Smartnation

Trong xu hướng toàn cầu về bảo vệ dữ liệu, các quốc gia đều đối mặt với thách thức tương đồng về quản trị và khai thác dữ liệu. Nhiều nước, đặc biệt là các nền kinh tế dẫn đầu như Liên minh Châu Âu (EU), Hoa Kỳ, Singapore hay Hàn Quốc, đã ban hành các đạo luật và cơ chế quản lý dữ liệu tương đối toàn diện. Việc tham khảo kinh nghiệm của họ giúp Việt Nam tránh được các *"bài học đắt giá"*, rút ngắn quá trình thử - sai và định hình nhanh hơn khung pháp lý phù hợp với xu thế quốc tế. Do đó, định hướng này đòi hỏi yêu cầu quá trình xây dựng pháp luật về dữ liệu ở Việt Nam cần nghiên cứu có hệ thống các mô hình quốc tế như Data Governance Act và Data Act của EU về quản trị và chia sẻ dữ liệu; Cloud Act của Hoa Kỳ về quyền tiếp cận dữ liệu xuyên biên giới; chính sách Smart Nation của Singapore về dữ liệu mở và hạ tầng dữ liệu; Luật Bảo vệ thông tin cá nhân của Hàn Quốc… Trong đó, nhà nước không áp dụng kiểu rập khuôn, máy móc mà phải điều chỉnh để phù hợp với điều kiện pháp lý, mức độ phát triển hạ tầng số, năng lực quản lý và đặc thù kinh tế - xã hội của Việt Nam và tham chiếu các tiêu chuẩn quốc tế như tiêu chuẩn dữ liệu mở W3C; khung quản trị dữ liệu DAMA - DMBOK…).

Thứ sáu, định hướng chính sách cần bảo đảm tính khả thi và bền vững. Trong quá trình chuyển đổi số quốc gia, nếu khung pháp luật thiếu tính thích ứng sẽ nhanh chóng lạc hậu, gây khó khăn cho triển khai và hạn chế hiệu quả công tác quản lý. Ngược lại, nếu pháp luật thay đổi quá thường xuyên, sẽ tạo ra sự bất ổn, làm gián đoạn hoạt động quản lý nhà nước và ảnh hưởng tới niềm tin của doanh nghiệp, người dân. Do đó, Luật Dữ liệu phải được thiết kế với tầm nhìn mở, đủ linh hoạt để cập nhật theo tiến bộ công nghệ và thay đổi của môi trường kinh tế - xã hội, nhưng vẫn giữ được sự ổn định cần thiết cho quản trị và thực thi. Cùng với luật, hệ thống văn bản dưới luật phải cụ thể hóa rõ ràng các quy trình, tiêu chuẩn và trách nhiệm, tạo điều kiện thuận lợi cho triển khai thực tế ở cả cấp trung ương và địa phương. Theo đó, các cơ quan chịu trách nhiệm nghiên cứu, xây dựng chính sách, pháp luật về dữ liệu cần thiết kế luật với tầm nhìn mở, cấu trúc luật cần cho phép điều chỉnh linh hoạt thông qua các cơ chế sửa đổi, bổ sung hoặc cập nhật quy định kỹ thuật mà không làm thay đổi toàn bộ khung pháp lý.

Bên cạnh đó, cần có các nguyên tắc cơ bản về quản trị dữ liệu, bảo vệ dữ liệu và phân quyền trách nhiệm phải giữ ổn định để tạo niềm tin cho các chủ thể tham gia. Ngoài ra, những điều khoản cần cụ thể hóa bằng các văn bản dưới luật. Cùng với luật, hệ thống nghị định, thông tư cần quy định chi tiết quy trình, tiêu chuẩn, định mức kỹ thuật và phân công trách nhiệm, nhằm tạo điều kiện thuận lợi cho triển khai thống nhất từ trung ương tới địa phương, phù hợp với năng lực triển khai, các quy định phải tính đến sự khác biệt về nguồn lực, hạ tầng và nhân sự giữa các bộ, ngành, địa phương, có lộ trình thực hiện hợp lý.

Như vậy, định hướng chính sách xây dựng pháp luật về dữ liệu ở Việt Nam không chỉ là việc hoàn thiện khuôn khổ pháp lý, mà còn là bước chiến

lược để biến dữ liệu thành động lực tăng trưởng mới, thúc đẩy cải cách hành chính, nâng cao hiệu quả quản trị, phát triển kinh tế số, xã hội số và bảo đảm vững chắc an ninh dữ liệu quốc gia.

1.4.3.1. Quy định về xây dựng, phát triển, quản trị, xử lý dữ liệu, ứng dụng khoa học công nghệ trong xử lý dữ liệu, quản lý nhà nước về dữ liệu.

- Xác định vấn đề bất cập

Hiện nay, có hơn một trăm văn bản quy phạm pháp luật có quy định liên quan đến dữ liệu, tuy nhiên các văn bản này chưa có quy định thống nhất về việc xây dựng, thu thập, quản lý, vận hành, kết nối, chia sẻ, khai thác, sử dụng thông tin trong các cơ sở dữ liệu; chưa có quy định về bảo vệ dữ liệu, hoạt động truy cập, truy xuất, thu hồi, mã hóa, giải mã, sao chép, chia sẻ, truyền, chuyển giao, xóa, hủy dữ liệu; chưa có quy định đầy đủ về quản trị dữ liệu, các dịch vụ liên quan đến dữ liệu, xác định và quản lý rủi ro có thể phát sinh trong chuỗi cung ứng dữ liệu, ứng dụng khoa học công nghệ trong xử lý dữ liệu dạng có xu hướng phát triển phổ biến trên thế giới như công nghệ trí tuệ nhân tạo, điện toán đám mây, công nghệ chuỗi khối, công nghệ truyền thông dữ liệu, công nghệ intemet vạn vật, công nghệ dữ liệu lớn và các công nghệ hiện đại khác... Do đó, công tác quản lý dữ liệu còn bộc lộ một số bất cập, thiếu sót, hạn chế; chưa thúc đẩy sự phát triển các sản phẩm, dịch vụ liên quan đến dữ liệu. Vì vậy, cần phải ban hành luật để điều chỉnh các hoạt động liên quan đến dữ liệu, nhất là các chính sách về xây dựng, phát triển, xử lý, quản trị, bảo vệ dữ liệu, ứng dụng khoa học công nghệ trong xử lý dữ liệu, xác định và quản lý rủi ro có thể phát sinh trong chuỗi cung ứng dữ liệu; hợp tác quốc tế dữ liệu để góp phần nâng cao hiệu lực quản lý nhà nước về dữ liệu và thúc đẩy phát triển kinh tế - xã hội.

Bên cạnh đó, hiện nay tại nước ta chỉ có tiêu chuẩn dữ liệu thông tin đầu vào của cơ sở dữ liệu tài liệu lưu trữ ban hành theo Thông tư số 02/2019/TT-BNV về quy định tiêu chuẩn dữ liệu thông tin đầu vào và yêu cầu bảo quản tài liệu lưu trữ điện tử tiêu chuẩn quốc gia TCVN 9250:2021 về yêu cầu hạ tầng kỹ thuật viễn thông của Trung tâm dữ liệu; chưa có tiêu chuẩn chung về dữ liệu, do vậy, cần có một tiêu chuẩn chung để áp dụng thống nhất, đồng bộ.



Luật chồng chéo - Ảnh: HẢI LÂM

Ngoài ra hiện nay chưa có quỹ phát triển dữ liệu quốc gia để hỗ trợ việc đầu tư xây dựng, phục vụ hoạt động của Trung tâm dữ liệu quốc gia; hỗ trợ việc nghiên cứu giải pháp gia tăng bảo vệ dữ liệu, chuyển giao công nghệ về dữ liệu, phát triển ứng dụng công nghệ cao liên quan đến dữ liệu; hỗ trợ khen thưởng tổ chức, cá nhân có thành tích trong công tác xây dựng, phát triển dữ

liệu và hỗ trợ hợp tác quốc tế về dữ liệu. Vì vậy cần phải có quy định để quản lý các hoạt động của Quỹ phát triển dữ liệu quốc gia.

- Mục tiêu giải quyết vấn đề

Quy định về chiến lược dữ liệu; xử lý dữ liệu (gồm các hoạt động thu thập, ghi, phân tích, tổng hợp, xác nhận, xác thực, lưu trữ, truy xuất, truy hồi, mã hóa, giải mã, sao chép, chia sẻ, truyền đưa, chuyển giao, xóa, hủy dữ liệu hoặc các hoạt động khác có liên quan); quản trị dữ liệu, bảo vệ dữ liệu, chất lượng dữ liệu, cung cấp dữ liệu; xác định và quản lý rủi ro có thể phát sinh trong chuỗi cung ứng dữ liệu; hợp tác quốc tế về dữ liệu; ứng dụng khoa học - công nghệ trong xử lý dữ liệu đang có xu hướng phát triển phổ biến trên thế giới như công nghệ truyền thông dữ liệu, công nghệ internet vạn vật và công nghệ dữ liệu lớn…

Quy định về Quỹ phát triển dữ liệu quốc gia là quỹ tài chính Nhà nước ngoài ngân sách, được hình thành ở Trung ương để huy động nguồn lực xã hội hỗ trợ việc xây dựng, phát triển dữ liệu quốc gia và dự kiến được hình thành từ các nguồn tài chính: Đóng góp tự nguyện của các tổ chức, cá nhân trong nước, ngoài nước; đóng góp từ doanh thu của đơn vị sự nghiệp công lập thuộc Trung tâm dữ liệu quốc gia.

- Giải pháp

Một là, quy định về thu thập, ghi, phân tích, tổng hợp, xác nhận, xác thực, lưu trữ, chỉnh sửa, cập nhật, điều chỉnh, công khai, kết hợp, truy cập, truy xuất, thu hồi, mã hóa, giải mã, sao chép, chia sẻ, truyền đưa, chuyển giao, xóa, hủy dữ liệu; chất lượng dữ liệu, cung cấp dữ liệu. Đầu tiên, thu thập và ghi dữ liệu cần được thực hiện theo phương thức minh bạch và hợp pháp, đảm bảo rằng các nguồn chủ thể dữ liệu như công dân, tổ chức, doanh nghiệp và cơ quan nhà nước phải tuân thủ tiêu chuẩn bảo mật nghiêm ngặt,

bảo vệ quyền riêng tư và nhận được sự đồng thuận của các bên liên quan khi thu thập thông tin nhạy cảm. Việc phân tích và tổng hợp dữ liệu phải được quy định rõ ràng, nhằm đảm bảo dữ liệu được sử dụng hợp lý và không xâm phạm quyền lợi cá nhân, đồng thời phù hợp với mục đích đã được thông báo từ trước. Các quy trình xác thực và chỉnh sửa dữ liệu cần được thiết lập để đảm bảo tính chính xác và cập nhật của dữ liệu, cùng với cơ chế thông báo cho các bên liên quan khi có sự thay đổi.



Quy định cụ thể càng cụ thể, minh mạch càng thúc đẩy kinh tế số phát triển - Ảnh: FPT IS

Về quyền công khai, truy cập, truy xuất và thu hồi dữ liệu, dữ liệu cần được công khai minh bạch theo quy định của pháp luật hoặc cam kết với người dân, nhưng cũng phải có cơ chế bảo vệ quyền riêng tư, hạn chế quyền truy cập nếu không có sự đồng ý của người dân, đồng thời bảo vệ quyền thu hồi dữ liệu của họ. Để bảo vệ an toàn dữ liệu, các biện pháp mã hóa phải được áp dụng trong quá trình truyền tải hoặc lưu trữ, và giải mã chỉ có thể thực hiện khi có yêu cầu hợp pháp, đảm bảo không xâm phạm quyền riêng tư. Việc chia sẻ và chuyển giao dữ liệu giữa các tổ chức hoặc quốc gia cần tuân thủ các

nguyên tắc bảo vệ dữ liệu cá nhân và an ninh quốc gia, đồng thời các thỏa thuận hợp tác quốc tế cần được xác minh và thực hiện một cách đầy đủ.

Ngoài ra, quy định về việc xóa và hủy dữ liệu là rất quan trọng để bảo vệ quyền riêng tư và giảm thiểu nguy cơ bị lạm dụng, với yêu cầu các tổ chức phải xóa hoặc hủy dữ liệu khi không còn cần thiết hoặc khi có yêu cầu hợp pháp từ cá nhân hoặc cơ quan nhà nước. Những quy định này không chỉ bảo vệ quyền lợi của cá nhân mà còn đảm bảo sự an toàn và bảo mật của hệ thống dữ liệu trong môi trường pháp lý quốc gia và quốc tế.

Hai là, quy định về quản lý nhà nước về dữ liệu. Quản lý nhà nước về dữ liệu là một yếu tố thiết yếu trong việc đảm bảo sự phát triển bền vững của hạ tầng dữ liệu quốc gia và bảo vệ quyền lợi của công dân. Để thực hiện nhiệm vụ này, cần thiết lập một cơ quan trung ương có đủ quyền lực và trách nhiệm giám sát mọi hoạt động liên quan đến thu thập, xử lý, bảo vệ và công khai dữ liệu. Cơ quan này sẽ đóng vai trò quyết định trong việc xây dựng các chính sách, quy trình và tiêu chuẩn pháp lý về quản lý dữ liệu, từ đó tạo ra khung pháp lý vững chắc giúp các tổ chức và cá nhân tuân thủ các quy định về bảo mật và quyền riêng tư. Các bộ, ngành liên quan cần phối hợp chặt chẽ trong việc xây dựng các chính sách này để đảm bảo tính đồng bộ và hiệu quả trong việc quản lý và xử lý dữ liệu trên phạm vi toàn quốc.

Hệ thống giám sát này cũng phải bao gồm các cơ chế xử lý vi phạm về dữ liệu, chẳng hạn như các hình thức xử phạt hành chính đối với các tổ chức vi phạm các quy định về bảo vệ dữ liệu cá nhân hoặc các hoạt động thu thập, sử dụng dữ liệu trái phép. Đồng thời, cơ quan quản lý nhà nước sẽ thực thi các biện pháp bảo vệ quyền lợi của người dân, đảm bảo rằng quyền riêng tư của cá nhân không bị xâm phạm, và mọi hoạt động xử lý dữ liệu phải được thực hiện minh bạch và hợp pháp.



Vai trò của Nhà nước trong quản lý dữ liệu số là không thể thay thế - Ảnh: CEBID

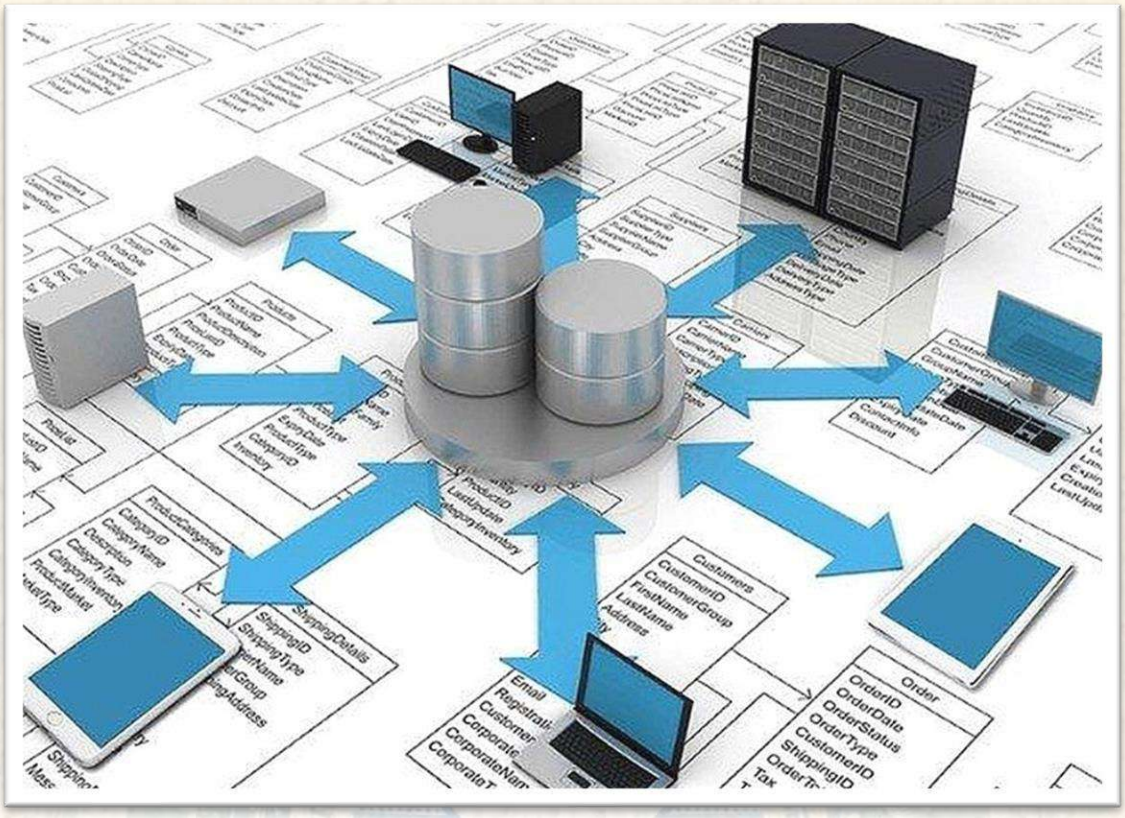
Một phần quan trọng của quy định về quản lý nhà nước là việc xây dựng các cơ sở dữ liệu quốc gia. Các cơ sở dữ liệu này cần được xây dựng và quản lý dưới sự giám sát chặt chẽ của cơ quan nhà nước, nhằm phục vụ các mục tiêu quản lý, thống kê, và ra quyết định của chính phủ. Việc xây dựng các hệ thống lưu trữ và xử lý dữ liệu tập trung không chỉ giúp tối ưu hóa việc sử dụng dữ liệu trong các lĩnh vực công, mà còn giúp giảm thiểu tình trạng quản lý phân tán, thiếu đồng bộ, đảm bảo tính nhất quán và chính xác trong các quyết định của chính phủ. Bên cạnh đó, các hệ thống này cần phải được bảo vệ an toàn khỏi các mối đe dọa từ các cuộc tấn công mạng và bảo vệ khỏi sự truy cập trái phép, đồng thời hỗ trợ việc chia sẻ thông tin giữa các cơ quan nhà nước và các tổ chức liên quan một cách hợp pháp và có kiểm soát.

Do đó, quản lý nhà nước về dữ liệu không chỉ là việc xây dựng các cơ sở hạ tầng công nghệ mà còn liên quan đến việc tạo dựng một hệ thống pháp lý hoàn thiện, đảm bảo tính minh bạch, bảo vệ quyền lợi cá nhân và tối ưu hóa việc sử dụng dữ liệu trong quản lý nhà nước.

Ba là, quy định về chiến lược dữ liệu. Chiến lược dữ liệu là yếu tố nền tảng trong việc xây dựng và triển khai chính sách dữ liệu quốc gia, giúp xác định hướng đi dài hạn và các mục tiêu quan trọng cho việc phát triển và quản lý dữ liệu. Để đạt được hiệu quả trong việc sử dụng dữ liệu, chiến lược dữ liệu cần bắt đầu từ việc xác định các mục tiêu cụ thể và thực tế, bao gồm việc đảm bảo an toàn và bảo mật dữ liệu. Điều này không chỉ bao gồm việc triển khai các biện pháp bảo vệ dữ liệu cá nhân mà còn phải bảo vệ dữ liệu quốc gia khỏi các mối đe dọa từ các cuộc tấn công mạng, hacker, và các yếu tố bên ngoài có thể ảnh hưởng đến tính toàn vẹn của dữ liệu.

Một trong những mục tiêu quan trọng của chiến lược dữ liệu là thúc đẩy sự minh bạch và khả năng chia sẻ dữ liệu trong cả khu vực công và tư. Việc này không chỉ giúp tăng cường sự hợp tác giữa các cơ quan nhà nước và các tổ chức, mà còn tạo ra nền tảng cho sự phát triển của các dịch vụ công trực tuyến, cũng như các sản phẩm, dịch vụ mới trong khu vực tư nhân. Để làm được điều này, chiến lược dữ liệu cần đề ra các quy định cụ thể về việc chia sẻ, trao đổi và sử dụng dữ liệu giữa các tổ chức, cũng như các tiêu chuẩn về bảo mật và quyền riêng tư nhằm tạo sự tin tưởng cho người dân và các tổ chức trong việc sử dụng và chia sẻ dữ liệu.

Ngoài ra, một chiến lược dữ liệu hiệu quả cần thúc đẩy sự phát triển của hạ tầng kỹ thuật số phục vụ cho việc xử lý và lưu trữ dữ liệu. Điều này bao gồm việc đầu tư vào các công nghệ tiên tiến như các trung tâm dữ liệu, các nền tảng đám mây, và các hệ thống phần mềm hỗ trợ việc phân tích, quản lý và bảo mật dữ liệu. Sự phát triển này không chỉ giúp nâng cao khả năng xử lý dữ liệu mà còn tạo ra cơ sở vững chắc cho việc tối ưu hóa việc sử dụng dữ liệu trong quản lý nhà nước và phát triển kinh tế.



Việc chia sẻ, trao đổi và sử dụng dữ liệu giữa khu vực tư và công cần được đẩy mạnh - Ảnh: Tạp chí Tài chính

Thêm vào đó, chiến lược dữ liệu cần bao gồm các sáng kiến thúc đẩy ứng dụng các công nghệ mới như Big Data (Dữ liệu lớn), AI (Trí tuệ nhân tạo), và IoT (Internet vạn vật). Big Data có thể giúp khai thác khối lượng dữ liệu khổng lồ và đưa ra những phân tích sâu sắc, phục vụ cho công tác quản lý và ra quyết định của các cơ quan nhà nước. AI có thể được ứng dụng trong việc phân tích dữ liệu, dự đoán các xu hướng và tối ưu hóa các quy trình công việc, trong khi IoT giúp kết nối và thu thập dữ liệu từ các thiết bị, tạo ra cơ sở dữ liệu phong phú phục vụ cho việc giám sát, quản lý trong nhiều lĩnh vực như giao thông, y tế, và nông nghiệp.

Tóm lại, một chiến lược dữ liệu hiệu quả không chỉ đảm bảo an toàn, bảo mật, và minh bạch trong việc quản lý và sử dụng dữ liệu mà còn cần tích hợp các công nghệ mới để tối ưu hóa việc sử dụng dữ liệu trong các hoạt

động quản lý nhà nước và phát triển kinh tế. Điều này đòi hỏi sự phối hợp chặt chẽ giữa các cơ quan nhà nước, doanh nghiệp, và các tổ chức nghiên cứu khoa học để triển khai các giải pháp công nghệ tiên tiến và xây dựng hệ thống dữ liệu quốc gia hiện đại.

Bốn là, quy định về quản trị dữ liệu. Quản trị dữ liệu là một yếu tố quan trọng trong việc đảm bảo rằng dữ liệu được quản lý, tổ chức và sử dụng một cách có trách nhiệm, bảo mật và tuân thủ pháp luật. Quy trình quản trị dữ liệu phải được xây dựng trên một cơ cấu rõ ràng và chặt chẽ, không chỉ từ các cơ quan nhà nước mà còn bao gồm các doanh nghiệp và tổ chức tư nhân. Điều này giúp tạo ra một môi trường đồng bộ và hiệu quả trong việc xử lý, lưu trữ và chia sẻ dữ liệu, đồng thời bảo vệ quyền lợi của các cá nhân và tổ chức liên quan.



Quản trị dữ liệu là khâu cực kì quan trọng trong vận hành, khai thác Trung tâm dữ liệu quốc gia - Ảnh: Xboss ERP

Đầu tiên, một trong những yếu tố quan trọng nhất trong quản trị dữ liệu là phân quyền truy cập và bảo vệ dữ liệu. Quy định này yêu cầu phải có hệ thống phân quyền rõ ràng, đảm bảo rằng chỉ những cá nhân và tổ chức có thẩm quyền mới được phép truy cập vào dữ liệu nhạy cảm. Các biện pháp bảo vệ dữ liệu phải được thực hiện nghiêm ngặt để ngăn chặn các truy cập trái phép và đảm bảo tính bảo mật trong suốt quá trình thu thập, lưu trữ và truyền tải dữ liệu. Điều này bao gồm việc sử dụng các công nghệ mã hóa, xác thực đa yếu tố, và các phương pháp bảo mật hiện đại để bảo vệ dữ liệu khỏi các mối đe dọa từ tấn công mạng hoặc vi phạm an ninh.

Tiếp theo, một quy trình quản trị dữ liệu hiệu quả cần phải bao gồm đào tạo và nâng cao năng lực cho đội ngũ quản lý dữ liệu. Các tổ chức cần phải đảm bảo rằng nhân viên quản lý dữ liệu được đào tạo bài bản và có đủ kiến thức về các nguyên tắc, quy trình và quy định liên quan đến bảo vệ dữ liệu. Các khóa đào tạo này không chỉ bao gồm các kỹ năng kỹ thuật, mà còn phải trang bị cho đội ngũ quản lý dữ liệu những hiểu biết về các yêu cầu pháp lý và đạo đức trong việc xử lý dữ liệu. Đồng thời, tổ chức cần xây dựng các chính sách đào tạo thường xuyên để nâng cao năng lực của đội ngũ quản lý, giúp họ đáp ứng được yêu cầu ngày càng cao trong việc bảo mật và quản lý dữ liệu.

Cuối cùng, đảm bảo tính minh bạch trong các hoạt động xử lý dữ liệu là yếu tố không thể thiếu trong quy trình quản trị dữ liệu. Tính minh bạch không chỉ giúp xây dựng sự tin tưởng giữa các tổ chức và cá nhân mà còn tạo ra một môi trường pháp lý rõ ràng, nơi mà tất cả các bên liên quan đều hiểu rõ về cách thức thu thập, xử lý và sử dụng dữ liệu. Các tổ chức phải công khai các chính sách về quyền riêng tư, bảo mật và việc sử dụng dữ liệu của mình, đồng thời phải cung cấp cho người dân quyền truy cập vào thông

tin về dữ liệu mà họ cung cấp và các mục đích sử dụng dữ liệu đó. Ngoài ra, việc minh bạch còn giúp các cơ quan nhà nước dễ dàng giám sát và kiểm tra các hoạt động xử lý dữ liệu, từ đó đảm bảo rằng dữ liệu được xử lý đúng theo quy định của pháp luật và không xâm phạm quyền lợi của cá nhân.

Năm là, quy định về bảo vệ dữ liệu. Bảo vệ dữ liệu là một trong những yếu tố then chốt trong việc xây dựng và thực thi chính sách dữ liệu, nhằm bảo đảm rằng dữ liệu được xử lý và lưu trữ một cách an toàn, tránh bị xâm phạm hoặc lạm dụng. Quy định bảo vệ dữ liệu không chỉ bao gồm các biện pháp kỹ thuật mà còn đòi hỏi phải có các biện pháp tổ chức để quản lý và giám sát việc xử lý dữ liệu một cách hiệu quả. Điều này giúp bảo vệ dữ liệu khỏi các mối đe dọa từ hacker, các cuộc tấn công mạng, và các rủi ro tiềm ẩn khác mà dữ liệu có thể phải đối mặt trong môi trường số.

Một trong những yếu tố cơ bản trong chính sách bảo vệ dữ liệu là xác định rõ quyền và nghĩa vụ của tổ chức trong việc bảo vệ dữ liệu cá nhân. Các tổ chức, cơ quan, và doanh nghiệp có trách nhiệm đảm bảo rằng dữ liệu cá nhân của người dân được thu thập, lưu trữ và sử dụng đúng mục đích, với các biện pháp bảo mật thích hợp. Quy định này cần phải xác định các biện pháp bảo vệ dữ liệu từ khâu thu thập đến khâu tiêu hủy, bao gồm việc sử dụng các công nghệ bảo mật như mã hóa dữ liệu, xác thực mạnh mẽ, và kiểm soát quyền truy cập để hạn chế việc tiếp cận dữ liệu bởi các cá nhân hoặc tổ chức không có thẩm quyền.

Cùng với đó, các chính sách bảo vệ dữ liệu cần phải yêu cầu các tổ chức thực hiện đánh giá rủi ro định kỳ đối với hệ thống và cơ sở hạ tầng dữ liệu của mình. Việc đánh giá này giúp các tổ chức nhận diện và giảm thiểu các rủi ro tiềm ẩn có thể ảnh hưởng đến an toàn dữ liệu, từ các mối đe dọa như các cuộc tấn công mạng (ví dụ, tấn công DDoS, mã độc…), đến các yếu tố

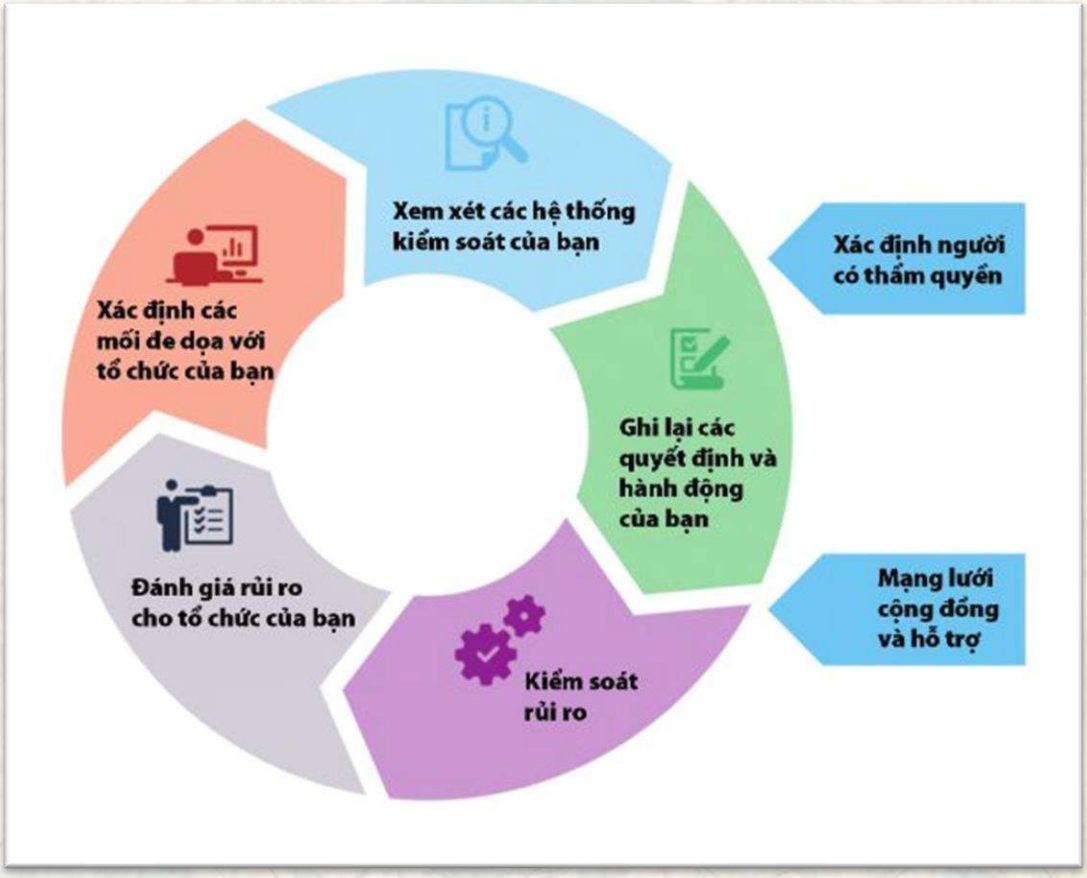
nội bộ như rủi ro từ việc lạm dụng quyền truy cập dữ liệu hoặc sai sót trong quy trình xử lý dữ liệu. Các đánh giá này cần được thực hiện định kỳ và cập nhật thường xuyên để đảm bảo rằng các biện pháp bảo vệ luôn phù hợp với các mối đe dọa mới và có hiệu quả trong việc ngăn ngừa các rủi ro.

Bên cạnh các biện pháp bảo mật truyền thống, các chính sách bảo vệ dữ liệu cần chú trọng đặc biệt đến bảo vệ dữ liệu trong các hệ thống đám mây và các ứng dụng trực tuyến. Các hệ thống đám mây hiện nay ngày càng được sử dụng rộng rãi, nhưng cũng tiềm ẩn nhiều rủi ro bảo mật do việc lưu trữ và xử lý dữ liệu không còn nằm trong khuôn khổ kiểm soát trực tiếp của tổ chức. Do đó, các biện pháp bảo vệ dữ liệu trong môi trường đám mây cần bao gồm việc lựa chọn các nhà cung cấp dịch vụ đám mây đáng tin cậy, đảm bảo rằng họ tuân thủ các tiêu chuẩn bảo mật quốc tế, như các tiêu chuẩn ISO 27001 về quản lý bảo mật thông tin. Thêm vào đó, các ứng dụng trực tuyến cũng cần phải được xây dựng với các biện pháp bảo mật mạnh mẽ, bao gồm mã hóa dữ liệu trong quá trình truyền tải, bảo vệ thông tin đăng nhập bằng xác thực hai yếu tố (2FA), và thiết lập các cơ chế kiểm soát truy cập rõ ràng.

Ngoài các biện pháp kỹ thuật, các tổ chức cũng cần có các quy trình tổ chức và chính sách nội bộ nhằm giám sát và đảm bảo rằng các biện pháp bảo vệ dữ liệu luôn được thực hiện nghiêm ngặt và có hiệu quả. Điều này bao gồm việc huấn luyện nhân viên về các quy định bảo vệ dữ liệu và các phương thức bảo mật cơ bản, đồng thời xây dựng một kế hoạch ứng phó với sự cố bảo mật dữ liệu để nhanh chóng xử lý các sự kiện rủi ro như rò rỉ hoặc mất mát dữ liệu.

Sáu là, quy định về xác định và quản lý rủi ro phát sinh trong xử lý dữ liệu. Quy định về xác định và quản lý rủi ro phát sinh trong xử lý dữ liệu là

một phần quan trọng trong việc bảo vệ thông tin và đảm bảo tính an toàn, bảo mật của dữ liệu. Các tổ chức cần xây dựng các cơ chế rõ ràng và hiệu quả để xác định và đánh giá các rủi ro liên quan đến việc xử lý dữ liệu, đặc biệt là những rủi ro về bảo mật và quyền riêng tư. Việc này không chỉ giúp các tổ chức phát hiện và ngăn chặn các mối đe dọa tiềm ẩn, mà còn tạo ra một hệ thống bảo vệ dữ liệu mạnh mẽ, đảm bảo rằng dữ liệu của cá nhân và tổ chức luôn được bảo mật và không bị xâm phạm.



Quản trị rủi ro quy mô doanh nghiệp - Ảnh: Học viện Agile

Đầu tiên, xác định và đánh giá rủi ro là bước quan trọng trong quy trình quản lý dữ liệu. Các tổ chức phải thực hiện các bài kiểm tra bảo mật định kỳ để đánh giá mức độ bảo vệ của hệ thống trước các cuộc tấn công và sự cố có thể xảy ra. Các kiểm tra này cần tập trung vào việc phát hiện các lỗ hổng bảo mật trong phần mềm, hệ thống mạng và các công cụ xử lý dữ liệu đang được

sử dụng. Bên cạnh đó, các tổ chức cũng cần tiến hành các bài kiểm tra thâm nhập (penetration testing) để mô phỏng các cuộc tấn công thực tế và đánh giá khả năng của hệ thống trong việc ngăn chặn các cuộc xâm nhập này.

Bên cạnh việc kiểm tra bảo mật, quy trình giám sát và báo cáo sự cố bảo mật cũng cần được xây dựng để theo dõi và phát hiện các sự cố liên quan đến dữ liệu. Các tổ chức cần có hệ thống giám sát liên tục để phát hiện sớm các hoạt động bất thường hoặc các dấu hiệu của cuộc tấn công mạng, chẳng hạn như xâm nhập trái phép vào hệ thống, sự thay đổi không hợp lý trong dữ liệu hoặc truy cập bất hợp pháp vào thông tin cá nhân. Các quy trình này cần đảm bảo rằng mọi sự cố được ghi nhận, xử lý kịp thời và báo cáo đúng hạn theo yêu cầu của pháp luật hoặc các quy định liên quan. Việc có hệ thống báo cáo sự cố rõ ràng giúp các tổ chức không chỉ đối phó nhanh chóng với các sự kiện bảo mật mà còn hỗ trợ việc cải thiện các biện pháp bảo mật trong tương lai.

Một phần không thể thiếu trong quy trình quản lý rủi ro dữ liệu là đào tạo về an toàn dữ liệu cho nhân viên. Các tổ chức cần tổ chức các chương trình đào tạo định kỳ để nâng cao nhận thức và kỹ năng bảo mật cho đội ngũ nhân viên. Đào tạo này không chỉ bao gồm các kỹ thuật bảo mật cơ bản mà còn cần trang bị cho nhân viên các kiến thức về quyền riêng tư, các quy định bảo vệ dữ liệu và những biện pháp cần thiết để phòng ngừa, phát hiện và ứng phó với các sự cố bảo mật. Việc đào tạo nhân viên giúp giảm thiểu các rủi ro phát sinh từ các sai sót của con người, là yếu tố quan trọng trong việc bảo vệ dữ liệu khỏi các mối đe dọa.

Ngoài ra, phương án đối phó với các sự cố về dữ liệu cũng phải được xây dựng và thử nghiệm thường xuyên. Các tổ chức cần có các kế hoạch ứng phó sự cố rõ ràng, bao gồm các bước cụ thể để xử lý khi có sự cố xảy ra, từ việc phát hiện và cô lập sự cố cho đến việc phục hồi dữ liệu và thông báo cho các

bên liên quan. Các kế hoạch này cần được thử nghiệm định kỳ để đảm bảo tính hiệu quả trong trường hợp khẩn cấp và đảm bảo rằng tổ chức có thể nhanh chóng khôi phục lại hệ thống và dữ liệu sau khi sự cố được giải quyết.

Bảy là, quy định về hợp tác quốc tế về dữ liệu. Hợp tác quốc tế về dữ liệu đóng vai trò quan trọng trong việc phát triển chính sách dữ liệu quốc gia, giúp Việt Nam hội nhập và tận dụng các cơ hội trong kỷ nguyên số. Trong bối cảnh toàn cầu hóa và sự phát triển mạnh mẽ của công nghệ, việc trao đổi và chia sẻ dữ liệu giữa các quốc gia là một yếu tố không thể thiếu trong việc thúc đẩy các lĩnh vực kinh tế, khoa học, và công nghệ. Để phát huy tiềm năng này, Việt Nam cần thiết lập và tham gia vào các thỏa thuận quốc tế về dữ liệu, qua đó đảm bảo quyền lợi và bảo vệ an ninh quốc gia trong việc xử lý và chia sẻ dữ liệu xuyên biên giới.

Các thỏa thuận quốc tế về dữ liệu cần bao gồm các nguyên tắc và điều kiện rõ ràng để đảm bảo rằng việc chia sẻ dữ liệu giữa các quốc gia không chỉ phục vụ cho các mục đích hợp tác, mà còn tuân thủ các tiêu chuẩn bảo mật và quyền riêng tư. Trong các lĩnh vực như thương mại điện tử, nghiên cứu, y tế và giáo dục, việc chia sẻ và trao đổi dữ liệu có thể mang lại lợi ích lớn, từ việc thúc đẩy sự phát triển của các doanh nghiệp, tăng cường khả năng nghiên cứu và phát triển, cho đến việc cải thiện chất lượng dịch vụ y tế và giáo dục. Tuy nhiên, việc này cũng cần được thực hiện dưới sự giám sát chặt chẽ và theo các quy định pháp lý quốc tế nhằm đảm bảo rằng dữ liệu không bị lợi dụng hoặc xâm phạm quyền lợi của người dân.

Một trong những cơ chế hợp tác quốc tế quan trọng mà Việt Nam có thể tham gia là các hiệp định quốc tế về dữ liệu, như Hiệp định Đối tác Thương mại và Kinh tế xuyên Thái Bình Dương (CPTPP). Hiệp định này không chỉ tạo cơ hội cho việc thúc đẩy thương mại và đầu tư, mà còn mở ra cơ hội cho

việc chia sẻ dữ liệu trong các lĩnh vực kinh tế và công nghệ, giúp các doanh nghiệp và tổ chức Việt Nam tiếp cận với thị trường quốc tế và ứng dụng các công nghệ mới. Việc gia nhập các hiệp định này sẽ giúp Việt Nam nâng cao năng lực xử lý và quản lý dữ liệu, đồng thời giúp các tổ chức và cá nhân trong nước tuân thủ các tiêu chuẩn quốc tế về bảo mật và quyền riêng tư.



Ngày 05/11/2021, Thủ tướng Chính phủ Phạm Minh Chính và ông Mathias Cormann, Tổng thư ký Tổ chức Hợp tác và phát triển kinh tế (OECD) chứng kiến lễ ký kết Biên bản ghi nhớ hợp tác (MOU) Việt Nam - OECD giai đoạn 2022-2026 - Ảnh: TTXVN

Bên cạnh đó, việc tham gia vào các tổ chức quốc tế như Tổ chức Hợp tác và Phát triển Kinh tế (OECD) cũng sẽ mang lại những lợi ích thiết thực cho Việt Nam trong việc xây dựng và triển khai các chính sách dữ liệu. OECD không chỉ là một diễn đàn quan trọng để trao đổi kinh nghiệm và chia sẻ các sáng kiến chính sách, mà còn là nơi để các quốc gia cùng nhau phát triển các khung pháp lý và tiêu chuẩn quốc tế về quản lý và bảo vệ dữ liệu. Tham gia các tổ chức này sẽ giúp Việt Nam học hỏi từ các quốc gia tiên tiến

trong việc xây dựng các chiến lược dữ liệu quốc gia, đồng thời hỗ trợ việc hội nhập quốc tế của Việt Nam trong các lĩnh vực công nghệ và kinh tế số.

Ngoài ra, hợp tác quốc tế còn mở ra cơ hội cho việc xây dựng các mạng lưới chia sẻ dữ liệu quốc tế trong các lĩnh vực như y tế, khoa học và giáo dục, giúp các quốc gia cùng nhau đối phó với các thách thức toàn cầu như dịch bệnh, biến đổi khí hậu, và phát triển bền vững. Việc tham gia vào các dự án nghiên cứu quốc tế cũng sẽ giúp Việt Nam nâng cao năng lực nghiên cứu và phát triển, cũng như tiếp cận với các nguồn dữ liệu quan trọng để giải quyết các vấn đề cấp bách trong nước.

Tám là, quy định về Quỹ phát triển dữ liệu quốc gia. Quỹ Phát triển Dữ liệu Quốc gia là một công cụ tài chính quan trọng, đóng vai trò then chốt trong việc thúc đẩy sự phát triển và nâng cao chất lượng hệ thống dữ liệu quốc gia. Quỹ này không chỉ hỗ trợ các dự án nghiên cứu và phát triển dữ liệu mà còn cung cấp nguồn lực tài chính để xây dựng và hoàn thiện các cơ sở hạ tầng dữ liệu quốc gia, đảm bảo sự phát triển bền vững của hệ thống quản lý và bảo vệ dữ liệu trong các lĩnh vực quan trọng như y tế, giáo dục, và thương mại điện tử.

Để đảm bảo hiệu quả trong việc sử dụng quỹ, quy định về Quỹ Phát triển Dữ liệu Quốc gia cần phải xác định rõ các nguồn tài chính đóng góp vào quỹ này, bao gồm các khoản đóng góp tự nguyện từ các tổ chức, doanh nghiệp, cá nhân trong và ngoài nước. Các đóng góp này có thể đến từ các doanh nghiệp công nghệ, tổ chức nghiên cứu, và các cá nhân quan tâm đến sự phát triển của hệ thống dữ liệu quốc gia. Một phần của quỹ có thể được huy động từ doanh thu của các đơn vị sự nghiệp công lập liên quan đến việc quản lý và cung cấp dịch vụ dữ liệu, như các trung tâm dữ liệu quốc gia. Điều này không chỉ giúp quỹ có nguồn tài chính ổn định mà còn đảm bảo

rằng các tổ chức và cá nhân có thể tham gia tích cực vào quá trình phát triển và bảo vệ dữ liệu quốc gia.



Quỹ Phát triển dữ liệu quốc gia là quỹ tài chính nhà nước ngoài ngân sách, hoạt động không vì mục đích lợi nhuận và giao Bộ Công an quản lý - Ảnh: Cổng thông tin điện tử Công an Thành phố Hồ Chí Minh

Mục đích sử dụng nguồn quỹ cần được quy định rõ ràng để đảm bảo tính minh bạch và hiệu quả trong việc chi tiêu. Quỹ này sẽ được phân bổ cho các dự án nghiên cứu và phát triển dữ liệu, bao gồm việc triển khai các sáng kiến nghiên cứu về công nghệ dữ liệu mới, như Big Data, Trí tuệ nhân tạo (AI), và Internet vạn vật (IoT), nhằm cải thiện khả năng phân tích và xử lý dữ liệu trong các cơ quan nhà nước và doanh nghiệp. Bên cạnh đó, một phần nguồn quỹ cũng cần được dành cho xây dựng và nâng cấp hạ tầng dữ liệu quốc gia, bao gồm các trung tâm dữ liệu, hệ thống lưu trữ và xử lý dữ liệu hiện đại, đáp ứng yêu cầu ngày càng cao về bảo mật, tốc độ xử lý và khả năng lưu trữ dữ liệu khối lượng lớn.

Ngoài các dự án nghiên cứu và hạ tầng, quỹ này cũng có thể được sử dụng để phát triển ứng dụng công nghệ mới phục vụ cho việc quản lý dữ liệu

trong các lĩnh vực công, như quản lý thông tin công dân, giám sát môi trường, và phân tích dữ liệu lớn trong các ngành kinh tế trọng điểm. Các sáng kiến này không chỉ thúc đẩy sự đổi mới trong việc sử dụng dữ liệu mà còn giúp tối ưu hóa việc ra quyết định trong quản lý nhà nước và các doanh nghiệp, đồng thời tạo ra các cơ hội mới trong nền kinh tế số.

Để đảm bảo tính minh bạch và hiệu quả trong việc sử dụng nguồn tài chính từ Quỹ Phát triển Dữ liệu Quốc gia, các cơ quan nhà nước cần thiết lập cơ chế giám sát chặt chẽ việc chi tiêu quỹ, bao gồm các báo cáo tài chính định kỳ và kiểm toán độc lập. Điều này giúp tránh tình trạng lãng phí hoặc sử dụng không đúng mục đích các nguồn lực, đồng thời đảm bảo rằng quỹ được sử dụng đúng mục tiêu, giúp xây dựng nền tảng hạ tầng dữ liệu quốc gia vững chắc và phát triển bền vững.

Tóm lại, Quỹ Phát triển Dữ liệu Quốc gia là một yếu tố quan trọng trong việc xây dựng và phát triển hệ thống dữ liệu quốc gia. Việc quy định rõ ràng về các nguồn tài chính và mục đích sử dụng quỹ sẽ giúp đảm bảo rằng quỹ này không chỉ phục vụ cho các dự án nghiên cứu và phát triển công nghệ mới mà còn giúp xây dựng cơ sở hạ tầng dữ liệu hiện đại, phục vụ tốt cho nhu cầu quản lý và sử dụng dữ liệu trong các lĩnh vực công và tư.

Chín là, quy định về ứng dụng khoa học - công nghệ trong xử lý dữ liệu, bao gồm các nội dung về: ***(1)*** Nhà nước ưu tiên việc xử lý, quản trị dữ liệu thông qua ứng dụng khoa học công nghệ hiện đại để phục vụ công tác quản lý nhà nước, phát triển kinh tế, xã hội; đáp ứng yêu cầu trong chuyển đổi số, phát triển kinh tế số, xã hội số; ***(2)*** Nguyên tắc phát triển công nghệ trong xử lý dữ liệu; ***(3)*** Nguyên tắc trong ứng dụng công nghệ vào công tác quản lý nhà nước, phát triển kinh tế - xã hội và phục vụ hoạt động khác của xã hội; ***(4)*** Định hướng phát triển, sử dụng các công nghệ tại nước ta.

1.4.3.2. Quy định về Cơ sở dữ liệu tổng hợp quốc gia

- Xác định vấn đề bất cập

Qua triển khai thực hiện việc xây dựng, tạo lập, kết nối, chia sẻ dữ liệu đến nay, bước đầu khởi tạo và hình thành được ***07*** Cơ sở dữ liệu quốc gia; một số Cơ sở dữ liệu quốc gia đã có sự kết nối liên thông, chia sẻ dữ liệu góp phần cải cách, đơn giản hóa thủ tục hành chính cho người dân… Tuy nhiên, hạ tầng dữ liệu quốc gia còn rời rạc, chất lượng không đồng đều và chưa cao; nhiều cơ sở dữ liệu được thu thập, lưu trữ trùng lặp, chồng chéo, chưa được chuẩn hóa, thống nhất về tiêu chuẩn, danh mục nên không có khả năng kế thừa, khó khăn khi kết nối, chia sẻ, khai thác dùng chung, người dân vẫn phải khai báo thông tin nhiều lần; đồng thời, sự kết nối liên thông, chia sẻ dữ liệu để tạo lập nguồn tài nguyên dữ liệu quốc gia quan trọng còn yếu và thiếu đồng bộ, chưa đáp ứng được tốt việc đẩy mạnh ứng dụng các thành tựu của cuộc cách mạng công nghiệp lần thứ Tư; tốc độ phát triển tài nguyên số, đặc biệt là tài nguyên dữ liệu phục vụ cho phát triển kinh tế dữ liệu chưa theo kịp tốc độ phát triển kinh tế - xã hội.

Qua rà soát của Bộ Công an thì đối với 80 thủ tục hành chính triển khai trên Công dịch vụ công quốc gia (68 thủ tục hành chính ưu tiên theo Đề án 06 và 12 thủ tục hành chính có lượng yêu cầu lớn nhất) cần phải truy cập, khai thác, sử dụng thông tin ở rất nhiều cơ sở dữ liệu khác nhau; trong đó, có nhiều thông tin cơ bản về công dân như họ tên, ngày tháng năm sinh, giới tính, dân tộc… thì đều được lưu trữ, truy xuất từ nhiều nguồn cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành khác nhau chưa có sự chuẩn hóa, khó bảo đảm tính thống nhất, chính xác (không kiểm tra, xác minh với dữ liệu gốc hoặc thực hiện truy xuất tới cơ sở dữ liệu chứa dữ liệu gốc), như thông tin về địa chỉ hiện tại của công dân (thu thập, lưu trữ tại 26 cơ sở dữ liệu),

thông tin về dân tộc (thu thập, lưu trữ tại 20 cơ sở dữ liệu), thông tin về giới tính (thu thập, lưu trữ tại 29 cơ sở dữ liệu)…

Từ đó, đặt ra yêu cầu phải có quy định về Cơ sở dữ liệu tổng hợp quốc gia, để tập hợp, tích hợp, đồng bộ, lưu trữ, chia sẻ, phân tích, khai thác dữ liệu của các cơ quan nhà nước và dữ liệu của doanh nghiệp, tổ chức, cá nhân theo quy định của pháp luật nhằm hình thành kho dữ liệu về con người và kho dữ liệu tổng hợp từ các cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành, cơ sở dữ liệu của doanh nghiệp, tổ chức, cá nhân; dữ liệu tại cớ ở dữ liệu tổng hợp quốc gia là nền tảng cốt lõi cung cấp các dịch vụ liên quan đến dữ liệu, hỗ trợ hoạch định chính sách, kiến tạo phát triển, xây dựng Chính phủ số, xã hội số và kinh tế số, bảo đảm quốc phòng - an ninh.

- Mục tiêu giải quyết vấn đề

Quy định Cơ sở dữ liệu tổng hợp quốc gia là nơi tích hợp, đồng bộ, lưu trữ, khai thác, chia sẻ và chia sẻ dữ liệu tổng hợp từ các cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành, cơ sở dữ liệu của doanh nghiệp, tổ chức, cá nhân nhằm đẩy mạnh ứng dụng các thành tựu của cuộc cách mạng công nghiệp 4.0 trong phát triển, khai thác dữ liệu lớn. Ứng dụng phân tích chuyên sâu dữ liệu để hỗ trợ tốt hơn cho công tác xây dựng các cơ chế, chính sách, quy hoạch, chiến lược phát triển quốc gia. Từ đó, tạo điều kiện phát triển nhiều sản phẩm dịch vụ mới trên nền các dữ liệu số được khai thác góp phần thúc đẩy phát triển kinh tế - xã hội.

- Giải pháp

Quy định về Cơ sở dữ liệu quốc gia (trên cơ sở đồng bộ toàn bộ dữ liệu mở, dữ liệu dùng chung từ các cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành về Cơ sở dữ liệu tổng hợp quốc gia), cụ thể:

(1) Đồng bộ toàn bộ các thông tin, dữ liệu từ các cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành về cơ sở dữ liệu tổng hợp quốc gia, cơ sở dữ liệu chuyên ngành về Cơ sở dữ liệu tổng hợp quốc gia, tạo lập kho dữ liệu mở, kho dữ liệu dùng chung để thống kê, phân tích, tổng hợp phục vụ công tác quản lý nhà nước, các dịch vụ công của Chính phủ và phát triển kinh tế - xã hội;

(2) Hoạt động xử lý, quản trị, chia sẻ dữ liệu liên quan đến Cơ sở dữ liệu tổng hợp quốc gia;

(3) Trách nhiệm cung cấp thông tin, dữ liệu của cơ quan nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội, cá nhân, tổ chức khác;

(4) Mối quan hệ giữa Cơ sở dữ liệu tổng hợp quốc gia với cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành, cổng dịch vụ công quốc gia và cơ sở dữ liệu, hệ thống thông tin khác;

(5) Phí, giá khai thác, sử dụng công nghệ thông tin trong Cơ sở dữ liệu tổng hợp quốc gia;

Quy định đồng bộ dữ liệu của doanh nghiệp, tổ chức, cá nhân tự nguyện cung cấp hoặc bắt buộc cung cấp về Cơ sở dữ liệu tổng hợp quốc gia trong trường hợp ứng phó với tình trạng khẩn cấp (như trường hợp khẩn cấp về quốc phòng - an ninh, sức khỏe cộng đồng hoặc các thảm họa lớn do thiên nhiên hoặc do con người gây ra).

1.4.3.3. Quy định về Trung tâm dữ liệu quốc gia

- Xác định vấn đề bất cập

Ở nước ta, qua triển khai xây dựng Chính phủ điện tử, Chính phủ số, đặc biệt qua thực hiện Quyết định số 06/QĐ-TTg ngày 06/01/2021 của Thủ tướng Chính phủ về phê duyệt Đề án phát triển ứng dụng dữ liệu về dân cư, định danh và xác thực điện tử phục vụ chuyển đổi số quốc gia giai đoạn 2022

- 2025, tầm nhìn đến năm 2030 (Đề án 06) cho thấy bức tranh về hạ tầng, công nghệ, dữ liệu của nước ta còn nhiều hạn chế, như: ***(1)*** Một số bộ, ngành không có hoặc có nhưng chưa đầy đủ hạ tầng để triển khai các hệ thống công nghệ thông tin cốt lõi phục vụ cho các công tác nghiệp vụ; ***(2)*** Nhiều cơ sở dữ liệu được thu thập, lưu trữ trùng lặp, chồng chéo, chưa thống nhất về danh mục dữ liệu dùng chung gây khó khăn khi kết nối, chia sẻ, khai thác dữ liệu; ***(3)*** Các Trung tâm dữ liệu đầu tư thiếu đồng bộ, không đồng nhất về tiêu chuẩn, quy chuẩn kĩ thuật, không thường xuyên được kiểm tra, bảo trì, nâng cấp dẫn đến nguy cơ không đảm bảo an ninh an toàn hệ thống; ***(4)*** Một số bộ, ngành, địa phương thuê dịch vụ hạ tầng công nghệ thông tin tiềm ẩn nhiều rủi ro về an ninh, an toàn thông tin do chưa thực sự quản lý, kiểm soát được dữ liệu nhà nước trên hạ tầng của doanh nghiệp; ***(5)*** Nhân lực vận hành, quản trị các hệ thống thông tin vừa thiếu, vừa yếu; ***(6)*** Các cơ sở dữ liệu quốc gia theo Quyết định số 714/QĐ-TTg ngày 22/5/2015 của Thủ tướng Chính phủ chưa được xây dựng đầy đủ; ***(7)*** Nhiều hệ thống thông tin còn lỗ hổng bảo mật, không đủ điều kiện kết nối với Cơ sở dữ liệu quốc gia về dân cư…

- Mục tiêu giải quyết vấn đề

Giúp Chính phủ và các bộ, ngành, địa phương: ***(1)*** Tập trung nguồn lực, hạ tầng công nghệ; ***(2)*** Giải quyết các vấn đề hạn chế của các hệ thống thông tin, của việc tích hợp, chia sẻ dữ liệu giữa các cơ quan; ***(3)*** Tăng cường hiệu quả, tính minh bạch trong quản lý nhà nước, hiện đại hóa quy trình quản trị quốc gia; ***(4)*** Tiết kiệm nguồn lực đầu tư của nhà nước và xã hội, tạo nguồn thu cho ngân sách Nhà nước.

+ Xây dựng, vận hành Trung tâm dữ liệu quốc gia là nơi lưu trữ dữ liệu, hệ thống của các cơ sở dữ liệu quốc gia kết nối liên thông dữ liệu với các cơ

sở dữ liệu chuyên ngành, các hệ thống thông tin trong nước và tổ chức, Chính phủ các nước để phục vụ các hoạt động trên môi trường số.

+ Quy hoạch lưu trữ và thiết lập các chính sách an ninh, an toàn thông tin phù hợp với đối tượng, phương thức truy cập, quyền khai thác đối với từng loại dữ liệu.

+ Triển khai các công nghệ, giải pháp hiện đại và đào tạo được chuyên gia khoa học dữ liệu, đặc biệt là chuyên gia phân tích dữ liệu để thực hiện công tác phát triển, tổng hợp và khai thác, phân tích dữ liệu tổng thể, đa chiều, khách quan… Bảo đảm trên 90% các hoạt động hành chính, trao đổi, cung cấp thông tin giữa các cơ quan nhà nước được thay thế bằng chia sẻ dữ liệu số của Trung tâm dữ liệu quốc gia.

+ Cơ bản các hệ thống của bộ, ngành (các địa phương có nhu cầu) được quản lý, lưu trữ ở Trung tâm dữ liệu quốc gia (trừ các hệ thống phục vụ quốc phòng, an ninh, các hệ thống đặc thù do Chính phủ quyết định).



Công nghệ là huyết mạch của công cuộc chuyển đổi số quốc gia - Ảnh: Trang thông tin chuyển đổi số Bộ Tư Pháp

- Giải pháp

Thứ nhất, quy định về việc xây dựng, phát triển, sử dụng chung hệ tầng Trung tâm dữ liệu quốc gia phục vụ hoạt động quản trị cơ sở dữ liệu của các cơ quan nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội (trừ hệ thống phục vụ quốc phòng, an ninh, các hệ thống chuyên ngành đặc thù khác do Thủ tướng Chính phủ quyết định). Theo quy định, các cơ quan này sẽ phải kết nối và lưu trữ các cơ sở dữ liệu quốc gia tại Trung tâm dữ liệu quốc gia, nhằm đảm bảo sự đồng bộ và kết nối chặt chẽ trong việc quản lý, chia sẻ và xử lý dữ liệu. Tuy nhiên, các hệ thống phục vụ cho quốc phòng, an ninh và các hệ thống chuyên ngành đặc thù sẽ không thuộc phạm vi quản lý của Trung tâm dữ liệu quốc gia, mà sẽ được quản lý độc lập theo các quy định đặc thù đã được Thủ tướng Chính phủ phê duyệt.

Về mặt bảo mật và an ninh thông tin, Trung tâm dữ liệu quốc gia phải tuân thủ các tiêu chuẩn bảo mật quốc tế nghiêm ngặt, bao gồm mã hóa dữ liệu và xác thực người dùng bằng các phương thức bảo mật mạnh mẽ như xác thực đa yếu tố. Tất cả các dữ liệu lưu trữ tại Trung tâm sẽ phải được mã hóa ở tất cả các cấp, cả khi lưu trữ và khi truyền tải, nhằm đảm bảo an toàn tuyệt đối trước các mối đe dọa từ hacker và các cuộc tấn công mạng. Hệ thống bảo mật phải được giám sát liên tục, với cơ chế cảnh báo sớm để phát hiện và ngăn chặn các hành vi xâm nhập trái phép.

Một yêu cầu quan trọng khác là Trung tâm dữ liệu quốc gia phải có khả năng mở rộng và linh hoạt để đáp ứng nhu cầu tăng trưởng dữ liệu không ngừng của các cơ quan nhà nước và tổ chức chính trị - xã hội. Quy định này yêu cầu Trung tâm phải có khả năng mở rộng không giới hạn về dung lượng lưu trữ và năng lực xử lý. Hệ thống hạ tầng phải được xây dựng sao cho có thể dễ dàng nâng cấp khi cần thiết, mà không làm gián đoạn các hoạt động

quan trọng, giúp đảm bảo tính liên tục và ổn định trong việc quản lý và sử dụng dữ liệu.



Đại tướng Lương Tam Quang, Ủy viên Bộ Chính trị, Bộ trưởng Bộ Công an thông tin, đến năm 2030, Trung tâm dữ liệu quốc gia sẽ thu hút, đào tạo, tập huấn, bồi dưỡng đội ngũ nhân lực đáp ứng tiêu chuẩn quốc gia, quốc tế.

Ngoài ra, Trung tâm dữ liệu quốc gia phải đảm bảo cơ chế chia sẻ và quản lý dữ liệu hiệu quả, giúp các cơ quan và tổ chức dễ dàng truy cập và sử dụng dữ liệu một cách minh bạch và an toàn. Việc chia sẻ dữ liệu giữa các cơ quan sẽ phải tuân thủ các quyền truy cập rõ ràng, đảm bảo rằng chỉ những người có thẩm quyền mới có quyền truy cập vào dữ liệu nhạy cảm. Đồng thời, Trung tâm cũng cần có hệ thống kiểm tra và ghi lại lịch sử truy cập, giúp theo dõi và giám sát mọi hoạt động trên các hệ thống dữ liệu để bảo đảm tính minh bạch và tránh hành vi lạm dụng, xâm phạm quyền lợi của các cá nhân và tổ chức. Điều này không chỉ giúp bảo vệ dữ liệu mà còn nâng cao tính minh bạch trong việc sử dụng và chia sẻ dữ liệu giữa các cơ quan nhà nước.

Thứ hai, quy định về việc bảo đảm, cung cấp hạ tầng cho hoạt động quản trị hệ thống thông tin khác của các cơ quan nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội. Giải pháp này yêu cầu các cơ quan phải sử dụng các dịch vụ hạ tầng công nghệ thông tin đã được Chính phủ phê duyệt, nhằm đảm bảo tính đồng bộ và khả năng tương thích trong việc triển khai các hệ thống. Quy định này yêu cầu các cơ quan phải tuân thủ các tiêu chuẩn kỹ thuật khi triển khai hệ thống, bao gồm việc sử dụng máy chủ, phần mềm và các công cụ kết nối đồng bộ, giúp bảo đảm bảo mật và hiệu quả trong việc quản lý dữ liệu. Bên cạnh đó, các biện pháp dự phòng và khôi phục sau sự cố cũng được quy định rõ ràng, yêu cầu mỗi cơ quan phải xây dựng kế hoạch dự phòng định kỳ và kiểm tra hệ thống sao lưu, nhằm đảm bảo rằng dữ liệu không bị mất trong trường hợp xảy ra sự cố và có khả năng phục hồi nhanh chóng.

Ngoài ra, các cơ quan nhà nước và tổ chức chính trị - xã hội phải áp dụng các quy định bảo mật chặt chẽ, bao gồm việc triển khai các hệ thống giám sát và cảnh báo an ninh thông minh để phát hiện và ngăn chặn các cuộc tấn công mạng. Các biện pháp bảo mật như mã hóa, kiểm tra an ninh định kỳ, và đánh giá các lỗ hổng bảo mật phải được thực hiện thường xuyên để bảo vệ an toàn thông tin. Khi sử dụng các dịch vụ lưu trữ và xử lý dữ liệu trên đám mây, các cơ quan này cũng cần tuân thủ các quy định nghiêm ngặt về bảo mật và pháp lý, yêu cầu các dịch vụ đám mây phải đáp ứng tiêu chuẩn bảo mật quốc tế và có cam kết bảo vệ dữ liệu của khách hàng. Các hệ thống thông tin cần phải tuân thủ các yêu cầu bảo vệ dữ liệu cá nhân theo các quy định pháp lý quốc tế như GDPR (Quy định bảo vệ dữ liệu chung của Liên minh Châu Âu) hoặc các hiệp định thương mại quốc tế mà Việt Nam tham gia.

Để đảm bảo tính minh bạch và an toàn trong việc chia sẻ và quản lý dữ liệu, các quy định về quy trình cấp quyền truy cập yêu cầu rằng chỉ những

nhân viên, cán bộ có thẩm quyền và có nhu cầu công việc mới được phép truy cập vào hệ thống dữ liệu quốc gia. Mọi hành động truy cập và thay đổi dữ liệu trong Trung tâm dữ liệu quốc gia phải được ghi lại và giám sát chặt chẽ, với hệ thống báo cáo tự động để theo dõi các hoạt động truy cập và xử lý dữ liệu, giúp phát hiện các dấu hiệu bất thường và đảm bảo tính minh bạch trong quá trình chia sẻ thông tin.



8 nguyên tắc bảo vệ dữ liệu cá nhân - Ảnh: Dự thảo Nghị định Quy định về bảo vệ dữ liệu cá nhân của Bộ Công an

Không chỉ vậy, việc đào tạo và phát triển nhân lực cũng là một yếu tố quan trọng để đảm bảo các cơ quan nhà nước và tổ chức chính trị có đủ năng lực quản lý và xử lý dữ liệu an toàn. Các chương trình đào tạo chuyên gia khoa học dữ liệu cần được triển khai để cung cấp kiến thức về bảo mật dữ liệu, phân tích dữ liệu lớn và sử dụng các công nghệ hiện đại như AI và Big

Data. Đồng thời, các khóa đào tạo về bảo mật thông tin phải được tổ chức định kỳ để giúp nhân viên hiểu rõ về các quy định bảo mật và các mối đe dọa tiềm ẩn từ các cuộc tấn công mạng, đảm bảo mọi người tham gia vào quản lý và xử lý dữ liệu đều có kiến thức đầy đủ về các vấn đề bảo mật.

1.4.3.4. Quy định về các sản phẩm, dịch vụ liên quan đến dữ liệu

- Xác định vấn đề bất cập

Dữ liệu là nguồn tài nguyên mới, là huyết mạch của các cơ quan, tổ chức hiện nay, nó được tạo lập từ nhiều nguồn khác nhau để mở ra không gian hoạt động và phát triển kinh tế - xã hội cho các quốc gia. Ở nước ta những năm qua, Đảng, Nhà nước đã có nhiều chủ trương, giải pháp đẩy mạnh ứng dụng khoa học, công nghệ phục vụ công cuộc chuyển đổi số quốc gia, xây dựng Chính phủ điện tử, Chính phủ số, kinh tế số, xã hội số. Theo đó, bước đầu khởi tạo và hình thành được ***07 cơ sở dữ liệu quốc gia***, một số cơ sở dữ liệu quốc gia đã có sự kết nối liên thông, chia sẻ dữ liệu góp phần cải cách, đơn giản hóa thủ tục hành chính cho người dân; các trung tâm dữ liệu bước đầu được quan tâm, đầu tư xây dựng hạ tầng công nghệ. Tuy nhiên, một số dịch vụ dữ liệu đang phát triển và là xu hướng trên thế giới thì chưa được quy định trong các luật, như: Sàn giao dịch dữ liệu, dịch vụ trung gian dữ liệu, dịch vụ phân tích - tổng hợp dữ liệu… Trong khi đó, việc thiết lập thị trường dữ liệu, xây dựng và phát triển các sản phẩm, dịch vụ liên quan đến dữ liệu hiện nay lại có vai trò rất quan trọng, đó được xem là yếu tố đột phá để từng bước tạo lập và thúc đẩy mở thị trường dữ liệu, lấy thị trường dữ liệu làm động lực phát triển dữ liệu và kích thích thúc đẩy chuyển đổi số các ngành, các lĩnh vực, tăng năng lực cạnh tranh, bảo đảm cho tiến trình chuyển đổi số ở nước ta. Do vậy, để tạo cơ sở pháp lý thúc đẩy hoạt động phát triển sản phẩm dịch, dịch vụ về dữ liệu đáp ứng yêu cầu phát triển kinh

tế - xã hội, cần thiết phải quy định hoàn thiện các sản phẩm, dịch vụ liên quan đến dữ liệu.

Theo Chiến lược dữ liệu quốc gia quy định tại Quyết định số 142/QĐ-TTg ngày 02/02/2024 của Thủ tướng Chính phủ thì sẽ giao Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) chủ trì việc xây dựng các sàn giao dịch dữ liệu. Tuy nhiên, hoạt động giao dịch dữ liệu tiềm ẩn nhiều nguy cơ tác động lớn đến lớn lên an ninh quốc gia, trật tự, an toàn xã hội. Vì vậy. cần thiết phải quy phạm hóa việc xây dựng, quản lý sàn giao dịch dữ liệu và quy định tại Luật Dữ liệu để thực hiện quản lý, bảo đảm chặt chẽ, thống nhất. Đồng thời, Bộ Công an sẽ là cơ quan thực hiện cấp phép và quản lý đối với các sàn dữ liệu. Việc triển khai sàn giao dịch dữ liệu được thực hiện bởi các doanh nghiệp nhà nước và các đơn vị sự nghiệp công lập thuộc cơ quan quản lý nhà nước.

Qua rà soát, Bộ Công an thấy rằng hiện nay một số luật quy định liên quan đến dịch vụ dữ liệu như: Luật Giao dịch điện tử, Luật An ninh mạng, Luật An toàn thông tin mạng, Luật Viễn thông. Tuy nhiên, để quản lý nhà nước đối với các dịch vụ dữ liệu được thống nhất, bảo đảm an ninh, an toàn thì việc bổ sung quy định về các sản phẩm, dịch vụ liên quan đến dữ liệu tại Luật Dữ liệu là cần thiết để phù hợp với thực tiễn và không xung đột với các văn bản quy phạm pháp luật hiện hành.

- Mục tiêu giải quyết vấn đề

Quy định về sản phẩm, dịch vụ liên quan đến dữ liệu tạo cơ sở pháp lý để triển khai thực hiện đồng bộ, thống nhất, từ đó thể hiện vai trò của Nhà nước trong việc phát huy vai trò của cả hệ thống chính trị, xã hội tham gia thu thập, xây dựng, phát triển, khai thác, sử dụng, làm giàu dữ liệu và dẫn dắt, định hướng phát triển, quản lý các sản phẩm, dịch vụ liên quan đến dữ

liệu, đồng thời tạo cơ hội cho tổ chức, doanh nghiệp được tiếp cận các hỗ trợ của Nhà nước và người dân có nhiều cơ hội tiếp cận, lựa chọn, sử dụng các sản phẩm, dịch vụ liên quan đến dữ liệu.

- Giải pháp

Quy định về các sản phẩm, dịch vụ liên quan đến dữ liệu (dựa trên dữ liệu do cơ quan nhà nước tạo lập và dữ liệu do cá nhân, tổ chức khác tạo lập) và quản lý đối với tổ chức cung cấp sản phẩm, dịch vụ liên quan đến dữ liệu. Để thực hiện giải pháp này, Nhà nước cần thiết lập các quy định rõ ràng về việc cung cấp sản phẩm, dịch vụ từ dữ liệu công và dữ liệu tư. Các cơ quan nhà nước phải đảm bảo kết nối và lưu trữ dữ liệu quốc gia tại Trung tâm dữ liệu quốc gia, đồng thời cung cấp các sản phẩm, dịch vụ công cộng từ dữ liệu của Nhà nước như dịch vụ hành chính công trực tuyến, các báo cáo thống kê, dữ liệu nghiên cứu khoa học.



Thủ tướng Phạm Minh Chính: Chuyển đổi số là công cụ quan trọng để hỗ trợ thực thi công lý - Ảnh: VGP/Nhật Bắc

Đối với dữ liệu từ cá nhân và tổ chức ngoài Nhà nước, các quy định cần bảo vệ quyền lợi của các chủ thể dữ liệu, đảm bảo rằng dữ liệu cá nhân được sử dụng đúng mục đích và tuân thủ các tiêu chuẩn bảo mật quốc tế như GDPR. Đồng thời, Chính phủ cần khuyến khích các doanh nghiệp và tổ chức phát triển sản phẩm và dịch vụ sáng tạo từ dữ liệu bằng cách cung cấp các chính sách hỗ trợ tài chính và hỗ trợ kỹ thuật. Ngoài ra, các tổ chức cung cấp sản phẩm, dịch vụ liên quan đến dữ liệu phải tuân thủ các quy định bảo mật chặt chẽ, bao gồm việc triển khai các hệ thống bảo mật như mã hóa, xác thực đa yếu tố, và giám sát an ninh liên tục. Chính phủ cũng cần giám sát và cấp phép đối với các tổ chức này để bảo đảm rằng việc sử dụng và chia sẻ dữ liệu được thực hiện minh bạch, công bằng, và bảo vệ quyền lợi của người dân.

Các quy định về quản lý quyền truy cập, chia sẻ và xử lý dữ liệu phải được xây dựng để bảo vệ tính riêng tư, an ninh dữ liệu và tạo điều kiện cho sự phát triển của nền kinh tế số, đồng thời đảm bảo rằng tất cả các bên tham gia đều có trách nhiệm và nghĩa vụ bảo vệ dữ liệu.

Câu 2

Quyền, nghĩa vụ và trách nhiệm của chủ thể dữ liệu, chủ sở hữu dữ liệu, chủ quản dữ liệu? Cơ chế bảo đảm thực hiện các quyền, nghĩa vụ này đối với tổ chức, cá nhân không phải là cơ quan nhà nước?



2.1. MỘT SỐ KHÁI NIỆM CÓ LIÊN QUAN

2.1.1. Dữ liệu

2.1.1.1. Dữ liệu số

- Lịch sử về dữ liệu tại Việt Nam

Tri thức là sức mạnh. Trong ngữ nghĩa Hán Việt, cả "tri" lẫn "thức" đều mang nghĩa "biết". Biết, nghĩa là nắm thông tin trong tay. Có thông tin, người ta tăng hiểu biết. Thiếu thông tin, người ta mù mờ và dễ đi đến những quyết định sai lầm. Trong xã hội hiện đại, việc nắm bắt thông tin nhanh chóng đóng vai trò then chốt trong việc ra quyết định, góp phần định hình hành vi xử sự của con người với nhau và hình thành xã hội văn minh. Song sự hình thành của các quy tắc xử sự xoay quanh việc thu thập, lưu trữ và xử lý thông tin có nguồn gốc sâu xa hơn trong lịch sử hình thành của nhân loại.



Từ "tri thức" trong chữ Nôm - Ảnh: Từ điển Hán Nôm

Thực chất, không cần đợi đến lúc xuất hiện chữ viết, nhu cầu ghi chép, hay *kí lục*, dưới những hình thức muôn hình vạn trạng đã xuất hiện xuyên suốt từ Đông sang Tây, hiện diện ở khắp mọi nền văn minh và gắn liền với quá trình khai sáng của nhân loại. Là một sinh thể có khả năng tự ý thức về

chính mình, con người ta luôn tìm cách lưu giữ dấu tích về bản thân và cuộc sống xung quanh dưới hình thức này hay hình thức khác. Các thành tựu khảo cổ đã phát hiện mẩu thông tin dân sự xưa nhất còn sót lại đến nay là "Kushim", một cái tên xuất hiện trên phiến đất sét từ thời Uruk (khoảng 3400 - 3000 năm trước Công nguyên).



Phiến đá Uruk - Ảnh: The History Blog

Cái tên xuất hiện trong một đoạn văn bản ghi chép nội dung và số lượng giao dịch đối với đại mạch - một thứ hàng hóa nông sản phổ biến của nền văn minh lúa nước Lưỡng Hà. Nội dung của văn bản đại khái là "29,086 đơn vị đại mạch 37 tháng Kushim". Theo các nhà nghiên cứu, cái tên "Ku-Shim" rất có thể là tên riêng của một người đàn ông Sumer chuyên phụ trách việc

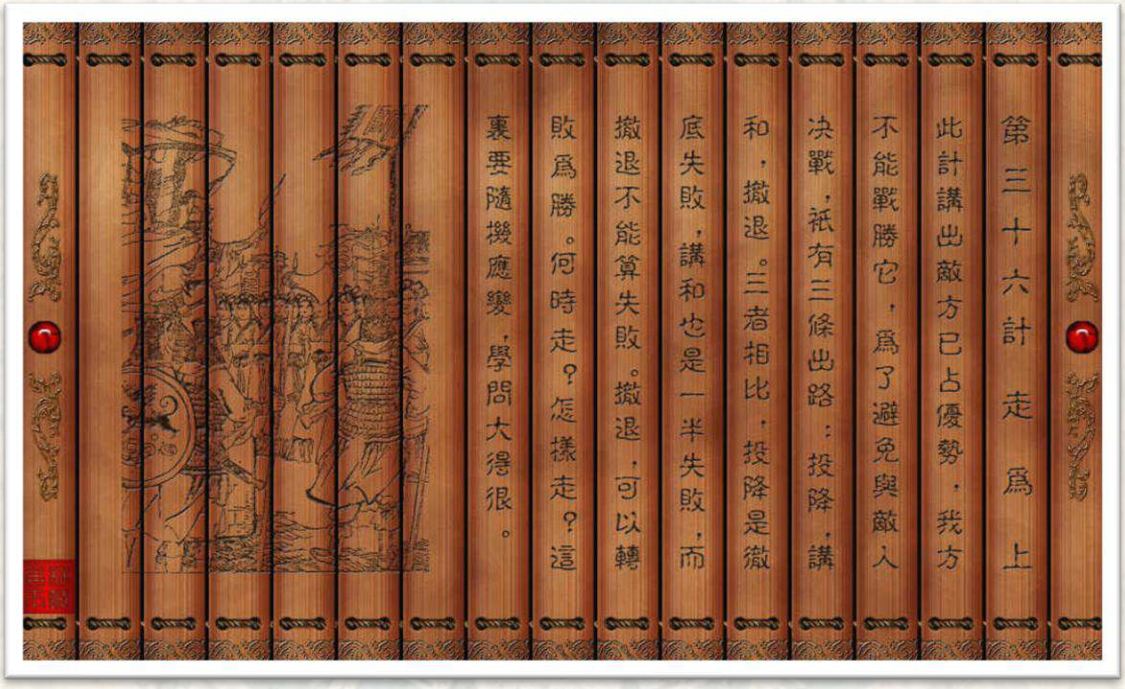
kiểm đếm hàng hóa, song cũng có quan điểm cho rằng đây là tên gọi của một chức danh công vụ nào đó trong nền văn minh Sumer. Ông Yuval Harrari đã giải nghĩa câu trên thành "Đã nhận tổng cộng 29,086 đơn vị đại mạch trong vòng 37 tháng. Ký tên, Kushim". Còn theo Nissen và cộng sự, Kushim rất có thể là chức danh chỉ người có chuyên môn trong ngành kế toán, vì nội dung trước sau của văn bản này liên quan đến việc kiểm đếm hàng hóa và đối chiếu tồn kho - là những dấu hiệu xưa nhất của nghề kế toán theo cách hiểu của chúng ta ngày nay.



Thời kỳ chiếm hữu nô lệ, giai đoạn sơ khai của hàng hóa - Ảnh: Internet

Nếu những phân tích vừa nêu là đáng tin cậy, thì việc thu thập, lưu trữ bảo quản và sử dụng dữ liệu đã xuất hiện như một sản phẩm tự nhiên của đời sống dân sự. Khi tư hữu xuất hiện, người ta sản xuất và trao đổi hàng hóa, của cải tạo ra làm gia tăng khối lượng tư bản và được đưa vào trao đổi nhằm

tối đa hóa lợi ích cho cuộc sống từng người. Cùng với đó, xuất hiện nhu cầu quản lý khối lượng tài sản tích trữ thông qua các công cụ sổ sách, chứng từ, ghi nhận thông tin. Từ giao lưu kinh tế, xuất hiện nhu cầu lưu giữ để thông tin có thể được lần lại, tra cứu và phục vụ nhu cầu quản lý, đối chiếu trong tương lai dưới hình thức dữ liệu. Hiểu theo cách này, *lưu trữ thông tin và khai thác giá trị thông tin của dữ liệu được lưu trữ* gắn liền với nhu cầu kinh tế, xã hội của loài người.



Thẻ tre Ngân Tước Sơn - Ảnh : Internet

Từ tạc, đẽo, khắc, ghi chú, kí hiệu, kí âm, kí họa, cho đến rất gần đây là "ghi âm, ghi hình", và "nhập liệu", đều là những hành vi gắn liền với việc kí lục thông tin thành dữ liệu để phục vụ cho việc lưu trữ, tra cứu. Sự xuất hiện của các công cụ mới trong lưu trữ và tư duy giúp việc nhập liệu trở nên nhanh và dễ dàng hơn. Có thể phân chia sự xuất hiện của công nghệ lưu trữ làm nhiều giai đoạn, gắn liền với các sự kiện lịch sử lớn của loài người. Trong số các phát kiến lưu trữ, có thể kể đến thẻ tre (thời điểm ra đời còn tranh cãi,

nhưng không sớm hơn thời nhà Thương), giấy (ra đời vào năm 105 ở Trung Hoa), đá, phiến đất sét, sách, máy tinh, vi mạch, bộ nhớ... Đi kèm với những phương tiện lưu trữ mới là những hình thức nhập liệu hiện đại hơn và dễ tiếp cận với người dùng cá nhân hơn. Nếu ở thời cổ đại, đầu bút lông mềm mại đã góp phần ghi chép những khuynh đảo của triều đại, thì bước sang ki nguyên máy tính, sự lên ngôi của mạng internet và các thiết bị thông minh đã kích hoạt sự chia sẻ liên tục của từng mẫu thông tin trong đời sống ngày thường của mỗi người. Mạng xã hội dần thế chỗ nhà văn hóa làng xã để trở thành nơi mọi người quần tụ và chia sẻ từng mẫu thông tin nhỏ diễn ra xung quanh mình. Một khi được nhập vào thì thông tin trở thành một hình thức tồn tại khác: dữ liệu. Khi công nghệ càng hiện đại và cả nhân hóa thì lượng dữ liệu được kí lục, lưu trữ và chia sẽ càng đi sâu hơn vào tiểu tiết. Dữ liệu về đời sống riêng của từng cá nhân được ghi chép và chia sẽ nhanh chóng hơn, cũng đồng nghĩa với việc loài người đứng trước nguy cơ đánh mất những hàng rào xã hội cuối cùng bảo vệ cho đời sống riêng tư của mình.

Bên cạnh những động lực kinh tế - xã hội, động lực mang tính chính trị cũng đã góp phần tạo nên các nguyên tắc xử sự xung quanh công tác thu thập, lưu trữ và xử lý dữ liệu trong dòng chảy lịch sử. Từ Tả Khâu Minh đến Tư Mã Thiên và các sử quan đời sau, việc ghi chép sự kiện và học thuộc các điển cổ xưa để "ôn cố tri tân" đã góp phần tạo nên một nền văn hiến độc đảo ở khu vực Đông Bắc Á và Đông Á. Nếu bên thế giới phương Tây, toàn bộ nền văn hiến Hy - La được xây dựng trên sự hiểu biết về xứ Địa Trung Hải cổ qua giọng kể sự lôi cuốn song không kém phần hoang đường của Thucydides; thì bên kia thế giới, nền văn minh Á Đông đã được biết đến sớm nhất qua lời tưởng thuật lạnh lùng, song chin chu về kĩ thuật biên niên, thống kê, lại thấm đẫm hơi thở triều đại của Tư Mã Thiên. "Thông cổ

kim chi biến", tuyệt tác Sử ký của Tư Mã Thiên đã mở đầu cho Nhị thập tứ sử hai mươi bốn bộ sử ghi lại sự biến thiên xuyên suốt mọi triều đại của Tầu. Ở một phạm vi rộng lớn hơn, đối với nền văn hóa Á Đông, Sử Ký chính là mẫu mực, là khuôn bản đầu tiên mở đầu cho kĩ thuật chép sử trong cả một nền văn minh Đông Á.



Tư Mã Thiên (145 TCN hoặc 135 TCN - 86 TCN) được coi là cha đẻ của ngành sử học Trung Quốc với bộ Sử ký Tư Mã Thiên - Ảnh: Internet

Không những sáng tạo ra nét và chữ tượng hình, người Trung Hoa xưa còn có công phát kiến ra ***"văn phòng tứ bảo":*** bút, nghiên, mực, giấy. Khi

đã sẵn có những công cụ tuyệt vời hỗ trợ cho việc ghi chép, văn truyền khẩu tự nhiên sẽ được ghi lại thành tư liệu và được lưu trữ theo những quy chuẩn nghiêm ngặt để truyền cho hậu thế. Giấy, dù làm từ da thú hay từ vỏ cây, đều dễ ẩm, mốc, dễ mục và dễ chảy. Vì giấy khó bảo quản hơn đất, đá, quy trình lưu trữ, bảo quản tài liệu đã được xác lập thành những bộ quy tắc chặt chẽ và được giao cho các viên quan đặc trách công việc này. Ngành lưu trữ, với những quy tắc nghề nghiệp rất đặc thù và nghiêm cẩn, đã ra đời như một hệ luận tất yếu từ những động lực chính trị của các triều đại ở khu vực Đông Á.



Đền Đô đài Ngự sử Bùi Cầm Hổ - vị quan chịu trách nhiệm ghi chép, lưu trữ vào triều đại vua Lê - Ảnh: Báo Hà Tĩnh

Trước những thực tế đó, pháp luật về dữ liệu phải vừa đảm bảo quá trình lưu trữ toàn diện, đúng đắn và tra cứu được khi cần thiết, nhưng cũng phải ngăn chặn những mưu đồ tiếp cận, thay đổi và xóa sổ tùy tiện, vô căn cứ. Tiếc thay, cổ luật Việt Nam chưa hẳn đã hệ thống hóa một cách đúng mức

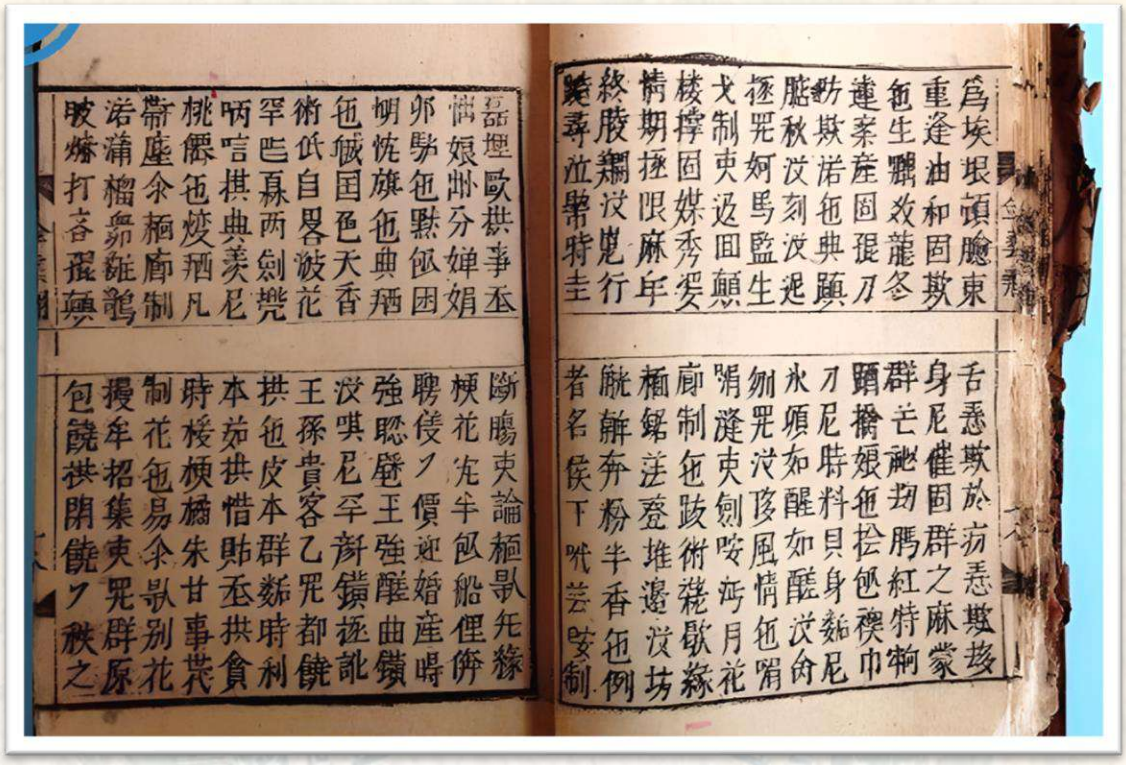
các quy định pháp luật về công tác sao lục, lưu trữ thông tin. Song rải rác đó đây, có thể nhận thấy những điểm đặc sắc về nguyên tắc kí lục, lưu trữ dữ liệu trong xã hội đương thời[187].

Về quyền tiếp cận, thay đổi và tiêu hủy các dữ liệu này, cổ luật chứa những quy định nghiêm ngặt về bảo vệ sách, vở thư tịch thuộc sở hữu của hoàng tộc cầm quyền. Chẳng hạn, sách vở được lưu trữ trong quốc khổ hoàng gia, được liệt vào hạng *"đồ ngự dụng"* thì thường dân không được động vào, nếu không sẽ phạm phải tội Đại bất kính (Điều 2.6, Phần Danh Lệ, Quốc Triều Hình Luật, Hậu Lê). Bên cạnh đó, người thường cũng không thể tiếp cận quốc khố bởi những quy định vô cùng nghiêm ngặt về vệ cấm (tham khảo Điều 6. Vệ Cấm, Quốc triều Hình luật). Tuy nhiên, liên quan đến công tác đăng bạ, hộ tịch, ta phát hiện văn hóa kí lục, lưu trữ thông qua hệ thống sổ sách và nhập dữ liệu qua quy định về đăng ký, đăng bạ vào, ra kinh thành. (Điều 11, Vệ Cẩm, Quốc triều Hình luật).

Về mặt sổ sách hộ tịch, những quy định về dữ liệu dân cư trong Quốc triều Hình luật tỏ ra nghiêm ngặt và thể hiện nguyên tắc thông tin đúng sự thật từ rất sớm. Chẳng hạn, Điều 98 Chương Vi Chế quy định, đối với các tờ trạng, số sách tâu lên, các quan sảnh quan viện phải biên rõ năm, tháng và ngày giao cho viên thuộc lại đối chiếu, và việc lưu trữ, lưu chuyển và đối chiếu phải thực hiện xong trong thời hạn quy định, không được nề hà. Bên cạnh đó, các xã quan làm số hộ khẩu mà khai sót số dân định thì phải tội (Điều 2, Hộ Hôn, Quốc triều Hình luật). Nhai lại ở cấp sảnh hay viện mà khai thêm hoặc khai bớt số dân trong số hộ tịch so với số dân thực sự tại địa phương thi phải tội (Điều 4, Hộ Hôn, Quốc triều Hình luật). Nếu khai dân định thành chức sắc thì

[187] Huỳnh Lê Tứ, Lê Thùy Khanh (2024), *Nghiên cứu tiếp cận pháp lý đối với dữ liệu số và cơ chế điều chỉnh quyền về dữ liệu số trong pháp luật Việt Nam*, Research Paper, UEH University.

phạt 70 trượng, người dân đinh được khai đó cũng chịu trượng, biếm hai tư và bị bắt lao địch. (Điều 28, Hộ Hôn, Quốc triều Hình luật).



Quốc triều Hình luật thời kỳ Lê Trung Hưng - Ảnh: Tạp chí Pháp lý

Tóm lại, việc lưu trữ thông tin thành dữ liệu là sản phẩm tự nhiên của đời sống dân sự và kinh tế. Khi tư hữu xuất hiện, người ta sản xuất và trao đổi hàng hóa, của cải tạo ra làm gia tăng khối lượng tư bản và được đưa vào trao đổi nhằm tối đa hóa lợi ích cho cuộc sống từng người, cùng với đó là nhu cầu quản lý khối lượng tài sản tích trữ thông qua các công cụ sổ sách, chứng từ, ghi nhận thông tin. Từ giao lưu kinh tế, xuất hiện nhu cầu lưu giữ để thông tin có thể được lần lại, tra cứu và phục vụ nhu cầu quản lý, đối chiếu trong tương lai dưới hình thức dữ liệu. Hiểu theo cách này, lưu trữ thông tin và khai thác giá trị thông tin của dữ liệu được lưu trữ là các quyền dân sự gắn liền với chức năng kinh tế, xã hội của loài người.

- Khái niệm dữ liệu và pháp luật về dữ liệu

Trước làn sóng của các cuộc cách mạng công nghiệp cùng với những đặc trưng về việc sử dụng các thiết bị công nghệ điện toán và kết nối internet trong công nghiệp và thương mại, khái niệm dữ liệu được tiếp cận và mở rộng thành *"dữ liệu số"*, hiểu như là các thông tin được ghi lại dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc những hình thức tương tự trên môi trường điện tử.



Dữ liệu ngày càng trở nên quan trọng đối với phát triển kinh tế, xã hội - Ảnh: Base.vn

Dữ liệu là *"nguyên liệu thô"* cần qua các bước xử lý để trở thành thông tin và tri thức, phục vụ giải quyết vấn đề[188]. S. Gualandi (2022) định nghĩa "Dữ liệu là những đơn vị thông tin, thường mang tính định lượng nhưng không nhất thiết, được thu thập, quan sát hoặc tạo ra và có thể được sử dụng cho mục đích suy luận, thảo luận hoặc tính toán"[189]. Tiếp cận dưới góc độ khoa học xã

[188] Cao, L. (2020), Data Science: A Comprehensive Overview.

[189] Gualandi, S., Pareschi, L., & Peroni, S. (2022), What do we mean by 'data'? A proposed classification of data types in the arts and humanities.

hội, dữ liệu không bao giờ trung lập, luôn gắn với quyền lực và tồn tại trong không gian thông tin mang tính động, được định hình bởi bối cảnh xã hội - chính trị[190].

Theo quy định tại Khoản 5 Điều 4 Luật giao dịch điện tử 2005, "dữ liệu" là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự". Khái niệm này vẫn giữ nguyên trong Luật giao dịch điện tử 2023, tuy nhiên, có sự phân loại chi tiết dựa trên nguồn gốc hình thành như sau:

"Dữ liệu là ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh, hoặc dạng tương tự khác. Dữ liệu điện tử là dữ liệu được tạo ra, xử lý bằng phương tiện điện tử. Dữ liệu số là dữ liệu điện tử được tạo lập bằng phương pháp dùng tín hiệu số". (Điều 3 (6), 3 (7), 3 (8) Luật giao dịch điện tử 2023).

Tuy nhiên, đến năm 2024, khái niệm về dữ liệu số đã được mở rộng và thay đổi mang tính phổ quát hơn. Khoản 1 Điều 3 Luật Dữ liệu 2024 nêu rõ: *"Dữ liệu số là dữ liệu về sự vật, hiện tượng, sự kiện, bao gồm một hoặc kết hợp các dạng âm thanh, hình ảnh, chữ số, chữ viết, ký hiệu được thể hiện dưới dạng kỹ thuật số"*. Nói cách khác, bất kỳ thông tin nào về đối tượng, sự kiện được biểu diễn dưới dạng tín hiệu số (các dãy bit) mà máy tính có thể đọc được thì đều là dữ liệu số. Ví dụ, văn bản, hình ảnh, âm thanh, video ở định dạng điện tử đều là dữ liệu số.

Một số khái niệm khác có thể đề cập như: Theo Nguyễn Như Ý (2013), dữ liệu là *"những thông tin như văn bản, số liệu, âm thanh, hình ảnh... được biểu diễn trong máy tính dưới dạng quy ước, nhằm tạo sự dễ dàng cho việc lưu trữ, xử lí"*. Khoản 1 Điều 2 Luật Dữ liệu châu Âu (EU Data Act) định nghĩa: dữ liệu là *"bất kỳ biểu diễn kỹ thuật số nào của các hành vi, sự kiện*

[190] Iliadis, A., & Russo, F. (2016), Critical Data Studies: An Introduction.

hoặc thông tin và bất kỳ tập hợp nào của các hành vi, sự kiện hoặc thông tin đó, bao gồm dưới dạng bản ghi âm thanh, hình ảnh hoặc nghe nhìn".



Minh họa cho dữ liệu số - Ảnh: TM Forum

Từ các quan niệm trên, có thể hiểu dữ liệu số là tập hợp thông tin phản ánh các sự vật, hiện tượng trong thế giới khách quan, được được số hóa, lưu trữ và xử lý bằng thiết bị kỹ thuật số. Nói cách khác, dữ liệu số chính là phiên bản số hóa của thông tin, cho phép máy móc thu nhận, đọc hiểu và xử lý phục vụ các mục đích khác nhau. Về nội hàm, khái niệm "dữ liệu số" theo Luật Dữ liệu 2024 nhấn mạnh hai yếu tố: ***(i)*** Nội dung thông tin mà dữ liệu thể hiện (về sự vật, hiện tượng, sự kiện); và ***(ii)*** Hình thức thể hiện kỹ thuật số (âm thanh, hình ảnh, ký tự số hóa). Điều này cho thấy dữ liệu số bao gồm mọi dạng thông tin có thể được chuyển thành bit và byte trong hệ thống máy tính. Dữ liệu số có thể xuất phát từ nhiều nguồn (cảm biến IoT thu thập dữ liệu môi trường, người dùng nhập liệu, hệ thống doanh nghiệp ghi nhận giao dịch…) nhưng điểm chung là đều được chuyển đổi thành dạng số để lưu trữ, xử lý.

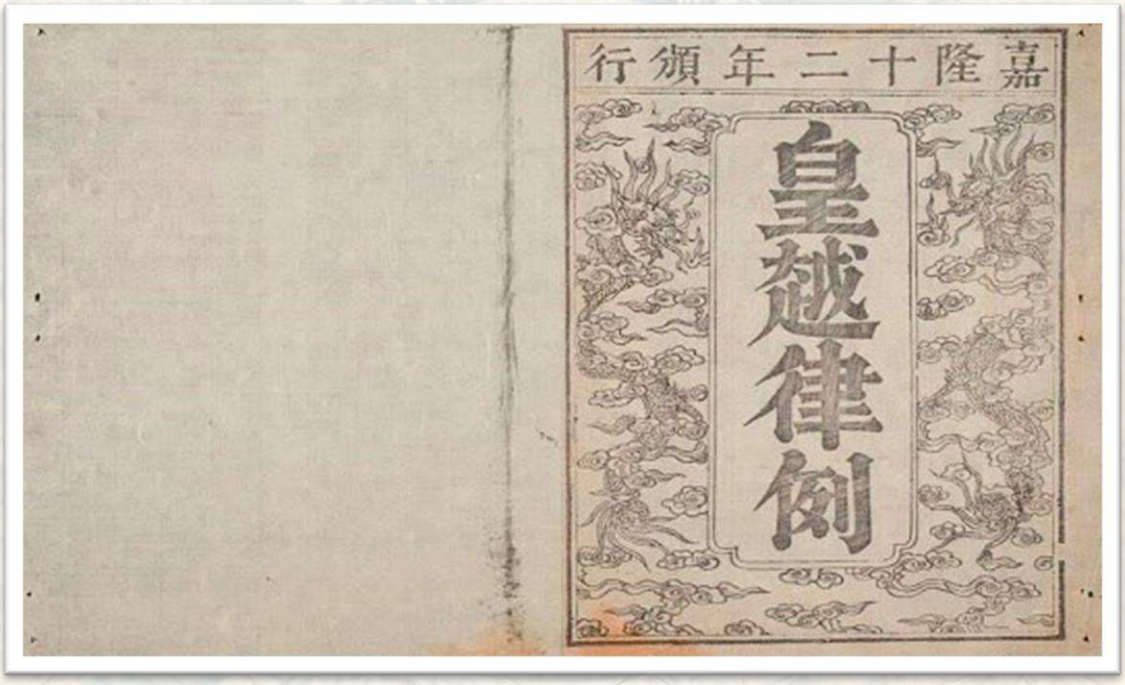
Như vậy, dữ liệu số là một khái niệm rộng, bao hàm từ dữ liệu văn bản, đa phương tiện đến dữ liệu do máy móc tự động tạo ra trong kỷ nguyên số.

Từ những khái niệm nêu trên, có thể thấy *pháp luật về dữ liệu* là hệ thống các quy tắc xử sự của chủ thể có liên quan đến dữ liệu. Về góc độ lý luận, có thể nhận định dữ liệu là đối tượng của quyền lực, trong quan hệ pháp luật thì dữ liệu là đối tượng vật chất bên ngoài liên quan đến nội dung của quan hệ pháp luật. Các quan hệ xã hội liên quan đến các dữ liệu được pháp luật điều chỉnh được gọi là pháp luật dữ liệu. Tầm quan trọng của pháp luật dữ liệu với tư cách là một lĩnh vực pháp luật đặc thù được thể hiện qua hai chức năng của pháp luật dữ liệu, cụ thể như sau:

Thứ nhất, việc nắm bắt và kiểm soát bằng pháp luật đối với chu trình thụ đắc, lưu trữ, chu chuyển thông tin kinh tế - xã hội dưới dạng dữ liệu là biểu hiện của quyền lực nhà nước và là công cụ để bộ máy nhà nước thực hiện chức năng kinh tế và chức năng xã hội. Luận điểm này có thể được làm rõ thông qua ví dụ về các quy phạm pháp luật liên quan đến việc ghi chép thông tin và bảo quản dữ liệu trong của luật Việt Nam.

Chẳng hạn, theo quy định trong Luật Hồng Đức, các quan liêm phóng (mật tra) khi xét sự việc phải đúng sự thực, nếu có sai lầm thì sẽ chịu tội *biếm* hoặc nặng hơn là chịu hình phạt lao dịch, khổ sai. Nếu quan điều tra cố tình bóp méo sự thật vì tư thù thì sẽ bị lưu đày nơi non thiên nước độc, hoặc nặng hơn, là chịu tội chết (Điều 101, Vệ Cấm, Quốc triều Hình luật nhà Lê). Đối với thông tin về chuyên cần của quan lại, nếu viên quan cấp cao hơn ghi chép và khai báo không chính xác thì sẽ bị biếm hoặc mất chức (Điều 122, Vệ Cấm Quốc triều Hình luật nhà Lê); nếu vì sợ quyền thế hay vì che giấu cho người thân thích mà ém nhẹm thông tin không khai báo cho vua khi tiếp nhận tờ tâu thì bị khổ sai (Điều 115 Vệ Cấm, Quốc Triều Hình luật nhà Lê).

Tuy nhiên, thông tin không chỉ phải được khai báo trung thực đối với cấp trên, nếu quan lại nhận được chiếu lệnh của Triều đình ban xuống mà không sao lục, niêm yết và công báo cho dân chúng thì sẽ bị phạt bị biếm hoặc bị bãi chức (Điều 124 Vệ cấm, Quốc Triều hình luật nhà Lê). Bên cạnh đó, theo quy định tại Điều 99 Chương Vi Chế, Lê Triều Hình luật, thì sổ phê, sổ lưu trữ của quan phải được trình lên quan trên để cất vào tủ công chứ không được cất giữ làm của riêng. Xa hơn, theo Luật Gia Long, nếu các thông tin này được lưu trữ dưới dạng chế thư thì việc đánh cắp những phương tiện lưu trữ đó bị phạt rất nặng (Điều 227).



Bộ luật Hồng Đức - Ảnh: Tạp chí Pháp lý

Sẽ là khiên cưỡng khi nói rằng các nhà cầm quyền đã sớm nghĩ đến khía cạnh quyền đối với các phương tiện chuyên chở dữ liệu. Song có thể khẳng định rằng, nhà làm luật xưa, ít nhất từ thời nhà Hậu Lê cho tới nhà Nguyễn, đã ý thức được về mức độ cần thiết của việc hạn chế quyền tiếp cận dữ liệu, bằng những quy định về hạn chế thời hạn lưu trữ dữ liệu, hạn

chế phương thức lưu trữ dữ liệu, quản lý mục đích lưu trữ dữ liệu và giới hạn những chủ thể nào được phép tiếp cận và xử lý dữ liệu. Trong bối cảnh xây dựng nhà nước pháp quyền, phát huy quyền tự do kinh doanh và các quyền hợp pháp, chính đáng của người dân nảy sinh nhu cầu phải kiểm soát quyền thực thi quyền lực nhà nước trong việc thu thập, lưu trữ và xử lý các dữ liệu dân cư và kinh tế - xã hội.



Dữ liệu cần phải được khai thác có kiểm soát, có hiệu quả - Ảnh: Internet

Thứ hai, pháp luật về dữ liệu phản ánh quyền con người, quyền công dân trong bối cảnh chuyển đổi số. Đứng trước cuộc cách mạng công nghiệp 4.0, dữ liệu đóng vai trò quan trọng, sống còn đối với việc phát triển kinh tế và bảo đảm an sinh xã hội. Vì dữ liệu là phương tiện chuyên chở thông tin, sự kết hợp một cách đúng đắn các mẩu dữ liệu sẽ kiến tạo nên thông tin ý nghĩa, bổ sung và làm giàu thêm cho kiến thức của con người Như vậy, khi thực hiện quyền chiếm hữu, sử dụng và quyết định việc kết hợp các mẩu dữ liệu để tạo ra kiến thức, người dân sẽ phát huy tốt các quyền dân sự, kinh tế để đáp ứng nhu cầu phát triển của mình. Bên cạnh đó, việc tiếp cận và dụng ích thông tin từ dữ liệu phải đặt trong sự cân bằng với những quyền và lợi ích chính đáng

khác, trong đó bao gồm quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân, bí mật gia đình. Điều chỉnh quan hệ dữ liệu bằng pháp luật phải đảm bảo những nguyên tắc tổ chức bộ máy nhà nước và quản lý xã hội, vừa phải cân bằng được quyền và lợi ích chính đáng của người dân.

2.1.1.2. Đặc điểm của dữ liệu

Dữ liệu, đặc biệt là dữ liệu số, mang nhiều đặc tính khác biệt so với các loại tài sản truyền thống. Những đặc điểm này không chỉ bắt nguồn từ bản chất kỹ thuật của dữ liệu mà còn từ cách dữ liệu được khai thác, lưu trữ, và sử dụng trong xã hội hiện đại. Cụ thể như sau:

- Tính phi vật chất nhưng có giá trị tài sản.

Dữ liệu không có hình thái vật chất cụ thể, song lại có giá trị kinh tế to lớn. Bản chất phi vật chất của dữ liệu khiến giá trị của nó phụ thuộc vào khả năng số hóa, lưu trữ, xử lý và phân tích bằng công nghệ. Cùng một tập dữ liệu, khi áp dụng công nghệ AI và khoa học tiên tiến có thể khai thác giá trị cao hơn rất nhiều so với cách tiếp cận thủ công. Điều này biến dữ liệu thành "nguyên liệu số" có thể liên tục được tái chế và nâng cấp giá trị theo thời gian [93]. Pháp luật Việt Nam đã xác định *"dữ liệu là tài nguyên"* và định hướng phát triển dữ liệu trở thành một loại tài sản trong nền kinh tế số. Quyền của chủ sở hữu dữ liệu đối với dữ liệu cũng được thừa nhận là quyền tài sản theo pháp luật dân sự. Các nghiên cứu của McKinsey Global Institute (2011) chỉ ra rằng việc sử dụng dữ liệu lớn có thể thúc đẩy năng suất lao động, tối ưu chuỗi cung ứng và tạo ra mô hình kinh doanh mới. Bên cạnh đó, việc định giá dữ liệu thường dựa trên các tiêu chí như độ chính xác, tính đầy đủ, tính độc quyền và khả năng khai thác thương mại. Dữ liệu khách hàng, dữ liệu hành vi tiêu dùng hay dữ liệu nghiên cứu khoa học đều có thể trở thành tài sản giao dịch, mua bán, hoặc cấp phép sử dụng trên thị trường. Các công ty

công nghệ lớn như Google, Meta đã xây dựng mô hình kinh doanh dựa gần như hoàn toàn vào việc khai thác và thương mại hóa dữ liệu người dùng (OECD, 2015). Điều này cho thấy dữ liệu có thể được khai thác, mua bán, trao đổi giá trị như một loại hàng hóa đặc biệt trong thị trường số.



Dữ liệu số tồn tại dưới tổ hợp của nhiều kí tự "0" và "1" - Ảnh: National Highways

- Tính nhân bản và tiếp cận dễ dàng.

Khác với tài sản hữu hình như nhà cửa, xe cộ… dữ liệu có thể được sao chép, truyền gửi gần như không giới hạn với chi phí rất thấp mà không làm mất đi bản gốc. Đây là đặc tính xuất phát từ bản chất phi vật chất của dữ liệu và hạ tầng mạng hiện đại (Internet, giao thức truyền tải, lưu trữ phân tán), nơi việc truyền dẫn thông tin diễn ra nhanh chóng với chi phí gần như bằng không [137]. Một mẩu dữ liệu số có thể được nhiều người truy cập, sử dụng đồng thời mà không bị *"tiêu hao"* khi sử dụng. Chính tính phi đối kháng

(non-rivalrous) này khiến dữ liệu trở thành nguồn lực đặc biệt, đó là càng nhiều người dùng khai thác thì dữ liệu càng phát huy giá trị [111], [137].



Dữ liệu số có thể được sao chép, nhân bản, truyền gửi - Ảnh: VnEconomy

Tuy nhiên, cũng vì dễ sao chép nên dữ liệu dễ bị rò rỉ, mất kiểm soát nếu không được bảo mật tốt. Khả năng sao chép nhanh chóng đồng nghĩa với việc một khi dữ liệu đã thoát khỏi phạm vi kiểm soát ban đầu, việc thu hồi gần như bất khả thi. Khác với tài sản vật chất, vốn có thể bị thu giữ lại, dữ liệu số chỉ cần một bản sao ngoài tầm kiểm soát là có thể tiếp tục bị sao chép vô hạn. Ví dụ, một tệp dữ liệu khách hàng bị tải xuống từ hệ thống nội bộ và lưu trên USB cá nhân. Chỉ mất vài giây để tệp này được chuyển qua email hoặc ứng dụng nhắn tin, và ngay lập tức tồn tại hàng chục bản sao ở nhiều vị trí khác nhau. Khi dữ liệu bị sao chép và lan truyền mất kiểm soát, đối với cá nhân, nó xâm phạm quyền riêng tư, dẫn đến lừa đảo, tấn công có mục tiêu (spear phishing), hoặc giả mạo danh tính; đối với doanh nghiệp, chiến lược, bí mật kinh doanh có thể bị lộ, mất lợi thế cạnh tranh; đối với nhà nước, nguy cơ xâm phạm an ninh quốc gia nếu thông tin nhạy cảm bị chuyển ra ngoài biên giới.

- Tính phụ thuộc vào công nghệ.

Dữ liệu số tồn tại dưới dạng chuỗi bit "0" và "1" và không thể được con người trực tiếp hiểu nếu không có sự hỗ trợ của hệ thống công nghệ như phần cứng (máy tính, thiết bị lưu trữ), phần mềm (chương trình đọc/ghi dữ liệu, ứng dụng phân tích) và hạ tầng mạng (Internet, mạng nội bộ). Việc thu thập, lưu trữ, xử lý dữ liệu đòi hỏi hạ tầng kỹ thuật (máy tính, mạng, phần mềm). Do đó, chất lượng và giá trị của dữ liệu gắn liền với trình độ công nghệ. Ví dụ, trong thương mại điện tử: Một tập dữ liệu về hành vi mua hàng trực tuyến chỉ cho thấy giá trị lớn khi được phân tích bằng thuật toán gợi ý sản phẩm. Nếu chỉ xử lý thủ công, doanh nghiệp khó phát hiện xu hướng tiêu dùng hoặc tối ưu chiến dịch marketing. Một ví dụ khác, trong y tế, dữ liệu hình ảnh y khoa (MRI, CT scan) cần phần mềm xử lý hình ảnh và AI để phát hiện sớm tổn thương. Nếu không có công nghệ, dữ liệu này chỉ là chuỗi số vô nghĩa đối với phần lớn người dùng. Ngược lại, trong môi trường công nghệ hạn chế, việc xử lý thường chỉ dừng lại ở các thao tác cơ bản như lọc, sắp xếp, thống kê đơn giản, dẫn đến giá trị ứng dụng của dữ liệu không cao. Bên cạnh đó, chất lượng dữ liệu chịu ảnh hưởng trực tiếp từ công cụ thu thập như độ chính xác của cảm biến, độ phân giải của thiết bị ghi nhận, và tần suất thu thập quyết định mức độ tin cậy cũng như khả năng ứng dụng dữ liệu trong thực tiễn.

Sự chênh lệch về trình độ công nghệ cũng có thể kéo theo các hệ quả đáng chú ý về mặt pháp lý và trong công tác quản trị dữ liệu. ***Thứ nhất,*** xuất hiện nguy cơ bất bình đẳng về công nghệ khi các tổ chức hoặc doanh nghiệp sở hữu hạ tầng tiên tiến có thể khai thác dữ liệu hiệu quả hơn, tạo khoảng cách cạnh tranh lớn so với các đơn vị thiếu năng lực công nghệ. ***Thứ hai,*** khi dữ liệu được lưu trữ và phân tích thông qua nhà cung cấp dịch vụ bên thứ ba,

nguy cơ mất kiểm soát dữ liệu hoặc phụ thuộc vào công nghệ độc quyền gia tăng, đặc biệt nếu hạ tầng đó không thuộc quyền quản lý trực tiếp của chủ sở hữu dữ liệu. ***Thứ ba,*** để đảm bảo dữ liệu có thể được xử lý an toàn, bảo mật và liên thông giữa các hệ thống, cần ban hành các tiêu chuẩn thống nhất về định dạng dữ liệu, giao thức trao đổi và yêu cầu bảo mật, phù hợp với bối cảnh hội nhập quốc tế và sự phát triển nhanh chóng của công nghệ [89].

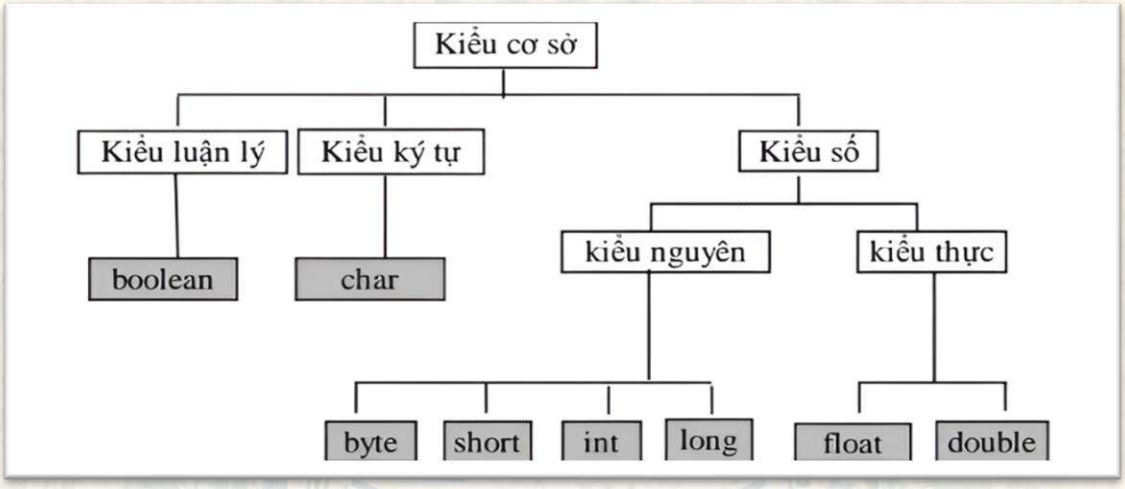


Công nghệ càng phát triển, hình thức tồn tại của dữ liệu số càng đa dạng - Ảnh: Báo và đài phát thanh truyền hình Lạng Sơn

- Tính đa dạng và phức tạp

Trong môi trường nghiên cứu, việc nghiên cứu quản lý dữ liệu là rất cần thiết, vì dữ liệu được tạo ra có thể rất phong phú, có nhiều định dạng khác nhau, đến từ nhiều nguồn khác nhau, được sử dụng cho nhiều mục đích khác

nhau và được sử dụng bởi nhiều ngành nghề và nghề nghiệp khác nhau[191]. Do đó, dữ liệu ngày nay rất đa dạng về định dạng (văn bản, hình ảnh, âm thanh, video, mã nhị phân), nguồn gốc (do con người nhập liệu, do thiết bị thu thập tự động), và dung lượng (từ vài byte dữ liệu cảm biến đến hàng petabyte dữ liệu lớn).



Các loại dữ liệu cơ bản trong máy tính - Ảnh: Internet

Về cấu trúc, dữ liệu không còn giới hạn ở dạng văn bản, mà hiện nay tồn tại trong nhiều cấu trúc khác nhau, như: Dữ liệu có cấu trúc được tổ chức thành bảng, hàng, cột, dễ lưu trữ và xử lý bằng cơ sở dữ liệu truyền thống; Dữ liệu bán cấu trúc (semi-structured), như XML, JSON, có nhãn mô tả nhưng không tuân thủ hoàn toàn mô hình bảng; Dữ liệu phi cấu trúc (unstructured), như video, hình ảnh, file âm thanh, thường cần công nghệ AI/ML để trích xuất thông tin. Ngoài ra, dữ liệu còn có vòng đời riêng: sinh ra, biến đổi, tích lũy, có thể lỗi thời và cần cập nhật. Do đó, quản trị dữ liệu đòi hỏi phương pháp tiếp cận toàn diện để đảm bảo tính chính xác, đầy đủ, kịp thời của dữ liệu trong suốt vòng đời của nó.

[191] Rosini, Rahmatunnisa, M., Sunardi, Priyanto, I. F. (2025). Research Data Management in Environmental Studies: Scoping Review and Bibliometrics Analysis. Data Science Journal, 24: 20, pp. 1–18. DOI: https://doi.org/10.5334/dsj-2025-020

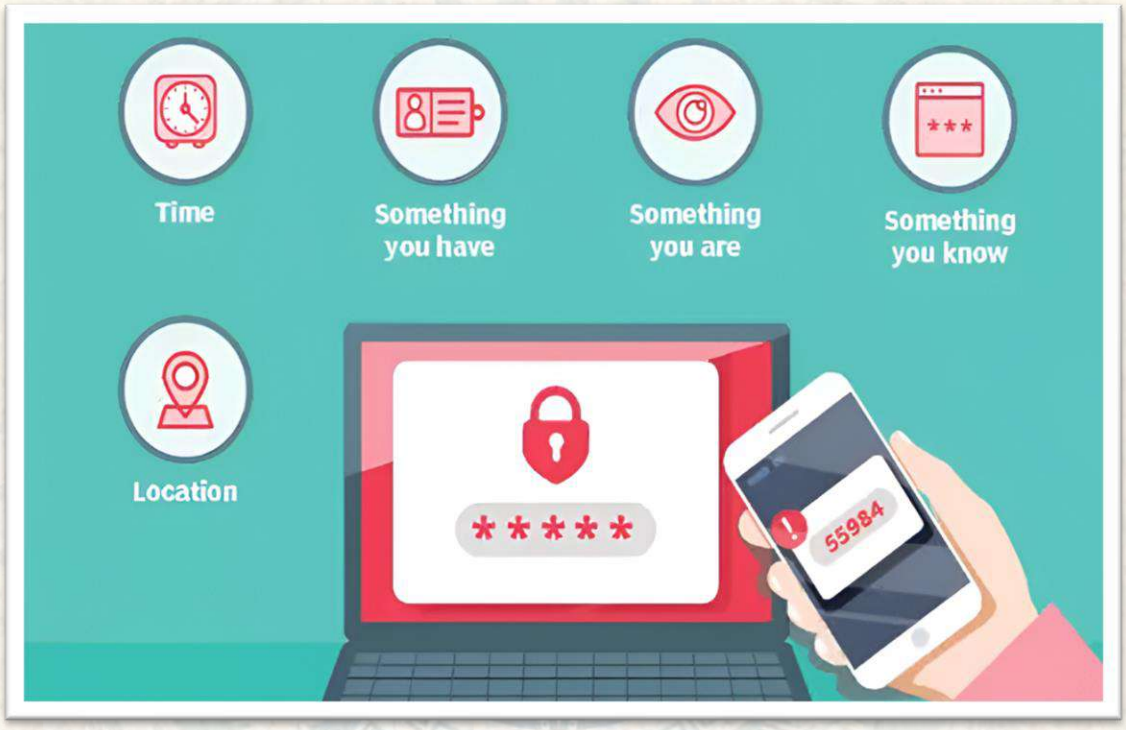
- Tính nhạy cảm và cần bảo vệ

Do không giới hạn về thông tin mà dữ liệu phản ánh, một bộ phận đáng kể dữ liệu số chứa đựng thông tin quan trọng liên quan trực tiếp đến quyền, lợi ích hợp pháp của cá nhân, hoặc an ninh, lợi ích chiến lược của quốc gia. Sự nhạy cảm này xuất phát từ hai yếu tố chính: ***(1)*** *Giá trị thông tin cao* - dữ liệu có thể tiết lộ danh tính, hành vi, bí mật thương mại hoặc thông tin chiến lược; ***(2)*** *Tính dễ sao chép và lan truyền* - chỉ cần một lỗ hổng bảo mật, dữ liệu có thể bị phát tán ra ngoài phạm vi kiểm soát gần như ngay lập tức. Một số loại dữ liệu nhạy cảm thường gặp như dữ liệu cá nhân đặc biệt (thông tin sức khỏe, sinh trắc học, vân tay, ADN, định vị, tài chính, tôn giáo, đời sống riêng tư), bí mật kinh doanh (công thức sản xuất, chiến lược kinh doanh, dữ liệu khách hàng, kế hoạch nghiên cứu phát triển), dữ liệu về an ninh quốc gia (bản đồ quân sự, tin tình báo, kế hoạch phòng thủ, thông tin hạ tầng trọng yếu).

Dữ liệu nhạy cảm, nếu bị lộ lọt hoặc sử dụng sai mục đích, có thể gây ra những hệ quả nghiêm trọng ở nhiều cấp độ. *Ở cấp độ cá nhân*, rủi ro bao gồm xâm phạm quyền riêng tư, bị lừa đảo, đánh cắp danh tính và chịu phân biệt đối xử dựa trên thông tin cá nhân bị khai thác. *Ở cấp độ doanh nghiệp*, việc rò rỉ dữ liệu có thể dẫn tới mất lợi thế cạnh tranh, thiệt hại tài chính đáng kể và suy giảm uy tín thương hiệu trên thị trường. *Ở cấp độ quốc gia*, những vụ lộ lọt dữ liệu chiến lược có thể đe dọa an ninh, xâm phạm chủ quyền và gây bất ổn chính trị - xã hội. Một ví dụ điển hình là vụ rò rỉ dữ liệu 500 triệu tài khoản Facebook năm 2019, trong đó thông tin như số điện thoại, email và địa chỉ của người dùng bị khai thác cho các hoạt động spam, lừa đảo và thao túng chính trị [140].

Để hạn chế các rủi ro này, việc tuân thủ các nguyên tắc bảo vệ dữ liệu nhạy cảm là bắt buộc. Trước hết, bảo mật đảm bảo rằng chỉ những cá nhân

hoặc tổ chức được ủy quyền mới có quyền truy cập dữ liệu. Tiếp đó, tính toàn vẹn yêu cầu dữ liệu phải được bảo vệ khỏi mọi hành vi thay đổi, giả mạo trong quá trình lưu trữ và truyền tải. Cuối cùng, tính sẵn sàng bảo đảm dữ liệu luôn khả dụng cho các mục đích hợp pháp nhưng phải dưới sự kiểm soát chặt chẽ.



Cơ chế xác thực đa yếu tố - Ảnh: Viblo

Từ góc độ thực thi, các cơ quan và doanh nghiệp cần triển khai đồng bộ cả giải pháp kỹ thuật, tổ chức và pháp lý. Về kỹ thuật, nên áp dụng mã hóa dữ liệu, xác thực đa yếu tố và hệ thống phát hiện xâm nhập (IDS/IPS) để giảm thiểu nguy cơ tấn công. Về tổ chức, cần đào tạo nhân sự về an toàn dữ liệu, đồng thời xây dựng quy trình ứng phó nhanh với các sự cố rò rỉ. Về pháp lý, cần ban hành và tuân thủ chính sách bảo vệ dữ liệu phù hợp với quy định quốc gia và tiêu chuẩn quốc tế, chẳng hạn như ISO/IEC 27001 hoặc hướng dẫn của NIST, nhằm bảo đảm tính thống nhất và hiệu lực trong quản trị dữ liệu nhạy cảm.



Tiêu chuẩn ISO 27001 - Ảnh: ISO

Những đặc điểm trên cho thấy dữ liệu vừa là một loại tài sản đặc biệt có giá trị, vừa đòi hỏi chế độ quản lý, bảo vệ riêng. Trong bối cảnh chuyển đổi số, hiểu rõ đặc tính của dữ liệu giúp xây dựng khung pháp lý phù hợp để khai thác dữ liệu hiệu quả đi đôi với bảo vệ quyền và lợi ích hợp pháp.

2.1.1.3. Phân loại

Nếu xem dữ liệu là đối tượng điều chỉnh của pháp luật, thì dữ liệu phải đáp ứng những tiêu chí về đối tượng của quan hệ pháp luật mà lý luận về pháp luật đặt ra. Trước khi Luật Dữ liệu ra đời, khung pháp lý Việt Nam phân loại dữ liệu ra thành nhiều nhóm với quan hệ tương ứng với tính chất của các dữ liệu đó, cụ thể như sau:

Thứ nhất, nhóm dữ liệu liên quan đến hoạt động kiểm soát và quản lý xã hội của cơ quan nhà nước, hay dữ liệu dân cư. Nhóm này bao gồm các dữ liệu thống kê về tình hình kinh tế, xã hội trong và ngoài nước, bí mật nhà nước, dữ liệu hộ tịch, nhân thân của người dân, dữ liệu dân cư, dân số, dữ

liệu về tài nguyên quốc gia… Đối với các dữ liệu này, hiện pháp luật về dữ liệu tại Việt Nam đang xác định chủ thể thực hiện quyền thu thập, xử lý, khai thác chúng là cơ quan nhà nước.



Nhóm dữ liệu của cổng dữ liệu quốc gia - Ảnh: Báo Điện tử Chính phủ

Thứ hai, nhóm dữ liệu mà người dân có thể tự do tiếp cận, chiếm hữu, dụng ích và định đoạt để tạo ra giá trị về mặt kinh tế, xã hội. Vì các loại dữ liệu thuộc khối dân sự này rất đa dạng nên các quy phạm pháp luật hiện hành điều chỉnh các quan hệ liên quan đang được phân loại dựa trên những tiêu chí không thống nhất, tiêu biểu như:

+ ***Tùy thuộc vào nguồn gốc hình thành,*** Luật Giao dịch điện tử 2023 chia dữ liệu thành "dữ liệu", "dữ liệu số", "dữ liệu điện tử", và "dữ liệu chủ", đồng thời định nghĩa "dữ liệu" nói chung (khoản 6, 7, 8, 9 Điều 3, Luật Giao dịch điện tử 2023).

+ ***Tùy thuộc vào tính chất gắn liền với lợi ích nhân thân,*** Nghị định 13/2023/NĐ-CP đưa ra tiêu chí để xác định *"dữ liệu cá nhân"* và chia làm

hai loại là *"dữ liệu cá nhân cơ bản"* và *"dữ liệu cá nhân nhạy cảm"* (Điều 2, Nghị định 13/2023/NĐ-CP về Bảo vệ dữ liệu cá nhân). Việc phân chia này giả định rằng có sự tồn tại của những dữ liệu không phải là dữ liệu cá nhân, và từ đó, không thuộc đối tượng điều chỉnh của Nghị định.

+ ***Tùy thuộc vào tính chất là thông tin dân cư, hộ tịch,*** Luật căn cước công dân đưa ra hai loại dữ liệu là "dữ liệu quốc gia về dân cư", "dữ liệu căn cước công dân", và "dữ liệu chuyên ngành", gắn trong các khái niệm rộng hơn (khoản 4, 5, 6 Điều 3, Luật Căn cước công dân 2014).

+ ***Tùy thuộc vào chức năng chuyên môn,*** Luật lưu trữ đưa ra khái niệm "tài liệu", "tài liệu trữ", "tài liệu của cá nhân, gia đình, dòng họ", "tài liệu lưu trữ điện tử",... (khoản 2, 3 Điều 2 Luật lưu trữ 2011).

Từ những thống kê sơ bộ trên, không khó để nhận thấy rằng thời điểm đó, pháp luật Việt Nam không đưa ra các tiêu chí thống nhất để phân loại dữ liệu, để từ đó xây dựng các quy phạm pháp luật liên quan để điều chỉnh. Sâu xa hơn, phần lớn các sự phân loại hiện có được đặt cơ sở trên tiêu chí tính chất của dữ liệu. Tuy nhiên, sau khi Luật Dữ liệu 2024 được phê duyệt và có hiệu lực từ ngày 01/7/2025, dữ liệu đã có căn cứ cụ thể để xác định, cụ thể tại Điều 13 Luật Dữ liệu 2024, bao gồm:

- Đối với cơ quan nhà nước

+ ***Dựa trên tính chất chia sẻ dữ liệu,*** bao gồm dữ liệu dùng chung, dữ liệu dùng riêng, dữ liệu mở. Điều 3 Luật Dữ liệu 2024 quy định: *"2. Dữ liệu dùng chung là dữ liệu được tiếp cận, chia sẻ, khai thác, sử dụng chung trong các cơ quan Đảng, Nhà nước, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội; 3. Dữ liệu dùng riêng là dữ liệu được tiếp cận, chia sẻ, khai thác, sử dụng trong phạm vi nội bộ của cơ quan Đảng, Nhà nước, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội; 4. Dữ*

liệu mở là dữ liệu mà mọi cơ quan, tổ chức, cá nhân có nhu cầu đều được tiếp cận, chia sẻ, khai thác, sử dụng". Có thể thấy rằng, "dữ liệu dùng chung" và "dữ liệu dùng riêng" có phạm vi truy cập, khai thác hẹp hơn so với "dữ liệu mở". Đó là những dữ liệu được dùng phục vụ cho hoạt động quản lý xã hội của cơ quan nhà nước, trong đó, dữ liệu dùng riêng có phạm vi hẹp nhất, đó là chỉ được dùng riêng (Ví dụ: Hồ sơ nhân sự, kế hoạch nội bộ của một Bộ, ngành) trong nội bộ của một cơ quan, tổ chức nhà nước. Ngược lại, dữ liệu mở (ví dụ: Dữ liệu thời tiết, bản đồ hành chính, số liệu thống kê công khai) là dữ liệu mà mọi cơ quan, tổ chức, cá nhân có nhu cầu đều được tiếp cận, chia sẻ, khai thác, sử dụng nhằm khuyến khích sáng tạo, phát triển dịch vụ và sản phẩm dữ liệu mới. Quyền truy cập dữ liệu mở không hạn chế, trừ trường hợp luật khác có quy định bảo mật.

+ ***Dựa trên tính chất quan trọng***, ta xác định loại dữ liệu quan trọng, dữ liệu cốt lõi và dữ liệu khác. Theo Luật Dữ liệu 2024, dữ liệu quan trọng là dữ liệu *có thể* tác động đến quốc phòng, an ninh, đối ngoại, kinh tế vĩ mô, ổn định xã hội, sức khỏe và an toàn cộng đồng thuộc danh mục do Thủ tướng Chính phủ ban hành. Trong khi đó, dữ liệu cốt lõi chính là dữ liệu quan trọng *trực tiếp* tác đến các khách thể quan trọng của xã hội như trên. Sở dĩ cần thiết phải quy định loại dữ liệu này nhằm có cơ sở phân công các cơ quan ban ngành phối hợp tiến hành các biện pháp quản lý chặt chẽ để phòng ngừa, ngăn chặn các hoạt động xâm phạm đến an toàn của dữ liệu quan trọng. Các thông tin trong dữ liệu quan trọng thường ở mức bảo mật cao, có cấp độ mật từ "mật" đến "tuyệt mật" và yêu cầu phải được bảo vệ nghiêm ngặt trong quá trình thu thập, khai thác. Quy phạm pháp luật được áp dụng đối với loại dữ liệu này do Chính phủ ban hành và triển khai thực hiện, như: Luật bảo vệ bí mật nhà nước, Quyết định số 20/QĐ-

TTg ngày 01/7/2025 của Thủ tướng Chính phủ về ban hành danh mục dữ liệu quan trọng, dữ liệu cốt lõi…



Các cán bộ, chiến sĩ đang theo dõi dữ liệu của trung tâm điều hành thông minh - Ảnh: VnEconomy

+ ***Dựa trên nguồn gốc hình thành***, bao gồm tài liệu gốc, tài liệu đã xử lý. Theo Luật Dữ liệu 2024, dữ liệu gốc là dữ liệu được tạo lập trong quá trình hoạt động của cơ quan, tổ chức, cá nhân hoặc thu thập, tạo lập từ số hóa bản chính giấy tờ, tài liệu, các dạng vật chất khác. Về bản chất, dữ liệu gốc chính là *"bản chính"* của dữ liệu, có giá trị pháp lý cao nhất để đối chiếu, xác thực như bản scan căn cước công dân gốc, bản ghi âm cuộc họp gốc. Đặc điểm của dữ liệu gốc là có tính xác thực và giá trị chứng cứ phục vụ hoạt động tố tụng dân sự và hình sự.

- Đối với tổ chức, doanh nghiệp tư nhân

Tại Khoản 2 Điều 13 Luật Dữ liệu 2024 quy định: *"2. Chủ sở hữu dữ liệu, chủ quản dữ liệu không thuộc quy định tại khoản 1 Điều này phải phân loại dữ liệu theo quy định tại điểm b khoản 1 Điều này và được phân loại dữ liệu theo các tiêu chí khác"*. Có thể thấy, đối tượng áp dụng ở khoản này là

chủ sở hữu dữ liệu và chủ quản dữ liệu là các cá nhân, tổ chức tư nhân không thuộc phạm vi cơ quan nhà nước (ví dụ: doanh nghiệp, tổ chức xã hội, cá nhân sở hữu dữ liệu). Theo quy định, họ bắt buộc phải thực hiện phân loại dữ liệu theo nhóm về tính chất quan trọng được nêu ở điểm b, Khoản 1, tức là phải xác định dữ liệu của mình thuộc dữ liệu cốt lõi, dữ liệu quan trọng, hay dữ liệu khác.

Ngoài tiêu chí bắt buộc trên, họ được quyền tự quyết bổ sung thêm các tiêu chí phân loại khác phù hợp với nhu cầu quản trị, xử lý, bảo vệ dữ liệu của mình (ví dụ: phân loại theo phòng ban, theo thời hạn lưu trữ, theo mức độ nhạy cảm thương mại). Nói cách khác, khoản này quy định một nghĩa vụ tối thiểu (phân loại theo tầm quan trọng) và quyền mở rộng (chọn thêm tiêu chí khác) cho tổ chức, cá nhân ngoài khối nhà nước. Qua đó, tạo ra sự thống nhất về tiêu chuẩn phân loại dữ liệu quan trọng trong cả khối cơ quan nhà nước và khối tư nhân, đảm bảo một cái nhìn chung để nhận diện, đánh giá và áp dụng các biện pháp bảo vệ phù hợp.

Thêm vào đó, cơ chế này còn tạo điều kiện để cơ quan quản lý đánh giá mức độ rủi ro, phòng ngừa các hành vi vi phạm, áp dụng biện pháp xử lý và chế tài tương xứng với giá trị của dữ liệu bị ảnh hưởng. Việc giữ lại quyền tự quyết trong việc bổ sung tiêu chí khác ngoài tiêu chí bắt buộc thể hiện sự linh hoạt cần thiết, cho phép các tổ chức thiết kế hệ thống phân loại dữ liệu gắn với đặc thù ngành nghề, chiến lược kinh doanh và yêu cầu tuân thủ tiêu chuẩn quốc tế. Mục tiêu kép mà quy định này hướng tới vừa là thiết lập *"ngôn ngữ chung"* về phân loại dữ liệu để phục vụ quản trị thống nhất ở tầm quốc gia, vừa khuyến khích khu vực tư nhân chủ động sáng tạo trong quản trị và bảo vệ dữ liệu, từ đó nâng cao hiệu quả sử dụng, bảo mật và giá trị kinh tế của nguồn tài nguyên dữ liệu.

Như vậy, hệ thống phân loại dữ liệu trong Luật Dữ liệu 2024 tạo ra một khuôn khổ quản lý đa chiều, cân bằng giữa nhu cầu khai thác, chia sẻ và bảo vệ dữ liệu. Việc phân loại dựa trên các tiêu chí chính như trên đã cho phép áp dụng các chế độ tiếp cận, bảo mật và phòng ngừa hệ quả khác nhau, thay vì một cơ chế đồng nhất cho mọi loại dữ liệu. Ở trục *"phạm vi truy cập"*, quy định về dữ liệu dùng chung, dùng riêng và mở vừa bảo đảm tính liên thông và tiết kiệm nguồn lực trong khu vực công, vừa tạo hành lang cho việc công khai dữ liệu phục vụ sáng tạo, phát triển sản phẩm, dịch vụ mới trong khu vực tư.



Xây dựng chính phủ số, xã hội số, kinh tế số lấy trọng tâm là dữ liệu - Ảnh: VnEconomy

Trong khi đó, trục *"quan trọng/cốt lõi"* gắn dữ liệu trực tiếp với các lĩnh vực chiến lược như quốc phòng, an ninh, kinh tế vĩ mô…, đặt ra yêu cầu bảo vệ cao hơn cho các loại dữ liệu có tác động tức thời và nghiêm trọng nếu bị xâm phạm. So với thông lệ quốc tế vốn thường dừng ở phân loại công

khai - nội bộ, cách tiếp cận của Việt Nam có nét tương đồng ở việc kiểm soát theo phạm vi truy cập, nhưng đặc biệt ở chỗ gắn chặt phân loại dữ liệu với quản trị nhà nước và chiến lược phát triển kinh tế số. Luật không chỉ xác định dữ liệu là đối tượng quản lý mà còn là tài nguyên và tài sản, cần huy động và phát triển có kiểm soát; đồng thời áp dụng cho cả cơ quan, tổ chức, cá nhân trong và ngoài lãnh thổ Việt Nam nếu có hoạt động liên quan.



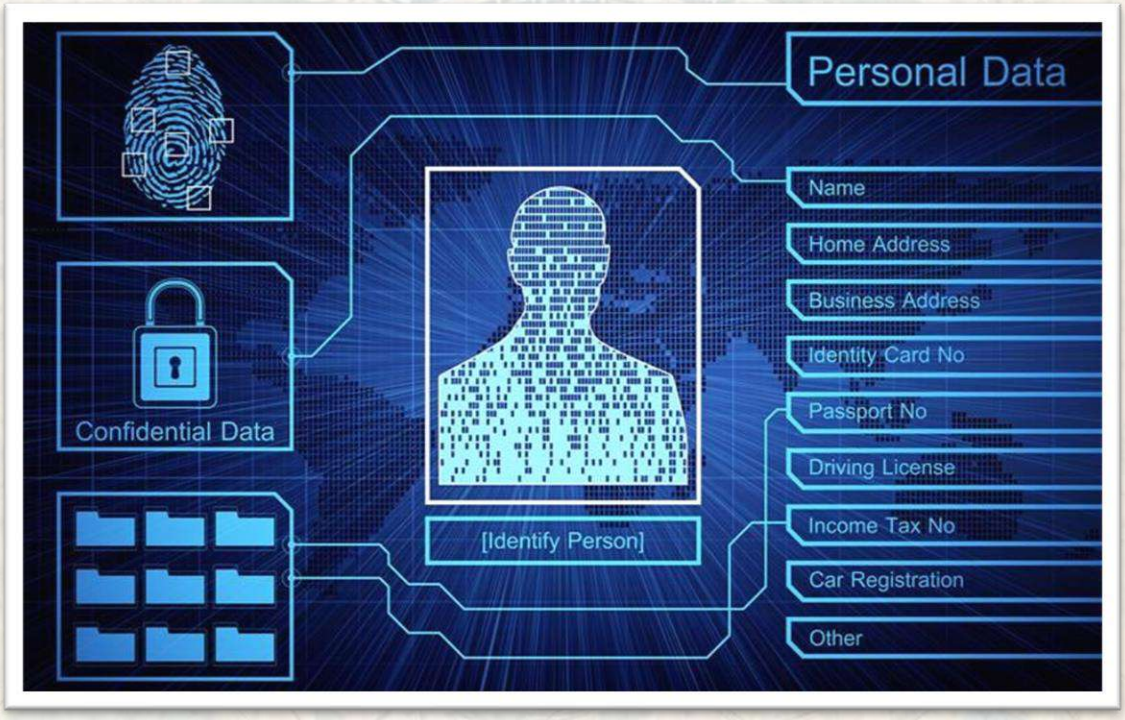
Dữ liệu vừa là động lực, vừa là mục tiêu của phát triển kinh tế số - Ảnh: Báo Điện tử Chính phủ

Điều này tạo ra một cấu trúc quản trị dữ liệu *"nhiều lớp đan xen"*, trong đó, dữ liệu mở nuôi dưỡng hệ sinh thái số; dữ liệu dùng chung tối ưu hóa hoạt động nhà nước; dữ liệu dùng riêng bảo vệ bí mật cơ quan, tổ chức; dữ liệu gốc bảo đảm tính xác thực và khả năng truy nguyên; còn dữ liệu quan trọng và cốt lõi đóng vai trò *"vành đai an ninh"* cao nhất. Tất cả được vận hành trong một cơ chế thống nhất về nghĩa vụ phân loại, bảo đảm chất lượng và lưu trữ an toàn, nhằm vừa thúc đẩy phát triển kinh tế số vừa bảo vệ an ninh, chủ quyền dữ liệu quốc gia.

2.1.2. Chủ thể dữ liệu

- Về khái niệm

Chủ thể dữ liệu (data subject) là thuật ngữ chỉ đối tượng mà một tập dữ liệu phản ánh. Theo Khoản 12 Điều 3 Luật dữ liệu 2024 quy định: *"Chủ thể dữ liệu là cơ quan, tổ chức, cá nhân được dữ liệu phản ánh"*. Nói cách khác, bất kỳ ai hoặc thực thể nào mà thông tin trong dữ liệu đề cập đến đều là chủ thể của dữ liệu đó. Ví dụ, một công dân có thông tin trong Cơ sở dữ liệu quốc gia về dân cư là chủ thể dữ liệu cá nhân; một doanh nghiệp có hồ sơ kinh doanh trong Cơ sở dữ liệu đăng ký doanh nghiệp là chủ thể dữ liệu tổ chức.



Cá nhân là tổng hòa của nhiều trường thông tin-Ảnh: thuvienphapluat.vn

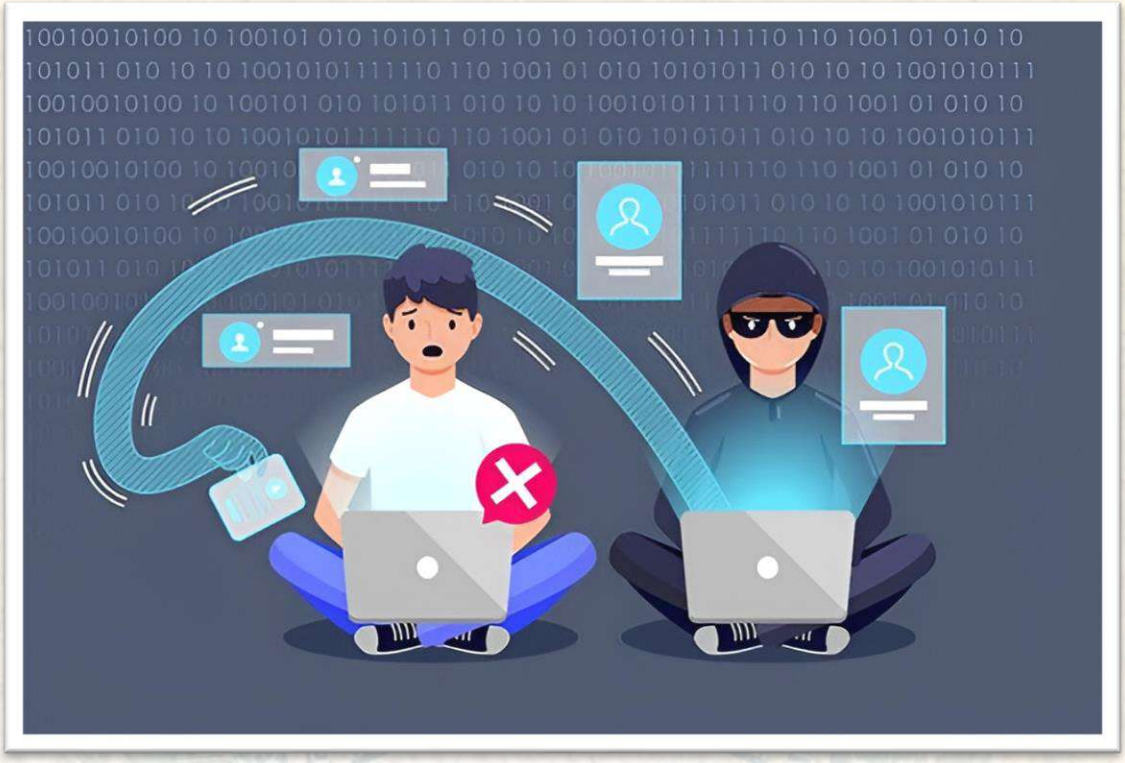
So với pháp luật hiện hành, khái niệm này tương đồng với Khoản 6 Điều 2 Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, trong đó định nghĩa *"chủ thể dữ liệu cá nhân là cá nhân mà dữ liệu cá nhân đó phản ánh"* (hoặc Khoản 5 Điều 2 Luật Bảo vệ dữ liệu cá nhân 2025 khi văn bản này có hiệu lực). Luật An toàn thông tin mạng 2015 cũng tiếp cận gần gũi khi quy

định *"thông tin cá nhân là thông tin gắn với việc xác định danh tính của một người cụ thể"* (Khoản 15, Điều 3). Tuy nhiên, điểm mới của Luật Dữ liệu 2024 là phạm vi bao quát rộng hơn, không chỉ giới hạn ở dữ liệu cá nhân, mà còn bao gồm dữ liệu của tổ chức, doanh nghiệp, và cơ quan nhà nước. Điều này thể hiện sự thích ứng của pháp luật Việt Nam với thực tiễn quản trị dữ liệu trong nền kinh tế số, nơi dữ liệu tổ chức và dữ liệu công có giá trị chiến lược không kém dữ liệu cá nhân.

Có thể khẳng định rằng, chủ thể dữ liệu tương ứng với cá nhân mà dữ liệu cá nhân đó gắn liền. Chẳng hạn, dữ liệu về tên, tuổi, số căn cước công dân của một người thì người đó là chủ thể dữ liệu tương ứng. Lưu ý rằng Luật Dữ liệu mở rộng khái niệm này bao gồm cả tổ chức, cơ quan. Ví dụ, doanh nghiệp cũng có thể là chủ thể dữ liệu nếu dữ liệu đề cập đến doanh nghiệp đó (như dữ liệu đăng ký kinh doanh của công ty A thì công ty A là chủ thể dữ liệu). Tuy nhiên, phổ biến nhất, thuật ngữ chủ thể dữ liệu được dùng trong bối cảnh dữ liệu cá nhân, khi nói về cá nhân có thông tin liên quan. Như vậy, phạm vi chủ thể dữ liệu rất rộng, tương ứng với sự phong phú của dữ liệu trong xã hội.

Tuy nhiên, cần phân biệt rõ chủ thể dữ liệu không đồng nghĩa với chủ sở hữu dữ liệu. Chủ thể dữ liệu là người hay tổ chức mà dữ liệu đề cập, còn chủ sở hữu dữ liệu là cá nhân hoặc tổ chức nắm quyền sở hữu, quyết định đối với dữ liệu. Ví dụ, một khách hàng A có dữ liệu cá nhân do công ty B thu thập. Khách hàng A là chủ thể của dữ liệu cá nhân đó, nhưng chủ sở hữu dữ liệu lại là công ty B - là bên thu thập và quản lý dữ liệu. Điều này dẫn tới việc chủ thể dữ liệu (A) có quyền nhân thân liên quan đến dữ liệu (như quyền riêng tư, quyền yêu cầu xóa dữ liệu cá nhân của mình), trong khi công ty B có quyền tài sản đối với dữ liệu và quyết định việc sử dụng nó. Sự tách bạch

khái niệm này giúp xác định đúng chủ thể của các quyền và nghĩa vụ pháp lý trong quản trị dữ liệu.



Các hacker luôn tìm cách thu thập trái phép dữ liệu của người dùng - Ảnh: Tạp chí điện tử luật sư Việt Nam

- Về đặc điểm

Trên cơ sở nghiên cứu các quy định pháp luật về dữ liệu và thực tiễn triển khai các quy định này, có thể xác định một số đặc điểm của chủ thể dữ liệu như sau:

Thứ nhất, chủ thể dữ liệu luôn gắn liền trực tiếp với thông tin mà dữ liệu phản ánh hoặc dữ liệu đó liên quan đến quyền và lợi ích hợp pháp của họ. Mối quan hệ này tồn tại bất kể dữ liệu được lưu trữ hoặc xử lý ở đâu, trong hay ngoài lãnh thổ Việt Nam (Luật Dữ liệu, 2024, Điều 3; GDPR, Điều 4).

Thứ hai, chủ thể dữ liệu có quyền kiểm soát và quyết định đối với dữ liệu của mình. Quyền này bao gồm quyền được biết, truy cập, chỉnh sửa, hạn

chế xử lý, phản đối xử lý, yêu cầu xóa dữ liệu và yêu cầu bồi thường thiệt hại khi quyền bị xâm phạm. Những quyền này được quy định cụ thể tại các điều của Luật Dữ liệu 2024, tương đồng với các quyền được bảo vệ trong Nghị định 13/2023/NĐ-CP (Điều 9 - 16) và GDPR (Điều 12 - 22), cho thấy Việt Nam đang tiệm cận các chuẩn mực quốc tế về bảo vệ dữ liệu cá nhân và tổ chức.

Thứ ba, bên cạnh quyền, chủ thể dữ liệu có nghĩa vụ cung cấp thông tin trung thực, chính xác, đầy đủ khi pháp luật yêu cầu. Đồng thời không lợi dụng quyền của mình để cản trở hoạt động hợp pháp của tổ chức hoặc cơ quan quản lý dữ liệu. Chẳng hạn, khi thực hiện thủ tục hành chính trực tuyến, cá nhân phải đảm bảo thông tin kê khai là đúng sự thật; việc cố ý cung cấp sai sự thật có thể bị xử phạt hành chính theo Nghị định 144/2021/NĐ-CP.

Thứ tư, chủ thể dữ liệu không nhất thiết phải trực tiếp nắm giữ hay quản lý dữ liệu của mình. Trong nhiều trường hợp, dữ liệu được lưu trữ bởi bên kiểm soát dữ liệu (data controller) hoặc bên xử lý dữ liệu (data processor), nhưng chủ thể dữ liệu vẫn giữ quyền pháp lý đối với dữ liệu đó. Ví dụ, hồ sơ bệnh án điện tử được bệnh viện quản lý nhưng bệnh nhân có quyền yêu cầu trích xuất bản sao hoặc giới hạn việc chia sẻ với bên thứ ba [141].

Thứ năm, phạm vi quyền của chủ thể dữ liệu phụ thuộc vào loại dữ liệu và quy định pháp luật áp dụng. Đối với dữ liệu cá nhân thông thường, quyền truy cập, sửa đổi hoặc xóa thường rộng hơn; trong khi đối với dữ liệu nhạy cảm hoặc dữ liệu thuộc bí mật nhà nước, quyền bị giới hạn nghiêm ngặt và kèm yêu cầu bảo vệ ở mức cao hơn, chẳng hạn như mã hóa hoặc kiểm soát truy cập[192].

[192] GDPR, Art. 9.

Thứ sáu, chủ thể dữ liệu được pháp luật bảo vệ bất kể quốc tịch hoặc vị trí lưu trữ dữ liệu. Luật Dữ liệu 2024 áp dụng đối với dữ liệu liên quan đến công dân và tổ chức Việt Nam kể cả khi dữ liệu được xử lý ở nước ngoài, phản ánh nguyên tắc tác động ngoài lãnh thổ tương tự GDPR (Điều 3). Điều này đặc biệt quan trọng trong bối cảnh dữ liệu xuyên biên giới ngày càng phổ biến, giúp bảo đảm quyền và lợi ích hợp pháp của chủ thể dữ liệu trước các hành vi xâm phạm từ bên ngoài lãnh thổ Việt Nam.



Không gian mạng có tính quốc tế cao, đòi hỏi phải có cơ chế kiểm soát - Ảnh: Forbes

- Về phân loại

+ ***Căn cứu vào loại dữ liệu,*** chủ thể dữ liệu bao gồm: ***(i)*** Cá nhân, mọi công dân đều là chủ thể dữ liệu của các thông tin cá nhân họ (hồ sơ hộ tịch, dữ liệu y tế, thông tin tài khoản ngân hàng của một người đều có người đó là chủ thể dữ liệu). Như đã đề cập, dữ liệu cá nhân theo GDPR là "bất kỳ thông tin nào liên quan đến hoặc cho phép xác định một cá nhân cụ thể". Vì vậy, chủ thể dữ liệu cá nhân chính là cá nhân mà từ dữ liệu có thể nhận dạng được họ; ***(ii)*** Pháp nhân, tổ chức là chủ thể dữ liệu nếu pháp nhân, tổ chức

đó có dữ liệu phản ánh hoạt động kinh doanh, tài chính, nghiên cứu phát triển hoặc các bí mật thương mại. Ví dụ, một doanh nghiệp X là chủ thể dữ liệu trong cơ sở dữ liệu đăng ký doanh nghiệp quốc gia (các thông tin về doanh nghiệp X như mã số thuế, ngành nghề, vốn điều lệ… phản ánh chính doanh nghiệp đó); ***(iii)*** Cơ quan nhà nước, bản thân các cơ quan này cũng có dữ liệu phản ánh hoạt động của mình (ví dụ dữ liệu thống kê về một Ủy ban nhân dân tỉnh Y, thì Ủy ban nhân dân Y là chủ thể của dữ liệu ấy).

+ ***Căn cứ vào mức độ nhạy cảm của dữ liệu***, chủ thể dữ liệu bao gồm: Chủ thể dữ liệu thông thường, dữ liệu không chứa thông tin nhạy cảm, chủ yếu phục vụ các mục đích thương mại hoặc dịch vụ; Chủ thể dữ liệu nhạy cảm của dữ liệu liên quan đến bí mật cá nhân, sức khỏe, tài chính, tôn giáo, chính trị, hoặc dữ liệu an ninh quốc gia.

+ ***Căn cứ vào nguồn gốc***, chủ thể dữ liệu bao gồm: *Chủ thể dữ liệu gốc,* là nơi dữ liệu phát sinh lần đầu; *Chủ thể dữ liệu thứ cấp* do dữ liệu phát sinh gián tiếp thông qua phân tích, tổng hợp, hoặc từ nguồn dữ liệu khác. Ví dụ: Một khách hàng mua hàng online là chủ thể dữ liệu gốc (thông tin cá nhân, lịch sử mua hàng), còn hồ sơ phân tích hành vi mua sắm là dữ liệu thứ cấp gắn với họ.

2.1.3. Chủ sở hữu dữ liệu

- Về khái niệm

Chủ sở hữu dữ liệu (data owner) là chủ thể có quyền sở hữu đối với dữ liệu, có thể hiểu là người hoặc tổ chức chiếm hữu và định đoạt dữ liệu như một loại tài sản của mình. Khoản 14 Điều 3 Luật dữ liệu 2024 quy định: *"Chủ sở hữu dữ liệu là cơ quan, tổ chức, cá nhân có quyền quyết định việc xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng và trao đổi giá trị của dữ liệu do mình sở hữu".* Như vậy, định nghĩa này xác định rõ

chủ sở hữu dữ liệu là chủ thể có quyền chiếm hữu, sử dụng và định đoạt dữ liệu như một loại tài sản, đồng thời nắm quyền kiểm soát cao nhất trong toàn bộ vòng đời dữ liệu, từ khâu tạo lập, thu thập, đến khai thác, chia sẻ và mua bán.

Chủ sở hữu dữ liệu tương ứng với bên nắm quyền kiểm soát cao nhất đối với dữ liệu. Họ chính là người đầu tư nguồn lực để thu thập hoặc tạo ra dữ liệu, do đó pháp luật công nhận dữ liệu thuộc quyền sở hữu của họ. Chủ sở hữu quyết định mục đích và phương thức xử lý dữ liệu, đồng thời chịu trách nhiệm sau cùng về dữ liệu đó. Chủ sở hữu dữ liệu có thể là cá nhân, ví dụ một nhiếp ảnh gia chụp ảnh thì người đó là chủ sở hữu dữ liệu ảnh chụp của mình (trừ trường hợp có thỏa thuận khác). Thường gặp hơn, chủ sở hữu dữ liệu là tổ chức, doanh nghiệp, chẳng hạn công ty cung cấp dịch vụ trực tuyến sở hữu toàn bộ dữ liệu người dùng mà công ty thu thập được trên nền tảng của họ. Trong khu vực công, các cơ quan nhà nước tạo lập cơ sở dữ liệu (như Bộ Tài chính với cơ sở dữ liệu thuế, Bộ Y tế với cơ sở dữ liệu tiêm chủng) đóng vai trò chủ sở hữu đối với những dữ liệu đó nhân danh Nhà nước.

Theo Luật Dữ liệu, quyền của chủ sở hữu dữ liệu đối với dữ liệu được bảo hộ như quyền tài sản. Chủ sở hữu dữ liệu có quyền chiếm hữu, sử dụng, định đoạt dữ liệu tương tự như quyền sở hữu tài sản hữu hình. Đây là điểm mới quan trọng: luật pháp số hóa tài sản hóa dữ liệu, cho phép chủ sở hữu dữ liệu được pháp luật bảo vệ quyền lợi và cho phép khai thác giá trị kinh tế từ dữ liệu. Tất nhiên, quyền sở hữu dữ liệu cũng có những giới hạn nhất định nhằm bảo vệ lợi ích công và quyền của chủ thể dữ liệu.

Một số chủ sở hữu dữ liệu điển hình như: ***(i)*** Doanh nghiệp công nghệ, Công ty vận hành mạng xã hội là chủ sở hữu kho dữ liệu người dùng trên

nền tảng đó. ***(ii)*** Cơ quan nhà nước, doanh nghiệp nhà nước, Chính phủ (thông qua các bộ ngành) là chủ sở hữu các cơ sở dữ liệu quốc gia, vì dữ liệu được hình thành từ ngân sách nhà nước và phục vụ quản lý nhà nước. ***(iii)*** Cá nhân: Một tác giả viết sách và lưu bản thảo điện tử, người đó có thể xem là chủ sở hữu dữ liệu bản thảo đó. Trong thực tiễn, cá nhân thường ít được nhắc đến như chủ sở hữu dữ liệu (trừ phi dữ liệu có giá trị thương mại như bộ sưu tập ảnh, tác phẩm số…); còn lại đa số dữ liệu cá nhân do người khác thu thập thì cá nhân chỉ đóng vai trò chủ thể dữ liệu chứ không sở hữu theo nghĩa pháp lý.



Số lượng doanh nghiệp công nghệ số Việt Nam liên tục phát triển, tăng lên trong thời gian qua - Ảnh: VnEconomy

Về quan hệ giữa chủ sở hữu dữ liệu và chủ quản dữ liệu, chủ sở hữu dữ liệu có thể trực tiếp quản trị dữ liệu của mình hoặc ủy quyền cho chủ quản dữ liệu. Trong mọi trường hợp, chủ sở hữu giữ quyền quyết định tối

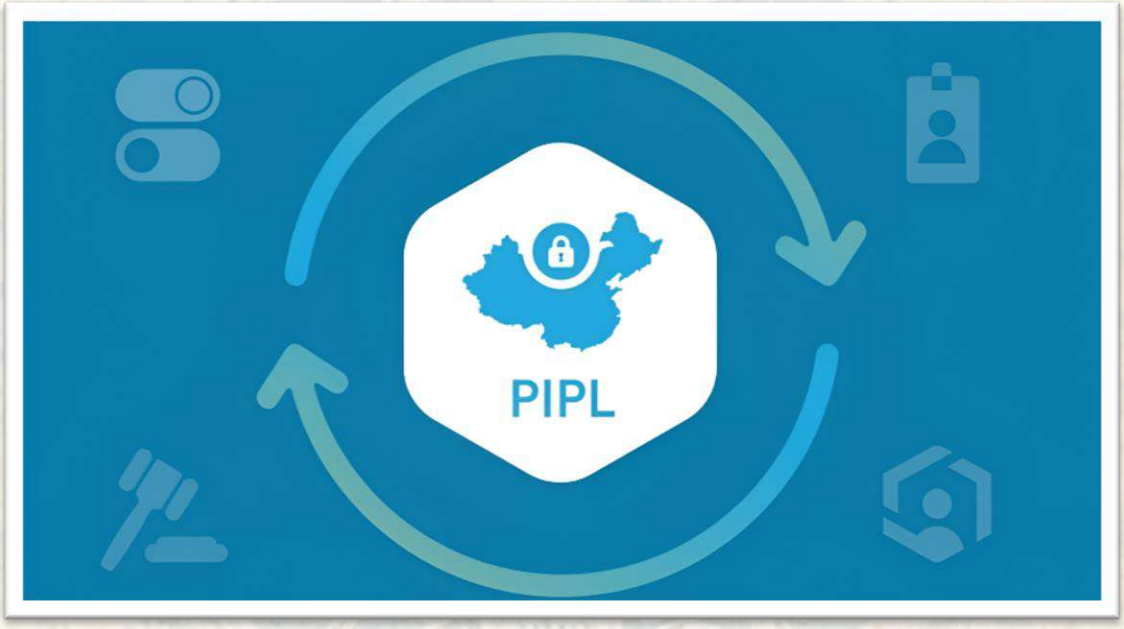
thượng. Chủ quản chỉ được hành động trong phạm vi và mục đích mà chủ sở hữu cho phép. Ví dụ, nếu chủ sở hữu (doanh nghiệp) chỉ đạo chủ quản phải xóa một tập dữ liệu, chủ quản có nghĩa vụ tuân thủ. Sự phân định này giúp tạo ra chế độ trách nhiệm: chủ sở hữu chịu trách nhiệm về định hướng và mục đích sử dụng dữ liệu, còn chủ quản chịu trách nhiệm về vận hành và tuân thủ kỹ thuật.

- Về đặc điểm

+ ***Có quyền kiểm soát tối cao đối với dữ liệu.*** Chủ sở hữu dữ liệu nắm giữ quyền quyết định cao nhất về mục đích, phương thức và phạm vi xử lý dữ liệu. Quyền này bao gồm việc xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng và trao đổi giá trị dữ liệu. Trong bối cảnh Luật Dữ liệu 2024, quyền kiểm soát này được bảo hộ như quyền sở hữu tài sản (Điều 7, Điều 14), đồng nghĩa với việc chủ sở hữu có thể định đoạt dữ liệu thông qua mua bán, chuyển nhượng, cấp phép hoặc cho thuê. Ở EU, quyền này tương đồng với vai trò data controller trong GDPR (Khoản 7 Điều 4), tuy nhiên tại Việt Nam khái niệm *"chủ sở hữu"* nhấn mạnh hơn đến yếu tố quyền tài sản, thay vì chỉ quản lý mục đích và phương thức xử lý.

+ ***Gắn liền với nghĩa vụ bảo vệ và tuân thủ pháp luật.*** Bên cạnh quyền lợi, chủ sở hữu dữ liệu có trách nhiệm bảo đảm việc xử lý dữ liệu tuân thủ quy định pháp luật, bao gồm các nguyên tắc bảo vệ dữ liệu cá nhân, an ninh mạng, và các quy định chuyên ngành. Chẳng hạn, doanh nghiệp thương mại điện tử là chủ sở hữu dữ liệu giao dịch phải tuân thủ Nghị định 52/2013/NĐ-CP về thương mại điện tử, Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, và các điều khoản của Luật An toàn thông tin mạng 2015. Điều này tương tự các nghĩa vụ mà GDPR đặt ra cho chủ sở hữu dữ liệu, như thực hiện biện pháp kỹ thuật và tổ chức phù hợp (Điều 24).

+ ***Phạm vi quyền sở hữu có giới hạn.*** Quyền sở hữu dữ liệu không phải là quyền tuyệt đối, mà bị giới hạn bởi lợi ích công cộng, quyền của chủ thể dữ liệu, và quy định bảo mật nhà nước. Ví dụ, một doanh nghiệp sở hữu dữ liệu cá nhân khách hàng nhưng không thể tùy ý công khai hoặc bán dữ liệu này nếu chưa được sự đồng ý của chủ thể dữ liệu (Điều 12 Luật Dữ liệu 2024; Điều 11 Nghị định 13/2023/NĐ-CP). Tại Trung Quốc, PIPL (2021) cũng áp đặt giới hạn tương tự, đặc biệt nghiêm ngặt với dữ liệu nhạy cảm và dữ liệu quan trọng liên quan đến an ninh quốc gia.



Đạo luật PIPL của chính phủ Trung Quốc có ảnh hưởng nhất định đến quá trình hoàn thiện luật dữ liệu của nhiều nước trên thế giới - Ảnh: PIPL

+ ***Tính đa dạng.*** Chủ sở hữu dữ liệu có thể là cá nhân, tổ chức tư nhân, hoặc cơ quan nhà nước. Cá nhân thường là chủ sở hữu khi chính họ tạo ra dữ liệu có giá trị kinh tế (ví dụ: tác phẩm số, ảnh nghệ thuật), trong khi tổ chức, doanh nghiệp thường đóng vai trò chủ sở hữu các tập dữ liệu lớn thu thập từ hoạt động kinh doanh. Cơ quan nhà nước sở hữu cơ sở dữ liệu công, dữ liệu quốc gia, hoặc dữ liệu hình thành từ ngân sách nhà nước. Trong nhiều

trường hợp, Nhà nước vừa là chủ sở hữu vừa là cơ quan quản lý dữ liệu, như đối với cơ sở dữ liệu dân cư hoặc dữ liệu về an ninh, quốc phòng.

+ ***Có thể trực tiếp quản lý hoặc ủy quyền.*** Chủ sở hữu dữ liệu có thể trực tiếp quản trị dữ liệu hoặc ủy quyền cho bên thứ ba (chủ quản dữ liệu) thực hiện nhiệm vụ lưu trữ, bảo mật và vận hành. Tuy nhiên, việc ủy quyền này không làm mất quyền kiểm soát pháp lý của chủ sở hữu, và mọi hành động của bên được ủy quyền phải nằm trong phạm vi cho phép.

+ ***Là bên chịu trách nhiệm pháp lý cuối cùng.*** Dù có thể ủy quyền, chủ sở hữu dữ liệu vẫn là bên chịu trách nhiệm pháp lý sau cùng khi xảy ra vi phạm hoặc sự cố liên quan đến dữ liệu. Trách nhiệm này bao gồm cả xử lý vi phạm hành chính (theo Nghị định 144/2021/NĐ-CP, Nghị định 15/2020/NĐ-CP) và bồi thường thiệt hại dân sự (theo Bộ luật Dân sự 2015). Đây là điểm quan trọng để bảo đảm tính minh bạch và tránh *"khoảng trống trách nhiệm"* trong quản lý dữ liệu.

Việc coi dữ liệu là tài sản và quy định cụ thể chủ sở hữu dữ liệu trong Luật dữ liệu 2024 nhìn chung có ưu điểm và nhược điểm. *Về ưu điểm*, việc quy định rõ ràng như trên góp phần xác lập rõ quyền tài sản: Khác với nhiều quốc gia (như EU trong GDPR hay Singapore trong PDPA) chỉ sử dụng khái niệm "data controller" (bên kiểm soát dữ liệu) và không chính thức coi dữ liệu là tài sản, Luật Dữ liệu 2024 của Việt Nam định nghĩa rõ "chủ sở hữu dữ liệu" và bảo hộ quyền này như quyền tài sản. Điều này tạo cơ sở pháp lý vững chắc cho các giao dịch thương mại dữ liệu, bao gồm mua bán, chuyển nhượng, thế chấp hoặc cho thuê dữ liệu (Điều 14, Luật Dữ liệu 2024). Bên cạnh đó, khi quyền sở hữu dữ liệu được pháp luật công nhận, các cá nhân, tổ chức và doanh nghiệp có động lực đầu tư vào thu thập, phân tích và phát triển dữ liệu, vì họ biết rằng giá trị kinh tế được tạo ra sẽ được bảo hộ và

khai thác hợp pháp [98], từ đó, tạo động lực kinh tế cho khai thác dữ liệu. Ngoài ra, việc xác định rõ *"chủ sở hữu dữ liệu"* giúp cơ quan quản lý và tòa án dễ dàng xác định ai là bên chịu trách nhiệm khi xảy ra tranh chấp, vi phạm hoặc sự cố liên quan đến dữ liệu. Điều này giảm nguy cơ "vùng xám" pháp lý về quyền và nghĩa vụ giữa các bên tham gia xử lý dữ liệu.



Tranh biếm họa về quyền riêng tư trong bảo đảm an ninh quốc gia - Ảnh: Tạp chí Quản lý Nhà nước

Về hệ quả pháp lý, việc chính thức coi dữ liệu là một loại tài sản vô hình trong Luật Dữ liệu 2024 kéo theo những tác động pháp lý sâu rộng. Trước hết phải thấy rằng, nó mở rộng phạm vi giao dịch dân sự khi dữ liệu có thể được định giá, mua bán, chuyển nhượng hoặc thế chấp tương tự các loại tài sản trí tuệ khác. Điều này đòi hỏi Nhà nước phải xây dựng một khung pháp lý bổ sung bao gồm các tiêu chuẩn định giá dữ liệu, mẫu hợp đồng dữ liệu, cơ chế đăng ký quyền sở hữu, và quy trình giải quyết tranh chấp phát sinh từ giao

dịch dữ liệu. Việc này cũng đặt ra câu hỏi về năng lực của cơ quan quản lý và cơ chế chứng minh quyền sở hữu trong các vụ kiện liên quan đến dữ liệu.



Dữ liệu là tài nguyên quốc gia, tài sản cá nhân - Ảnh: Báo Điện tử Chính phủ

Bên cạnh đó, việc tài sản hóa dữ liệu tác động trực tiếp đến cơ chế bảo vệ quyền của chủ thể dữ liệu. Khi dữ liệu cá nhân trở thành tài sản thuộc quyền sở hữu của một bên (thường là doanh nghiệp hoặc tổ chức), pháp luật buộc phải duy trì sự cân bằng giữa quyền tài sản của chủ sở hữu và quyền nhân thân của chủ thể dữ liệu. Các quyền như đồng ý, quyền truy cập, quyền xóa dữ liệu, quyền phản đối xử lý... vốn đã được quy định trong Nghị định 13/2023/NĐ-CP và Luật Dữ liệu 2024 cần được thực thi nghiêm ngặt để tránh xung đột lợi ích, đặc biệt trong các tình huống chủ sở hữu muốn khai thác dữ liệu thương mại mà không có sự đồng thuận đầy đủ của chủ thể dữ liệu.

Ngoài ra, việc coi dữ liệu là tài sản kéo theo yêu cầu minh bạch và kiểm toán dữ liệu. Tương tự như tài sản hữu hình hoặc quyền sở hữu trí tuệ, dữ

liệu cần được ghi nhận, định giá và báo cáo trong sổ sách kế toán của doanh nghiệp. Điều này mở đường cho việc áp dụng các chuẩn mực kế toán - kiểm toán chuyên biệt cho dữ liệu, bao gồm đánh giá rủi ro mất giá trị dữ liệu, hao mòn dữ liệu theo thời gian, hoặc tổn thất do rò rỉ. Một số quốc gia, như Singapore, đã triển khai thí điểm mô hình báo cáo giá trị dữ liệu trong báo cáo tài chính[193], cho thấy xu hướng này có thể trở thành tiêu chuẩn quốc tế.

2.1.4. Chủ quản dữ liệu

Chủ quản dữ liệu (data administrator) là khái niệm mới được Luật Dữ liệu 2024 giới thiệu để chỉ chủ thể thực hiện việc quản lý vận hành dữ liệu theo ủy quyền của chủ sở hữu. *Về mặt pháp lý*, Khoản 13 Điều 3 Luật dữ liệu 2024 quy định: *"Chủ quản dữ liệu là cơ quan, tổ chức, cá nhân thực hiện hoạt động xây dựng, quản lý, vận hành, khai thác dữ liệu theo yêu cầu của chủ sở hữu dữ liệu". Về bản chất*, chủ quản dữ liệu là bên được giao phụ trách việc tạo lập và duy trì dữ liệu thay cho chủ sở hữu.

Chủ quản dữ liệu thường có quyền kiểm soát trực tiếp dữ liệu về mặt kỹ thuật, nhưng phải tuân theo các chỉ đạo, mục đích do chủ sở hữu dữ liệu đặt ra. Chủ quản có thể chính là một đơn vị nội bộ của chủ sở hữu hoặc một bên độc lập được thuê (dịch vụ dữ liệu). Ví dụ, một doanh nghiệp (chủ sở hữu dữ liệu) có thể giao cho bộ phận công nghệ thông tin của mình làm chủ quản dữ liệu nội bộ; hoặc thuê một công ty dịch vụ cloud quản trị cơ sở dữ liệu khách hàng, công ty này sẽ đóng vai trò chủ quản dữ liệu, chịu trách nhiệm vận hành cơ sở dữ liệu theo hợp đồng với doanh nghiệp. Trong khu vực nhà nước, cơ quan chủ quản thường được nói đến khi một cơ quan được giao quản lý một cơ sở dữ liệu nào đó. Chẳng hạn, Bộ Công an được giao làm chủ quản Cơ sở dữ liệu quốc gia về dân cư; Bộ Tư pháp làm chủ quản

[193] Infocomm Media Development Authority, 2021.

cơ sở dữ liệu về Hộ tịch điện tử… Chủ quản dữ liệu có thể đồng thời chính là chủ sở hữu (nếu tự mình vận hành dữ liệu của mình), hoặc có thể tách biệt khi chủ sở hữu thuê ngoài.



Khái niệm về chủ quản dữ liệu chỉ vừa được giới thiệu tại luật Dữ liệu - Ảnh: Bizfly Cloud

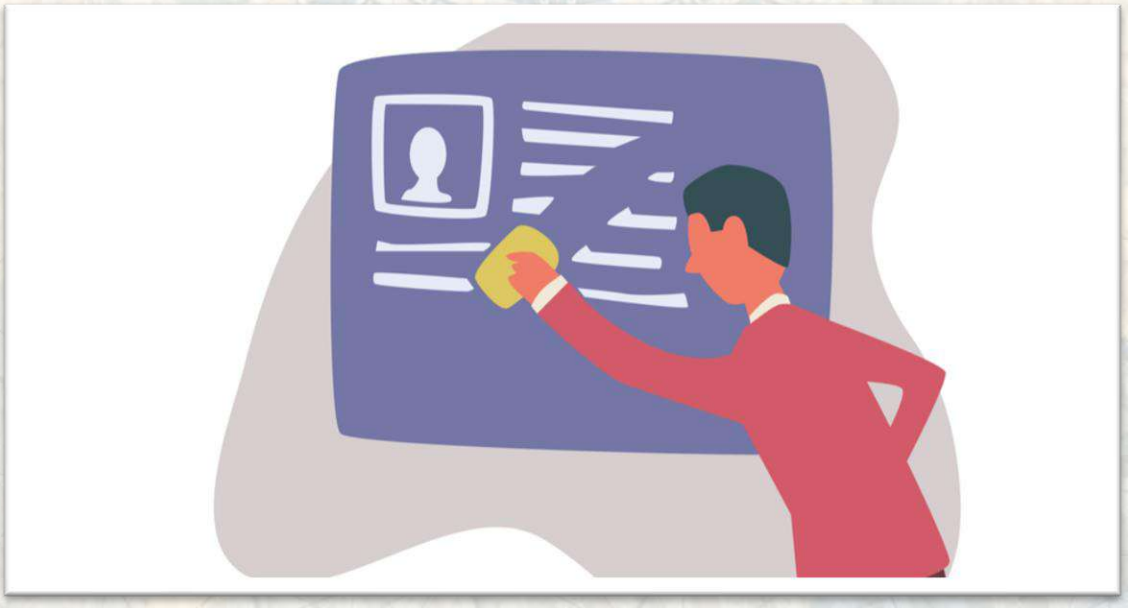
Có thể kể đến một số đơn vị chủ quản dữ liệu cụ thể: ***(i)*** Đơn vị chuyên trách công nghệ thông tin: Nhiều bộ, ngành có cục hoặc tổng cục phụ trách đến công nghệ thông tin hoặc trung tâm dữ liệu đóng vai trò chủ quản kỹ thuật cho các hệ thống thông tin của ngành. ***(ii)*** Doanh nghiệp cung cấp dịch vụ dữ liệu: các công ty cho thuê hạ tầng lưu trữ, dịch vụ điện toán đám mây có thể làm chủ quản dữ liệu cho nhiều khách hàng. ***(iii)*** Đơn vị sự nghiệp hoặc công ty con: Một số tập đoàn lớn lập công ty con chuyên quản trị dữ liệu tập đoàn; hoặc các cơ quan hành chính lập đơn vị sự nghiệp phụ trách vận hành cơ sở dữ liệu dùng chung.

2.2. QUYỀN, NGHĨA VỤ VÀ TRÁCH NHIỆM CỦA CHỦ THỂ DỮ LIỆU, CHỦ SỞ HỮU DỮ LIỆU, CHỦ QUẢN DỮ LIỆU

2.2.1. Quyền, nghĩa vụ và trách nhiệm của chủ thể dữ liệu

2.2.1.1. Về quyền của chủ thể dữ liệu

Theo Luật Dữ liệu 2024, nguyên tắc chung là việc sử dụng dữ liệu phải được sự đồng ý của chủ thể dữ liệu, trừ trường hợp luật có quy định đặc biệt. Chủ thể dữ liệu có quyền *đồng ý* hoặc *từ chối* cho người khác thu thập, chia sẻ dữ liệu của mình trong điều kiện bình thường. Ngoài ra, Luật Dữ liệu (Điều 26) ghi nhận quyền của chủ thể dữ liệu *yêu cầu xóa dữ liệu*. Cụ thể, chủ thể dữ liệu có quyền yêu cầu chủ sở hữu, chủ quản dữ liệu thu hồi, xóa hoặc hủy dữ liệu của mình đã cung cấp (trừ trường hợp pháp luật có quy định khác). Chủ quản dữ liệu phải thiết lập quy trình và biện pháp để thực hiện yêu cầu này một cách kịp thời. Quy định này tương tự *"quyền được quên"* trong hệ thống pháp luật về dữ liệu ở châu Âu, cho phép cá nhân chủ thể dữ liệu chủ động bảo vệ quyền riêng tư của mình.



Quyền được quên lần đầu được nghi nhận trong một bộ luật cụ thể - Ảnh: iPleaders

Riêng trong lĩnh vực bảo vệ dữ liệu cá nhân, Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 (được luật hóa tại Điều 4 Luật bảo vệ dữ liệu cá nhân năm 2025) đã liệt kê 11 quyền cụ thể của chủ thể dữ liệu cá nhân[194], bao gồm:

+ ***Quyền được biết:*** Cá nhân có quyền được thông báo về loại dữ liệu cá nhân đang được xử lý, mục đích xử lý, danh tính hoặc thông tin liên hệ của bên xử lý dữ liệu, cũng như các bên thứ ba có thể nhận dữ liệu. Quyền này giúp bảo đảm nguyên tắc minh bạch trong xử lý dữ liệu và ngăn chặn việc thu thập, sử dụng dữ liệu một cách bí mật hoặc trái phép.

+ ***Quyền đồng ý:*** Chủ thể dữ liệu có quyền quyết định cho phép hoặc không cho phép người khác thu thập, xử lý dữ liệu của mình, trừ một số trường hợp ngoại lệ được pháp luật quy định bao gồm: ứng phó với tình trạng khẩn cấp; khi có nguy cơ đe dọa an ninh quốc gia nhưng chưa đến mức ban bố tình trạng khẩn cấp; Có thảm họa và phòng, chống bạo loạn, khủng bố (Điều 18 Luật Dữ liệu năm 2024). Quyền này gắn liền với nguyên tắc *tự nguyện, cụ thể và có thông tin đầy đủ* trong pháp luật về dữ liệu, tức là sự đồng ý phải được đưa ra một cách tự nguyện, chủ thể biết rõ nội dung, mục đích của việc đồng ý và sự đồng ý được cụ thể hóa thành văn bản hoặc các định dạng khác có thể kiểm chứng được. Xuất phát từ vai trò pháp lý quan trọng của sự đồng ý, Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân đã có quy định chi tiết đối với thuật ngữ này:

"Điều 11. Sự đồng ý của chủ thể dữ liệu

1. Sự đồng ý của chủ thể dữ liệu được áp dụng đối với tất cả các hoạt động trong quy trình xử lý dữ liệu cá nhân, trừ trường hợp luật có quy định khác.

---

[194] An ninh Hải Phòng (2023), *Nghị định 13/2023/NĐ-CP: 11 quyền, 5 nghĩa vụ của chủ thể dữ liệu*, https://anhp.vn/nghi-dinh-132023nd-cp-11-quyen-5-nghia-vu-cua-chu-the-du-lieu-d55151.html, Truy cập ngày 10/8/2025.

2. Sự đồng ý của chủ thể dữ liệu chỉ có hiệu lực khi chủ thể dữ liệu tự nguyện và biết rõ các nội dung sau:

a) Loại dữ liệu cá nhân được xử lý;

b) Mục đích xử lý dữ liệu cá nhân;

c) Tổ chức, cá nhân được xử lý dữ liệu cá nhân;

d) Các quyền, nghĩa vụ của chủ thể dữ liệu.

3. Sự đồng ý của chủ thể dữ liệu phải được thể hiện rõ ràng, cụ thể bằng văn bản, giọng nói, đánh dấu vào ô đồng ý, cú pháp đồng ý qua tin nhắn, chọn các thiết lập kỹ thuật đồng ý hoặc qua một hành động khác thể hiện được điều này.

4. Sự đồng ý phải được tiến hành cho cùng một mục đích. Khi có nhiều mục đích, Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân liệt kê các mục đích để chủ thể dữ liệu đồng ý với một hoặc nhiều mục đích nêu ra.

5. Sự đồng ý của chủ thể dữ liệu phải được thể hiện ở một định dạng có thể được in, sao chép bằng văn bản, bao gồm cả dưới dạng điện tử hoặc định dạng kiểm chứng được.

6. Sự im lặng hoặc không phản hồi của chủ thể dữ liệu không được coi là sự đồng ý.

7. Chủ thể dữ liệu có thể đồng ý một phần hoặc với điều kiện kèm theo.

8. Đối với xử lý dữ liệu cá nhân nhạy cảm, chủ thể dữ liệu phải được thông báo rằng dữ liệu cần xử lý là dữ liệu cá nhân nhạy cảm.

9. Sự đồng ý của chủ thể dữ liệu có hiệu lực cho tới khi chủ thể dữ liệu có quyết định khác hoặc khi cơ quan nhà nước có thẩm quyền yêu cầu bằng văn bản.

10. Trong trường hợp có tranh chấp, trách nhiệm chứng minh sự đồng ý của chủ thể dữ liệu thuộc về Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân.

11. Thông qua việc ủy quyền theo quy định của Bộ luật Dân sự, tổ chức, cá nhân có thể thay mặt chủ thể dữ liệu thực hiện các thủ tục liên quan tới xử lý dữ liệu cá nhân của chủ thể dữ liệu với Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân trong trường hợp chủ thể dữ liệu đã biết rõ và đồng ý theo quy định tại khoản 3 Điều này, trừ trường hợp luật có quy định khác."



Quyền truy cập dữ liệu cá nhân và quyền chỉnh sửa dữ liệu giúp cho quyền con người được đảm bảo - Ảnh: CyberPilot

+ ***Quyền truy cập:*** Cá nhân có quyền yêu cầu truy cập dữ liệu cá nhân của mình để xem, kiểm tra và yêu cầu chỉnh sửa nếu dữ liệu không chính xác hoặc không đầy đủ. Quyền này giúp duy trì tính toàn vẹn và tính chính xác của dữ liệu. Về điều kiện, cá nhân, tổ chức phải gửi yêu cầu hợp lệ, xác minh danh tính để tránh tiết lộ dữ liệu cho người không có quyền. Trong một số trường hợp, quyền này có thể bị từ chối cung cấp nếu việc truy cập gây

nguy hiểm đến an ninh quốc gia, tiết lộ bí mật thương mại, hoặc xâm phạm quyền và lợi ích hợp pháp của người khác.

+ ***Quyền rút lại sự đồng ý:*** Ngay cả khi đã cho phép xử lý dữ liệu, chủ thể dữ liệu vẫn có quyền rút lại sự đồng ý bất kỳ lúc nào. Cơ chế rút lại phải dễ dàng và thuận tiện như lúc đồng ý, bảo đảm cá nhân luôn kiểm soát dữ liệu của mình. Đồng thời, Luật Bảo vệ dữ cá nhân cũng đã có quy định rõ ràng đối với quyền này của chủ thể dữ liệu, cụ thể:

"Điều 12. Rút lại sự đồng ý

1. Việc rút lại sự đồng ý không ảnh hưởng đến tính hợp pháp của việc xử lý dữ liệu đã được đồng ý trước khi rút lại sự đồng ý.

2. Việc rút lại sự đồng ý phải được thể hiện ở một định dạng có thể được in, sao chép bằng văn bản, bao gồm cả dưới dạng điện tử hoặc định dạng kiểm chứng được.

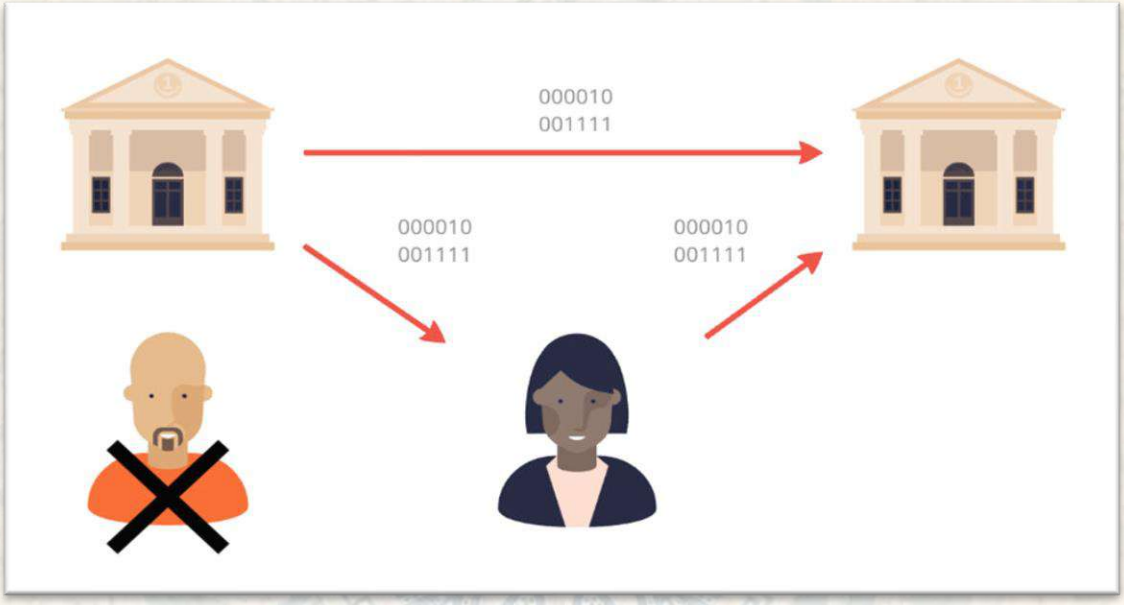
3. Khi nhận yêu cầu rút lại sự đồng ý của chủ thể dữ liệu, Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân thông báo cho chủ thể dữ liệu về hậu quả, thiệt hại có thể xảy ra khi rút lại sự đồng ý.

4. Sau khi thực hiện quy định tại khoản 2 Điều này, Bên Kiểm soát dữ liệu, Bên Xử lý dữ liệu, Bên Kiểm soát và xử lý dữ liệu, Bên thứ ba phải ngừng và yêu cầu các tổ chức, cá nhân có liên quan ngừng xử lý dữ liệu của chủ thể dữ liệu đã rút lại sự đồng ý".

+ ***Quyền xóa dữ liệu:*** Chủ thể dữ liệu có thể yêu cầu xóa bỏ dữ liệu cá nhân của mình khi dữ liệu không còn cần thiết cho mục đích đã thu thập, hoặc khi rút lại sự đồng ý. Đây là một biện pháp bảo vệ quyền riêng tư quan trọng, đặc biệt trong môi trường số nơi dữ liệu dễ bị lưu trữ và chia sẻ không giới hạn.

+ ***Quyền hạn chế xử lý:*** Khi cá nhân muốn tạm dừng hoặc giới hạn một số mục đích xử lý, cá nhân có thể yêu cầu giới hạn phạm vi hoặc mục đích

xử lý dữ liệu của mình, ví dụ không sử dụng cho quảng cáo hoặc phân tích hồ sơ tiêu dùng. Điều này đảm bảo dữ liệu chỉ được xử lý theo mục đích đã thỏa thuận. Tuy nhiên, cần xác định rõ phạm vi hạn chế; bên xử lý phải tuân thủ và chỉ xử lý trong giới hạn mới. Quyền này cũng không áp dụng nếu việc hạn chế trái với yêu cầu của pháp luật hoặc nghĩa vụ hợp đồng hợp pháp mà chủ thể đã tham gia.

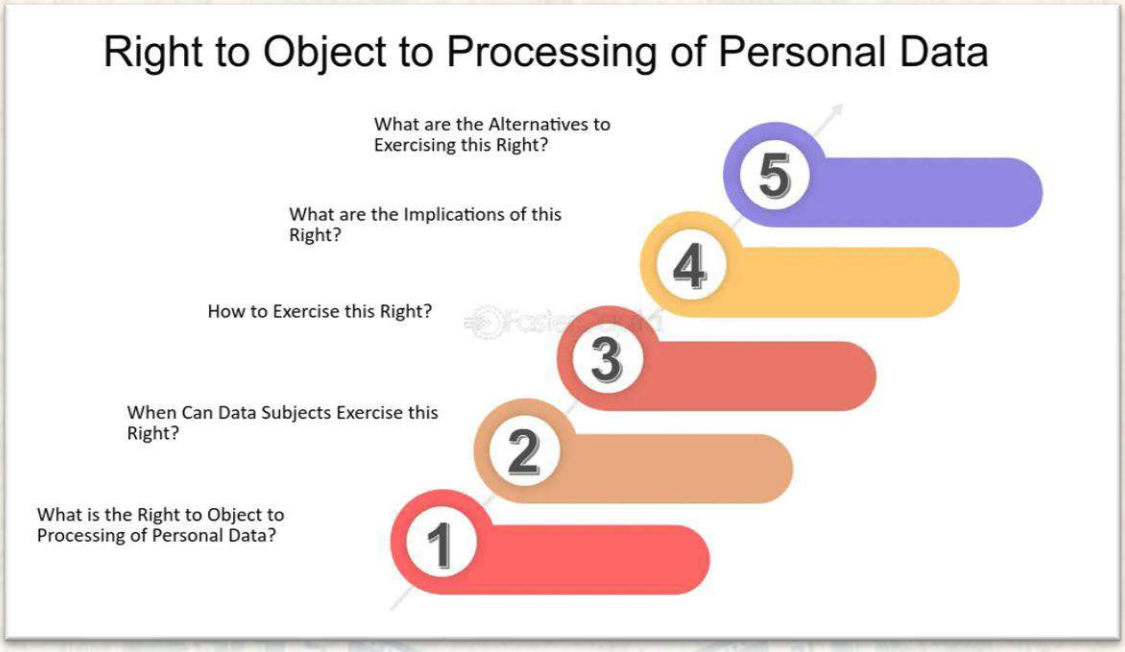


Minh họa về quyền cung cấp dữ liệu - Ảnh: Michalsons

+ ***Quyền cung cấp dữ liệu:*** Khi chủ thể dữ liệu muốn nhận một bản sao dữ liệu của mình hoặc chuyển dữ liệu sang nhà cung cấp dịch vụ khác, chủ thể dữ liệu có quyền yêu cầu bên kiểm soát dữ liệu cung cấp cho mình một bản sao dữ liệu cá nhân ở định dạng có thể đọc bằng máy và dễ dàng chuyển sang một bên khác. Quyền này thúc đẩy tính cạnh tranh và khả năng di chuyển dữ liệu giữa các dịch vụ. Tuy nhiên, quyền này không áp dụng với dữ liệu phát sinh từ hoạt động nội bộ hoặc dữ liệu có yếu tố bí mật thương mại không thể tách riêng.

+ ***Quyền phản đối việc xử lý dữ liệu:*** Cá nhân có quyền phản đối việc xử lý dữ liệu nếu việc đó gây ảnh hưởng đến quyền và lợi ích hợp pháp của

họ. Cá nhân, tổ chức có thể gửi yêu cầu phản đối kèm lý do hợp pháp, khi đó, bên xử lý phải chấm dứt trừ khi chứng minh được lý do chính đáng hoặc nghĩa vụ pháp lý vì lợi ích cộng đồng để tiếp tục xử lý.



Quyền phản đối việc xử lý dữ liệu theo dẫn giải của các luật dữ liệu của các quốc gia khác - Ảnh: FasterCapital

+ ***Quyền khiếu nại, tố cáo, khởi kiện:*** Chủ thể dữ liệu có quyền khiếu nại đến cơ quan có thẩm quyền, tố cáo hành vi vi phạm hoặc khởi kiện ra tòa để bảo vệ quyền lợi. Việc khiếu nại, tố cáo được thực hiện theo trình tự thủ tục khiếu nại, tố cáo, khởi kiện theo Luật Khiếu nại, Luật Tố cáo, Bộ luật Tố tụng dân sự. Đây là cơ chế thực thi quyền trong thực tế, gắn với hệ thống giải quyết tranh chấp và xử phạt vi phạm hành chính. Tuy nhiên, phải đảm bảo không lạm dụng quyền này để gây khó khăn hoặc cản trở hoạt động hợp pháp của bên xử lý dữ liệu.

+ ***Quyền yêu cầu bồi thường:*** Nếu bị thiệt hại vật chất hoặc tinh thần do vi phạm quy định bảo vệ dữ liệu cá nhân, chủ thể dữ liệu có quyền yêu cầu bồi thường theo quy định của pháp luật dân sự và pháp luật chuyên

ngành. Mức bồi thường lúc này phụ thuộc vào quy định của pháp luật dân sự và chứng cứ do chủ thể cung cấp.

+ ***Quyền yêu cầu bảo vệ:*** Khi cá nhân muốn chủ động bảo vệ dữ liệu của mình trước nguy cơ xâm phạm, họ có thể chủ động áp dụng các biện pháp hợp pháp để bảo vệ dữ liệu của mình (như mã hóa, thiết lập quyền truy cập, kiểm soát chia sẻ), đồng thời yêu cầu cơ quan chức năng can thiệp khi quyền bị xâm phạm sao cho không xâm phạm quyền và lợi ích của người khác.



Các đại biểu Quốc hội bấm nút biểu quyết thông qua Luật Dữ liệu ngày 30/11/2024 - Ảnh: Báo Điện tử Chính phủ

Các quyền trên tạo thành một chế định toàn diện về quyền chủ thể dữ liệu, đảm bảo cá nhân kiểm soát thông tin thuộc đời tư của mình một cách chủ động. Chẳng hạn, theo Nghị định 13, công dân Việt Nam có quyền tương tự công dân EU theo GDPR và Đạo Luật Dữ liệu châu Âu, đó là biết ai đang nắm dữ liệu của mình, tiếp cận, đính chính, xóa dữ liệu, phản đối xử lý vì mục đích marketing... Việc luật hóa các quyền này đánh dấu bước

tiến lớn trong việc bảo vệ quyền riêng tư và quyền tự quyết thông tin cá nhân ở Việt Nam.

Mặc khác, trên phương diện dữ liệu nói chung, Luật dữ liệu 2024 đã thiết lập cho chủ thể dữ liệu các quyền cơ bản sau:

+ Quyền được khai thác và sử dụng dữ liệu của chính mình

Quyền này được quy định cụ thể tại điểm b khoản 3 điều 35, đó là *"Chủ thể dữ liệu được khai thác và sử dụng dữ liệu phản ánh về chủ thể dữ liệu đó"*. Đây là quyền truy cập thông tin cơ bản, cho phép chủ thể dữ liệu biết được thông tin gì đang được lưu trữ về mình trong các hệ thống dữ liệu của nhà nước. Luật xác định một trong các chủ thể được khai thác và sử dụng Cơ sở dữ liệu tổng hợp quốc gia là chủ thể dữ liệu. Đồng thời, khi chủ thể dữ liệu khai thác dữ liệu của chính mình trong Cơ sở dữ liệu tổng hợp quốc gia và các cơ sở dữ liệu khác do cơ quan nhà nước quản lý thì không phải nộp phí. Quyền này đảm bảo tính minh bạch, cho phép cá nhân và tổ chức kiểm tra, đối chiếu thông tin mà nhà nước đang lưu giữ về mình. Đây là bước đầu tiên và cần thiết để có thể thực hiện các quyền khác như yêu cầu sửa đổi nếu thông tin có sai sót.

+ Quyền yêu cầu thu hồi, xóa, hoặc hủy dữ liệu

Tương tự như quyền xóa dữ liệu đã nêu, quyền này trao cho chủ thể dữ hiệu quyền năng kiểm soát đối với dữ hiệu của mình sau khi đã cung cấp, tương tự như "quyền được lãng quên" trong các quy định quốc tế. Điểm mới là Luật Dữ liệu 2024 đã mở rộng đối tượng điều chỉnh cho cả các tổ chức, pháp nhân khác về quyền này, không còn mặc định ở cá nhân. Điều này cho thấy sự tiến bộ và toàn diện của luật pháp Việt Nam trong việc bảo vệ dữ liệu, không chỉ dừng lại ở quyền của con người mà còn cả quyền của các thực thể pháp lý khác.



Quyền yêu cầu thu hồi, xóa hoặc hủy dữ liệu là đột phá trong bảo đảm quyền riêng tư - Ảnh: Internet

Tại khoản 1 Điều 20 Luật Dữ liệu quy định: *"Chủ thể dữ liệu có quyền yêu cầu chủ sở hữu dữ liệu, chủ quản dữ liệu thu hồi, xóa hoặc hủy dữ liệu của mình đã cung cấp, trừ trường hợp pháp luật có quy định khác"*. Để bảo đảm quyền này, Luật cũng yêu cầu *"chủ quản dữ liệu có trách nhiệm thiết lập quy trình, triển khai các biện pháp, phương thức thu hồi, xóa hoặc hủy dữ liệu theo yêu cầu của chủ thể dữ liệu"*. Chủ thể dữ liệu có thể thực thi quyền này khi họ rút lại sự đồng ý hoặc khi mục đích xử lý dữ liệu ban đầu đã không còn nữa. Tuy nhiên, quyền này không phải là tuyệt đối và bị giới hạn bởi vế "trừ trường hợp pháp luật có quy định khác", cho thấy các nghĩa vụ pháp lý khác (như lưu trữ chứng từ, dữ liệu phục vụ công tác quản lý nhà nước, phục vụ công tác bảo đảm an ninh, trật tự…) có thể được ưu tiên.

Có thể thấy rằng, quy định về quyền yêu cầu thu hồi, xóa hoặc hủy dữ liệu của chủ thể dữ liệu trong Luật Dữ liệu Việt Nam được xem là một bước tiến quan trọng, phản ánh sự đồng bộ với các chuẩn mực quốc tế về bảo vệ dữ liệu.

Về tiềm năng, quy định này trước hết thể hiện sự tăng cường quyền kiểm soát của người dùng đối với dữ liệu của chính họ. Bằng cách trao quyền cho chủ thể dữ liệu được yêu cầu xóa bỏ thông tin đã cung cấp, Luật Dữ liệu đã tạo ra một cơ chế bảo vệ quyền riêng tư hiệu quả. Điều này không chỉ giúp người dùng an tâm hơn khi tham gia vào các hoạt động trực tuyến, mà còn xây dựng nền tảng niềm tin vững chắc giữa người dùng và các tổ chức, doanh nghiệp.

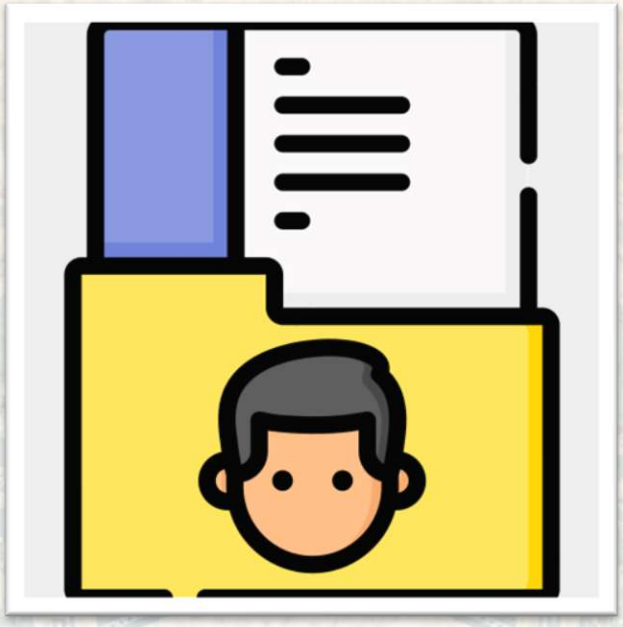
Từ góc độ của doanh nghiệp, quy định này thúc đẩy trách nhiệm và tính chuyên nghiệp. Các tổ chức phải chủ động đầu tư vào việc xây dựng hệ thống và quy trình quản lý dữ liệu an toàn, minh bạch hơn để hạn chế việc người dùng thu hồi dữ liệu đã cung cấp. Việc này không chỉ nâng cao tiêu chuẩn bảo mật, mà còn là một lợi thế cạnh tranh, giúp doanh nghiệp xây dựng hình ảnh đáng tin cậy trong mắt khách hàng và đối tác. Khi niềm tin được củng cố, người dùng sẽ sẵn sàng tham gia vào các giao dịch và tương tác số, từ đó hỗ trợ sự phát triển bền vững của nền kinh tế số.

+ Quyền đồng ý (cho phép) xử lý, chia sẻ và giao dịch dữ liệu

Như đã phân tích ở trên, không chỉ đối với chủ thể dữ liệu là cá nhân, mà đối với cả các tổ chức, đây là quyền cốt lõi, đặt chủ thể dữ liệu vào vị trí trung tâm, quyết định việc thông tín của mình có được phổ biến hay thương mại hóa hay không.

Trong khai thác dữ liệu, Luật Dữ liệu quy định rõ để khai thác dữ liệu cá nhân trong Cơ sở dữ liệu tổng hợp quốc gia, một tổ chức, cá nhân khác phải có "sự đồng ý của Trung tâm dữ liệu quốc gia và cá nhân là chủ thể dữ liệu được khai thác" (điểm c khoản 3 Điều 15 Luật Dữ liệu). Điều này tạo nên một cơ chế bảo vệ kép, đảm bảo rằng dữ liệu cá nhân không thể bị khai thác một cách tùy tiện. Quyền này trao cho mỗi cá nhân khả năng kiểm soát việc thông tin của họ có được sử dụng cho mục đích nào, bởi ai, từ đó củng cố niềm tin

vào hệ thống quản lý dữ liệu quốc gia. Việc yêu cầu phải có sự đồng ý của Trung tâm dữ liệu quốc gia cho thấy pháp luật giới hạn sự khai thác đối với dữ liệu cá nhân không được vượt quá giới hạn cho phép gây phương hại đến an ninh quốc gia như để phục vụ tình báo, gián điệp, phá hoại.



Cần có nhận thức đúng đắn hơn về vị trí, vai trò của dữ liệu - Ảnh: Flaticon

Trong giao dịch dữ liệu, Luật nghiêm cấm giao dịch trên sàn dữ liệu đối với "Dữ liệu không được chủ thể dữ liệu đồng ý, trừ trường hợp pháp luật có quy định khác" (điểm b khoản 3 Điều 42 Luật Dữ liệu). Quy định này đóng vai trò then chốt trong việc bảo vệ dữ liệu cá nhân, nó tạo thành một hàng rào pháp lý quan trọng để chống lại việc mua bán, trao đổi dữ liệu cá nhân trái phép. Điều đó khẳng định rằng giá trị thương mại của dữ liệu không thể được đặt cao hơn quyền tự quyết của chủ thể dữ liệu. Dù vậy, quyền này cũng có các ngoại lệ, đặc biệt là trong các trường hợp cung cấp dữ liệu cho cơ quan nhà nước vì lý do an ninh, khẩn cấp mà không cần sự đồng ý. Những ngoại lệ này phản ánh sự cân bằng giữa quyền riêng tư của cá nhân và nhu cầu an ninh, trật tự xã hội. Tuy nhiên, việc áp dụng các ngoại lệ này cần được thực hiện một cách thận trọng và có sự giám sát chặt chẽ để tránh lạm dụng,

đảm bảo rằng quyền tự quyết của người dân không bị xâm phạm một cách không cần thiết. Đồng thời cũng xác lập nguyên tắc minh bạch, yêu cầu mọi giao dịch dữ liệu phải được hợp pháp hóa. Quan trọng nhất, quy định này đề cao quyền tự quyết của chủ thể dữ liệu, khẳng định rằng giá trị thương mại không thể cao hơn quyền của người sở hữu thông tin.

Tóm lại, quy định về quyền đồng ý là một trụ cột quan trọng trong Luật Dữ liệu Việt Nam, là sự mở rộng khái niệm đồng ý của cá nhân trong các văn bản trước, thể hiện sự tiến bộ trong việc bảo vệ quyền riêng tư và thúc đẩy một môi trường số an toàn. Quy định này không chỉ tạo ra một hàng rào pháp lý mạnh mẽ chống lại việc lạm dụng dữ liệu mà còn đóng vai trò then chốt trong việc xây dựng một nền kinh tế dữ liệu bền vững, nơi niềm tin của người dùng được đặt lên hàng đầu.

+ Quyền được bảo vệ và được thông báo trong các trường hợp đặc biệt

Quy định này thể hiện một cách tiếp cận toàn diện và nhân văn của pháp luật Việt Nam, cho thấy Nhà nước ý thức sâu sắc rằng việc thu thập dữ liệu vì mục đích công không đồng nghĩa với việc có thể tùy tiện xâm phạm quyền riêng tư của cá nhân. Ngay cả khi quyền đồng ý bị giới hạn vì lý do an ninh quốc gia, pháp luật vẫn quy định các biện pháp bảo vệ lợi ích của chủ thể dữ liệu do yêu cầu bắt buộc, theo đó, cơ quan nhà nước có trách nhiệm "bảo đảm an ninh, an toàn dữ liệu, bảo vệ dữ liệu, lợi ích hợp pháp khác của chủ thể dữ liệu" (điểm b khoản 3 Điều 18). Đây là một nguyên tắc bảo vệ mang tính bắt buộc. Mặc dù dữ liệu có thể được thu thập mà không cần sự đồng ý, các cơ quan chức năng vẫn phải tuân thủ các quy tắc bảo mật nghiêm ngặt. Họ không được phép sử dụng dữ liệu cho mục đích khác ngoài mục đích đã yêu cầu, và phải đảm bảo dữ liệu không bị rò rỉ hoặc lạm dụng. Điều này giúp giảm thiểu rủi ro và tác động tiêu cực đến đời sống của chủ thể dữ liệu, dù họ không có quyền từ chối cung cấp thông tin.



Những "quy định vàng" trong các văn bản luật quốc tế về dữ liệu - Ảnh: Caring For Care

Mặt khác, cơ quan nhà nước phải "hủy dữ liệu ngay khi dữ liệu đó không còn cần thiết cho mục đích đã yêu cầu và thông báo cho chủ thể dữ liệu, tổ chức, cá nhân đã cung cấp dữ liệu" (điểm c khoản 3 Điều 18 Luật Dữ liệu). Quy định này thiết lập một cơ chế kiểm soát chặt chẽ, ngăn chặn việc lưu trữ dữ liệu tùy tiện hoặc vô thời hạn. Việc thông báo sau khi dữ liệu được hủy còn thể hiện sự tôn trọng đối với quyền của chủ thể, cho họ biết rằng thông tin của mình đã được xử lý đúng quy trình và không còn bị lưu giữ. Điều này củng cố lòng tin của người dân vào sự minh bạch của các cơ quan nhà nước.

Nhìn chung, các quy định trên thể hiện sự cân bằng trong chính sách của Nhà nước. Dù ưu tiên cho an ninh quốc gia trong các tình huống cấp bách. Luật vẫn yêu cầu các cơ quan chức năng phải có trách nhiệm bảo vệ và giảm thiểu tác động đến chủ thể dữ liệu, cũng như quản lý dữ liệu chặt chẽ trong thời gian lưu trữ.

Ngoài ra, chủ quản dữ liệu có trách nhiệm xác định rủi ro và thực hiện các biện pháp để bảo vệ dữ liệu; kịp thời khắc phục rủi ro phát sinh và thông

báo cho chủ thể dữ liệu (khoản 3 Điều 25 Luật Dữ liệu). Việc chủ động thông báo sự cố cho chủ thể dữ liệu biết có ý nghĩa rất lớn trong việc bảo vệ người dùng khỏi các sự cố rò rỉ dữ liệu. Khi một sự cố xảy ra, chủ thể dữ liệu sẽ được thông báo kịp thời để có thể tự bảo vệ mình, thay vì phải chờ đợi hoặc tự phát hiện.

2.2.1.2. Nghĩa vụ của chủ thể dữ liệu

Cùng với các quyền, Nghị định 13/2023/NĐ-CP hay gần nhất là Luật Bảo vệ dữ liệu cá nhân năm 2025 cũng đặt ra 5 nghĩa vụ, trách nhiệm của chủ thể dữ liệu cá nhân. Đó là: ***(1)*** Tự bảo vệ dữ liệu cá nhân của mình và yêu cầu các bên liên quan cùng bảo vệ. Xuất phát từ nguyên tắc tự định đoạt và tự chịu trách nhiệm đối với dữ liệu cá nhân; ***(2)*** Tôn trọng dữ liệu cá nhân của người khác (không xâm phạm quyền riêng tư của người khác); ***(3)*** Cung cấp đầy đủ, chính xác dữ liệu cá nhân của mình khi đồng ý cho xử lý (nghĩa là không được cố ý cung cấp sai thông tin); ***(4)*** Tham gia tuyên truyền, phổ biến kỹ năng bảo vệ dữ liệu cá nhân trong cộng đồng; ***(5)*** Tuân thủ pháp luật về bảo vệ dữ liệu cá nhân, chủ động phòng chống các hành vi vi phạm.



Đi đôi với quyền, các chủ thể dữ liệu cũng cần thực hiện nghĩa vụ của mình - Ảnh: Data Privacy Manager

Từ các nghĩa vụ trên, có thể cụ thể hóa các nghĩa vụ của của chủ thể dữ liệu bao gồm cả cá nhân, tổ chức trong Luật dữ liệu 2024 như sau:

+ Nghĩa vụ cung cấp dữ liệu chính xác và không được làm sai lệch dữ liệu.

Xuất phát từ việc cố ý cung cấp thông tin sai lệch gây ra những hậu quả, hệ lụy nghiêm trọng, ảnh hưởng trên nhiều phương diện, mọi mặt của đời sống xã hội, như ***(i)*** trực tiếp làm giảm chất lượng của các cơ sở dữ liệu quốc gia. Khi dữ liệu đầu vào không chính xác, các phân tích thống kê và mô hình dự báo sẽ trở nên thiếu tin cậy, dẫn đến những quyết sách quản lý không hiệu quả. Điều này có thể gây ra những tổn thất không nhỏ cho cả nền kinh tế và xã hội. ***(ii)*** Hành vi này có thể ảnh hưởng trực tiếp đến quyền lợi của chính chủ thể dữ liệu. Dữ liệu cá nhân là yếu tố quan trọng trong nhiều giao dịch và thủ tục hành chính. Khi một người khai sai thông tin của mình, họ có thể gặp phải những rắc rối pháp lý, bị từ chối trong các giao dịch, hoặc thậm chí mất đi những quyền lợi hợp pháp trong các lĩnh vực như an sinh xã hội, tài chính, hay y tế. Do đó, đây là nghĩa vụ cơ bản và quan trọng nhất, bảo đảm tính toàn vẹn và đúng đắn của các cơ sở dữ liệu quốc gia.

Về khung pháp lý, có thể xác định nghĩa vụ trên thông qua các quy định như: khoản 4 Điều 10 Luật nghiêm cấm hành vi: "Cố ý cung cấp dữ liệu sai lệch"; khoản 3 Điều 10 Luật cũng nghiêm cấm hành vi: "Giả mạo, cố ý làm sai lệch, làm mất, làm hư hỏng dữ liệu trong cơ sở dữ liệu của cơ quan Đảng, Nhà nước, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội". Vì "chủ thể dữ liệu" là nguồn cung cấp thông tin ban đầu về chính mình, họ có nghĩa vụ phải trung thực và chính xác khi cung cấp dữ liệu cho các cơ quản, tổ chức. Việc cố ý cung cấp thông tin sai lệch không chỉ là hành vi bị cấm mà còn có thể làm ảnh hưởng đến chất lượng của Cơ sở dữ liệu

tổng hợp quốc gia, gây khó khăn cho công tác quản lý nhà nước và ảnh hưởng đến quyền lợi của Chính chủ thể đó trong các giao dịch sau này.

Nhìn chung, nghĩa vụ cung cấp dữ liệu chính xác là một trụ cột của Luật Dữ liệu, thể hiện sự coi trọng của Nhà nước đối với tính toàn vẹn của thông tin. Quy định này không chỉ bảo vệ hệ thống quản lý quốc gia mà còn bảo vệ chính quyền lợi của người dân, khuyến khích mỗi cá nhân và tổ chức có trách nhiệm hơn khi tham gia vào môi trường số.

+ Nghĩa vụ cung cấp dữ liệu khi có yêu cầu của cơ quan có thẩm quyền

Trong một số trường hợp đặc biệt, quyền kiểm soát dữ liệu của chủ thể sẽ phải nhường bước cho các yêu cầu pháp lý nhằm bảo vệ lợi ích công cộng và an ninh quốc gia. Đây là một nguyên tắc cơ bản và cần thiết, thể hiện sự ưu tiên của pháp luật đối với an toàn chung của toàn xã hội.

Về cơ sở pháp lý, tại khoản 4 Điều 10 Luật quy định nghiên cấm hành vi "không cung cấp dữ liệu theo quy định pháp luật". Thêm vào đó, tại khoản 2 Điều 18 Luật quy định các trường hợp tổ chức, cá nhân cung cấp dữ liệu cho cơ quan nhà nước mà không cần sự đồng ý của chủ thể dữ liệu, bao gồm: ***(1)*** Ứng phó với tình trạng khẩn cấp; ***(2)*** Khi có nguy cơ đe dọa an ninh quốc gia nhưng chưa đến mức ban bố tình trạng khẩn cấp; thảm họa; ***(3)*** Phòng, chống bạo loạn, khủng bố.

Mặc dù nghĩa vụ cung cấp trực tiếp trong Điều 18 thuộc về bên đang nắm giữ dữ liệu, điều này tạo ra một cơ sở pháp lý vững chắc buộc dữ liệu của chủ thể phải được chia sẻ trong các tình huống cấp bách. Điều này có nghĩa là chủ thể dữ liệu có nghĩa vụ phải tuân thủ và không được cản trở quá trình cung cấp dữ liệu hợp pháp này khi các điều kiện trên được đáp ứng. Đây là sự thể hiện rõ ràng cho nguyên tắc cân bằng giữa quyền riêng tư cá nhân và nghĩa vụ đối với an ninh, an toàn của cộng đồng và quốc gia. Những

quy định này tạo ra một cơ sở pháp lý vững chắc, cho phép các cơ quan chức năng tiếp cận thông tin cần thiết một cách nhanh chóng và hiệu quả trong các tình huống cấp bách, khi việc trì hoãn có thể gây ra những hậu quả nghiêm trọng.



Xây dựng Luật Dữ liệu là để thắt chặt quản lý dữ liệu cá nhân, đảm bảo an toàn thông tin - Ảnh: Danh Trọng

Quyền riêng tư là một quyền cơ bản, nhưng nó không phải là quyền tuyệt đối. Trong một xã hội, quyền lợi cá nhân phải được đặt trong mối quan hệ với lợi ích chung. Quy định này cho thấy, khi có xung đột, lợi ích của an ninh và an toàn cộng đồng có thể được ưu tiên hơn. Tuy nhiên, như đã phân tích ở phần trước, Luật cũng yêu cầu các cơ quan chức năng phải bảo đảm an toàn dữ liệu và hủy dữ liệu khi không còn cần thiết, thể hiện sự cân bằng và bảo vệ quyền lợi của chủ thể dữ liệu ngay cả trong những trường hợp này.

+ Nghĩa vụ tuân thủ các quy định chung của pháp luật về dữ liệu

Luật Dữ liệu của Việt Nam đã thiết lập một hệ thống các nghĩa vụ cốt lõi, đảm bảo rằng quyền của chủ thể dữ liệu không thể bị lạm dụng để gây hại cho lợi ích chung. Là một "cơ quan, tổ chức, cá nhân" có liên quan đến

hoạt động dữ liệu, chủ thể dữ liệu phải tuân thủ tất cả các hành vi bị nghiêm cấm trong Luật.

Về cơ sở pháp lý, tại khoản 1 Điều 10 Luật quy định nghiêm cấm việc "Lợi dụng việc xử lý dữ liệu... để xâm phạm đến lợi ích quốc gia, dân tộc, quốc phòng, an ninh, trật tự, an toàn xã hội...". khoản 2 Điều 10 Luật cũng nghiêm cấm việc "Cản trở hoặc ngăn chặn trái pháp luật quá trình xử lý dữ liệu, quản trị dữ liệu hoặc tấn công, chiếm đoạt, phá hoại cơ sở dữ liệu...".

Các nghĩa vụ này bảo đảm chủ thể dữ liệu không thể lạm dụng các quyền của mình hoặc sử dụng dữ liệu của chính mình vào các mục đích trái pháp luật. Ví dụ, một cá nhân không thể viện dẫn quyền tự do dữ liệu để xử lý thông tin của mình theo cách gây phương hại đến an ninh quốc gia, hoặc một tổ chức không thể cản trở việc kết nối, chia sẻ dữ liệu hợp pháp mà pháp luật yêu cầu.



Bảo vệ an ninh dữ liệu vì một Việt Nam hùng cường - Ảnh: VnExpress

Các nghĩa vụ của chủ thể dữ liệu được quy định trong Luật Dữ liệu năm 2024 không nhiều nhưng rất cốt lõi, chủ yếu tập trung vào tính trung thực khi cung cấp dữ liệu và trách nhiệm tuân thủ các yêu cầu của pháp luật vì lợi ích chung. Cấu trúc của Luật cho thấy vai trò của chủ thể dữ liệu được định hình chủ yếu là đối tượng được bảo vệ, với các nghĩa vụ chính là bảo đảm sự chính xác của hệ thống và hợp tác với nhà nước khi các vấn đề trọng yếu về an ninh, trật tự xã hội phát sinh.

Những nghĩa vụ này nhấn mạnh rằng chủ thể dữ liệu cũng phải có ý thức trách nhiệm đối với dữ liệu của chính mình và của người khác. Ví dụ, cá nhân không nên cho người khác mượn hoặc sử dụng dữ liệu nhạy cảm của mình vào mục đích phạm pháp; nếu làm vậy có thể bị liên đới trách nhiệm. Trên thực tế đã có trường hợp cá nhân cho mượn thông tin, giấy tờ để người khác thực hiện hành vi vi phạm, hành vi này có thể bị xử lý tùy mức độ. Do đó, pháp luật khuyến cáo mỗi người dân cần chủ động bảo mật thông tin cá nhân, không tùy tiện chia sẻ dữ liệu nhạy cảm và hợp tác với cơ quan chức năng trong bảo vệ dữ liệu.



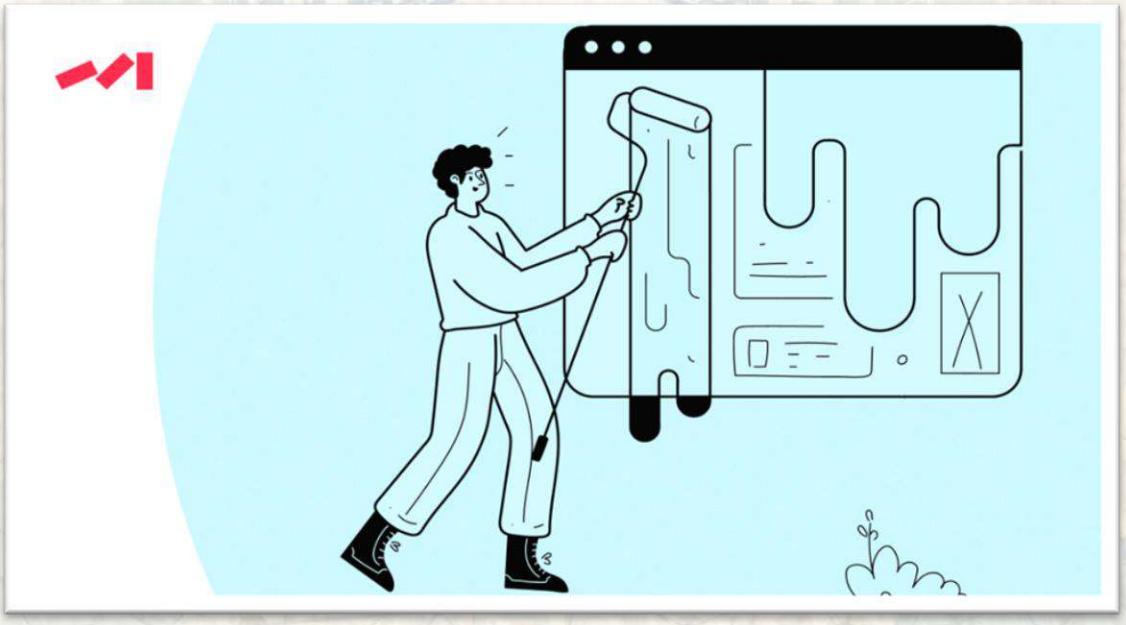
Chủ thể dữ liệu cần phải nắm vững quyền và nghĩa vụ của bản thân - Ảnh: Báo Công an Nhân dân

2.2.2.3. Trách nhiệm của chủ thể dữ liệu

Trong khi Luật dành phần lớn các điều khoản để quy định trách nhiệm của cơ quan nhà nước và các bên quản lý dữ liệu, đồng thời cũng xác lập một số trách nhiệm pháp lý quan trọng đối với chủ thể dữ liệu. Các trách nhiệm này chủ yếu nhằm bảo đảm tính chính xác, toàn vẹn của nguồn tài nguyên dữ liệu quốc gia và sự tuân thủ pháp luật vì lợi ích công cộng và an ninh quốc gia. Cụ thể như sau:

+ Trách nhiệm đối với dữ liệu do mình tạo lập

Đây là trách nhiệm trực tiếp và rõ ràng nhất được quy định trong Luật, nhấn mạnh trách nhiệm giải trình của chủ thể dữ liệu đối với thông tin mà họ cung cấp. Phân tích sâu hơn, quy định này cho thấy một tầm nhìn chiến lược của nhà lập pháp trong việc xây dựng một hệ thống dữ liệu quốc gia toàn vẹn và đáng tin cậy.



Ảnh minh họa - Ảnh: Darwin

Tại điểm a khoản 3 Điều 11 Luật quy định tổ chức, cá nhân (bao gồm chủ thể dữ liệu khi tự tạo lập dữ liệu) có trách nhiệm: *"Chịu trách nhiệm đối với dữ liệu do mình thu thập, tạo lập theo quy định của pháp luật"*. Luật Dữ

liệu đã xác lập một cách rõ ràng và trực tiếp trách nhiệm của tổ chức, cá nhân đối với dữ liệu mà họ thu thập hoặc tự tạo lập. Điều này bao gồm cả chủ thể dữ liệu khi họ khai báo thông tin của chính mình. Quy định này đóng vai trò như một lời khẳng định về nguyên tắc "chịu trách nhiệm về lời nói và hành động" trong môi trường số. Khi một cá nhân đăng ký tài khoản trực tuyến, khi một doanh nghiệp khai báo thông tin để xin giấy phép kinh doanh, hay khi một công dân thực hiện các thủ tục hành chính, họ không chỉ đang cung cấp thông tin mà còn cam kết về tính chính xác của nó. Trách nhiệm này không chỉ là một yêu cầu hình thức, mà còn là cơ sở để xử lý các hành vi gian lận, lừa đảo, hoặc cố ý cung cấp thông tin sai lệch.

Quy định này mang ý nghĩa nền tảng. Khi một cá nhân hoặc một tổ chức, với tư cách là chủ thể dữ liệu, khai báo thông tin để đăng ký dịch vụ, thực hiện thủ tục hành chính, hoặc tạo lập bất kỳ hồ sơ dữ liệu nào về chính mình, họ phải chịu trách nhiệm pháp lý về tính trung thực và chính xác của dữ liệu đó. Trách nhiệm này là cơ sở để xử lý các hành vi cung cấp thông tin sai lệch, bảo đảm chất lượng "đầu vào" cho các cơ sở dữ liệu và duy trì sự tin cậy của cả hệ thống. Không chỉ vậy, khi người dùng và các tổ chức biết rằng mọi dữ liệu được tạo lập đều có trách nhiệm đi kèm, họ sẽ có niềm tin hơn vào toàn bộ hệ thống. Niềm tin này là yếu tố sống còn trong nền kinh tế số, nơi mọi giao dịch và tương tác đều dựa trên dữ liệu.

Trong trường hợp giả định, nếu không có quy định này, hệ thống dữ liệu sẽ dễ bị tổn thương trước các hành vi thiếu trách nhiệm. Một cá nhân có thể khai báo thông tin giả để trốn tránh nghĩa vụ thuế, hoặc một tổ chức có thể cung cấp dữ liệu sai lệch để được hưởng lợi ích không chính đáng. Những hành vi này không chỉ gây thiệt hại cho Nhà nước mà còn ảnh hưởng đến quyền lợi hợp pháp của những người dùng khác, làm suy yếu toàn bộ hệ thống.

Có thể thấy rằng, trách nhiệm đối với dữ liệu do mình tạo lập là một quy định cốt lõi của Luật Dữ liệu Việt Nam. Nó không chỉ là một yêu cầu pháp lý mà còn là nền tảng cho sự minh bạch, trung thực và tin cậy trong môi trường số. Bằng cách đặt trách nhiệm giải trình lên vai mỗi cá nhân và tổ chức, Luật Dữ liệu đã góp phần xây dựng một hệ thống dữ liệu vững mạnh, phục vụ hiệu quả cho công tác quản lý của Nhà nước và bảo vệ lợi ích của toàn xã hội.

+ Trách nhiệm tuân thủ các quy định cấm của pháp luật

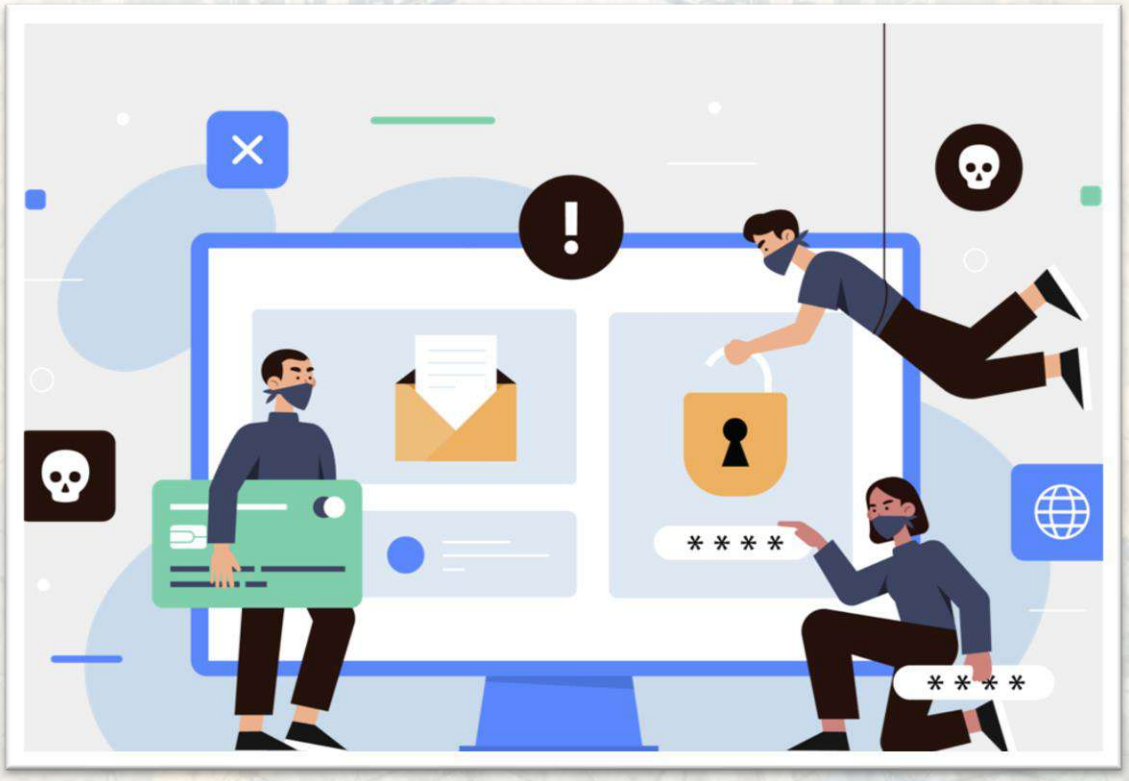
Luật Dữ liệu Việt Nam xác định rằng mọi chủ thể dữ liệu, từ cá nhân đến tổ chức, đều có trách nhiệm không thực hiện các hành vi bị nghiêm cấm được quy định tại Điều 10. Điều này không chỉ giới hạn ở việc bảo vệ quyền riêng tư mà còn mở rộng sang việc bảo đảm tính an toàn và ổn định của toàn bộ hệ sinh thái dữ liệu quốc gia. Từ việc nghiên cứu quy định của pháp luật, có thể khái quát nhóm trách nhiệm này như sau:

Một là, trách nhiệm cung cấp dữ liệu trung thực và tuân thủ yêu cầu pháp luật: khoản 4 Điều 10 Luật quy định nghiêm cấm hành vi "Cố ý cung cấp dữ liệu sai lệch hoặc không cung cấp dữ liệu theo quy định của pháp luật". Trách nhiệm này có 02 nội dung chính, ***(1)*** trách nhiệm không cung cấp thông tin sai sự thật, liên kết trực tiếp với trách nhiệm tại Điều 11 đã phân tích ở trên; ***(2)*** trách nhiệm phải cung cấp dữ liệu khi pháp luật yêu cầu. Điều này có nghĩa là chủ thể dữ liệu không thể từ chối cung cấp thông tin một cách tùy tiện nếu việc cung cấp đó là một nghĩa vụ được quy định trong một văn bản pháp luật khác.

Hai là, trách nhiệm không lạm dụng và phá hoại hệ sinh thái dữ liệu: Luật quy định chủ thể dữ liệu có trách nhiệm không *"Lợi dụng việc xử lý dữ liệu, quản trị dữ liệu, phát triển, kinh doanh, lưu hành sản phẩm, dịch vụ về*

dữ liệu để xâm phạm đến lợi ích quốc gia, dân tộc, quốc phòng, an ninh, trật tự, an toàn xã hội, lợi ích công cộng, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân" (khoản 1 Điều 10) và không *"Cản trở hoặc ngăn chặn trái pháp luật quá trình xử lý dữ liệu, quản trị dữ liệu hoặc tấn công, chiếm đoạt, phá hoại cơ sở dữ liệu, hệ thống thông tin phục vụ quản lý, xử lý, quản trị, bảo vệ dữ liệu"* (khoản 2 Điều 10).

Trách nhiệm này định vị chủ thể dữ liệu như một thành viên có nghĩa vụ giữ gìn sự ổn định của hệ sinh thái dữ liệu chung. Chủ thể dữ liệu không thể nhân danh các quyền của mình để thực hiện các hành vi gây phương hại đến lợi ích công cộng hoặc làm tổn hại đến hạ tầng dữ liệu quốc gia. Điều này một lần nữa thể hiện sự cân bằng giữa quyền lợi cá nhân và trách nhiệm xã hội, đảm bảo rằng việc phát triển và sử dụng dữ liệu luôn đi đôi với việc bảo vệ an ninh và trật tự chung.



Ảnh minh họa - Ảnh: National Privacy Commission

+ Trách nhiệm tuân thủ (một cách gián tiếp) trong các trường hợp liên quan đến an ninh, quốc phòng

Trong một xã hội hiện đại, quyền cá nhân không phải là tuyệt đối mà luôn song hành cùng với trách nhiệm đối với cộng đồng. Luật Dữ liệu Việt Nam đã thể hiện rõ nguyên tắc này, tạo ra một sự cân bằng tinh tế giữa quyền kiểm soát dữ liệu của cá nhân và lợi ích an ninh, quốc phòng của đất nước. Mặc dù chủ thể dữ liệu được trao quyền mạnh mẽ, họ vẫn có trách nhiệm tuân thủ gián tiếp trong các trường hợp đặc biệt, khi lợi ích chung được đặt lên hàng đầu.

Tại khoản 2 Điều 18 Luật quy định cho phép cơ quan có thẩm quyền yêu cầu cung cấp dữ liệu mà không cần chủ thể dữ liệu đồng ý trong các trưởng hợp như "ứng phó với tình trạng khẩn cấp", "khi có nguy cơ đe dọa an ninh quốc gia", "thảm họa", và "phòng, chống bạo loạn, khủng bố". Quy định này không trực tiếp yêu cầu chủ thể dữ liệu phải tự mình cung cấp thông tin, mà đặt ra một nghĩa vụ mang tính chấp nhận và không cản trở.

Mặc dù nghĩa vụ cung cấp trực tiếp thuộc về bên đang nắm giữ dữ liệu, quy định này tạo ra một cơ chế pháp lý mà chủ thể dữ liệu phải chấp nhận (như các doanh nghiệp viễn thông, mạng xã hội, hay các cơ quan chính phủ khác). Trách nhiệm của chủ thể này trong trường hợp này là không cản trở, không chống đối quá trình cung cấp dữ liệu hợp pháp khi các điều kiện an ninh, khẩn cấp được kích hoạt. Đây là sự thể hiện rõ nhất cho nguyên tắc lợi ích quốc gia được đặt lên trên quyền kiểm soát dữ liệu cá nhân trong những tình huống đặc biệt.

Như vậy, các trách nhiệm của chủ thể dữ liệu trong Luật Dữ liệu năm 2024 tuy không nhiều nhưng rất rõ ràng và mang tính cốt lõi; tập trung vào ba điểm chính: ***(1)*** Chịu trách nhiệm về tính chính xác của dữ liệu do mình

tạo ra, ***(2)*** Có trách nhiệm tuân thủ các quy định của pháp luật, không cung cấp thông tin sai lệch và phải cung cấp thông tin khi được yêu cầu hợp pháp; ***(3)*** Có trách nhiệm không gây phương hại đến an ninh quốc gia và sự ổn định của hệ sinh thái dữ liệu. Về cơ bản, pháp luật định hình vai trò của chủ thể dữ liệu là một mắt xích quan trọng, có trách nhiệm đóng góp vào sự "đúng, đủ, sạch, sống" và an toàn của nguồn tài nguyên dữ liệu quốc gia. Một sự thật hiển nhiên rằng, điều này không làm suy yếu quyền của chủ thể dữ liệu mà chỉ làm cho quyền đó trở nên thực tế và hài hòa hơn với bối cảnh xã hội. Nó cho thấy sự trưởng thành của hệ thống pháp luật, không chỉ bảo vệ quyền con người mà còn cân nhắc đến trách nhiệm công dân, đảm bảo rằng một xã hội an toàn và vững mạnh là nền tảng để mọi quyền cá nhân được phát triển một cách bền vững.



Đi từng ngõ - gõ từng nhà - rà soát thông tin dữ liệu dân cư đảm bảo "đúng, đủ, sạch, sống" - Ảnh: Trang TTĐT Công an tỉnh Nghệ An

2.2.2. Quyền, nghĩa vụ và trách nhiệm của chủ quản dữ liệu

2.2.2.1. Quyền của chủ quản dữ liệu

Do chủ quản dữ liệu là bên thừa hành, không phải chủ sở hữu, nên luật không quy định riêng *"quyền"* cho chủ quản ngoài phạm vi được chủ sở hữu ủy quyền. Nói cách khác, quyền của chủ quản là những gì phát sinh từ hợp đồng hoặc quyết định bổ nhiệm với chủ sở hữu dữ liệu. Ví dụ, chủ quản có quyền truy cập, sử dụng dữ liệu trong phạm vi cần thiết để vận hành hệ thống; có quyền đề xuất phương án quản trị dữ liệu; và được pháp luật bảo vệ khi thực hiện đúng vai trò (nếu tuân thủ yêu cầu của chủ sở hữu, chủ quản sẽ không bị coi là xâm phạm dữ liệu).

Luật Dữ liệu năm 2024 gián tiếp thừa nhận quyền này thông qua việc bảo vệ quyền sở hữu dữ liệu: tổ chức, cá nhân thu thập tạo lập dữ liệu sẽ *"được bảo vệ các quyền đối với chủ sở hữu dữ liệu"* theo luật định. Điều đó có nghĩa, nếu chủ quản được giao thu thập, vận hành dữ liệu cho người khác, thì thành quả thu thập đó thuộc quyền chủ sở hữu và được luật bảo vệ, chủ quản có quyền lợi gắn với vai trò thực thi, miễn là không vượt quá thẩm quyền được giao. Có thể khái quát quyền của chủ quản dữ liệu thành các nhóm quyền sau đây:

Thứ nhất, quyền trong quản trị và tổ chức dữ liệu.

Đây là nhóm quyền cho phép chủ quản dữ liệu thiết lập các quy tắc và câu trúc để quản lý dữ liệu một cách hiệu quả, cụ thể, bao gồm:

+ ***Quyền thực hiện quản trị, quản lý dữ liệu*** (Điều 15 Luật Dữ liệu)

Chủ quản dữ liệu được trao quyền thực hiện các hoạt động quản trị, bao gồm việc xây dựng các chính sách, kế hoạch, quy trình và tiêu chuẩn về dữ liệu. Đối với các tổ chức, cá nhân không phải cơ quan nhà nước, họ được quyền "căn cứ vào điều kiện thực tế thực hiện quản trị, quản lý dữ liệu do

minh thu thập, tạo lập, sở hữu". Quyền này đặt chủ quản dữ liệu vào vị trí kiến trúc sư của hệ thống dữ liệu mà họ quản lý. Họ không chỉ vận hành mà còn có quyền xây dựng các quy tắc vận hành độ, tất nhiên phải nằm trong khuôn khổ yêu cầu của chủ sở hữu và quy định của pháp luật.

+ Quyền quyết định việc phân loại dữ liệu

Chủ quản dữ liệu là cơ quan nhà nước có quyền quyết định việc phân loại dữ liệu theo các tiêu chi khác ngoài các tiêu chí bắt buộc, nhằm đáp ứng yêu cầu quản trị, xử lý, bảo vệ dữ liệu (khoản 1 Điều 13 Luật Dữ liệu).

Chủ quản dữ liệu không phải là cơ quan nhà nước cũng được trao quyền này (khoản 2 Điều 13 Luật Dữ liệu).

Quyền này cho phép chủ quân dữ liệu tổ chức, sắp xếp khối dữ liệu mình quản lý một cách linh hoạt và khoa học, phù hợp với đặc thù hoạt động. Việc phân loại tốt sẽ giúp cho việc bảo vệ, khai thác và chia sẻ dữ liệu sau này trở nên hiệu quả và an toàn hơn.

Thứ hai, quyền trong vận hành và xử lý kỹ thuật dữ liệu.

Đây là nhóm quyền cốt lõi, liên quan đến các thao tác kỹ thuật trực tiếp trên dữ liệu trong suốt vòng đời của dữ liệu.

+ Quyền quyết định việc mã hóa, giải mã dữ liệu: Khoản 3 Điều 22 Luật Dữ liệu quy định rõ: *"Chủ sở hữu dữ liệu, chủ quản dữ liệu quyết định việc mã hóa, giải mã dữ liệu"*. Đây là một quyền hạn rất quan trọng, trao cho chủ quân dữ liệu công cụ để chủ động bảo vệ an toàn cho dữ liệu mình quản lý. Họ có thể quyết định áp dụng các giải pháp kỹ thuật bảo mật phù hợp với mức độ quan trọng của dữ liệu và các rủi ro tiềm tàng.

+ Quyền thực hiện các hoạt động xử lý dữ liệu đa dạng: Đối với chủ quân dữ liệu không phải là cơ quan nhà nước, họ được quyền "thực hiện kết hợp, điều chỉnh, cập nhật, sao chép, truyền đưa, chuyển giao dữ liệu" theo

quy định của pháp luật (khoản 3 Điều 26 Luật Dữ liệu). Điều khoản này trao một loạt các quyền tác nghiệp cần thiết cho việc quản lý dữ liệu hàng ngày, từ việc làm sạch, làm giàu dữ liệu (điều chỉnh, cập nhật) đến việc lưu trữ, di chuyển dữ liệu (sao chép, truyền đưa, chuyển giao). Quyền này nâng cao vai trò và sự tin cậy của chủ quán dữ liệu. Họ không chỉ là người lưu giữ mà còn là người có thể bảo chứng cho tính hợp lệ và giá trị pháp lý của dữ liệu mình quản lý.

Thứ ba, quyền trong việc kết nối và cung cấp dữ liệu.

Đây là nhóm quyền thể hiện vai trò hướng ngoại của chủ quản dữ liệu, cho phép họ đưa dữ liệu vào lưu thông và khai thác; cụ thể chủ quản dữ liệu được quyền "kết nối, chia sẻ dữ liệu cho người dùng dữ liệu theo quy định của pháp luật hoặc theo thỏa thuận, bằng cách trực tiếp hoặc thông qua một bên trung gian" (khoản 1 Điều 17 Luật Dữ liệu). Đây là quyền then chốt để khai thác giá trị của dữ liệu. Chủ quản dữ liệu, dưới sự chỉ đạo của chủ sở hữu, có thể chủ động cung cấp dữ liệu cho các bên có nhu cầu, phục vụ các mục tiêu phát triển kinh tế - xã hội hoặc các mục tiêu khác của tổ chức.

Nhìn chung, Luật Dữ liệu năm 2024 đã quy định vai trò rõ ràng cho chủ quản dữ liệu với một bộ quyền hạn mang tính vận hành, quản lý và kỹ thuật. Họ là những *"người quản gia chuyên nghiệp"* của dữ liệu. Các quyền của chủ thể này không phải là quyền sở hữu tuyệt đối mà là các quyền được trao để thực hiện nhiệm vụ quản lý một cách hiệu quả, luôn gắn liền với cụm từ khóa "theo yêu cầu của chủ sở hữu dữ liệu" và trong khuôn khổ của pháp luật. Vị trí của chủ quản dữ liệu là vô cùng quan trọng, đóng vai trò là cầu nối giữa chiến lược của chủ sở hữu và việc triển khai kỹ thuật trên thực tế, bảo đảm dữ liệu được tổ chức, bảo vệ và khai thác một cách chuyên nghiệp và an toàn.



Chủ quản dữ liệu cần phải làm đúng vai trò của mình - Ảnh: Internet

2.2.2.2. Nghĩa vụ của chủ quản dữ liệu

Chủ quản dữ liệu có nhiều nghĩa vụ quan trọng xuất phát từ trách nhiệm quản lý vận hành dữ liệu. Một số nghĩa vụ chính bao gồm:

+ ***Nghĩa vụ tuân thủ pháp luật:*** Đây là nhóm nghĩa vụ rộng nhất, áp dụng cho chủ quán dữ liệu với tư cách là một "tổ chức, cá nhân" tham gia vào hoạt động dữ liệu. Theo đó, chủ quản dữ liệu có nghĩa vụ ***(1)*** không được lợi dụng việc xử lý, quản trị dữ liệu để xâm phạm đến lợi ích quốc gia, dân tộc, quốc phòng, an ninh, trật tự, an toàn xã hội, và các lợi ích hợp pháp khác; ***(2)*** không được cản trở, ngăn chặn trái pháp luật hoặc tấn công, chiếm đoạt, phá hoại các cơ sở dữ liệu và hệ thống thông tin; ***(3)*** không được giả mạo, cố ý làm sai lệch, làm mất, làm hư hỏng dữ liệu trong các cơ sở dữ liệu quan trọng của Đảng và Nhà nước; ***(4)*** không được cố ý cung cấp dữ liệu sai lệch hoặc không cung cấp dữ liệu khi pháp luật yêu cầu. Nhóm nghĩa vụ này yêu cầu chủ quản dữ liệu phải hành động một cách liêm chính, không chỉ thực hiện các yêu cầu kỹ thuật mà còn phải chịu trách nhiệm về tác động tự hành động của mình trong việc quản lý, quản trị, xử lý dữ liệu.

+ ***Bảo đảm chất lượng và an toàn dữ liệu:*** Chủ quản phải thực hiện các biện pháp duy trì dữ liệu chính xác, đầy đủ, được cập nhật kịp thời và bảo vệ dữ liệu khỏi sai sót, mất mát. Điều 12 Luật Dữ liệu yêu cầu cơ quan quản lý cơ sở dữ liệu thường xuyên kiểm tra, khắc phục sai sót và đồng bộ, cập nhật dữ liệu. Mặc dù điều này quy định cho cơ quan nhà nước, nhưng xét về nguyên tắc quản trị dữ liệu, chủ quản tư nhân cũng phải đảm bảo chất lượng dữ liệu mà mình phụ trách. Bên cạnh đó, chủ quản dữ liệu phải đánh giá và quản lý rủi ro, phải tự đánh giá, xác định rủi ro và thực hiện các biện pháp bảo vệ: kịp thời khắc phục rủi ro và thông báo cho các bên liên quan quản lý chặt chẽ dữ liệu cốt lõi, dữ liệu quan trọng và bắt buộc phải định kỳ tiến hành đánh giá rủi ro, thông báo tới ton vị chuyên trách về an ninh mạng, an toàn thông tin thuộc Bộ Công an. Bộ Quốc phòng và cơ quan có liên quan để phối hợp thực hiện việc bao vệ an toàn, an ninh dữ liệu (Điều 25 Luật Dữ liệu).

Nghĩa vụ này đánh dấu một sự thay đổi căn bản, Luật không cho phép chủ quản dữ liệu ở thế bị động. Chủ quan dữ liệu phải chủ động và liên tục thực hiện các hành động quản trị rủi ro. Đặc biệt, nghĩa vụ phải đánh giá rủi ro định kỳ và báo cáo cho Bộ Công an, Bộ Quốc phòng đối với dữ liệu quan trọng đã tạo ra một cơ chế giám sát trực tiếp từ các cơ quan nhà nước. Điều này đặt chủ quản dữ liệu vào một vị trí có trách nhiệm giải trình rất cao, đòi hỏi chủ quản dữ liệu phải có quy trinh chuyên nghiệp và minh bạch.

+***Phân loại và quản lý dữ liệu theo quy định:*** Đây là nghĩa vụ chuyên môn sâu, thể hiện rõ nhất vai trò chuyên nghiệp và yêu cầu năng lực cao của chủ quản dữ liệu. Đối với chủ quản không phải cơ quan nhà nước, luật bắt buộc phải phân loại dữ liệu theo mức độ quan trọng (cốt lõi, quan trọng, khác - Điều 12 Luật Dữ liệu). Do vậy, chủ quản dữ liệu trong doanh nghiệp hoặc

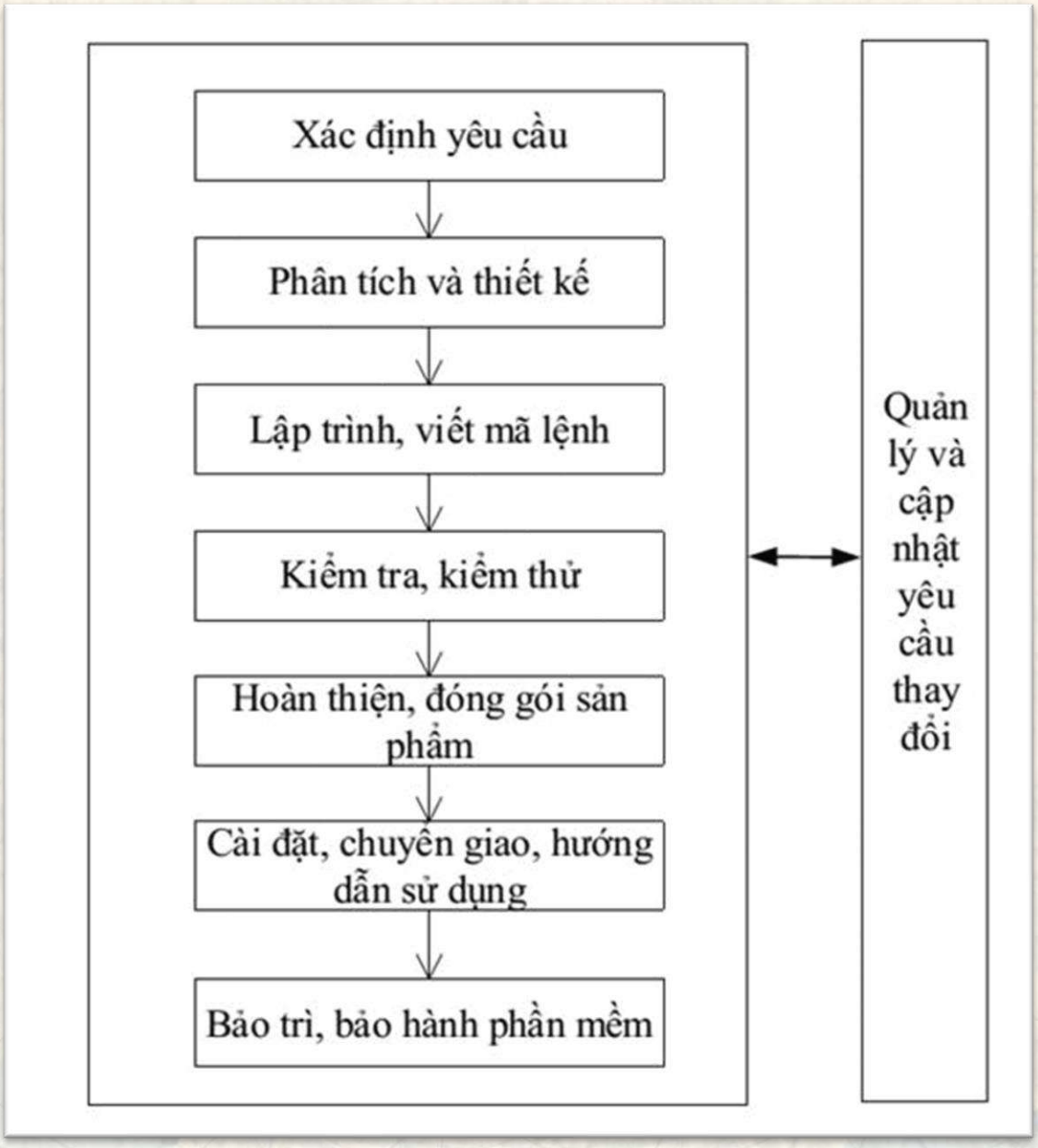
tổ chức tư nhân có nghĩa vụ rà soát dữ liệu mà mình quản lý, xác định đúng nhóm dữ liệu quan trọng, cốt lõi để có biện pháp bảo vệ tương xứng. Nếu chủ quản quản lý dữ liệu cốt lõi hoặc quan trọng, luật yêu cầu phải tuân thủ các quy định nghiêm ngặt về bảo vệ dữ liệu đó. Điều này có thể bao gồm việc mã hóa, lưu trữ trên hạ tầng đạt tiêu chuẩn, hạn chế người truy cập... Chủ quản cũng phải phối hợp với Trung tâm Dữ liệu quốc gia (do Bộ Công an vận hành) nếu là cơ quan nhà nước, hoặc tự thực hiện quản trị dữ liệu phù hợp nếu là tổ chức tư nhân.

+ ***Nghĩa vụ tôn trọng và thực thi quyền của chủ thể dữ liệu.*** Chủ quán dữ liệu không chỉ phục vụ chủ sở hữu dữ liệu mà còn có trách nhiệm trực tiếp với người mà dữ liệu đó phản ánh.

Tại khoản 1 Điều 26 Luật Dữ liệu quy định: *"Chủ quản dữ liệu có trách nhiệm thiết lập quy trình, triển khai các biện pháp, phương thức thu hồi, xóa hoặc hủy dữ liệu theo yêu cầu của chủ thể dữ liệu"*. Đây là một nghĩa vụ vô cùng quan trọng, biến quyền "được lãng quên" của chủ thể dữ liệu từ một khái niệm trừu tượng thành một yêu cầu tác nghiệp cụ thể. Chủ quản dữ liệu phải xây dựng sẵn các công cụ và quy trình để đáp ứng các yêu cầu này một cách kịp thời và hiệu quả. Nghĩa vụ này khẳng định vai trò phục vụ của chủ quản dữ liệu đối với các quyền chính đáng của cá nhân, góp phần xây dựng lòng tin của công chúng.

Ngoài ra, chủ quản tuân thủ yêu cầu xóa hoặc hủy dữ liệu từ chủ thể dữ liệu. Đó là khi chủ thể dữ liệu yêu cầu xóa dữ liệu, chủ quản dữ liệu có trách nhiệm thiết lập quy trình và thực hiện các biện pháp cần thiết để thu hồi, xóa hoặc hủy dữ liệu theo yêu cầu đó. Đây là nghĩa vụ mới và quan trọng, đảm bảo chủ thể dữ liệu có thể thực thi quyền của mình thông qua hành động cụ thể của chủ quản. Ví dụ, một cá nhân yêu cầu xóa thông tin của mình trên hệ

thống, bộ phận chủ quản dữ liệu (quản trị hệ thống) phải có quy trình xác minh yêu cầu và xóa dữ liệu trên cơ sở dữ liệu, đồng thời thông báo lại cho người yêu cầu sau khi hoàn tất.



Thông tư 20/2019/TT-BTNMT Quy trình kỹ thuật xây dựng duy trì vận hành hệ thống thông tin - Ảnh: LuatVietnam

+ Đảm bảo tuân thủ các quy trình, tiêu chuẩn kỹ thuật về dữ liệu:

Chủ quản phải vận hành dữ liệu đúng quy trình, quy chuẩn do chủ sở hữu đề

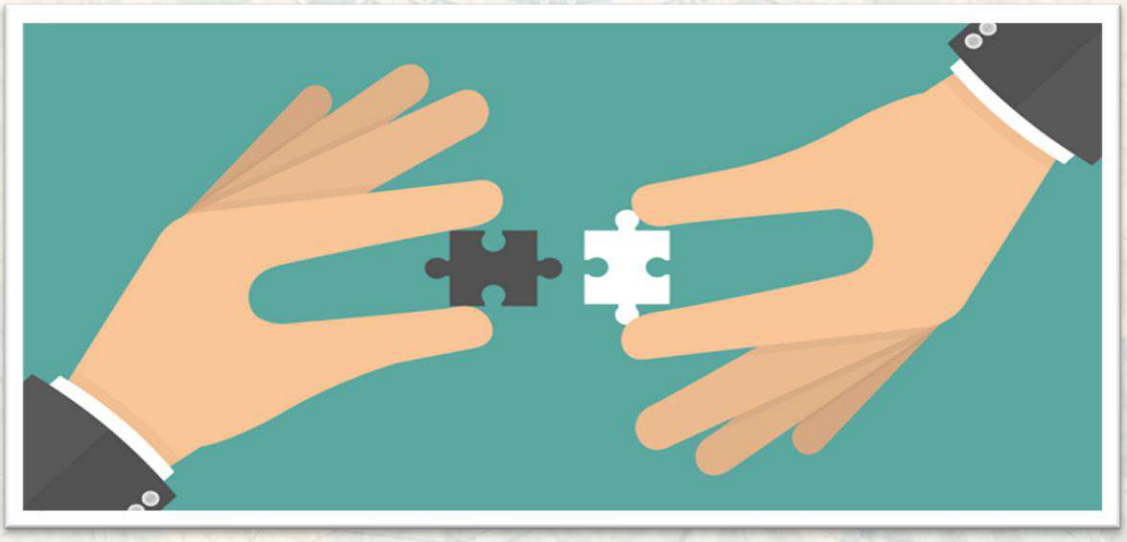
ra và theo quy định pháp luật. Điều 15 Luật Dữ liệu nêu rõ quản trị dữ liệu bao gồm việc xây dựng các chính sách, tiêu chuẩn, quy trình về dữ liệu của chủ sở hữu hoặc chủ quản để quản lý dữ liệu liên tục, hiệu quả, đảm bảo tính đầy đủ, chính xác, toàn vẹn, an toàn. Chủ quản có nghĩa vụ tổ chức thực hiện các quy định đó trong thực tế. Như vậy, nếu chủ sở hữu ban hành quy định nội bộ về phân quyền truy cập, sao lưu định kỳ, mã hóa dữ liệu…, chủ quản phải tuân thủ chặt chẽ. Đây chính là trách nhiệm quản lý dữ liệu (data management) mà luật đề cập.

+ ***Cung cấp, chia sẻ dữ liệu theo quy định:*** Chủ quản dữ liệu, đặc biệt trong khu vực công, có nghĩa vụ kết nối, chia sẻ dữ liệu với các bên được phép. Luật Dữ liệu quy định chủ sở hữu và chủ quản phải kết nối, chia sẻ dữ liệu cho người dùng dữ liệu khi có căn cứ pháp luật hoặc thỏa thuận. Đối với tổ chức, cá nhân không phải cơ quan nhà nước, luật khuyến khích chia sẻ dữ liệu cho cơ quan nhà nước và sẽ có cơ chế hỗ trợ khi thực hiện kết nối. Do đó, nếu một doanh nghiệp tư nhân (chủ sở hữu) yêu cầu chủ quản của mình chia sẻ một phần dữ liệu cho cơ quan chức năng theo luật (ví dụ báo cáo dữ liệu phòng chống dịch bệnh), chủ quản phải phối hợp thực hiện. Thậm chí trong trường hợp đặc biệt (tình trạng khẩn cấp, nguy cơ an ninh…), chủ quản có thể phải cung cấp dữ liệu cho Nhà nước mà không cần sự đồng ý của chủ thể dữ liệu.

+ ***Nghĩa vụ hợp tác và phối hợp.*** Hoạt động phối hợp nhằm bảo đảm tính nhất quán và đồng bộ của dữ liệu quốc gia, chủ quản dữ liệu phải có trách nhiệm hợp tác với các bên liên quan. Tại khoản 3 Điều 15 Luật Dữ liệu quy định: "Chủ sở hữu dữ liệu, chủ quản dữ liệu là cơ quan nhà nước có trách nhiệm phối hợp với Trung tâm dữ liệu quốc gia thực hiện quản trị, quản lý dữ liệu". Nghĩa vụ này ngăn chặn tình trạng "cát cứ dữ liệu" trong các cơ quan nhà nước. Điều này buộc các chủ quán dữ liệu cấp bộ, ngành, địa

phương phải tuân thủ sự điều phối của Trung tâm dữ liệu quốc gia. Điều này là cần thiết để bảo đảm tính liên thông, thống nhất, và hiệu quả của Cơ sở dữ liệu tổng hợp quốc gia.

Tóm lại, chủ quản dữ liệu có trách nhiệm bảo đảm dữ liệu được vận hành an toàn, chính xác, thông suốt theo mục tiêu của chủ sở hữu và quy định pháp luật. Chủ quản đóng vai trò *"quản gia"* cho tài sản dữ liệu, nên phải trung thành với mục đích sử dụng dữ liệu, bảo mật dữ liệu như của chính mình và nhanh chóng thực hiện các yêu cầu hợp pháp liên quan đến dữ liệu (từ cả phía chủ sở hữu lẫn cơ quan chức năng và chủ thể dữ liệu). Các nghĩa vụ của chủ quản dữ liệu trong Luật Dữ liệu năm 2024 là rất toàn diện và chặt chẽ, đòi hỏi sự kết hợp giữa năng lực kỹ thuật, kiến thức pháp lý và kỹ năng quản trị. Chủ quản dữ liệu là những người lính gác ở tuyến đầu, chịu trách nhiệm trực tiếp cho sự an toàn, tuân thủ và hiệu quả của dữ liệu. Việc pháp luật hóa các nghĩa vụ này một cách chi tiết đã nâng tầm vai trò của người quản lý dữ liệu, coi đây là một hoạt động chuyên nghiệp, then chốt trong công tác xây dựng, quản trị, quản lý, xử lý dữ liệu.



Các chủ quản dữ liệu cấp bộ, ngành, địa phương phải tuân thủ sự điều phối của Trung tâm dữ liệu quốc gia - Ảnh: VietnamBiz

2.2.2.3. Trách nhiệm của chủ quản dữ liệu

+ Trách nhiệm với chủ sở hữu dữ liệu

Luật quy định chủ quản dữ liệu không được phép quản lý dữ liệu một cách thụ động mà phải chủ động đánh giá rủi ro, phái triển khai các biện pháp bảo vệ, và phải tuân thủ các quy định bảo vệ dữ liệu (Điều 25, Điều 27 Luật Dữ liệu). Đây là một trách nhiệm pháp lý đòi hỏi sự mẫn cán và chuyên môn cao, bảo đảm dữ liệu được bảo vệ, quản lý một cách tốt nhất.

Ngoài ra, chủ quản dữ liệu còn phải bảo đảm tuân thủ các yêu cầu đã thỏa thuận với chủ sở hữu dữ liệu (theo khái niệm tại Điều 3 Luật Dữ liệu) và bảo đảm tuân thủ pháp luật, thể hiện qua việc chấp hành nghiêm các quy định về hành vi bị nghiêm cấm tại Điều 10 Luật Dữ liệu; ngay cả khi yêu cầu của chủ sở hữu có thể đi ngược lại pháp luật, trách nhiệm tuân thủ pháp luật của chủ quán vẫn là tối cao.

Việc nhìn nhận trách nhiệm của chủ quản dữ liệu dưới lăng kính của một nghĩa vụ ủy thác đã nâng tầm vai trò này. Đâu không còn là một công việc IT đơn thuần, mà là một vị trí của sự tín nhiệm, đòi hỏi không chỉ kỹ năng kỹ thuật mà cả phán đoán về đạo đức và sự am hiểu pháp luật.

+ Trách nhiệm với Nhà nước

Luật dữ liệu đã chính thức cụ thể hóa vai trò của chủ quản dữ liệu trong công tác bảo vệ dữ liệu quốc gia. Theo đó, tại khoản 4 Điều 25 Luật Dữ liệu quy định rõ chủ quản dữ liệu cốt lõi, dữ liệu quan trọng phải định kỳ tiến hành đánh giá rủi ro và thông báo tới đơn vị chuyên trách về an ninh mạng, an toàn thông tin của Bộ Công an, Bộ Quốc phòng. Quy định này tạo ra một kênh báo cáo và giám sát trực tiếp từ các chủ quản dữ liệu đến thẳng các cơ quan quản lý. Chủ quản dữ liệu là người có trách nhiệm phát hiện sớm nhất các lỗ hổng, các nguy cơ trong hệ thống dữ liệu quan trọng trước khi chúng

bị các đối tượng thù địch khai thác. Sự cẩn trọng hay lơ là của một chủ quản dữ liệu giờ đây có thể tác động trực tiếp đến an ninh của mỗi ngành, một lĩnh vực và thậm chí là cả quốc gia (như đối với dữ liệu cốt lõi).

+ Trách nhiệm trong vai trò là một nhà cung cấp dịch vụ chuyên nghiệp

Đối với các tổ chức kinh doanh, vai trò của chủ quản dữ liệu thường gắn liền với việc cung cấp dịch vụ cho khách hàng (chủ sở hữu dữ liệu). Khi đó, các trách nhiệm của chủ thể này còn được làm rõ thêm tại Điều 43 Luật dữ liệu với trách nhiệm theo Hợp đồng (phải cung cấp dịch vụ trên cơ sở một hợp đồng rõ ràng; phải bảo đảm kênh tiếp nhận và sử dụng dịch vụ thông suốt, liên tục; phải thường xuyên quản lý, kiểm tra, giám sát an toàn bảo mật dữ liệu; phòng ngừa, ngăn chặn và xử lý rủi ro).

Các quy định này thiết lập một tiêu chuẩn chuyên nghiệp tối thiểu cho ngành công nghiệp dịch vụ dữ liệu tại nước ta. Một công ty cung cấp dịch vụ lưu trữ đám mây hoặc phân tích dữ liệu không thể chỉ bán sản phẩm rồi "phủi tay". Với tư cách là chủ quản dữ liệu cho khách hàng, họ có trách nhiệm pháp lý phải duy trì dịch vụ ổn định và bảo mật chủ động. Điều này sẽ thúc đẩy các nhà cung cấp phải đầu tư nghiêm túc hơn vào hạ tầng quy trình và nhân sự an ninh, từ đó nâng cao chất lượng và sự an toàn của toàn thị trường dữ liệu.

Các trách nhiệm vụ chủ quản dữ liệu trong Luật Dữ liệu năm 2024 đã được định hình một cách toàn diện và chặt chẽ. Chủ quản dữ liệu không chỉ là người vận hành kỹ thuật, mà còn là người được ủy thác một nghĩa vụ cẩn trọng, là một mắt xích trong hệ thống bảo vệ dữ liệu của quốc gia và là một nhà cung cấp dịch vụ chuyên nghiệp phải tuân thủ các tiêu chuẩn cao.

2.2.3. Quyền, nghĩa vụ và trách nhiệm của chủ sở hữu dữ liệu

2.2.3.1. Quyền của chủ sở hữu dữ liệu

Luật dữ liệu đã thiết lập một vị thế pháp lý vô cùng mạnh mẽ cho chủ sở hữu dữ liệu chủ sở hữu dữ liệu có quyền định đoạt chiến lược đối với dữ liệu của mình. Theo đó, quyền của chủ sở hữu dữ liệu đối với dữ liệu là quyền tài sản theo quy định của pháp luật về dân sự (khoản 15 Điều 3 Luật Dữ liệu 2024).



Chủ sở hữu dữ liệu được Luật Dữ liệu và các văn bản pháp lý liên tạo lành lang pháp lý liên quan đến nhiều quyền, trong đó có quyền chiếm hữu, quyền sử dụng, quyền định đoạt dữ liệu - Ảnh: Internet

Theo pháp luật về dân sự, *"Quyền tài sản"* có nghĩa là quyền trị giá được bằng tiền, bao gồm quyền tài sản đối với đối tượng, quyền sở hữu trí tuệ, quyền sử dụng và các quyền tài sản khác (Điều 115, Bộ Luật Dân sự 2015). Theo đó, cá nhân và tổ chức có quyền chuyển nhượng "quyền tài sản" đối với dữ liệu theo quy định tại Điều 450 Bộ Luật Dân sự (tức là trong

trường hợp mua bán, bên bán phải chuyển giấy tờ và làm thủ tục chuyển quyền sở hữu cho bên mua, bên mua phải trả tiền cho bên bán). Có thể thấy rằng, Luật Dữ liệu 2024 đã xác lập địa vị pháp lý của dữ liệu tương tự như một loại tài sản phi vật chất có giá trị kinh tế.

Về nội hàm của quyền sở hữu đối với dữ liệu, theo Điều 158 và Điều 159 Bộ Luật Dân sự 2015, có thể hiểu là chủ sở hữu dữ liệu có quyền chiếm hữu, quyền sử dụng, quyền định đoạt dữ liệu và một số quyền khác đối với dữ liệu theo quy định của pháp luật, như quyền hưởng dụng (hưởng lợi ích, hoa lợi từ dữ liệu), quyền ngăn chặn xâm phạm dữ liệu... Việc công nhận quyền đối với dữ liệu là một quyền tài sản đã nâng dữ liệu từ một khái niệm thông tin trừu tượng lên thành một loại tài sản được pháp luật dân sự bảo hộ, tương tự như các tài sản vật chất hay tài sản trí tuệ. Điều này mang những ý nghĩa sâu sắc. Đó là: ***(1)*** Tạo cơ sở cho kinh tế số: Dữ liệu có thể được định giá, mua bán, chuyển nhượng và có thể được sử dụng làm tài sản bảo đảm. Đây là nền móng pháp lý vững chắc nhất để xây dựng một thị trường dữ liệu đúng nghĩa. ***(2)*** Khẳng định quyền lực tối cao: Tất cả các quyền cụ thể khác được liệt kê trong luật đều xuất phát từ quyền tài sản gốc này. Chủ sở hữu có toàn quyền định đoạt số phận dữ liệu của mình trong khuôn khổ pháp luật.

Xuất phát từ các ý nghĩa trên, có thể khái quát một số quyền cụ thể của chủ sở hữu dữ liệu như sau:

+ ***Quyền chiếm hữu dữ liệu.*** Xuất phát từ việc dữ liệu là một tồn tại phi vật chất và có thể bị sao chép, nhân bản, sự "chiếm hữu" đối với dữ liệu chủ yếu là quyền "kiểm soát quá trình truy cập, xử lý dữ liệu", không phải sự nắm giữ cơ học, thuần túy. Theo đó, khi thực hiện chiếm hữu, chủ sở hữu có quyền duy trì sự kiểm soát đối với dữ liệu và giới hạn người được tiếp cận. Một cách dễ hiểu, chiếm hữu là việc chủ sở hữu dữ liệu được phép kiểm

soát truy cập đối với dữ liệu mình tạo lập hoặc được cấp quyền. Việc kiểm soát dữ liệu bao gồm việc quyết định ai được truy cập dữ liệu và hình thức truy cập như thế nào. Ví dụ, một công ty sở hữu cơ sở dữ liệu khách hàng có quyền quyết định ai trong nội bộ được phép truy cập, đồng thời cấm bộ phận khác hoặc bên thứ ba không được phép truy cập.



Phó Chủ tịch Quốc hội Trần Quang Phương điều hành kỳ họp thứ 8, Quốc hội khóa XV - Ảnh: Báo Điện tử Chính phủ

+ ***Quyền sử dụng dữ liệu.*** Khoản 14 Điều 3 Luật quy định rõ: "Chủ sở hữu dữ liệu là cơ quan, tổ chức, cá nhân có quyền quyết định việc xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng và trao đổi giá trị của dữ liệu do mình sở hữu. Theo đó, chủ sở hữu tự do khai thác, sử dụng dữ liệu để phục vụ mục đích của mình, bao gồm nghiên cứu, phân tích, kinh doanh, phát triển sản phẩm mới... miễn là nó không vi phạm pháp luật, không xâm phạm quyền riêng tư của chủ thể dữ liệu. Quyền này cũng bao gồm việc tạo ra sản phẩm hoặc dịch vụ từ dữ liệu và chủ sở hữu có toàn quyền tận dụng giá trị từ sản phẩm, dịch vụ dữ liệu đó. Ngay trong định nghĩa về chủ sở hữu dữ

liệu, Luật Dữ liệu cũng đã ghi nhận chủ sở hữu có quyền quyết định việc xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng và trao đổi giá trị của dữ liệu do mình sở hữu (Điều 3).

+ ***Quyền định đoạt và quản trị dữ liệu.*** Theo Điều 192 Bộ luật Dân sự 2015, quyền định đoạt là quyền chuyển giao quyền sở hữu tài sản, từ bỏ quyền sở hữu, tiêu dùng hoặc tiêu hủy tài sản. Tương tự, đối với dữ liệu, chủ sở hữu dữ liệu có quyền bán, cho thuê, chuyển nhượng quyền sở hữu, cấp phép quyền khai thác dữ liệu cho bên khác theo thỏa thuận. Có thể thấy quyền này đã biến dữ liệu thành tài sản có thể định giá, giao dịch trong thị trường dữ liệu. Thể chế hóa nội dung trên, việc định quyền tài sản chính là cơ sở pháp lý cho phép nhiều doanh nghiệp thực hiện mua bán dữ liệu như một hàng hóa. Pháp luật Việt Nam hiện không cấm hoạt động này, trừ trường hợp dữ liệu thuộc danh mục cấm giao dịch theo quy định (gồm dữ liệu là bí mật nhà nước, dữ liệu cá nhân, dữ liệu quan trọng, dữ liệu cốt lõi). Chủ sở hữu cũng có thể chia sẻ dữ liệu của mình với đối tác hoặc công khai một phần dữ liệu nếu muốn. Luật Dữ liệu khuyến khích chủ sở hữu dữ liệu cung cấp dữ liệu cho cơ quan nhà nước phục vụ mục tiêu chung, trong điều kiện bình thường là trên cơ sở tự nguyện, thỏa thuận. Ngoài ra, chủ sở hữu dữ liệu có toàn quyền quyết định các chính sách và quy tắc áp dụng cho dữ liệu của mình tại Chương 2 của Luật Dữ liệu như:

(1) Quyền quyết định về quản trị: Chủ sở hữu dữ liệu có quyền xây dựng các chính sách, kế hoạch, chương trình, quy trình về dữ liệu. Các chủ sở hữu không phải cơ quan nhà nước được quyền tự thực hiện quản trị, quản lý dữ liệu phù hợp với điều kiện thực tế (Điều 15 Luật Dữ liệu).

(2) Quyền quyết định về phân loại: Có quyền quyết định các tiêu chí phân loại dữ liệu để phục vụ mục đích quản lý (trừ trường hợp phân loại dữ liệu theo tính chất quan trọng của dữ liệu, khoản 2 Điều 13 Luật Dữ liệu).

(3) Quyền quyết định về lưu trữ: Có quyền quyết định việc lưu trữ dữ liệu do mình sở hữu (áp dụng cho chủ sở hữu không phải là cơ quan nhà nước, khoản 2 Điều 14 Luật Dữ liệu).

(4) Quyền quyết định về bảo mật: Có quyền quyết định việc mã hóa, giải mã dữ liệu (khoản 3 Điều 22 Luật Dữ liệu).

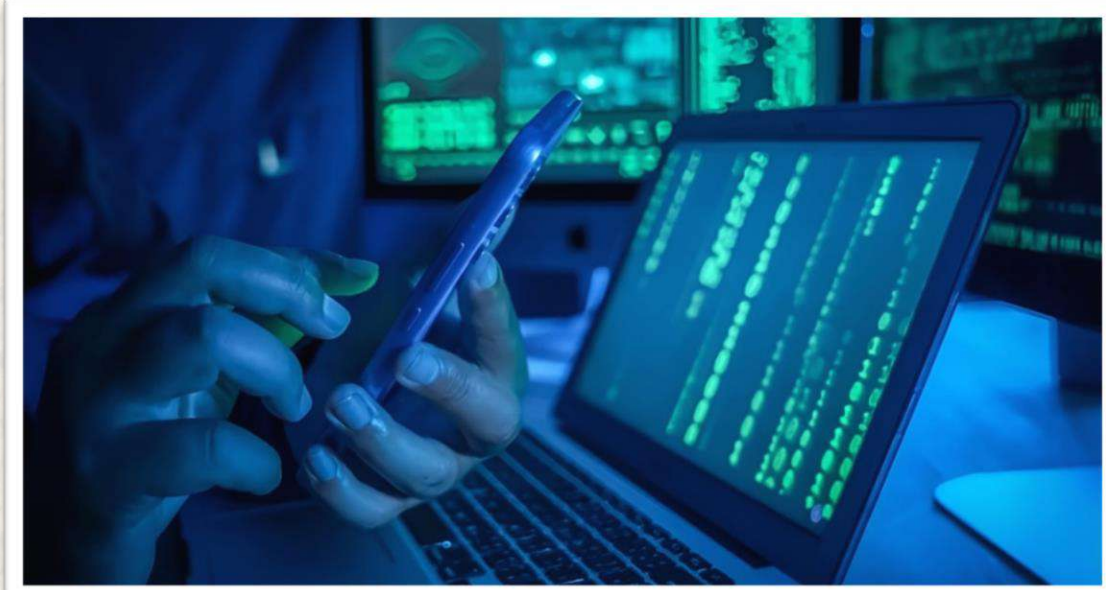
Nhóm quyền này cho phép chủ sở hữu dữ liệu đóng vai trò là nhà hoạch định chiến lược, chủ động thiết lập "luật lệ" về quyền sở hữu dữ liệu theo quy định của pháp luật. Họ được quyết định xem đó là dữ liệu nào, được lưu trữ ở đâu và cách thức quản lý nó như thế nào. Chủ sở hữu dữ liệu vừa là nhà hoạch định và là người đưa ra quyết định cuối cùng và là chủ sở hữu của tài sản đó. Chủ sở hữu dữ liệu có quyền bảo vệ dữ liệu ở cấp độ cao nhất.



Quyền bí mật đời tư được cụ thể hóa hơn trong Luật Dữ liệu - Ảnh: lsvn.vn

+ ***Quyền được bảo vệ bởi pháp luật.*** Nếu có hành vi xâm phạm dữ liệu, chẳng hạn một đối thủ đánh cắp hoặc sử dụng trái phép dữ liệu mà doanh nghiệp đang sở hữu, thì chủ sở hữu có quyền yêu cầu cơ quan có thẩm quyền xử lý hành vi đó. Hành vi tấn công, chiếm đoạt dữ liệu bị pháp luật nghiêm

cấm và có chế tài nghiêm khắc. Chủ sở hữu dữ liệu có thể tố cáo, khởi kiện hoặc nhờ cơ quan chức năng can thiệp để bảo vệ quyền sở hữu của mình. Ví dụ, nếu phát hiện một cá nhân bán trái phép dữ liệu khách hàng thuộc sở hữu công ty, công ty có thể đề nghị Công an điều tra hành vi này. Pháp luật hiện hành (Nghị định 98/2020/NĐ-CP) đã có chế tài xử phạt hành vi mua bán dữ liệu khách hàng trái phép (mức phạt tiền lên tới hàng trăm triệu đồng) và dự kiến bổ sung mức phạt lên tới 5% doanh thu của doanh nghiệp vi phạm trong lĩnh vực dữ liệu cá nhân.



Dữ liệu cá nhân là tài nguyên chiến lược, tài sản và "hàng hóa" đặc biệt

+ ***Quyền khai thác và trao đổi giá trị kinh tế.*** Đây là nhóm quyền hiện thực hóa giá trị tài sản của dữ liệu, cụ thể:

(1) Quyền khai thác chung: Có quyền thực hiện các hoạt động kết hợp, điều chỉnh, cập nhật, sao chép, truyền đưa, chuyển giao dữ liệu (khoản 2 Điều 26 Luật Dữ liệu).

(2) Quyền phát triển các tiện ích, công cụ, ứng dụng phân tích, tổng hợp dữ liệu cung cấp cho cơ quan nhà nước, tổ chức, cá nhân khác để phục vụ phát triển kinh tế - xã hội và các hoạt động khác (khoản 3 Điều 19 Luật Dữ liệu).

(3) Quyền tham gia thị trường: Có quyền thiết lập các mối quan hệ thương mại thông qua các đơn vị trung gian dữ liệu (Điều 40 Luật Dữ liệu).

Nếu *"quyền tài sản"* là nền tảng thì nhóm quyền này chính là cơ chế để khai thác giá trị từ nền tảng đó. Luật cho phép chủ sở hữu không chỉ sử dụng dữ liệu cho mục đích nội bộ mà còn có thể thương mại hóa dữ liệu thông qua việc chia sẻ cung cấp dịch vụ hoặc tham gia vào các sàn dữ liệu. Đây chính là động lực kinh tế lớn nhất, khuyến khích các tổ chức, doanh nghiệp đầu tư vào việc thu thập, làm giàu và sáng tạo dựa trên dữ liệu.

Ngoài ra, chủ sở hữu dữ liệu nếu là cá nhân còn được hưởng các quyền nhân thân liên quan. Thí dụ, một người viết nhật ký điện tử thì người đó vừa là chủ thể dữ liệu (vì dữ liệu nói về họ), vừa là chủ sở hữu (vì họ tạo ra dữ liệu). Họ có quyền giữ bí mật hoặc công bố dữ liệu đó tùy ý, theo quyền về đời sống riêng tư được Hiến pháp và Bộ luật Dân sự bảo hộ. Thêm vào đó, Luật Dữ liệu còn mở rộng cho chủ sở hữu dữ liệu quyền đồng ý. Việc kết nối chia sẻ dữ liệu giữa cơ sở dữ liệu tổng hợp quốc gia và hệ thống thông tin của chủ sở hữu dữ liệu phải được thực hiện trên cơ sở thống nhất bằng văn bản giữa Bộ Công an và chủ sở hữu dữ liệu (khoản 3 Điều 36 Luật Dữ liệu). Quyền này yêu cầu sự đồng ý bằng văn bản trước khi kết nối hệ thống của mình với Cơ sở dữ liệu tổng hợp quốc gia đã trao cho chủ sở hữu dữ liệu một vị thế rất quan trọng. Quy định này bảo đảm rằng việc tích hợp vào hệ thống dữ liệu lớn của quốc gia không phải là một mệnh lệnh hành chính đơn phương, mà phải là một quá trình có sự đồng thuận, thương lượng và thống nhất về các điều kiện kỹ thuật, pháp lý. Điều này đặc biệt quan trọng đối với doanh nghiệp lớn và các tổ chức sở hữu các bộ dữ liệu có giá trị cao giúp họ bảo vệ lợi ích và tài sản của mình.

Có thể thấy rằng, Luật Dữ liệu năm 2024 đã xây dựng một hình mẫu chủ sở hữu dữ liệu với đầy đủ quyền năng của một chủ tài sản thực thụ. Từ việc xác lập dữ liệu là "quyền tài sản", trao quyền định đoạt chiến lược, cho phép khai thác giá trị kinh tế, đến việc trao quyền đồng ý tối hậu trong các kết nối quan trọng. Luật đã tạo ra một hành lang pháp lý vững chắc và một động lực mạnh mẽ. Mục tiêu là khuyến khích mọi tổ chức cá nhân đầu tư làm giàu tài nguyên dữ liệu, đồng thời trao cho họ công cụ pháp lý đủ mạnh để quản lý và bảo vệ tài sản chiến lược đó trong kỹ thuật số.

2.2.3.2. Nghĩa vụ của chủ sở hữu dữ liệu



Hội thảo khoa học quốc tế "Truyền thông chính sách trong bối cảnh chuyển đổi số và hội nhập quốc tế" - Ảnh: Báo Điện tử Chính phủ

Trong bối cảnh chuyển đổi số và sự phát triển mạnh mẽ của công nghệ thông tin, việc quy định các nghĩa vụ này là hết sức cần thiết, không chỉ giúp bảo vệ quyền riêng tư của cá nhân mà còn góp phần bảo vệ an ninh quốc gia và phát triển bền vững hệ thống dữ liệu. Các văn bản của Đảng và Nhà nước,

như Nghị quyết số 52-NQ/TW của Bộ Chính trị về phát triển chính phủ điện tử, Luật An toàn thông tin mạng (2015), Luật Bảo vệ quyền lợi người tiêu dùng (2010), và Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, đều khẳng định vai trò quan trọng của chủ sở hữu dữ liệu trong việc tuân thủ các quy định pháp lý, bảo vệ thông tin cá nhân và đảm bảo an toàn mạng. Việc thực hiện đầy đủ các nghĩa vụ này không chỉ là trách nhiệm pháp lý mà còn là yếu tố then chốt để xây dựng lòng tin của người dân, tổ chức và cộng đồng trong quản lý, bảo vệ và sử dụng dữ liệu, từ đó tạo dựng một nền tảng an toàn và hiệu quả cho việc phát triển nền kinh tế số. Theo đó, đi đôi với quyền lợi, chủ sở hữu dữ liệu phải thực hiện một số nghĩa vụ, như:

Thứ nhất, bảo vệ dữ liệu và quyền lợi của chủ thể dữ liệu. Chủ sở hữu dữ liệu (đặc biệt khi xử lý dữ liệu cá nhân) có nghĩa vụ tôn trọng quyền riêng tư và các quyền của chủ thể dữ liệu. Họ phải có biện pháp bảo vệ dữ liệu không bị lộ lọt, sử dụng đúng mục đích đã thông báo. Đối với dữ liệu cốt lõi, dữ liệu quan trọng, Khoản 3 Điều 27 Luật Dữ liệu quy định *"Chủ sở hữu dữ liệu, chủ quản dữ liệu quản lý dữ liệu cốt lõi, dữ liệu quan trọng phải tuân thủ các quy định về bảo vệ dữ liệu"*.

Nghị định số 13/2023/NĐ-CP yêu cầu bên kiểm soát dữ liệu cá nhân (tương ứng với chủ sở hữu dữ liệu) phải áp dụng các biện pháp kỹ thuật và quản lý để bảo đảm dữ liệu được bảo mật, an toàn; trường hợp vi phạm phải chịu trách nhiệm bồi thường cho chủ thể dữ liệu. Chủ sở hữu cũng phải ngừng hoặc hạn chế xử lý dữ liệu cá nhân nếu chủ thể rút lại sự đồng ý hoặc phản đối vì lý do chính đáng. Bên cạnh đó, nghĩa vụ này cũng được quy định bởi Luật Dữ liệu. trong đó, các biện pháp bảo vệ dữ liệu được áp dụng trong toàn bộ quá trình xử lý dữ liệu, bao gồm: Xây dựng và tổ chức thực hiện chính sách, quy định bảo vệ dữ liệu; Quản lý hoạt động xử lý dữ liệu; Xây

dựng và triển khai các giải pháp kỹ thuật; Đào tạo, bồi dưỡng, phát triển, quản lý nguồn nhân lực; Các biện pháp bảo vệ dữ liệu khác theo quy định của pháp luật. Việc tuân thủ các quy định về bảo vệ dữ liệu đòi hỏi chủ sở hữu phải chủ động triển khai các chính sách, quy trình và giải pháp kỹ thuật cần thiết để bảo đảm an toàn cho dữ liệu trong suốt vòng đời của dữ liệu, đây là một nghĩa vụ liên tục và đòi hỏi sự đầu tư về nguồn lực.

Thứ hai, tuân thủ quy định phân loại và lưu trữ dữ liệu. Đối với tổ chức hoặc cá nhân sở hữu dữ liệu không phải cơ quan nhà nước, luật bắt buộc phải phân loại dữ liệu theo mức độ quan trọng và tuân thủ các yêu cầu lưu trữ an toàn cho dữ liệu quan trọng, cốt lõi. Nếu chủ sở hữu (ví dụ một công ty) có dữ liệu cốt lõi hoặc quan trọng, họ phải lưu trữ dữ liệu đó theo quy định tại khoản 2 Điều 14 Luật Dữ liệu. Có thể hiểu việc lưu trữ phải bảo đảm trên hạ tầng đáp ứng tiêu chuẩn (được "khuyến khích" lưu ở Trung tâm dữ liệu quốc gia). Chủ sở hữu tư nhân cũng được phép thỏa thuận lưu trữ dữ liệu của mình tại Trung tâm dữ liệu quốc gia thông qua hợp đồng dịch vụ - nhưng đó là quyền lựa chọn, không hẳn là nghĩa vụ.

Thứ ba, đảm bảo quản trị, quản lý dữ liệu hiệu quả. Chủ sở hữu chịu trách nhiệm cao nhất trong quản trị dữ liệu. Điều 15 Luật Dữ liệu yêu cầu chủ sở hữu dữ liệu thiết lập chính sách, quy trình, tiêu chuẩn để quản lý dữ liệu hiệu quả, bảo đảm tính đầy đủ, chính xác, thống nhất, an toàn của dữ liệu. Do vậy, nghĩa vụ của chủ sở hữu là phải ban hành và thực thi hệ thống quản trị phù hợp. Ví dụ, một doanh nghiệp phải ban hành quy định nội bộ về phân quyền truy cập dữ liệu khách hàng, chu kỳ sao lưu dữ liệu, quy trình xử lý khi có sự cố lộ dữ liệu... và đảm bảo các quy định này được thực hiện. Nếu chủ sở hữu không xây dựng được văn hóa và cơ chế quản trị dữ liệu tốt, bản thân họ có thể bị thiệt hại và có thể bị coi là thiếu trách nhiệm nếu xảy ra vi phạm.

Thứ tư, tuân thủ yêu cầu của cơ quan quản lý nhà nước. Chủ sở hữu dữ liệu phải chấp hành các yêu cầu hợp pháp từ phía Nhà nước liên quan đến dữ liệu. Điển hình, nghĩa vụ cung cấp dữ liệu trong trường hợp đặc biệt: Luật Dữ liệu 2024 quy định khi xảy ra tình trạng khẩn cấp, nguy cơ đe dọa an ninh quốc gia, thảm họa hoặc để phòng chống tội phạm nghiêm trọng, cơ quan có thẩm quyền có quyền yêu cầu tổ chức, cá nhân phải cung cấp dữ liệu mà không cần sự đồng ý của chủ thể dữ liệu. Chủ sở hữu dữ liệu trong trường hợp này buộc phải tuân thủ lệnh yêu cầu. Ví dụ, một nhà mạng viễn thông (chủ sở hữu dữ liệu liên lạc) khi có yêu cầu phục vụ điều tra khủng bố phải cung cấp ngay dữ liệu theo yêu cầu của cơ quan An ninh, không được trì hoãn vì lý do bảo vệ dữ liệu cá nhân. Ngoài ra, chủ sở hữu còn phải tuân thủ các nghĩa vụ báo cáo, thống kê về dữ liệu nếu pháp luật chuyên ngành yêu cầu (như báo cáo cho cơ quan quản lý về hiện trạng cơ sở dữ liệu).



Quản lý nhà nước phải tập trung xây dựng thể chế, chính sách thay vì giải quyết sự vụ - Ảnh: Báo Điện tử Chính phủ

Thứ năm, chịu trách nhiệm pháp lý khi vi phạm. Nếu chủ sở hữu dữ liệu vi phạm các quy định về bảo vệ dữ liệu (thu thập dữ liệu cá nhân nhạy cảm không xin phép, mua bán dữ liệu công dân trái phép,...), họ sẽ phải chịu chế tài tương ứng.



Chủ sở hữu dữ liệu sẽ phải chịu trách nhiệm pháp lý cho hành vi vi phạm pháp luật về dữ liệu - Ảnh: Internet

Việc chủ sở hữu dữ liệu chịu trách nhiệm pháp lý khi vi phạm các quy định về bảo vệ dữ liệu là một yêu cầu thiết yếu nhằm bảo vệ quyền lợi của cá nhân, tổ chức và cộng đồng. Bảo vệ dữ liệu không chỉ đơn thuần là một hoạt động kỹ thuật mà còn liên quan mật thiết đến các quy định pháp lý nghiêm ngặt, phản ánh trách nhiệm đạo đức và xã hội trong việc xử lý thông tin.

Khi chủ sở hữu dữ liệu vi phạm các quy định về bảo vệ dữ liệu, như thu thập dữ liệu cá nhân nhạy cảm mà không có sự đồng ý của chủ thể dữ liệu, hay mua bán, trao đổi dữ liệu cá nhân một cách trái phép, họ sẽ phải đối mặt

với các chế tài pháp lý nghiêm khắc, nhằm bảo vệ quyền lợi của các bên liên quan và duy trì trật tự xã hội. Các vi phạm này có thể ảnh hưởng trực tiếp đến quyền riêng tư của cá nhân, tạo ra rủi ro lớn đối với sự an toàn của thông tin và tài sản cá nhân.

Ngoài việc quy định chế tài, các tổ chức, doanh nghiệp và cá nhân giữ vai trò chủ sở hữu dữ liệu cũng cần thực hiện các biện pháp phòng ngừa để tránh vi phạm. Điều này bao gồm việc xây dựng các chính sách bảo vệ dữ liệu nội bộ chặt chẽ, đào tạo nhân viên về quy định bảo vệ dữ liệu, sử dụng công nghệ bảo mật tiên tiến và thực hiện các cuộc kiểm tra định kỳ về tính bảo mật và tuân thủ các quy định pháp lý. Hơn nữa, việc có trách nhiệm pháp lý khi vi phạm không chỉ giúp ngăn ngừa hành vi vi phạm mà còn tạo ra một động lực thúc đẩy các chủ sở hữu dữ liệu nâng cao ý thức và cam kết bảo vệ dữ liệu của người dân. Việc thực thi các chế tài này sẽ góp phần tạo dựng một môi trường số an toàn, bảo mật và đáng tin cậy cho tất cả các bên tham gia trong xã hội thông tin.

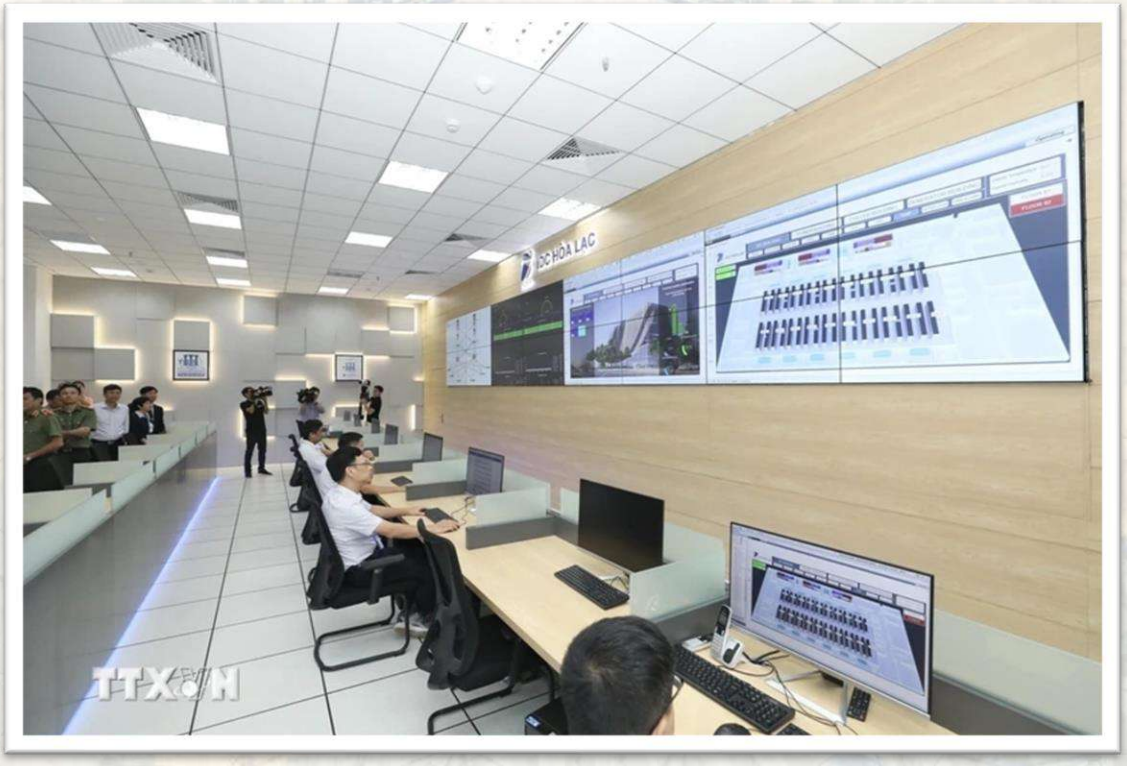
Thứ sáu, nghĩa vụ khi lưu trữ dữ liệu cốt lõi, dữ liệu quan trọng.

Theo khoản 2 Điều 14 Luật quy định trường hợp lưu trữ dữ liệu cốt lõi, dữ liệu quan trọng thì chủ sở hữu dữ liệu phải bảo đảm tuân thủ theo quy định tại khoản 3 Điều 27 của Luật Dữ liệu. Nghĩa vụ này đặc biệt nhấn mạnh tầm quan trọng của việc bảo vệ các loại dữ liệu nhạy cảm. "Dữ liệu cốt lõi là dữ liệu quan trọng trực tiếp tác động đến quốc phòng, an ninh, đối ngoại, kinh tế vĩ mô, ổn định xã hội, sức khỏe và an toàn cộng đồng thuộc Danh mục do Thủ tướng Chính phủ ban hành". "Dữ liệu quan trọng là dữ liệu có thể tác động đến quốc phòng, an ninh, đối ngoại, kinh tế vĩ mô, ổn định xã hội, sức khỏe và an toàn cộng đồng thuộc Danh mục do Thủ tướng Chính phủ ban hành". Việc lưu trữ những dữ liệu này đòi hỏi tuân thủ các quy định

nghiêm ngặt về bảo mật, an toàn và quản lý rủi ro được quy định chi tiết tại Điều 27. Điều này cho thấy Nhà nước đặc biệt quan tâm đến việc bảo vệ những dữ liệu có ảnh hưởng lớn đến quốc gia và xã hội.

Thứ bảy, nghĩa vụ kết nối chia sẻ dữ liệu.

Khoản 1 Điều 17 Luật quy định *"Chủ sở hữu dữ liệu, chủ quản dữ liệu kết nối, chia sẻ dữ liệu cho người dùng dữ liệu theo quy định của pháp luật hoặc theo thỏa thuận, bằng cách trực tiếp hoặc thông qua một bên trung gian"*. Quy định này có ý nghĩa thúc đẩy việc lưu thông và sử dụng dữ liệu một cách hiệu quả. Chủ sở hữu dữ liệu không chỉ có quyền mà còn có trách nhiệm tạo điều kiện cho việc chia sẻ dữ liệu. Việc chia sẻ dữ liệu có thể dựa trên các quy định pháp luật (ví dụ: chia sẻ dữ liệu mở) hoặc theo thỏa thuận thương mại, cho phép hình thành các hệ sinh thái dữ liệu đa dạng. Điều này cũng mở ra cơ hội phát triển các dịch vụ trung gian dữ liệu.



Thủ tướng chỉ đạo đẩy mạnh thực hiện Đề án Trung tâm dữ liệu quốc gia - Ảnh: Thông tấn xã Việt Nam

Tổng kết lại, các nghĩa vụ của chủ sở hữu dữ liệu trong Luật Dữ liệu thể hiện một cách tiếp cận toàn diện, từ trách nhiệm cơ bản về nguồn gốc và chất lượng dữ liệu, đến các yêu cầu phức tạp hơn về quản trị, bảo vệ, chia sẻ và vận hành dữ liệu. Đặc biệt, Luật nhấn mạnh nghĩa vụ tăng cường đối với dữ liệu cốt lõi và dữ liệu quan trọng, phản ánh mức độ nhạy cảm và tầm ảnh hưởng của chúng đối với quốc gia. Sự phân biệt nghĩa vụ giữa cơ quan nhà nước và tổ chức cá nhân khác cho thấy tính linh hoạt trong áp dụng nhưng vẫn đảm bảo mục tiêu chung là phát triển và bảo vệ dữ liệu hiệu quả trong xã hội số.



Tổng Bí thư Tô Lâm và Thủ tướng Chính phủ Phạm Minh Chính tham dự phiên thảo luận về dự án Luật Bảo vệ dữ liệu cá nhân - Ảnh: VOV.vn

2.2.3.3. Trách nhiệm của chủ sở hữu dữ liệu

+ Trách nhiệm chung đối với dữ liệu do mình thu thập, tạo lập dữ liệu

Đây là trách nhiệm cơ bản và bao trùm nhất của chủ sở hữu dữ liệu. Chủ sở hữu dữ liệu phải bảo đảm tính chính xác, hợp pháp và đầy đủ của dữ

liệu ngay từ khâu thu thập và tạo lập. Nếu dữ liệu không đúng hoặc vi phạm pháp luật trogn quá trình này, chủ sở hữu dư liệu sẽ phải chịu trách nhiệm về hậu quả. Điều này cũng liên quan đến việc bảo đảm "dữ liệu được thu thập, tạo lập và phải đảm bảo việc xác thực, truy nguyên được đến bản số hóa giấy tờ, tài liệu".

+ Trách nhiệm phối hợp quản trị, quản lý dữ liệu.

Khoản 3 Điều 15 Luật quy định chủ sở hữu dữ liệu là cơ quan nhà nước có trách nhiệm phối hợp với Trung tâm dữ liệu quốc gia thực hiện quản trị, quản lý dữ liệu theo quy định của Luật.

Trách nhiệm này áp dụng riêng cho các chủ sở hữu dữ liệu là cơ quan nhà nước; qua đó, nhấn mạnh sự cần thiết của việc hợp tác và đồng bộ hóa trong quản lý dữ liệu ở các quốc gia. Việc phối hợp với Trung tâm dữ liệu quốc gia bảo đảm rằng dữ liệu của các cơ quan nhà nước được quản lý một cách thống nhất, hiệu quả và an toàn phục vụ mục tiêu chung là xây dựng Chính phủ số, kinh tế số, xã hội số.

Bên cạnh đó, khoản 4 Điều 15 Luật Dữ liệu cũng quy định chủ sở hữu dữ liệu là tổ chức, cá nhân không thuộc cơ quan nhà nước phải căn cứ vào điều kiện thực tế thực hiện quản trị, quản lý dữ liệu do mình thu thập, tạo lập, sở hữu.

Có thể thấy đây là một trách nhiệm liên tục và bao trùm, đòi hỏi chủ sở hữu dữ liệu phải thiết lập và duy trì một hệ thống quản lý dữ liệu hiệu quả đối với cơ quan Nhà nước, nghĩa vụ này còn bao gồm sự phối hợp chặt chẽ với Trung tâm dữ liệu quốc gia để bảo đảm tính đồng bộ và hiệu quả trong quản lý dữ liệu quốc gia. Đối với tổ chức, cá nhân khác về quản trị và quản lý dữ liệu cần phù hợp với điều kiện thực tế, thể hiện sự linh hoạt nhưng vẫn bảo đảm các nguyên tắc cơ bản về chất lượng và an toàn dữ liệu.

+ Trách nhiệm thực hiện các hoạt động xử lý dữ liệu khác.

Trách nhiệm này bảo đảm rằng dữ liệu được duy trì tính năng động và cập nhật. Chủ sở hữu dữ liệu phải bảo đảm các hoạt động như điều chỉnh, cập nhật, sao chép, truyền đưa và chuyển giao dữ liệu được thực hiện một cách chính xác và tuân thủ các quy định pháp luật hiện hành. Điều này cũng góp phần vào việc bảo đảm chất lượng dữ liệu.

Các trách nhiệm của chủ sở hữu dữ liệu quy định trong Luật Dữ liệu rất chặt chẽ và toàn diện, đặt ra các yêu cầu cao về quản lý, bảo vệ và chia sẻ dữ liệu. Trách nhiệm đó không chỉ dừng lại ở việc lưu trữ, mà còn bao gồm cả việc bảo đảm tính chính xác, hợp pháp, an toàn và hiệu quả trong việc sử dụng dữ liệu. Đặc biệt có sự phân cấp trách nhiệm dựa trên loại dữ liệu (cốt lõi, quan trọng) và chủ thể (cơ quan nhà nước hay tổ chức, cá nhân khác), phản ánh sự cần thiết của các biện pháp bảo vệ và quản lý phù hợp với tính chất của dữ liệu và đối tượng quản lý.

2.3. CƠ CHẾ BẢO ĐẢM THỰC HIỆN CÁC QUYỀN, NGHĨA VỤ TRÊN ĐỐI VỚI TỔ CHỨC, CÁ NHÂN KHÔNG PHẢI LÀ CƠ QUAN NHÀ NƯỚC

Việc đảm bảo quyền và nghĩa vụ về dữ liệu không chỉ phụ thuộc vào ý thức tự giác tuân thủ của các tổ chức và cá nhân, mà còn đòi hỏi một hệ thống cơ chế pháp lý toàn diện, minh bạch và mạnh mẽ. Điều này có ý nghĩa vô cùng quan trọng trong bối cảnh Việt Nam đang đối mặt với cuộc cách mạng chuyển đổi số và gia nhập sâu rộng vào nền kinh tế số toàn cầu. Do đó, việc xây dựng các cơ chế giám sát, hỗ trợ và chế tài xử lý vi phạm là cần thiết và là yêu cầu vô cùng cấp bách.

Thứ nhất, *cơ chế phân công cơ quan quản lý nhà nước chuyên trách.* Luật Dữ liệu 2024 thiết lập một đầu mối quản lý nhà nước thống nhất về

dữ liệu. Cụ thể, Chính phủ thống nhất quản lý nhà nước về dữ liệu, Bộ Công an là cơ quan đầu mối chịu trách nhiệm trước Chính phủ về quản lý nhà nước đối với dữ liệu (trừ phạm vi Bộ Quốc phòng). Bộ Quốc phòng quản lý dữ liệu trong lĩnh vực quốc phòng, và các bộ, ngành khác phối hợp với Bộ Công an trong quản lý dữ liệu thuộc phạm vi của mình. Đối với địa phương, Ủy ban nhân dân cấp tỉnh quản lý nhà nước về dữ liệu tại địa bàn. Cơ cấu này đảm bảo có cơ quan chuyên trách (Bộ Công an) theo dõi việc thực thi pháp luật về dữ liệu trên phạm vi cả nước. Bộ Công an sẽ ban hành thông tư hướng dẫn, thiết lập các quy chuẩn kỹ thuật về an toàn dữ liệu, đồng thời thanh tra, kiểm tra định kỳ và đột xuất các tổ chức cá nhân trong việc chấp hành luật. Chẳng hạn, Bộ Công an có thể yêu cầu doanh nghiệp báo cáo về công tác phân loại và bảo vệ dữ liệu quan trọng; hoặc tiến hành thanh tra một công ty có dấu hiệu thu thập dữ liệu cá nhân trái phép. Việc có cơ quan chủ quản rõ ràng giúp các tổ chức, cá nhân ngoài nhà nước biết đầu mối liên hệ để hỏi đáp, xin hướng dẫn hoặc báo cáo khi cần, qua đó nâng cao hiệu quả tuân thủ.

Thứ hai, *khung pháp lý toàn diện và chi tiết quy định những hành vi bị cấm trong quản trị, xử lý dữ liệu của cơ quan, tổ chức, cá nhân.* Để có khung pháp lý đầy đủ và chi tiết về dữ liệu, Chính phủ đã ban hành các nghị định, đề án hướng dẫn để cụ thể hóa Luật Dữ liệu, tạo hành lang pháp lý rõ ràng cho doanh nghiệp, tổ chức thực hiện. Ví dụ, Chính phủ đã ban hành danh mục về dữ liệu cốt lõi, dữ liệu quan trọng, thời gian tới tiếp tục xây dựng và ban hành tiêu chí xác định các tiêu chuẩn, quy chuẩn kỹ thuật về an toàn dữ liệu, kết nối chia sẻ dữ liệu để công ty, doanh nghiệp tư nhân tuân theo. Hiện tại, Chính phủ đã ban hành Nghị định 47/2020/NĐ-CP quy định về kết nối, chia sẻ dữ liệu số trong cơ quan nhà nước, tạo tiền đề kỹ thuật cho chia sẻ

dữ liệu công - tư trong tương lai. Bên cạnh đó, Nghị định 13/2023/NĐ-CP đã đưa ra 8 nguyên tắc bảo vệ dữ liệu cá nhân và phân công trách nhiệm cụ thể cho các bên (bên kiểm soát, bên xử lý, bên thứ ba) trong quy trình xử lý dữ liệu cá nhân. Ngoài ra, Luật quy định cụ thể các hành vi bị nghiêm cấm bao gồm: ***(1)*** Lợi dụng việc xử lý dữ liệu, quản trị dữ liệu, phát triển kinh doanh, lưu hành sản phẩm, dịch vụ về dữ liệu để xâm phạm đến lợi ích quốc gia - dân tộc, quốc phòng, an ninh, trật tự, an toàn xã hội, lợi ích công cộng, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; ***(2)*** Cản trở hoặc ngăn chặn trái pháp luật quá trình xử lý dữ liệu, quản trị dữ liệu hoặc tấn công chiếm đoạt, phá hoại cơ sở dữ liệu, hệ thống thông tin phục vụ quản lý, xử lý, quản trị, bảo vệ dữ liệu; ***(3)*** Giả mạo, cố ý làm sai lệch, làm mất, làm hư hỏng dữ liệu trong cơ sở dữ liệu của cơ quan Đảng, Nhà nước, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội; ***(4)*** Cố ý cung cấp dữ liệu sai lệch hoặc không cung cấp dữ liệu theo quy định của pháp luật. Điều này giúp các doanh nghiệp hiểu rõ phải làm gì để đảm bảo quyền chủ thể dữ liệu không bị vi phạm.

Thứ ba, *chế tài xử lý nghiêm minh*. Khi xảy ra tranh chấp hoặc vi phạm pháp luật về dữ liệu, một số cơ chế bảo đảm thực hiện các quyền, nghĩa vụ của các tổ chức cá nhân sẽ được áp dụng, như:

+ ***Khiếu nại tố cáo:*** Tổ chức, cá nhân có quyền khiếu nại, tố cáo hành vi vi phạm quy định về dữ liệu đến cơ quan có thẩm quyền.

+ ***Khởi kiện dân sự:*** Chủ thể dữ liệu có thể khởi kiện ra tòa án để yêu cầu bồi thường thiệt hại khi quyền và lợi ích hợp pháp của mình bị xâm phạm, đặc biệt trong các trường hợp như vi phạm về quyền tài sản, vi phạm thỏa thuận giữa các bên liên quan.

+ ***Xử phạt hành chính và hình sự:*** Các hành vi vi phạm quy định về dữ liệu có thể bị xử phạt hành chính hoặc truy cứu trách nhiệm hình sự tùy theo mức độ vi phạm.

Về hành chính, như đã đề cập, Chính phủ đang đề xuất mức phạt rất cao cho các vi phạm về dữ liệu cá nhân - tối đa 3 tỷ đồng hoặc 5% doanh thu năm của tổ chức vi phạm (tùy mức nào cao hơn). Ngoài phạt tiền, có thể áp dụng biện pháp đình chỉ hoạt động xử lý dữ liệu đến 24 tháng, tịch thu tang vật, phương tiện nếu vi phạm nghiêm trọng. Ví dụ, một công ty bán lậu dữ liệu khách hàng có thể vừa bị phạt tiền lớn, vừa bị đình chỉ hoạt động kinh doanh dữ liệu.

Về hình sự, Bộ luật Hình sự hiện hành đã có các tội danh liên quan như tội "Xâm phạm bí mật hoặc an toàn thư tín, điện thoại, điện tín hoặc hình thức trao đổi thông tin riêng tư khác của người khác" (Điều 159) và tội "Đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông" (Điều 288). Các tội này có mức phạt tù tối đa từ 3 đến 7 năm, áp dụng cho hành vi thu thập, phát tán dữ liệu cá nhân trái phép ở mức nghiêm trọng. Ngoài ra, khi Luật Dữ liệu có hiệu lực, cơ quan chức năng có thể đề xuất bổ sung tội danh hoặc tình tiết tăng nặng mới liên quan đến dữ liệu (ví dụ tội vi phạm quy định về quản lý dữ liệu cốt lõi quốc gia...). Hiện nay, Luật Xử lý Vi phạm hành chính 2020 đã bổ sung quy định xử phạt đối với hành vi vi phạm hành chính trong lĩnh vực dữ liệu. Trong thời gian tới, Bộ Công an sẽ nghiên cứu đề xuất Chính phủ ban hành nghị định, quy định xử phạt hành chính đối với hành vi vi phạm trong lĩnh vực dữ liệu để xử phạt những hành vi vi phạm hành chính trong lĩnh vực này, mức phạt tiền có thể tính theo tỷ lệ % doanh thu, tương tự cách tiếp cận của EU (GDPR).. Đồng thời sẽ nghiên cứu đề xuất quy định các hành vi vi phạm pháp luật bị coi là tội phạm trong lĩnh vực dữ liệu.

Việc áp dụng chế tài nghiêm minh sẽ đảm bảo tổ chức, cá nhân tuân thủ nghĩa vụ vì nếu không, cái giá phải trả có thể rất lớn - thậm chí đánh đổi bằng sự "tồn vong" của doanh nghiệp (nếu bị phạt % doanh thu hoặc rút giấy phép). Đây có thể xem là biện pháp *"răn đe từ gốc"* hết sức quan trọng. Như vậy, với một khung pháp luật ngày càng hoàn thiện, việc thực thi các quyền, nghĩa vụ sẽ có cơ sở vững chắc và thống nhất trên cả nước.

Thứ tư, *cơ chế giám sát và chế tài dân sự.* Bên cạnh sự giám sát của cơ quan quản lý, bản thân chủ thể dữ liệu và đối tác kinh doanh cũng là một kênh đảm bảo việc tuân thủ. Chủ thể dữ liệu có quyền khởi kiện dân sự đòi bồi thường nếu bị xâm phạm dữ liệu cá nhân. Những bản án tiền lệ sẽ tạo sức ép để các công ty cẩn trọng hơn trong xử lý dữ liệu người dùng. Ví dụ, nếu một ngân hàng làm lộ dữ liệu khách hàng và bị kiện đòi bồi thường tổn thất, các ngân hàng khác sẽ nhìn đó làm gương mà đầu tư hơn cho bảo mật. Mặt khác, trong môi trường kinh doanh, các doanh nghiệp cũng tự giám sát lẫn nhau về tuân thủ dữ liệu thông qua yêu cầu hợp đồng. Ngày nay, đối tác nước ngoài thường yêu cầu công ty Việt Nam chứng minh tuân thủ quy định bảo vệ dữ liệu (như GDPR, Nghị định 13) khi ký kết hợp đồng chia sẻ dữ liệu. Do đó, để làm ăn, doanh nghiệp phải chủ động tuân thủ hoặc thậm chí đạt các chứng chỉ quốc tế (ISO 27001 về an ninh thông tin chẳng hạn). Sự dịch chuyển này tạo ra *"áp lực thị trường"* buộc các chủ sở hữu dữ liệu trong khu vực tư không thể lơ là nghĩa vụ pháp lý về dữ liệu nếu không muốn mất uy tín, mất cơ hội kinh doanh.

Thứ năm, *hỗ trợ và khuyến khích tự nguyện tuân thủ.* Nhà nước không chỉ yêu cầu các tổ chức, cá nhân tuân thủ các quy định về dữ liệu mà còn chủ động hỗ trợ, khuyến khích khu vực tư nhân thực hiện các nghĩa vụ bảo vệ dữ liệu một cách hiệu quả.



Tăng cường cơ chế giám sát bảo đảm liêm chính tư pháp trong tiến trình cải cách tư pháp - Ảnh: Tạp chí Tổ chức Nhà nước

Luật Dữ liệu có các quy định khuyến khích tổ chức, cá nhân không phải cơ quan nhà nước thực hiện một số quyền của mình, ví dụ như: Khuyến khích chủ sở hữu dữ liệu, chủ quản dữ liệu khác thực hiện cung cấp công cụ truy cập, truy xuất dữ liệu (khoản 2 Điều 16); Khuyến khích tổ chức, cá nhân trong nước và ngoài nước cung cấp dữ liệu thuộc quyền sở hữu cho cơ quan nhà nước (khoản 1 Điều 18); Khuyến khích chủ sở hữu dữ liệu, chủ quản dữ liệu phát triển các tiện ích, công cụ, ứng dụng phân tích, tổng hợp dữ liệu cung cấp cho cơ quan nhà nước, tổ chức, cá nhân khác để phục vụ phát triển kinh tế - xã hội và các hoạt động khác (khoản 3 Điều 19). Các quy định trên có vai trò thúc đẩy sự gắn kết, phối hợp giữa các tổ chức, doanh nghiệp tư nhân chia sẻ dữ liệu cho cơ quan nhà nước để một mặt bảo đảm các quyền và lợi ích của các tổ chức, doanh nghiệp này, mặt khác bảo đảm sự quản lý chặt chẽ và chuyển giao dữ liệu nhanh chóng khi có yêu cầu cấp bách về an ninh, quốc phòng, lợi ích công cộng.

Mặt khác, chính sách của Nhà nước về dữ liệu đang hướng tới việc huy động tối đa nguồn lực xã hội để phát triển hạ tầng dữ liệu quốc gia, đồng thời khuyến khích doanh nghiệp đầu tư mạnh mẽ vào công nghệ bảo mật và các giải pháp bảo vệ dữ liệu. Một trong những biện pháp quan trọng là việc thành lập Quỹ Phát triển Dữ liệu quốc gia (theo quy định tại Chương II Luật Dữ liệu), qua đó sẽ cung cấp nguồn tài chính hỗ trợ cho các dự án nâng cấp hạ tầng bảo vệ dữ liệu, đặc biệt là đối với các doanh nghiệp nhỏ và vừa, giúp họ duy trì và bảo vệ dữ liệu một cách an toàn. Bên cạnh đó, cơ quan nhà nước sẽ đẩy mạnh công tác tuyên truyền, tập huấn và cung cấp các tài liệu hướng dẫn về pháp luật dữ liệu cho cả doanh nghiệp và người dân. Khi nhận thức về bảo vệ dữ liệu được nâng cao và trở thành một phần trong văn hóa tuân thủ, việc áp dụng các biện pháp bảo vệ sẽ trở thành một thói quen tự nhiên trong mọi hoạt động của các tổ chức và cá nhân.



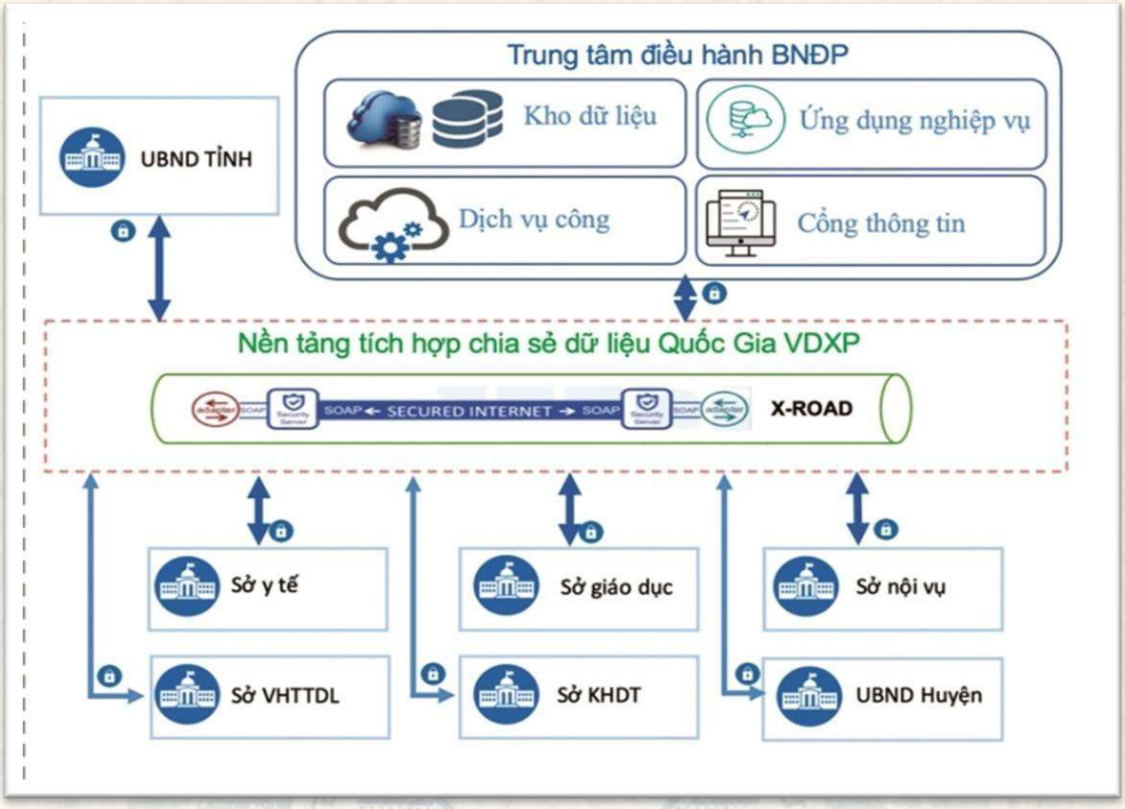
Chú trọng phát triển nguồn lực dữ liệu - Ảnh: Thông tấn xã Việt Nam

Ví dụ, Bộ Công an đã chủ động xuất bản các cẩm nang hướng dẫn và tổ chức hội thảo để hỗ trợ các doanh nghiệp trong việc thực thi Luật Dữ liệu,

Luật Bảo vệ dữ liệu cá nhân. Các hiệp hội ngành nghề cũng có thể đóng vai trò quan trọng trong việc xây dựng các quy tắc ứng xử về bảo vệ dữ liệu trong phạm vi ngành của mình, từ đó tạo ra các tiêu chuẩn đạo đức chung, giúp củng cố ý thức và trách nhiệm của các thành viên trong ngành đối với bảo mật thông tin. Việc tạo ra một môi trường như vậy không chỉ giúp các tổ chức dễ dàng tiếp cận các tài liệu và hướng dẫn cần thiết mà còn tự nguyện tuân thủ pháp luật, từ đó nâng cao chất lượng bảo vệ dữ liệu trong toàn xã hội.

Sáu là, *các biện pháp kỹ thuật hỗ trợ.*

Cuối cùng, không thể thiếu các giải pháp kỹ thuật như triển khai nền tảng chia sẻ, điều phối dữ liệu quốc gia. Luật Dữ liệu đề cập đến việc xây dựng Trung tâm Dữ liệu quốc gia và Nền tảng kết nối, chia sẻ dữ liệu giữa trung tâm này với các bên. Khi có hạ tầng quốc gia tin cậy, doanh nghiệp tư nhân có thể kết nối và sử dụng, giảm nguy cơ vi phạm do sử dụng hệ thống kém an toàn. Chẳng hạn, nếu một doanh nghiệp nhỏ không đủ năng lực bảo mật dữ liệu, họ có thể thuê lưu trữ tại Trung tâm Dữ liệu quốc gia với chi phí hỗ trợ - như vậy dữ liệu vừa an toàn hơn vừa nằm trong tầm giám sát của cơ quan quản lý. Bên cạnh đó, các công cụ kỹ thuật như hệ thống quản lý cấp quyền, hệ thống ghi nhận nhật ký truy cập cũng sẽ được khuyến khích áp dụng. Cơ quan chức năng có thể yêu cầu doanh nghiệp tích hợp chức năng cho phép chủ thể dữ liệu xem quản lý sự đồng ý của mình (một dạng "cổng thông tin quyền riêng tư"). Đây là cách giúp quyền chủ thể dữ liệu được thực thi tự động, giảm gánh nặng giám sát thủ công.



Kỹ thuật kết nối trên nền tảng tích hợp chia sẻ dữ liệu quốc gia - Ảnh: Tạp chí An toàn thông tin

Tóm lại, để các quy định về quyền và nghĩa vụ dữ liệu đi vào cuộc sống, Nhà nước thiết lập cả *"nhân tố thúc đẩy"* và *"nhân tố cưỡng chế"*. Một mặt, tạo điều kiện thuận lợi (hướng dẫn, hạ tầng hỗ trợ, khuyến khích đầu tư bảo mật); mặt khác, đặt ra chế tài nghiêm và giám sát chặt chẽ. Đối với tổ chức, cá nhân khu vực tư nhân, các cơ chế này vừa là áp lực tuân thủ vừa là hỗ trợ cần thiết. Trong bối cảnh chuyển đổi số, việc tuân thủ tốt luật về dữ liệu không chỉ để tránh mắc phải các hình phạt, mà còn giúp doanh nghiệp, tổ chức nâng cao uy tín, năng lực cạnh tranh khi khách hàng ngày càng coi trọng quyền riêng tư và bảo mật. Có thể thấy, với khung pháp lý mới và cơ chế bảo đảm đồng bộ, Việt Nam đang từng bước xây dựng môi trường dữ liệu an toàn, tin cậy, nơi quyền và lợi ích của các bên (Nhà nước - doanh nghiệp - người dân) được cân bằng hài hòa dưới sự thượng tôn pháp luật về dữ liệu.

Câu 3

Quy định về hành vi bị nghiêm cấm trong Luật Dữ liệu năm 2024? Giải pháp xây dựng, hoàn thiện quy định pháp luật về xử lý vi phạm hành chính trong lĩnh vực dữ liệu?

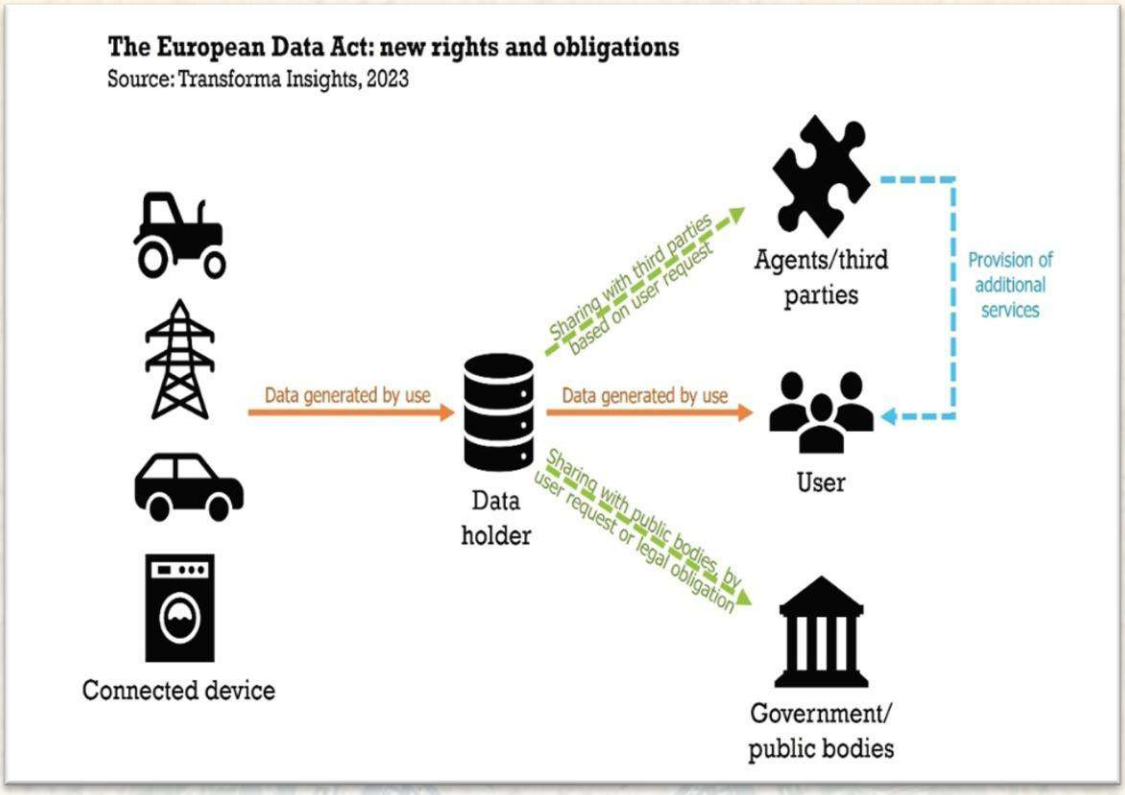


3.1. MỘT SỐ HÀNH VI BỊ NGHIÊM CẤM TRONG PHÁP LUẬT VỀ DỮ LIỆU Ở MỘT SỐ QUỐC GIA TRÊN THẾ GIỚI

Trên thế giới, nhiều quốc gia đã ban hành các đạo luật nhằm bảo vệ dữ liệu và quyền riêng tư, trong đó quy định rõ những hành vi bị nghiêm cấm liên quan đến dữ liệu. Điển hình, tại Liên minh Châu Âu, GDPR nghiêm cấm việc xử lý các *dữ liệu cá nhân nhạy cảm* nếu không có cơ sở pháp lý rõ ràng. Nguyên tắc chung của GDPR là mọi xử lý dữ liệu cá nhân đều phải hợp pháp, minh bạch và có mục đích chính đáng; việc thu thập hoặc sử dụng dữ liệu cá nhân mà không có căn cứ pháp lý phù hợp (như sự đồng ý của người dữ liệu hoặc nghĩa vụ pháp luật) bị xem là trái phép và có thể bị chế tài nghiêm khắc. Nhiều quốc gia châu Âu khác cũng có luật tương tự GDPR, nghiêm cấm các hành vi xâm phạm đời tư và yêu cầu bảo mật dữ liệu cá nhân; vi phạm có thể dẫn đến phạt tiền hàng chục triệu euro hoặc tỷ lệ phần trăm doanh thu, nhằm răn đe việc xử lý dữ liệu trái phép.



Quy định chung về Bảo vệ Dữ liệu của Liên minh Châu Âu, có hiệu lực từ ngày 25/5/2018 - Ảnh: Base.vn



Mô hình luật dữ liệu của EU - Ảnh: Tranforma insights

Qua nghiên cứu văn bản mới về dữ liệu ở Châu Âu đó là Đạo luật về Dữ liệu của Liên minh Châu Âu (European Union Data Act) được Nghị viện và Hội đồng châu Âu thông qua năm 2023, EU Data Act không liệt kê các hành vi bị cấm trong một điều riêng, mà lồng ghép vào nghĩa vụ của từng nhóm chủ thể, có thể khái quát như sau: Hành vi hạn chế quyền truy cập dữ liệu trái quy định[195]; Hành vi lạm dụng dữ liệu được chia sẻ[196]; Hành vi phân biệt đối xử trong cung cấp dữ liệu[197]; Hành vi cản trở việc chuyển đổi dịch

[195] Điều 4(3) quy định: *"Bên nắm giữ dữ liệu không được từ chối cung cấp dữ liệu cho người sử dụng hoặc gây cản trở việc truy cập dữ liệu mà người sử dụng có quyền nhận theo quy định của luật này"*. European Union. (2023). *Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023* (Data Act). Official Journal of the European Union, L, 2023(2854), 1–98.

[196] Điều 5(8) quy định: *"Bên thứ ba nhận dữ liệu không được sử dụng dữ liệu cho mục đích khác ngoài mục đích được người sử dụng hoặc luật định cho phép, và không được tiết lộ dữ liệu cho bên khác trừ khi có sự đồng ý rõ ràng hoặc nghĩa vụ pháp luật"*. European Union. (2023), *Tài liệu đã dẫn.*

[197] Điều 5(4) quy định: *"Bên nắm giữ dữ liệu không được phân biệt đối xử giữa các bên thứ ba có cùng điều kiện truy cập dữ liệu"*. European Union. (2023), *Tài liệu đã dẫn.*

vụ điện toán đám mây[198]; Hành vi truy cập dữ liệu trái phép từ bên ngoài lãnh thổ EU[199].

Tại Hoa Kỳ, dù không có danh mục *"hành vi bị cấm"* thống nhất ở cấp liên bang, pháp luật Mỹ vẫn nghiêm cấm nhiều hành vi xâm hại dữ liệu thông qua các đạo luật chuyên biệt và cơ chế thực thi của các cơ quan quản lý. FTC sử dụng thẩm quyền theo Đạo luật FTC để trừng phạt các hành vi thương mại "không công bằng hoặc lừa dối", bao gồm việc vi phạm cam kết bảo mật, đánh cắp hoặc tiết lộ trái phép thông tin người dùng. Chẳng hạn, việc doanh nghiệp tự ý bán dữ liệu khách hàng trong khi đã cam kết giữ bí mật, hoặc không bảo vệ an ninh thông tin dẫn đến rò rỉ dữ liệu, đều bị FTC coi là hành vi vi phạm pháp luật và bị xử phạt. Ngoài ra, Hoa Kỳ có luật chuyên ngành cấm tiết lộ trái phép một số loại dữ liệu nhạy cảm (ví dụ: luật HIPAA cấm tiết lộ thông tin y tế cá nhân nếu không được phép). Song nhìn chung, do thiếu luật bảo vệ dữ liệu toàn diện, việc xác định hành vi bị cấm ở Mỹ dựa nhiều vào án lệ và các vụ xử phạt cụ thể hơn là một danh mục liệt kê sẵn như các nước khác.

Tại Châu Á, nhiều quốc gia cũng ban hành đạo luật bảo vệ dữ liệu nghiêm ngặt, liệt kê rõ các hành vi bị cấm nhằm ngăn chặn việc lạm dụng dữ liệu. Tại Trung Quốc Luật Bảo vệ Thông tin Cá nhân (PIPL) và Luật An ninh Dữ liệu (DSL) đã đưa những điều khoản cấm rất cụ thể. PIPL quy định không một cá nhân hay tổ chức nào được phép thu thập, sử dụng, xử lý, truyền tải, mua bán hoặc công bố trái phép thông tin cá nhân của người khác

---

[198] Điều 23(2): *"Nhà cung cấp dịch vụ không được áp dụng biện pháp kỹ thuật, hợp đồng hoặc tổ chức nhằm cản trở hoặc làm chậm quá mức quá trình chuyển đổi sang nhà cung cấp dịch vụ khác."* European Union. (2023), *Tài liệu đã dẫn.*

[199] Điều 27(1) quy định: *"Bên nắm giữ dữ liệu hoặc bên trung gian dữ liệu không được tuân thủ yêu cầu của cơ quan nước thứ ba về việc truy cập dữ liệu nếu yêu cầu đó trái với luật của Liên minh hoặc của quốc gia thành viên".* European Union. (2023), *Tài liệu đã dẫn.*

(Điều 44 PIPL). Đặc biệt, luật này cấm việc xử lý dữ liệu cá nhân nhằm mục đích xâm phạm an ninh quốc gia hoặc lợi ích cộng đồng, tương tự như cách Việt Nam và nhiều nước yêu cầu dữ liệu không được sử dụng vào mục đích phương hại đến an ninh, trật tự (Điều 25 PIPL). Song song đó, Luật An ninh Dữ liệu Trung Quốc kiểm soát chặt chẽ dữ liệu quan trọng: nghiêm cấm việc cung cấp dữ liệu lưu trữ ở Trung Quốc ra nước ngoài cho cơ quan tư pháp hoặc chấp pháp nước ngoài nếu chưa được sự cho phép của giới chức Trung Quốc (Điều 36 DSL). Quy định này nhằm ngăn chặn hành vi tùy tiện chuyển dữ liệu, đặc biệt là dữ liệu nhạy cảm, "dữ liệu lõi" ra nước ngoài, bảo vệ chủ quyền dữ liệu quốc gia. Vi phạm các lệnh cấm này ở Trung Quốc có thể bị phạt rất nặng, ví dụ doanh nghiệp vi phạm quy định về "dữ liệu lõi" có thể bị phạt tới 10 triệu nhân dân tệ (hơn 1,5 triệu USD) và đình chỉ hoạt động.

Nhiều quốc gia khác trong khu vực cũng có quy định tương tự nhằm bảo vệ dữ liệu cá nhân và an toàn thông tin. Singapore với Đạo luật Bảo vệ Dữ liệu Cá nhân 2022 (PDPA) đã hình sự hóa một số hành vi liên quan đến dữ liệu: bất kỳ cá nhân hay tổ chức nào cố ý hoặc liều lĩnh tiết lộ trái phép dữ liệu cá nhân, sử dụng dữ liệu cá nhân trái phép nhằm trục lợi hoặc gây hại cho người khác, hay thu thập hoặc khôi phục dữ liệu đã ẩn danh khi không được phép, đều bị coi là tội phạm (Điều 51(3) và 51(4)). Chẳng hạn, một nhân viên cố ý rò rỉ dữ liệu khách hàng cho bên thứ ba mà không có quyền sẽ vi phạm PDPA và có thể bị phạt tiền (tối đa 5.000 đô la Singapore) và phạt tù tới 2 năm. Ở Nhật Bản, Đạo luật Bảo vệ Thông tin Cá nhân 2020 (APPI) cũng nghiêm cấm doanh nghiệp sử dụng dữ liệu cá nhân ngoài mục đích đã thông báo hoặc chuyển cho bên thứ ba nếu không có sự đồng ý, nếu vi phạm có thể bị lệnh cải tổ và chế tài hành chính nghiêm khắc (Điều 16(1) và 23(1) APPI). Hàn Quốc với Đạo luật Bảo vệ Thông tin Cá nhân 2020 thậm chí quy định

các hành vi thu thập thông tin nhạy cảm của người dùng mà không được phép là bất hợp pháp, có trường hợp bị truy cứu hình sự (Điều 23(1)). Nhìn chung, xu hướng chung của pháp luật các nước là cấm các hành vi xâm phạm quyền riêng tư cá nhân, đánh cắp, tiết lộ, mua bán dữ liệu trái phép, cũng như các hành vi tấn công, phá hoại hệ thống dữ liệu. Những hành vi này được xác định rõ trong luật nhằm tạo cơ sở pháp lý để xử lý nghiêm, bảo đảm dữ liệu được quản lý, sử dụng an toàn và đúng mục đích.

3.2. CÁC HÀNH VI BỊ NGHIÊM CẤM TRONG PHÁP LUẬT VỀ DỮ LIỆU TẠI VIỆT NAM

Trong bối cảnh chuyển đổi số và phát triển nền kinh tế dữ liệu, việc xử lý, quản trị, kinh doanh và lưu hành các sản phẩm, dịch vụ về dữ liệu đang ngày càng trở nên phổ biến và có ảnh hưởng sâu đậm đến mọi mặt của đời sống xã hội. Dữ liệu không còn chỉ là một dạng tài nguyên thông thường mà đã trở thành tài sản chiến lược của từng tổ chức, doanh nghiệp cũng như của quốc gia. Sự phát triển nhanh chóng của công nghệ số, trí tuệ nhân tạo, Big Data, Internet vạn vật (IoT) đã thúc đẩy hình thành hệ sinh thái dữ liệu đa tầng, tạo ra cả cơ hội phát triển lẫn thách thức lớn về bảo mật, quyền riêng tư và an ninh quốc gia.

Tuy nhiên, song hành với những lợi ích to lớn, việc xử lý và kinh doanh dữ liệu cũng ẩn chứa nhiều nguy cơ về lợi dụng để xâm phạm các lợi ích trọng yếu của đất nước và cộng đồng. Luật Dữ liệu năm 2024 của Việt Nam (số 60/2024/QH15) lần đầu tiên đưa ra một khung pháp lý tổng quát về quản lý, phát triển và bảo vệ dữ liệu. Để ngăn ngừa các nguy cơ xâm hại dữ liệu, Điều 10 Luật Dữ liệu 2024 đã liệt kê bốn nhóm hành vi bị nghiêm cấm trong hoạt động dữ liệu.

Thứ nhất, hành vi *"lợi dụng việc xử lý dữ liệu, quản trị dữ liệu, phát triển, kinh doanh, lưu hành sản phẩm, dịch vụ về dữ liệu để xâm phạm đến lợi*

ích quốc gia, dân tộc, quốc phòng, an ninh, trật tự, an toàn xã hội, lợi ích công cộng, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân" (Khoản 1). Quy định này mang tính bao quát, nhằm ngăn chặn mọi hành vi sử dụng dữ liệu vào mục đích xấu, gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội hoặc quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

Xét về tính nguy hiểm, hành vi trên đặc biệt nguy hiểm, nguy cơ xâm phạm trực tiếp đối với an ninh quốc gia và lợi ích quốc gia dân tộc. Dữ liệu ngày nay là nguồn lực chiến lược, dữ liệu cốt lõi chứa đựng thông tin về kinh tế, chính trị, quân sự, dân cư, tài nguyên… Nếu bị khai thác sai mục đích, dữ liệu có thể bị sử dụng để hạ uy tín của Đảng, Nhà nước và lực lượng vũ trang, gây bất ổn chính trị, kích động tư tưởng dân tộc hẹp hòi, ly khai, phá hoại khối đại đoàn kết dân tộc, đoàn kết lương - giáo hoặc can thiệp vào quá trình hoạch định chính sách, từ từ phá hoại chế độ từ bên trong. Không chỉ vậy, do thông tin có thể lan tỏa với tốc độ cực nhanh trên không gian mạng, hậu quả do hành vi này gây cực kì khó lường, lan nhanh và kéo dài có thể gây thiệt hại kinh tế, phá vỡ niềm tin xã hội và uy tín quốc gia. Ngoài ra, xuất phát từ tính ẩn danh của dữ liệu, các hoạt động xử lý, khai thác dữ liệu trái phép thường diễn ra tinh vi, thông qua hệ thống công nghệ cao, mạng lưới trung gian phức tạp gây khó khăn cho cơ quan chức năng trong việc phát hiện và xử lý kịp thời.

Có thể kể đến *một số biểu hiện cụ thể* có hành vi này như: ***(i)*** Khai thác dữ liệu để phục vụ hoạt động gián điệp, khủng bố, phá hoại. Đó là thu thập, xử lý dữ liệu về hệ thống quốc phòng, an ninh, kết cấu hạ tầng trọng yếu, hệ thống tài chính - ngân hàng, cơ sở năng lượng, để cung cấp cho tổ chức, cá nhân nước ngoài hoặc nhóm đối tượng chống phá; ***(ii)*** Sử dụng dữ liệu để thao túng dư luận, tấn công truyền thông nhằm gây rối trật tự xã hội. Các đối

tượng phân tích dữ liệu mạng xã hội để lập kế hoạch phát tán thông tin sai sự thật, kích động bạo loạn, biểu tình trái pháp luật, gây chia rẽ khối đại đoàn kết dân tộc, tiền đề xảy ra cách mạng màu tại Việt Nam; ***(iii)*** Kinh doanh, mua bán trái phép dữ liệu cá nhân, dữ liệu quan trọng như rao bán hoặc trao đổi dữ liệu về thông tin cá nhân, hồ sơ sức khỏe, thông tin tài chính, bí mật kinh doanh mà không được sự đồng ý của chủ thể dữ liệu, dẫn tới lừa đảo, chiếm đoạt tài sản; ***(iv)*** Lợi dụng dịch vụ dữ liệu để thực hiện hành vi vi phạm pháp luật như cung cấp sản phẩm, dịch vụ dữ liệu chứa nội dung kích động bạo lực, phân biệt chủng tộc, truyền bá văn hóa phẩm đồi trụy, hoặc hướng dẫn hoạt động phạm tội; ***(v)*** Thao túng thị trường, cạnh tranh không lành mạnh như khai thác dữ liệu về thị trường, khách hàng, đối thủ để phá hoại hoạt động sản xuất - kinh doanh hoặc chiếm đoạt bí mật kinh doanh; ***(vi)*** Chia sẻ dữ liệu cá nhân nhạy cảm mà không được sự đồng ý của chủ thể; ***(vii)*** phát triển các ứng dụng phần mềm trá hình để thu thập thông tin phục vụ cho mục đích bất hợp pháp, hoặc tung ra thị trường các sản phẩm số chứa mã độc, công cụ theo dõi nhằm kiểm soát người dùng.

Hành vi này gây ra hàng loạt hệ lụy nghiêm trọng. Trước hết, nguy cơ rò rỉ thất thoát các thông tin nhạy cảm về quốc phòng, an ninh, tài chính, dân cư, làm tổn hại tới vị thế cạnh tranh và chủ quyền quốc gia. Tiếp theo là việc xâm phạm quyền riêng tư, danh dự, nhân phẩm của cá nhân; xâm phạm quyền tự do kinh doanh, quyền sở hữu trí tuệ của doanh nghiệp; đồng thời gây mất ổn định xã hội, làm xói mòn niềm tin vào môi trường số. Không ít vụ việc cho thấy dữ liệu công dân, dữ liệu hành chính bị thu thập, buôn bán trái phép qua các sàn giao dịch ngầm, gây ra nhiều hiệu quả như lừa đảo tín dụng đen, tấn công mạng, giả mạo danh tính…



Nguy cơ mất an ninh trước các cuộc tấn công APT - Ảnh: VnEconomy

Mục đích của việc quy định cấm hành vi này nhằm đạt được mục tiêu chiến lược về bảo vệ an ninh, chủ quyền và lợi ích quốc gia - dân tộc, ngăn chặn từ sớm, từ xa các hành vi sử dụng dữ liệu để đe dọa nền tảng chính trị, kinh tế, xã hội của đất nước; bảo đảm trật tự, an toàn xã hội và lợi ích công cộng, giữ vững môi trường ổn định để phát triển kinh tế - xã hội, tránh tình trạng dữ liệu bị lợi dụng để gây rối loạn, hỗn loạn xã hội; bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân: Đảm bảo mọi chủ thể được sử dụng dữ liệu một cách an toàn, không bị xâm phạm quyền riêng tư, bí mật kinh doanh hoặc tài sản trí tuệ; Tạo hành lang pháp lý minh bạch cho kinh tế số phục vụ xây dựng môi trường dữ liệu số an toàn, lành mạnh, khuyến khích đổi mới sáng tạo nhưng có kiểm soát, qua đó nâng cao niềm tin của nhà đầu tư, doanh nghiệp và người dân phù hợp với xu thế pháp luật quốc tế hiện nay, hợp tác hiệu quả trong bảo vệ dữ liệu xuyên biên giới.

Về mặt pháp lý, hành vi lợi dụng dữ liệu để xâm phạm lợi ích quốc gia, tổ chức, cá nhân bị nghiêm cấm tuyệt đối. Luật an ninh mạng năm 2018,

Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân cùng các quy định liên quan trong Bộ luật Hình sự năm 2015 (sửa đổi, bổ sung năm 2017) đã xác lập khung pháp lý vững chắc để phòng ngừa, phát hiện và xử lý các vi phạm. Cụ thể, các hình thức xử phạt bao gồm xử phạt hành chính, truy cứu trách nhiệm hình sự, đình chỉ hoạt động, tịch thu tang vật, phương tiện vi phạm, buộc bồi thường thiệt hại, công khai xin lỗi và khôi phục trạng thái ban đầu.

Thực tiễn cho thấy, để phòng ngừa hiệu quả hành vi này, không chỉ cần hoàn thiện khung pháp lý mà còn phải nâng cao nhận thức pháp luật, đạo đức số trong cộng đồng, xây dựng hệ thống kiểm soát, giám sát dữ liệu nhiều lớp; tăng cường hợp tác quốc tế trong trao đổi thông tin, xử lý vi phạm về dữ liệu xuyên biên giới; đồng thời ứng dụng các công nghệ bảo mật, xác thực dữ liệu hiện đại như mã hóa, blockchain, xác thực đa yếu tố… Đặc biệt, các cơ quan quản lý nhà nước, tổ chức chính trị - xã hội, doanh nghiệp và từng cá nhân cần chủ động bảo vệ dữ liệu của mình, không cung cấp hoặc chia sẻ dữ liệu nhạy cảm cho các bên không đáng tin cậy, thường xuyên kiểm tra, rà soát hệ thống và kịp thời báo cáo các dấu hiệu vi phạm.

Có thể khẳng định, việc nghiêm cấm lợi dụng hoạt động dữ liệu để xâm phạm lợi ích chung là giải pháp thiết yếu nhằm bảo vệ chủ quyền số, lợi ích quốc gia, quyền và lợi ích hợp pháp của tổ chức, cá nhân trong thời đại số hóa toàn cầu. Sự minh bạch, liêm chính và trách nhiệm trong quản trị kinh doanh và lưu hành dữ liệu chính là nền tảng vững chắc để phát triển bền vững, giữ vững an ninh và tạo dựng niềm tin cho xã hội số Việt Nam.

Thứ hai, Luật Dữ liệu 2024 nghiêm cấm các hành vi *"cản trở trái pháp luật quá trình xử lý, quản trị dữ liệu, cũng như tấn công, chiếm đoạt hoặc phá hoại cơ sở dữ liệu, hệ thống thông tin về dữ liệu"* (Khoản 2 Điều 10). Trong bối cảnh chuyển đổi số toàn diện và việc ứng dụng công nghệ thông

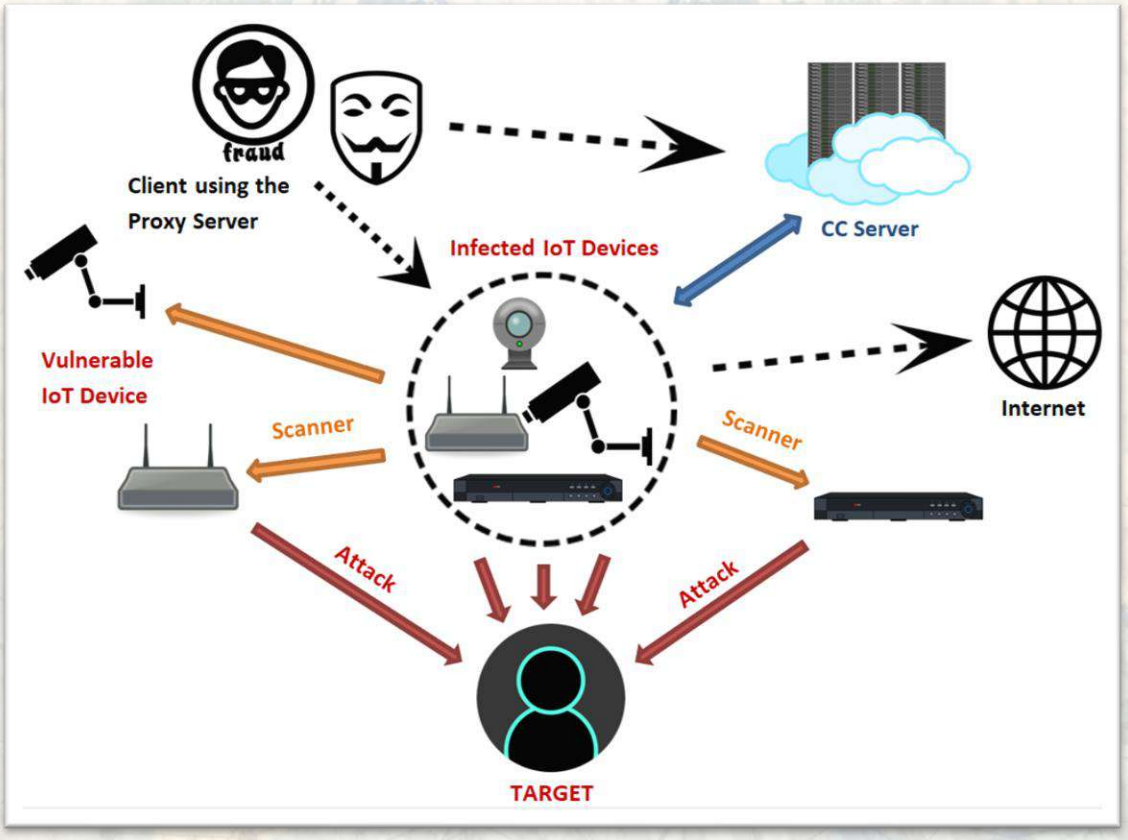
tin vào quản lý Nhà nước, các hoạt động xử lý, lưu trữ và quản trị dữ liệu đóng vai trò sống còn trong mọi lĩnh vực: từ quốc phòng, an ninh, tài chính đến y tế, giáo dục, dịch vụ công. Khi dữ liệu trở thành "hạ tầng mềm" của quốc gia, nguy cơ bị cản trở, phá hoại, chiếm đoạt bởi các chủ thể xấu ngày càng gia tăng cả về mức độ tinh vi lẫn hậu quả để lại. Do đó, quy định này hướng đến việc bảo vệ hạ tầng dữ liệu và hệ thống công nghệ thông tin trước các hành vi xâm nhập, phá hoại.



Hoạt động của các cơ sở dữ liệu cần không chỉ cần được diễn ra bình thường mà còn phải cần được tiến hành có hiệu quả - Ảnh: Internet

Việc cản trở quá trình xử lý, quản trị dữ liệu hoặc tấn công, chiếm đoạt, phá hoại cơ sở dữ liệu và hệ thống thông tin về dữ liệu có một số hình thức cụ thể như: Cản trở việc xử lý, quản lý thông tin trái pháp luật (Tự ý ngắt kết nối hệ thống xử lý dữ liệu, gây đình trệ hoạt động; Từ chối cung cấp quyền truy cập dữ liệu khi có yêu cầu hợp pháp từ cơ quan có thẩm quyền; Sử dụng phần mềm hoặc công cụ kỹ thuật để làm chậm, sai lệch hoặc vô hiệu hóa hoạt động xử lý dữ liệu…); Tấn công, xâm nhập trái phép hệ thống dữ liệu (Thực hiện

hành vi tấn công mạng (DDoS, phishing, malware…) vào hệ thống lưu trữ hoặc xử lý dữ liệu; Truy cập trái phép vào cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành hoặc hệ thống thông tin của cơ quan, tổ chức để đánh cắp thông tin); Chiếm đoạt hoặc phá hoại dữ liệu, hệ thống thông tin về dữ liệu (Xóa, sửa, mã hóa dữ liệu để đòi tiền chuộc (ransomware); Phá hoại hạ tầng kỹ thuật (máy chủ, thiết bị lưu trữ) hoặc phá vỡ cấu trúc phần mềm quản trị dữ liệu; Lợi dụng quyền quản trị hệ thống để chuyển dữ liệu ra ngoài, chiếm đoạt quyền sở hữu hoặc kiểm soát dữ liệu…); hoặc thao túng hệ thống dữ liệu quản lý dân cư, thuế, tài chính, quốc phòng… Các hành vi này không chỉ gây thiệt hại vật chất (gián đoạn dịch vụ, mất dữ liệu, thiệt hại tài chính, tiêu tốn nguồn lực khắc phục) mà còn tác động nghiêm trọng đến an ninh quốc gia, lợi ích xã hội, có thể dẫn đến những thảm họa nên không lường trước.



Cách thức tấn công của Botnet Mirai - Ảnh: Fortinet

Thực tiễn tại nước ta cũng như thế giới ghi nhận nhiều trường hợp các hệ thống thông tin trọng yếu bị tấn công hoặc gián đoạn, như vụ tấn công vào hệ thống hàng không, ngân hàng, cơ sở dữ liệu quản lý tiêm chủng, y tế trong thời gian đại dịch COVID-19,… Không ít vụ việc có nguồn gốc từ các tổ chức tội phạm mạng quốc tế, cho thấy nguy cơ xuyên quốc gia của loại tội phạm này. Theo đó, những biểu hiện trên là mối đe dọa trực tiếp đến an ninh mạng và an toàn dữ liệu, chỉ một cuộc tấn công hoặc phá hoại thành công cũng có thể làm tê liệt hệ thống thông tin quốc gia, gây gián đoạn hoạt động của Chính phủ, doanh nghiệp và dịch vụ công thiết yếu, kéo theo thiệt hại kinh tế khổng lồ và hậu quả xã hội sâu rộng. Nguy hiểm hơn, nhiều cơ sở dữ liệu chứa thông tin gốc hoặc dữ liệu quan trọng liên quan tới quốc phòng, an ninh, kinh tế, dân cư; khi bị chiếm đoạt hoặc phá hoại, không chỉ khó khôi phục toàn vẹn mà còn có thể bị lợi dụng để thao túng, phá hoại từ xa.

Trong bối cảnh chuyển đổi số toàn diện, hạ tầng dữ liệu trở thành *"huyết mạch"* của quốc gia, mọi hành vi xâm hại đều tiềm ẩn khả năng gây rối loạn diện rộng, làm suy giảm niềm tin của người dân và cộng đồng quốc tế vào năng lực bảo vệ dữ liệu, ảnh hưởng trực tiếp tới chủ quyền số và an ninh quốc gia. Hiện nay, Bộ Luật hình sự 2015 sửa đổi, bổ sung năm 2017 cũng đã có những quy định về các tội có liên quan đến hành vi này như: Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 287); Tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác (Điều 289); Tội đưa hoặc sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông (Điều 288) và Tội phá hoại cơ sở vật chất - kỹ thuật của mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 294). Đối với các cá nhân, tổ chức vi phạm các quy định trên đều có thể sẽ đối mặt với hình phạt tù cùng với hình phạt bổ sung là

cấm đảm nhiệm chức vụ, hành nghề hoặc làm công việc liên quan đến công nghệ thông tin từ 01 đến 05 năm. Tuy nhiên, ngoài các biện pháp, chế tài nêu trên cần có quy định chặt chẽ hơn trong xử phạt vi phạm hành chính đối với các hành vi khác để bảo đảm phòng ngừa; nâng cao hiệu quả công tác ngăn chặn, tố giác các hành vi cản trở, phá hoại, tấn công dữ liệu; góp phần xây dựng môi trường số an toàn, lành mạnh và bền vững.

Thứ ba, Luật nghiên cấm hành vi *"giả mạo, làm sai lệch, làm mất hoặc làm hư hỏng dữ liệu trong các cơ sở dữ liệu của cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc và các tổ chức chính trị - xã hội"*.

Đây là quy định nhằm bảo vệ sự chính xác và toàn vẹn của dữ liệu công do các cơ quan công quyền quản lý. Trong thời đại chuyển đổi số mạnh mẽ, dữ liệu trở thành nền tảng quan trọng để vận hành toàn bộ hệ thống quản trị quốc gia. Dữ liệu của các Đảng, Nhà nước, Mặt trận Tổ quốc và các tổ chức chính trị - xã hội không chỉ phản ánh lịch sử, thành tích, cấu trúc tổ chức mà còn là căn cứ quan trọng cho việc hoạch định chính sách, quản lý nhân sự, giám sát quyền lực và thực thi pháp luật. Chính vì thế, tính toàn vẹn, khách quan, trung thực của dữ liệu được đặt lên hàng đầu. Khi dữ liệu bị giả mạo, sai lệch, làm mất hoặc hư hỏng, nguy cơ đe dọa không chỉ dừng lại ở phạm vi một cơ quan, tổ chức mà có thể lan rộng, gây hậu quả lâu dài cho xã hội và đất nước.

Về động cơ, hành vi giả mạo dữ liệu có thể xuất phát từ nhiều động cơ khác nhau: trục lợi cá nhân, che giấu sai phạm, phục vụ lợi ích nhóm hoặc thậm chí là phá hoại có chủ đích từ các thế lực thù địch. Điển hình như trường hợp làm giả hồ sơ lý lịch, văn bằng, giấy tờ nhân sự để hợp thức hóa việc tuyển dụng, đề bạt, bổ nhiệm sai quy trình; hoặc tạo các hợp đồng giả để rút ngắn ngân sách, trục lợi chính sách xã hội. Ở cấp độ

nghiêm trọng hơn, việc chỉnh sửa, làm sai lệch dữ liệu tài sản công, dữ liệu tài chính hoặc dữ liệu dân cư có thể mở đường cho tham nhũng, thất thoát lớn tài sản quốc gia. Sự phát triển của công nghệ thông tin khiến cho các hành vi này ngày càng tinh vi, khó kiểm soát hơn, thậm chí có thể được thực hiện từ xa hoặc thông qua các phần mềm độc hại mà cơ quan chủ quản không phát hiện kịp thời.

Ngoài việc giả mạo, việc cố ý làm sai lệch dữ liệu nhằm che đậy sai phạm, nâng cao thành tích và chuyển hóa thất bại thành thành công cũng rất phổ biến. Đây là một trong những nguyên nhân sâu xa gây bệnh thành tích trong quản lý công, khiến các số liệu báo cáo không còn phản ánh đúng thực trạng, dẫn tới chính sách điều hành thiếu hiệu quả, lãng phí nguồn lực quốc gia. Không dừng lại ở đó, một số đối tượng còn có hành vi xóa, phá hủy, làm mất hoặc làm hư hỏng dữ liệu với mục đích gây rối loạn hoạt động của cơ quan, che giấu dấu vết tội phạm, hoặc để trả thù, cạnh tranh không lành mạnh giữa các tổ chức, cá nhân. Những hậu quả kéo theo là mất mát thông tin quan trọng, gián đoạn hoạt động hành chính, ảnh hưởng đến quyền lợi của người dân và doanh nghiệp.

Một số biểu hiện của hành vi này có thể kể đến như: Giả mạo hồ sơ dữ liệu - tạo lập dữ liệu giả mạo trong cơ sở dữ liệu dân cư, cơ sở dữ liệu đảng viên, hoặc các cơ sở dữ liệu hành chính khác nhằm trục lợi hoặc phục vụ mục đích xấu, hành vi này tương tự hành vi "làm giả tài liệu, con dấu" nhưng mở rộng ra môi trường số; Cố ý làm sai lệch nội dung - Sửa đổi thông tin trong hồ sơ quản lý đất đai, đăng ký kinh doanh, tài chính ngân sách, dẫn đến thay đổi quyền lợi hoặc nghĩa vụ của tổ chức, cá nhân; Xóa, làm mất dữ liệu quan trọng - Xóa dữ liệu quản lý nhân sự, dữ liệu hồ sơ cán bộ, dữ liệu kết quả thi cử… để che giấu vi phạm hoặc gây rối loạn quản lý; Làm hư hỏng

dữ liệu - Cài mã độc, virus hoặc thao tác kỹ thuật khiến dữ liệu bị hỏng, không thể truy xuất hoặc sử dụng.



Chuyên gia cảnh báo tình trạng giả mạo cơ quan nhà nước - Ảnh: VOV

Trên phương diện hậu quả, hành vi này là mối nguy lớn đối với xã hội. Theo chuẩn quốc tế về an toàn thông tin (ISO/IEC 27001), tính toàn vẹn là một trong ba trụ cột của nguyên tắc CIA (Confidentiality - Integrity - Availability), là yếu tố nền tảng đảm bảo dữ liệu không bị sửa đổi trái phép từ khi tạo lập cho đến khi sử dụng. Hậu quả của việc làm sai lệch dữ liệu công là rất nghiêm trọng, đầu tiên, có thể dẫn tới ra quyết định sai lầm, quản trị kém hiệu quả và thất thoát ngân sách. Không chỉ vậy, khi tính toàn vẹn dữ liệu bị ảnh hưởng, niềm tin của công dân vào khả năng Nhà nước quản trị minh bạch và hiệu quả sẽ bị suy giảm, làm phai nhạt mối liên kết xã hội và tăng nguy cơ hỗn loạn xã hội[200]. Bên cạnh đó, hành vi này là một

[200] Schmidthuber, L., Willems, J., & Krabina, B (2023), *Trust in public performance information: The effect of data accessibility and data source,* Public Administration Review. https://doi.org/10.1111/puar.13603, Truy cập ngày 01/8/2025.

trong những nguy cơ xâm phạm an ninh phi truyền thống về thông tin và dữ liệu, mặc dù không hủy hoại về cơ sở vật chất ngay lập tức nhưng có thể phá vỡ nền tảng vận hành của hệ thống chính trị - xã hội.

Về mặt pháp lý, đây là nhóm hành vi bị xử lý rất nghiêm khắc. Bộ luật Hình sự đã quy định các cụ thể các tội danh liên quan như Tội xâm nhập trái phép vào mạng máy tính mạng, mạng viễn thông; Tội cản trở hoặc gây rối loạn hoạt động của hệ thống thông tin; Tội sửa chữa, làm sai lệch nội dung thông tin của người khác; Tội hủy hoại hoặc cố ý làm hư hỏng thiết bị, phương tiện lưu trữ thông tin. Hình phạt có thể lên tới nhiều năm tù, phạt tiền, tịch thu tài sản, cấm đảm nhiệm chức vụ hoặc cấm hành nghề trong một thời hạn nhất định, đồng thời yêu cầu bồi thường thiệt hại vật chất, tinh thần do hành vi vi phạm gây ra. Ngoài ra, các quy định về xử lý kỷ luật, trách nhiệm công vụ và trách nhiệm dân sự cũng được áp dụng song song nhằm đảm bảo tính răn đe, giáo dục và phòng ngừa chung.

Từ góc độ quản trị, các cơ quan, tổ chức cần xây dựng quy trình kiểm tra, giám sát, đánh giá an toàn dữ liệu một cách thường xuyên, sử dụng các giải pháp công nghệ hiện đại như blockchain, lưu vết lịch sử chỉnh sửa dữ liệu, phân quyền truy cập rõ ràng và mã hóa thông tin nhạy cảm. Việc đào tạo, nâng cao nhận thức về đạo đức nghề nghiệp và trách nhiệm pháp lý cho cán bộ, công chức, viên chức là yếu tố then chốt để phòng ngừa vi phạm ngay từ bên trong. Song song đó, việc khuyến khích, bảo vệ những người phát hiện, tố giác các hành vi giả mạo, sai lệch, phá hoại dữ liệu cũng là biện pháp quan trọng giúp xã hội đồng lòng bảo vệ hệ thống dữ liệu quốc gia.

Cuối cùng, cần khẳng định rằng bảo vệ sự toàn vẹn, trung thực của dữ liệu công chính là bảo vệ trật tự, kỷ cương, hiệu lực pháp luật, đồng thời giữ vững niềm tin của nhân dân vào bộ máy nhà nước và hệ thống chính

trị. Chỉ khi các dữ liệu được bảo vệ an toàn, công bằng, khách quan, nền quản trị quốc gia mới thực sự phát triển bền vững, minh bạch và hiện đại.



Các đối tượng lợi dụng phần mềm Deepfake để giả mạo giọng nói, khuôn mặt để lừa đảo tài sản - Ảnh: VnEconomy

Thứ tư, Luật Dữ liệu 2024 nghiêm cấm hành vi *"cố ý cung cấp dữ liệu sai lệch hoặc không cung cấp dữ liệu theo quy định của pháp luật"* (Khoản 4 Điều 10).

Trong xã hội hiện đại, nơi dữ liệu là cơ sở để các cơ quan quản lý nhà nước, tổ chức xã hội và doanh nghiệp hoạch định chính sách, triển khai hoạt động, cũng như bảo đảm quyền và lợi ích hợp pháp của cá nhân, cộng đồng. Việc cung cấp dữ liệu một cách chính xác, đầy đủ, kịp thời theo quy định pháp luật không chỉ là trách nhiệm pháp lý mà còn là nghĩa vụ đạo đức của mỗi cá nhân, tổ chức đối với xã hội. Tuy nhiên, trên thực tế, hành vi cố ý cung cấp dữ liệu sai lệch hoặc từ chối cung cấp dữ liệu - dù do động cơ trục lợi, che giấu sai phạm, hay né tránh trách nhiệm vẫn diễn ra khá phổ biến và

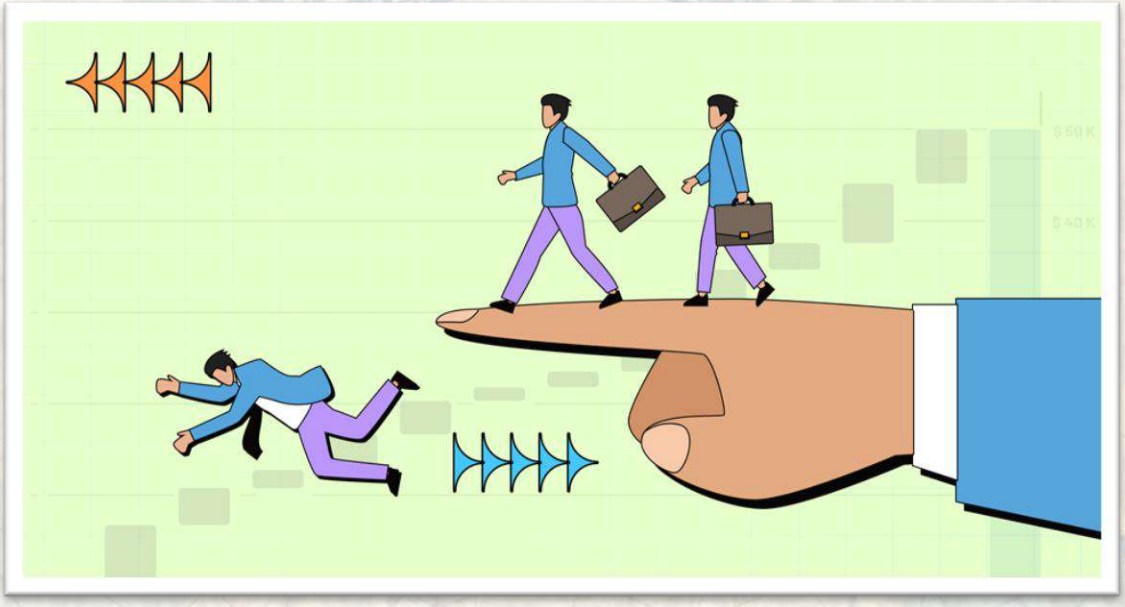
để lại hậu quả nghiêm trọng cho sự phát triển của xã hội, nền kinh tế cũng như sự ổn định của bộ máy quản trị nhà nước.

Có thể kể đến những trường hợp doanh nghiệp cố tình báo cáo sai số liệu thuế, khai gian doanh thu hoặc che giấu nợ xấu nhằm tránh nghĩa vụ tài chính đối với nhà nước. Ở lĩnh vực lao động, không ít doanh nghiệp không cung cấp hoặc khai sai dữ liệu về hợp đồng lao động, lương, số lượng lao động nhằm trốn tránh đóng bảo hiểm xã hội, bảo hiểm y tế, bảo hiểm thất nghiệp cho người lao động. Cá nhân cũng có thể cố ý khai man thông tin khi làm thủ tục hưởng các chính sách an sinh xã hội, đăng ký học tập, thi cử hoặc xin cấp các loại giấy tờ, bằng cấp. Ở cấp độ nhà nước, một số cán bộ, công chức vì động cơ vụ lợi hoặc sợ bị xử lý kỷ luật mà báo cáo sai lệch, không đầy đủ về tình hình thực tế - từ đó dẫn đến quyết sách sai lầm, lãng phí nguồn lực, thậm chí tiếp tay cho tham nhũng, tiêu cực nảy sinh.

Về hậu quả, cố ý cung cấp dữ liệu sai lệch hoặc không cung cấp dữ liệu theo quy định pháp luật là hành vi trực tiếp xâm hại tính chính xác và tính đầy đủ của hệ thống dữ liệu, vốn là cơ sở cho việc hoạch định chính sách, quản lý nhà nước và ra quyết định của cơ quan hoạch định chính sách. Trong bối cảnh quản trị dựa trên dữ liệu, khi dữ liệu đầu vào không đúng, các phân tích, dự báo, hoạch định chính sách sẽ dựa trên nền tảng sai lầm, kéo theo nhiều quyết định sai, gây thất thoát tài sản công, triệt tiêu động lực đổi mới sáng tạo, giảm hiệu quả thực thi pháp luật và suy giảm lòng tin xã hội. Không chỉ vậy, hành vi cố ý cung cấp dữ liệu sai lệch hay từ chối cung cấp dữ liệu không chỉ làm mất đi tính khách quan, minh bạch trong quản lý nhà nước, mà còn ảnh hưởng trực tiếp tới quyền lợi chính đáng của người dân, doanh nghiệp và toàn xã hội. Đặc biệt, trong các lĩnh vực nhạy cảm như y tế, giáo dục, tài chính, đất đai…, hậu quả do

dữ liệu sai lệch còn có thể gây ra bất bình đẳng, tranh chấp, khiếu kiện kéo dài và ảnh hưởng tới an sinh xã hội. Nguy hiểm hơn, hành vi này có thể được lợi dụng để che giấu vi phạm, tham ô, tham nhũng, thao túng thông tin hoặc phục vụ mục đích chống phá khác.

Một số biểu hiện cụ thể của hành vi này có thể kể đến, như: Báo cáo số liệu không đúng sự thật, doanh nghiệp cố ý khai báo sai dữ liệu về sản xuất, kinh doanh để trốn thuế hoặc nhận ưu đãi không hợp pháp; Không cung cấp dữ liệu khi pháp luật yêu cầu, cơ quan, tổ chức, cá nhân không gửi dữ liệu thống kê, báo cáo hoặc thông tin bắt buộc theo quy định, cản trở quá trình giám sát, quản lý; Cung cấp dữ liệu giả mạo như nhập thông tin sai về nhân thân, tình trạng pháp lý, tình trạng tài sản vào hệ thống dữ liệu để trục lợi hoặc hợp thức hóa hành vi vi phạm; Chậm trễ hoặc cố tình trì hoãn việc cung cấp dữ liệu nhằm gây khó khăn cho công tác quản lý hoặc điều tra...



Nguyên tắc "no false or misleading data" - Ảnh: Ninja Tables

Quy định này nhằm đảm bảo cho các kho dữ liệu dùng chung của Nhà nước được đầy đủ, chính xác, đồng thời ngăn chặn tình trạng cung cấp thông tin sai để trục lợi hoặc che giấu vi phạm. Có thể thấy, khoản cấm này bổ sung

cho chế tài về báo cáo thống kê, báo cáo dữ liệu trong nhiều lĩnh vực, yêu cầu các bên phải trung thực và tuân thủ quy định khi chia sẻ dữ liệu, phù hợp với thông lệ quốc tế về nguyên tắc "tính chính xác và đầy đủ" (Khoản 1 Điều 5, GDPR) và nguyên tắc *"no false or misleading data"* trong nhiều luật dữ liệu quốc gia khác.

Về mặt pháp lý, hành vi cung cấp dữ liệu sai lệch hoặc không cung cấp dữ liệu theo quy định đã được nhiều văn bản luật quy định xử lý nghiêm khắc. Bộ luật Hình sự năm 2015 (sửa đổi bổ sung năm 2017) quy định nhiều tội danh liên quan như tội làm giả con dấu, tài liệu, tội khai báo gian dối, tội trốn thuế, tội che giấu tội phạm… Ngoài ra, các luật chuyên ngành như Luật Kế toán, Luật Doanh nghiệp, Luật Bảo hiểm xã hội, Luật Thống kê, Luật Đất đai, Luật Quản lý thuế, Luật Cư trú… đều có quy định chế tài đối với cá nhân, tổ chức cố tình cung cấp thông tin sai hoặc không cung cấp thông tin theo yêu cầu quản lý. Hình thức xử phạt gồm phạt tiền, truy thu các khoản lợi bất hợp pháp, buộc khôi phục trạng thái ban đầu, thậm chí truy cứu trách nhiệm hình sự, cấm đảm nhiệm chức vụ, hành nghề trong một thời gian nhất định.

Để phòng ngừa và ngăn chặn hành vi này, giải pháp hiệu quả là xây dựng hệ thống quản lý dữ liệu đồng bộ, số hóa, minh bạch và dễ dàng kiểm tra, đối chiếu liên ngành; đồng thời, tăng cường trách nhiệm giải trình của cán bộ, công chức, doanh nghiệp, cá nhân khi cung cấp dữ liệu. Vai trò của truyền thông, kiểm toán xã hội, sự giám sát của các tổ chức xã hội và cơ chế tố cáo, bảo vệ người tố giác hành vi vi phạm cũng cần được phát huy mạnh mẽ. Việc áp dụng công nghệ mới như blockchain, trí tuệ nhân tạo vào quản lý và kiểm tra dữ liệu sẽ tạo ra "hàng rào" kỹ thuật ngăn ngừa, phát hiện kịp thời các sai phạm, nâng cao chất lượng dữ liệu phục vụ công tác quản lý và phát triển xã hội.

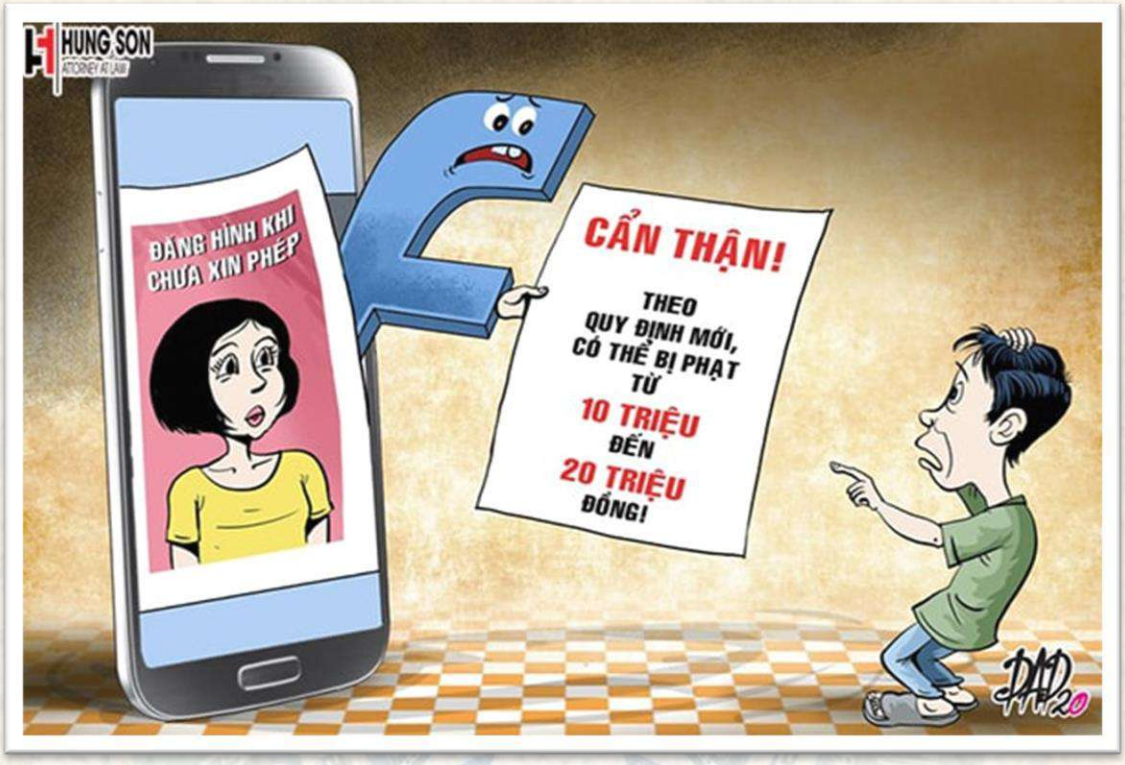
Có thể khẳng định, việc nghiêm cấm và xử lý nghiêm hành vi cố ý cung cấp dữ liệu sai lệch hoặc không cung cấp dữ liệu theo quy định là cơ sở để bảo đảm hiệu lực, hiệu quả của nền quản lý nhà nước hiện đại, tạo dựng môi trường kinh doanh lành mạnh, bảo vệ quyền lợi chính đáng của từng người dân, doanh nghiệp, đồng thời giữ vững niềm tin của xã hội vào pháp luật và công lý.

Như vậy, bốn nhóm hành vi cấm kể trên cho thấy Luật Dữ liệu 2024 tập trung bảo vệ hai khía cạnh chính: ***(i)*** bảo vệ lợi ích an ninh quốc gia, trật tự an toàn xã hội và quyền hợp pháp của tổ chức, cá nhân trước sự lạm dụng dữ liệu; ***(ii)*** bảo vệ tính toàn vẹn, chính xác và an toàn của các hệ thống dữ liệu, đặc biệt là dữ liệu do nhà nước quản lý.

So với các đạo luật nước ngoài, các hành vi bị cấm của Luật Dữ liệu Việt Nam có nét tương đồng khi đặt trọng tâm vào chống lợi dụng dữ liệu gây hại (giống quy định của EU và Trung Quốc về cấm xử lý dữ liệu xâm hại an ninh, lợi ích công cộng) và chống tấn công, phá hoại dữ liệu (giống luật nhiều nước về an ninh mạng). Tuy nhiên, phạm vi Luật Dữ liệu 2024 không đi sâu vào dữ liệu cá nhân (vốn được điều chỉnh chuyên biệt bởi Nghị định 13/2023/NĐ-CP và Luật Bảo vệ Dữ liệu cá nhân 2025), mà hướng tới quản lý tổng thể tài nguyên dữ liệu quốc gia và hoạt động dữ liệu của các tổ chức công lẫn tư.

Chính vì vậy, các hành vi như mua bán dữ liệu cá nhân trái phép tuy không được liệt kê trực tiếp trong Luật Dữ liệu, nhưng đã được điều chỉnh tại văn bản pháp luật khác - cụ thể Luật Bảo vệ Dữ liệu Cá nhân cấm tuyệt đối việc mua bán dữ liệu cá nhân dưới mọi hình thức. Như vậy, bộ khung pháp lý về dữ liệu của Việt Nam có sự phân định rõ ràng: Luật Dữ liệu 2024 định ra các hành vi cấm mang tính bao quát về quản lý, khai thác dữ liệu nói chung, còn pháp luật chuyên ngành về dữ liệu cá nhân sẽ cấm chi tiết

các hành vi xâm phạm riêng tư, mua bán dữ liệu cá nhân. Sự kết hợp này tạo nên hệ thống chế tài tương đối đầy đủ nhằm phòng chống các vi phạm trong lĩnh vực dữ liệu ở Việt Nam.



Cần phải cẩn trọng trước khi đăng tải thông tin cá nhân lên không gian mạng - Ảnh: CTU

3.3. MỘT SỐ HẠN CHẾ, VƯỚNG MẮC TRONG QUY ĐỊNH CỦA PHÁP LUẬT VỀ XỬ LÝ VI PHẠM HÀNH CHÍNH VỀ DỮ LIỆU TẠI VIỆT NAM

Ở Việt Nam, việc xử lý vi phạm hành chính liên quan đến dữ liệu chủ yếu được điều chỉnh thông qua các văn bản pháp luật chung và các văn bản dưới luật. Điển hình, Luật Dữ liệu 2024 đã liệt kê ***04 nhóm hành vi bị nghiêm cấm*** trong khai thác, quản lý dữ liệu. Tuy nhiên, hiện chưa quy định trực tiếp chế tài xử phạt hành chính đối với các hành vi vi phạm đó. Thay vào đó, việc xử lý vi phạm thường áp dụng Luật Xử lý vi phạm hành chính 2012 sửa đổi, bổ sung năm 2020, 2024 gần nhất là sửa đổi,

bổ sung vào năm 2025 có hiệu lực từ ngày 01/7/2025 và các nghị định liên quan như: ***(1)*** Nghị định 118/2021/NĐ-CP ngày 23/12/2021 sửa đổi, bổ sung một số điều bởi Nghị định số 120/2021/NĐ-CP ngày 24/12/2021, Nghị định số 68/2025/NĐ-CP ngày 18/4/2025 và gần nhất là Nghị định 190/2025/NĐ-CP ngày 01/7/2025 *"quy định chi tiết một số điều và biện pháp thi hành Luật xử lý vi phạm hành chính"*; ***(2)*** Nghị định 15/2020/NĐ-CP ngày 03/02/2020 sửa đổi, bổ sung tại Nghị định số 14/2022/NĐ-CP ngày 21/01/2022 của Chính phủ về *"xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, công nghệ thông tin và giao dịch điện tử"*, Nghị định 144/2021/NĐ-CP ngày 31/12/2021 về *"quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh, trật tự, an toàn xã hội; phòng chống tệ nạn xã hội; phòng cháy, chữa cháy; cứu nạn cứu hộ; phòng chống bạo lực gia đình"*.

Một trong các văn bản quan trọng là Nghị định 15/2020/NĐ-CP ngày 03/02/2020 sửa đổi, bổ sung tại Nghị định số 14/2022/NĐ-CP ngày 21/01/2022 của Chính phủ[201]. Theo đó, các hành vi vi phạm về dữ liệu cá nhân và an toàn thông tin mạng bước đầu đã có những hành vi xử lý cụ thể (từ đều 84 đến Điều 93). Điển hình, Điều 84 Nghị định trên quy định phạt tiền từ 10 đến 20 triệu đồng đối với hành vi *"Thu thập thông tin cá nhân khi chưa có sự đồng ý của chủ thể thông tin cá nhân về phạm vi, mục đích của việc thu thập và sử dụng thông tin đó; Cung cấp thông tin cá nhân cho bên thứ ba khi chủ thể thông tin cá nhân đã yêu cầu ngừng cung cấp"* (Khoản 1).

Hành vi *"sử dụng không đúng mục đích thông tin cá nhân đã thỏa thuận khi thu thập hoặc khi chưa có sự đồng ý của chủ thể thông tin cá nhân; Cung cấp hoặc chia sẻ hoặc phát tán thông tin cá nhân đã thu thập, tiếp cận, kiểm*

[201] Bộ Thông tin và Truyền thông (2022), *Văn bản hợp nhất số 08/VBHN-BTTTT của Bộ Thông tin và Truyền thông về xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử,* Thư viện pháp luật.

soát cho bên thứ ba khi chưa có sự đồng ý của chủ thông tin cá nhân và Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác" bị phạt từ 40 đến 60 triệu đồng (Khoản 2), Nghị định cũng quy định biện pháp khắc phục hậu quả như buộc hủy bỏ thông tin cá nhân do vi phạm. Ngoài ra, Nghị định 15/2020 còn quy định mức phạt tương tự đối với hành vi vi phạm quy định về cập nhật, sửa đổi và hủy bỏ thông tin cá nhân (Điều 85); vi phạm quy chuẩn kỹ thuật về an toàn thông tin mạng (Điều 86). Các quy định này thể hiện nỗ lực pháp lý xử lý vi phạm liên quan dữ liệu, chủ yếu từ góc độ bảo vệ thông tin cá nhân và an toàn hệ thống thông tin.



Hành vi thu thập trái phép thông tin cá nhân bị pháp luật nghiêm cấm - Ảnh: Thư viện pháp luật

Bên cạnh đó, Điều 22 Nghị định 144/2021/NĐ-CP ngày 31/12/2021 cũng có quy định xử phạt vi phạm hành chính đối với hành vi vi phạm quy định về xây dựng, quản lý, sử dụng Cơ sở dữ liệu quốc gia về dân cư, Cơ sở dữ liệu về cư trú, Cơ sở dữ liệu Căn cước công dân, như: Làm sai lệch sổ

sách, hồ sơ, giấy tờ, tài liệu, dữ liệu và thông tin công dân; Khai thác, sử dụng dữ liệu, thông tin về công dân trong trong các cơ sở dữ liệu trên nhưng không được sự đồng ý của chủ thể dữ liệu; Cản trở hoặc ngăn chặn, làm gián đoạn hoạt động quá trình truyền, gửi, nhận dữ liệu...

Mặc dù khung pháp luật về xử lý vi phạm hành chính trên lĩnh vực dữ liệu của Việt Nam đã bước đầu hoàn thiện, tuy nhiên, trên thực tế vẫn tồn tại một số hạn chế và vướng mắc cần được nhìn nhận để tiếp tục điều chỉnh.

Thứ nhất, có sự chồng chéo và phân tán giữa các văn bản pháp luật điều chỉnh về dữ liệu. Hiện nay, việc xử lý vi phạm hành chính trên lĩnh vực dữ liệu chịu sự điều chỉnh bởi nhiều luật khác nhau: Luật An toàn thông tin mạng 2015, Luật An ninh mạng 2018, Nghị định 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân, Luật xử lý vi phạm hành chính 2012 sửa đổi, bổ sung năm 2020, các nghị định có liên quan và gần nhất là Luật Dữ liệu 2024 cùng dự kiến Luật Bảo vệ Dữ liệu Cá nhân (2025). Sự phân tán này dẫn đến nguy cơ chồng chéo hoặc bỏ sót trong quy định, điều này đòi hỏi người áp dụng luật phải phối hợp nhiều văn bản, nếu không sẽ lúng túng xác định chế tài. Ngoài ra, một số khái niệm cốt lõi vẫn chưa được định nghĩa đồng bộ giữa các luật. Chẳng hạn phân loại *"dữ liệu cá nhân"* và *"dữ liệu phi cá nhân"* - có thể dẫn đến cách hiểu khác nhau. Hạn chế này đòi hỏi sự hướng dẫn chi tiết hơn từ Quốc hội hoặc Chính phủ để đảm bảo các luật về dữ liệu được thống nhất, không mâu thuẫn khi áp dụng.

Thứ hai, mức xử phạt hiện tại tương đối thấp, chủ yếu tính theo mức tiền cố định (triệu đồng), chưa đảm bảo răn đe với các tổ chức lớn. Bên cạnh đó, trách nhiệm và thẩm quyền xử lý còn chưa rõ ràng. Chưa có cơ quan chuyên trách duy nhất phụ trách xử lý hành chính về dữ liệu; việc phối hợp giữa các bộ, ngành chưa đồng bộ.

Thứ ba, sự phối hợp của các cơ quan quản lý dữ liệu còn bất cập. Luật Dữ liệu 2024 giao Bộ Công an là cơ quan chủ trì quản lý nhà nước về dữ liệu (trừ dữ liệu do Bộ Quốc phòng quản lý). Vì chưa có một cơ sở dữ liệu tổng hợp, sự phối hợp giữa Bộ Công an với Bộ Thông tin & Truyền thông, Bộ Tư pháp và các cơ quan khác trong quản lý dữ liệu sẽ phức tạp, bởi dữ liệu là lĩnh vực liên ngành. Nếu không có cơ chế phối hợp thông suốt, doanh nghiệp có thể phải báo cáo nhiều nơi, hoặc có tình huống *"trống đánh xuôi, kèn thổi ngược"* trong thực thi pháp luật về dữ liệu. Đây là hạn chế về mặt thể chế thực thi cần sớm khắc phục bằng cách quy định rạch ròi chức năng từng cơ quan và thiết lập cơ chế liên thông khi xử lý vi phạm.

Thứ tư, nhìn vào chế tài xử lý vi phạm dữ liệu hiện nay, vẫn còn khoảng trống về quy định xử phạt vi phạm hành chính đối với một số hành vi mới. Luật Dữ liệu 2024 có hiệu lực từ 01/7/2025, do đó các nghị định xử phạt vi phạm hành chính tương ứng cần được ban hành kịp thời. Hiện tại, các hành vi vi phạm về thông tin, an ninh mạng thường được xử phạt theo Nghị định 15/2020/NĐ-CP hoặc Nghị định 14/2022/NĐ-CP. Tuy nhiên, những nghị định này chưa bao quát đầy đủ các hành vi vi phạm mới trong Luật Dữ liệu (như hành vi vi phạm quy định về chuyển dữ liệu xuyên biên giới). Nếu không sớm bổ sung quy định, khi luật có hiệu lực sẽ thiếu cơ sở để xử phạt nhiều vi phạm. Bên cạnh đó, Luật Bảo vệ Dữ liệu Cá nhân cũng đặt ra khung phạt rất nghiêm khắc (phạt tiền đến 5% doanh thu đối với vi phạm chuyển dữ liệu cá nhân ra nước ngoài, và đến 3 tỷ đồng với vi phạm khác), trong khi Luật Dữ liệu 2024 chưa có quy định cụ thể về mức phạt cho vi phạm tương ứng trong lĩnh vực dữ liệu phi cá nhân. Sự chênh lệch này có thể tạo ra bất hợp lý: vi phạm dữ liệu cá nhân bị phạt nặng, nhưng vi phạm dữ liệu khác (ví dụ dữ liệu doanh nghiệp, dữ liệu bí mật kinh doanh) có khi lại chưa có

chế tài đủ mạnh. Đây là hạn chế cần sớm được khắc phục bằng việc ban hành nghị định xử phạt riêng cho lĩnh vực dữ liệu, bảo đảm mọi hành vi vi phạm đều có mức xử phạt tương xứng với tính chất và hậu quả. Tóm lại, các hạn chế chủ yếu trong pháp luật về xử lí vi phạm hành chính về dữ liệu hiện hành của Việt Nam nằm ở khâu cụ thể hóa và thực thi. Luật mới đề ra nguyên tắc nhưng cần hướng dẫn rõ để thống nhất hiểu và dễ tuân thủ; đồng thời, bộ máy thực thi cần được kiện toàn, tránh chồng chéo và lấp đầy những "khoảng trống" về chế tài. Nhận diện được các vướng mắc này là tiền đề để đề ra các giải pháp hoàn thiện hiệu quả.

3.4. MỘT SỐ GIẢI PHÁP HOÀN THIỆN QUY ĐỊNH PHÁP LUẬT VỀ XỬ LÝ VI PHẠM HÀNH CHÍNH TRONG LĨNH VỰC DỮ LIỆU

Để khắc phục những hạn chế nêu trên và nâng cao hiệu lực của pháp luật về dữ liệu, cần triển khai một loạt giải pháp đồng bộ nhằm hoàn thiện quy định pháp luật về xử lý vi phạm hành chính trong lĩnh vực dữ liệu.

3.4.1. Nghiên cứu, xây dựng quy định của pháp luật về xử lý vi phạm hành chính trong lĩnh vực dữ liệu theo hướng bổ sung vào Luật Xử lý vi phạm hành chính các quy định liên quan đến xử lý vi phạm hành chính trong lĩnh vực dữ liệu; trên cơ sở đó, nghiên cứu, xây dựng Nghị định của Chính phủ quy định về xử phạt vi phạm hành chính trong lĩnh vực dữ liệu.

Dưới góc độ lập pháp, việc bổ sung quy định về xử lý vi phạm hành chính trong lĩnh vực dữ liệu vào Luật Xử lý vi phạm hành chính, đồng thời ban hành một nghị định chuyên ngành, là yêu cầu cấp thiết và hợp lý. Điều này nhằm bảo đảm tính hợp pháp của chế tài, bởi Luật Xử lý Vi phạm hành chính phải đặt ra nguyên tắc chỉ xử phạt khi có quy định pháp luật cụ thể, và giao Chính phủ thì Chính phủ mới có quyền quy định chi tiết hành vi, mức

phạt, biện pháp khắc phục và thẩm quyền trong từng lĩnh vực. Muốn xử phạt vi phạm về dữ liệu một cách chắc chắn, cần có một văn bản luật xác lập nguyên tắc và một nghị định chuyên ngành cụ thể hóa hành vi và mức phạt. Giải pháp này phù hợp với kỹ thuật lập pháp Việt Nam, bởi theo thông lệ, mỗi lĩnh vực đều có nghị định xử phạt riêng.



Xử lý vi phạm hành chính là công cụ quan trọng trong hoạt động quản lý nhà nước - Ảnh: Thư viện pháp luật

Bên cạnh đó, việc xây dựng nghị định xử phạt còn góp phần đồng bộ hóa với khung luật mới về dữ liệu. Luật Dữ liệu và Nghị định 165/2025/NĐ-CP đã tạo nền tảng pháp lý cho quản lý dữ liệu, nhưng chưa phải văn bản xử phạt. Vì vậy, cần có nghị định riêng để bảo đảm thi hành nghiêm các nguyên tắc và điều cấm trong hai văn bản này. Đồng thời, điều này cũng giúp khắc phục sự phân tán, chồng chéo của chế tài hiện hành, vốn nằm rải rác trong các nghị định truyền thống như Nghị định 15/2020/NĐ-CP, vốn chưa bao

trùm được các thực tiễn dữ liệu số mới. Do vậy, việc bổ sung quy định trên bảo đảm tính hợp hiến, hợp pháp, vừa đồng bộ với Luật Dữ liệu và Luật Bảo vệ dữ liệu cá nhân, đồng thời tạo sức răn đe, tính khả thi và minh bạch trong thực thi pháp luật về dữ liệu.

Về nội dung pháp luật về xử lý vi phạm hành chính trong lĩnh vực dữ liệu cần thiết để bổ sung vào Luật xử lý vi phạm hành chính (và xây dựng Nghị định), cơ quan được phân công phụ trách xây dựng quy định cần nghiên cứu, bổ sung đầy đủ nội dung về ***(i)*** các hành vi vi phạm pháp luật trên lĩnh vực dữ liệu; ***(ii)*** khung hình phạt; ***(iii)*** biện pháp khắc phục hậu quả; ***(iv)*** thẩm quyền ghi nhận và ra quyết định xử phạt (bao gồm cả trong trường hợp khẩn cấp).

Một là, đối với các hành vi vi phạm hành chính trên lĩnh vực dữ liệu, các nhà lập pháp cần tập trung nghiên cứu về xử lý vi phạm hành chính đối với 07 nhóm hành vi sau:

+ ***Nhóm 1.*** Nhóm hành vi vi phạm quy định về thu thập, xử lý, chia sẻ dữ liệu trái phép, gồm: ***(1)*** Thu thập dữ liệu cá nhân, dữ liệu nhạy cảm, dữ liệu cốt lõi, dữ liệu quan trọng của tổ chức, cá nhân khác mà không được sự đồng ý hoặc không có căn cứ pháp lý rõ ràng; ***(2)*** Xử lý dữ liệu (bao gồm lưu trữ, phân tích, tổng hợp, phân loại, đánh giá, kết nối dữ liệu) không có mục đích rõ ràng, không thông báo, không đăng ký với cơ quan có thẩm quyền theo quy định; ***(3)*** Chia sẻ, chuyển giao, cung cấp dữ liệu cho bên thứ ba mà không có sự đồng thuận của chủ thể dữ liệu hoặc vi phạm các quy định về bảo mật, an toàn thông tin.

+ ***Nhóm 2.*** Nhóm hành vi vi phạm quy định về bảo mật, làm rò rỉ, thất thoát dữ liệu gồm: ***(1)*** Không triển khai hoặc triển khai không đầy đủ các biện pháp kỹ thuật, tổ chức nhằm bảo vệ dữ liệu theo quy định; ***(2)*** Để xảy

ra sự cố an ninh mạng, mất mát, rò rỉ dữ liệu trong quá trình lưu trữ, truyền tải, xử lý do lỗi chủ quan hoặc thiếu kiểm soát; ***(3)*** Không báo cáo, không thông báo hoặc chậm thông báo về sự cố rò rỉ, thất thoát dữ liệu cho cơ quan nhà nước có thẩm quyền hoặc cho chủ thể dữ liệu theo quy định; ***(4)*** Không lưu giữ, không quản lý nhật ký truy cập, nhật ký vận hành hệ thống thông tin chứa dữ liệu theo quy định.

+ ***Nhóm 3.*** Nhóm hành vi vi phạm quy định về việc lưu trữ, đồng bộ, chuẩn hóa dữ liệu gồm: ***(1)*** Không lưu trữ dữ liệu đúng thời hạn, đúng định dạng, không đầy đủ hoặc không đúng vị trí theo quy định của pháp luật hoặc yêu cầu của cơ quan có thẩm quyền; ***(2)*** Không thực hiện đồng bộ dữ liệu với hệ thống dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành theo lộ trình, kế hoạch, quy chuẩn được phê duyệt; ***(3)*** Lưu trữ dữ liệu bằng phương pháp, công cụ, hạ tầng không bảo đảm an toàn, không bảo đảm khả năng truy xuất, xác thực, khôi phục; ***(4)*** Không tuân thủ quy định về chuẩn hóa dữ liệu theo mô hình dữ liệu quốc gia hoặc không áp dụng mã định danh thống nhất, cấu trúc dữ liệu chuẩn.

+ ***Nhóm 4.*** Nhóm hành vi vi phạm quy định về việc cung cấp dữ liệu theo yêu cầu của cơ quan có thẩm quyền gồm: ***(1)*** Không cung cấp hoặc cố tình trì hoãn việc cung cấp dữ liệu theo yêu cầu bằng văn bản hợp pháp của cơ quan nhà nước có thẩm quyền theo quy định của pháp luật; ***(2)*** Cung cấp dữ liệu không đầy đủ, sai lệch hoặc đã bị chỉnh sửa làm sai bản chất, ảnh hưởng đến việc sử dụng dữ liệu cho mục tiêu quản lý nhà nước; ***(3)*** Từ chối cung cấp dữ liệu viện dẫn lý do không phù hợp với pháp luật, trái với thỏa thuận chia sẻ dữ liệu hoặc nghĩa vụ pháp lý đã cam kết; ***(4)*** Không phối hợp kỹ thuật (mở kết nối API, chia sẻ file chuẩn hóa, xác thực truy cập…) phục vụ truy xuất, tích hợp, khai thác dữ liệu theo quy định.

+ ***Nhóm 5.*** Nhóm hành vi vi phạm quy định về mua bán, kinh doanh dữ liệu gồm: ***(1)*** Mua bán, trao đổi, cho thuê, chuyển nhượng dữ liệu cá nhân, dữ liệu nhạy cảm, dữ liệu cốt lõi, dữ liệu quan trọng mà không có sự đồng ý của chủ thể dữ liệu hoặc không có căn cứ pháp lý rõ ràng; ***(2)*** Kinh doanh dịch vụ cung cấp dữ liệu mà không có giấy phép, không thực hiện đăng ký, thông báo hoặc vi phạm điều kiện kinh doanh theo quy định. ***(3)*** Giao dịch dữ liệu thông qua các nền tảng số, sàn dữ liệu, hệ thống trung gian khi chưa được cơ quan có thẩm quyền cấp phép hoặc phê duyệt. ***(4)*** Thu lợi bất chính từ hành vi cung cấp, khai thác dữ liệu trái pháp luật.



Doanh nghiệp có thể đối mặt "hóa đơn" hàng nghìn tỷ nếu vi phạm mua bán dữ liệu cá nhân - Ảnh: Tạp chí Kinh tế Việt Nam

+ ***Nhóm 6.*** Nhóm hành vi vi phạm quy định trong vận hành sàn dữ liệu Trung tâm dữ liệu quốc gia gồm: ***(1)*** Vận hành sàn dữ liệu, trung tâm dữ liệu quốc gia, khu dữ liệu tập trung không đúng quy định về điều kiện kỹ thuật, an ninh mạng và an toàn hệ thống***;*** ***(2)*** Tự ý cung cấp, chia sẻ, khai thác dữ liệu cốt lõi, dữ liệu quan trọng, dữ liệu cá nhân qua sàn dữ liệu khi chưa được

cơ quan có thẩm quyền phê duyệt; ***(3)*** Không bảo đảm tính toàn vẹn, tính khả dụng và tính bảo mật của dữ liệu trong quá trình lưu trữ, trao đổi, xử lý tại trung tâm dữ liệu; ***(4)*** Không thực hiện kiểm toán, giám sát hệ thống định kỳ theo quy định hoặc che giấu, không báo cáo các sự cố kỹ thuật, tấn công mạng, mất an toàn dữ liệu trong hệ thống; ***(5)*** Không tuân thủ quy trình vận hành, sao lưu, phục hồi, dự phòng dữ liệu hoặc để thất thoát, gián đoạn hệ thống, ảnh hưởng đến hoạt động của các cơ quan nhà nước, tổ chức, cá nhân sử dụng dịch vụ.

+ ***Nhóm 7.*** Nhóm hành vi vi phạm quy định về trách nhiệm báo cáo, giám sát dữ liệu gồm: ***(1)*** Không thực hiện chế độ báo cáo định kỳ, đột xuất về tình hình thu thập, xử lý, lưu trữ, chia sẻ và bảo vệ dữ liệu theo yêu cầu của cơ quan quản lý nhà nước có thẩm quyền; ***(2)*** Báo cáo không đúng thời hạn, không đầy đủ, sai lệch nội dung so với thực tế, không đúng biểu mẫu quy trình được ban hành; ***(3)*** Không thực hiện nghĩa vụ tự giám sát, kiểm tra về hệ thống xử lý dữ liệu theo quy định; ***(4)*** Không lưu trữ hoặc lưu trữ không đầy đủ báo cáo, nhật ký hệ thống, nhật ký truy cập, thông tin liên quan bằng dữ liệu theo thời hạn tối thiểu được pháp luật quy định.

Hai là, nghiên cứu, đề xuất khung hình phạt và biện pháp khắc phục phù hợp. Chế tài mạnh sẽ giúp nâng cao tính nghiêm minh của pháp luật và phòng ngừa vi phạm hành chính trong lĩnh vực dữ liệu. Về khung hình phạt, cơ quan chuyên trách cần tham khảo các khung hình phạt xử lý vi phạm hành chính trên lĩnh vực ở các quốc gia khác trên thế giới như EU (GDPR), Trung Quốc (PIPL) hay Nhật Bản (APPI)… nhằm xác định các hình thức phạt và khung hình phạt cho phù hợp với thực tiễn kinh tế - xã hội tại Việt Nam.

Về phạm vi, nguyên tắc, cơ quan lập pháp cần áp dụng nguyên tắc lượng hình trong xử lý vi phạm hành chính. Theo Luật xử lý vi phạm hành chính,

chỉ xử phạt khi pháp luật quy định, mức phạt xác định theo mức trung bình khung và tăng (giảm) theo tình tiết tăng nặng, giảm nhẹ. Ngoài ra, cần cho phép tính mức phạt theo phần trăm giá trị (hoặc khối lượng, doanh thu, lợi tức) từ vi phạm khi cần thiết nhưng không vượt quá mức phạt trần tối đa theo Điều 24, trừ trường hợp có quy định khác được Quốc hội phê duyệt. Đối với mức phạt tối đa, vì hành vi vi phạm trên lĩnh vực dữ liệu thường là các hành vi vi phạm nghiêm trọng, hậu quả lâu dài và lớn nên mức phạt trần cao nhất có thể quy định khoảng 1 tỷ đồng đối với cá nhân và 2 tỷ đồng đối với tổ chức trừ các lĩnh vực mà luật dữ liệu có quy định khác. Riêng đối với vi phạm trên lĩnh vực dữ liệu cá nhân, có thể tính toán phạt 3 tỷ đồng (theo Luật bảo vệ dữ liệu cá nhân).



Cần phải đẩy nhanh tiến độ ban hành luật, tránh để chồng chéo, trùng dẫm thẩm quyền pháp lý - Ảnh: Báo điện tử Chính phủ

Về các hình thức xử phạt chính, bao gồm cảnh cáo, phạt tiền, các hình thức bổ sung như: Tước quyền sử dụng giấy phép/chứng chỉ; Đình chỉ hoạt động có thời hạn; Tịch thu tang vật, phương tiện; Bắt buộc xóa dữ liệu xử lý

trái phép; Thu hồi dữ liệu đã cung cấp/bán trái phép; Cấm tái định danh với bộ dữ liệu đã ẩn danh; Tạm đình chỉ một phần hoặc toàn bộ hoạt động xử lý liên quan; đình chỉ chuyển dữ liệu ra nước ngoài cho đến khi khắc phục (Áp dụng mạnh với dữ liệu quan trọng/cốt lõi); Buộc thông báo vi phạm cho cơ quan chuyên trách và người bị ảnh hưởng trong thời hạn; Buộc nộp lại số lợi bất hợp pháp; Kiểm toán tuân thủ định kỳ bởi đơn vị độc lập; Bổ nhiệm DPO và xây dựng chương trình tuân thủ bắt buộc.

Về mức phạt, khung xử phạt hành chính đối với các hành vi vi phạm trong lĩnh vực dữ liệu được đề xuất theo bảy nhóm như sau, bảo đảm tính hệ thống, tương xứng với mức độ hậu quả và phù hợp với kỹ thuật lượng hình hiện hành:

+ ***Nhóm 1*** - Thu thập, xử lý, chia sẻ dữ liệu trái phép: **mức nhẹ** (quy mô nhỏ, chưa gây hại thực tế) phạt 100 - 300 triệu đồng và buộc xóa/thu hồi dữ liệu thu thập trái phép; **trung bình** (10.000 - 100.000 chủ thể dữ liệu hoặc có ảnh hưởng liên cơ quan) phạt 300 - 800 triệu đồng kèm nghĩa vụ thông báo và lập kế hoạch khắc phục; **nghiêm trọng** (>100.000 chủ thể, liên quan dữ liệu nhạy cảm/quan trọng) phạt 800 triệu - 2 tỷ đồng, đình chỉ hoạt động xử lý liên quan 1 - 3 tháng, nộp lại số lợi bất hợp pháp (nếu có); **đặc biệt nghiêm trọng** (dữ liệu cá nhân quy mô lớn, tác động lan tỏa) phạt đến 3 tỷ đồng theo Luật Bảo vệ dữ liệu cá nhân; nếu có chuyển dữ liệu cá nhân xuyên biên giới trái phép, cân nhắc đến 5% doanh thu năm trước.

+ ***Nhóm 2*** - Bảo mật, rò rỉ, thất thoát dữ liệu: **mức nhẹ** (thiếu biện pháp tối thiểu, chưa rò rỉ) phạt 80 - 250 triệu đồng, buộc triển khai biện pháp an ninh tối thiểu và kiểm toán bảo mật; **trung bình** (rò rỉ hạn chế, chậm thông báo < 72 giờ) phạt 250 - 700 triệu đồng kèm nghĩa vụ thông báo, khắc phục, lưu trữ nhật ký; **nghiêm trọng** (rò rỉ lớn, dữ liệu nhạy cảm; không thông

báo/không báo cáo) phạt 700 triệu - 2 tỷ đồng, đình chỉ 1 - 3 tháng khu vực xử lý liên quan và buộc kiểm toán độc lập; **đặc biệt nghiêm trọng** (tác động diện rộng đến dữ liệu cá nhân) phạt đến 3 tỷ đồng và buộc thông báo trong 72 giờ cho cơ quan chuyên trách và chủ thể dữ liệu theo Luật bảo vệ dữ liệu cá nhân.

+ ***Nhóm 3*** - Lưu trữ, đồng bộ, chuẩn hóa dữ liệu: **mức nhẹ** (sai định dạng/vị trí, chưa ảnh hưởng khai thác) phạt 50 - 150 triệu đồng và buộc chuẩn hóa, đồng bộ; **trung bình** (không đồng bộ theo lộ trình; hạ tầng không bảo đảm truy xuất) phạt 150 - 500 triệu đồng; **nghiêm trọng** (không bảo đảm khả năng khôi phục; gián đoạn chia sẻ liên ngành) phạt 500 triệu - 1,5 tỷ đồng, đình chỉ triển khai hạng mục 1 - 3 tháng để khắc phục; **đặc biệt nghiêm trọng** (ảnh hưởng hệ thống dữ liệu quốc gia/cơ sở dữ liệu chuyên ngành) phạt 1,5 - 2 tỷ đồng.

+ ***Nhóm 4*** - Cung cấp dữ liệu theo yêu cầu cơ quan có thẩm quyền: **nhẹ** (chậm cung cấp không có yếu tố cản trở) phạt 80 - 200 triệu đồng; **trung bình** (cung cấp thiếu/sai lệch; trì hoãn không lý do chính đáng) phạt 200 - 700 triệu đồng và buộc cung cấp đúng, đủ; **nghiêm trọng** (cố ý từ chối; chỉnh sửa làm sai bản chất; không mở kết nối kỹ thuật theo quy định) phạt 700 triệu - 1,8 tỷ đồng, đình chỉ một phần dịch vụ dữ liệu 1 - 3 tháng; **đặc biệt nghiêm trọng** (gây đình trệ quản lý nhà nước, ảnh hưởng an ninh) phạt 1,8-2 tỷ đồng.

+ ***Nhóm 5*** - Mua bán, kinh doanh dữ liệu: **nhẹ** (trao đổi hạn chế, chưa thu lợi đáng kể) phạt 200 - 500 triệu đồng, buộc xóa/thu hồi dữ liệu và tịch thu công cụ, phương tiện; **trung bình** (kinh doanh dịch vụ dữ liệu không phép/không thông báo; giao dịch trên nền tảng chưa được cấp phép) phạt 500 triệu - 1,5 tỷ đồng, đình chỉ hoạt động 1 - 3 tháng; **nghiêm trọng** (tổ

chức đường dây, thu lợi lớn; liên quan dữ liệu nhạy cảm/quan trọng) phạt 1,5 - 2 tỷ đồng, buộc nộp lại toàn bộ số lợi bất hợp pháp và tước quyền kinh doanh 3 - 6 tháng; **đặc biệt nghiêm trọng** (mua, bán dữ liệu cá nhân quy mô lớn) phạt tới 10 lần khoản thu bất hợp pháp và, nếu có yếu tố xuyên biên giới hoặc nền tảng lớn, có thể áp dụng thêm cơ chế phần trăm doanh thu theo Luật bảo vệ dữ liệu cá nhân.

+ ***Nhóm 6*** - Vận hành sàn dữ liệu/Trung tâm dữ liệu quốc gia: **nhẹ** (thiếu chuẩn vận hành cục bộ, chưa ảnh hưởng dịch vụ) phạt 200 - 600 triệu đồng; **trung bình** (không bảo đảm tính toàn vẹn/khả dụng/bảo mật ở phân đoạn; không kiểm toán định kỳ) phạt 600 triệu - 1,5 tỷ đồng, buộc kiểm toán độc lập và khắc phục kỹ thuật; **nghiêm trọng** (tự ý cung cấp/khai thác dữ liệu cốt lõi/quan trọng; gián đoạn dịch vụ diện rộng; che giấu sự cố) phạt 1,5 - 2 tỷ đồng, đình chỉ hoạt động 1 - 6 tháng và nộp lại số lợi; **đặc biệt nghiêm trọng** (xâm hại dữ liệu cá nhân quy mô lớn qua sàn; ảnh hưởng an ninh quốc gia) phạt đến 3 tỷ đồng theo Luật bảo vệ dữ liệu cá nhân, kèm đình chỉ 6 - 12 tháng hạng mục vi phạm.



Đánh cắp dữ liệu là nỗi lo hàng đầu trong bối cảnh kinh tế số - Ảnh: Steadfast Solutions

+ ***Nhóm 7*** - Trách nhiệm báo cáo, giám sát dữ liệu: **nhẹ** (không báo cáo định kỳ đúng mẫu, chưa ảnh hưởng thực tiễn) phạt 30 - 100 triệu đồng; **trung bình** (báo cáo chậm/thiếu; không lưu trữ nhật ký theo hạn tối thiểu) phạt 100 - 300 triệu đồng; **nghiêm trọng** (báo cáo sai lệch có chủ ý; không tự giám sát, kiểm tra; không cung cấp nhật ký phục vụ thanh tra) phạt 300 - 700 triệu đồng; **đặc biệt nghiêm trọng** (che giấu vi phạm; tái phạm) phạt 700 triệu - 1,2 tỷ đồng và đình chỉ 1 - 3 tháng một phần hoạt động xử lý liên quan.

Về cơ quan có thẩm quyền xử phạt, lực lượng Công an nhân dân hiện nay đang là lực lượng đi đầu trong lĩnh vực chuyển đổi số, đặc biệt, sau khi thành lập Trung tâm dữ liệu quốc gia và hoàn thành Cơ sở dữ liệu tổng hợp quốc gia, Bộ Công an sẽ trở thành đầu mối quan trọng quản lý việc thu thập, khai thác, chia sẻ dữ liệu trong và ngoài nước. Do đó, cơ quan có thẩm quyền và là lực lượng nòng cốt trong xử phạt vi phạm hành chính trên lĩnh vực dữ liệu đối với các cơ quan, tổ chức, cá nhân là lực lượng Công an cấp tỉnh và cấp Bộ theo bộ máy hành chính 3 cấp Bộ, tỉnh, xã mới. Giám đốc Công an tỉnh là người có thẩm quyền ra quyết định xử phạt hành chính đối với hành vi vi phạm pháp luật về dữ liệu.

Bên cạnh đó, Bộ Tư pháp và Sở Tư pháp tỉnh với vai trò kiểm soát việc tuân thủ pháp luật và ban hành văn bản quy phạm pháp luật có thể phối hợp với lực lượng Công an trong giám sát, thanh tra và xử phạt các trường hợp vi phạm nghĩa vụ báo cáo, giám sát, không chấp hành yêu cầu pháp lý về dữ liệu. Bộ Khoa học và Công nghệ chịu trách nhiệm quản lý về hạ tầng số, mạng viễn thông, Internet, nền tảng trung gian và dịch vụ dữ liệu có thể phối hợp với lực lượng Công an xử phạt các hành vi vi phạm trong thu thập, xử lý, kinh doanh dữ liệu trên môi trường mạng, bao gồm cả hoạt động sàn

dữ liệu và trung gian dữ liệu. Khi áp dụng cách thức trao thẩm quyền như trên, các cơ quan cấp Bộ gồm Bộ Công an, Bộ Tư pháp, Bộ Khoa học và Công nghệ cần xây dựng quy chế phối hợp liên ngành, các thông tư liên tịch để tránh chồng chéo, bảo đảm mỗi hành vi vi phạm chỉ do một cơ quan xử phạt chính, tránh tình trạng *"xử lý hai lần cho một hành vi"* và tạo sự kết nối đồng bộ, thống nhất và công khai minh bạch kết quả xử phạt.



Bộ trưởng Công an, Đại tướng Lương Tam Quang thông tin đã triệt phá 28 chuyên án phạm tội sử dụng công nghệ cao khởi tố 22 vụ án, 72 bị can - Ảnh: VietNamNet

Tóm lại, việc nghiên cứu và xây dựng các quy định xử lý vi phạm hành chính trong lĩnh vực dữ liệu là yêu cầu tất yếu, xuất phát từ thực tiễn phát triển mạnh mẽ của nền kinh tế số và yêu cầu bảo đảm an ninh, an toàn dữ liệu quốc gia. Việc bổ sung các nguyên tắc cơ bản vào Luật Xử lý vi phạm hành chính, đồng thời ban hành nghị định chuyên ngành quy định chi tiết các hành vi vi phạm, mức phạt và biện pháp khắc phục hậu quả sẽ tạo hành

lang pháp lý chặt chẽ, rõ ràng và minh bạch. Khung pháp lý này không chỉ khắc phục tình trạng phân tán, chồng chéo hiện nay, mà còn bảo đảm tính răn đe, tương thích với thông lệ quốc tế và phù hợp với điều kiện thực tiễn của Việt Nam. Đây chính là bước đi quan trọng, tạo nền tảng để Luật Dữ liệu 2024 và Luật Bảo vệ dữ liệu cá nhân 2025 được thực thi hiệu quả, góp phần xây dựng môi trường số an toàn, tin cậy và thúc đẩy phát triển bền vững kinh tế - xã hội trong kỷ nguyên chuyển đổi số.

3.4.2. Rà soát để đề xuất sửa đổi, bổ sung các văn bản quy phạm pháp luật khác có liên quan đến xử lý vi phạm hành chính trong lĩnh vực dữ liệu, bảo đảm tính thống nhất trong hệ thống văn bản quy phạm pháp luật có liên quan.

Dưới góc độ kỹ thuật lập pháp, việc rà soát, sửa đổi, bổ sung các văn bản liên quan cần được triển khai theo hướng bảo đảm tính nhất quán nội tại của hệ thống và khả năng thi hành thực tế. Trước hết, phải thừa nhận bối cảnh pháp luật về dữ liệu của Việt Nam đang chuyển động nhanh: Luật Dữ liệu đã được ban hành, kèm theo Nghị định 165/2025/NĐ-CP quy định chi tiết thi hành; tiếp đó là Luật Bảo vệ dữ liệu cá nhân có hiệu lực từ 01/01/2026, bên cạnh khung sẵn có của Luật An toàn thông tin mạng 2015 và Luật Giao dịch điện tử 2023. Hệ quả là nhiều quy phạm cùng điều chỉnh một nhóm hành vi nhưng ở các tầng luật khác nhau, đòi hỏi một chương trình "điều hòa" quy tắc và chế tài đồng bộ từ luật đến nghị định, thông tư.

Một là, thống nhất khái niệm và thuật ngữ ở trong các văn bản pháp luật về dữ liệu. Cần đối chiếu, chuẩn hóa các thuật ngữ "dữ liệu số", "dữ liệu cá nhân", "dữ liệu cá nhân cơ bản/nhạy cảm", "xử lý dữ liệu" giữa Luật Dữ liệu và Luật Bảo vệ dữ liệu cá nhân để cơ quan áp dụng pháp luật không phải "lấn cấn" khi chuyển từ văn bản này sang văn bản khác. Chẳng hạn, Luật

Bảo vệ dữ liệu cá nhân đã định danh rõ "dữ liệu cá nhân cơ bản" và "dữ liệu cá nhân nhạy cảm"; khi xây dựng nghị định xử phạt chuyên ngành về dữ liệu, các khái niệm này cần được viện dẫn thống nhất để xác định chính xác đối tượng hành vi và mức độ nguy hiểm. Đồng thời, các chuẩn mực về chuyển dữ liệu xuyên biên giới, nghĩa vụ thông báo - đồng ý - rút lại đồng ý trong xử lý dữ liệu cũng cần được đồng bộ hóa giữa hai luật và văn bản dưới luật tương ứng.

Hai là, điều chỉnh hành vi và mức phạt tại các nghị định hiện hành để "ăn khớp" với khuôn khổ mới. Hiện nhiều hành vi liên quan đến thu thập, sử dụng, chia sẻ thông tin cá nhân đang được xử phạt theo Nghị định 15/2020/NĐ-CP (lĩnh vực bưu chính, viễn thông, công nghệ thông tin, giao dịch điện tử) với các mức phạt 10 - 20 triệu đồng cho thu thập khi chưa có sự đồng ý; 20 - 30 triệu đồng cho sử dụng, chia sẻ trái phép; một số nhóm hành vi khác bị xử phạt ở các ngưỡng 30 - 50 - 70 triệu đồng. Đây là các nấc phạt được thiết kế cho giai đoạn trước khi có Luật Dữ liệu, Luật Bảo vệ dữ liệu cá nhân, nên cần được rà soát để nâng ngưỡng, tái cấu trúc nhóm hành vi đã phân tích ở trên. Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, vốn đóng vai trò cầu nối trước khi có luật cần được rà soát, chỉnh lý chế định nhiệm vụ, thẩm quyền, quy trình phối hợp để tương thích với luật mới (nhất là cơ chế thông báo sự cố, đánh giá tác động và trách nhiệm của cơ quan chuyên trách bảo vệ dữ liệu cá nhân).

Ba là, sửa đổi các luật và nghị định có liên quan để tránh "cắt lớp" khi điều chỉnh. Luật ninh mạng và Luật Giao dịch điện tử cần được rà soát các điều về bảo vệ thông tin cá nhân/dữ liệu, an toàn hệ thống và giá trị pháp lý của thông điệp dữ liệu nhằm loại trùng lặp, khép kín khoảng trống quản lý trong môi trường số mới (dịch vụ trung gian dữ liệu, trung tâm dữ liệu, sàn

dữ liệu, AI sinh dữ liệu…). Việc này vừa bảo đảm tính thống nhất về thuật ngữ, vừa làm rõ ranh giới giữa chuẩn mực an toàn hệ thống (an ninh mạng) với chuẩn mực xử lý dữ liệu (dữ liệu số, dữ liệu cá nhân).

Bốn là, bảo đảm tính chuyển tiếp và phối hợp khi thi hành. Nghị định 165/2025/NĐ-CP đã được ban hành để hướng dẫn chi tiết Luật Dữ liệu; Luật Bảo vệ dữ liệu cá nhân cũng thiết lập các quy định chuyển tiếp đối với hồ sơ, quy trình đã thực hiện theo Nghị định 13/2023/NĐ-CP. Vì vậy, khi sửa đổi và ban hành mới các nghị định xử phạt, cần "cài lại" điều khoản chuyển tiếp tương thích, tránh xáo trộn không cần thiết cho cơ quan, tổ chức đang tuân thủ theo khuôn khổ cũ.



Cần phải làm tốt việc rà soát, sửa đổi, bổ sung các văn bản liên quan - Ảnh: Internet

Như vậy, yêu cầu đặt ra không chỉ là bổ sung một vài quy định đơn lẻ, mà là tiến hành một cuộc rà soát tổng thể, bảo đảm sự đồng bộ giữa các đạo luật, nghị định và thông tư hiện hành có liên quan đến dữ liệu. Việc chuẩn

hóa khái niệm, điều chỉnh hành vi và mức phạt, đồng thời sửa đổi những quy định chồng chéo hay chưa theo kịp bối cảnh mới sẽ góp phần hình thành một chỉnh thể pháp lý thống nhất, khép kín và khả thi. Đây là điều kiện tiên quyết để các quy định xử lý vi phạm hành chính trong lĩnh vực dữ liệu vận hành hiệu quả, hạn chế khoảng trống pháp lý, nâng cao tính răn đe và củng cố niềm tin xã hội vào hệ thống pháp luật dữ liệu quốc gia.

3.4.3. Tổ chức thu thập thông tin, các ý kiến đề xuất xây dựng quy định về xử phạt hành chính đối với hành vi vi phạm pháp luật trên lĩnh vực dữ liệu

Khi xây dựng chính sách pháp luật, một yếu tố tiên quyết là việc lấy ý kiến và thu thập thông tin cần được tổ chức theo một quy trình rõ ràng, có mục tiêu cụ thể và phương pháp phù hợp. Quan trọng là phải bảo đảm mọi ý kiến đều được ghi nhận, phân tích và sử dụng làm cơ sở để hoàn thiện quy định pháp luật.

- Về mục tiêu và phạm vi

Hoạt động tham vấn nhằm đạt tối thiểu ba mục đích: ***(i)*** kiểm định tính hợp lý - hợp pháp của phương án chính sách trên nền các quy định hiện hành; ***(ii)*** đo lường tính khả thi trong triển khai, bao gồm năng lực tổ chức, chi phí tuân thủ, và rủi ro phát sinh; ***(iii)*** gia tăng tính minh bạch, trách nhiệm giải trình và đồng thuận xã hội. Phạm vi tham vấn không chỉ xoay quanh mức phạt và hành vi vi phạm, mà còn bao trùm các vấn đề kỹ thuật (chuẩn dữ liệu, quy trình kết nối - chia sẻ - đồng bộ), tổ chức thực thi (thẩm quyền, phối hợp liên ngành, quy trình xử phạt), và các điều khoản chuyển tiếp.

- Về nguyên tắc vận hành

Hoạt động phải được tổ chức theo các nguyên tắc: công khai - minh bạch (công bố dự thảo, lịch trình và tài liệu tham vấn); cơ chế đa chiều - đại

diện nhân dân (bảo đảm có tiếng nói từ cơ quan quản lý, giới chuyên gia, cộng đồng doanh nghiệp, hiệp hội nghề nghiệp và người dân); dựa trên bằng chứng (ý kiến kèm dẫn liệu, tình huống điển hình, đánh giá tác động); và bảo vệ dữ liệu cá nhân trong chính quá trình tham vấn (ẩn danh hóa phản hồi, quản trị xung đột lợi ích, chỉ thu thập tối thiểu thông tin cần thiết).

- Về đối tượng tham vấn

Ở tầng cơ quan nhà nước, cơ quan chủ trì soạn thảo gửi yêu cầu góp ý tới các bộ, ngành có liên quan trực tiếp đến quản trị và thực thi (Bộ Công an; Bộ Khoa học và Công nghệ; Bộ Tư pháp; Thanh tra Chính phủ; cùng các cơ quan chuyên môn về dữ liệu). Ở tầng lập pháp - giám sát, phối hợp lấy ý kiến các ủy ban của Quốc hội và Mặt trận Tổ quốc để bảo đảm sự giám sát và phản biện chính sách. Ở tầng chuyên gia - học thuật, mời nhà nghiên cứu, luật sư, chuyên gia an ninh mạng, kiến trúc sư dữ liệu, chuyên gia quản trị rủi ro công nghệ. Ở tầng xã hội - thị trường, huy động doanh nghiệp công nghệ, nền tảng số, đơn vị trung gian dữ liệu, hiệp hội ngành nghề; đồng thời mở kênh để người dân, đặc biệt là nhóm dễ bị tổn thương bởi vi phạm dữ liệu, có thể gửi ý kiến.

- Về phương thức và công cụ

Kết hợp tham vấn bằng văn bản (công văn, phiếu góp ý theo biểu mẫu), tọa đàm - hội thảo chuyên đề (theo nhóm chủ đề: hành vi - mức phạt; quyền và nghĩa vụ; thẩm quyền - thủ tục; kỹ thuật bảo mật; cơ chế chuyển tiếp), khảo sát trực tuyến diện rộng (bảng hỏi định lượng và câu hỏi mở), cũng như kênh phản biện xã hội trên cổng thông tin điện tử. Tài liệu dự thảo cần đi kèm bản tóm tắt chính sách, ma trận so sánh phương án, và các tình huống minh họa điển hình để người góp ý dễ hình dung tác động thực tế.

- Về quy trình tổ chức

Có thể triển khai theo sáu bước liên hoàn: ***(1)*** Lập kế hoạch tham vấn, xác định nhóm đối tượng, lịch trình, bộ câu hỏi trọng tâm và tiêu chí đánh giá; (2) Công bố dự thảo và hồ sơ tóm tắt, mở các kênh tiếp nhận ý kiến; ***(3)*** Thu thập có kiểm soát: ghi nhận, mã hóa, gắn thẻ ý kiến theo chủ đề để tránh thất lạc và trùng lặp; ***(4)*** Phân tích - tổng hợp: phân loại ý kiến theo nhóm vấn đề (khái niệm - phạm vi, hành vi - mức phạt, biện pháp khắc phục, thẩm quyền - thủ tục, chuyển tiếp - thi hành), đánh giá theo tiêu chí hợp hiến - hợp pháp, tính khả thi, chi phí - lợi ích và rủi ro; ***(5)*** Chuyển hóa chính sách: xây dựng ma trận "ý kiến chuyển đổi thành phương án chỉnh lý", nêu rõ tiếp thu/tiếp thu một phần/không tiếp thu kèm lý do; ***(6)*** Giải trình - phản hồi: công khai báo cáo tiếp thu, chỉnh lý dự thảo và cập nhật bản dự thảo sau khi đã hiệu đính, bảo đảm người góp ý nhìn thấy dấu vết của tác động tham vấn lên nội dung cuối cùng.

- Về tiêu chí đánh giá chất lượng ý kiến

Để tránh "lấy ý kiến hình thức", mỗi phản hồi được chấm theo bộ tiêu chí: tính liên quan đến mục tiêu điều chỉnh; độ cụ thể và khả năng áp dụng; cơ sở bằng chứng (dữ liệu, tình huống, so sánh quốc tế); đánh giá tác động (chi phí tuân thủ, ảnh hưởng tới quyền, lợi ích hợp pháp của tổ chức, cá nhân); và tính nhất quán với hệ thống pháp luật. Các ý kiến đáp ứng chuẩn sẽ được ưu tiên trong ma trận tiếp thu; các ý kiến trùng lặp được gộp; các ý kiến xung đột được phân tích phương án dung hòa và lựa chọn tối ưu.

- Về sản phẩm đầu ra bắt buộc

Kết thúc tham vấn, hồ sơ phải có: báo cáo tổng hợp ý kiến có phân nhóm; bảng tiếp thu, giải trình theo từng điều, khoản; ma trận hành động (TOWS, SWOT, SPACE) mức phạt, biện pháp khắc phục, thẩm quyền; đề

xuất điều khoản chuyển tiếp và lộ trình thi hành; đánh giá tác động chính sách/đánh giá thủ tục hành chính (nếu có). Đồng thời, thiết lập cơ sở dữ liệu điện tử lưu trữ toàn bộ phản hồi, phục vụ kiểm tra, đối chiếu và cập nhật ở các vòng chỉnh lý tiếp theo.

- Về bảo đảm đạo đức và an toàn thông tin

Quá trình tổ chức phải tuân thủ nguyên tắc bảo vệ dữ liệu cá nhân của người tham gia: chỉ thu thập tối thiểu, mục đích rõ ràng, lưu trữ an toàn, ẩn danh khi công bố, xóa dữ liệu khi mục đích đã đạt được. Đồng thời, công bố công khai phương án xử lý xung đột lợi ích (chuyên gia tham vấn đồng thời là nhà cung cấp dịch vụ liên quan), tránh thiên lệch trong kết luận chính sách.



Ký kết Quy chế phối hợp, trao đổi thông tin, dữ liệu số liên quan đến đăng ký và thống kê hộ tịch - Ảnh: Báo Điện tử Chính phủ

- Về cơ chế phối hợp và duy trì đối thoại

Cần thiết lập đầu mối điều phối liên ngành để đồng bộ lịch tham vấn, tránh trùng lặp và mâu thuẫn giữa các nhóm soạn thảo; duy trì kênh đối thoại mở trong suốt vòng đời văn bản, từ giai đoạn đề nghị xây dựng đến khi ban hành và triển khai, để kịp thời cập nhật dữ kiện mới phát sinh từ thực tiễn.

Cách tổ chức như vậy bảo đảm quy định được ban hành vừa có cơ sở khoa học vững chắc, vừa phản ánh đúng nhu cầu quản trị dữ liệu trong đời sống số; qua đó nâng cao tính đồng thuận xã hội, giảm chi phí tuân thủ và tăng cường hiệu lực thi hành khi đi vào thực tế.

3.4.4. Tăng cường hợp tác quốc tế, tiếp thu các bài học kinh nghiệm quốc tế để hoàn thiện hơn việc xử lý vi phạm dữ liệu

Trong bối cảnh dữ liệu lưu chuyển xuyên biên giới và các hành vi xâm phạm ngày càng tinh vi, hợp tác quốc tế là đòn bẩy then chốt để nâng cao hiệu lực thực thi. Kinh nghiệm của Liên minh châu Âu cho thấy, cơ chế phối hợp giữa các cơ quan bảo vệ dữ liệu giúp chia sẻ thông tin, hỗ trợ điều tra và tiến tới xử phạt đồng bộ đối với các vi phạm có yếu tố nước ngoài. Từ đó, Việt Nam cần chủ động thiết lập và mở rộng mạng lưới hợp tác song phương, đa phương với cơ quan chức năng của các quốc gia và tổ chức quốc tế, tập trung vào: ***(i)*** thiết lập đầu mối liên lạc quốc gia về bảo vệ dữ liệu; ***(ii)*** ký kết hoặc tham gia thỏa thuận trao đổi thông tin, tương trợ tư pháp, tương trợ hành chính trong điều tra vi phạm dữ liệu; ***(iii)*** vận hành cơ chế "đường dây nóng" và quy trình chuẩn về tiếp nhận, xử lý yêu cầu hợp tác liên quan đến máy chủ, nền tảng hoặc đối tượng vi phạm đặt ở nước ngoài; ***(iv)*** chia sẻ kinh nghiệm về phương pháp giám định kỹ thuật số, quản trị chứng cứ điện tử và thu hồi dữ liệu bị rò rỉ.

Cùng với hợp tác thực thi, hệ thống pháp luật cần được cập nhật thường xuyên để theo kịp xu hướng công nghệ. Đối với trí tuệ nhân tạo, nên bổ sung quy định về nguồn gốc và tính hợp pháp của dữ liệu huấn luyện; cơ chế đánh giá tác động trước và trong khi vận hành (bao gồm quyền riêng tư, an ninh mạng, thiên lệch thuật toán); yêu cầu minh bạch tối thiểu (hồ sơ dữ liệu, nhật ký xử lý); và cấm rõ ràng các hành vi sử dụng dữ liệu xâm phạm đời tư,

chiếm đoạt, tấn công hệ thống hoặc tái định danh trái phép. Đồng thời, cần xây dựng *"cơ chế quét chân trời"* (horizon scanning) và không gian thử nghiệm có kiểm soát (regulatory sandbox) cho công nghệ mới, qua đó dự báo và ứng phó sớm với các mô hình vi phạm mới nổi như trích xuất dữ liệu quy mô lớn, theo dõi bí mật, deepfake và các hình thức gian lận dựa trên AI.

Không chỉ vậy, Việt Nam cần chủ động hài hòa khuôn khổ lập pháp và chuẩn mực chế tài. Chủ động tham chiếu, đối sánh và từng bước hài hòa với các chuẩn mực quốc tế/khung khu vực (ASEAN Data Management Framework và ASEAN Model Contractual Clauses; nguyên tắc OECD về luồng dữ liệu xuyên biên giới; kinh nghiệm EU về cơ chế "một cửa" và tính phạt theo doanh thu). Trên cơ sở đó, xây dựng "bảng ánh xạ" giữa khái niệm - hành vi - mức phạt của Việt Nam với các hệ thống điển hình, nhằm: ***(1)*** thống nhất thuật ngữ, tiêu chí phân loại dữ liệu; ***(2)*** chuẩn hóa phương pháp lượng hình; ***(3)*** đồng bộ thủ tục bảo đảm quyền của đối tượng bị xử phạt. Thêm vào đó, Việt Nam cần tham gia mạng lưới hợp tác chuyên môn, chủ động kết nối hoặc xin tham gia hoặc thiết lập cơ chế phối hợp với các mạng lưới như Global Privacy Enforcement Network (GPEN), Global Privacy Assembly (GPA), mạng lưới CERT/CSIRT khu vực.

Định kỳ tổ chức chiến dịch kiểm tra theo chủ đề (sàn dữ liệu, chéo mục đích xử lý, chuyển dữ liệu xuyên biên giới, AI và tái định danh) để đồng bộ cách hiểu, cách lượng hình và phương thức cưỡng chế. Có thể tính toán thiết kế "điểm liên lạc quốc gia" và quy trình một cửa đối ngoại thông qua thành lập đầu mối quốc gia về thực thi dữ liệu có chức năng tiếp nhận, điều phối yêu cầu hợp tác; chuẩn hóa biểu mẫu và cam kết Thỏa thuận mức dịch vụ; duy trì đường dây nóng pháp lý; công bố công khai hướng dẫn hợp tác cho cơ quan nước ngoài và doanh nghiệp toàn cầu.

Hơn nữa, cần xây dựng lộ trình tiếp cận các điều ước quốc tế phù hợp. Từng bước nghiên cứu tiếp cận, gia nhập những điều ước, chuẩn mực mở liên quan quản trị dữ liệu và chứng cứ điện tử (ví dụ cơ chế chuẩn mực về bảo vệ dữ liệu, hợp tác điều tra tội phạm công nghệ, công nhận chữ ký điện tử), đồng thời nội luật hóa các nghĩa vụ, tiêu chuẩn cốt lõi theo cách không làm suy giảm chủ quyền dữ liệu và yêu cầu bảo đảm an ninh quốc gia.



Logo Thỏa thuận quốc tế của EU -
Ảnh: European Data Protection Supervisor

Ngoài ra, cần thiết lập cơ chế trợ giúp hành chính qua biên giới về xử phạt. Bên cạnh các hiệp định tương trợ tư pháp (thường phục vụ hình sự, dân sự), cần phát triển bản ghi nhớ (MoU) và thoả thuận hợp tác hành chính giữa cơ quan có thẩm quyền của Việt Nam và các cơ quan bảo vệ dữ liệu số ở quốc gia, vùng lãnh thổ khác để trao đổi thông tin vụ việc; hỗ trợ xác minh danh tính pháp lý của tổ chức vi phạm; hỗ trợ tống đạt quyết định xử phạt, thu thập chứng cứ điện tử, và thực thi biện pháp khắc phục. Với nền tảng xuyên biên giới, khuyến khích cơ chế điều tra phối hợp hoặc kiểm toán từ xa theo quy trình chung.

Để chính sách đi vào cuộc sống, cần kết hợp đồng bộ ba trụ cột: ***(i)*** giải pháp lập pháp - hoàn thiện khung quy phạm và nghị định xử phạt chuyên ngành; ***(ii)*** giải pháp tổ chức thực thi - nâng cao năng lực điều tra số, cơ chế phối hợp liên ngành và hạ tầng kỹ thuật phục vụ giám sát, truy vết; ***(iii)*** giải pháp hỗ trợ tuân thủ - tuyên truyền, hướng dẫn kỹ thuật, cơ chế chứng nhận, chứng chỉ và công cụ đánh giá rủi ro dành cho doanh nghiệp, đặc biệt là doanh nghiệp nhỏ và vừa. Một hệ thống quy tắc rõ ràng, chế tài nghiêm minh gắn với hợp tác quốc tế hiệu quả và sự tuân thủ tự giác của các chủ thể sẽ kiến tạo môi trường dữ liệu an toàn, lành mạnh, bảo vệ lợi ích quốc gia và quyền của công dân, đồng thời thúc đẩy sự phát triển bền vững của kinh tế số./.



Tổng hợp các hành vi bị nghiêm cấm theo Luật Dữ liệu - Ảnh: CSANDLS

Danh mục tài liệu tham khảo

I. Tiếng Việt

1. Ban Chấp hành Trung ương Đảng (2022), *Nghị quyết số 29-NQ/TW về tiếp tục đẩy mạnh công nghiệp hóa, hiện đại hóa đất nước đến năm 2030, tầm nhìn đến năm 2045,* Hà Nội.
2. Bộ Chính trị (2018), *Nghị quyết số 23-NQ/TW về định hướng xây dựng chính sách phát triển công nghiệp quốc gia đến năm 2030, tầm nhìn đến năm 2045,* Hà Nội.
3. Bộ Chính trị (2019), *Nghị quyết số 52-NQ/TW ngày 27/9/2019 về một số chủ trương, chính sách chủ động tham gia cuộc Cách mạng công nghiệp lần thứ Tư,* Hà Nội.
4. Bộ Công an (2024), *Dự thảo Nghị định xử phạt vi phạm hành chính về bảo vệ dữ liệu cá nhân,* Hà Nội.
5. Bộ Công an (2024), *Tài liệu giới thiệu Luật Dữ liệu*, Hà Nội
6. Bộ Quốc phòng (2025), *Thông tư số 76/2025/TT-BQP ban hành Quy chuẩn kỹ thuật quốc gia về xác thực lưu trữ tài liệu số lâu dài của các cơ quan Đảng, Nhà nước (hiệu lực từ 02/09/2025)*, Hà Nội.
7. Bộ Thông tin và Truyền thông. (2022), *Báo cáo thường niên kinh tế số Việt Nam năm 2022,* Hà Nội.
8. Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam (2020), *Nghị định 47/2020/NĐ-CP ngày 9/4/2020 về quản lý, kết nối, chia sẻ dữ liệu số của cơ quan nhà nước,* Hà Nội.
9. Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam (2023), *Nghị định số 13/2023/NĐ-CP của Chính phủ về bảo vệ dữ liệu cá nhân,* Hà Nội.

10. Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam (2025), *Nghiêm cấm mua bán dữ liệu cá nhân; mức xử phạt vi phạm hành chính trong lĩnh vực bảo vệ dữ liệu cá nhân,* Cổng thông tin điện tử Chính phủ, https://xaydungchinhsach.chinhphu.vn/nghiem-cam-mua-ban-du-lieu-ca-nhan-muc-xu-phat-vi-pham-hanh-chinh-trong-linh-vuc-bao-ve-du-lieu-ca-nhan-119250728102154903.htm, Truy cập ngày 13/8/2025.

11. Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam (2018), *Nghị định số 165/2018/NĐ-CP về giao dịch điện tử trong hoạt động tài chính,* Hà Nội.

12. Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam (2021), *Nghị quyết số 76/NQ-CP ban hành Chương trình tổng thể cải cách hành chính nhà nước giai đoạn 2021 - 2030,* Hà Nội.

13. Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam (2021), *Nghị định số 144/2021/NĐ-CP ngày 31/12/2021 quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh, trật tự, an toàn xã hội; phòng, chống tệ nạn xã hội; phòng cháy, chữa cháy; cứu nạn, cứu hộ; phòng, chống bạo lực gia đình,* Hà Nội.

14. Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam (2025), *Nghị định số 165/2025/NĐ-CP quy định chi tiết một số điều và biện pháp thi hành Luật Dữ liệu*, Hà Nội.

15. Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam (2025), *Nghị định số 194/2025/NĐ-CP quy định chi tiết một số điều của Luật Giao dịch điện tử về cơ sở dữ liệu quốc gia, kết nối và chia sẻ dữ liệu, dữ liệu mở phục vụ giao dịch điện tử của cơ quan nhà nước,* Hà Nội.

16. Đại hội đồng Liên Hợp Quốc (1966), *Công ước quốc tế về các Quyền dân sự và Chính trị,* Bộ Tư pháp Việt Nam, https://moj.gov.vn

/tttp/tintuc/Lists/CongUocQuocTe/Attachments/10/1.%20Cong%20uoc%20ICCPR%20-%20VN.pdf, Truy cập ngày 13/8/2025.

17. Hà Nhi (2020), *Mỹ thừa nhận CIA theo dõi các giao dịch tài chính thông qua SWIFT,* Báo Nhân Dân, https://nhandan.vn/my-thua-nhan-cia-theo-doi-cac-giao-dich-tai-chinh-thong-qua-swift-post489020.html, Truy cập ngày 13/8/2025.
18. Huỳnh Thiên Tứ, Lê Thùy Khanh (2024), *Nghiên cứu tiếp cận pháp lý đối với dữ liệu số và cơ chế điều chỉnh quyền về dữ liệu số trong pháp luật Việt Nam*, Research Pape, UEH University.
19. Nguyễn Quỳnh Trang (2022), *Pháp luật về bảo hộ dữ liệu cá nhân trong bối cảnh phát triển trí tuệ nhân tạo*, Tạp chí Pháp luật và Thực tiễn, số 50/2022.
20. Nguyễn Thu Trang (2025), *Một số nội dung đáng chú ý tại Luật Dữ liệu 2024*, Cổng thông tin Viettel DSC.
21. Nguyễn Văn Tùng (2023), *Bảo vệ dữ liệu cá nhân trong pháp luật Việt Nam: Thực trạng và kiến nghị,* Tạp chí Luật học.
22. Phạm Huyền Trang (2024), *Vai trò của dữ liệu số và những vấn đề đặt ra*, Tạp chí Quản lý Nhà nước, số 342 (7/2024).
23. Phạm Thị Hiền, Nguyễn Thu Dung (2021), *Pháp luật về bảo vệ dữ liệu cá nhân trong nền kinh tế số ở Việt Nam hiện nay*, Tạp chí Công thương, số 25/2021.
24. Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam (2024), *Luật Dữ liệu năm 2024*, Hà Nội.
25. Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam (2025), *Luật Bảo vệ dữ liệu cá nhân năm 2025,* Hà Nội.

26. Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam (2023), *Luật Giao dịch điện tử năm 2023,* Hà Nội.

27. Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam (2023), *Nghị quyết số 81/2023/QH15 về Quy hoạch tổng thể quốc gia thời kỳ 2021 - 2030, tầm nhìn đến năm 2050*, Hà Nội.

28. Tạp chí Kinh tế Sài Gòn (2025), *Chuyển dữ liệu xuyên biên giới trong Luật Dữ liệu 2024,* Tạp chí Kinh tế Sài Gòn Online, Truy cập ngày 13/8/2025.

29. Thủ tướng Chính phủ (2020), *Quyết định số 2289/QĐ-TTg ngày 31/12/2020 ban hành Chiến lược quốc gia về Cách mạng công nghiệp lần thứ tư đến năm 2030,* Hà Nội.

30. Thủ tướng Chính phủ (2020), *Quyết định số 749/QĐ-TTg ngày 03/6/2020 phê duyệt Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030,* Hà Nội.

31. Thủ tướng Chính phủ (2025), *Quyết định số 20/2025/QĐ-TTg ngày 10/02/2025 ban hành danh mục dữ liệu quan trọng, dữ liệu cốt lõi,* Hà Nội.

32. Trần Thế Hệ (2025), *"Kinh nghiệm quốc tế về bảo vệ dữ liệu người tiêu dùng sử dụng dịch vụ ngân hàng số và gợi ý cho Việt Nam"*, Tạp chí Khoa học Đại học Huế, Vol.134, 6S-1/2025.

33. Trung tâm Khoa học Công nghệ và Truyền thông Nghệ An (2023), *Số vụ tấn công mạng nhắm vào các hệ thống tại Việt Nam tăng 9,5%, Báo điện tử,* https://naict.tttt.nghean.gov.vn/attt/nam-2023-so-vu-tan-cong-mang-nham-vao-cac-he-thong-tai-viet-nam-tang-9-5571.html, Truy cập ngày 13/8/2025.

34. Văn phòng Trung ương Đảng, *Công văn số 7455/CV - VPTW ngày 31/7/2023 thông báo kết luận của Bộ Chính trị về Đề án Trung tâm Dữ liệu quốc gia,* Hà Nội.

35. Vietnamnet (2019), *Google bị phạt 50 triệu Euro vì vi phạm luật bảo vệ dữ liệu của EU,* Vietnamnet, https://vietnamnet.vn/google-bi-phat-50-trieu-eur-vi-vi-pham-luat-bao-ve-du-lieu-cua-eu-i27065.html, Truy cập ngày 13/8/2025.

II. Tiếng Anh

35. Belgian Parliament (1993), *Act on the Protection of the Private Life concerning the Processing of Personal Data,* Belgian Official Gazette (B.S.).

36. American Law Institute (1977), *Restatement (Second) of Torts § 652B, American Law Institute,* https://www.ali.org/publications/show/torts/, Truy cập ngày 13/8/2025.

37. Baker McKenzie (2025), *Global data & cyber handbook - Singapore,* Baker McKenzie.

38. Longbing Cao (2020), *Data Science: A Comprehensive Overview*.

39. *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

40. Carson A (2019), *FTC touts historic YouTube settlement as "game changer" for COPPA enforcement,* https://iapp.org/news/a/ftc-touts-historic-youtube-settlement-as-game-changer-for-coppa-enforcement/, truy cập ngày 5/8/2025.

41. Fred H. Cate (2011), *The growing importance (and irrelevance) of international data protection law,* http://www.lcil.cam.ac.uk/news/article.php?.section26&article=1581, truy cập ngày 5/8/2025.

42. Chambre (2018), *Proposed Act on the Protection of Natural Persons concerning the Processing of Personal Data,* Travaux Préparatoires, Document 3126/001.

43. Chander A, Kaminski M, McGeveran W (2019), *Catalyzing privacy law,* Georgetown Law faculty publications and other works, https://scholarship.law.georgetown.edu/facpub/2190/, Truy cập ngày 05/8/2025.

44. China Justice Observer (2023), *A look into cybercrime in China: Infringement of privacy as a crime*, China Justice Observer, https://www.chinajusticeobserver.com/a/-a-look-into-cybercrime-in-china, Truy cập ngày 15/8/2025.

45. China Briefing (2024), *China Issues New Regulations on Network Data Security Management, Effective January 1, 2025,* China Briefing, https://www.china-briefing.com/news/china-issues-new-regulations-on-network-data-security-management-effective-january-1-2025/, Truy cập ngày 17/8/2025.

46. China Data Compliance (n.d.), *Regulatory Updates,* China Data Compliance, https://www.chinadatacompliance.com/regulatory-updates/, Truy cập ngày 17/8/2025.

47. Committee on the Judiciary, *Subcommittee on Privacy, Technology and the Law (2012),* The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century, U.S. Senate Committee on the Judiciary, https://www.judiciary.senate.gov/imo/media/doc/CHRG-112shrg87342.pdf, Truy cập ngày 05/8/2025.

48. Council of State (2017), *Opinion 61.267/2/AG, on the Proposed Act establishing the Data Protection Authority*, pp. 43-47..

49. Council of State (2018), *Opinion No. 62.834/3 on the proposed decree by the Flemish Community and the Flemish Region concerning the amendments to the decrees based on Regulation (EU) 2016/679*, Data Protection Around the World: Privacy Laws in Action, T.M.C. Asser Press.

50. Dansac Le Clerc, M., Dehareng, E., & Leportois, J. (2025), *"Sensitive data" under the CJEU's spotlight: Practical implications,* Connect on Tech (Baker McKenzie), https://connectontech.bakermckenzie.com/sensitive-data-under-the-cjeus-spotlight-practical-implications/, Truy cập ngày 13/8/2025.

51. De Busser E (2009), *EU-US data protection in criminal matters,* Maklu, Antwerp.

52. De Hert P (2003), *Handboek Privacy: Persoonsgegevens in België [Privacy Handbook, Personal Data in Belgium],* Politeia, Brussels.

53. De Hert P, Gutwirth S (2013), *Anthologie Privacy [Privacy Anthology],* ASP, Brussels.

54. DeVries W (2003), *Protecting privacy in the digital age,* Berkeley Technology Law Journal, 18:283-311.

55. Dechert LLP (2021), *Navigating China's Data Protection Laws*, Dechert LLP Publications, https://www.dechert.com/knowledge/publication/2021/7/navigating-china-s-data-protection-laws.html, Truy cập ngày 17/8/2025.

56. DLA Piper (.n.d), *Data protection laws in China*, DLA Piper Data Protection Laws of the World, https://www.dlapiperdataprotection.com/index.html?c=CN, Truy cập ngày 06/8/2025

57. Electronic Privacy Information Center (EPIC) (2022), *Enforcement of privacy laws in the U.S.*, EPIC website, https://epic.org/issues/data-protection/enforcement-of-privacy-laws/, Truy cập ngày 13/8/2025.

58. European Commission (2020), *A European strategy for data,* European Commission,https://ec.europa.eu/info/sites/default/files/communication-european-strategy-data-19feb2020_en.pdf, Truy cập ngày 13/8/2025.

59. European Union (2016), *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), Official Journal of the European Union*, L 119, 1-88, https://eur-lex.europa.eu/eli/reg/2016/679/oj, Truy cập ngày 10/8/2025.

60. Fazlioglu, M (2019), *Consensus and controversy in the debate over US federal data privacy legislation*, International Association of Privacy Professionals, Portsmouth, https://iapp.org/store/books/a191P000002YpUzQAK/, Truy cập ngày 10/8/2025.

61. Federal Communications Commission (2015), *Cable television*, Federal Communications Commission, https://www.fcc.gov/media/engineering/cabletelevision, Truy cập ngày 10/8/2025.

62. Federal Trade Commission (2002), *How to comply with the privacy of consumer financial information rule of the Gramm-Leach-Bliley Act*, Federal Trade Commission, https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm, Truy cập ngày 10/8/2025.

63. Federal Trade Commission (2011), *FTC charges deceptive privacy practices in Google's rollout of its Buzz social network,* Federal Trade Commission, https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz, Truy cập ngày 10/8/2025.

64. Federal Trade Commission (2012), *FTC approves final settlement with Facebook,* Federal Trade Commission, https://www.ftc.gov/news-

events/press-releases/2012/08/ftc-approves-final-settlement-facebook, Truy cập ngày 11/8/2025.

65. Federal Trade Commission (2015), *Complying with COPPA: Frequently asked questions,* Federal Trade Commission, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General%20Questions, Truy cập ngày 10/8/2025.
66. Federal Trade Commission (2016), *Fair Credit Reporting Act, 15 U.S.C. § 1681,* Federal Trade Commission, https://www.ftc.gov/system/files/fcra_2016.pdf, Truy cập ngày 3/8/2018.
67. Federal Trade Commission (2019), *FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook,* Federal Trade Commission, https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions, Truy cập ngày 11/8/2025.
68. Federal Trade Commission (2019), *Google and YouTube will pay record $170 million for alleged violations of children's privacy law,* Federal Trade Commission, https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations ?utm_source=govdelivery, Truy cập ngày 8/8/2025.
69. Flemish Decree on electronic administrative data traffic (2008), *Flemish Decree on electronic administrative data traffic*, Belgian Official Gazette (B.S.).
70. Future of Privacy Forum (nd.), *China's new comprehensive data protection law: Context, stated objectives, & key provisions,* FPF Blog, https://fpf.org/blog/chinas-new-comprehensive-data-protection-law-context-stated-objectives-key-provisions/, Truy cập ngày 13/8/2025.

71. González Fuster G, De Hert P, Gutwirth S (2008), *SWIFT and the vulnerability of transatlantic data transfers*, International Review of Law, Computers & Technology, 22:191-202.

72. Government of the People's Republic of China (2019), *Administrative Procedure Law of the People's Republic of China [Article 40 on freedom and confidentiality of correspondence],* Government of the People's Republic of China, https://english.www.gov.cn/archive/lawsregulations/201911/20/content_WS5ed8856ec6d0b3f0e949913.html, Truy cập ngày 13/8/2025.

73. Gratton É (2014), *If personal information is privacy's gatekeeper, then risk of harm is the key: A proposed method for determining what counts as personal information,* Albany Law Journal of Science & Technology, 24:1-90.

74. Greenleaf, G., & Waters, N. (2020), *Global Data Privacy Laws 2020: Strengthening Laws, Slow Enforcement*, Privacy Laws & Business International Report.

75. Greenleaf, G.W. (2014), *Asian Data Privacy Laws: Trade & Human Rights Perspectives,* Oxford University Press, Oxford.

76. Griswold v Connecticut (1965), *Griswold v Connecticut,* 381 U.S. 479.

77. Lawrence v Texas (2003), *Lawrence v Texas*, 539 U.S. 558.

78. Gualandi, S., Pareschi, L., & Peroni, S. (2022), *What do we mean by 'data'? A proposed classification of data types in the arts and humanities.*

79. Haynes v. Alfred A. Knopf, Inc. (1993), *Haynes v. Alfred A. Knopf,* Inc., 8 F.3d 1222 (7th Cir.).

80. Helscher D (1994), *Griswold v. Connecticut and the unenumerated right of privacy*, Northern Illinois University Law Review, 15:33-61.

81. Hoofnagle C (2016), *Federal Trade Commission privacy law and policy*, Cambridge University Press, New York.

82. Hornuf, L., Mangold, S. & Yang, Y. (2023), *Data Privacy and Crowdsourcing: A Comparison of Selected Problems in China, Germany and the United States, Advanced Studies in Diginomics and Digitalization,* Springer Cham, https://doi.org/10.1007/978-3-031-32064-4.

83. Iliadis, A., & Russo, F. (2016), *Critical Data Studies: An Introduction*.

84. International Labour Organization (1958), *Discrimination (Employment and Occupation) Convention,* C111, International Labour Organization.

85. ISACA (2022), *Demystifying China's Personal Information Protection Law,* ISACA Blog, https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/demystifying-chinas-personal-information-protection-law, Truy cập ngày 13/8/2025.

86. Jarrett H and Bailie M (2015), *Prosecuting Computer Crimes*, U.S. Department of Justice, https://www.justice.gov/sites/default/files/criminalccips/legacy/2015/01/14/ccmanual.pdf, Truy cập ngày 3/6/2018.

87. Kerry, C. F. (2021), *China's Personal Information Protection Law: A GDPR Lookalike or Something Else?*, Brookings Institution.

88. Kiesow Cortez, E. (ed.) (2021), *Data Protection Around the World: Privacy Laws in Action*, T.M.C. Asser Press, The Hague, https://doi.org/10.1007/978-94-6265-407-5.

89. Kingdom of Belgium (2015), *Royal Decree establishing certain ministerial competences (Belgian Official Gazette No. XX)*, Moniteur Belge.

90. Kitchin, R. (2014), *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*, SAGE.

91. Kuner, C., Bygrave, L. A., & Docksey, C. (2020), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press.

92. Lexology (không có ngày), *A Few Key Points of the China Personal Information Protection Law*, Lexology, https://www.lexology.com/library/detail.aspx?g=2830ff2c-cbcd-4a56-8ff0-852a09086169, Truy cập ngày 13/8/2025.

93. Maximillian Schrems v. Data Protection Commissioner (2015), *Case C-362/14, Judgment of the Court (Grand Chamber), ECLI:EU:C:2015:650*, EUR-Lex.

94. Mayer-Schönberger, V., & Cukier, K. (2013), *Big data: A revolution that will transform how we live, work, and think*, Houghton Mifflin Harcourt.

95. Mayer-Schönberger, V., & Cukier, K. (2013), *Big data: A revolution that will transform how we live, work, and think*, Eamon Dolan/Houghton Mifflin Harcourt.

96. McKinsey Global Institute (2011), *Big data: The next frontier for innovation, competition, and productivity*, McKinsey & Company, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation, Truy cập ngày 13/8/2025.

97. McKinsey Global Institute (2011), *Big data: The next frontier for innovation, competition, and productivity*, McKinsey & Company.

98. Nissen, H. J., Damerow, P., & Englund, R. K. (1993), *Archaic bookkeeping: Early writing and techniques of economic administration in the ancient Near East*, University of Chicago Press.

99. OECD (2015), *Data-driven innovation: Big data for growth and well-being*, OECD Publishing, https://doi.org/10.1787/9789264229358-en, Truy cập ngày 13/8/2025.

100. Privacilla.org (2002), *How U.S. state law quietly leads the way in privacy protection*, Privacilla.org, http://www.privacilla.org/releases/Torts_ Report.html, Truy cập ngày 12/8/2025.

101. PwC Indonesia (n.d.), *A comparison of cybersecurity regulations: China*, PwC, https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/china.html, Truy cập ngày 13/8/2025.

102. Reidenberg J (2000), *Resolving conflicting international data privacy rules in cyberspace*, Stanford Law Review, 52:1315-1371.

103. Ren, Z., & Li, J. (không có ngày), *China: Data protection laws and regulations*, International Comparative Legal Guide: Data Protection Laws and Regulations 2024, https://iclg.com/practice-areas/data-protection-laws-and-regulations/china, Truy cập ngày 13/8/2025.

104. Rotenberg M (2012), *The reform of the EU data protection framework-building trust in a digital and global world*, EPIC, https://epic.org/privacy/Rotenberg_EP_Testimony_10_10_12.pdf, Truy cập ngày 13/8/2025.

105. Sacks, S. (2019), *Behind the Façade of China's Cyber Super-Regulator*, DigiChina Project, Stanford University, https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/, Truy cập ngày 17/8/2025.

106. Sartor, G. (2018), *The right to data portability in the GDPR: Towards user-centric interoperability of digital services*, Computer Law & Security Review, 34(2), 193-203.

107. Schwartz P (2009), *Preemption and privacy*, Yale Law Journal, 118:902-947.

108. Schwartz P, Solove D (2014), *Reconciling personal information in the United States and European Union*, California Law Review, 102:877-916.

109. U.S. Department of Health, Education & Welfare, Secretary's Advisory Committee on Automated Personal Data Systems (1973), *Records, Computers, and the Rights of Citizens*, U.S. Department of Health and Human Services, https://aspe.hhs.gov/report/records-computers-and-rights-citizens, Truy cập ngày 13/8/2025.

110. SECRSS (2021), *《网络安全法》第七十六条第五项规定的"个人信息"如何理解？*, SECRSS, https://www.secrss.com/articles/27769, Truy cập ngày 13/8/2025.

111. Chambre (2017), *Proposed Act establishing the Data Protection Authority*, Travaux Préparatoires, Document 2648/001, pp. 103-133.

112. Shapiro, C., & Varian, H. R. (1999), *Information Rules: A Strategic Guide to the Network Economy*, Harvard Business School Press.

113. Simitis S (2010), *Privacy - an endless debate?*, California Law Review, 98:1989-2006.

114. Singapore Parliament (2020), *Personal Data Protection (Amendment) Act 2020 (PDPA)*, Singapore Statutes Online.

115. Skadden Arps Slate Meagher & Flom LLP (2021), *China's new data security and personal information protection laws: What they mean for multinationalcompanies*, Skadden, https://www.skadden.com/insights/publications/2021/11/chinas-new-data-security-and-personal-information-protection-laws, Truy cập ngày 13/8/2025.

116. Skadden, Arps, Slate, Meagher & Flom LLP (2021), *China's new data security and personal information protection laws: What they mean for multinational companies*, Connect on Tech, https://www.skadden.

com/en/insights/publications/2021/11/chinas-new-data-security-and-personal-information-protection-laws, Truy cập ngày 13/8/2025.

117. Skinner-Thompson S (2015), *Outing privacy*, Northwestern University Law Review, 110:159-222.
118. Solove D, Hartzog W (2014), *The FTC and the new common law of privacy*, Columbia Law Review, 114:583-676.
119. Solove, D. J. (2006), *A taxonomy of privacy*, University of Pennsylvania Law Review, 154(3), 477-560.
120. Sun, A. Y., & Chomiak, L. W. (2024), *China Relaxes Requirements for Cross-Border Data Transfers,* Greenberg Traurig, https://www.gtlaw.com/en/insights/2024/3/china-relaxes-requirements-for-cross-border-data-transfers, Truy cập ngày 17/8/2025.
121. Sun, K., & Li, Z. (2024), *Research on Data Security Risks and Prevention Mechanisms of Large Models under the Background of Artificial Intelligence*, Law, Education and Technology, 2(1), 32-37, https://pdf.elspublishing.com/paper/journal/open/LETE/2024/let20240004.pdf, Truy cập ngày 17/8/2025.
122. Standing Committee of the National People's Congress (2021), *Data Security Law of the People's Republic of China (President Order No. 84)*, Official Gazette of the People's Republic of China, https://en.spp.gov.cn/ 2021-06/10/c_948426.html, Truy cập ngày 13/8/2025.
123. Swire P, Ahmad K (2012), *Foundations of information privacy and data protection: A survey of global concepts, laws and practices*, International Association of Privacy Professionals, Portsmouth.
124. U.S. Department of Education (2018), *Family Educational Rights and Privacy Act*, U.S. Department of Education, https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html, Truy cập ngày 28/5/2018.

125. U.S. Department of Health & Human Services (2017), *Your rights under HIPPA*, U.S. Department of Health & Human Services, https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html, Truy cập ngày 28/5/2018.
126. U.S. Department of Justice (2013), *Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22*, U.S. Department of Justice, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285, Truy cập ngày 13/8/2025.
127. U.S. Equal Employment Opportunity Commission (2008), *The Genetic Information Nondiscrimination Act of 2008*, U.S. Equal Employment Opportunity Commission, https://www.eeoc.gov/laws/statutes/gina.cfm, Truy cập ngày 3/6/2018.
128. United Nations Commission on International Trade Law (1996), *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, 1996*, United Nations, New York.
129. United Nations Commission on International Trade Law (2022), *UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services*, United Nations.
130. United Nations Commission on International Trade Law (2024), *UNCITRAL Model Law on Automated Contracting with Guide to Enactment*, United Nations.
131. United Nations Educational, Scientific and Cultural Organization (1960), *Convention against Discrimination in Education*, UNESCO.
132. United Nations General Assembly (1990), *Guidelines concerning computerized data files (G.A. res. 45/95)*, U.N. Doc. A/45/49/Add.1.
133. United Nations (1948), *Universal Declaration of Human Rights*, G.A. Res. 217A (III), U.N. Doc A/810.

134. United Nations (1989), *Convention on the Rights of the Child*, G.A. Res. 44/25.

135. United States (1789), *U.S. Constitution, amend. IV*, National Archives, https://www.archives.gov/founding-docs/amendments-11-27#toc-amendment-iv, Truy cập ngày 13/8/2025.

136. United States (1974), *Privacy Act of 1974, 5 U.S.C. § 552a (as amended)*, U.S. Government Publishing Office, https://www.govinfo.gov/content/pkg/USCODE-2022-title5/html/USCODE-2022-title5-partI-chap5-subchapII-sec552a.htm, Truy cập ngày 13/8/2025.

137. United States (2012), *15 U.S.C. § 45 - Unfair methods of competition unlawful; prevention by Commission (as amended)*, U.S. Government Publishing Office, https://uscode.house.gov/view.xhtml?req=(title:15%20section:45%20edition:prelim, Truy cập ngày 13/8/2025.

138. Varian, H. R. (2010), *Computer mediated transactions*, American Economic Review, 100(2), 1-10.

139. Voigt, P., & von dem Bussche, A. (2017), *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer International Publishing.

140. Warren S D, Brandeis L D (1890), *The right to privacy*, Harvard Law Review, 4:193-220.

141. Whittaker, Z. (2019), *Facebook says millions of Instagram passwords were stored in plain text*, TechCrunch.

142. World Health Organization (2021), *Electronic health records: Technical and policy considerations*, WHO Press.

143. Yang, S., & Blackmore, N. (2020), *New Chinese Civil Code restates and strengthens Chinese data privacy laws*, China Law Vision,

https://www.chinalawvision.com/2020/07/uncategorized/new-chinese-civil-code-restates-and-strengthens-chinese-data-privacy-laws/, Truy cập ngày 13/8/2025.

144. Zhou, Q. (2020), *New Chinese Civil Code Restates and Strengthens Chinese Data Privacy Laws*, China Law Vision, https://www.chinalawvision.com/2020/07/uncategorized/new-chinese-civil-code-restates-and-strengthens-chinese-data-privacy-laws/, Truy cập ngày 13/8/2025.

Mục lục 3

Lời mở đầu 8

Tóm tắt nội dung 11

Câu 1: Chính sách pháp luật về dữ liệu của các nước trên thế giới? Sự cần thiết, quan điểm, mục tiêu và chính sách xây dựng, hoàn thiện quy định pháp luật về dữ liệu tại Việt Nam? 16

1.1. CHÍNH SÁCH, PHÁP LUẬT VỀ DỮ LIỆU TRONG CÁC VĂN BẢN PHÁP LUẬT QUỐC TẾ 17

1.1.1. Công ước Quốc tế về các Quyền Dân sự và Chính trị (International Covenant on Civil and Political Rights - ICCPR) năm 1966 17

1.1.2. Hướng dẫn của Liên hợp quốc về Hồ sơ dữ liệu trên máy tính (UN Guidelines on Computerized Data Files) (Nghị quyết Đại hội đồng 45/95, ngày 14 tháng 12 năm 1990) 18

1.1.3. Một số văn bản của Ủy ban Liên Hợp Quốc về Luật Thương mại Quốc tế (UNCITRAL) 22

1.1.4. Công ước về Quyền Trẻ em (Convention on the Rights of the Child - CRC) năm 1989 25

1.2. CHÍNH SÁCH, PHÁP LUẬT VỀ DỮ LIỆU TẠI MỘT SỐ QUỐC GIA, KHU VỰC TRÊN THẾ GIỚI 29

1.2.1. Liên minh châu Âu 39

1.2.1.1. Quy định Bảo vệ Dữ liệu Chung (GDPR) và Đạo Luật dữ liệu Châu Âu (EU Data Act) 39

- Về mục tiêu chính sách 42

- Tổng quan các nội dung lớn của Đạo luật Dữ liệu Châu Âu 44

- Một số khái niệm 47

- Các nguyên tắc nền tảng 56

- Quyền và nghĩa vụ của cá nhân đối với dữ liệu 61

- Quyền và nghĩa vụ của các "doanh nghiệp số" 69

- Tác động của Đạo luật dữ liệu đối với nền kinh tế và xã hội 76

1.2.1.2. Luật Quản trị dữ liệu (DGA) 76

1.2.1.3. Những điểm mạnh của mô hình pháp luật dữ liệu tại EU 80

1.2.1.4. Một số hạn chế và thách thức trong quá trình thực thi chính sách, pháp luật về dữ liệu tại EU 85

1.2.2. Hoa Kỳ 87

1.2.2.1. Tu chính án thứ Tư (The Fourth Amendment) 89

1.2.2.2. Luật chuyên ngành 91

1.2.2.3. Hành vi xâm phạm quyền riêng tư 94

1.2.2.4. Ủy ban Thương mại Liên bang 95

1.2.2.5. Hệ thống Cơ sở dữ liệu tại Hoa Kỳ 98

1.2.3. Trung Quốc 99

1.2.3.1. Tổng quan về chính sách, pháp luật về dữ liệu tại Trung Quốc 99

1.2.3.2. Các nguyên tắc và quy định chính 108

1.2.3.3. Ưu, nhược điểm của khung pháp luật về dữ liệu tại Trung Quốc 112

1.2.4. Hàn Quốc 123

1.2.5. Nhật Bản 134

1.2.6. Bỉ 144

1.2.6.1. Tổng quan về pháp luật dữ liệu tại Bỉ 144

1.2.6.2. Bối cảnh bảo vệ dữ liệu ở Bỉ trước GDPR 146

1.2.6.3. Đạo luật Bảo vệ Dữ liệu năm 1992 148

1.2.6.4. Các vấn đề mới liên quan đến GDPR 153

1.2.7. Thổ Nhĩ Kỳ 163

1.2.7.1. Tổng quan về Luật Bảo vệ Dữ liệu của Thổ Nhĩ Kỳ.. 163

1.2.7.2. Sự tương tác giữa GDPR và chính sách pháp luật của Thổ Nhĩ Kỳ..... 170

1.2.7.3. Các vấn đề nổi bật..... 179

1.2.8. Liên bang Nga..... 187

1.2.9. Ấn Độ..... 193

1.2.10. Đan Mạch..... 196

1.2.11. Úc 197

1.2.12. Các quốc gia Đông Nam Á (ASEAN) 200

- Singapore 201

- Malaysia 218

- Thái lan 227

- Indonesia 227

- Philippines..... 228

1.2.13. Một số quốc gia khác 230

1.2.14. So sánh các mô hình chính sách pháp luật về dữ liệu và bài học kinh nghiệm cho Việt Nam 234

1.2.14.1. Điểm tương đồng trong chính sách, pháp luật về dữ liệu của các quốc gia 234

1.2.14.2. Sự tương tác giữa GDPR và pháp luật Hoa Kỳ 238

1.2.14.3. Điểm khác trong chính sách pháp luật về dữ liệu giữa Trung Quốc và Liên minh châu Âu 244

1.2.14.4. Bài học kinh nghiệm cho Việt Nam trong xây dựng chính sách pháp luật về dữ liệu..... 249

1.3. SỰ CẦN THIẾT XÂY DỰNG VÀ HOÀN THIỆN PHÁP LUẬT VỀ DỮ LIỆU Ở VIỆT NAM 257

1.3.1. Bối cảnh trong nước và quốc tế 257

1.3.1.1. Xu hướng toàn cầu về xây dựng và ban hành chính sách pháp luật về dữ liệu 257

1.3.1.2. Bối cảnh trong nước 276

1.3.2. Cơ sở chính trị 282

1.3.3. Cơ sở thực tiễn 315

1.4. QUAN ĐIỂM, MỤC TIÊU VÀ ĐỊNH HƯỚNG CHÍNH SÁCH XÂY DỰNG, HOÀN THIỆN PHÁP LUẬT VỀ DỮ LIỆU TẠI VIỆT NAM 336

1.4.1. Quan điểm chỉ đạo 336

1.4.2. Mục đích 343

1.4.3. Định hướng chính sách xây dựng, hoàn thiện pháp luật về dữ liệu tại Việt Nam 351

1.4.3.1. Quy định về xây dựng, phát triển, quản trị, xử lý dữ liệu, ứng dụng khoa học công nghệ trong xử lý dữ liệu, quản lý nhà nước về dữ liệu 359

1.4.3.2. Quy định về Cơ sở dữ liệu tổng hợp quốc gia 378

1.4.3.3. Quy định về Trung tâm dữ liệu quốc gia 380

1.4.3.4. Quy định về các sản phẩm, dịch vụ liên quan đến dữ liệu 387

Câu 2: Quyền, nghĩa vụ và trách nhiệm của chủ thể dữ liệu, chủ sở hữu dữ liệu, chủ quản dữ liệu? Cơ chế bảo đảm thực hiện các quyền, nghĩa vụ này đối với tổ chức, cá nhân không phải là cơ quan nhà nước? 391

2.1. MỘT SỐ KHÁI NIỆM CÓ LIÊN QUAN 392

2.1.1. Dữ liệu 392

2.1.1.1. Dữ liệu số 392

2.1.1.2. Đặc điểm của dữ liệu 407

2.1.1.3. Phân loại 415

2.1.2. Chủ thể dữ liệu 423

2.1.3. Chủ sở hữu dữ liệu 428

2.1.4. Chủ quản dữ liệu 436

2.2. QUYỀN, NGHĨA VỤ VÀ TRÁCH NHIỆM CỦA CHỦ THỂ DỮ LIỆU, CHỦ SỞ HỮU DỮ LIỆU, CHỦ QUẢN DỮ LIỆU 438

2.2.1. Quyền, nghĩa vụ và trách nhiệm của chủ thể dữ liệu 438

2.2.1.1. Về quyền của chủ thể dữ liệu 438

2.2.1.2. Nghĩa vụ của chủ thể dữ liệu 452

2.2.2.3. Trách nhiệm của chủ thể dữ liệu 458

2.2.2. Quyền, nghĩa vụ và trách nhiệm của chủ quản dữ liệu 464

2.2.2.1. Quyền của chủ quản dữ liệu 464

2.2.2.2. Nghĩa vụ của chủ quản dữ liệu 467

2.2.2.3. Trách nhiệm của chủ quản dữ liệu 473

2.2.3. Quyền, nghĩa vụ và trách nhiệm của chủ sở hữu dữ liệu 475

2.2.3.1. Quyền của chủ sở hữu dữ liệu 475

2.2.3.2. Nghĩa vụ của chủ sở hữu dữ liệu 482

2.2.3.3. Trách nhiệm của chủ sở hữu dữ liệu 489

2.3. CƠ CHẾ BẢO ĐẢM THỰC HIỆN CÁC QUYỀN, NGHĨA VỤ TRÊN ĐỐI VỚI TỔ CHỨC, CÁ NHÂN KHÔNG PHẢI LÀ CƠ QUAN NHÀ NƯỚC 491

Câu 3: Quy định về hành vi bị nghiêm cấm trong Luật Dữ liệu năm 2024? Giải pháp xây dựng, hoàn thiện quy định pháp luật về xử lý vi phạm hành chính trong lĩnh vực dữ liệu? 500

3.1. MỘT SỐ HÀNH VI BỊ NGHIÊM CẤM TRONG PHÁP LUẬT VỀ DỮ LIỆU Ở MỘT SỐ QUỐC GIA TRÊN THẾ GIỚI 501

3.2. CÁC HÀNH VI BỊ NGHIÊM CẤM TRONG PHÁP LUẬT VỀ DỮ LIỆU TẠI VIỆT NAM 505

3.3. MỘT SỐ HẠN CHẾ, VƯỚNG MẮC TRONG QUY ĐỊNH CỦA PHÁP LUẬT VỀ XỬ LÝ VI PHẠM HÀNH CHÍNH VỀ DỮ LIỆU TẠI VIỆT NAM 522

3.4. MỘT SỐ GIẢI PHÁP HOÀN THIỆN QUY ĐỊNH PHÁP LUẬT VỀ XỬ LÝ VI PHẠM HÀNH CHÍNH TRONG LĨNH VỰC DỮ LIỆU . 527

3.4.1. Nghiên cứu, xây dựng quy định của pháp luật về xử lý vi phạm hành chính trong lĩnh vực dữ liệu theo hướng bổ sung vào Luật Xử lý vi phạm hành chính các quy định liên quan đến xử lý vi phạm hành chính trong lĩnh vực dữ liệu; trên cơ sở đó, nghiên cứu, xây dựng Nghị định của Chính phủ quy định về xử phạt vi phạm hành chính trong lĩnh vực dữ liệu. 527

3.4.2. Rà soát để đề xuất sửa đổi, bổ sung các văn bản quy phạm pháp luật khác có liên quan đến xử lý vi phạm hành chính trong lĩnh vực dữ liệu, bảo đảm tính thống nhất trong hệ thống văn bản quy phạm pháp luật có liên quan. 539

3.4.3. Tổ chức thu thập thông tin, các ý kiến đề xuất xây dựng quy định về xử phạt hành chính đối với hành vi vi phạm pháp luật trên lĩnh vực dữ liệu 542

3.4.4. Tăng cường hợp tác quốc tế, tiếp thu các bài học kinh nghiệm quốc tế để hoàn thiện hơn việc xử lý vi phạm dữ liệu 546

Danh mục tài liệu tham khảo 550