

HỌC VIỆN CHÍNH TRỊ QUỐC GIA HỒ CHÍ MINH

CAO NGUYỄN HÙNG

BẢO VỆ QUYỀN ĐỐI VỚI DỮ LIỆU CÁ NHÂN
TRONG XÂY DỰNG CHÍNH QUYỀN SỐ CẤP TỈNH
Ở VIỆT NAM

LUẬN ÁN TIẾN SĨ

NGÀNH: PHÁP LUẬT VỀ QUYỀN CON NGƯỜI

MÃ SỐ: Đào tạo thí điểm

HÀ NỘI - 2026

HỌC VIỆN CHÍNH TRỊ QUỐC GIA HỒ CHÍ MINH

CAO NGUYỄN HÙNG

**BẢO VỆ QUYỀN ĐỐI VỚI DỮ LIỆU CÁ NHÂN
TRONG XÂY DỰNG CHÍNH QUYỀN SỐ CẤP TỈNH
Ở VIỆT NAM**

LUẬN ÁN TIẾN SĨ
NGÀNH: PHÁP LUẬT VỀ QUYỀN CON NGƯỜI
MÃ SỐ: Đào tạo thí điểm

Người hướng dẫn khoa học: 1. PGS.TS Vũ Trọng Lâm



2. TS Trần Thị Hồng Hạnh



HÀ NỘI - 2026

LỜI CAM ĐOAN

Tôi cam đoan Luận án ***“Bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh ở Việt Nam”*** là công trình nghiên cứu của tôi. Các nội dung nghiên cứu và kết quả được trình bày trong Luận án là hoàn toàn trung thực và chưa từng được công bố. Tôi hoàn toàn chịu trách nhiệm về lời cam đoan này.

Tác giả luận án



CAO NGUYỄN HÙNG

MỤC LỤC

MỞ ĐẦU	1
Chương 1: TỔNG QUAN TÌNH HÌNH NGHIÊN CỨU LIÊN QUAN ĐẾN ĐỀ TÀI	10
1.2. Tình hình nghiên cứu ở ngoài nước liên quan đến đề tài luận án.....	221
1.3. Những vấn đề luận án tiếp tục nghiên cứu.....	333
1.4. Giả thuyết và câu hỏi nghiên cứu.....	365
Chương 2: CƠ SỞ LÝ LUẬN VỀ BẢO VỆ QUYỀN ĐỐI VỚI DỮ LIỆU CÁ NHÂN TRONG XÂY DỰNG CHÍNH QUYỀN SỐ CẤP TỈNH	388
2.1. Khái niệm, đặc điểm, vai trò của bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh.....	388
2.2. Nội dung, phương thức và các yếu tố tác động đến bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh	522
2.3. Pháp luật quốc tế và kinh nghiệm của một số nước về bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số	678
Chương 3: THỰC TRẠNG BẢO VỆ QUYỀN ĐỐI VỚI DỮ LIỆU CÁ NHÂN TRONG XÂY DỰNG CHÍNH QUYỀN SỐ CẤP TỈNH Ở VIỆT NAM	988
3.1. Khái quát chung thực trạng và các yếu tố tác động đến xây dựng chính quyền số cấp tỉnh liên quan đến dữ liệu cá nhân	988
3.2. Thực trạng triển khai các nội dung, phương thức bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh ở Việt Nam.....	113
3.3. Đánh giá thực trạng về bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh	146
Chương 4: QUAN ĐIỂM, GIẢI PHÁP BẢO VỆ QUYỀN ĐỐI VỚI DỮ LIỆU CÁ NHÂN TRONG XÂY DỰNG CHÍNH QUYỀN SỐ CẤP TỈNH Ở VIỆT NAM HIỆN NAY	167
4.1. Dự báo bối cảnh và các yếu tố tác động đến bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh trong thời gian tới....	167

4.2. Quan điểm bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh ở Việt Nam.....	172
4.3. Giải pháp về bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh ở Việt Nam.....	1755
5. Lộ trình thực hiện	191
KẾT LUẬN	196
DANH MỤC CÁC CÔNG TRÌNH KHOA HỌC ĐÃ CÔNG BỐ CỦA TÁC GIẢ LIÊN QUAN ĐẾN LUẬN ÁN.....	199
DANH MỤC TÀI LIỆU THAM KHẢO.....	200

DANH MỤC TỪ VIẾT TẮT

Chữ viết tắt

Chữ viết đầy đủ

CĐS	:	Chuyển đổi số
CNS	:	Công nghệ số
CNTT	:	Công nghệ thông tin
CP	:	Chính phủ
CQS	:	Chính quyền số
CSL	:	Luật An ninh mạng
DLCN	:	Dữ liệu cá nhân
DSL	:	Luật An ninh dữ liệu
IOC.	:	Trung tâm giám sát, điều hành thông minh
NQ	:	Nghị quyết
NĐ	:	Nghị định
NXB	:	Nhà xuất bản
PIPL	:	Luật Bảo vệ thông tin cá nhân
QCN	:	Quyền con người
QĐ	:	Quyết định
SOC	:	Điều hành an toàn thông tin
TTg	:	Thủ tướng
TTHC	:	Thủ tục hành chính
TW	:	Trung ương
UBND	:	Ủy ban nhân dân
VJST	:	Tạp chí Khoa học & Công nghệ Việt Nam
VNeID	:	Hệ thống định danh điện tử
AI	:	Artificial intelligence (Trí tuệ nhân tạo)
IoT	:	Internet of Things (Internet vạn vật)
EU	:	European Union (Liên minh Châu Âu)
APEC	:	Asia-Pacific Economic Cooperation (Diễn đàn Hợp tác Kinh tế châu Á - Thái Bình Dương)
GDPR	:	General Data Protection Regulation (Quy định chung về bảo vệ dữ liệu)

ICCPR	:	International Covenant on Civil and Political Rights (Công ước quốc tế về các quyền dân sự và chính trị)
ICT	:	Information and Communication Technologies (Công nghệ thông tin và truyền thông)
OECD	:	Organisation for Economic Co-operation and Development (Tổ chức Hợp tác và Phát triển Kinh tế)
ASEAN	:	Association of South East Asian Nations (Hiệp hội các quốc gia Đông Nam Á)
OZG	:	Onlinezugangsgesetz
DPIA	:	Data Protection Impact Assessment
EGDI	:	E-Government Development Index

MỞ ĐẦU

1. Tính cấp thiết của đề tài

Trong bối cảnh Cách mạng công nghiệp lần thứ tư diễn ra sâu rộng, dữ liệu, đặc biệt là dữ liệu cá nhân (DLCN), đã trở thành nguồn tài nguyên quan trọng, có vai trò nền tảng đối với quá trình phát triển kinh tế - xã hội, đổi mới quản trị quốc gia và xây dựng chính quyền số. Ở Việt Nam, chủ trương chuyển đổi số quốc gia, xây dựng Chính phủ số, chính quyền số được Đảng và Nhà nước xác định là một trong những nhiệm vụ trọng tâm, mang tính chiến lược lâu dài. Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII của Đảng khẳng định yêu cầu *“đẩy mạnh chuyển đổi số quốc gia, phát triển kinh tế số, xã hội số; xây dựng Chính phủ số, chính quyền số, đô thị thông minh”* [24] và nhấn mạnh quản trị dữ liệu là trụ cột quan trọng trong tiến trình này. Nghị quyết số 57-NQ/TW, ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia cũng đã xác định rõ *“Phát triển hạ tầng, nhất là hạ tầng số, công nghệ số trên nguyên tắc hiện đại, đồng bộ, an ninh, an toàn, hiệu quả, tránh lãng phí; làm giàu, khai thác tối đa tiềm năng của dữ liệu, đưa dữ liệu thành tư liệu sản xuất chính, thúc đẩy phát triển nhanh cơ sở dữ liệu lớn, công nghiệp dữ liệu, kinh tế dữ liệu”* [4]. Văn kiện Đại hội đại biểu toàn quốc lần thứ XIV của Đảng nhấn mạnh *“lấy khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số làm động lực chính”* [25]. Trong bối cảnh đó, vấn đề bảo vệ quyền đối với DLCN đặt ra như một yêu cầu tất yếu, có ý nghĩa vừa cấp bách, vừa lâu dài.

Chính quyền số cấp tỉnh giữ vai trò đặc biệt quan trọng trong hệ thống quản trị nhà nước ở Việt Nam. Trên môi trường số, chính quyền số cấp tỉnh trực tiếp tổ chức thực hiện phần lớn các chính sách công, quản lý nhiều lĩnh vực liên quan trực tiếp đến đời sống người dân và cung cấp các dịch vụ công thiết yếu. Quá trình xây dựng chính quyền số đòi hỏi các cơ quan nhà nước ở địa phương phải thường xuyên thu thập, lưu trữ, kết nối, chia sẻ và xử lý khối lượng rất lớn dữ liệu cá nhân trong các lĩnh vực như dân cư, hộ tịch, đất đai, y tế, giáo dục, lao động, việc làm, bảo hiểm, an sinh xã hội, thuế và nhiều lĩnh vực khác. Cấp tỉnh đồng thời là đầu mối kết nối giữa cơ sở dữ liệu quốc gia với các cơ sở dữ liệu chuyên ngành và cơ sở dữ liệu địa phương, là nơi diễn ra hoạt động chia sẻ dữ liệu giữa nhiều cơ quan, tổ chức trong quá trình quản lý nhà nước. Vì vậy, việc bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh có ý nghĩa đặc biệt quan trọng, tác động trực tiếp đến hiệu quả quản trị nhà nước và niềm tin của người dân đối với chính quyền số. Cùng với những lợi ích mà chuyển đổi số mang lại qua hoạt động của chính quyền số cấp tỉnh,

một thách thức hiện nay là những nguy cơ xâm phạm quyền đối với DLCN đang gia tăng. Thực tiễn thời gian qua cho thấy, tình trạng lộ, lọt, mua bán trái phép DLCN, khai thác dữ liệu không đúng mục đích, không có sự đồng ý của chủ thể dữ liệu diễn ra ngày càng phức tạp, gây ảnh hưởng nghiêm trọng đến quyền, lợi ích hợp pháp của cá nhân, làm suy giảm niềm tin của xã hội đối với hoạt động của cơ quan nhà nước và tiến trình chuyển đổi số. Trong khi đó, ở cấp tỉnh, năng lực bảo đảm an toàn dữ liệu, nhận thức pháp lý về quyền đối với DLCN, cũng như cơ chế kiểm soát quyền lực trong thu thập, xử lý dữ liệu vẫn còn những hạn chế nhất định. Điều này đặt ra yêu cầu phải nghiên cứu một cách hệ thống, chuyên sâu về bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh, nhằm góp phần khắc phục những bất cập hiện nay.

Bảo vệ quyền đối với DLCN là yêu cầu nội tại của Nhà nước pháp quyền xã hội chủ nghĩa Việt Nam, nơi quyền con người (QCN), quyền công dân được tôn trọng, bảo vệ và bảo đảm theo Hiến pháp và pháp luật. Việt Nam đang trong quá trình đẩy mạnh chuyển đổi số và hoàn thiện hành lang pháp lý về quyền dữ liệu, nhằm tham gia sâu vào các hiệp định thương mại tự do thế hệ mới và hợp tác quốc tế, vì vậy, cần chuẩn hóa quy trình bảo vệ dữ liệu theo các tiêu chuẩn chặt chẽ. Hiến pháp năm 2013 đã ghi nhận quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân, bí mật gia đình và trách nhiệm của Nhà nước trong việc bảo vệ các quyền này. Trên cơ sở đó, nhiều văn bản pháp luật đã được ban hành nhằm bảo vệ thông tin cá nhân và bảo đảm an toàn dữ liệu trong môi trường số. Đặc biệt, việc Quốc hội thông qua Luật Bảo vệ dữ liệu cá nhân, có hiệu lực từ ngày 01/01/2026 đã đánh dấu bước phát triển quan trọng trong quá trình hoàn thiện hệ thống pháp luật về quyền con người trong môi trường số ở Việt Nam. Đây là lần đầu tiên Việt Nam có một đạo luật chuyên ngành điều chỉnh toàn diện các quan hệ liên quan đến dữ liệu cá nhân, xác lập rõ hơn quyền của chủ thể dữ liệu và trách nhiệm của các chủ thể tham gia xử lý dữ liệu. Tuy nhiên, việc ban hành luật mới chỉ là bước khởi đầu. Thách thức lớn hiện nay là tổ chức thực hiện hiệu quả các quy định của pháp luật trong thực tiễn xây dựng và vận hành chính quyền số cấp tỉnh. Nhiều vấn đề mới đang đặt ra như bảo đảm quyền của chủ thể dữ liệu trong hoạt động quản lý nhà nước; kiểm soát việc thu thập, xử lý, chia sẻ dữ liệu giữa các cơ quan nhà nước; xác định trách nhiệm pháp lý khi xảy ra vi phạm; xây dựng cơ chế giám sát, kiểm tra và xử lý các hành vi xâm phạm dữ liệu cá nhân; bảo đảm sự cân bằng giữa yêu cầu khai thác dữ liệu phục vụ phát triển kinh tế - xã hội với yêu cầu bảo vệ quyền con người. Đây là những vấn đề có tính lý luận và thực tiễn

cấp bách cần được nghiên cứu để bảo đảm tính khả thi và hiệu quả của pháp luật về bảo vệ dữ liệu cá nhân trong giai đoạn hiện nay.

Bên cạnh đó, giai đoạn 2026 - 2030 được xác định là giai đoạn tăng tốc xây dựng Chính phủ số và chính quyền số trên phạm vi toàn quốc. Các địa phương đang triển khai mạnh mẽ việc xây dựng cơ sở dữ liệu dùng chung, trung tâm dữ liệu, nền tảng số và các hệ thống chia sẻ dữ liệu phục vụ quản lý nhà nước. Quy mô và mức độ xử lý dữ liệu cá nhân ngày càng lớn, trong khi năng lực quản trị dữ liệu, nguồn nhân lực, điều kiện kỹ thuật và cơ chế kiểm soát ở nhiều địa phương vẫn còn những hạn chế nhất định. Điều này làm gia tăng nguy cơ phát sinh các hành vi xâm phạm quyền đối với dữ liệu cá nhân và đặt ra yêu cầu cấp thiết phải hoàn thiện cơ sở lý luận, pháp luật và cơ chế bảo đảm thực thi quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh.

Từ góc độ khoa học pháp lý, mặc dù đã có một số công trình nghiên cứu về dữ liệu cá nhân, bảo vệ dữ liệu cá nhân, quyền riêng tư, chính phủ điện tử hoặc chính quyền số, song các nghiên cứu chuyên sâu, có tính hệ thống về bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh ở Việt Nam còn tương đối hạn chế. Đặc biệt, chưa có nhiều công trình tiếp cận vấn đề này dưới góc độ quyền con người, gắn với yêu cầu xây dựng Nhà nước pháp quyền xã hội chủ nghĩa, thực hiện chuyển đổi số quốc gia và triển khai Luật Bảo vệ dữ liệu cá nhân trong thực tiễn hoạt động của chính quyền địa phương. Trên cơ sở đó, nghiên cứu sinh đã lựa chọn đề tài: ***“Bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh ở Việt Nam”*** làm đề tài luận án tiến sĩ pháp luật về QCN.

2. Mục tiêu và nhiệm vụ nghiên cứu của đề tài

2.1. Mục tiêu nghiên cứu

Trên cơ sở nghiên cứu những vấn đề lý luận và thực tiễn về bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh ở Việt Nam, luận án sẽ đi sâu phân tích, đánh giá thực trạng bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh nhằm góp phần hoàn thiện về mặt lý luận; từ đó đề xuất các giải pháp hiệu quả về bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh ở Việt Nam hiện nay, bảo đảm sự cân bằng giữa mục tiêu phát triển công nghệ quản trị với mục tiêu tôn trọng, bảo vệ và thúc đẩy quyền con người, quyền công dân.

2.2. Nhiệm vụ nghiên cứu

Để đạt được mục tiêu trên, luận án thực hiện các nhiệm vụ chủ yếu sau:

Một là, nghiên cứu tổng quan những công trình khoa học có liên quan đến bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh ở Việt Nam và trên thế giới, nhằm đánh giá những nội dung đã được nghiên cứu, đồng thời chỉ ra những vấn đề cần tiếp tục nghiên cứu của đề tài.

Hai là, nghiên cứu, làm rõ cơ sở lý luận cơ bản về quyền đối với DLCN trong xây dựng chính quyền số, gồm: khái niệm, đặc điểm, vai trò, nội dung, hình thức, phương pháp, các yếu tố tác động, pháp luật quốc tế, pháp luật của một số quốc gia trên thế giới và những giá trị tham khảo cho Việt Nam; mối liên hệ với quyền riêng tư, QCN trong bối cảnh chuyển đổi số.

Ba là, nghiên cứu, phân tích, đánh giá thực trạng pháp luật và thực tiễn bảo vệ DLCN trong quá trình xây dựng chính quyền số cấp tỉnh ở Việt Nam hiện nay, từ đó nhận diện các bất cập, hạn chế và nguyên nhân của hạn chế.

Bốn là, đề xuất các quan điểm, giải pháp, kiến nghị hoàn thiện chính sách, pháp luật và nâng cao năng lực thực thi nhằm bảo vệ tốt hơn quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh ở Việt Nam hiện nay.

3. Đối tượng và phạm vi nghiên cứu của đề tài

3.1. Đối tượng nghiên cứu

Đối tượng nghiên cứu của luận án là hệ thống các quan hệ xã hội, các quan điểm lý luận, quy định pháp luật và thực tiễn thực thi pháp luật về bảo vệ quyền đối với dữ liệu cá nhân trong tiến trình xây dựng chính quyền số cấp tỉnh ở Việt Nam. Cụ thể:

Về mặt lý luận: Nghiên cứu hệ thống quan điểm học thuật, tư tưởng pháp lý về quyền đối với dữ liệu cá nhân dưới góc độ quyền con người, quyền công dân; nội hàm, đặc điểm, các nguyên tắc và tiêu chí bảo đảm quyền này trong môi trường quản trị công ở cấp độ địa phương.

Về mặt thể chế pháp lý: Nghiên cứu các quy định của pháp luật Việt Nam hiện hành, trọng tâm là Nghị định số 13/2023/NĐ-CP, Luật số 91/2026/QH15 về Bảo vệ dữ liệu cá nhân và các văn bản hướng dẫn thi hành, các quy định liên quan đến cấu trúc chính quyền số cấp tỉnh, như: quy định về trách nhiệm pháp lý của cơ quan nhà

nước cấp tỉnh (HĐND, UBND, các sở, ban, ngành) và các chủ thể liên quan trong xử lý dữ liệu; quy định về các biện pháp bảo đảm an ninh, an toàn dữ liệu (mã hóa, phân quyền, kiểm soát truy cập); quy định về cơ chế liên thông, chia sẻ dữ liệu và cơ chế kiểm soát, thanh tra, kiểm tra việc bảo vệ quyền đối với dữ liệu cá nhân tại địa phương.

Về mặt thực tiễn: Nghiên cứu thực trạng tổ chức thực hiện pháp luật, những rào cản, xung đột lợi ích, các hành vi vi phạm và bất cập trong cơ chế vận hành hệ thống chính quyền số cấp tỉnh hiện nay dưới góc độ bảo vệ quyền con người.

3.2. Phạm vi nghiên cứu

- *Về phạm vi nội dung:* Về mặt lý luận và thực tiễn, việc xây dựng chính quyền số cấp tỉnh tác động đến nhiều khía cạnh quản trị công. Tuy nhiên, dưới tiếp cận của khoa học pháp lý về quyền con người, Luận án tập trung nghiên cứu khía cạnh bảo vệ quyền đối với dữ DLCN trong mối quan hệ pháp lý song phương giữa Công dân (Chủ thể mang quyền) và Chính quyền địa phương cấp tỉnh (Chủ thể mang nghĩa vụ bảo vệ). Để bảo đảm tính tập trung và giải quyết đúng những “điểm nóng” thực tiễn, Luận án giới hạn phạm vi nội dung vào 03 không gian tương tác công vụ cốt lõi sau đây, bởi các lý do khoa học cụ thể:

Thứ nhất, lĩnh vực giải quyết Thủ tục hành chính (TTHC): Đây là không gian giao thoa mang tính bắt buộc, nơi công dân có nghĩa vụ pháp lý phải cung cấp DLCN (hộ tịch, đất đai, lý lịch tư pháp, tài chính...) để đổi lấy các quyết định hành chính hoặc quyền lợi hợp pháp. Đây là lĩnh vực thể hiện rõ nhất tính bất cân xứng về quyền lực thông tin giữa bộ máy hành chính và cá nhân. Việc nghiên cứu phạm vi này nhằm đánh giá việc tuân thủ các nguyên tắc cốt lõi về “giới hạn mục đích” và “tối thiểu hóa dữ liệu” tại Bộ phận Một cửa các cấp, ngăn ngừa nguy cơ lạm dụng quyền lực công để thu thập tràn lan dữ liệu ngoài quy định của luật.

Thứ hai, lĩnh vực cung cấp Dịch vụ công (DVC) trực tuyến: Đây là không gian tương tác số hóa hoàn toàn thông qua Cổng dịch vụ công trực tuyến và các ứng dụng công dân số cấp tỉnh (như iHanoi, Hue-S...). Phạm vi này là nơi công dân thực thi trực tiếp các quyền tự quyết thông tin như: quyền truy cập, tra cứu lịch sử xử lý, đính chính, rút lại sự đồng ý hoặc yêu cầu xóa dữ liệu. Nghiên cứu phạm vi này giúp làm rõ thực trạng chính quyền số đã thiết lập các công cụ kỹ thuật và quy trình hành chính để bảo đảm quyền thực chất cho người dân hay chưa, đồng thời kiểm soát rủi ro từ

sự tham gia của các doanh nghiệp công nghệ (Bên thứ ba xử lý dữ liệu) trong mô hình thuê dịch vụ CNTT.

Thứ ba, lĩnh vực Quản trị xã hội thông minh: Đây là phạm vi chính quyền số cấp tỉnh ứng dụng các công nghệ hiện đại (dữ liệu lớn - Big Data, trí tuệ nhân tạo - AI, hệ thống camera nhận diện trắc sinh học và giám sát đô thị tại Trung tâm IOC) để điều hành trật tự, giao thông và an ninh địa phương. Khác với TTHC và DVC (vốn xử lý dữ liệu có hồ sơ cụ thể), quản trị xã hội bằng công nghệ mới thu thập dữ liệu công dân theo thời gian thực (Real-time) trên diện rộng mà không dựa trên sự đồng ý trước của chủ thể dữ liệu. Việc lựa chọn phạm vi này nhằm giải quyết bài toán mâu thuẫn giữa yêu cầu tối ưu hóa quản lý đô thị với nghĩa vụ chống lạm quyền giám sát, chống phân biệt đối xử số và bảo vệ bí mật đời tư Hiến định của công dân. Đặc biệt là dựa trên hệ thống văn bản quy phạm pháp luật quốc tế (Điều 17 Công ước ICCPR, chuẩn mực GDPR) và pháp luật Việt Nam, trọng tâm là: Hiến pháp năm 2013 (các quy định về quyền con người, quyền riêng tư), Nghị định số 13/2023/NĐ-CP, Luật Bảo vệ dữ liệu cá nhân (Luật số 91/2025/QH15), cùng các văn bản quy phạm pháp luật chuyên ngành (Luật Căn cước, Luật An ninh mạng, Luật Lưu trữ...) và các Quy chế quản lý dữ liệu do HĐND, UBND cấp tỉnh ban hành tính đến thời điểm hiện tại.

- *Về không gian*: Luận án tập trung vào cá nhân là công dân có DLCN do các cơ quan nhà nước và hệ thống thông tin chính quyền số cấp tỉnh thu thập, lưu trữ, kết nối, chia sẻ và khai thác; nghiên cứu hành vi công vụ, thẩm quyền, trách nhiệm pháp lý và trách nhiệm giải trình của các cơ quan nhà nước thuộc cấu trúc chính quyền địa phương cấp tỉnh (HĐND, UBND cấp tỉnh, các sở, ban, ngành chuyên môn) và các đơn vị trực tiếp vận hành hạ tầng số cấp tỉnh (Trung tâm Giám sát điều hành thông minh - IOC, Trung tâm Chuyển đổi số, Cổng dịch vụ công trực tuyến tỉnh). Phân tích chính sách, pháp luật ở cấp quốc gia, đi sâu đánh giá thực tiễn triển khai ở một số địa phương đại diện (các tỉnh, thành phố như: Hà Nội, Quảng Ninh, Nghệ An, Huế, Đà Nẵng, Quảng Ngãi, Bình Dương, Thành phố Hồ Chí Minh).

- *Về thời gian*: Luận án tập trung nghiên cứu thực trạng thực thi pháp luật trong giai đoạn từ năm 2020 đến năm 2025 và 6 tháng đầu năm 2026 (Giai đoạn đẩy mạnh chuyển đổi số theo Chương trình chuyển đổi số quốc gia). Các giải pháp, kiến nghị và tầm nhìn của luận án hướng tới giai đoạn từ nay đến năm 2030, tầm nhìn 2035, phù hợp với Chương trình Chuyển đổi số quốc gia của Chính phủ.

4. Cơ sở lý luận và phương pháp nghiên cứu của đề tài

4.1. Cơ sở lý luận

Đề tài được thực hiện dựa trên phương pháp luận duy vật biện chứng, duy vật lịch sử của chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh và quan điểm của Đảng, Nhà nước ta về QCN, quyền công dân.

4.2. Phương pháp nghiên cứu

Đề tài kết hợp sử dụng các phương pháp nghiên cứu dưới đây để giải quyết các nhiệm vụ nghiên cứu đặt ra:

- *Phương pháp nghiên cứu tài liệu* được sử dụng làm nền tảng cho toàn bộ quá trình nghiên cứu. Thông qua việc thu thập, lựa chọn và khai thác có hệ thống các công trình nghiên cứu trong và ngoài nước, tài liệu khoa học, báo cáo chuyên đề, văn bản chính sách và văn bản quy phạm pháp luật có liên quan, luận án hình thành cơ sở lý luận và thực tiễn cho việc phân tích quyền đối với DLCN trong bối cảnh xây dựng chính quyền số cấp tỉnh. Việc nghiên cứu tài liệu giúp xác định khung khái niệm, cách tiếp cận pháp lý, cũng như các vấn đề đã được nghiên cứu và những khoảng trống cần tiếp tục làm rõ.

- *Phương pháp phân tích - thống kê - tổng hợp* được sử dụng để nghiên cứu, đánh giá các quan điểm, lý thuyết, cách tiếp cận pháp lý và quy định pháp luật hiện hành liên quan đến quyền đối với DLCN. Trên cơ sở phân tích từng yếu tố cấu thành như nguyên tắc xử lý dữ liệu, quyền của chủ thể dữ liệu, nghĩa vụ của cơ quan xử lý dữ liệu và cơ chế bảo đảm thực thi, luận án tiến hành tổng hợp nhằm làm rõ mức độ đầy đủ, thống nhất và hợp lý của pháp luật Việt Nam trong bảo vệ quyền đối với DLCN, đặc biệt trong hoạt động của chính quyền cấp tỉnh. Kết quả tổng hợp là cơ sở để đánh giá thực trạng và đề xuất giải pháp hoàn thiện.

- *Phương pháp so sánh* được vận dụng để đối chiếu pháp luật Việt Nam về bảo vệ quyền đối với DLCN với pháp luật của một số quốc gia và khu vực có hệ thống bảo vệ dữ liệu phát triển như Đức, Trung Quốc, Liên bang Nga, Singapo, Thái Lan. Việc so sánh tập trung vào các nội dung cốt lõi như: phạm vi bảo vệ quyền DLCN, điều kiện xử lý dữ liệu trong khu vực công, quyền của chủ thể dữ liệu, cơ chế giám sát và chế tài xử lý vi phạm. Trên cơ sở đó, luận án rút ra các bài học kinh nghiệm có giá trị tham khảo và đề xuất hướng hoàn thiện pháp luật Việt Nam phù hợp với điều kiện thể chế và thực tiễn xây dựng chính quyền số cấp tỉnh.

- *Phương pháp phỏng vấn/tham vấn chuyên gia, nhà quản lý* được sử dụng nhằm phản ánh khách quan tình hình thực tiễn triển khai bảo vệ quyền đối với DLCN tại cấp tỉnh. Thông qua việc thu thập thông tin từ các báo cáo, tài liệu thực tiễn, kết quả trao đổi, nắm bắt thực tiễn các chuyên gia, nhà quản lý và cán bộ trực tiếp tham

gia vận hành hệ thống thông tin, luận án làm rõ cách thức xử lý, chia sẻ và bảo vệ quyền đối với DLCN trong thực tế. Phương pháp này giúp đánh giá khoảng cách giữa quy định pháp luật và thực tiễn thực thi, nhận diện những khó khăn, vướng mắc và rủi ro phát sinh trong quá trình xây dựng chính quyền số.

- *Phương pháp hệ thống hóa - logic và quy nạp* được sử dụng trong việc sắp xếp, tổ chức nội dung nghiên cứu và xây dựng lập luận khoa học cho luận án. Trên cơ sở phương pháp này, các vấn đề nghiên cứu được trình bày theo trật tự logic từ cơ sở lý luận, khung pháp lý, thực trạng triển khai đến các kiến nghị hoàn thiện. Đồng thời, phương pháp này giúp bảo đảm tính thống nhất, chặt chẽ và liên kết giữa các giải pháp đề xuất, hướng tới việc xây dựng cơ chế bảo vệ quyền đối với DLCN mang tính đồng bộ trong quá trình phát triển chính quyền số cấp tỉnh.

- *Phương pháp luận biện chứng* được vận dụng để xem xét vấn đề bảo vệ quyền đối với DLCN trong mối quan hệ tương tác giữa yêu cầu phát triển chính quyền số và yêu cầu bảo vệ QCN, quyền công dân. Phương pháp này cho phép phân tích các mâu thuẫn và thách thức phát sinh trong thực tiễn, như nhu cầu chia sẻ dữ liệu để nâng cao hiệu quả quản lý nhà nước với nguy cơ xâm phạm quyền đối với DLCN, qua đó làm rõ tính tất yếu của việc thiết lập cơ chế cân bằng giữa hiệu quả quản trị và bảo vệ quyền cá nhân.

- *Phương pháp nghiên cứu điển hình* được sử dụng để phân tích sâu một số trường hợp tiêu biểu trong triển khai chính quyền số và bảo vệ quyền đối với DLCN ở cấp tỉnh. Việc lựa chọn các điển hình dựa trên mức độ phát triển chính quyền số, đặc điểm kinh tế - xã hội và tính đặc thù của lĩnh vực xử lý dữ liệu. Thông qua nghiên cứu điển hình, luận án làm rõ các mô hình triển khai, cách thức quản trị dữ liệu và những vấn đề thực tiễn phát sinh, từ đó rút ra nhận xét và kiến nghị có giá trị khái quát.

5. Những đóng góp mới của đề tài

Đây là công trình khoa học nghiên cứu về bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh một cách toàn diện và có hệ thống. Kết quả nghiên cứu của luận án sẽ có một số đóng góp mới về mặt khoa học như sau:

Thứ nhất, luận án góp phần hệ thống hóa và làm rõ cơ sở lý luận về bảo vệ quyền đối với DLCN trong bối cảnh xây dựng chính quyền số cấp tỉnh, cụ thể là các khái niệm cốt lõi, nguyên tắc, nội dung quyền và phương thức bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh trong điều kiện liên thông dữ liệu, số hóa quy trình thủ tục hành chính và cung cấp dịch vụ công trực tuyến.

Thứ hai, luận án xây dựng và phát triển khung phân tích pháp lý - quản trị đa tầng để nghiên cứu và đánh giá hiệu quả bảo vệ quyền đối với DLCN trong chính quyền số cấp tỉnh, bao gồm: tầng chuẩn mực pháp luật quốc tế về QCN và quyền

riêng tư; tầng pháp luật và thể chế quốc gia về bảo vệ DLCN và quản trị dữ liệu trong cơ quan nhà nước; tầng vận hành ở địa phương gắn với mô hình tổ chức, quy trình nghiệp vụ và hạ tầng kỹ thuật số.

Trên nền tảng đó, luận án làm rõ mối quan hệ giữa quyền của chủ thể dữ liệu và nghĩa vụ của các chủ thể tham gia xử lý dữ liệu (cơ quan quản lý cơ sở dữ liệu, cơ quan khai thác sử dụng, đơn vị vận hành hệ thống, đơn vị cung cấp nền tảng kỹ thuật), qua đó nhấn mạnh yêu cầu trách nhiệm giải trình, minh bạch và kiểm soát quyền lực dữ liệu trong khu vực công.

Thứ ba, luận án thực hiện nghiên cứu so sánh có chọn lọc thông qua các nghiên cứu pháp luật quốc tế về quyền đối với DLCN và pháp luật một số quốc gia điển hình như: Đức, Liên bang Nga, Trung Quốc, Singapo, Thái Lan, qua đó rút ra các bài học có giá trị tham khảo cho Việt Nam.

Thứ tư, trên cơ sở đánh giá thực trạng ở cấp tỉnh, luận án chỉ ra các hạn chế và thách thức đặc thù trong bảo vệ quyền đối với DLCN, tập trung vào các vấn đề như: nguy cơ tái sử dụng dữ liệu vượt mục đích trong liên thông dữ liệu; thiếu minh bạch đối với chủ thể dữ liệu; hạn chế về cơ chế thực thi quyền (tiếp cận, chỉnh sửa, hạn chế xử lý, phản đối, rút lại sự đồng ý); bất cập trong truy vết và chứng minh vi phạm; cũng như hiệu lực răn đe và cơ chế khôi phục quyền, khắc phục hậu quả. Từ đó, luận án cung cấp luận cứ khoa học cho việc hoàn thiện cơ chế bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh, phục vụ hoạch định chính sách, xây dựng quy chế vận hành và nâng cao năng lực thực thi ở địa phương.

6. Ý nghĩa lý luận và thực tiễn của đề tài

6.1. Ý nghĩa lý luận

Luận án là công trình nghiên cứu toàn diện, chuyên sâu về bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh ở nước ta. Luận án cung cấp nhiều kiến thức, thông tin, luận điểm và đề xuất mới có giá trị tham khảo với việc thúc đẩy quyền này ở nước ta trong thời gian tới.

6.2. Ý nghĩa thực tiễn

Luận án là tài liệu tham khảo cho việc giảng dạy, nghiên cứu chuyên ngành QCN ở Viện Quyền con người, Học viện Chính trị quốc gia Hồ Chí Minh và các cơ sở đào tạo khác của nước ta.

7. Kết cấu của luận án

Ngoài phần mở đầu, phần kết luận, danh mục tài liệu tham khảo và phụ lục, nội dung của luận án được kết cấu thành 4 chương, 12 tiết.

Chương 1

TỔNG QUAN TÌNH HÌNH NGHIÊN CỨU LIÊN QUAN ĐẾN ĐỀ TÀI

1.1. TÌNH HÌNH NGHIÊN CỨU TRONG NƯỚC LIÊN QUAN ĐẾN ĐỀ TÀI LUẬN ÁN

1.1.1. Các công trình nghiên cứu về Chính phủ điện tử, chính quyền số trong bối cảnh chuyển đổi số quốc gia

Trong bối cảnh chuyển đổi số quốc gia đang được đẩy mạnh, nghiên cứu về Chính phủ điện tử và chính quyền số ở Việt Nam phát triển nhanh cả về số lượng lẫn chiều sâu nội dung. Nhìn tổng thể, các công trình trong nước không chỉ tiếp cận từ góc độ công nghệ, mà còn mở rộng sang quản trị công, pháp lý, tổ chức bộ máy và cung ứng dịch vụ công. Trên cơ sở đó, có thể phân nhóm các hướng nghiên cứu tiêu biểu trong nước như sau.

Thứ nhất, các công trình nghiên cứu tập trung vào hệ thống khái niệm, đặc trưng và mô hình phát triển.

Trong nhóm nghiên cứu nền tảng về khái niệm, đặc trưng và mô hình của Chính phủ điện tử/chính quyền số, các công trình trong nước nhìn chung khởi đầu từ yêu cầu xác lập đối tượng nghiên cứu: làm rõ Chính phủ điện tử là gì, phạm vi đến đâu và ranh giới phân biệt với Chính phủ số/chính quyền số. Theo đó, cuốn sách “*Chính phủ điện tử*” của tác giả Nguyễn Đăng Hậu, Nguyễn Hoài Anh, Cao Thu Hoài, năm 2010, NXB Thông tin và Truyền thông, Hà Nội, chủ yếu hệ thống hóa tổng quan về Chính phủ điện tử, đồng thời phân tích các nội dung trụ cột như kiến trúc, dịch vụ công, giao dịch điện tử, tổ chức hệ thống thông tin và kinh nghiệm triển khai ở một số quốc gia. Các tác giả cho rằng Chính phủ điện tử không chỉ là ứng dụng CNTT đơn lẻ, mà là công cụ cải cách quản trị thông qua chuẩn hóa quy trình và nâng cao năng lực cung ứng dịch vụ công [42]. Đề cập sâu hơn đến yếu tố quản trị và pháp lý, cuốn sách của các tác giả Nguyễn Thị Quế Anh, Vũ Công Giao, Vũ Ngọc Anh, Nguyễn Thị Minh Hà “*Chính phủ mở, chính phủ điện tử và quản trị nhà nước hiện đại*”, năm 2019 NXB Hồng Đức, Hà Nội, tập trung luận giải mối liên hệ giữa Chính phủ mở/Chính phủ điện tử với mô hình quản trị hiện đại. Nghiên cứu của các tác giả nhấn mạnh Chính phủ điện tử như một phần thúc đẩy minh bạch hóa, tăng cường trách nhiệm giải trình và cải thiện chất lượng quản trị, không còn xem Chính phủ điện tử là sự tin học hóa hoạt động hành chính [2].

Một số giáo trình tiêu biểu có liên quan như *Giáo trình Chính phủ điện tử: Dành cho đào tạo đại học ngành Quản lý nhà nước*, của các tác giả Bế Trung Anh (chủ biên), Nguyễn Mạnh Hùng, Nguyễn Đình Quý, Dương Văn Ninh, NXB Bách khoa Hà Nội, năm 2020, trình bày từ cơ sở hình thành và phát triển, tác động kinh tế - xã hội, đến vấn đề kiến trúc và tham chiếu kinh nghiệm quốc tế và Việt Nam. Qua đó, giáo trình cung cấp cơ sở pháp lý theo hướng quản trị và tổ chức thực thi [1]; giáo trình của TS. Đỗ Văn Thắng (chủ biên) *Giáo trình Chính phủ điện tử và văn phòng điện tử*, NXB Đại học Quốc gia TP.HCM, năm 2023, hướng đến kết nối giữa lý luận và thực tiễn xây dựng Chính phủ điện tử - văn phòng điện tử, nhấn mạnh trọng tâm số hóa vận hành nội bộ, chuẩn hóa quy trình và nâng cao năng lực tổ chức, từ đó đặt nền cho việc hình thành năng lực số của khu vực công [52].

Những nghiên cứu nền tảng này còn được củng cố bởi các công trình chuyên sâu và bài viết khoa học, vừa bổ sung chiều sâu lý luận, vừa mở rộng luận cứ cho mô hình triển khai. Luận án tiến sĩ của Phạm Hải Sơn, *Nghiên cứu đề xuất một số giải pháp công nghệ trong xây dựng khung kiến trúc Chính phủ điện tử tại Việt Nam*, Viện Công nghệ Thông tin - Đại học Quốc gia Hà Nội, năm 2024 phản ánh cách tiếp cận Chính phủ điện tử như một hệ thống kiến trúc cần phương pháp luận xây dựng và giải pháp triển khai tương thích với khung kiến trúc ở Việt Nam [51]; qua đó đóng góp về khung kỹ thuật nhằm chuyển hóa định hướng chính sách thành hệ thống cụ thể. Ở phương diện quản trị nhà nước, bài viết của Vũ Công Giao và Nguyễn Văn Quân “*Chính phủ điện tử và quản trị nhà nước hiện đại*”, VNU Journal of Science: Legal Studies, Vol. 35, No. 3, năm 2019 đã nhấn mạnh sự gắn kết giữa Chính phủ điện tử với cải cách hành chính và quản trị hiện đại, đặc biệt là định hướng lấy người dân làm trung tâm và nâng cao hiệu lực, hiệu quả quản trị trong môi trường số [30]; bài viết của Bùi Ngọc Hiền “*Xây dựng chính quyền số hiện nay*” trên Tạp chí Quản lý nhà nước, số 09/2021, làm rõ cách hiểu về chính quyền số và các đặc điểm then chốt như dữ liệu số, môi trường tác nghiệp số, liên thông nội bộ gắn với phục vụ người dân/doanh nghiệp; đồng thời gợi mở lộ trình triển khai theo chuỗi bước số hóa dữ liệu - số hóa quy trình - ứng dụng công nghệ - vận hành và kiểm soát, góp phần cụ thể hóa nội hàm khái niệm trong điều kiện Việt Nam [33].

Thứ hai, các công trình tiếp cận dưới góc độ thể chế, chính sách và pháp luật.

Các công trình trong nước thường phân tích yêu cầu hoàn thiện thể chế số, các

hành lang pháp lý cho dữ liệu, định danh và xác thực điện tử, chia sẻ - kết nối dữ liệu, bảo vệ DLCN, an toàn thông tin mạng, cũng như cơ chế trách nhiệm giải trình trong môi trường số. Theo hướng tiếp cận này, luận án tiến sĩ của Nguyễn Thị Thục “*Hoàn thiện pháp luật về tổ chức và hoạt động của Chính phủ đáp ứng yêu cầu quản trị quốc gia hiện đại ở Việt Nam*”, năm 2025 tại Học viện Chính trị Quốc gia Hồ Chí Minh, Hà Nội hướng trọng tâm nghiên cứu vào việc nâng cấp nền tảng pháp lý của bộ máy hành pháp theo các tiêu chí quản trị hiện đại như minh bạch, trách nhiệm giải trình, sự tham gia và hiệu lực, hiệu quả, qua đó gợi mở khung thể chế để Chính phủ số không dừng ở tin học hóa mà trở thành một phương thức quản trị mới [57]. Cùng với đó, cuốn sách của Đặng Minh Tuấn (chủ biên), “*Pháp luật trong bối cảnh cách mạng công nghiệp lần thứ tư*” NXB Chính trị quốc gia Sự thật, năm 2021 tiếp cận Chính phủ điện tử như một “bài toán pháp lý liên ngành”, đặt trong chính thể các vấn đề pháp luật của thời đại số (chính phủ điện tử, an ninh mạng, AI...), nhấn mạnh nhu cầu đồng bộ hóa pháp luật để theo kịp tốc độ đổi mới công nghệ [59].

Ở góc độ hạ tầng pháp lý cho dữ liệu và niềm tin số, các bài viết khoa học có xu hướng xem bảo vệ DLCN là điều kiện tiên quyết để mở rộng dịch vụ công số và liên thông dữ liệu, như bài viết của các tác giả Nguyễn Minh Thu, Đỗ Thị Kim Lương và Trần Thị Thanh Mai “*Khung pháp lý về bảo vệ DLCN trong bối cảnh xây dựng Chính phủ số tại Việt Nam*” trên Tạp chí Công Thương, số 9/2025, đã phân tích tình trạng phân tán thuật ngữ, hiệu lực của văn bản dưới luật và yêu cầu nâng chuẩn lập pháp, qua đó làm rõ mối liên hệ giữa bảo vệ DLCN, năng lực cung ứng dịch vụ công trực tuyến và mức độ tin cậy của người dân đối với Chính phủ số [53]. Cũng theo hướng thể chế hóa hoạt động cung cấp dịch vụ số, bài viết của Bùi Quốc Lộc, “*Dịch vụ công trực tuyến đến chính quyền điện tử: một số yêu cầu và giải pháp*”, Tạp chí Quản lý nhà nước, số tháng 6/2025 đã nhấn mạnh vai trò của khuôn khổ chính sách, pháp luật trong chuẩn hóa quy trình, tổ chức thực thi, đánh giá kết quả cuối cùng (mức độ người dân/doanh nghiệp thực sự sử dụng dịch vụ), qua đó phản ánh chuyển dịch trọng tâm từ “có dịch vụ” sang “dịch vụ hiệu quả” [39].

Ở nhóm nghiên cứu về kiến trúc, nền tảng số và quản trị dữ liệu - liên thông, các công trình trong nước chủ yếu tiếp cận theo hướng “kỹ thuật hóa” các khái niệm Chính phủ điện tử/chính quyền số thành khung kiến trúc, mô hình kết nối - tích hợp, chuẩn dữ liệu và cơ chế dùng chung. Điển hình là tài liệu khung kiến trúc do cơ quan quản lý nhà nước ban hành như Bộ Thông tin và Truyền thông, *Khung Kiến trúc*

Chính phủ điện tử Việt Nam - Phiên bản 1.0 (ban hành kèm Văn bản số 1178/BTTTT-THH, ngày 21/4/2015), Hà Nội, tháng 4/2015 [10]. Cùng với đó là một số bài viết trên tạp chí chuyên ngành đi sâu vào “hạ tầng liên thông dữ liệu” như một giải pháp kỹ thuật - quản trị để hiện thực hóa kiến trúc, điển hình như bài viết của tác giả Phúc Lâm “*Kết nối và chia sẻ dữ liệu thông qua nền tảng tích hợp chia sẻ dữ liệu quốc gia*”, Tạp chí Ngân hàng điện tử, ngày 5/4/2024, phân tích vai trò hạ tầng trung gian phục vụ kết nối, tích hợp, chia sẻ dữ liệu trên quy mô quốc gia, đồng thời mô tả các thành phần chức năng nhằm kiểm soát truy cập, xác thực, cấp quyền và bảo đảm an toàn trong trao đổi dữ liệu liên cơ quan [118]; bài viết của Đỗ Hưng “*Hơn 90 bộ, ngành, địa phương, tổ chức kết nối nền tảng tích hợp, chia sẻ dữ liệu quốc gia*”, Tạp chí Khoa học & Công nghệ Việt Nam điện tử, ngày 30/6/2023 cho thấy cách tiếp cận đánh giá hiệu quả kiến trúc không chỉ dừng ở “có khung”, mà được phản ánh qua mức độ kết nối, số lượng hệ thống/cơ sở dữ liệu tham gia và năng lực cung cấp dịch vụ dữ liệu dùng chung, tức chuyển trọng tâm từ xây dựng sang vận hành và mở rộng kết nối dữ liệu [117].

Trong thời gian qua, vấn đề xây dựng Chính phủ điện tử, Chính phủ số và chính quyền số trong bối cảnh chuyển đổi số quốc gia và Cách mạng công nghiệp lần thứ tư đã được nhiều cơ quan nghiên cứu và nhà khoa học trong nước quan tâm. Ở cấp độ nghiên cứu chính sách, tiêu biểu là đề tài khoa học cấp Bộ của Học viện Chính trị quốc gia Hồ Chí Minh “*Phát triển chính quyền số trong bối cảnh cách mạng công nghiệp lần thứ tư*”, trong đó tập trung làm rõ cơ sở lý luận, thực tiễn và định hướng phát triển chính quyền số ở Việt Nam, tạo nền tảng học thuật cho các nghiên cứu tiếp theo.

Trên các tạp chí khoa học chuyên ngành, nhiều công trình đã phân tích khái niệm, đặc trưng và yêu cầu phát triển Chính phủ điện tử, Chính phủ số, như: bài viết “*Cơ hội, thách thức trong xây dựng Chính phủ điện tử hướng tới Chính phủ số ở Việt Nam hiện nay*”, của Đỗ Thị Tâm trên Tạp chí Quản lý nhà nước điện tử, ngày 27/4/2023, đã phân tích những thuận lợi và khó khăn trong quá trình chuyển tiếp từ Chính phủ điện tử sang Chính phủ số, đồng thời đề xuất một số giải pháp thúc đẩy tiến trình này trong điều kiện Việt Nam [119]; tác giả Đinh Thị Hương Giang (2020) với bài viết “*Những rào cản trong xây dựng Chính phủ số ở Việt Nam hiện nay*”, tiếp cận theo hướng nhận diện các điểm nghẽn, trên Tạp chí Lý luận chính trị, số 12/2020, đã chỉ ra các rào cản chủ yếu về thể chế, tổ chức bộ máy, nguồn nhân lực và hạ tầng

công nghệ trong quá trình xây dựng Chính phủ số ở Việt Nam [28]. Ở góc độ phân tích mô hình và giải pháp chính sách, tác giả Lại Đức Vượng và Nguyễn Thị Sự trong bài “*Chính phủ số và giải pháp xây dựng Chính phủ số ở Việt Nam hiện nay*”, Tạp chí Tổ chức nhà nước, tháng 7/2024, đã làm rõ những đặc điểm khác biệt cơ bản giữa Chính phủ số và Chính phủ điện tử, xác định mục tiêu xây dựng Chính phủ số ở Việt Nam và đề xuất các nhóm giải pháp mang tính thể chế, tổ chức và công nghệ [66]; tác giả Hoàng Thị Kim Chi với bài “*Thực trạng và giải pháp xây dựng Chính phủ điện tử hướng tới Chính phủ số ở Việt Nam*”, Tạp chí Tổ chức nhà nước, số 10/2023, đã đánh giá quá trình xây dựng Chính phủ điện tử của Việt Nam và đề xuất các giải pháp nhằm tiếp tục thúc đẩy chuyển đổi sang Chính phủ số [11].

Ngoài ra, một số công trình tiếp cận từ góc độ chuyên ngành quản lý thông tin và lưu trữ, như bài viết “*Xây dựng Chính quyền điện tử - Thực trạng và đề xuất một số giải pháp*” của tác giả Lê Văn Năng, năm 2024 đã làm rõ khái niệm, cơ sở pháp lý, hạ tầng thông tin và thực trạng ứng dụng CNTT trong cơ quan nhà nước, qua đó đề xuất các giải pháp công nghệ để tiến tới Chính quyền điện tử [41].

Nhìn chung, các công trình nghiên cứu nêu trên đã tiếp cận tương đối toàn diện các vấn đề về khái niệm, đặc trưng, vai trò, mô hình và giải pháp xây dựng Chính phủ điện tử, Chính phủ số và chính quyền số ở Việt Nam. Tuy nhiên, các nghiên cứu này chủ yếu tập trung vào khía cạnh quản trị, tổ chức bộ máy, hạ tầng công nghệ và cải cách hành chính, trong khi vấn đề bảo vệ quyền đối với DLCN trong quá trình xây dựng chính quyền số, đặc biệt ở cấp tỉnh, mới chỉ được đề cập gián tiếp, chưa trở thành đối tượng nghiên cứu chuyên sâu dưới góc độ pháp lý. Đây là khoảng trống nghiên cứu mà luận án hướng tới làm rõ.

1.1.2. Các công trình nghiên cứu về bảo vệ dữ liệu cá nhân và bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số

1.1.2.1. Các công trình nghiên cứu về bảo vệ DLCN trong xây dựng chính quyền số

Trong những năm gần đây, cùng với tiến trình chuyển đổi số quốc gia và xây dựng chính quyền số, vấn đề bảo vệ DLCN và quyền đối với DLCN ngày càng nhận được sự quan tâm của giới nghiên cứu pháp lý, quản lý nhà nước và hoạch định chính sách ở Việt Nam.

Trước hết, về nhóm công trình mang tính lý luận nền tảng, tiêu biểu là luận án tiến sĩ “*Hoàn thiện pháp luật về bảo vệ thông tin cá nhân ở Việt Nam hiện nay*”

(2018) của Trần Thị Hồng Hạnh. Luận án tiếp cận quyền bảo vệ thông tin cá nhân như một bộ phận của QCN, quyền công dân trong Nhà nước pháp quyền XHCN Việt Nam, tập trung phân tích khái niệm thông tin cá nhân, nội dung quyền bảo vệ thông tin cá nhân, các nguyên tắc xử lý thông tin cá nhân, cũng như các yếu tố bảo đảm thực thi quyền này. Đặc biệt, công trình đã đặt vấn đề hoàn thiện pháp luật bảo vệ thông tin cá nhân trong mối liên hệ với yêu cầu xây dựng chính phủ điện tử, coi đây là bối cảnh tất yếu làm gia tăng nguy cơ xâm phạm quyền riêng tư và quyền đối với DLCN [32].

Bên cạnh các luận án, nhóm sách chuyên khảo, sách tham khảo và kỷ yếu hội thảo khoa học đóng vai trò quan trọng trong việc hệ thống hóa và cập nhật các vấn đề lý luận - thực tiễn về bảo vệ DLCN, điển hình như Kỷ yếu hội thảo khoa học *“Pháp luật về bảo vệ DLCN trong kỷ nguyên số: Những vấn đề lý luận và thực tiễn ở Việt Nam hiện nay”*, Nxb Công an nhân dân, năm 2023. Kỷ yếu tập hợp nhiều bài viết của các nhà khoa học, chuyên gia pháp lý và nhà quản lý, tiếp cận vấn đề bảo vệ DLCN dưới nhiều góc độ khác nhau, từ lý luận chung, kinh nghiệm quốc tế, cho đến thực trạng pháp luật và thực tiễn áp dụng tại Việt Nam. Nội dung kỷ yếu làm rõ những thách thức đặt ra đối với bảo vệ DLCN trong bối cảnh số hóa mạnh mẽ các hoạt động của Nhà nước, doanh nghiệp và xã hội, qua đó cung cấp cơ sở học thuật quan trọng cho việc nghiên cứu quyền bảo vệ DLCN trong xây dựng chính quyền số [58].

Đặc biệt, trong thời gian gần đây đã có các bài viết chuyên đề tiếp cận trực tiếp mối quan hệ giữa bảo vệ DLCN và xây dựng chính quyền số. Trong các công trình trong nước về bảo vệ quyền đối với DLCN, bài viết của Vũ Công Giao, Lê Trần Như Tuyên (2020), *“Bảo vệ quyền đối với DLCN trong pháp luật quốc tế, pháp luật ở một số quốc gia và giá trị tham khảo cho Việt Nam”*, Tạp chí Nghiên cứu Lập pháp, số 09 (409) là một nghiên cứu mang tính nền tảng. Công trình phân tích khái niệm và bản chất của quyền đối với DLCN trong bối cảnh toàn cầu hóa và số hóa, tiếp cận quyền này như một quyền cơ bản của con người. Trên cơ sở đó, các tác giả hệ thống hóa các quy định pháp luật quốc tế quan trọng liên quan đến bảo vệ DLCN, đặc biệt là Công ước quốc tế về các quyền dân sự và chính trị (ICCPR), Công ước châu Âu về bảo vệ cá nhân đối với xử lý DLCN (Convention 108) và Quy định bảo vệ dữ liệu chung của Liên minh châu Âu (GDPR). Bài viết cũng so sánh pháp luật của một số quốc gia và khu vực như Liên minh châu Âu, Hoa Kỳ và Nhật Bản, làm rõ các khung pháp lý tiên tiến và các nguyên tắc xử lý dữ liệu như đồng thuận, giới hạn mục đích, bảo mật và minh bạch.

Trên cơ sở đánh giá thực trạng pháp luật Việt Nam, công trình chỉ ra việc thiếu một đạo luật riêng về bảo vệ DLCN, các quy định còn rời rạc và thiếu cơ chế thực thi hiệu quả, từ đó đề xuất ban hành Luật Bảo vệ DLCN, thiết lập cơ quan quản lý chuyên trách, áp dụng các nguyên tắc “*privacy by design*” (Bảo vệ quyền riêng tư ngay từ khâu thiết kế), “*privacy by default*” (Bảo vệ quyền riêng tư theo mặc định) và khẳng định bảo vệ DLCN là quyền cơ bản của con người [29].

Tiếp cận vấn đề trong bối cảnh cách mạng công nghiệp lần thứ tư, các tác giả Bùi Duy Khánh, Trần Minh Phú, Dương Yến Nhi (2021), “*Bảo vệ DLCN trong giai đoạn cách mạng công nghiệp 4.0 - Bài học kinh nghiệm của các quốc gia trên thế giới*”, Báo cáo tổng kết đề tài nghiên cứu khoa học, Trường Đại học Luật Hà Nội đã phân tích các thách thức mới đối với bảo vệ DLCN khi các công nghệ như trí tuệ nhân tạo, Internet vạn vật và dữ liệu lớn được ứng dụng rộng rãi. Công trình so sánh mô hình pháp lý và thực tiễn bảo vệ DLCN tại Liên minh châu Âu, Hoa Kỳ, Nhật Bản và Hàn Quốc, từ đó rút ra bài học kinh nghiệm cho Việt Nam. Trên cơ sở đó, nhóm tác giả đề xuất hoàn thiện khung pháp lý, ban hành luật riêng về bảo vệ DLCN, nâng cao nhận thức xã hội và phát triển hạ tầng CNTT an toàn [37]. Công trình cung cấp cơ sở lý luận và thực tiễn quan trọng cho nghiên cứu bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh, song chưa phân tích sâu đặc thù quản lý dữ liệu của chính quyền địa phương.

Ở góc độ phương pháp tiếp cận so sánh pháp luật, tác giả Hoàng Văn Đoàn, Mai Văn Thắng (2018), “*Ảnh hưởng của pháp luật phương Tây đến pháp luật Nhật Bản trong lịch sử và những giá trị tham khảo đối với Việt Nam trong bối cảnh hiện nay*”, Tạp chí Khoa học Đại học Quốc gia Hà Nội, Luật học, Tập 34, Số 3 đã nghiên cứu quá trình Nhật Bản tiếp nhận pháp luật phương Tây theo hướng chọn lọc, phù hợp với điều kiện kinh tế - xã hội và văn hóa bản địa. Mặc dù không trực tiếp đề cập đến bảo vệ DLCN hay chính quyền số, công trình có giá trị lý luận quan trọng trong việc gợi mở phương pháp tiếp cận đối với Việt Nam khi xây dựng các đạo luật mới, trong đó có Luật Bảo vệ DLCN, theo hướng nội luật hóa có chọn lọc các chuẩn mực pháp lý quốc tế [26].

Trong mạch nghiên cứu pháp luật so sánh chuyên sâu, tác giả Lê Xuân Tùng (2020), trong bài viết “*Bảo vệ DLCN tại Nhật Bản thông qua Đạo luật về Bảo vệ thông tin cá nhân và một số khuyến nghị đối với Việt Nam*”, đăng tải trên Tạp chí Nghiên cứu Lập pháp, số 13 (413) đã phân tích hệ thống pháp luật Nhật Bản về bảo vệ DLCN thông qua Đạo luật về Bảo vệ thông tin cá nhân (APPI), làm rõ các nguyên tắc xử lý dữ liệu, quyền của chủ thể dữ liệu, trách nhiệm của bên xử lý dữ liệu và cơ

chế thực thi thông qua Ủy ban Bảo vệ Thông tin cá nhân. Trên cơ sở đó, tác giả khuyến nghị Việt Nam ban hành đạo luật riêng về bảo vệ DLCN, thành lập cơ quan quản lý độc lập và nâng cao nhận thức xã hội về quyền đối với DLCN. Công trình cung cấp mô hình tham chiếu phù hợp cho Việt Nam trong quá trình xây dựng thể chế bảo vệ quyền đối với DLCN trong bối cảnh chính quyền số [61].

Bên cạnh các nghiên cứu so sánh, một số công trình tập trung đánh giá thực trạng pháp luật Việt Nam. Tác giả Lê Khánh Tùng trong bài viết “*Một số vấn đề về bảo vệ quyền riêng tư trong không gian internet*”, Khoa Luật - Đại học Quốc gia Hà Nội chỉ ra khoảng trống pháp lý trong bảo vệ quyền riêng tư trên môi trường Internet, đặc biệt là việc giới hạn quyền chưa được quy định đầy đủ bằng luật, chưa bảo đảm nguyên tắc hiến định tại Hiến pháp năm 2013 [60]. Trong khi đó, bài viết của Nguyễn Văn Cương (2020) “*Thực trạng pháp luật về bảo vệ thông tin cá nhân ở Việt Nam hiện nay và hướng hoàn thiện*”, Tạp chí Nghiên cứu Lập pháp, số 15 (415) đã phân tích hệ thống các quy định pháp luật hiện hành và chỉ ra những hạn chế như thiếu đạo luật chuyên biệt, quy định thiếu đồng bộ và cơ chế thực thi chưa hiệu quả, từ đó đề xuất ban hành Luật Bảo vệ thông tin cá nhân và tăng cường cơ chế giám sát, xử lý vi phạm [22]; Bạch Thị Nhã Nam (2022), trong bài viết “*Hướng tiếp cận và hoàn thiện pháp luật bảo vệ DLCN tại Việt Nam trước tác động lập pháp của thế giới và khu vực*”, Tạp chí Luật học đã tổng quan các mô hình pháp luật bảo vệ DLCN tiêu biểu trên thế giới và khu vực như Liên minh châu Âu, Nhật Bản, Hàn Quốc, Singapore và ASEAN, đồng thời đánh giá thực trạng pháp luật Việt Nam và đề xuất xây dựng Luật Bảo vệ DLCN riêng biệt, thiết lập cơ quan giám sát độc lập và hoàn thiện cơ chế thực thi [40]. Tuy nhiên, các công trình nêu trên nhìn chung mới tiếp cận bảo vệ DLCN ở bình diện chung hoặc so sánh pháp luật, chưa làm rõ một cách hệ thống vấn đề bảo vệ quyền đối với DLCN trong quá trình xây dựng và vận hành chính quyền số, đặc biệt ở cấp tỉnh. Đây chính là khoảng trống nghiên cứu mà luận án tập trung làm rõ.

1.1.2.2. Công trình nghiên cứu về bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số

Trong hệ thống các công trình nghiên cứu trong nước, nhóm sách chuyên khảo, sách tham khảo và giáo trình đóng vai trò quan trọng trong việc hình thành nền tảng lý luận cho nghiên cứu bảo vệ quyền đối với DLCN, đặc biệt khi đặt trong bối cảnh xây dựng chính quyền số và Nhà nước pháp quyền XHCN Việt Nam. Trước hết, cuốn sách của Thái Thị Tuyết Dung, “*Quyền tiếp cận thông tin và quyền riêng tư ở Việt Nam và một số quốc gia*” đã tiếp cận vấn đề quyền riêng tư trong mối quan hệ với

quyền tiếp cận thông tin và yêu cầu minh bạch của hoạt động công quyền [27]. Công trình này làm rõ tính hai mặt của việc mở rộng tiếp cận thông tin và ứng dụng CNTT trong quản lý nhà nước: một mặt góp phần nâng cao hiệu quả quản trị, mặt khác làm gia tăng nguy cơ xâm phạm đời sống riêng tư và thông tin cá nhân.

Về pháp luật dân sự, cuốn sách của Đỗ Văn Đại, *“Bình luận khoa học những điểm mới của Bộ luật dân sự năm 2015”*, có giá trị trong việc làm rõ nội hàm các quyền nhân thân, đặc biệt là quyền về đời sống riêng tư, bí mật cá nhân và cơ chế bảo vệ các quyền này trong hệ thống pháp luật Việt Nam [23]. Mặc dù không trực tiếp đề cập đến khái niệm DLCN theo nghĩa hiện đại, tác giả xem DLCN như một dạng thông tin gắn liền với nhân thân của cá nhân, từ đó đặt nền tảng pháp lý để mở rộng nghiên cứu bảo vệ DLCN trong môi trường số, đồng thời cho thấy việc xây dựng và vận hành chính quyền số cần được đặt trong khuôn khổ bảo vệ quyền nhân thân, chứ không chỉ dừng lại ở các biện pháp kỹ thuật hay quản lý hành chính.

Từ góc độ QCN và cơ sở hiến định, *“Giáo trình Lý luận và pháp luật về QCN”* của Khoa Luật - Đại học Quốc gia Hà Nội cung cấp hệ khái niệm và nguyên tắc bảo đảm QCN trong pháp luật quốc tế và pháp luật Việt Nam, qua đó tạo nền tảng lý luận để tiếp cận quyền bảo vệ DLCN như một quyền gắn với nhân phẩm, đời sống riêng tư và quyền tự do cá nhân. Giáo trình đặt vấn đề bảo vệ DLCN trong mối quan hệ với nghĩa vụ của Nhà nước trong việc tôn trọng, bảo vệ và bảo đảm QCN, đặc biệt trong bối cảnh Nhà nước sử dụng công nghệ số và dữ liệu lớn để quản lý xã hội [38]. Trên cơ sở đó, yêu cầu xây dựng chính quyền số cần được tiếp cận đồng thời như một quá trình đổi mới phương thức quản trị và một quá trình tái cấu trúc cơ chế bảo đảm QCN trong môi trường số.

Cùng với đó, cuốn sách của Viện Khoa học pháp lý - Bộ Tư pháp, *“Quyền con người trong Hiến pháp năm 2013 - Quan điểm mới, cách tiếp cận mới và các quy định mới”*, góp phần làm rõ cơ sở hiến định của các quyền liên quan đến đời sống riêng tư, bí mật cá nhân và nguyên tắc hạn chế QCN. Nghiên cứu nhấn mạnh rằng mọi sự hạn chế quyền chỉ có thể được thực hiện theo luật, trên cơ sở tính cần thiết, tương xứng và vì lợi ích chung [65]. Đây là luận cứ quan trọng để đánh giá tính hợp hiến của các hoạt động thu thập, chia sẻ và khai thác DLCN trong vận hành chính quyền số, đồng thời đặt ra yêu cầu hoàn thiện khuôn khổ pháp lý nhằm kiểm soát quyền lực dữ liệu của cơ quan nhà nước và bảo đảm trách nhiệm giải trình.

Kỷ yếu Hội thảo *“Pháp luật về bảo vệ DLCN trong kỷ nguyên số: Những vấn đề lý luận và thực tiễn ở Việt Nam hiện nay”*, Nxb Công an nhân dân, năm 2023 đã

tập hợp nhiều nghiên cứu tiếp cận trực tiếp bảo vệ DLCN trong bối cảnh số hóa. Các bài viết trong kỷ yếu đề cập đến nguyên tắc xử lý dữ liệu, mô hình thiết chế bảo vệ DLCN, cơ chế thực thi và xử lý vi phạm, qua đó cung cấp những gợi mở quan trọng cho việc xây dựng các giải pháp pháp lý và tổ chức nhằm bảo vệ quyền đối với DLCN trong hoạt động của cơ quan nhà nước [58].

Nhìn chung, các công trình trên đã tạo lập nền tảng lý luận quan trọng cho việc nghiên cứu bảo vệ quyền đối với DLCN, từ góc độ QCN, quyền nhân thân, cơ sở hiến định và yêu cầu quản trị công hiện đại. Tuy nhiên, các công trình này chủ yếu tiếp cận ở bình diện chung, tập trung vào cơ sở lý luận và khung pháp lý tổng quát, trong khi vấn đề bảo vệ quyền đối với DLCN trong quá trình xây dựng và vận hành chính quyền số, đặc biệt là cơ chế bảo đảm thực thi quyền trong hoạt động quản lý nhà nước ở cấp địa phương, vẫn chưa được phân tích một cách hệ thống và chuyên sâu.

Các bài viết trên tạp chí chuyên ngành đã góp phần cụ thể hóa cơ sở lý luận và đề xuất giải pháp hoàn thiện pháp luật bảo vệ quyền đối với DLCN trong bối cảnh chuyển đổi số. Trước hết, nghiên cứu của Vũ Anh Tiến, *“Pháp luật một số quốc gia về bảo vệ quyền thông tin cá nhân và khuyến nghị hoàn thiện pháp luật Việt Nam trong thời kỳ chuyển đổi số”*, Trường Đại học Luật Hà Nội cho thấy xu hướng tiếp cận so sánh pháp luật nhằm định vị các chuẩn mực bảo vệ thông tin cá nhân trong trật tự pháp lý hiện đại. Tác giả phân tích kinh nghiệm của một số mô hình tiêu biểu như GDPR ở châu Âu, pháp luật bảo vệ thông tin cá nhân tại một số bang của Hoa Kỳ và Nhật Bản, đồng thời đối chiếu với các quy định hiện hành của Việt Nam về bảo vệ thông tin cá nhân. Trên cơ sở nhận diện những hạn chế của hệ thống pháp luật Việt Nam, công trình đưa ra khuyến nghị nhằm hoàn thiện pháp luật Việt Nam về quyền bảo vệ thông tin cá nhân theo hướng tiệm cận các chuẩn mực quốc tế, đáp ứng yêu cầu quản trị nhà nước trong môi trường số; các tác giả Nguyễn Tấn Hoàng Hải, Trần Võ Kiều Anh, Hoàng Thị Khánh Hiền, Nguyễn Phạm Thanh Hoa (2021) với nghiên cứu *“Chủ thể dữ liệu, chủ thể kiểm soát dữ liệu và chủ thể xử lý dữ liệu trong pháp luật về bảo vệ DLCN”*, trong Tuyển tập “Bảo đảm chủ quyền quốc gia trên không gian mạng”, tập 1, tập trung làm rõ sự khác biệt giữa ba khái niệm trung tâm của pháp luật bảo vệ DLCN. Theo đó, chủ thể dữ liệu (Data Subject) được xác định là cá nhân mà DLCN gắn với họ và có quyền kiểm soát, yêu cầu xử lý đối với dữ liệu của mình; chủ thể kiểm soát dữ liệu (Data Controller) là tổ chức hoặc cá nhân quyết định mục đích và phương thức xử lý DLCN; còn chủ thể xử lý dữ liệu (Data Processor) là tổ

chức hoặc cá nhân thực hiện việc xử lý theo chỉ dẫn của chủ thể kiểm soát dữ liệu [31].

Bên cạnh các bài nghiên cứu chuyên đề, nhóm công trình có tính hệ thống như luận án tiến sĩ của Trần Thị Hồng Hạnh, *“Hoàn thiện pháp luật về bảo vệ thông tin cá nhân ở Việt Nam hiện nay”*, Học viện Chính trị quốc gia Hồ Chí Minh, năm 2018, cung cấp nền tảng lý luận và gợi mở giải pháp hoàn thiện thể chế theo hướng tổng thể. Luận án xây dựng hệ thống khái niệm và thuật ngữ liên quan đến thông tin cá nhân và hệ thống pháp luật về thông tin cá nhân; đồng thời xác lập các tiêu chí, yếu tố tác động đến quá trình hoàn thiện pháp luật bảo vệ thông tin cá nhân ở Việt Nam, đặt trong bối cảnh chuyển đổi số và hội nhập quốc tế. Trên cơ sở đánh giá thực trạng các quy định pháp luật hiện hành (như Bộ luật Dân sự, Luật An toàn thông tin mạng, Luật An ninh mạng và các văn bản hướng dẫn), luận án chỉ ra những vấn đề đặt ra đối với tính đầy đủ, đồng bộ và hiệu lực thực thi của hệ thống pháp luật. Đồng thời, thông qua so sánh với các mô hình pháp luật quốc tế và khu vực (đặc biệt là GDPR của Liên minh châu Âu, pháp luật Nhật Bản, Hàn Quốc và ASEAN), công trình rút ra bài học kinh nghiệm và đề xuất các giải pháp hoàn thiện, nhấn mạnh yêu cầu xây dựng đạo luật chuyên biệt về bảo vệ DLCN, hoàn thiện cơ chế giám sát - xử lý vi phạm và nâng cao nhận thức cộng đồng về quyền, nghĩa vụ liên quan đến DLCN [32]. Những đề xuất này có ý nghĩa như các luận cứ phục vụ hoạch định chính sách và hoàn thiện thể chế nhằm bảo đảm QCN trong điều kiện chuyển đổi phương thức quản trị nhà nước sang môi trường số.

Từ các công trình nêu trên có thể khái quát rằng, các nghiên cứu này đã đóng góp theo hai hướng chủ yếu: (i) Tiếp cận so sánh pháp luật để rút ra các chuẩn mực và mô hình tham chiếu, qua đó đề xuất hoàn thiện khung pháp lý bảo vệ thông tin cá nhân/DLCN trong bối cảnh chuyển đổi số; và (ii) Tiếp cận kỹ thuật pháp lý để làm rõ cấu trúc chủ thể, phân định trách nhiệm, từ đó đặt nền tảng cho cơ chế thực thi và trách nhiệm giải trình trong xử lý dữ liệu. Tuy nhiên, xét riêng trong khuôn khổ nghiên cứu bảo vệ quyền đối với DLCN trong xây dựng và vận hành chính quyền số, đặc biệt ở cấp địa phương, vẫn đặt ra yêu cầu tiếp tục nghiên cứu các cơ chế bảo vệ quyền trong quản trị công: từ việc nhận diện mô hình và nguyên tắc chung sang việc xây dựng cơ chế bảo đảm thực thi quyền đối với DLCN trong quy trình nghiệp vụ số của cơ quan nhà nước, bao gồm các yêu cầu về mục đích xử lý, căn cứ pháp lý, giới hạn quyền lực dữ liệu, trách nhiệm giải trình, giám sát và chế tài trong điều kiện chính quyền số đang được triển khai ngày càng sâu rộng.

1.2. TÌNH HÌNH NGHIÊN CỨU Ở NGOÀI NƯỚC LIÊN QUAN ĐẾN ĐỀ TÀI LUẬN ÁN

1.2.1. Các công trình nghiên cứu ở ngoài nước về Chính phủ điện tử, chính quyền số

Trong nghiên cứu quốc tế, Chính phủ điện tử và Chính phủ số/chính quyền số đã được tiếp cận dưới nhiều góc độ, từ lý thuyết quản trị công, mô hình tiến hóa, khung chính sách cho đến các nghiên cứu thực chứng và mô hình tích hợp. Các công trình này đã góp phần hình thành nền tảng học thuật quan trọng cho việc lý giải bản chất, đặc trưng và yêu cầu phát triển của Chính phủ số trong bối cảnh chuyển đổi số toàn cầu.

Ở phương diện lý thuyết và mô hình phát triển, các tác giả Patrick Dunleavy, Helen Margetts, Simon Bastow và Jane Tinkler (2006) với bài viết “*New Public Management Is Dead - Long Live Digital-Era Governance*” (Quản lý công mới đã kết thúc - Kỷ nguyên quản trị số lên ngôi), đăng trên *Journal of Public Administration Research and Theory*, tập 16, số 3, tháng 7/2006, đã đề xuất khung tiếp cận “Digital-Era Governance”, coi công nghệ số là động lực tái cấu trúc khu vực công thông qua tái tích hợp chức năng quản trị, xây dựng lại dịch vụ công theo nhu cầu và tăng cường vai trò của dữ liệu trong quản lý nhà nước [99].

Tiếp cận theo hướng tiến hóa của Chính phủ số, tác giả Tomasz Janowski (2015) trong bài “*Digital government evolution: From transformation to contextualization*” (Sự tiến hóa của Chính phủ số: từ chuyển đổi đến ngữ cảnh hóa), đăng trên *Government Information Quarterly*, tập 32, số 3 (2015), đã đề xuất mô hình tiến hóa bốn giai đoạn của Chính phủ điện tử, gồm: (i) Digitization - Số hóa, tập trung ứng dụng CNTT vào hoạt động nội bộ của Chính phủ; (ii) Transformation - Chuyển đổi, phát triển Chính phủ điện tử với dịch vụ công trực tuyến; (iii) Engagement - Tương tác, mở rộng sang quản trị điện tử (e-Governance), thúc đẩy sự tham gia của công dân; và (iv) Contextualization - Bối cảnh hóa, tức quản trị điện tử định hướng chính sách, thích ứng với đặc thù quốc gia và bối cảnh xã hội. Mô hình này nhấn mạnh tính phụ thuộc bối cảnh và có ý nghĩa quan trọng khi nghiên cứu chính quyền số ở cấp địa phương [108].

Ở góc độ khái niệm và chức năng, tác giả Ponkin (2021) trong công trình nghiên cứu “*Digital Government: Concept, Structure and Functions*” (Chính phủ số: khái niệm, cấu trúc và chức năng) đã định nghĩa Chính phủ số là một hệ thống hành chính công được số hóa, trong đó CNTT giữ vai trò trung tâm nhằm nâng cao hiệu

quả quản trị, chất lượng dịch vụ công và tính minh bạch trong hoạt động của cơ quan nhà nước [71].

Tiếp cận theo hướng chuyển đổi tổ chức và chiến lược, tác giả Alenezi (2022) với bài viết “*Digital Government Transformation: Organizational and Strategic Perspectives*” (Chuyển đổi Chính phủ số: góc nhìn tổ chức và chiến lược), đăng trên *Government Information Quarterly* (2022), đã chỉ ra rằng chuyển đổi Chính phủ điện tử sang Chính phủ số không chỉ là áp dụng công nghệ mới mà còn bao gồm sự thay đổi về văn hóa tổ chức, cấu trúc quản lý và chiến lược phát triển [87]. Theo tác giả Alenezi, các yếu tố quyết định thành công của chuyển đổi Chính phủ số gồm năng lực số của đội ngũ công chức, vai trò của lãnh đạo số và một chiến lược chuyển đổi rõ ràng, nhất quán [87]; tác giả Di Giulio và Vecchi (2023) trong bài viết “*A Digital Government Framework: Technology, Administration and Governance*” (Khung Chính phủ số: công nghệ, hành chính và quản trị), đăng trên *Public Management Review* (2023), đã đề xuất mô hình Chính phủ số dựa trên ba trụ cột: CNTT và truyền thông (ICT); cơ quan hành chính; và quản trị. Mô hình này nhấn mạnh yêu cầu tích hợp công nghệ vào cấu trúc tổ chức và chiến lược quản trị nhằm nâng cao hiệu quả cung cấp dịch vụ công và ra quyết định công [91].

Bên cạnh các nghiên cứu học thuật, các tổ chức quốc tế đã ban hành nhiều khung chính sách và báo cáo thực tế có ảnh hưởng lớn. Hội đồng OECD (2014) với “*Recommendation of the Council on Digital Government Strategies*” (“Khuyến nghị của Hội đồng OECD về chiến lược Chính phủ số”), thông qua ngày 15/7/2014 [97] và “*The OECD Digital Government Policy Framework*” (Khung chính sách Chính phủ số của OECD), năm 2020, đã xác lập các nguyên tắc nền tảng cho phát triển Chính phủ số như lấy người dùng làm trung tâm, quản trị dựa trên dữ liệu, phối hợp liên cơ quan và tăng cường trách nhiệm giải trình [98]. Ở cấp độ khu vực, Ủy ban châu Âu (2016) ban hành “*EU eGovernment Action Plan 2016 - 2020: Accelerating the digital transformation of government*” (Kế hoạch hành động Chính phủ điện tử EU giai đoạn 2016-2020: Thúc đẩy chuyển đổi số của chính phủ), nhấn mạnh nguyên tắc “*digital by default*” và liên thông hệ thống hành chính công [83].

Ngoài ra, các báo cáo so sánh quốc tế như “*UN E-Government Survey 2024*” (Khảo sát Chính phủ điện tử của Liên hợp quốc năm 2024) và “*GovTech Maturity Index, 2022 Update*” (Chỉ số mức độ trưởng thành GovTech - Cập nhật năm 2022) của Ngân hàng Thế giới đã cung cấp cơ sở thực chứng quan trọng để đánh giá mức

độ phát triển và trưởng thành của Chính phủ điện tử/Chính phủ số trên phạm vi toàn cầu [110].

Tổng hợp các công trình nghiên cứu ngoài nước cho thấy:

Thứ nhất, giới hạn mang tính hệ thống của lý thuyết “Kỷ nguyên quản trị số” (DEG) và Mô hình Tiến hóa (Janowski): Các mô hình của Dunleavy (2006) hay Janowski (2015) được đúc kết từ thực tiễn của các quốc gia phát triển (như Anh, EU) - nơi có hệ thống pháp luật về quyền riêng tư đã hoàn thiện hàng thập kỷ (tiền thân là Công ước châu Âu về quyền con người, sau đó là GDPR). Họ giả định rằng khi xã hội bước vào giai đoạn “Bối cảnh hóa” (Contextualization), thì nền tảng bảo hộ quyền con người của họ đã vững chắc. Tuy nhiên, Việt Nam là quốc gia đang phát triển, thực hiện “đi tắt đón đầu” về công nghệ. Hệ quả là Việt Nam tiến thẳng lên xây dựng Chính quyền số trong bối cảnh khung thể chế bảo vệ quyền dữ liệu (Luật số 91/2025/QH15) vừa mới được ban hành và đi vào thực thi. Sự chênh lệch giữa tốc độ số hóa bộ máy hành chính và năng lực bảo vệ quyền dữ liệu của chính quyền địa phương là một thách thức thực tiễn mang tính đặc thù của các quốc gia đang phát triển. Việc các khung lý thuyết quản trị số quốc tế chưa đi sâu giải quyết thỏa đáng mối quan hệ này chính là cơ sở để luận án tập trung nghiên cứu và bổ sung các luận cứ khoa học phù hợp với bối cảnh Việt Nam.

Thứ hai, điểm mù của Khung chính sách OECD và EU về “Quản trị dựa trên dữ liệu” (Data-driven Governance): Khung chính sách của OECD (2020) hay EU (2016) nhấn mạnh nguyên tắc “Số hoá theo mặc định” (Digital by default) và chia sẻ dữ liệu tối đa giữa các cơ quan. Họ xây dựng điều này dựa trên giả định về một hệ thống kiểm soát quyền lực công có tính độc lập cao (các Tòa án hành chính độc lập, các Ủy ban bảo vệ dữ liệu độc lập như ICO ở Anh hay CNIL ở Pháp). Tuy nhiên, việc áp dụng các khuyến nghị về quản trị dữ liệu từ các công trình quốc tế cần được xem xét trong mối quan hệ với đặc thù thể chế chính trị và mô hình tổ chức bộ máy nhà nước tại Việt Nam. Với mô hình phân công, phối hợp và kiểm soát quyền lực nhà nước có tính tập trung và thống nhất thì việc kết nối và chia sẻ dữ liệu qua Trục liên thông cấp tỉnh (LGSP) giữa HĐND, UBND và các sở, ngành chuyên môn tạo ra sự đồng bộ và tối ưu hóa hiệu lực quản lý nhà nước. Trong bối cảnh đó, nhằm bảo đảm sự cân bằng giữa mục tiêu liên thông dữ liệu và yêu cầu bảo vệ quyền con người, việc hoàn thiện một cơ chế kiểm soát quyền lực công đặc thù trên không gian số là một đòi hỏi khách quan. Điều này hoàn toàn phù hợp với nhiệm vụ và giải pháp của Nghị quyết số 66-NQ/TW, ngày 30/4/2025 về đổi mới công tác xây dựng và thi hành pháp

luật đáp ứng yêu cầu phát triển đất nước trong kỷ nguyên mới; trong đó nêu rõ: “... Thực hiện nghiêm kỷ cương, kỷ luật, các quy định về kiểm soát quyền lực, phòng, chống tham nhũng, lãng phí, tiêu cực, “lợi ích nhóm” trong xây dựng và thi hành pháp luật”.

Thứ ba, bản chất của “Sự đồng ý” (Consent) trong Dịch vụ công trực tuyến: Các nghiên cứu của Ponkin (2021) hay Alenezi (2022) tiếp cận dịch vụ công số dưới góc độ “nâng cao chất lượng dịch vụ” và “lấy người dùng làm trung tâm”. Cách tiếp cận này coi người dân gần như một “khách hàng” có quyền lựa chọn sử dụng hoặc từ chối dịch vụ. Tuy nhiên, dưới khía cạnh quyền con người, mối quan hệ giữa công dân và chính quyền số cấp tỉnh trong dịch vụ công trực tuyến là mối quan hệ bất đối xứng quyền lực. Người dân không thể chọn một nhà cung cấp dịch vụ hành chính khác nếu họ không đồng ý cung cấp dữ liệu sinh trắc học hay cư trú cho tỉnh. Trong quan hệ hành chính công, công dân luôn ở vị thế yếu thế hơn so với cơ quan quyền lực nhà nước. Khi người dân thực hiện các thủ tục hành chính thiết yếu (như đăng ký khai sinh, đất đai, cấp đổi giấy tờ), họ buộc phải sử dụng các cổng dịch vụ công hoặc ứng dụng số của chính quyền. Khi giao diện hệ thống hiển thị bảng điều khoản yêu cầu thu thập, xử lý dữ liệu kèm theo nút bấm “Tôi đồng ý”, người dân thực chất không có lựa chọn thứ hai (không thể bấm “Từ chối”, vì nếu từ chối thì hồ sơ hành chính sẽ không được tiếp nhận). Sự đồng ý trong trường hợp này không phải là sự tự nguyện thực chất, làm mất đi bản chất quyền tự quyết của công dân. Các nghiên cứu quốc tế chưa giải quyết được bài toán “Làm thế nào để bảo vệ quyền tự quyết dữ liệu khi công dân bắt buộc phải giao nộp dữ liệu để đổi lấy các quyền an sinh, hộ tịch tối thiểu?”

Thứ tư, sự thiếu vắng lý thuyết về “Xung đột lợi ích địa phương” trong chuyển đổi số: Tác giả Di Giulio và Vecchi (2023) chỉ tập trung vào 3 trụ cột (ICT - Hành chính - Quản trị) một cách cơ học để tối ưu hóa hiệu quả ra quyết định công. Tuy nhiên, nghiên cứu này bỏ qua một thực tế tại các quốc gia đang phát triển: Áp lực về chỉ số thành tích. Chính quyền cấp tỉnh ở Việt Nam chịu áp lực rất lớn về Chỉ số chuyển đổi số (DTI) và cải cách hành chính. Khi hiệu quả công nghệ được đặt lên làm ưu tiên hàng đầu để chạy đua thành tích, quyền dữ liệu cá nhân (vốn đòi hỏi quy trình mã hóa, phân quyền, đánh giá rủi ro DPIA phức tạp, làm chậm tốc độ xử lý hồ sơ) thường bị xem nhẹ hoặc bị coi là cản trở sự phát triển.

Thứ năm, thách thức mang tính đặc thù, “Bất bình đẳng số” (Digital Divide) gắn liền với “Bất bình đẳng quyền”: Mặc dù các báo cáo như UN E-Government

Survey 2024 có nhắc đến “phân biệt đối xử số”, nhưng các báo cáo này tiếp cận chủ yếu dưới góc độ kỹ thuật: thiếu thiết bị, thiếu mạng internet. Ở các tỉnh có nhiều đồng bào dân tộc thiểu số hoặc vùng sâu vùng xa, sự mù mờ về công nghệ dẫn đến việc họ không hề ý thức được mình có “Quyền đối với dữ liệu” và cũng không biết mình đang bị xâm phạm khi cán bộ thao tác sai quy trình. Sự bất bình đẳng về năng lực tiếp cận công nghệ tại địa phương trực tiếp chuyển hóa thành sự bất bình đẳng trong việc thụ hưởng quyền con người trên không gian số.

Tóm lại, mặc dù các công trình quốc tế trên đã đặt nền móng lý thuyết vững chắc về Chính phủ số, nhưng chúng tồn tại các giới hạn xuất phát từ bối cảnh thể chế - chính trị đặc thù của từng quốc gia. Đa số các nghiên cứu đều xuất phát từ bối cảnh các quốc gia phát triển, nơi hệ thống bảo hộ quyền riêng tư đã hoàn thiện từ trước. Khi đặt vào bối cảnh một quốc gia đang phát triển như Việt Nam - nơi việc xây dựng chính quyền số cấp tỉnh diễn ra song song và có phần nhanh hơn tốc độ hoàn thiện thể chế pháp lý, đồng thời vận hành trong mối quan hệ bất đối xứng quyền lực công - tư đặc thù; các lý thuyết phương Tây bộc lộ những “khoảng trống” lớn. Vì vậy, luận án này hướng tới việc thiết lập một khung lý luận và giải pháp thực thi mang tính địa phương, giải quyết bài toán tối ưu hóa chính quyền số cấp tỉnh trên nền tảng Luật số 91/2025/QH15, bảo đảm công nghệ phục vụ quyền con người chứ không xâm phạm quyền con người.

Tổng hợp các công trình nghiên cứu trong và ngoài nước cho thấy, CNTT và chuyển đổi số được xác định là yếu tố trung tâm trong phát triển Chính phủ điện tử và Chính phủ số/chính quyền số. Tuy nhiên, các nghiên cứu cũng khẳng định rằng hiệu quả của quá trình này phụ thuộc vào sự kết hợp đồng bộ giữa công nghệ, chiến lược phát triển, tổ chức bộ máy và nguồn nhân lực, cũng như mức độ tham gia của công dân trong quản trị công. Mặc dù vậy, tổng quan các công trình hiện có cho thấy vẫn tồn tại những khoảng trống nghiên cứu đáng kể. Cụ thể, còn thiếu các nghiên cứu chuyên sâu ở cấp tỉnh, thành phố, đặc biệt tại những địa phương có hạn chế về năng lực số. Bên cạnh đó, đa số các nghiên cứu chưa đi sâu phân tích khía cạnh pháp lý và QCN trong chính quyền số, nhất là quyền riêng tư và bảo vệ quyền đối với DLCN trong hoạt động của cơ quan nhà nước. Các nghiên cứu mang tính liên ngành (kết hợp quản lý công - luật học - công nghệ) còn hạn chế; thiếu các nghiên cứu định lượng, định tính có hệ thống về mức độ hài lòng và tương tác của người dân; đồng thời chưa đề cập đầy đủ đến các rủi ro và thách thức như lạm quyền trong thu thập dữ liệu, mất an toàn thông tin, phân biệt đối xử số và nguy cơ xâm phạm QCN trong môi trường

số. Đây chính là khoảng trống khoa học mà luận án hướng tới làm rõ trong bối cảnh xây dựng chính quyền số cấp tỉnh ở Việt Nam hiện nay.

1.2.2. Các công trình nghiên cứu nước ngoài về bảo vệ dữ liệu cá nhân và bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số

1.2.2.1. Các công trình nghiên cứu nước ngoài về bảo vệ dữ liệu cá nhân

Về góc độ quốc tế, nghiên cứu về bảo vệ DLCN (*personal data protection*) được hình thành và phát triển sớm, gắn liền với quá trình nhận thức và bảo đảm quyền riêng tư như một quyền cơ bản của con người trong xã hội hiện đại. Các công trình nghiên cứu nước ngoài có thể được tiếp cận theo những hướng chủ đạo, từ nền tảng lý luận về quyền riêng tư, đến xây dựng chuẩn mực pháp lý quốc tế, mô hình pháp luật khu vực và các nghiên cứu gắn với quản trị dữ liệu trong khu vực công và chính quyền số.

Ở hướng tiếp cận nền tảng, có thể kể đến sách chuyên khảo của tác giả Alan F. Westin (1967), *“Privacy and Freedom”* (Quyền riêng tư và tự do), Hoa Kỳ. Trong công trình này, tác giả tiếp cận quyền riêng tư như quyền của cá nhân trong việc kiểm soát thông tin về bản thân mình, qua đó đặt nền móng lý luận cho sự hình thành khái niệm quyền kiểm soát DLCN trong khoa học pháp lý hiện đại [70]. Tiếp nối cách tiếp cận đó, sách chuyên khảo của Daniel J. Solove (2008), *“Understanding Privacy”* (Hiểu về quyền riêng tư), Hoa Kỳ đã hệ thống hóa các dạng xâm phạm quyền riêng tư trong xã hội thông tin và đề xuất mô hình phân tích rủi ro (*privacy harms*), giúp chuyển trọng tâm từ khái niệm trừu tượng sang các tác động thực tiễn của việc thu thập, xử lý và khai thác DLCN [80]. Từ góc độ điều chỉnh pháp lý, những nghiên cứu của Paul M. Schwartz và Daniel J. Solove, tiêu biểu như *“Information Privacy Law”* (Pháp luật về quyền riêng tư thông tin), Hoa Kỳ, đã làm rõ sự chuyển dịch từ bảo vệ quyền riêng tư truyền thống sang bảo vệ DLCN trong nền kinh tế số [100]. Nhóm công trình này nhấn mạnh vai trò của pháp luật trong việc thiết lập các nguyên tắc xử lý dữ liệu, quyền của chủ thể dữ liệu và trách nhiệm giải trình của chủ thể xử lý dữ liệu, tạo nền tảng học thuật cho nhiều mô hình pháp luật hiện đại về bảo vệ dữ liệu.

Ở bình diện chuẩn mực quốc tế và khu vực, nhiều công trình nghiên cứu nước ngoài tập trung phân tích vai trò của các văn kiện pháp lý quốc tế trong việc định hình khung pháp lý bảo vệ DLCN. Tiêu biểu là các nghiên cứu bình luận và phân tích về *“Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data”* (Công ước về bảo vệ cá nhân đối với xử lý tự động DLCN - Convention 108), năm 1981, sửa đổi năm 2018 (Convention 108+), do Hội đồng châu

Âu ban hành. Trong số các công trình học thuật, có thể kể đến nghiên cứu của Lee A. Bygrave, “*Data Protection Law: Approaching Its Rationale, Logic and Limits*” (Pháp luật bảo vệ dữ liệu: Cơ sở lý luận, logic và giới hạn), sách chuyên khảo, 2002, Na Uy/Anh, trong đó tác giả coi Convention 108 là nền tảng pháp lý khu vực đầu tiên thiết lập các nguyên tắc phổ quát về xử lý DLCN, có ảnh hưởng vượt ra ngoài phạm vi châu Âu [90]. Các nghiên cứu này cho rằng Convention 108 không chỉ đặt nền móng cho pháp luật bảo vệ dữ liệu của các quốc gia thành viên Hội đồng châu Âu, mà còn trở thành khuôn mẫu tham chiếu cho nhiều quốc gia ngoài châu Âu trong quá trình xây dựng pháp luật bảo vệ DLCN.

Đặc biệt, mạch nghiên cứu đồ sộ tập trung vào “*General Data Protection Regulation - GDPR*” (Quy định bảo vệ dữ liệu chung của Liên minh châu Âu), Quy định (EU) số 2016/679, có hiệu lực từ năm 2018, được triển khai dưới dạng sách chuyên khảo, bình luận luật và các bài viết trên tạp chí pháp lý uy tín của châu Âu và quốc tế. Tiêu biểu có thể kể đến các tác giả Christopher Kuner, Lee A. Bygrave, Christopher Docksey (chủ biên) với công trình “*The EU General Data Protection Regulation (GDPR): A Commentary*” (Bình luận về Quy định bảo vệ dữ liệu chung của Liên minh châu Âu), năm 2020, phân tích một cách hệ thống các nguyên tắc xử lý dữ liệu, căn cứ hợp pháp cho việc xử lý, quyền của chủ thể dữ liệu, cơ chế bảo vệ dữ liệu ngay từ khâu thiết kế và theo mặc định (privacy/data protection by design and by default), nghĩa vụ đánh giá tác động bảo vệ dữ liệu, cũng như vai trò và thẩm quyền của cơ quan bảo vệ dữ liệu độc lập [78]. Bên cạnh đó, các tác giả Paul Voigt và Axel von dem Bussche, “*The EU General Data Protection Regulation (GDPR): A Practical Guide*” (Hướng dẫn thực tiễn về GDPR), sách tham khảo, 2017, Đức, tiếp cận GDPR như một mô hình quản trị dữ liệu dựa trên rủi ro và trách nhiệm giải trình. Nhiều nghiên cứu trong mạch này nhấn mạnh rằng GDPR không chỉ là văn bản bảo vệ quyền riêng tư, mà còn là khuôn khổ quản trị dữ liệu hiện đại, có ý nghĩa tham chiếu quan trọng đối với việc xây dựng chính sách bảo vệ dữ liệu trong khu vực công và quá trình phát triển chính quyền số [101].

Song song với mô hình châu Âu, các nghiên cứu so sánh pháp luật cũng tập trung phân tích các quốc gia ngoài Liên minh châu Âu. Ở Hoa Kỳ, nhiều công trình nghiên cứu của các tác giả Daniel J. Solove và Paul M. Schwartz, tiêu biểu như “*Information Privacy Law*” (Pháp luật về quyền riêng tư thông tin), sách tham khảo, 2022, Hoa Kỳ, đã làm rõ đặc trưng của mô hình điều chỉnh theo lĩnh vực (sectoral approach). Các nghiên cứu này đồng thời phân tích sự ra đời của “*California Consumer*

Privacy Act - CCPA” (Đạo luật về quyền riêng tư của người tiêu dùng bang California), năm 2018, như một bước chuyển quan trọng theo hướng tăng cường quyền của chủ thể dữ liệu trong bối cảnh Hoa Kỳ chưa có đạo luật liên bang thống nhất về bảo vệ DLCN [80]. Qua đó, các tác giả chỉ ra xu hướng tiệm cận dần với cách tiếp cận dựa trên quyền của chủ thể dữ liệu, dù vẫn duy trì đặc thù thể chế của Hoa Kỳ.

Ở châu Á, nhiều công trình nghiên cứu tập trung vào các mô hình pháp luật tương đối thống nhất và có mức độ tương thích quốc tế cao. Tiêu biểu là các nghiên cứu về “*Act on the Protection of Personal Information - APPI*” (Đạo luật về bảo vệ thông tin cá nhân của Nhật Bản), ban hành năm 2003, sửa đổi các năm 2015 và 2020, được phân tích trong các công trình so sánh pháp luật của tác giả Graham Greenleaf, “*Asian Data Privacy Laws*” (Pháp luật bảo vệ DLCN ở châu Á), sách chuyên khảo, 2014 và các bản cập nhật sau, Úc. Bên cạnh đó, các nghiên cứu về “*Personal Information Protection Act - PIPA*” (Đạo luật bảo vệ thông tin cá nhân), Hàn Quốc, thường nhấn mạnh vai trò của luật thống nhất, cơ quan quản lý chuyên trách và cơ chế bảo đảm luồng dữ liệu xuyên biên giới. Các công trình này cho thấy mô hình Nhật Bản và Hàn Quốc có nhiều điểm tương đồng với cách tiếp cận của Liên minh châu Âu, song được điều chỉnh phù hợp với điều kiện thể chế và văn hóa pháp lý khu vực châu Á [87].

Tổng hợp các công trình nêu trên cho thấy, nghiên cứu nước ngoài về bảo vệ DLCN đã hình thành hệ chuẩn mực tương đối hoàn chỉnh, không chỉ cung cấp nền tảng lý luận và pháp lý cho bảo vệ DLCN, mà còn gợi mở các mô hình quản trị dữ liệu và cơ chế trách nhiệm giải trình có giá trị tham chiếu quan trọng đối với việc xây dựng chính sách bảo vệ DLCN trong khu vực công và trong quá trình xây dựng chính quyền số.

Cùng với đó, nghiên cứu về Chính phủ số (Digital Government) đã được hình thành và phát triển từ sớm, gắn với quá trình ứng dụng CNTT và truyền thông trong quản trị nhà nước. Các công trình nghiên cứu tập trung làm rõ khái niệm Chính phủ số, mô hình vận hành và vai trò của Chính phủ số trong phát triển kinh tế - xã hội, đồng thời chỉ ra các nguy cơ tiềm ẩn và tác động của Chính phủ số đối với việc bảo vệ DLCN và QCN trong môi trường số.

Theo hướng tiếp cận nền tảng về quản trị số, tác giả Daniel Veit và Jan Huntgeburth trong công trình “*Incorporated Foundations of Digital Government: Leading and Managing in the Digital Era*” (Nền tảng tích hợp của Chính phủ số: Lãnh đạo và quản lý trong kỷ nguyên số), sách chuyên khảo, Springer Publishing Company, năm 2013, cho rằng Chính phủ số là việc sử dụng có mục đích CNTT và

truyền thông (ICT), đặc biệt là Internet, nhằm chuyển đổi mối quan hệ giữa Chính phủ và xã hội theo hướng tích cực [81]. Công trình phân tích bối cảnh, triển vọng và nền tảng của Chính phủ số thông qua các trường hợp thực tiễn trong quản lý hành chính, qua đó làm rõ vai trò của Internet, cơ hội của nền dân chủ số và những thách thức phát sinh khi chuyển dịch dịch vụ công sang môi trường trực tuyến.

Tiếp cận Chính phủ số từ góc độ chiến lược và hiệu quả khu vực công, các tác giả Svenja Falk, Andrea Römmele và Michael Silverman trong sách chuyên khảo *“Digital Government: Leveraging Innovation to Improve Public Sector Performance and Outcomes for Citizens”* (Chính phủ số: Tận dụng đổi mới để nâng cao hiệu quả khu vực công và kết quả cho công dân), Springer, 2016, đã phân tích việc triển khai các chiến lược số trong khu vực công tại nhiều quốc gia như Hoa Kỳ, Mexico, Brazil, Ấn Độ và Đức. Thông qua các nghiên cứu tình huống, công trình chỉ ra rằng nhiều quốc gia đã xây dựng chiến lược Chính phủ số tương đối đầy đủ nhưng còn hạn chế trong khâu triển khai và thực thi chính sách, từ đó gợi mở các mô hình và định hướng cải thiện hiệu quả Chính phủ số trong tương lai [107]. Trong khi đó, ở hướng tiếp cận hệ thống, tác giả Bernd W. Wirtz trong sách chuyên khảo *“Digital Government, Strategy, Government Models, and Technology”* (Chính phủ số, chiến lược, mô hình chính phủ và công nghệ), Springer International Publishing, năm 2022, nhấn mạnh số hóa, mạng lưới toàn cầu và sự chuyển đổi từ xã hội công nghiệp sang xã hội thông tin là những yếu tố cốt lõi làm gia tăng tầm quan trọng của Chính phủ số [73]. Công trình đánh giá tác động sâu rộng của Internet và truyền thông toàn cầu đối với hiệu suất dịch vụ công, đồng thời cung cấp khái niệm và các gợi ý chiến lược nhằm triển khai và duy trì hiệu quả các hệ thống Chính phủ số.

Song song với các nghiên cứu về Chính phủ số, nhiều công trình nước ngoài tiếp cận vấn đề bảo vệ DLCN và QCN trong bối cảnh số hóa. Yvonne McDermott trong bài viết *“Conceptualising the Right to Data Protection in an Era of Big Data”* (Khái niệm hóa quyền bảo vệ dữ liệu trong thời đại dữ liệu lớn), Big Data & Society, 2017, đã phân tích lịch sử hình thành quyền bảo vệ DLCN, các giá trị nền tảng của quyền này và những thách thức mới phát sinh trong kỷ nguyên dữ liệu lớn [111]; tác giả Maria Tzanou trong bài viết *“Data Protection as a Fundamental Right next to Privacy? “Reconstructing a Not So New Right”* (Bảo vệ dữ liệu như một quyền cơ bản bên cạnh quyền riêng tư? “Tái cấu trúc” một quyền không hoàn toàn mới), International Data Privacy Law, tập 3, số 2, năm 2013, thông qua phân tích các án lệ của Tòa án Công lý châu Âu (ECJ), đã lập luận rằng cần tái cấu trúc cách tiếp cận để bảo đảm

quyền bảo vệ DLCN được thừa nhận như một quyền độc lập, cơ bản trong trật tự pháp lý hiện đại [92]; tác giả Florent Thouvenin trong bài viết *“Information Self-Determination: A Convincing Rationale for Data Protection Law?”* (Quyền tự quyết thông tin: Cơ sở thuyết phục cho pháp luật bảo vệ dữ liệu?), JIPITEC, năm 2021, nhấn mạnh rằng pháp luật bảo vệ dữ liệu cần được xây dựng trên nền tảng quyền kiểm soát và tự chủ thông tin của chủ thể dữ liệu, đặc biệt trong bối cảnh gia tăng các hành vi xử lý dữ liệu khi chưa có sự đồng ý [85]; tác giả Cécile de Terwangne trong bài viết *“The Right to Be Forgotten and the Informational Autonomy in the Digital Environment”* (Quyền được lãng quên và quyền tự chủ thông tin trong môi trường số), EUR - Scientific and Technical Research Series, đã phân tích cơ sở lý luận của quyền được lãng quên, giới hạn thời gian lưu trữ dữ liệu và mối quan hệ giữa quyền này với quyền đồng ý của chủ thể dữ liệu [77]... Nhìn chung, các công trình nghiên cứu nước ngoài đã hình thành hệ tri thức tương đối toàn diện về Chính phủ số và bảo vệ DLCN, từ nền tảng lý luận, mô hình quản trị đến các quyền cụ thể của chủ thể dữ liệu. Tuy nhiên, việc chuyển hóa các kết quả nghiên cứu này vào bối cảnh xây dựng và vận hành chính quyền số ở từng quốc gia, đặc biệt ở cấp địa phương, vẫn đặt ra yêu cầu nghiên cứu tiếp tục nhằm bảo đảm sự phù hợp và hiệu quả trong bảo vệ quyền đối với DLCN.

1.2.2.2. Các công trình nghiên cứu về bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số

Trong nghiên cứu quốc tế, cùng với sự phát triển của Chính phủ số/chính quyền số, vấn đề bảo vệ quyền đối với DLCN ngày càng được đặt ra như một yêu cầu cốt lõi của quản trị nhà nước hiện đại và bảo đảm QCN trong môi trường số. Các công trình nghiên cứu thuộc hướng này không chỉ tiếp cận từ góc độ kỹ thuật số hóa khu vực công, mà còn mở rộng sang quản trị dữ liệu, trách nhiệm giải trình của Nhà nước, bảo vệ QCN trên không gian mạng và kiểm soát rủi ro phát sinh từ công nghệ mới.

Trước hết, các công trình nghiên cứu về Chính phủ số đã chỉ ra rằng số hóa hoạt động quản lý nhà nước tất yếu dẫn đến việc thu thập, xử lý và liên thông khối lượng lớn DLCN của công dân, từ đó làm gia tăng yêu cầu bảo vệ quyền đối với DLCN. Các nghiên cứu như *“Incorporated Foundations of Digital Government: Leading and Managing in the Digital Era”* (Nền tảng tích hợp của Chính phủ số: Lãnh đạo và quản lý trong kỷ nguyên số), của tác giả Daniel Veit và Jan Huntgeburth, 2013; nghiên cứu *“Digital Government: Leveraging Innovation to Improve Public Sector Performance and Outcomes for Citizens”* (Chính phủ số: Tận dụng đổi mới để nâng cao hiệu quả khu vực công và kết quả cho công dân), của các tác giả Svenja

Falk, Andrea Römmele và Michael Silverman, năm 2016; và “*Digital Government, Strategy, Government Models, and Technology*” (Chính phủ số, chiến lược, mô hình chính phủ và công nghệ), của tác giả Bernd W. Wirtz, năm 2022, dù tập trung vào chiến lược và hiệu quả quản trị, đều thống nhất ở nhận định rằng dữ liệu trở thành “hạ tầng mềm” của Chính phủ số. Từ đó, các tác giả đều gợi mở nhu cầu xây dựng khuôn khổ pháp lý và cơ chế quản trị dữ liệu nhằm bảo đảm tính hợp pháp, minh bạch và tin cậy của hệ thống chính quyền số.

Gắn trực tiếp với khía cạnh QCN trong không gian mạng, các tác giả Iwona Florek và Susran Erkan Eroglu (Đại học Alcide De Gasperi University of Euroregional Economy in Józefów) trong bài viết “*The Need for Protection of Human Rights in Cyberspace*” (Sự cần thiết phải bảo vệ QCN trong không gian mạng), đăng trên Journal of Modern Science, số 3/42, năm 2019, đã phân tích mối quan hệ giữa không gian mạng và bảo vệ QCN dưới góc độ xã hội và pháp lý. Thông qua việc chỉ ra các nguy cơ và mối đe dọa phát sinh khi con người sử dụng mạng máy tính, các tác giả cho rằng các khung pháp lý hiện hành, kể cả pháp luật quốc tế về bảo vệ dữ liệu, vẫn chưa đủ để bảo đảm an toàn cho DLCN [89]. Công trình nhấn mạnh rằng, để bảo vệ QCN nói chung và quyền đối với DLCN nói riêng trong không gian mạng, cần kết hợp giữa biện pháp pháp lý, biện pháp kỹ thuật và giáo dục nâng cao nhận thức của người dùng - một luận điểm có ý nghĩa trực tiếp đối với việc xây dựng chính quyền số lấy con người làm trung tâm.

Ở hướng tiếp cận quyền đối với DLCN trong môi trường công nghệ cao, tác giả Yvonne McDermott trong bài viết “*Conceptualising the Right to Data Protection in an Era of Big Data*” (Khái niệm hóa quyền bảo vệ dữ liệu trong thời đại dữ liệu lớn), Big Data & Society, 2017, đã nhấn mạnh nền tảng giá trị và các thách thức mới của quyền bảo vệ dữ liệu trong bối cảnh dữ liệu lớn. Công trình chỉ ra rằng sự mở rộng quy mô và mục đích xử lý dữ liệu trong các hệ thống số, đặc biệt là hệ thống do Nhà nước quản lý, đặt ra nguy cơ xói mòn quyền kiểm soát dữ liệu của cá nhân nếu thiếu cơ chế bảo đảm quyền hiệu quả [111]. Trong khi đó, theo hướng tiếp cận quyền cơ bản độc lập, Maria Tzanou trong bài viết “*Data Protection as a Fundamental Right next to Privacy? ‘Reconstructing’ a Not So New Right*” (Bảo vệ dữ liệu như một quyền cơ bản bên cạnh quyền riêng tư? “Tái cấu trúc” một quyền không hoàn toàn mới), International Data Privacy Law, tập 3, số 2, năm 2013, thông qua phân tích các án lệ của Tòa án Công lý châu Âu (ECJ), đã lập luận rằng quyền bảo vệ DLCN cần được tái cấu trúc và thừa nhận như một quyền cơ bản độc lập [92]. Lập luận này có ý

nghĩa đặc biệt trong bối cảnh chính quyền số, khi Nhà nước giữ vai trò trung tâm trong việc quyết định mục đích và phương thức xử lý dữ liệu công dân; còn ở góc độ quyền tự quyết thông tin, tác giả Florent Thouvenin trong bài viết *“Information Self-Determination: A Convincing Rationale for Data Protection Law?”* (Quyền tự quyết thông tin: Cơ sở thuyết phục cho pháp luật bảo vệ dữ liệu?), JIPITEC, năm 2021, nhấn mạnh rằng pháp luật bảo vệ DLCN cần được xây dựng trên nền tảng quyền kiểm soát và tự chủ thông tin của chủ thể dữ liệu. Tác giả cho rằng trong môi trường số, sự “đồng ý” của chủ thể dữ liệu không thể chỉ mang tính hình thức, mà phải gắn với khả năng thực chất làm chủ và kiểm soát thông tin của mình - một yêu cầu then chốt khi xây dựng các hệ thống chính quyền số [85].

Liên quan trực tiếp đến môi trường Internet và công nghệ khai thác dữ liệu, Lilian Edwards (University of Newcastle) trong sách tham khảo *“Law, Policy and the Internet”* (Pháp luật, chính sách và Internet), năm 2018, với chương *“Data Protection and e-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling”* (Bảo vệ dữ liệu và quyền riêng tư điện tử: Từ thư rác, cookie đến dữ liệu lớn, học máy và hồ sơ hóa), đã phân tích các hình thức thu thập và khai thác dữ liệu người dùng ngày càng tinh vi. Tác giả chỉ ra rằng DLCN không chỉ được thu thập qua máy tính kết nối Internet, mà thông qua mọi thiết bị có khả năng kết nối mạng, từ đó đặt ra yêu cầu phải hiểu lại nội hàm của sự đồng ý và quyền kiểm soát dữ liệu trong kỷ nguyên số [88].

Ở bình diện lập pháp hiện đại, nhà nghiên cứu Puneet Bhasin trong sách *“Practical Guide to Digital Personal Data Protection Act, 2023: Law and Compliance”* (Hướng dẫn thực tiễn về Đạo luật bảo vệ DLCN kỹ thuật số năm 2023: Pháp luật và tuân thủ), OakBridge, 2024, đã phân tích chi tiết Đạo luật bảo vệ DLCN kỹ thuật số của Ấn Độ - quốc gia có tốc độ chuyển đổi số nhanh và quy mô dữ liệu lớn. Công trình làm rõ phạm vi điều chỉnh, ngoại lệ, cơ chế thực thi, nghĩa vụ tuân thủ và chế tài, qua đó cung cấp kinh nghiệm tham khảo quan trọng cho các quốc gia đang xây dựng khuôn khổ pháp lý bảo vệ DLCN trong chính quyền số [102]; sách chuyên khảo *“Data Protection, Privacy and Artificial Intelligence”* (Bảo vệ dữ liệu, quyền riêng tư và trí tuệ nhân tạo), của nhóm tác giả Eleni Kosta, Dara Hallinan, Paul De Hert và Suzanne Nusselder (chủ biên), Bloomsbury Publishing, năm 2025, đã tập hợp các nghiên cứu từ Hội nghị CPDP 2024, phân tích mối quan hệ giữa bảo vệ dữ liệu, AI và QCN. Công trình đặc biệt nhấn mạnh các rủi ro đối với quyền cơ bản khi AI được sử dụng trong khu vực công và thực thi pháp luật, đồng thời chỉ ra những

khoảng trống trong các cơ chế quản trị hiện hành - một vấn đề có ý nghĩa trực tiếp đối với việc xây dựng chính quyền số an toàn và tôn trọng quyền đối với DLCN [82].

1.3. NHỮNG VẤN ĐỀ LUẬN ÁN TIẾP TỤC NGHIÊN CỨU

1.3.1. Đánh giá chung các công trình nghiên cứu trước và khoảng trống học thuật

Các công trình nghiên cứu trong và ngoài nước liên quan đến bảo vệ dữ liệu cá nhân và chính quyền số có thể được phân thành ba hướng tiếp cận chủ yếu.

Qua tổng hợp và phân tích hệ thống các công trình nghiên cứu trong và ngoài nước có liên quan đến bảo vệ DLCN và chính quyền số, có thể định vị các hướng tiếp cận hiện nay thành ba nhóm chủ yếu sau: (1) Nhóm tiếp cận từ quyền con người và quyền riêng tư; (2) Nhóm tiếp cận từ luật học so sánh và quản trị dữ liệu khu vực tư; (3) Nhóm tiếp cận từ khoa học hành chính số và chính phủ điện tử.

Mặc dù các công trình đi trước đã đặt nền móng quan trọng, song dưới lăng kính phản biện khoa học, các nghiên cứu này vẫn bộc lộ những giới hạn lý luận và để lại các khoảng trống học thuật cốt lõi sau đây: *Thứ nhất*, thiếu hụt nền tảng khung lý luận chuyên sâu về cơ chế bảo đảm thực thi quyền trong khu vực công. Phần lớn các công trình nghiên cứu hiện nay thường dừng lại ở tiếp cận chuẩn mực hình thức; nghĩa là tập trung mô tả, giải thích các quy định pháp luật hoặc kiến nghị xây dựng khung chính sách số mang tính lý thuyết, thiếu tính gắn kết với thực tiễn vận hành công vụ. Về mặt lý luận, các nghiên cứu trước đây còn tồn tại một khoảng cách lớn giữa quyền năng trên văn bản và cơ chế vận hành thực tế. Các nghiên cứu này chưa lý giải được một cách hệ thống cách thức chuyển hóa các nghĩa vụ bảo vệ quyền của Nhà nước thành các quy trình bắt buộc mang tính công vụ trong khu vực công. Hạn chế lý luận này khiến quyền đối với DLCN khi đi vào môi trường chính quyền số dễ bị lu mờ trước mục tiêu tối đa hóa hiệu năng quản lý, hành chính.

Thứ hai, khoảng trống về một “Khung mô hình lý luận và cơ chế bảo đảm” đặc thù cho cấp chính quyền địa phương: Các công trình đã công bố chủ yếu xem xét mô hình bảo vệ dữ liệu ở cấp vĩ mô (quốc gia) hoặc đặt trong bối cảnh thương mại hóa dữ liệu của khu vực tư, nơi mà sự đồng ý (consent) của chủ thể là tuyệt đối. Tuy nhiên, tại chính quyền địa phương cấp tỉnh - nơi trực tiếp diễn ra hoạt động tích tụ, liên thông dọc - ngang và khai thác một khối lượng lớn dữ liệu nhạy cảm của công dân qua dịch vụ công trực tuyến, cơ chế xử lý dữ liệu chủ yếu dựa trên căn cứ thực thi quyền lực công và nhiệm vụ pháp định (không cần sự đồng ý). Hiện nay, hoàn toàn thiếu vắng một nghiên cứu lý luận chuyên sâu thiết lập hệ thống các nguyên tắc

kiểm soát can thiệp (tính tương xứng, tính cần thiết, trách nhiệm giải trình) để định hình một cơ chế bảo đảm lập quy và thực thi đặc thù cho mô hình chính quyền số cấp tỉnh.

Thứ ba, sự chia cắt giữa các phương thức bảo vệ pháp lý, tổ chức và kỹ thuật: Các nghiên cứu hiện tại có sự phân mảnh rõ nét về mặt phương pháp luận; các công trình luật học chuyên sâu thường bỏ qua yếu tố kiến trúc hạ tầng số; ngược lại, các nghiên cứu công nghệ lại thuần túy xử lý bài toán an ninh mạng mà thiếu đi chiều sâu bảo vệ quyền con người. Chưa có công trình nào tích hợp được các phương thức này thành một chỉnh thể biện chứng, từ hoàn thiện quy phạm, thiết lập định chế tuân thủ nội bộ DPO, đến công nghệ lưu vết tự động và nâng cao nhận thức và kỹ năng bảo vệ dữ liệu của người dân.

Hướng giải quyết và đóng góp mới của Luận án: Chính những khoảng trống lý luận về “cơ chế bảo đảm thực thi quyền” nêu trên là dư địa và mục tiêu trọng tâm mà Luận án tập trung giải quyết. Bằng việc làm rõ bản chất mối quan hệ giữa Chủ thể mang quyền và Bên có nghĩa vụ trong môi trường số, Luận án hướng tới việc:

Về mặt lý luận (Chương 2): Xây dựng một Khung mô hình lý luận toàn diện về cơ chế bảo đảm quyền đối với DLCN tại chính quyền số cấp tỉnh thông qua hệ thống các nguyên tắc kiểm soát quyền lực dữ liệu và 06 phương thức bảo vệ đồng bộ (pháp lý, tổ chức bộ máy, kỹ thuật công nghệ, thanh tra tài phán, bảo hộ quyền hiến định, truyền thông nhận thức và hợp tác kiểm soát luồng dữ liệu).

Về mặt thực tiễn (Chương 3 và Chương 4): Sử dụng chính Khung mô hình lý luận này làm hệ tiêu chí soi chiếu để đánh giá, kiểm định toàn diện thực trạng lập quy, thực thi tại địa phương, từ đó đề xuất mô hình giải pháp đồng bộ có tính khả thi cao tại Việt Nam hiện nay.

1.3.2. Những nội dung luận án tiếp tục nghiên cứu

Trên cơ sở kế thừa các kết quả nghiên cứu đi trước và giải quyết triệt để các khoảng trống lý luận về “cơ chế bảo đảm thực thi quyền” đối với DLCN trong khu vực công, Luận án tập trung nghiên cứu sâu và làm sáng tỏ các nội dung trọng tâm sau đây:

Một là, xây dựng Khung mô hình lý luận toàn diện về cơ chế bảo đảm quyền đối với DLCN tại chính quyền số cấp tỉnh: Luận án đi sâu nghiên cứu bản chất triết học pháp lý và xã hội học của quyền dữ liệu dưới góc độ quyền con người. Trọng tâm là phân tích mối quan hệ biện chứng giữa Chủ thể mang quyền (công dân) và Bên có nghĩa vụ (cơ quan hành chính công địa phương). Từ đó, vận dụng các nguyên tắc giới

hạn quyền của luật quốc tế (tính hợp pháp, tính cần thiết, tính tương xứng, trách nhiệm giải trình) để định hình một cơ chế kiểm soát can thiệp và thiết lập hệ thống 06 phương thức bảo vệ đồng bộ (bao gồm: pháp lý, cấu trúc tổ chức, kỹ thuật - công nghệ, thanh tra tài phán, bảo hộ quyền hiến định, truyền thông nhận thức và kiểm soát luồng dữ liệu) đặc thù cho không gian quản trị của chính quyền cấp tỉnh.

Hai là, phân tích đối chiếu kinh nghiệm lập pháp và mô hình thực thi quốc tế: Nghiên cứu cách thức giải quyết bài toán cân bằng giữa bảo vệ quyền công dân và khai thác tài nguyên dữ liệu trong xây dựng Chính phủ số, chính quyền số tại một số quốc gia điển hình (Đức, Trung Quốc, Nga) và đặc biệt là các quốc gia có sự tương đồng thể chế trong khu vực Đông Nam Á (Singapore, Thái Lan). Nội dung này tập trung rút ra các kinh nghiệm hợp lý về mặt mô hình quản trị tuân thủ nội bộ (DPO), cơ chế kiểm soát pháp lý trong chia sẻ thông tin công - tư (PPP) và cơ chế phản ứng nhanh trước rủi ro an ninh xuyên biên giới để làm bài học tham chiếu cho Việt Nam.

Ba là, kiểm định thực trạng lập quy và thực thi bảo vệ quyền đối với DLCN tại chính quyền số cấp tỉnh ở Việt Nam: Sử dụng Khung mô hình lý luận đã xây dựng ở Chương 2 làm hệ tiêu chí soi chiếu để phân tích, đánh giá toàn diện hệ thống văn bản quy phạm pháp luật hiện hành của trung ương và các văn bản chỉ đạo, điều hành của địa phương. Đồng thời, Luận án đi sâu phân tích thực tiễn hành chính số tại cấp tỉnh hiện nay: từ kiến trúc kỹ thuật của Cổng dịch vụ công trực tuyến, quy trình công vụ xử lý dữ liệu của công chức, ranh giới bảo mật khi thuê ngoài dịch vụ công nghệ (khối tư), đến thực trạng nhận thức xã hội và cơ chế tiếp nhận, giải quyết khiếu nại của người dân khi xảy ra sự cố lộ lọt thông tin. Từ đó, chỉ rõ các điểm nghẽn, xung đột pháp lý và nguyên nhân của những hạn chế này.

Bốn là, đề xuất hệ thống giải pháp đồng bộ và mô hình bảo đảm thực thi quyền khả thi tại Việt Nam: Xác lập quan điểm định hướng đối với cơ chế bảo đảm quyền dữ liệu gắn với tiến trình cải cách hành chính và xây dựng chính quyền số. Trên cơ sở đó, thiết lập hệ thống giải pháp lập pháp và thực thi đồng bộ bao quát cả 06 phương thức bảo vệ đã xác lập ở phần lý luận: từ kiến nghị hoàn thiện cấu trúc Luật Bảo vệ dữ liệu cá nhân; chuẩn hóa quy trình thao tác công vụ (SOP) và định chế nhân sự chuyên trách bảo vệ dữ liệu (DPO) tại địa phương; áp dụng các giải pháp công nghệ mã hóa, ẩn danh hóa và tự động lưu vết (Log); đến đổi mới phương thức truyền thông nâng cao năng lực an toàn hành vi của xã hội và kiểm soát luồng dữ liệu trong các dự án đô thị thông minh.

1.4. GIẢ THUYẾT VÀ CÂU HỎI NGHIÊN CỨU

1.4.1. Giả thuyết nghiên cứu

Trong tiến trình xây dựng chính quyền số cấp tỉnh ở Việt Nam, mâu thuẫn lớn nhất đang diễn ra giữa yêu cầu thu thập, kết nối, chia sẻ dữ liệu quy mô lớn phục vụ tối ưu hóa quản lý hành chính và nghĩa vụ tôn trọng, bảo vệ quyền đối với dữ liệu cá nhân của công dân.

Giả thuyết nghiên cứu của Luận án cho rằng: Hiệu quả bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh hiện nay bị hạn chế không phải do rào cản kỹ thuật - công nghệ thuần túy, mà xuất phát từ khoảng trống thể chế và tư duy quản hành chính; cụ thể là sự thiếu hụt cơ chế kiểm soát quyền lực công trong xử lý dữ liệu và sự thụ động của công dân trong việc tự vệ số.

Do đó, hiệu quả bảo vệ quyền đối với DLCN tại chính quyền số cấp tỉnh chỉ có thể đạt được một cách thực chất và bền vững khi thực hiện sự chuyển dịch từ tư duy quản lý hành chính sang tiếp cận dựa trên quyền con người, thông qua 03 trụ cột pháp lý cốt lõi: Đối với cơ quan nhà nước (Chủ thể mang nghĩa vụ); chuyển hóa các chuẩn mực của Nghị định số 13/2023/NĐ-CP và Luật Bảo vệ DLCN năm 2025 thành Quy chế trách nhiệm giải trình công vụ, xác lập giới hạn ủy quyền pháp lý trong hợp tác công - tư và kiểm soát quyền lực công trong xử lý dữ liệu (đặc biệt là dữ liệu từ hệ thống IOC, AI). Đối với công dân (Chủ thể mang quyền); chuyển từ trạng thái được bảo vệ thụ động sang xây dựng năng lực tự vệ pháp lý chủ động, được bảo đảm bằng các công cụ tương tác quyền tự quyết số trên Cổng dịch vụ công. Đối với Cơ chế bảo đảm; chuyển từ xử lý vi phạm sau sự cố sang quản trị rủi ro pháp lý định kỳ, kết hợp cơ chế kiểm toán độc lập và trách nhiệm bồi thường thiệt hại trực tiếp cho chủ thể dữ liệu.

1.4.2. Câu hỏi nghiên cứu

1. Cơ sở lý luận và tiêu chuẩn pháp lý quốc tế về bảo vệ quyền đối với dữ liệu cá nhân dưới tiếp cận quyền con người trong xây dựng chính quyền số cấp tỉnh là gì? Bao gồm những nội dung và phương thức nào? Pháp luật Việt Nam hiện hành (trọng tâm là Nghị định số 13/2023/NĐ-CP và Luật Bảo vệ dữ liệu cá nhân năm 2025) đã thể chế hóa nghĩa vụ của chính quyền địa phương và các bên liên quan như thế nào?

2. Thực trạng thực thi bảo vệ quyền dữ liệu cá nhân tại chính quyền số cấp tỉnh ở Việt Nam hiện nay đã đạt được kết quả gì, đang đối mặt với những bất cập, xung đột pháp lý cốt lõi nào? Đây là nguyên nhân thể chế, tổ chức thực thi và nhận thức dẫn đến tình trạng này?

3. Cơ chế kiểm soát quyền lực công, trách nhiệm giải trình công vụ và cơ chế tự vệ pháp lý của công dân trong hoạt động thu thập, lưu trữ, chia sẻ dữ liệu của chính quyền số cấp tỉnh có những hạn chế gì so với yêu cầu bảo vệ quyền con người?

4. Cần có những giải pháp đột phá nào về hoàn thiện thể chế, nâng cao năng lực trách nhiệm công vụ, thiết lập cơ chế kiểm soát hợp tác công - tư và lộ trình triển khai cụ thể để bảo đảm sự cân bằng hài hòa giữa yêu cầu phát triển chính quyền số cấp tỉnh với nghĩa vụ bảo vệ quyền đối với dữ liệu cá nhân ở Việt Nam đến năm 2030 và những năm tiếp theo?

Chương 2

CƠ SỞ LÝ LUẬN VỀ BẢO VỆ QUYỀN ĐỐI VỚI DỮ LIỆU CÁ NHÂN TRONG XÂY DỰNG CHÍNH QUYỀN SỐ CẤP TỈNH

2.1. KHÁI NIỆM, ĐẶC ĐIỂM, VAI TRÒ CỦA BẢO VỆ QUYỀN ĐỐI VỚI DỮ LIỆU CÁ NHÂN TRONG XÂY DỰNG CHÍNH QUYỀN SỐ CẤP TỈNH

2.1.1. Khái niệm bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh

2.1.1.1. Khái niệm dữ liệu cá nhân

Các văn bản pháp lý có tính quốc tế đã đưa ra những khái niệm về DLCN như sau: Hiệp ước 108 của châu Âu nêu: *“Dữ liệu cá nhân” có nghĩa là bất kỳ thông tin liên quan đến một cá nhân được xác định hoặc mang tính chất cá nhân*”. Chỉ thị 95/46/EC (Directive 95/46/EC of the European Parliament and of the Council) của châu Âu nêu: *“Dữ liệu cá nhân có nghĩa là bất kỳ thông tin liên quan đến một người được xác định hoặc có thể xác định; một người có thể được xác định, trực tiếp hoặc gián tiếp, đặc biệt bằng cách tham chiếu đến một số nhận dạng, cho một hoặc nhiều yếu tố đặc trưng cho bản sắc của họ về thể chất, sinh lý, tâm thần, kinh tế, văn hóa, xã hội”* [84]. Hướng dẫn bảo vệ bí mật cá nhân và chuyển giao dữ liệu cá nhân (Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data) của Tổ chức Hợp tác và Phát triển Kinh tế (OECD) ban hành nêu: *“Dữ liệu cá nhân” có nghĩa là bất kỳ thông tin liên quan đến một cá nhân được xác định hoặc có thể nhận dạng*. Khuôn khổ chung về bảo vệ DLCN trong thương mại điện tử APEC đưa ra quan niệm: *“Thông tin cá nhân là bất kỳ thông tin nào để xác định được hay có thể xác định được một cá nhân cụ thể”* [96].

Dưới góc độ pháp lý, DLCN được hiểu là những thông tin “đi cùng” một con người cụ thể hoặc có thể giúp xác định người đó. Quan điểm hẹp (gắn với định danh/identity-based) thường coi DLCN chủ yếu là thông tin “gắn với việc xác định danh tính” của một người (cách tiếp cận dễ áp dụng trong quản lý, nhấn mạnh các định danh trực tiếp). Cách hiểu này thể hiện rõ trong định nghĩa “thông tin cá nhân” của Luật An toàn thông tin mạng 2015: “thông tin cá nhân là thông tin gắn với việc xác định danh tính của một người cụ thể”. Trong khi đó, quan điểm rộng (liên quan đến người có thể xác định/relating & identifiable), tiêu biểu là GDPR của EU, xem

DLCN là “*bất kỳ thông tin nào liên quan tới một người đã được xác định hoặc có thể xác định*”, kể cả định danh gián tiếp như dữ liệu vị trí, online identifier... Tương ứng ở Việt Nam, Luật Bảo vệ dữ liệu cá nhân năm 2025 ghi nhận rõ: dữ liệu sau khi khử nhận dạng thì “không còn là dữ liệu cá nhân” - tạo cơ sở pháp lý cho các kỹ thuật giảm rủi ro như de-identification/pseudonymization trong thực tiễn. Theo khoản 1, Điều 2, Luật số 91/2025/QH15, ngày 26/6/2025 thì khái niệm về DLCN được nêu như sau: “*Dữ liệu cá nhân là dữ liệu số hoặc thông tin dưới dạng khác xác định hoặc giúp xác định một con người cụ thể, bao gồm: DLCN cơ bản và DLCN nhạy cảm. Dữ liệu cá nhân sau khi khử nhận dạng không còn là DLCN*” [50].

Theo quy định đó, có thể hiểu:

Dữ liệu cá nhân cơ bản là DLCN phản ánh các yếu tố nhân thân, lai lịch phổ biến, thường xuyên sử dụng trong các giao dịch, quan hệ xã hội, thuộc danh mục do Chính phủ ban hành. Dữ liệu cá nhân cơ bản bao gồm: họ, chữ đệm và tên khai sinh, tên gọi khác (nếu có); ngày, tháng, năm sinh; ngày, tháng, năm chết hoặc mất tích; giới tính; nơi sinh, nơi đăng ký khai sinh, nơi thường trú, nơi tạm trú, nơi ở hiện tại, quê quán, địa chỉ liên hệ; quốc tịch; hình ảnh của cá nhân; số điện thoại, số chứng minh nhân dân, số định danh cá nhân, số hộ chiếu, số giấy phép lái xe, số biển số xe, số mã số thuế cá nhân, số bảo hiểm xã hội, số thẻ bảo hiểm y tế; tình trạng hôn nhân; thông tin về mối quan hệ gia đình (cha mẹ, con cái); thông tin về tài khoản số của cá nhân; DLCN phản ánh hoạt động, lịch sử hoạt động trên không gian mạng; các thông tin khác gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể không thuộc quy định tại khoản 4 Điều này.

Dữ liệu cá nhân nhạy cảm, theo GDPR và khoản 2 Điều 2 Luật Bảo vệ DLCN thì “*DLCN nhạy cảm là DLCN gắn liền với quyền riêng tư của cá nhân, khi bị xâm phạm sẽ gây ảnh hưởng trực tiếp đến quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân, thuộc danh mục do Chính phủ ban hành*”, bao gồm dữ liệu tiết lộ nguồn gốc chủng tộc hoặc dân tộc; quan điểm chính trị, niềm tin tôn giáo hoặc triết học; thành viên công đoàn; dữ liệu di truyền, dữ liệu sinh trắc học; dữ liệu về sức khỏe, đời sống tình dục hoặc xu hướng tình dục của một người [50].

2.1.1.2. Khái niệm quyền đối với DLCN

Quyền đối với DLCN (*right to personal data*) là một quyền con người, xuất hiện và phát triển mạnh trong bối cảnh xã hội số, thường được nhìn nhận như một cấu phần trung tâm của quyền riêng tư (*right to privacy*), là QCN cơ bản bảo đảm

tính tự chủ, phẩm giá và “không gian cá nhân” của mỗi con người. Ở góc độ QCN, quyền riêng tư trước hết mang ý nghĩa bảo vệ cá nhân khỏi các can thiệp tùy tiện hoặc bất hợp pháp vào đời sống riêng tư, gia đình, chỗ ở, thư tín và danh dự, uy tín. Tuyên ngôn Nhân quyền phổ quát năm 1948 khẳng định rõ nội dung này tại Điều 12 và tiếp tục được chuẩn hóa trong Công ước quốc tế về các quyền dân sự và chính trị (ICCPR), với Điều 17 ghi nhận quyền được pháp luật bảo vệ trước các can thiệp tùy tiện/bất hợp pháp vào đời sống riêng tư, gia đình, chỗ ở, thư tín, cũng như các cuộc tấn công bất hợp pháp vào danh dự và uy tín. Trên nền tảng đó, quyền riêng tư còn được tái khẳng định trong nhiều điều ước quốc tế chuyên biệt: Công ước về quyền của người lao động nhập cư (Điều 14), Công ước về quyền trẻ em (Điều 16), và Công ước về quyền của người khuyết tật (nhấn mạnh nghĩa vụ bảo vệ “thông tin cá nhân, sức khỏe và phục hồi chức năng” - Điều 22).

Quyền đối với DLCN không thay thế quyền riêng tư, mà hình thành như một cách cụ thể hóa quyền riêng tư trong điều kiện thông tin cá nhân được thu thập, xử lý và lưu chuyển bằng các hệ thống số với quy mô lớn. Trên thực tế, một số hệ thống pháp luật còn ghi nhận bảo vệ DLCN như một quyền cơ bản độc lập bên cạnh quyền riêng tư; điển hình là Hiến chương Quyền cơ bản của Liên minh châu Âu khi tách Điều 7 (tôn trọng đời sống riêng tư) và Điều 8 (bảo vệ DLCN). Cách ghi nhận này cho thấy xu hướng chuyên biệt hóa quyền đối với DLCN trong môi trường số, dù về mặt nội hàm, quyền này vẫn gắn chặt với hệ giá trị nền của quyền riêng tư.

Nội hàm quyền này có thể được trình bày theo nhóm quyền năng gắn với vòng đời dữ liệu như quyền được biết và quyền được thông tin; quyền đồng ý và quyền rút lại sự đồng ý; quyền truy cập, chỉnh sửa và cập nhật dữ liệu; quyền yêu cầu xóa, hủy dữ liệu hoặc hạn chế xử lý; quyền được bảo đảm an toàn và quyền yêu cầu khắc phục khi bị xâm hại, bảo mật dữ liệu và quyền được bảo vệ trước các rủi ro xâm phạm; là một quyền con người phái sinh từ quyền riêng tư, được kỹ thuật hóa và thể chế hóa thành một tập hợp các quyền năng pháp lý độc lập tương đối nhằm hiện thực hóa quyền riêng tư trong môi trường số. Theo đó, cá nhân có quyền yêu cầu cơ quan, tổ chức xử lý dữ liệu áp dụng các biện pháp kỹ thuật và tổ chức phù hợp nhằm ngăn chặn truy cập trái phép, rò rỉ, mất mát hoặc sử dụng sai mục đích. Khi xảy ra vi phạm, chủ thể dữ liệu có quyền được thông báo, được khiếu nại, yêu cầu bồi thường thiệt hại và được bảo vệ bằng các cơ chế pháp lý hữu hiệu.

Nói cách khác, *quyền đối với dữ liệu cá nhân không phải là quyền đơn lẻ mà là tổng hợp các quyền năng pháp lý cho phép cá nhân nắm giữ mức độ kiểm soát nhất định đối với việc thu thập, xử lý, sử dụng, lưu trữ, chia sẻ và chấm dứt xử lý dữ liệu liên quan trực tiếp đến mình nhằm bảo đảm đời sống riêng tư, tôn trọng nhân phẩm và an toàn thông tin.*

Trong điều kiện xây dựng chính quyền số, việc bảo đảm đầy đủ nội hàm quyền này không chỉ nhằm bảo vệ lợi ích của cá nhân, mà còn là điều kiện thiết yếu để củng cố niềm tin của người dân, nâng cao tính chính danh và hiệu quả hoạt động của Nhà nước trong môi trường quản trị số.

Đặc trưng pháp lý của quyền đối với DLCN thể hiện ở một số phương diện cơ bản sau đây:

Thứ nhất, quyền đối với DLCN mang bản chất của quyền nhân thân, gắn chặt với cá nhân. Dữ liệu cá nhân phản ánh các đặc điểm nhận dạng, tình trạng pháp lý - xã hội và các mối quan hệ của cá nhân; do đó, việc thu thập, lưu trữ và xử lý dữ liệu có khả năng tác động trực tiếp đến danh dự, nhân phẩm, đời sống riêng tư cũng như sự an toàn của chủ thể dữ liệu. Chính vì vậy, quyền đối với DLCN cần được nhìn nhận như một biểu hiện cụ thể của quyền nhân thân trong bối cảnh xã hội số.

Thứ hai, quyền đối với DLCN có tính chủ động và kiểm soát của chủ thể dữ liệu. Không chỉ dừng lại ở việc được bảo vệ trước các hành vi xâm phạm, cá nhân còn được trao quyền tham gia tích cực vào quá trình xử lý dữ liệu của mình thông qua các cơ chế pháp lý như quyền đồng ý hoặc từ chối, quyền rút lại sự đồng ý, quyền tiếp cận, chỉnh sửa, hạn chế xử lý và yêu cầu xóa dữ liệu. Đặc điểm này thể hiện sự chuyển dịch từ mô hình bảo vệ thụ động sang mô hình bảo vệ dựa trên quyền kiểm soát của cá nhân.

Thứ ba, quyền đối với DLCN mang tính kỹ thuật và quản trị cao. Việc bảo đảm và thực thi quyền này phụ thuộc đáng kể vào hệ thống CNTT, quy trình quản lý dữ liệu, cơ chế phân quyền truy cập, ghi nhận và giám sát hoạt động xử lý dữ liệu, cũng như các biện pháp bảo đảm an toàn, an ninh thông tin. Do đó, quyền đối với DLCN không chỉ là vấn đề pháp lý thuần túy mà còn gắn liền với năng lực quản trị và trình độ công nghệ của chủ thể xử lý dữ liệu.

Thứ tư, quyền đối với DLCN mang tính cân bằng lợi ích. Trong khu vực công, DLCN thường được xử lý nhằm phục vụ mục tiêu quản lý nhà nước, cung cấp dịch vụ công và bảo đảm lợi ích chung của xã hội. Vì vậy, việc bảo vệ quyền đối với

DLCN cần được đặt trong mối quan hệ hài hòa giữa bảo đảm QCN và yêu cầu hiệu lực, hiệu quả của hoạt động quản trị nhà nước, trên cơ sở các điều kiện hạn chế quyền được pháp luật quy định một cách chặt chẽ, cần thiết và tương xứng.

Về hình thức thể hiện Quyền đối với dữ liệu cá nhân (Tập hợp quyền năng độc lập tương đối). Để hiện thực hóa quyền riêng tư trong môi trường số, quyền đối với DLCN cấu thành một hệ thống các quyền năng cụ thể. Theo khoản 1, Điều 4, Luật Bảo vệ dữ liệu cá nhân 2025, quyền đối với dữ liệu cá nhân là 6 nhóm quyền cơ bản của chủ thể dữ liệu cá nhân bao gồm: Quyền được biết về hoạt động xử lý dữ liệu cá nhân; quyền đồng ý hoặc không đồng ý, yêu cầu rút lại sự đồng ý cho phép xử lý dữ liệu cá nhân; quyền xem, chỉnh sửa hoặc yêu cầu chỉnh sửa dữ liệu cá nhân; quyền yêu cầu cung cấp, xóa, hạn chế xử lý dữ liệu cá nhân, gửi yêu cầu phản đối xử lý dữ liệu cá nhân; quyền khiếu nại, tố cáo, khởi kiện, yêu cầu bồi thường thiệt hại theo quy định của pháp luật; quyền yêu cầu cơ quan có thẩm quyền hoặc cơ quan, tổ chức, cá nhân liên quan đến xử lý dữ liệu cá nhân thực hiện các biện pháp, giải pháp bảo vệ dữ liệu cá nhân của mình theo quy định của pháp luật [50].

Quyền đối với DLCN không hoàn toàn tách biệt khỏi quyền riêng tư (vì quyền riêng tư là gốc rễ lý luận và giá trị tối cao), nhưng nó đã trở nên độc lập tương đối về mặt thuật ngữ và cơ chế thực thi. Việc xác định này vừa giữ vững nền tảng quyền con người (theo Hiến pháp và Công ước quốc tế), vừa thiết lập được các công cụ pháp lý sắc bén để công dân kiểm soát quyền lực công trong chính quyền số.

2.1.1.3. Khái niệm về bảo vệ quyền đối với dữ liệu cá nhân

(1). *Chủ thể dữ liệu cá nhân*, là người được dữ liệu cá nhân phản ánh theo khoản 5 Điều 2 Luật Bảo vệ dữ liệu cá nhân 2025. Đây chính là người sở hữu thông tin (như họ tên, số điện thoại, địa chỉ, căn cước công dân...) và được pháp luật bảo vệ, có quyền kiểm soát, đồng ý hoặc rút lại sự đồng ý cho phép xử lý dữ liệu của mình.

(2). *Bảo vệ quyền đối với dữ liệu cá nhân*: Tại khoản 4, Điều 2, Luật Bảo vệ dữ liệu cá nhân 2025 nêu: Bảo vệ dữ liệu cá nhân là việc cơ quan, tổ chức, cá nhân sử dụng lực lượng, phương tiện, biện pháp để phòng, chống hoạt động xâm phạm dữ liệu cá nhân. Từ đó có thể nêu một cách tổng quát về *bảo vệ quyền đối với dữ liệu cá nhân*: là tổng thể các biện pháp pháp lý, kỹ thuật và tổ chức nhằm bảo đảm cá nhân có các quyền đối với dữ liệu cá nhân của mình và ngăn chặn mọi sự xâm phạm trái phép đến quyền đó.

(3).Khái niệm chính quyền địa phương cấp tỉnh

Theo Điều 16 và 17, Luật 77/2015/QH13, Luật Tổ chức chính quyền địa phương năm 2015: “*Chính quyền địa phương cấp tỉnh* là cấp chính quyền địa phương gồm có Hội đồng nhân dân tỉnh và Ủy ban nhân dân tỉnh”.

Có nhiệm vụ và quyền hạn như: “Tổ chức và bảo đảm việc thi hành Hiến pháp và pháp luật trên địa bàn tỉnh. Quyết định những vấn đề của tỉnh trong phạm vi được phân quyền, phân cấp theo quy định của Luật này và quy định khác của pháp luật có liên quan. Thực hiện nhiệm vụ, quyền hạn do cơ quan hành chính nhà nước ở trung ương ủy quyền. Kiểm tra, giám sát tổ chức và hoạt động của chính quyền địa phương ở các đơn vị hành chính trên địa bàn. Chịu trách nhiệm trước cơ quan nhà nước cấp trên về kết quả thực hiện các nhiệm vụ, quyền hạn của chính quyền địa phương ở tỉnh. Phối hợp với các cơ quan nhà nước ở trung ương, các địa phương thúc đẩy liên kết kinh tế vùng, thực hiện quy hoạch vùng, bảo đảm tính thống nhất của nền kinh tế quốc dân. Quyết định và tổ chức thực hiện các biện pháp nhằm phát huy quyền làm chủ của Nhân dân, huy động các nguồn lực xã hội để xây dựng và phát triển kinh tế - xã hội, bảo đảm quốc phòng, an ninh trên địa bàn tỉnh” [45].

Có thể khái quát: *Chính quyền địa phương cấp tỉnh là cấp trung gian then chốt, vừa mang tính chất đại diện cho nhân dân địa phương, vừa thực thi quyền hành pháp của Nhà nước trên một địa bàn lãnh thổ cụ thể.*

2.1.1.4. Khái niệm chính quyền số và chính quyền số cấp tỉnh

Thuật ngữ “*chính quyền số*” được hình thành trên cơ sở khái niệm “*Chính phủ số*”, vốn được xác định là một trong ba trụ cột của chuyển đổi số quốc gia cùng với kinh tế số và xã hội số. Trong cấu trúc này, Chính phủ số thường được xem là mắt xích then chốt do giữ vai trò định hướng, dẫn dắt và điều phối sự phát triển của kinh tế số và xã hội số. Vai trò đó bắt nguồn từ chức năng cơ bản của Nhà nước trong quản trị và phát triển kinh tế - xã hội. Trong bối cảnh kỷ nguyên số, Chính phủ số vì thế giữ vị trí trung tâm trong việc định hướng, quản lý và thúc đẩy kinh tế số, xã hội số như một yêu cầu mang tính tất yếu.

Theo cách tiếp cận khái quát, Chính phủ số là khái niệm chỉ phương thức vận hành của Chính phủ (mở rộng hơn là toàn bộ cơ quan công quyền) dựa trên ứng dụng công nghệ số và các giải pháp thông minh trong hoạt động quản trị trên môi trường số. Ở góc nhìn khác, thuật ngữ này cũng được dùng để mô tả một mô hình chính phủ, chính quyền được tổ chức và vận hành theo hướng hiệu lực, hiệu quả, lấy công nghệ

số và các giải pháp thông minh làm nền tảng; đồng thời tăng cường khả năng tương tác, tiếp nhận phản hồi và phục vụ người dân, doanh nghiệp một cách kịp thời, nhịp nhàng.

Từ nền tảng khái niệm Chính phủ số, có thể hiểu “*chính quyền số*” là mô hình chính quyền vận hành chủ yếu dựa trên ứng dụng công nghệ số nhằm liên tục đổi mới phương thức quản trị, qua đó nâng cao hiệu lực, hiệu quả hoạt động của bộ máy. Nói cách khác, chính quyền số phản ánh phương thức tổ chức và thực thi chức năng quản trị nhà nước của chính quyền trong môi trường số.

Theo quy định của pháp luật về tổ chức hành chính và tổ chức chính quyền địa phương, cấp tỉnh được hiểu là cấp đơn vị hành chính gồm tỉnh và thành phố trực thuộc trung ương, đồng thời tương ứng với một cấp chính quyền địa phương được tổ chức với hai thiết chế cơ bản là Hội đồng nhân dân và UBND để thực hiện chức năng quản trị nhà nước trong phạm vi địa bàn cấp tỉnh. Trên cơ sở đó, nếu chính quyền số được hiểu là mô hình chính quyền vận hành chủ yếu dựa trên ứng dụng công nghệ số nhằm liên tục đổi mới phương thức quản trị, qua đó nâng cao hiệu lực, hiệu quả hoạt động của bộ máy, phản ánh phương thức tổ chức và thực thi chức năng quản trị nhà nước trong môi trường số, thì *chính quyền số cấp tỉnh có thể được hiểu là mô hình chính quyền địa phương ở cấp tỉnh trong đó các cơ quan của chính quyền cấp tỉnh, nòng cốt là Hội đồng nhân dân và Ủy ban nhân dân, tổ chức vận hành và thực thi nhiệm vụ, quyền hạn chủ yếu trên môi trường số, dựa trên hạ tầng số, nền tảng số, dữ liệu số và các ứng dụng công nghệ số để cải tiến quy trình quản trị, tăng cường năng lực điều hành dựa trên dữ liệu, nâng cao chất lượng cung ứng dịch vụ công, bảo đảm tính minh bạch và khả năng tương tác với người dân, doanh nghiệp, qua đó nâng cao hiệu lực, hiệu quả quản lý nhà nước ở phạm vi cấp tỉnh.*

Thứ nhất, công nghệ số là nền tảng của hoạt động quản lý nhà nước và cung cấp dịch vụ công. Theo định hướng chuyển đổi số quốc gia, chính quyền số được xây dựng trên cơ sở ứng dụng đồng bộ CNTT và truyền thông, internet và các công nghệ số chủ đạo như dữ liệu lớn, trí tuệ nhân tạo, internet vạn vật, điện toán đám mây và công nghệ di động, nhằm đổi mới phương thức điều hành và tổ chức thực thi công vụ.

Thông tin phục vụ quản lý được số hóa, chuẩn hóa, tích hợp và chia sẻ trong các cơ sở dữ liệu và hệ thống thông tin, hình thành nền tảng dữ liệu phục vụ điều hành, quản lý kinh tế - xã hội. Việc khai thác dữ liệu dùng chung thông qua các cơ

chế xác thực điện tử cho phép các cơ quan phối hợp xử lý công việc trên môi trường số, thay thế dần mô hình quản lý dựa trên hồ sơ giấy.

Thứ hai, môi trường hoạt động chủ yếu của chính quyền số là không gian mạng và các nền tảng số. Phần lớn hoạt động nội bộ của cơ quan nhà nước, quy trình giải quyết thủ tục hành chính, cũng như tương tác giữa chính quyền với người dân và doanh nghiệp được thực hiện trên môi trường trực tuyến, thông qua các nền tảng số thống nhất.

Thứ ba, chính quyền số hướng tới quản trị dựa trên dữ liệu và nâng cao hiệu lực, hiệu quả quản lý nhà nước. Thông qua việc ứng dụng các công nghệ phân tích và xử lý dữ liệu, hoạt động điều hành ngày càng dựa trên bằng chứng, có khả năng dự báo và hỗ trợ ra quyết định; đồng thời, việc giám sát, kiểm soát các lĩnh vực kinh tế - xã hội được thực hiện kịp thời và chính xác hơn.

Thứ tư, chính quyền số thúc đẩy sự tham gia và tăng cường tương tác giữa Nhà nước với người dân và doanh nghiệp. Thông qua các nền tảng số và ứng dụng công nghệ thông minh, chính quyền có điều kiện tiếp nhận phản hồi liên tục, đa chiều từ xã hội, qua đó nâng cao khả năng đáp ứng nhu cầu của người dân, doanh nghiệp và tăng cường mức độ đồng thuận xã hội.

2.1.1.5. Khái niệm bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh

Trong tiến trình chuyển đổi số quốc gia, xây dựng chính quyền số cấp tỉnh không chỉ thuần túy là việc ứng dụng công nghệ để nâng cao hiệu quả quản trị hành chính, mà bản chất là quá trình tái cấu trúc mối quan hệ pháp lý giữa chính quyền (Bên kiểm soát dữ liệu, chủ thể mang nghĩa vụ) và công dân (Chủ thể dữ liệu, chủ thể mang quyền) trên môi trường số.

Dưới tiếp cận pháp luật về quyền con người, việc xử lý DLCN quy mô lớn trong các dịch vụ công trực tuyến, thủ tục hành chính và hệ thống giám sát đô thị thông minh (IOC) luôn chứa đựng nguy cơ tiềm ẩn về lạm dụng quyền lực công và xâm phạm quyền riêng tư. Do đó, bảo vệ quyền đối với DLCN trở thành điều kiện tiên quyết bảo đảm tính chính đáng pháp lý của chính quyền số.

Từ sự phân tích tổng hợp các cách tiếp cận lập pháp, hành pháp và bảo vệ quyền con người, Luận án xác định bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh bao hàm 03 nội dung cốt lõi:

(1). *Về chủ thể mang nghĩa vụ*: Là nghĩa vụ pháp lý bắt buộc của các cơ quan nhà nước thuộc cấu trúc chính quyền địa phương cấp tỉnh (HĐND, UBND, các sở, ban, ngành và đơn vị vận hành hạ tầng số) trong việc tuân thủ các nguyên tắc cốt lõi về xử lý dữ liệu (giới hạn mục đích, tối thiểu hóa dữ liệu, tính minh bạch và trách nhiệm giải trình).

(2). *Về chủ thể mang quyền*: Là việc bảo đảm cho công dân công cụ và năng lực pháp lý thực chất để thực thi “Quyền tự quyết thông tin”, bao gồm quyền biết, truy cập, đồng ý, đính chính, hạn chế hoặc yêu cầu xóa dữ liệu trên các nền tảng số công cộng.

(3). *Về cơ chế bảo đảm*: Là sự kết hợp hài hòa giữa cơ chế kiểm soát quyền lực công nội bộ (thanh tra, kiểm tra, kiểm toán dữ liệu) với các biện pháp tự vệ pháp lý và kỹ thuật bảo mật, nhằm phòng ngừa, ngăn chặn rủi ro và bồi thường thiệt hại khi có vi phạm.

Từ những phân tích trên, Luận án thống nhất xác định khái niệm công cụ (khái niệm trung tâm) của đề tài như sau: *“Bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh là tổng thể các cơ chế kiểm soát quyền lực công, giải pháp pháp lý và quy trình vận hành do các cơ quan nhà nước thuộc chính quyền địa phương cấp tỉnh thực thi, nhằm bảo đảm nghĩa vụ tôn trọng, bảo vệ và thực hiện quyền tự quyết thông tin của công dân trong toàn bộ chu trình xử lý dữ liệu phục vụ quản trị công; qua đó phòng ngừa sự lạm dụng quyền lực công, bảo đảm an toàn dữ liệu và thiết lập sự cân bằng hài hòa giữa mục tiêu tối ưu hóa quản lý hành chính với nghĩa vụ bảo vệ quyền con người trong môi trường số”*.

2.1.1.6. Phân biệt quyền đối với DLCN với các khái niệm liên quan

Để phân biệt rõ quyền đối với DLCN với các khái niệm liên quan, được thể hiện qua bảng tiêu chí và luận giải sau:

Bảng phân định so sánh 5 khái niệm cốt lõi:

Tiêu chí phân biệt	Quyền đối với DLCN	Bảo vệ DLCN	An toàn thông tin	An ninh mạng	Quản trị dữ liệu
Bản chất	Là QCN, quyền công	Là hệ thống nghĩa vụ	Là tính chất kỹ thuật	Là trạng thái an	Là tổ chức, quy trình và

Tiêu chí phân biệt	Quyền đối với DLCN	Bảo vệ DLCN	An toàn thông tin	An ninh mạng	Quản trị dữ liệu
	dân (pháp lý nhân thân).	pháp lý, chính sách và cơ chế để bảo đảm quyền.	(tính bảo mật, toàn vẹn, khả dụng).	ninh quốc gia, trật tự an toàn xã hội trên không gian mạng.	chính sách quản lý tài nguyên dữ liệu của tổ chức.
Chủ thể trung tâm	Công dân, chủ thể dữ liệu	Nhà nước & các bên xử lý dữ liệu	Hệ thống CNTT, dữ liệu	Chủ quyền quốc gia, trật tự xã hội	Cơ quan nhà nước, tổ chức
Mục tiêu tối thượng	Bảo vệ nhân phẩm, danh dự, quyền riêng tư và sự tự trị của cá nhân.	Bảo đảm tính hợp pháp, minh bạch, đúng mục đích khi xử lý DLCN.	Chống truy cập trái phép, mất mát, biến đổi hoặc phá hoại dữ liệu kỹ thuật.	Bảo vệ chủ quyền số, hạ tầng số trọng yếu, phòng chống tội phạm mạng.	Tối ưu hóa khai thác, chia sẻ, dùng chung dữ liệu gắn với trách nhiệm.
Góc nhìn chính	Tiếp cận dựa trên Quyền con người	Tiếp cận dựa trên Tuân thủ Pháp lý	Tiếp cận dựa trên kỹ thuật, công nghệ	Tiếp cận dựa trên An ninh quốc gia	Tiếp cận dựa trên Quản trị công

Lược giải chi tiết sự kết nối và ranh giới:

Quyền đối với DLCN với bảo vệ DLCN: Quyền đối với DLCN là mục tiêu, nội dung (Khía cạnh chủ thể thuộc về người dân), còn Bảo vệ DLCN là phương tiện, nghĩa vụ (Khía cạnh thể chế thuộc về Nhà nước và chính quyền tỉnh). Chính quyền

số không “ban phát” quyền, mà có nghĩa vụ thiết lập cơ chế bảo vệ DLCN để quyền đối với DLCN được thực thi trên thực tế.

Bảo vệ DLCN với An toàn thông tin và An ninh mạng: An toàn thông tin và An ninh mạng là điều kiện kỹ thuật và môi trường cần thiết nhưng chưa đủ để bảo vệ DLCN. Một hệ thống chính quyền số có thể đạt chuẩn An toàn thông tin (mã hóa tốt, không bị tấn công mạng) và bảo đảm An ninh mạng, nhưng vẫn có thể vi phạm quyền đối với DLCN nếu chính quyền thu thập quá mức cần thiết, liên thông dữ liệu trái mục đích ban đầu hoặc không cung cấp công cụ cho người dân rút lại sự đồng ý.

Bảo vệ DLCN với quản trị dữ liệu: Quản trị dữ liệu trong chính quyền số hướng tới mục tiêu làm giàu, mở, chia sẻ và tối ưu hóa dữ liệu để phục vụ quản lý hành chính. Bản chất của quản trị dữ liệu là mở và chia sẻ, còn Bảo vệ DLCN đặt ra ranh giới và giới hạn. Do đó, Bảo vệ DLCN chính là khung giới hạn pháp lý bắt buộc đối với Quản trị dữ liệu số công quyền.

2.1.2. Đặc điểm của bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh

Dưới tiếp cận của pháp luật về quyền con người, bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh mang những đặc điểm pháp lý cơ bản sau:

2.1.2.1. Mang tính cân bằng pháp lý giữa yêu cầu tối ưu hóa quản trị công vụ và bảo đảm quyền tự quyết thông tin của công dân

Đặc điểm này phản ánh việc áp dụng nguyên tắc tương xứng trong kiểm soát quyền lực nhà nước. Trong chính quyền số, DLCN vừa là đối tượng bảo vệ, vừa là nguồn lực quản trị công vụ. Bảo vệ quyền dữ liệu không mang tính phủ quyết hay triệt tiêu việc lưu thông dữ liệu, mà là xác lập giới hạn pháp lý cho quyền lực hành chính.

Nội hàm pháp lý: Bất kỳ sự can thiệp, thu thập hay chia sẻ DLCN nào của chính quyền cấp tỉnh phục vụ mục đích công cộng chỉ được coi là hợp pháp khi bảo đảm tính cần thiết, tối thiểu và có mục đích chính đáng. Việc tuyệt đối hóa yêu cầu quản lý mà bỏ qua cơ chế kiểm soát tuân thủ sẽ dẫn đến nguy cơ lạm dụng quyền lực công, xâm phạm quyền riêng tư và làm suy giảm tính chính đáng pháp lý của bộ máy hành chính.

2.1.2.2. Mang tính chất giải quyết “bất cân xứng quyền lực” giữa Chính quyền địa phương và Công dân trên môi trường số

Đặc điểm này xuất phát từ bản chất của mối quan hệ pháp lý giữa Chủ thể mang quyền (Công dân) và Chủ thể mang nghĩa vụ (Chính quyền cấp tỉnh).

Về phía Chính quyền: Việc tích hợp, tập trung hóa dữ liệu quy mô lớn tại các cơ quan chuyên môn cấp tỉnh tạo ra “quyền lực thông tin” rất lớn cho bộ máy hành chính, tiềm ẩn nguy cơ giám sát quá mức hoặc làm lộ lọt dữ liệu diện rộng.

Về phía Công dân: Người dân thường ở thế yếu, thiếu công cụ tương tác pháp lý và gặp rào cản về năng lực số để thực thi các quyền tự vệ (quyền biết, truy cập, phản đối hoặc yêu cầu xóa dữ liệu). Do đó, bảo vệ quyền dữ liệu tại chính quyền số cấp tỉnh mang đặc thù là cơ chế bảo hộ pháp lý mang tính trợ giúp, nhằm tái lập sự cân bằng quyền lực và bảo vệ vị thế của công dân trước cơ quan công quyền.

2.1.2.3. Được thực hiện thông qua cơ chế phân định trách nhiệm pháp lý và trách nhiệm giải trình công vụ đa bên

Bảo vệ quyền dữ liệu trong khu vực công cấp tỉnh không còn là quan hệ đơn phương truyền thống giữa Nhà nước và Công dân, mà chuyển dịch sang mô hình quản trị đa bên với sự phân định rõ ràng về trách nhiệm pháp lý:

Cơ quan nhà nước và đội ngũ công chức cấp tỉnh: Mặc dù thẩm quyền xử lý dữ liệu bị phân tán sâu rộng (từ các sở, ngành đến bộ phận một cửa), HĐND và UBND cấp tỉnh vẫn là chủ thể chịu trách nhiệm pháp lý tối cao trong việc bảo đảm nghĩa vụ tôn trọng và bảo vệ quyền con người.

Doanh nghiệp công nghệ (Bên thứ ba được ủy quyền): Tham gia vận hành hạ tầng số của tỉnh với tư cách là Bên xử lý dữ liệu. Rủi ro pháp lý đặt ra là việc chuyển giao thẩm quyền công mà thiếu cơ chế kiểm soát, đòi hỏi phải xác lập giới hạn ủy quyền pháp lý để ngăn chặn hành vi lợi dụng dữ liệu công vụ phục vụ mục đích thương mại.

2.1.2.4. Đảm bảo tính thống nhất của tiêu chuẩn quyền con người quốc gia nhưng chịu sự chi phối bởi đặc thù thực thi ở địa phương

Đây là biểu hiện của mối quan hệ giữa tính thống nhất của thể chế và tính linh hoạt trong thực thi địa phương:

Tính thống nhất: Tiêu chuẩn bảo vệ quyền dữ liệu do Hiến pháp, Luật Bảo vệ DLCN và các điều ước quốc tế ghi nhận là khung pháp lý bắt buộc, mang tính tối thiểu mà tất cả các chính quyền cấp tỉnh phải tuân thủ tuyệt đối, không được phép hạ thấp tiêu chuẩn vì bất kỳ lý do quản lý nào.

Tính đặc thù địa phương: Hiệu quả thực thi quyền dữ liệu trên thực tế bị chi phối mạnh mẽ bởi các yếu tố thực chứng riêng biệt của từng tỉnh (sự chênh lệch về ngân sách bảo đảm quyền, trình độ nhận thức pháp lý của dân cư vùng sâu, vùng xa, hoặc đặc thù của các đô thị lớn có lượng dữ liệu biến động cao). Do đó, bảo vệ quyền

dữ liệu đòi hỏi chính quyền cấp tỉnh phải cụ thể hóa quy trình thực thi sao cho vừa phù hợp với điều kiện địa phương, vừa giữ vững chuẩn mực bảo vệ quyền con người của quốc gia.

2.1.3. Vai trò của bảo vệ quyền đối với dữ liệu cá nhân khi xây dựng chính quyền số cấp tỉnh

Thứ nhất, bảo vệ quyền đối với DLCN là điều kiện bảo đảm tính hợp hiến, hợp pháp của hoạt động quản trị dữ liệu trong khu vực công. Việc thu thập, chia sẻ và khai thác DLCN để phục vụ quản lý nhà nước, nếu không được giới hạn bởi các nguyên tắc pháp lý rõ ràng, có thể dẫn đến nguy cơ lạm quyền, xâm phạm đời sống riêng tư và quyền tự chủ thông tin của cá nhân. Ngược lại, khi bảo vệ DLCN được xây dựng như một phần cấu thành của quản trị dữ liệu, hoạt động xử lý dữ liệu sẽ có ranh giới pháp lý cụ thể, giúp chính quyền cấp tỉnh vừa khai thác dữ liệu phục vụ điều hành, vừa bảo đảm QCN và tránh các tranh chấp, khiếu kiện phát sinh.

Bảo vệ quyền đối với DLCN không chỉ là yêu cầu tuân thủ pháp luật và bảo đảm QCN, mà còn là điều kiện nền tảng quyết định chất lượng, tính chính danh và khả năng vận hành bền vững của mô hình chính quyền số cấp tỉnh. Trong bối cảnh chính quyền cấp tỉnh là nơi trực tiếp triển khai phần lớn hoạt động quản lý nhà nước gắn với người dân và doanh nghiệp, DLCN được thu thập, xử lý với tần suất cao, phạm vi rộng và mức độ liên thông ngày càng lớn. Do đó, bảo vệ DLCN giữ vai trò “hạ tầng mềm” của chính quyền số; nếu không có cơ chế bảo vệ hiệu quả, các nền tảng và dịch vụ số khó đạt được sự chấp nhận xã hội, khó mở rộng quy mô và tiềm ẩn rủi ro pháp lý, kỹ thuật nghiêm trọng.

Thứ hai, bảo vệ quyền đối với DLCN là cơ sở để tạo lập và duy trì niềm tin số giữa chính quyền cấp tỉnh với người dân, doanh nghiệp. Chính quyền số chỉ có thể vận hành hiệu quả khi người dân sẵn sàng cung cấp thông tin, sử dụng dịch vụ công trực tuyến và tham gia tương tác qua môi trường số. Niềm tin đó phụ thuộc lớn vào việc cá nhân cảm nhận dữ liệu của mình được xử lý minh bạch, an toàn, đúng mục đích và không bị lạm dụng. Vì vậy, bảo vệ DLCN không chỉ là “yêu cầu đạo lý, pháp lý”, mà còn là điều kiện để gia tăng mức độ chấp nhận và sử dụng dịch vụ số, qua đó quyết định hiệu quả thực thi của chính quyền số cấp tỉnh.

Thứ ba, bảo vệ quyền đối với DLCN góp phần nâng cao chất lượng quản lý nhà nước và hiệu quả cung ứng các dịch vụ công. Điều này thúc đẩy quản trị dữ liệu theo hướng chuẩn hóa và chuyên nghiệp hóa, từ đó nâng cao hiệu quả điều hành của

cấp tỉnh. Khi yêu cầu bảo vệ quyền DLCN được đặt ra nghiêm ngặt, các cơ quan buộc phải chuẩn hóa quy trình thu thập, lưu trữ, chia sẻ dữ liệu; phân quyền truy cập hợp lý; ghi nhận nhật ký xử lý; kiểm soát mục đích sử dụng; và duy trì chất lượng dữ liệu. Những yêu cầu này không chỉ bảo vệ quyền cá nhân mà còn góp phần làm cho dữ liệu “*đúng, đủ, sạch, sống, thống nhất, dùng chung*” qua đó nâng cao chất lượng phân tích, dự báo và ra quyết định dựa trên dữ liệu của chính quyền cấp tỉnh.

Bảo vệ quyền đối với DLCN góp phần hiện thực hóa mô hình chính quyền số, lấy người dân làm trung tâm và định hình chuẩn mực đạo đức số trong khu vực công. Một chính quyền số hiện đại không chỉ được đo bằng mức độ số hóa thủ tục hay số lượng dịch vụ công trực tuyến, mà còn bởi cách thức tôn trọng quyền, phẩm giá và lợi ích hợp pháp của cá nhân trong môi trường số.

Thứ tư, bảo vệ quyền đối với dữ liệu cá nhân là yêu cầu tất yếu trong hội nhập quốc tế và phát triển kinh tế địa phương. Đối với hội nhập quốc tế và toàn cầu hoá, trong bối cảnh nền kinh tế số, dữ liệu được ví như nguồn tài nguyên số quốc gia. Tuy nhiên, nguồn tài nguyên số chỉ phát huy hiệu quả trong quá trình hội nhập khi có sự tin tưởng và các rào cản pháp lý được tháo gỡ. Các quốc gia và khối kinh tế lớn hiện nay đều dựng lên những hàng rào pháp lý rất nghiêm ngặt về dữ liệu. Ví dụ điển hình là GDPR (Quy định chung về bảo vệ dữ liệu) của EU, hay các hiệp định thương mại thế hệ mới như CPTPP, EVFTA đều có các chương riêng về thương mại điện tử và luồng dữ liệu xuyên biên giới. Nếu không bảo vệ quyền dữ liệu cá nhân theo chuẩn quốc tế, Việt Nam sẽ tự loại mình khỏi môi trường thương mại số toàn cầu. Cần xây dựng “Niềm tin kỹ thuật số” trong quá trình hội nhập, không chỉ là ký kết hiệp định, mà là làm sao để các đối tác quốc tế dám “giao” dữ liệu cho các doanh nghiệp Việt Nam xử lý. Một hệ thống pháp lý bảo vệ dữ liệu nghiêm túc là lời cam kết mạnh mẽ nhất về độ an toàn của môi trường đầu tư. Bảo vệ dữ liệu cá nhân không còn là một vấn đề quyền con người thuần túy, mà đã dịch chuyển thành một công cụ bảo hộ thương mại và khẳng định chủ quyền số trong quan hệ quốc tế.

Dưới góc độ phát triển kinh tế địa phương: (1) Bảo vệ quyền dữ liệu cá nhân không chỉ là vấn đề vĩ mô ở tầm quốc gia mà còn tác động trực tiếp đến kinh tế địa phương cấp tỉnh. (2) Thu hút dòng vốn FDI chất lượng cao: các tập đoàn công nghệ lớn, các doanh nghiệp đa quốc gia khi lựa chọn địa phương để đặt đại bản doanh, trung tâm dữ liệu hoặc nhà máy thông minh, luôn đặt yếu tố an toàn thông tin lên hàng đầu. Địa phương nào có hạ tầng pháp lý và ý thức bảo mật tốt sẽ chiếm ưu thế

tuyệt đối. (3) Thúc đẩy kinh tế số địa phương bền vững: Khi người dân địa phương cảm thấy dữ liệu cá nhân của họ được bảo vệ, họ sẽ tự tin hơn khi tham gia vào các dịch vụ công trực tuyến, thương mại điện tử, ví điện tử và các mô hình kinh tế chia sẻ. Đây chính là bệ phóng cho các doanh nghiệp khởi nghiệp tại địa phương phát triển. (4) Giảm thiểu rủi ro và chi phí xã hội: Các vụ rò rỉ dữ liệu, lừa đảo công nghệ cao không chỉ gây thiệt hại về tài chính cho người dân mà còn làm xói mòn niềm tin vào chính quyền và môi trường kinh doanh tại địa phương. Chủ động bảo vệ quyền dữ liệu chính là cách bảo vệ tài sản và sự ổn định kinh tế của tỉnh nhà.

Tóm lại, bảo vệ quyền đối với dữ liệu cá nhân không phải là kìm hãm sự phát triển, mà ngược lại, nó là điều kiện nền tảng không thể thiếu. Nó vừa là “luật chơi” bắt buộc phải tuân thủ để hội nhập sâu rộng, vừa là chiến lược tạo lợi thế cạnh tranh cốt lõi để các địa phương bứt phá kinh tế trong thời đại số.

Thứ năm, bảo vệ quyền đối với DLCN là nhân tố quan trọng để phòng ngừa, giảm thiểu rủi ro và các hành vi vi phạm pháp luật trên không gian mạng, an toàn thông tin và rủi ro vận hành của hệ thống chính quyền số cấp tỉnh. DLCN có giá trị cao, thường trở thành mục tiêu của tấn công mạng, mua bán trái phép hoặc khai thác vì mục đích trục lợi. Khi xảy ra sự cố rò rỉ hay lộ lọt dữ liệu, hậu quả không chỉ dừng ở thiệt hại của cá nhân mà còn kéo theo suy giảm uy tín của chính quyền, gián đoạn cung cấp dịch vụ công, thậm chí ảnh hưởng đến trật tự, an toàn xã hội. Do đó, cơ chế bảo vệ DLCN (kết hợp biện pháp pháp lý, tổ chức và kỹ thuật) có vai trò như một “lớp phòng vệ” giúp tăng khả năng chống chịu và tính liên tục của hoạt động chính quyền số.

2.2. NỘI DUNG, PHƯƠNG THỨC VÀ CÁC YẾU TỐ TÁC ĐỘNG ĐẾN BẢO VỆ QUYỀN ĐỐI VỚI DỮ LIỆU CÁ NHÂN TRONG XÂY DỰNG CHÍNH QUYỀN SỐ CẤP TỈNH

2.2.1. Nội dung quyền và nội dung bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh

Dưới góc độ khoa học pháp lý về quyền con người, việc xây dựng chính quyền số cấp tỉnh tạo ra một quan hệ pháp lý song phương giữa Nhà nước và Công dân trên môi trường số. Việc làm rõ cấu trúc lý luận đòi hỏi phải phân định rạch ròi giữa hai mặt của cùng một vấn đề: Nội dung quyền đối với dữ liệu cá nhân (đóng vai trò là quyền năng của chủ thể mang quyền - Công dân) và Nội dung bảo vệ quyền đối với dữ liệu cá nhân (đóng vai trò là nghĩa vụ, cơ chế và phương thức thực thi của chủ thể

mang nghĩa vụ - Chính quyền cấp tỉnh). Sự phân định này là "khái niệm công cụ" trung tâm để Luận án tiến hành đánh giá thực trạng ở Chương 3 và đề xuất giải pháp ở Chương 4.

2.2.1.1. Nội dung quyền đối với dữ liệu cá nhân của công dân trong xây dựng chính quyền số cấp tỉnh

Quyền đối với DLCN của công dân trong mối quan hệ với chính quyền số cấp tỉnh là tập hợp các quyền năng pháp lý thuộc quyền tự quyết thông tin, định vị người dân từ chỗ là “đối tượng quản lý hành chính” trở thành “chủ thể sở hữu quyền” đối với tài sản số của mình. Cụ thể hóa các quy định của Luật Bảo vệ dữ liệu cá nhân (Luật 91/2025/QH15) [50], hệ thống quyền này trong môi trường chính quyền số cấp tỉnh cấu thành bởi 03 nhóm quyền năng cốt lõi:

(1) Nhóm quyền tiếp cận và xử lý thông tin:

Quyền được biết về hoạt động xử lý dữ liệu: Công dân có quyền được thông báo minh bạch, rõ ràng về việc cơ quan nhà nước cấp tỉnh thu thập, sử dụng, liên thông hay chia sẻ dữ liệu nào của mình, mục đích xử lý và thời gian lưu trữ trên các cổng dịch vụ công trực tuyến cấp tỉnh (như iHanoi, Hue-S...).

Quyền đồng ý hoặc không đồng ý, yêu cầu rút lại sự đồng ý cho phép xử lý dữ liệu cá nhân: Công dân có quyền quyết định cho phép hoặc từ chối cơ quan nhà nước và các bên liên quan khai thác DLCN của mình ngoài các trường hợp phục vụ công vụ bắt buộc theo quy định của luật.

Quyền truy cập và xem dữ liệu: Công dân có quyền truy cập trực tiếp vào “Kho dữ liệu điện tử của công dân” trên hệ thống thông tin giải quyết thủ tục hành chính cấp tỉnh để tự kiểm tra, trích xuất dữ liệu cư trú, đất đai, hộ tịch, thuế của chính mình.

(2). Nhóm quyền kiểm soát và chỉnh sửa dữ liệu:

Quyền xem, đính chính và cập nhật dữ liệu: Quyền yêu cầu chính quyền số cập nhật, sửa đổi, đính chính các thông tin sai lệch, không chính xác trong các cơ sở dữ liệu chuyên ngành cấp tỉnh theo thời gian thực (hộ tịch, đất đai, thuế...) nhằm bảo đảm quyền lợi thiết thân trong thụ hưởng dịch vụ công.

Quyền xóa, hủy hoặc hạn chế xử lý dữ liệu: Quyền yêu cầu ẩn danh, tiêu hủy hoặc dừng chia sẻ dữ liệu khi mục đích giải quyết thủ tục hành chính đã hoàn thành và hết thời hạn lưu trữ nghiệp vụ, như lịch sử định vị camera đô thị, tệp đính kèm thủ tục đã giải quyết (quyền được lãng quên).

Quyền phản đối xử lý tự động: Quyền từ chối các quyết định hành chính hoàn toàn tự động dựa trên thuật toán AI hoặc hệ thống chấm điểm tại Trung tâm điều hành thông minh (IOC) nếu quyết định đó gây bất lợi cho quyền, lợi ích hợp pháp của công dân.

(3). Nhóm quyền tự vệ và hỗ trợ pháp lý

Quyền yêu cầu áp dụng các biện pháp bảo vệ an toàn: Quyền chủ động kích hoạt các công cụ phản ánh (Tổng đài 1022, ứng dụng công dân số) để yêu cầu cơ quan có thẩm quyền ngăn chặn khẩn cấp các hành vi lạm dụng hoặc lỗ hổng bảo mật phát hiện được hoặc hành vi sai phạm của cán bộ công vụ.

Quyền khiếu nại, tố cáo và khởi kiện: Quyền sử dụng các thiết chế thanh tra, tư pháp để khiếu kiện các hành vi vi phạm về dữ liệu do lỗi tác nghiệp của cán bộ, công chức hoặc cơ quan nhà nước cấp tỉnh.

Quyền yêu cầu bồi thường thiệt hại: Quyền đòi bồi thường thiệt hại về vật chất và tinh thần theo quy định pháp luật khi bị xâm phạm quyền dữ liệu do sự cố rò rỉ, lộ lọt từ hệ thống chính quyền số dẫn đến bị lừa đảo, xúc phạm danh dự.

2.2.1.2. Nội dung bảo vệ quyền đối với DLCN của chính quyền số cấp tỉnh

Bảo vệ quyền đối với DLCN là quá trình Chính quyền số cấp tỉnh thực hiện nghĩa vụ quốc gia về quyền con người thông qua việc xác lập hành lang pháp lý, quy trình vận hành và giải pháp kỹ thuật nhằm bảo đảm cho hệ thống 6 nhóm quyền của công dân (theo Luật Bảo vệ dữ liệu cá nhân) được thực thi thực chất. Nội dung bảo vệ bao gồm các trụ cột chính sau:

(1). Bảo đảm các nguyên tắc pháp lý tối thiểu trong xử lý dữ liệu:

Hợp pháp, minh bạch và công bằng: Cấm việc đồng bộ hoặc liên thông “ngầm” dữ liệu giữa các sở, ngành khi thiếu căn cứ luật định. Công khai minh bạch chính sách bảo mật dữ liệu trên cổng dịch vụ công.

Nguyên tắc giới hạn mục đích và tối thiểu hóa dữ liệu: Loại bỏ hoàn toàn các trường thông tin thừa trên biểu mẫu điện tử (e-Form). Dữ liệu thu thập cho thủ tục nào chỉ được sử dụng đúng cho thủ tục đó, không tự ý chuyển giao cho bên thứ ba (doanh nghiệp đối tác công tư - PPP).

Nguyên tắc chính xác, giới hạn lưu trữ và trách nhiệm giải trình: Thiết lập thời hạn lưu trữ dữ liệu tạm thời, tự động ẩn danh, xóa dữ liệu sau khi hết thời hiệu khiếu nại. Quy định trách nhiệm giải trình trực tiếp của người đứng đầu (Chủ tịch UBND, Giám đốc Sở) khi xảy ra sự cố rò rỉ hoặc sai lệch dữ liệu.

(2). Phân định rạch ròi trách nhiệm pháp lý của các chủ thể tham gia quan hệ dữ liệu

Cơ quan nhà nước cấp tỉnh: Chịu trách nhiệm pháp lý trực tiếp trong việc quản lý, bảo mật và giải trình công vụ; bắt buộc áp dụng các biện pháp quản lý và kỹ thuật tương xứng với mức độ rủi ro. Lập hồ sơ Đánh giá tác động xử lý DLCN (DPIA), chỉ định bộ phận chuyên trách an toàn dữ liệu và giải trình trước công dân khi có sự cố.

Doanh nghiệp, đối tác công - tư (Bên thứ ba): Tuân thủ tuyệt đối nguyên tắc “Đồng ý rõ ràng”. Doanh nghiệp tham gia vận hành hạ tầng Cloud, IOC của tỉnh chỉ đóng vai trò xử lý theo ủy quyền kỹ thuật, chịu trách nhiệm bồi thường thiệt hại toàn diện và chịu các chế tài tài chính nghiêm khắc (phạt đến 5% doanh thu) nếu làm rò rỉ dữ liệu [50].

Đội ngũ cán bộ, công chức: Tuân thủ đạo đức công vụ số và quy định phân quyền tiếp cận.

Nghĩa vụ của Công dân (Chủ thể dữ liệu): Cung cấp thông tin trung thực khi làm thủ tục hành chính, chủ động nâng cao năng lực số và có trách nhiệm tự bảo mật tài khoản cá nhân.

(3). Thực hiện các biện pháp an ninh, an toàn kỹ thuật và quản trị nội bộ

Thế chế nội bộ: Ban hành quy chế phân quyền truy cập “Cần biết và tối thiểu”, bắt buộc xác thực 2 lớp đối với dữ liệu nhạy cảm và ghi vết nhật ký hệ thống (log-file) không thể xóa bỏ để phục vụ thanh tra.

Biện pháp kỹ thuật - công nghệ chủ động: Mã hóa dữ liệu ở cả hai trạng thái lưu trữ (At-rest) và di chuyển (In-transit); xác thực mạnh đa nhân tố (MFA); thiết lập giải pháp phát hiện và phản hồi thiết bị đầu cuối và phản hồi mở rộng (EDR/XDR) và vùng đệm an toàn tách biệt với mạng internet công cộng.

Kiểm soát hợp tác công - tư: Giữ quyền kiểm soát tối cao hệ thống, không khoán trắng quyền quản trị gốc cho nhà thầu tư nhân.

(4). Giải quyết mối quan hệ biện chứng giữa “Liên thông chia sẻ dữ liệu” và “Kiểm soát bảo mật an toàn”

Yêu cầu phát triển chính quyền số đòi hỏi dữ liệu phải được “mở” và lưu thông “thông suốt” nhằm xóa bỏ các “đảo dữ liệu”, thúc đẩy liên thông giữa các sở, ban, ngành và các cấp chính quyền. Dữ liệu càng được chia sẻ mạnh mẽ, dịch vụ công trực tuyến càng tối ưu. Ngược lại, yêu cầu bảo vệ quyền DLCN thông qua cơ chế kiểm

soát lại đòi hỏi sự thận trọng, thiết lập các rào cản kỹ thuật và pháp lý như: giới hạn mục đích khai thác, kiểm soát lịch sử truy cập và thắt chặt quyền hạn công chức.

Sự xung đột này dễ dẫn đến hai trạng thái cực đoan: (i) Quá thiên về chia sẻ, buông lỏng kiểm soát; dẫn đến nguy cơ rò rỉ dữ liệu diện rộng. (ii) Quá thiên về kiểm soát cứng nhắc; làm nảy sinh tâm lý sợ sai, sợ chịu trách nhiệm ở cơ quan hành chính, dẫn đến đình trệ việc chia sẻ dữ liệu.

Tuy nhiên, mối quan hệ giữa chia sẻ dữ liệu và kiểm soát bảo mật tuân theo quy luật thống nhất và đấu tranh của các mặt đối lập. Kiểm soát không phải là “lực cản” của chia sẻ, mà là điều kiện tiên quyết để xây dựng niềm tin số và tạo ra hành lang an toàn pháp lý - kỹ thuật (thông qua công cụ DPIA). Chính quyền số cấp tỉnh quản trị thông minh là chính quyền đạt được trạng thái cân bằng động, bảo đảm dữ liệu vừa được lưu chuyển mạnh mẽ phục vụ phát triển, vừa nằm trong tầm kiểm soát an toàn để bảo vệ tối đa quyền con người.

(5) Vận hành cơ chế kiểm soát, thanh tra, kiểm tra và nâng cao năng lực thực thi

Tuyên truyền và đào tạo: Chuyển đổi nhận thức của cán bộ công chức từ “quản lý hành chính thuần túy” sang “quản trị dữ liệu an toàn”; hướng dẫn người dân kỹ năng tự vệ pháp lý trên môi trường số.

Cơ chế kiểm soát đa tầng: Kết hợp 03 tuyến kiểm soát: (i) Kiểm soát nội bộ và giám sát thời gian thực qua log-file hệ thống; (ii) Thanh tra, kiểm tra chuyên ngành, xử lý kỷ luật công chức và phạt hành chính doanh nghiệp vi phạm; (iii) Giám sát xã hội của HĐND, Mặt trận Tổ quốc và kiểm toán an toàn dữ liệu độc lập từ bên thứ ba.

2.2.2. Phương thức bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh

Bảo vệ quyền đối với DLCN là quá trình Chính quyền số cấp tỉnh thực hiện nghĩa vụ quốc gia về quyền con người (Tôn trọng, bảo vệ và thực thi). Về mặt phương pháp luận, cách tiếp cận dựa trên quyền con người không tồn tại như một phương thức kỹ thuật đơn lẻ, mà đóng vai trò là nguyên tắc chỉ đạo và triết học pháp lý xuyên suốt, chi phối toàn bộ quá trình xây dựng chính sách, hoàn thiện pháp luật cũng như tổ chức thực thi pháp luật về dữ liệu.

Theo đó, mọi hoạt động quản trị dữ liệu của chính quyền cấp tỉnh đều lấy công dân làm trung tâm (Chủ thể mang quyền), đặt giới hạn cho quyền lực công (Chủ thể mang nghĩa vụ), và bảo đảm các nguyên tắc bình đẳng, không phân biệt đối xử, minh

bạch, trách nhiệm giải trình cùng sự tham gia của người dân. Trên nền tảng triết học pháp lý đó, nội dung bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh được hiện thực hóa thông qua 06 phương thức cụ thể sau:

2.2.2.1. Phương thức xây dựng chính sách, hoàn thiện pháp luật về bảo vệ quyền đối với dữ liệu cá nhân tại địa phương

Dưới khía cạnh khoa học pháp lý và quản trị công, pháp luật vừa là công cụ điều tiết quyền lực, vừa là bộ đỡ thể chế cho mọi hoạt động quản lý nhà nước. Trong tiến trình xây dựng chính quyền số cấp tỉnh, phương thức hoàn thiện pháp luật không đơn thuần là việc ban hành các quy định cấm đoán, mà là quá trình thiết lập hành lang thể chế, xác lập giới hạn quyền lực dữ liệu của khu vực công và bảo đảm quyền tự quyết thông tin của cá nhân. Liên hệ với nghĩa vụ quốc tế tại Điều 17 Công ước Quốc tế về các Quyền Dân sự và Chính trị (ICCPR), khuôn khổ pháp lý này phải đáp ứng các tiêu chí về tính hợp pháp, tính cần thiết và tính tương xứng đối với mọi hành vi can thiệp vào đời sống riêng tư. Về mặt lý luận, phương thức này cấu thành từ ba nội hàm cốt lõi sau:

Thứ nhất, địa phương hóa chuẩn mực pháp lý trung ương vào bối cảnh quản trị vùng: Các văn bản luật của trung ương mang tính nguyên tắc, phổ quát và áp dụng chung. Để các quy định này vận hành thực chất, lý luận pháp lý đòi hỏi phải cụ thể hóa các nguyên tắc bảo vệ quyền dữ liệu thành các quy chế, quy định của địa phương và thuộc thẩm quyền ban hành của chính quyền địa phương, phù hợp với năng lực hạ tầng và đặc thù quản lý hành chính của từng địa bàn cấp tỉnh.

Thứ hai, đồng bộ hóa quy trình kỹ thuật - công nghệ với quy phạm pháp lý: Áp dụng nguyên lý “Bảo vệ dữ liệu ngay từ khâu thiết kế pháp lý và hệ thống”. Quy trình hành chính số phải được chuẩn hóa về mặt pháp lý trước khi được mã hóa thành các lệnh công nghệ. Điều này đòi hỏi pháp lý hóa quy trình kiểm toán an toàn hệ thống, bắt buộc mọi nền tảng dịch vụ công trực tuyến trước khi đưa vào vận hành đều phải trải qua bước đánh giá tác động bảo vệ dữ liệu cá nhân (DPIA) để kiểm soát các biểu mẫu điện tử (e-Form) theo nguyên tắc tối thiểu hóa dữ liệu.

Thứ ba, xác lập thể chế trách nhiệm và chế tài phục hồi quyền năng: Khuôn khổ pháp lý địa phương phải định hình rõ đối tượng được bảo vệ thông qua việc phân loại dữ liệu (dữ liệu thông thường và dữ liệu nhạy cảm), luật hóa hệ thống nghĩa vụ giải trình của cơ quan công quyền khi hạn chế quyền của dân, đồng thời thiết lập cơ chế bồi thường thiệt hại (bao gồm cả thiệt hại vật chất và phi vật chất). Việc nội hóa

chi phí vi phạm vào chủ thể gây ra thiệt hại không chỉ mang tính trừng phạt, mà còn có chức năng phục hồi niềm tin của công dân vào tính trách nhiệm của chính quyền số.

2.2.2.2. Phương thức tổ chức bộ máy và xác lập cơ chế quản lý nội bộ về bảo vệ quyền dữ liệu cá nhân trong chính quyền số cấp tỉnh

Nếu pháp luật là hình thức thì bộ máy tổ chức và cơ chế vận hành là nội dung thực thi. Trong chính quyền số cấp tỉnh, dữ liệu cá nhân được hình thành, lưu chuyển và khai thác trong những chuỗi liên thông phức tạp, dễ dẫn đến nguy cơ phân tán trách nhiệm. Do đó, phương thức tổ chức bộ máy và quản trị nội bộ đóng vai trò là "hệ điều hành" đưa các nguyên tắc pháp lý vào thực tế công vụ thông qua ba trụ cột lý luận sau:

Thứ nhất, mô hình hóa vai trò chủ thể và phân định trách nhiệm pháp lý theo thực quyền: Để quyền đối với dữ liệu không rơi vào trạng thái vô chủ, lý luận quản trị hiện đại đòi hỏi phải phân định rõ ràng trách nhiệm dựa trên vai trò thực tế của chủ thể trong chuỗi xử lý dữ liệu. Mô hình này phân ra thành ba nhóm cấu phần:

(1). Bên kiểm soát dữ liệu (Cơ quan nhà nước cấp tỉnh): Chủ thể quyết định mục đích, căn cứ và phạm vi xử lý, chịu trách nhiệm giải trình cao nhất trước các tiêu chuẩn hợp hiến về quyền con người.

(2). Bên xử lý dữ liệu (Doanh nghiệp công nghệ, đơn vị phát triển nền tảng được ủy quyền hoặc thuê): Chủ thể trực tiếp thao tác kỹ thuật, chịu trách nhiệm độc lập về an toàn bảo mật trong phạm vi được ủy quyền, ngăn ngừa hiện tượng “tư nhân hóa rủi ro quyền con người” trong khu vực công.

(3). Người thực thi trực tiếp (Cán bộ, công chức): Đối tượng trực tiếp tiếp xúc với dữ liệu công dân trong quá trình tác nghiệp hành chính.

Thứ hai, xác lập cấu trúc chuyên trách và cá thể hóa trách nhiệm hành chính: Phương thức này đòi hỏi phải xóa bỏ trạng thái “trách nhiệm chung chung” bằng cách định hình các vị trí chuyên trách bảo vệ dữ liệu hoặc bộ phận đầu mối an ninh thông tin trong từng cơ quan chuyên môn cấp tỉnh. Đồng thời, trách nhiệm bảo vệ dữ liệu phải gắn chặt với trách nhiệm của người đứng đầu cơ quan công quyền, được thiết kế thành một tiêu chí cứng trong đánh giá hiệu quả thực thi công vụ (KPI).

Thứ ba, quy trình hóa quyền hạn tối thiểu và lưu vết công vụ khép kín: Về mặt nội bộ, cơ chế này vận dụng nguyên tắc “Quyền hạn tối thiểu”, nghiêm ngặt phân quyền tiếp cận dữ liệu dựa trên chức năng nhiệm vụ (cán bộ tiếp nhận hồ sơ, cán bộ xử lý chuyên môn và cán bộ quản trị hệ thống có quyền hạn khác nhau). Quy trình quản trị nội

bộ phải kiểm soát toàn bộ vòng đời của dữ liệu: từ phiếu đồng ý đầu vào, mã hóa lưu trữ, biên bản điện tử khi chia sẻ, cho đến tự động ẩn danh hóa/tiêu hủy khi hết thời hạn nghiệp vụ... Để ngăn ngừa rủi ro từ nhân sự bên trong, hệ thống phải tự động ghi lại lịch sử thao tác không thể tẩy xóa (lưu vết công vụ), chuyển các rủi ro hành vi thành chứng cứ pháp lý rõ ràng, sẵn sàng phục vụ hoạt động hậu kiểm và kỷ luật hành chính.

Tóm lại, tổ chức bộ máy và cơ chế quản lý nội bộ chính là hệ điều hành đưa các quy định pháp luật về bảo vệ dữ liệu vào thực tế công vụ. Một chính quyền số cấp tỉnh chỉ có thể an toàn khi từng mắt xích cấu thành nó, tức là từng cơ quan, từng cán bộ - hoạt động trong một cơ chế quản trị nội bộ chặt chẽ, kỷ cương và minh bạch. Đây chính là giải pháp gốc rễ để phòng ngừa từ sớm, từ xa các nguy cơ xâm phạm quyền dữ liệu cá nhân của công dân.

2.2.2.3. Phương thức sử dụng biện pháp hạ tầng kỹ thuật, công nghệ và quản trị dữ liệu hiện đại

Lý luận bảo vệ quyền con người trên không gian số đòi hỏi hiện thực hóa nguyên lý “Bảo vệ dữ liệu bằng biện pháp công nghệ”, biến hạ tầng kỹ thuật thành lớp bảo vệ cuối cùng. Phương thức này được cấu thành từ bốn trụ cột kỹ thuật nền tảng:

Thứ nhất, mã hóa dữ liệu đa trạng thái dưới nguyên lý cô lập rủi ro: Áp dụng mã hóa đồng bộ trên cả hai trạng thái: Data-at-rest (mã hóa kho dữ liệu nhạy cảm lưu trữ) và Data-in-transit (mã hóa đường truyền trên toàn bộ các trục liên thông, chia sẻ dữ liệu).

Thứ hai, cơ chế kiểm soát truy cập dựa trên nguyên tắc “Quyền hạn tối thiểu” và triết lý Zero Trust: Ngăn chặn sự can thiệp trái phép bằng cách thiết lập xác thực mạnh (MFA) và phân quyền sâu đến từng trường dữ liệu độc lập (RBAC/ABAC). Địa vị công vụ của một cán bộ không đồng nghĩa với quyền tiếp cận vô hạn đối với dữ liệu của công dân.

Thứ ba, công nghệ giám sát và ghi vết tự động tạo lập chứng cứ bất biến: Hệ thống tự động ghi nhận, tạo các tệp nhật ký hệ thống (System Logs) bảo mật cao (hướng tới ứng dụng Blockchain) ghi lại mọi hành vi đọc, ghi, sửa, xóa dữ liệu. Đây là cơ sở pháp lý tối thượng làm chứng cứ cho công tác hậu kiểm, giải trình và tố tụng.

Thứ tư, kỹ thuật ẩn danh hóa trong quản trị vòng đời dữ liệu thông minh: Sử dụng kỹ thuật ẩn danh hóa và làm mờ (Data Masking) để tự động bóc tách, loại bỏ

các trường thông tin định danh trực tiếp khi chuyển dịch dữ liệu từ mục đích quản lý hành chính sang mục đích thống kê, dự báo hoặc nghiên cứu.

Bảng: So sánh giữa giải pháp kỹ thuật số với quyền con người, nghĩa vụ công vụ và cơ chế hỗ trợ pháp lý

Giải pháp kỹ thuật (Hạ tầng số) PNG	Quyền cụ thể của Chủ thể dữ liệu được bảo vệ PNG	Nghĩa vụ pháp lý tương ứng của Chính quyền cấp tỉnh PNG	Cơ chế khắc phục/trợ giúp pháp lý khi quyền bị vi phạm PNG
Mã hóa dữ liệu (<i>At-rest, In-transit</i>)	Quyền bí mật đời tư, quyền riêng tư; Quyền được bảo đảm an toàn, bảo mật dữ liệu.	Nghĩa vụ bảo vệ dữ liệu theo tiêu chuẩn kỹ thuật bắt buộc; Chống truy cập trái phép.	Cơ chế bồi thường thiệt hại dân sự, nhà nước khi lộ lọt dữ liệu; Buộc khôi phục trạng thái an toàn.
Ghi nhật ký hệ thống (<i>Audit Logging</i>)	Quyền được biết, thông báo; Quyền truy cập lịch sử xử lý dữ liệu.	Nghĩa vụ minh bạch hóa quá trình xử lý công vụ; Nghĩa vụ lưu vết để kiểm toán công vụ.	Cung cấp bằng chứng kỹ thuật (log file) cho công dân phục vụ khiếu nại, tố tụng; Xử lý kỷ luật, hình sự cán bộ vi phạm.
Phân quyền truy cập (<i>RBAC/ABAC</i>) & Bảo mật API	Quyền hạn chế xử lý dữ liệu; Quyền chống lạm dụng dữ liệu vượt mục đích (<i>Function creep</i>).	Nghĩa vụ giới hạn truy cập theo đúng thẩm quyền công vụ và mục đích thu thập.	Hủy bỏ các quyết định hành chính dựa trên dữ liệu thu thập trái thẩm quyền; Áp dụng chế tài hành chính, hình sự.
Giao diện tương tác quyền (<i>Dashboard/Rút đồng ý, Xóa</i>)	Quyền rút lại sự đồng ý; Quyền chỉnh sửa, cập nhật; Quyền	Nghĩa vụ cung cấp công cụ kỹ thuật khả thi;	Khiếu nại hành chính hoặc khởi kiện vụ án hành chính nếu hệ

Giải pháp kỹ thuật (Hạ tầng số) PNG	Quyền cụ thể của Chủ thể dữ liệu được bảo vệ PNG	Nghĩa vụ pháp lý tương ứng của Chính quyền cấp tỉnh PNG	Cơ chế khắc phục/trợ giúp pháp lý khi quyền bị vi phạm PNG
	xóa, được lãng quên.	Nghĩa vụ phản hồi trong thời hạn luật định.	thông không cho phép thực hiện quyền hoặc chính quyền chậm trễ.
Giám sát SOC & Cảnh báo sự cố khẩn cấp	Quyền được thông báo về rủi ro, vi phạm dữ liệu; Quyền được bảo vệ an toàn nhân thân, tài sản.	Nghĩa vụ chủ động phát hiện, ứng phó và thông báo công khai, trực tiếp sự cố cho công dân.	Phong tỏa khẩn cấp tài khoản; Bồi thường thiệt hại do chậm trễ thông báo sự cố.

2.2.2.4. Phương thức thực hiện cơ chế thanh tra, kiểm tra, xử lý vi phạm và bồi thường thiệt hại

Phương thức hậu kiểm này đóng vai trò là chốt chặn công lý cuối cùng, duy trì kỷ cương hành chính và củng cố niềm tin số của xã hội. Về mặt lý luận, phương thức này vận hành dựa trên 03 cơ chế:

Thứ nhất, cơ chế thanh tra, kiểm tra công vụ dựa trên nguyên tắc trách nhiệm giải trình bắt buộc: Chuyển dịch từ tư duy “tìm lỗi sau sự cố” sang mô hình giám sát dựa trên rủi ro. Trọng tâm là đánh giá hệ thống cảnh báo sớm, thẩm định tính toàn vẹn của nhật ký hệ thống và kiểm tra mức độ tuân thủ các nguyên tắc tối thiểu hóa dữ liệu.

Thứ hai, hệ thống chế tài phân lớp mang tính răn đe: (1) Chế tài kỷ luật công vụ: Cá thể hóa trách nhiệm, xử lý nghiêm cán bộ, công chức lợi dụng thẩm quyền tra cứu thông tin trái mục đích. (2) Chế tài hành chính, kinh tế: Áp dụng phạt tiền kịch khung, đình chỉ tư cách tham gia hoặc chấm dứt hợp đồng ủy quyền xử lý dữ liệu đối với các doanh nghiệp công nghệ để xảy ra lỗ hổng bảo mật gây rò rỉ dữ liệu.

Thứ ba, hoàn thiện cơ chế bồi thường thiệt hại toàn diện và khôi phục trạng thái quyền năng: Mở rộng khái niệm thiệt hại bao gồm tổn thất vật chất và thiệt hại phi vật chất (tổn thương tinh thần, xáo trộn đời sống riêng tư). Kết hợp đền bù tài chính và biện pháp phi tài chính (công khai xin lỗi, hỗ trợ ẩn danh hóa lại thông tin).

Điểm mấu chốt lý luận là đảo ngược gánh nặng chứng minh. Khi xảy ra sự cố, công dân không có nghĩa vụ chứng minh sai phạm của chính quyền; ngược lại, cơ quan nhà nước và đơn vị vận hành phải có trách nhiệm giải trình và chứng minh mình đã thực hiện tối đa các biện pháp bảo vệ theo tiêu chuẩn pháp lý - kỹ thuật. Nếu không chứng minh được, chính quyền phải chịu trách nhiệm pháp lý và bồi thường thỏa đáng.

2.2.2.5. Phương thức truyền thông và giáo dục nhằm nâng cao nhận thức, năng lực số của xã hội về bảo vệ dữ liệu cá nhân

Ngay cả khi khuôn khổ pháp lý và hạ tầng công nghệ hoàn thiện, quyền con người vẫn có nguy cơ rơi vào trạng thái “vô hiệu” nếu chủ thể quyền không có tri thức về quyền hoặc thiếu kỹ năng tự vệ. Phương thức truyền thông, giáo dục là phương thức bảo vệ chủ động thông qua hai cấu phần:

Thứ nhất, tạo lập năng lực số và cơ chế tự bảo vệ của chủ thể dữ liệu (Công dân): Minh bạch hóa các quyền cốt lõi và kênh thực thi quyền trên môi trường số; quy trình hóa hành vi phản hồi khi quyền bị xâm phạm; trang bị kỹ năng nhận diện rủi ro, phòng chống lừa đảo định danh và tối thiểu hóa lỗ hổng an ninh từ hành vi người dùng.

Thứ hai, định hình văn hóa tuân thủ và đạo đức nghề nghiệp dữ liệu trong khu vực công: Đào tạo đội ngũ cán bộ, công chức toàn diện ở cả hai khía cạnh: Năng lực pháp lý (hiểu rõ ranh giới quyền lực dữ liệu, nghĩa vụ giải trình) và năng lực kỹ thuật - nghiệp vụ (thành thực quy trình thao tác chuẩn SOP về lưu vết công vụ, cô lập dữ liệu nhạy cảm).

2.2.2.6. Phương thức hợp tác quốc tế và chia sẻ thông tin có kiểm soát

Không một thực thể quản trị địa phương nào có thể tự thiết lập một cơ chế bảo hộ an toàn tuyệt đối nếu lựa chọn mô hình khép kín. Phương thức này giúp đạt trạng thái cân bằng giữa khai thác giá trị phát triển và bảo đảm an toàn dữ liệu thông qua 03 nội hàm:

Thứ nhất, nội hóa các chuẩn mực pháp lý và công nghệ phổ quát toàn cầu: Tiếp thu, tích hợp các khuôn khổ pháp lý tiên bộ (như GDPR) và tiêu chuẩn an ninh

thông tin quốc tế vào thực tiễn quản trị địa phương; chủ động tiếp nhận chuyển giao công nghệ mã hóa, ẩn danh hóa dữ liệu và chuẩn hóa năng lực cán bộ DPO.

Thứ hai, thiết lập cơ chế kiểm soát pháp lý và phân quyền trong cơ chế chia sẻ dữ liệu: (1) Kiểm soát nội bộ khu vực công: Tích hợp dữ liệu giữa các sở, ngành dựa trên nguyên tắc phân quyền tối thiểu, tự động lưu vết (Log) và minh bạch hóa mục đích công vụ. (2) Kiểm soát đối tác khu vực tư (PPP): Giới hạn quyền xử lý dữ liệu của doanh nghiệp trong phạm vi ủy quyền hành chính, cấm tuyệt đối hành vi lưu trữ thứ cấp hoặc thương mại hóa DLCN của công dân.

Thứ ba, cơ chế phối hợp đa tầng và phản ứng nhanh trước rủi ro an ninh phi biên giới: Thiết lập mạng lưới phối hợp liên địa phương, liên ngành và kết nối với các cơ quan an ninh mạng chuyên trách cấp vĩ mô nhằm phát hiện sớm, cảnh báo nhanh các lỗ hổng hệ thống và ngăn chặn hành vi rao bán, phát tán DLCN trái phép trên không gian mạng.

Tóm lại, phương thức “Hợp tác quốc tế và chia sẻ thông tin có kiểm soát” phản ánh tư duy quản trị mạng hiện đại: Không đóng cửa để an toàn, không mở toang để phát triển. Một chính quyền số cấp tỉnh thông minh là một chính quyền biết mở rộng biên độ hợp tác để tận dụng tri thức, công nghệ thế giới, đồng thời thiết lập được các cơ chế pháp lý và kỹ thuật để kiểm soát chặt chẽ từng hoạt động chia sẻ thông tin. Đây là cách thức giúp địa phương vừa tối ưu hóa được giá trị kinh tế - xã hội của dữ liệu, vừa bảo vệ vững chắc quyền tự do cá nhân và chủ quyền an ninh mạng của quốc gia từ cấp cơ sở.

2.2.3. Các yếu tố tác động đối với bảo vệ quyền dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh

Dưới góc độ khoa học pháp lý về quyền con người và quản trị công, bảo vệ quyền đối với DLCN không tồn tại trong một môi trường khép kín thuần túy quy phạm, mà chịu sự chi phối, tác động đa chiều của các yếu tố cơ sở chính trị, điều kiện kinh tế - xã hội, năng lực quản trị hành chính, hạ tầng công nghệ và nhận thức của chủ thể dữ liệu. Việc nhận diện đúng các yếu tố tác động này đóng vai trò là khung lý thuyết quan trọng để đánh giá khách quan thực trạng tại Chương 3 và xác định các giải pháp đột phá tại Chương 4.

2.2.3.1. Bảo vệ quyền đối với dữ liệu cá nhân phải được đặt trong khuôn khổ sự lãnh đạo của Đảng và định hướng Nhà nước pháp quyền xã hội chủ nghĩa

Quan điểm, đường lối của Đảng Cộng sản Việt Nam là cơ sở chính trị - lý luận cốt lõi định hướng cho sự chuyển dịch tư duy quản trị trong xây dựng chính quyền số cấp tỉnh: chuyển từ cách tiếp cận quản lý hành chính thuần túy sang mô hình quản trị lấy con người làm trung tâm. Theo đó, bảo vệ dữ liệu cá nhân không đơn thuần là giải pháp kỹ thuật an toàn thông tin của các cơ quan chuyên trách công nghệ, mà là một nhiệm vụ quản trị công mang tính hệ thống nhằm thực thi nghĩa vụ Hiến định về bảo vệ quyền con người, quyền riêng tư của công dân.

Định hướng chiến lược về con người và chuyển đổi số của Đảng là xuyên suốt. Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII và Chiến lược phát triển kinh tế - xã hội 10 năm 2021 - 2030 đã khẳng định nguyên tắc “phát huy tối đa nhân tố con người, coi con người là trung tâm, chủ thể... và mục tiêu của sự phát triển”. Bước sang giai đoạn phát triển mới, Văn kiện Đại hội XIV của Đảng tiếp tục nhấn mạnh yêu cầu “lấy khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số làm động lực chính”, đồng thời đặt vấn đề bảo đảm quyền con người trong tư tưởng chỉ đạo “Dân là gốc”, xác định nhân dân là trung tâm của công cuộc đổi mới và phát triển đất nước [25].

Về phương diện thể chế và hạ tầng số, Nghị quyết số 57-NQ/TW, ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia đã xác định rõ yêu cầu phát triển hạ tầng số trên nguyên tắc “hiện đại, đồng bộ, an ninh, an toàn, hiệu quả”, nhằm khai thác tối đa tiềm năng của dữ liệu như một tư liệu sản xuất chính [4]. Đặc biệt, định hướng đột phá thể chế đã được Tổng Bí thư Tô Lâm nhấn mạnh (tháng 5/2025): hệ thống pháp luật phải công nhận, tôn trọng, bảo vệ hiệu quả quyền con người, quyền công dân; dứt khoát từ bỏ tư duy “không quản được thì cấm”, tạo lập hành lang pháp lý phù hợp với thực tiễn nhằm bảo đảm quyền con người, quyền công dân.

Nhằm bảo đảm cho quá trình chuyển đổi số không chệch hướng, Nghị quyết số 66-NQ/TW, ngày 30/4/2025 của Bộ Chính trị về hoàn thiện thể chế pháp luật đã đặt ra yêu cầu “tăng cường kiểm soát quyền lực; phòng, chống tham nhũng... lợi ích nhóm...; phòng ngừa, ngăn chặn... trục lợi, hướng lái chính sách”, gắn liền với việc duy trì sự lãnh đạo toàn diện của Đảng [5]. Đây là căn cứ chính trị quan trọng để chính quyền cấp tỉnh thiết lập cơ chế quản trị dữ liệu cá nhân theo hướng hài hòa giữa thúc đẩy đổi mới sáng tạo với kiểm soát rủi ro, vừa ngăn ngừa nguy cơ lạm dụng quyền lực công, xâm phạm đời tư của người dân trên không gian số.

Mặc dù đường lối của Đảng đã tạo ra cơ sở chính trị vững chắc, thực tiễn thi hành cho thấy việc chuyển hóa các quan điểm này thành cơ chế bảo vệ quyền đối với dữ liệu cá nhân theo các chuẩn mực quốc tế, Hiến pháp và Luật Bảo vệ dữ liệu cá nhân vẫn đối mặt với không ít “điểm nghẽn” pháp lý và thể chế cần tiếp tục được nhận diện và tháo gỡ.

2.2.3.2. Đặc điểm quản trị hành chính công và năng lực chuyển hoá chính sách (quy chế) của bộ máy của chính quyền cấp tỉnh

Khác với quy phạm pháp luật quốc gia mang tính công cụ bảo vệ, năng lực quản trị hành chính và kỹ năng cụ thể hóa chính sách của bộ máy chính quyền cấp tỉnh là yếu tố thực tiễn tác động trực tiếp đến hiệu lực bảo vệ quyền trên địa bàn.

(1). Độ trễ hành chính và năng lực ban hành văn bản thi hành: Cấp tỉnh không có thẩm quyền lập pháp nhưng có thẩm quyền ban hành VBQPPL (Nghị quyết HĐND, Quyết định UBND) và các quy chế vận hành nội bộ. Sự chủ động, nhạy bén của chính quyền cấp tỉnh trong việc ban hành Quy chế chia sẻ dữ liệu, Quy trình đánh giá tác động bảo vệ DLCN (DPIA) đối với các phần mềm dịch vụ công sẽ quyết định việc quyền dữ liệu được bảo vệ thực chất hay chỉ dừng lại ở nguyên tắc chung của trung ương.

(2). Tâm lý công vụ và sự phân định ranh giới trách nhiệm: Trạng thái quản trị hành chính tại địa phương (ngần ngại, sợ trách nhiệm, sợ sai hoặc ngược lại là buông lỏng kiểm soát) tác động trực tiếp đến hoạt động chia sẻ dữ liệu. Một môi trường quản trị công minh bạch, phân định rõ ranh giới giữa “lỗi kỹ thuật” và “vi phạm hành vi công vụ” sẽ giải phóng tâm lý e ngại của cán bộ, thúc đẩy chia sẻ dữ liệu an toàn.

(3). Sự tương thích và tiệm cận với các chuẩn mực quản trị quốc tế (như GDPR): Mức độ chủ động của chính quyền cấp tỉnh trong việc tiếp thu các nguyên tắc quản trị tiên tiến (tối thiểu hóa dữ liệu, giới hạn mục đích, minh bạch hóa) tác động trực tiếp đến năng lực thu hút dòng vốn đầu tư nước ngoài (FDI), phát triển kinh tế số và thiết lập môi trường số an toàn cho công dân địa phương.

2.2.3.3. Mức độ phát triển của hạ tầng công nghệ và các giải pháp an ninh dữ liệu

DLCN trong chính quyền số không tồn tại dưới dạng hồ sơ giấy mà vận hành dưới dạng dữ liệu điện tử. Do đó, hạ tầng kỹ thuật là điều kiện vật chất quyết định khả năng chuyển hóa các quy phạm pháp luật thành các lệnh bảo vệ tự động.

(1). Tính đồng bộ và chuẩn hóa của hạ tầng số địa phương: Nếu hạ tầng CNTT của tỉnh bị chắp vá, manh mún, thiếu chuẩn tích hợp giữa các sở, ngành (ví dụ: phần mềm của Sở Tư pháp không đồng bộ chuẩn bảo mật với Sở Nội vụ), các lỗ hổng tại điểm kết nối sẽ xuất hiện, gia tăng nguy cơ bị tấn công mạng và rò rỉ dữ liệu điện rộng.

(2). Sự hiện diện của các giải pháp kỹ thuật bảo vệ cốt lõi: Khả năng bảo vệ quyền phụ thuộc vào việc hệ thống của tỉnh có được trang bị đồng bộ các giải pháp: mã hóa dữ liệu (At-rest/In-transit), kiểm soát truy cập phân quyền sâu (RBAC/ABAC), mô hình Zero Trust, công nghệ lưu vết tự động (Audit Log) và hệ thống giám sát an ninh mạng (SOC) hay không.

(3). Thách thức từ các công nghệ mới (AI, Big Data): Việc đưa trí tuệ nhân tạo và hệ thống phân tích dữ liệu tự động vào vận hành các Trung tâm Điều hành thông minh (IOC) đòi hỏi giải pháp kỹ thuật phải kiểm soát được nguy cơ định danh trái phép, phân biệt đối xử hoặc quyết định tự động gây bất lợi cho công dân.

2.2.3.4. Trình độ chuyên môn, năng lực số và đạo đức công vụ của đội ngũ cán bộ, công chức

Con người vừa là chủ thể vận hành hệ thống, vừa là yếu tố tiềm ẩn rủi ro lớn nhất đối với an toàn dữ liệu (thống kê cho thấy hơn 80% sự cố bảo mật thông tin xuất phát từ yếu tố con người). [63]

(1). Năng lực số và kỹ năng an toàn thông tin: Cán bộ, công chức (đặc biệt là lực lượng tiếp nhận hồ sơ tại bộ phận Một cửa cấp xã, phường) là những người trực tiếp thu thập, xử lý DLCN. Thiếu trình độ, kỹ năng an toàn thông tin (mật khẩu yếu, dùng tài khoản chung, cài đặt phần mềm lạ) sẽ vô tình tạo ra lỗ hổng cho tội phạm mạng xâm nhập.

(2). Đạo đức công vụ và tính kỷ luật hành chính: Trước áp lực và sức hút tài chính từ “thị trường dữ liệu đen”, nhận thức pháp lý, bản lĩnh chính trị và đạo đức công vụ của cán bộ quyết định việc ngăn chặn các hành vi chủ động trích xuất, sao chép hoặc mua bán thông tin công dân để trục lợi cá nhân.

(3). Văn hóa công sở và ý thức trách nhiệm giải trình: Sự chuyển biến về tư duy của cán bộ từ “người quản lý ban phát” sang “người phục vụ, có nghĩa vụ bảo vệ tài sản số của dân” là nhân tố quyết định tính thực chất của các quy trình bảo vệ dữ liệu.

2.2.3.5. Nguồn lực tài chính và đầu tư công cho an toàn thông tin

Bảo vệ dữ liệu là hoạt động kỹ thuật - pháp lý phức tạp, diễn ra liên tục và đòi hỏi nguồn lực tài chính rất lớn. Mọi chính sách hay quy chế quản trị đều trở nên vô hiệu nếu thiếu nguồn kinh phí tương ứng để thực thi.

(1). Tỷ lệ chi ngân sách cho an toàn thông tin: Thực tiễn phân bổ ngân sách CNTT tại các địa phương thường bị mất cân đối (tập trung mua sắm phần cứng, phần mềm, trong khi tỷ lệ chi cho an toàn thông tin và bảo vệ dữ liệu ở mức rất thấp so với chuẩn khuyến nghị 10 - 15%) [13].

(2). Khả năng duy trì và nâng cấp hệ thống: Hạn chế về nguồn kinh phí đầu tư công ảnh hưởng trực tiếp đến năng lực bảo trì hạ tầng, thuê dịch vụ kiểm thử bảo mật độc lập, diễn tập ứng cứu sự cố và tổ chức các khóa đào tạo chuyên sâu định kỳ cho lực lượng chuyên trách của tỉnh.

2.2.3.6. Nhận thức pháp lý, năng lực số của công dân và cơ chế giám sát, phản biện xã hội

Sự tham gia của công dân và xã hội là yếu tố tác động từ bên ngoài, tạo ra áp lực kiểm soát đối với bộ máy chính quyền trong việc tuân thủ các nghĩa vụ bảo vệ dữ liệu.

(1). Nhận thức pháp lý và năng lực tự vệ số của chủ thể dữ liệu (Công dân): Khi công dân có nhận thức cao về các quyền dữ liệu (được biết, truy cập, đính chính, xóa, rút lại sự đồng ý), họ sẽ chủ động thực thi quyền, đòi hỏi chính quyền phải giải trình và thận trọng khi xử lý dữ liệu. Ngược lại, nếu “năng lực số” của dân còn thấp (đặc biệt tại vùng sâu, vùng xa), quyền dữ liệu dễ rơi vào trạng thái bị hình thức hóa.

(2). Kênh thực thi và chi phí tuân thủ quyền: Sự tác động của công dân phụ thuộc vào việc chính quyền cấp tỉnh có thiết lập các công cụ thuận tiện (Dashboard cá nhân, Tổng đài 1022, biểu mẫu điện tử) để người dân dễ dàng phản ánh, khiếu nại hay yêu cầu rút lại sự đồng ý hay không.

(3). Sự giám sát của các cơ quan dân cử, truyền thông và doanh nghiệp đối tác: Hoạt động giám sát của HĐND các cấp, Mặt trận Tổ quốc, báo chí và tính tuân thủ pháp lý của các doanh nghiệp công nghệ (bên xử lý dữ liệu được ủy quyền trong dự án PPP) tạo thành cơ chế kiểm soát đa chiều, buộc chính quyền số cấp tỉnh phải duy trì kỷ cương và minh bạch trong quản trị dữ liệu cá nhân.

2.3. PHÁP LUẬT QUỐC TẾ VÀ KINH NGHIỆM CỦA MỘT SỐ NƯỚC VỀ BẢO VỆ QUYỀN ĐỐI VỚI DỮ LIỆU CÁ NHÂN TRONG XÂY DỰNG CHÍNH QUYỀN SỐ

2.3.1. Pháp luật quốc tế về bảo vệ quyền đối với dữ liệu cá nhân

Trong pháp luật quốc tế về QCN, bảo vệ quyền đối với DLCN được hình thành và phát triển trên nền tảng của quyền về sự riêng tư, vốn được thừa nhận như một quyền cơ bản và có giá trị phổ quát. Tuyên ngôn Nhân quyền phổ quát năm 1948 (UDHR) khẳng định nguyên tắc cốt lõi rằng: *“Không ai bị can thiệp một cách tùy tiện vào đời sống riêng tư, gia đình, chỗ ở hoặc thư tín của mình, cũng như không bị xâm phạm đến danh dự và uy tín. Mọi người đều có quyền được pháp luật bảo vệ chống lại những sự can thiệp hoặc xâm phạm như vậy.”* (Điều 12). Trên cơ sở đó, Công ước quốc tế về các quyền dân sự và chính trị năm 1966 (ICCPR) tiếp tục cụ thể hóa và nâng chuẩn nghĩa vụ của Nhà nước bằng việc nhấn mạnh: *“Không ai bị can thiệp một cách tùy tiện hoặc trái pháp luật vào đời sống riêng tư, gia đình, chỗ ở hoặc thư tín của mình, cũng như không bị xâm phạm trái pháp luật đến danh dự và uy tín”* (Điều 17(1)), đồng thời ghi nhận rõ *“Mọi người đều có quyền được pháp luật bảo vệ chống lại những sự can thiệp hoặc xâm phạm như vậy”* (Điều 17(2)) [109].

Trong bối cảnh xã hội số, khi thông tin cá nhân được thu thập, lưu trữ và phân tích trên quy mô lớn, nội hàm của quyền riêng tư ngày càng được diễn giải theo hướng bao hàm quyền kiểm soát thông tin và dữ liệu liên quan đến cá nhân. Cách tiếp cận này cho thấy quyền đối với DLCN không phải là một quyền tách rời khỏi quyền riêng tư, mà là sự phát triển tất yếu của quyền riêng tư trong môi trường số, nhằm bảo đảm cá nhân không bị đặt vào tình trạng bị giám sát, bị định danh, hoặc bị sử dụng dữ liệu vượt quá mục đích một cách không minh bạch. Đặc biệt, cơ quan giám sát thực thi ICCPR là Ủy ban Nhân quyền (Human Rights Committee) đã nhấn mạnh tính chất nghĩa vụ bảo đảm của Nhà nước đối với quyền riêng tư: *“Quyền được bảo vệ khỏi sự can thiệp vào đời sống riêng tư phải được bảo đảm trước các hành vi can thiệp và xâm phạm, dù những hành vi đó xuất phát từ các cơ quan nhà nước hay từ các cá nhân hoặc pháp nhân”* (Bình luận chung số 16 về Điều 17). Từ đó, có thể khái quát rằng pháp luật quốc tế về QCN đặt ra nghĩa vụ tích cực cho Nhà nước trong việc thiết lập khuôn khổ pháp lý, cơ chế tổ chức và biện pháp kỹ thuật để phòng ngừa lạm dụng DLCN, đặc biệt trong điều kiện Nhà nước ngày càng giữ vai trò trung tâm trong thu thập và xử lý dữ liệu thông qua các mô hình chính quyền điện tử và chính quyền số [109].

Song song với các văn kiện quốc tế chung về QCN, pháp luật quốc tế đã từng bước hình thành các chuẩn mực chuyên biệt về bảo vệ DLCN, nhằm điều chỉnh trực

tiếp hoạt động thu thập, lưu trữ và xử lý dữ liệu trong bối cảnh CNTT và truyền thông phát triển mạnh mẽ. Tiêu biểu trong số đó là Công ước năm 1981 của Hội đồng châu Âu về bảo vệ cá nhân liên quan đến việc xử lý tự động DLCN (*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*) - Công ước 108 và Hướng dẫn của Tổ chức Hợp tác và Phát triển Kinh tế (OECD) về bảo vệ quyền riêng tư và luồng DLCN xuyên biên giới. Đây là những văn kiện đầu tiên đặt nền móng cho việc tiếp cận DLCN như một đối tượng cần được bảo vệ bằng các nguyên tắc pháp lý riêng biệt, vượt ra ngoài khuôn khổ bảo vệ đời sống riêng tư theo nghĩa truyền thống. Công ước 108 khẳng định nghĩa vụ của các quốc gia thành viên trong việc bảo đảm rằng DLCN phải được “*thu thập và xử lý một cách công bằng và hợp pháp*”, “*được lưu trữ cho những mục đích cụ thể và hợp pháp, và không được sử dụng theo cách không phù hợp với các mục đích đó*”, đồng thời “*phải đầy đủ, thích hợp và không vượt quá những mục đích mà vì đó dữ liệu được lưu trữ*”. Công ước cũng yêu cầu DLCN phải “*chính xác và, khi cần thiết, được cập nhật*”, cũng như “*được lưu giữ dưới hình thức cho phép nhận dạng chủ thể dữ liệu không lâu hơn thời gian cần thiết cho mục đích lưu trữ*” [79]. Những quy định này phản ánh cách tiếp cận sớm nhưng toàn diện đối với vòng đời xử lý DLCN, đặc biệt nhấn mạnh trách nhiệm của chủ thể xử lý dữ liệu trong việc hạn chế quyền lực đối với thông tin cá nhân.

Tương tự, Hướng dẫn của Tổ chức Hợp tác và Phát triển Kinh tế (OECD) đã hệ thống hóa tám nguyên tắc cơ bản làm nền tảng cho nhiều đạo luật bảo vệ dữ liệu trên thế giới, bao gồm: nguyên tắc giới hạn thu thập; nguyên tắc chất lượng dữ liệu; nguyên tắc xác định mục đích; nguyên tắc giới hạn sử dụng; nguyên tắc biện pháp bảo mật; nguyên tắc công khai; nguyên tắc tham gia của cá nhân; và nguyên tắc trách nhiệm giải trình. Đáng chú ý, Hướng dẫn của Tổ chức Hợp tác và Phát triển Kinh tế (OECD) nhấn mạnh quyền của cá nhân được “*biết về sự tồn tại của dữ liệu liên quan đến mình, có quyền truy cập và yêu cầu chỉnh sửa dữ liệu đó*” [96], qua đó đặt cá nhân vào vị trí chủ thể trung tâm trong cơ chế bảo vệ dữ liệu.

Các chuẩn mực quốc tế chuyên biệt nêu trên có ý nghĩa đặc biệt quan trọng đối với khu vực công, nơi Nhà nước vừa là chủ thể ban hành pháp luật, vừa là chủ thể trực tiếp thu thập và xử lý khối lượng lớn DLCN phục vụ quản lý nhà nước và cung cấp dịch vụ công. Trong bối cảnh này, các nguyên tắc về mục đích xử lý, tối thiểu hóa dữ liệu, bảo mật và quyền kiểm soát của chủ thể dữ liệu đóng vai trò như

những giới hạn pháp lý cần thiết đối với quyền lực dữ liệu của Nhà nước, qua đó góp phần bảo đảm rằng việc ứng dụng công nghệ trong quản trị công không làm suy giảm QCN, mà trái lại, phải được đặt trong khuôn khổ tôn trọng và bảo vệ quyền đối với DLCN.

Một nội dung quan trọng khác của pháp luật quốc tế về bảo vệ quyền đối với DLCN, có liên hệ trực tiếp đến quá trình xây dựng và vận hành chính quyền số, là vấn đề chuyển giao dữ liệu xuyên biên giới và hợp tác quốc tế. Trong bối cảnh chính quyền số ngày càng phụ thuộc vào hạ tầng công nghệ hiện đại, điện toán đám mây, nền tảng số và các giải pháp kỹ thuật do doanh nghiệp công nghệ xuyên quốc gia cung cấp, DLCN của công dân có khả năng được lưu trữ, truy cập hoặc xử lý ngoài lãnh thổ quốc gia nơi dữ liệu được thu thập. Thực tiễn này làm gia tăng nguy cơ suy giảm mức độ bảo vệ quyền đối với DLCN nếu việc chuyển giao không được kiểm soát chặt chẽ.

Trước yêu cầu đó, pháp luật quốc tế hiện đại tiếp cận chuyển giao dữ liệu xuyên biên giới theo hướng không phủ nhận việc lưu chuyển dữ liệu, nhưng đặt ra các điều kiện nhằm bảo đảm rằng việc chuyển giao không làm suy giảm mức độ bảo vệ quyền của chủ thể dữ liệu. Nguyên tắc cốt lõi được hình thành là: DLCN chỉ được chuyển ra ngoài phạm vi lãnh thổ khi quốc gia, tổ chức hoặc chủ thể tiếp nhận bảo đảm mức độ bảo vệ tương đương hoặc đầy đủ so với mức độ bảo vệ tại quốc gia chuyển giao, hoặc khi có các biện pháp bảo đảm thích hợp để duy trì quyền và lợi ích hợp pháp của chủ thể dữ liệu. Cách tiếp cận này phản ánh việc coi quyền đối với DLCN là quyền cần được bảo vệ liên tục, không phụ thuộc vào biên giới địa lý của nơi xử lý dữ liệu.

Đối với chính quyền số, yêu cầu bảo đảm mức độ bảo vệ không suy giảm trong chuyển giao dữ liệu xuyên biên giới có ý nghĩa đặc biệt quan trọng. Nhà nước, với tư cách là chủ thể xử lý dữ liệu có quyền lực vượt trội, không thể chuyển giao trách nhiệm bảo vệ DLCN cho các nhà cung cấp dịch vụ công nghệ. Ngược lại, pháp luật quốc tế nhấn mạnh nghĩa vụ liên tục của Nhà nước trong việc giám sát, kiểm soát và chịu trách nhiệm giải trình đối với toàn bộ quá trình xử lý dữ liệu, kể cả khi dữ liệu được lưu trữ hoặc xử lý ngoài lãnh thổ quốc gia. Chính từ yêu cầu đó, pháp luật quốc tế thúc đẩy sự hình thành các cơ chế hợp tác và thừa nhận lẫn nhau về tiêu chuẩn bảo vệ DLCN, bao gồm các thỏa thuận song phương, khu vực hoặc đa phương về bảo vệ dữ liệu; cơ chế công nhận mức độ bảo vệ tương đương, cũng như các chuẩn mực

chung về an toàn, bảo mật và trách nhiệm giải trình. Đối với khu vực công, các cơ chế hợp tác này không chỉ góp phần bảo vệ quyền đối với DLCN của công dân trong môi trường số xuyên biên giới, mà còn tạo điều kiện cho chính quyền số vận hành hiệu quả, hợp pháp và bền vững trong bối cảnh hội nhập quốc tế ngày càng sâu rộng.

Quyền của chủ thể DLCN trong pháp luật quốc tế về bảo vệ DLCN

Trong pháp luật quốc tế hiện đại, quyền đối với DLCN được cụ thể hóa thông qua hệ thống các quyền của chủ thể dữ liệu, được ghi nhận rõ nét trong các chuẩn mực pháp lý tiêu biểu như Quy định Bảo vệ dữ liệu chung - GDPR của Liên minh châu Âu, Công ước 108/108+ của Hội đồng châu Âu “Công ước về bảo vệ cá nhân liên quan đến việc xử lý tự động DLCN” (*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*), và Hướng dẫn của Hội đồng OECD. Các quyền này nhằm bảo đảm cá nhân có khả năng kiểm soát thực chất đối với việc xử lý dữ liệu liên quan đến mình, đặc biệt trong bối cảnh Nhà nước và cơ quan công quyền giữ vai trò chủ thể xử lý dữ liệu trung tâm trong mô hình chính quyền số [78;79].

- Quyền được biết về hoạt động xử lý DLCN được ghi nhận như một quyền nền tảng bảo đảm tính minh bạch. Quy định Bảo vệ dữ liệu chung - GDPR quy định chủ thể dữ liệu có quyền được cung cấp thông tin khi dữ liệu được thu thập hoặc xử lý, bao gồm mục đích xử lý, căn cứ pháp lý, thời hạn lưu trữ và quyền của chủ thể dữ liệu (Điều 13 và Điều 14 GDPR). Công ước 108+ cũng yêu cầu DLCN phải được xử lý một cách công bằng và minh bạch và cá nhân phải có khả năng biết về sự tồn tại của việc xử lý dữ liệu liên quan đến mình (Điều 5 và Điều 9 Công ước 108+). Hướng dẫn của OECD khẳng định nguyên tắc công khai (Openness Principle), theo đó các chính sách và thực tiễn liên quan đến DLCN phải được công bố rõ ràng [78;79;98].

- Quyền đồng ý hoặc không đồng ý và quyền rút lại sự đồng ý là biểu hiện trực tiếp của quyền tự quyết thông tin. GDPR xác định sự đồng ý của chủ thể dữ liệu là một căn cứ pháp lý cho việc xử lý DLCN (Điều 6(1)(a)), đồng thời yêu cầu sự đồng ý phải “*tự nguyện, cụ thể, được thông tin đầy đủ và rõ ràng*” (Điều 4(11)). Quan trọng hơn, GDPR khẳng định chủ thể dữ liệu “*có quyền rút lại sự đồng ý của mình bất kỳ lúc nào*” (Điều 7(3)), và việc rút lại sự đồng ý không ảnh hưởng đến tính hợp pháp của việc xử lý đã thực hiện trước đó. Cách tiếp cận này cũng được phản ánh trong Công ước 108+ khi nhấn mạnh tính hợp pháp và sự tham gia của cá nhân trong xử lý dữ liệu [78;79].

- Quyền xem, chỉnh sửa hoặc yêu cầu chỉnh sửa DLCN được thừa nhận rộng rãi nhằm bảo đảm tính chính xác của dữ liệu. GDPR quy định quyền truy cập dữ liệu (Điều 15), cho phép cá nhân biết dữ liệu nào đang được xử lý và cách thức xử lý; đồng thời ghi nhận quyền yêu cầu chỉnh sửa dữ liệu không chính xác hoặc bổ sung dữ liệu chưa đầy đủ (Điều 16). Công ước 108+ cũng khẳng định cá nhân có quyền yêu cầu “chỉnh sửa hoặc xóa dữ liệu” nếu dữ liệu được xử lý không phù hợp với pháp luật (Điều 9) [78;79].

- Pháp luật quốc tế ghi nhận quyền yêu cầu xóa dữ liệu, hạn chế xử lý và quyền phản đối xử lý DLCN như những công cụ can thiệp sâu vào vòng đời dữ liệu. GDPR dành Điều 17 để quy định “quyền được xóa dữ liệu” (right to erasure, right to be forgotten), trong đó cho phép cá nhân yêu cầu xóa dữ liệu khi dữ liệu không còn cần thiết cho mục đích ban đầu hoặc việc xử lý là trái pháp luật. Điều 18 GDPR quy định quyền hạn chế xử lý dữ liệu, còn Điều 21 ghi nhận quyền phản đối việc xử lý dữ liệu trong những trường hợp nhất định. Các quyền này phản ánh xu hướng kiểm soát chặt chẽ việc mở rộng mục đích và thời gian xử lý dữ liệu trong quản trị số [78].

- Quyền khiếu nại, khởi kiện và yêu cầu bồi thường thiệt hại là cơ chế bảo đảm thực thi các quyền đối với DLCN. Quy định Bảo vệ dữ liệu chung - GDPR quy định chủ thể dữ liệu có quyền khiếu nại lên cơ quan giám sát (Điều 77), quyền khởi kiện tư pháp đối với cơ quan giám sát hoặc chủ thể xử lý dữ liệu (Điều 78 và Điều 79), và quyền được bồi thường thiệt hại vật chất hoặc phi vật chất phát sinh từ hành vi vi phạm quy định bảo vệ dữ liệu (Điều 82). Công ước 108+ cũng yêu cầu các quốc gia thành viên thiết lập cơ chế bảo vệ pháp lý hiệu quả cho cá nhân khi quyền đối với DLCN bị xâm phạm [78;79].

- Pháp luật quốc tế ghi nhận quyền yêu cầu áp dụng các biện pháp bảo vệ DLCN, thể hiện qua nghĩa vụ của chủ thể xử lý trong việc áp dụng các biện pháp kỹ thuật và tổ chức phù hợp. GDPR quy định nguyên tắc “bảo vệ dữ liệu theo thiết kế và theo mặc định” (Điều 25), yêu cầu chủ thể xử lý phải tích hợp các biện pháp bảo vệ ngay từ khâu xây dựng hệ thống và bảo đảm rằng theo mặc định chỉ dữ liệu cần thiết mới được xử lý. Bên cạnh đó, các nghĩa vụ về bảo mật xử lý dữ liệu (Điều 32 GDPR) và đánh giá tác động bảo vệ dữ liệu (Điều 35 GDPR) tạo cơ sở để cá nhân yêu cầu cơ quan, tổ chức có liên quan áp dụng các biện pháp bảo vệ phù hợp [78].

Từ các quy định nêu trên chúng ta thấy, pháp luật quốc tế đã xây dựng một khuôn khổ quyền toàn diện cho chủ thể DLCN, không chỉ dừng ở việc công nhận

quyền trên danh nghĩa mà còn thiết lập cơ chế bảo đảm thực thi hiệu quả. Hệ thống quyền này đóng vai trò đặc biệt quan trọng trong bối cảnh xây dựng chính quyền số, khi Nhà nước trở thành chủ thể xử lý dữ liệu có quyền lực vượt trội, đòi hỏi phải có các giới hạn pháp lý chặt chẽ nhằm bảo vệ QCN trong môi trường số. Từ đó, chúng ta có thể phân định các nội dung và phương thức cốt lõi bảo vệ quyền đối với DLCN của hệ thống pháp luật quốc tế như sau:

(1). *Bảo vệ bằng nguyên tắc “Tối thiểu hóa và giới hạn mục đích”*: Theo Công ước 108 và OECD, dữ liệu phải được “thu thập hợp pháp”, “lưu trữ cho mục đích cụ thể”, “đầy đủ, thích hợp và không vượt quá những mục đích” ban đầu và không lưu giữ lâu hơn thời gian cần thiết. Đây là phương thức phòng ngừa chủ động ở giai đoạn đầu vào, giới hạn quyền lực của chủ thể xử lý dữ liệu, ngăn chặn tình trạng lạm dụng thu thập tràn lan [79].

(2). *Bảo vệ bằng cơ chế “Minh bạch hóa và quyền được biết”*: Theo Điều 13, 14 GDPR và Nguyên tắc công khai (Openness Principle) của OECD. Chủ thể dữ liệu phải được biết về sự tồn tại của hoạt động xử lý, mục đích, căn cứ pháp lý và thời hạn lưu trữ. Phương thức này phá vỡ tính bất đối xứng thông tin giữa cơ quan công quyền và người dân, chuyển trạng thái xử lý dữ liệu từ “bí mật, một chiều” sang “công khai, chịu sự giám sát” [78;98].

(3). *Bảo vệ bằng cơ chế “Tự quyết thông tin và quyền đồng ý”*: Theo Điều 4, 6, 7 GDPR. Sự đồng ý phải “tự nguyện, cụ thể, được thông tin rõ ràng” và chủ thể có quyền “rút lại sự đồng ý bất kỳ lúc nào”. Đây là phương thức trao quyền chủ động tối cao cho công dân, khẳng định danh dự và quyền tự do cá nhân trong môi trường số, người dân là chủ thể quyết định đối với dữ liệu của mình [78].

(4). *Bảo vệ bằng cơ chế “Can thiệp sâu vào vòng đời dữ liệu”*: Theo Điều 15, 16, 17, 18, 21 GDPR và Công ước 108+. Bao gồm quyền truy cập để kiểm tra tính chính xác; quyền chỉnh sửa; quyền phản đối xử lý; quyền hạn chế xử lý và đặc biệt là “quyền được xóa dữ liệu, quyền được quên”. Phương thức hậu kiểm và điều chỉnh, cho phép công dân can thiệp, sửa chữa hoặc chấm dứt hoạt động xử lý dữ liệu của cơ quan nhà nước khi không còn căn cứ pháp lý [78;79].

(5). *Bảo vệ bằng giải pháp “Thiết kế hệ thống và Bảo mật mặc định”*: Theo Điều 25, 32, 35 GDPR. Yêu cầu tích hợp các biện pháp kỹ thuật/tổ chức ngay từ khâu xây dựng hệ thống, thiết lập chế độ bảo mật mặc định chỉ xử lý dữ liệu cần thiết và bắt buộc phải đánh giá tác động bảo vệ dữ liệu (DPIA). Phương thức bảo vệ bằng kỹ

thuật và công nghệ, dịch chuyển trách nhiệm bảo mật từ người dân sang chính cấu trúc hệ thống của tổ chức vận hành [78].

(6). *Bảo vệ bằng cơ chế “Kiểm soát chuyển giao dữ liệu xuyên biên giới”*: Pháp luật quốc tế đặt ra nguyên tắc “Bảo vệ liên tục”. Dữ liệu chỉ được chuyển ra ngoài lãnh thổ (như sử dụng dịch vụ đám mây xuyên quốc gia) khi bên tiếp nhận bảo đảm mức độ bảo vệ tương đương, không cho phép Nhà nước thoái thác nghĩa vụ giải trình. Phương thức bảo vệ không giới hạn địa giới, duy trì chủ quyền số và quyền con người của công dân bất kể dữ liệu đang nằm ở máy chủ nào trên thế giới.

(7). *Bảo vệ bằng chế tài “Tài phán, khiếu kiện và bồi thường thiệt hại”*: Theo Điều 77, 78, 79, 82 GDPR và Công ước 108+. Quyền khiếu nại lên cơ quan giám sát độc lập, quyền khởi kiện tư pháp và quyền được bồi thường thiệt hại vật chất hoặc phi vật chất (như tổn thất tinh thần). Phương thức bảo đảm tối hậu (bảo vệ quyền thông qua tư pháp), sử dụng quyền lực pháp lý để răn đe bên vi phạm và khôi phục, bù đắp quyền lợi cho nạn nhân [78;79].

2.3.2. Pháp luật một số quốc gia điển hình về bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số

Việc nghiên cứu kinh nghiệm quốc tế về bảo vệ quyền đối với DLCN trong xây dựng chính quyền số đòi hỏi một phương pháp luận so sánh luật học khách quan, trong đó cần phân định chính xác giá trị pháp lý của từng loại nguồn (từ các điều ước quốc tế có tính ràng buộc toàn cầu như ICCPR, điều ước khu vực như Convention 108+, văn bản quy phạm khu vực như GDPR, đến các tiêu chuẩn mềm của OECD và pháp luật quốc gia) cũng như khả năng chuyển giao mô hình pháp luật vào điều kiện thực tiễn của Việt Nam.

2.3.2.1. Phân định giá trị pháp lý của các nguồn chuẩn mực quốc tế và khu vực liên quan

Công ước quốc tế ràng buộc pháp lý toàn cầu (như ICCPR): Xác lập các nghĩa vụ pháp lý quốc tế tối thượng về quyền con người và quyền riêng tư (Điều 17 ICCPR), tạo nền tảng hiến định bắt buộc các quốc gia thành viên (trong đó có Việt Nam) phải nội luật hóa vào hệ thống pháp luật quốc gia. [109]

Điều ước quốc tế chuyên ngành (như Công ước 108 và Nghị định thư sửa đổi 108+ của Hội đồng Châu Âu): Là công ước quốc tế đa phương đầu tiên có tính ràng buộc pháp lý về bảo vệ dữ liệu, mở cho cả các quốc gia ngoài châu Âu tham gia, cung cấp bộ khung tiêu chuẩn về quyền chủ thể và cơ chế giám sát độc lập. [79]

Pháp luật khu vực (như GDPR của Liên minh Châu Âu): Là đạo luật mẫu có hiệu lực trực tiếp và ràng buộc pháp lý tại các quốc gia thành viên EU. Mặc dù GDPR không phải là điều ước quốc tế tạo nghĩa vụ trực tiếp cho Việt Nam, nhưng đây là những tiêu chuẩn và nguồn tham khảo đặc biệt quan trọng nhờ tính bao quát, nghiêm khắc và tư duy bảo vệ quyền toàn diện, tác động mạnh mẽ đến tư duy lập pháp của nhiều quốc gia trên thế giới khi xây dựng luật bảo vệ dữ liệu. [78]

Các chuẩn mực quản trị và hướng dẫn mềm (như Khuyến nghị của OECD): Không mang tính ràng buộc pháp lý cưỡng chế, nhưng đóng vai trò định hình các nguyên tắc quản trị tốt (Good Governance), minh bạch hóa và thúc đẩy dòng chảy dữ liệu an toàn trong kinh tế số toàn cầu. [98]

2.3.2.2. Khảo sát mô hình pháp luật và cấu trúc quyền lực Trung ương - Địa phương của các quốc gia điển hình về bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số

(1) Cộng hòa Liên bang Đức: Mô hình liên bang, án lệ hiến pháp và sự kết hợp GDPR - BDSG

Cộng hòa Liên bang Đức thường được xem là một trong những quốc gia thiết lập khuôn khổ bảo vệ quyền riêng tư và DLCN ở mức nghiêm ngặt. Đặc trưng của cách tiếp cận này là nền tảng bảo vệ không chỉ dựa trên các chính sách quản trị hiện đại, mà đã được ghi nhận trong hệ thống pháp luật thành văn và được định hình thông qua án lệ từ khá sớm, điển hình như phán quyết Volkszählungsurteil (Census Judgment) ngày 15/12/1983 của Tòa án Hiến pháp Đức. Trong phán quyết này, Tòa án xác định rằng quyền nhân thân chung theo Điều 2(1) kết hợp với Điều 1(1) của Luật Cơ bản (Basic Law) bao hàm cơ chế bảo vệ cá nhân trước việc thu thập, lưu trữ, sử dụng và chia sẻ DLCN một cách không bị giới hạn [76]. Đồng thời, quyền này bảo đảm cho cá nhân, về nguyên tắc, có quyền tự quyết định việc công bố và mục đích sử dụng dữ liệu liên quan đến mình (quyền tự quyết thông tin). Bên cạnh việc thừa nhận nội hàm quyền, Tòa án cũng đặt ra các điều kiện nghiêm ngặt đối với mọi biện pháp hạn chế quyền tự quyết thông tin: (i) Chỉ có thể được chấp nhận khi phục vụ một lợi ích công cộng vượt trội; (ii) Phải có cơ sở pháp lý rõ ràng, đáp ứng các yêu cầu về tính xác định và tính hợp hiến; (iii) Phải tuân thủ nguyên tắc tương xứng (proportionality); (iv) Nhà nước có nghĩa vụ xây dựng các bảo đảm về tổ chức và thủ tục nhằm giảm thiểu rủi ro xâm phạm quyền nhân thân trong quá trình áp dụng và thực thi. Cách tiếp cận của Đức cho thấy DLCN không đơn thuần là đối tượng của

quản lý nhà nước, mà trước hết được nhìn nhận như một quyền cơ bản, do đó cần có căn cứ pháp lý và thực tiễn khi tiến hành các hoạt động thu thập, liên thông hoặc khai thác dữ liệu. Hệ thống bảo vệ DLCN của Đức vận hành dựa trên hai trụ cột có quan hệ hỗ trợ.

Thứ nhất, Quy định chung về bảo vệ dữ liệu của Liên minh châu Âu (GDPR) - văn bản pháp quy của Liên minh châu Âu có hiệu lực từ ngày 25/05/2018 và được áp dụng trực tiếp, thống nhất tại các quốc gia thành viên. GDPR xác lập các nguyên tắc xử lý dữ liệu, hệ thống quyền của chủ thể dữ liệu, các nghĩa vụ cốt lõi của bên kiểm soát và bên xử lý dữ liệu, cũng như khung chế tài chung [78].

Thứ hai, Luật Bảo vệ Dữ liệu Liên bang Đức (Bundesdatenschutzgesetz - BDSG), có hiệu lực từ ngày 25/05/2018, đóng vai trò là đạo luật hỗ trợ của quốc gia nhằm (i) cụ thể hóa các quy định của GDPR trong bối cảnh pháp luật Đức; (ii) tận dụng các “điều khoản mở” (tức các khoảng trống lập quy mà GDPR cho phép quốc gia thành viên quy định chi tiết trong một số lĩnh vực nhất định) để thiết lập quy tắc phù hợp với điều kiện thể chế, hành chính và tư pháp của Đức [74]. Như vậy, nếu GDPR tạo ra “khung chuẩn” mang tính thống nhất của Liên minh, thì BDSG cung cấp “lớp quy phạm triển khai” ở cấp quốc gia, giúp hệ thống vận hành khả thi và nhất quán trong thực tiễn áp dụng.

- Về quyền của chủ thể dữ liệu, các quyền nền tảng chủ yếu được ghi nhận tại Chương III của GDPR (từ Điều 12 đến Điều 22) và có thể được hiểu như một “bộ công cụ pháp lý” cho phép cá nhân kiểm soát dữ liệu của mình trong toàn bộ vòng đời xử lý (từ thu thập, lưu trữ đến sử dụng và chia sẻ). GDPR đặt ra nghĩa vụ minh bạch và nghĩa vụ tạo điều kiện thực thi quyền (Điều 12). Theo đó, thông tin cung cấp cho chủ thể dữ liệu phải rõ ràng, dễ hiểu, dễ tiếp cận; thủ tục thực hiện quyền phải đơn giản, không mang tính cản trở và về nguyên tắc không thu phí. Khi nhận được yêu cầu, bên kiểm soát hoặc bên xử lý dữ liệu phải phản hồi trong thời hạn luật định (thường là một tháng), chỉ được gia hạn trong trường hợp phức tạp và phải nêu rõ lý do [78].

Trên nền tảng minh bạch, cá nhân có quyền được cung cấp thông tin khi dữ liệu được thu thập trực tiếp hoặc khi dữ liệu được tiếp nhận từ nguồn khác (Điều 13 và Điều 14). Nhờ đó, chủ thể dữ liệu có thể biết phạm vi dữ liệu đang được xử lý, mục đích và căn cứ pháp lý, thời hạn lưu trữ, đối tượng nhận dữ liệu, cũng như quyền khiếu nại tới cơ quan có thẩm quyền. Từ thông tin này, chủ thể dữ liệu có thể thực thi quyền truy cập

(Điều 15) để xác nhận việc dữ liệu có đang bị xử lý hay không và yêu cầu cung cấp bản sao dữ liệu. Quyền truy cập đồng thời tạo tiền đề cho quyền cải chính (Điều 16) đối với dữ liệu không chính xác, quyền xóa dữ liệu trong các trường hợp luật định (Điều 17 - thường được gọi là “quyền được quên”), và quyền hạn chế xử lý (Điều 18) như một cơ chế tạm thời nhằm “đóng băng” hoạt động xử lý khi phát sinh tranh chấp về tính chính xác của dữ liệu hoặc tính hợp pháp của việc xử lý [78].

Bên cạnh đó, GDPR ghi nhận quyền nhận dữ liệu và chuyển dữ liệu (right to data portability) (Điều 20), theo đó cá nhân có thể nhận dữ liệu của mình theo định dạng có cấu trúc, được sử dụng phổ biến và có thể đọc bằng máy, đồng thời yêu cầu chuyển dữ liệu sang nhà cung cấp khác trong những điều kiện nhất định. Quyền này góp phần tăng cường quyền tự chủ dữ liệu và hỗ trợ cạnh tranh dịch vụ dựa trên khả năng chuyển đổi. GDPR cũng bảo đảm quyền phản đối xử lý (Điều 21), đặc biệt khi việc xử lý dựa trên căn cứ “lợi ích hợp pháp” hoặc phục vụ “nhiệm vụ vì lợi ích công”; riêng đối với xử lý nhằm mục đích tiếp thị trực tiếp, chủ thể dữ liệu được trao quyền phản đối ở mức tăng cường và không phải chứng minh thêm lý do. Trong bối cảnh số hóa và ra quyết định dựa trên thuật toán, quyền không bị áp đặt quyết định hoàn toàn tự động, bao gồm cả việc lập hồ sơ có ý nghĩa đặc biệt (Điều 22). Quy định này hạn chế việc đưa ra quyết định chỉ dựa trên xử lý tự động khi quyết định đó tạo ra hệ quả pháp lý hoặc tác động đáng kể tương tự đối với cá nhân, trừ khi đáp ứng các điều kiện luật định và kèm theo các bảo đảm thích đáng. Về mặt chức năng, các bảo đảm này được xây dựng như cơ chế “phanh an toàn”, bao gồm yêu cầu có sự can thiệp của con người, quyền trình bày quan điểm và quyền khiếu nại, nhằm giảm thiểu rủi ro sai lệch, phân biệt đối xử hoặc xâm hại quyền lợi của chủ thể dữ liệu trong các hệ thống tự động quy mô lớn [78].

Cùng với các quyền nội dung, GDPR ghi nhận cơ chế bảo vệ quyền thông qua quyền khiếu nại tới cơ quan giám sát khi cá nhân cho rằng việc xử lý dữ liệu vi phạm quy định (Điều 77), và ở Đức, BfDI (đối với khu vực công liên bang và một số phạm vi thẩm quyền nhất định) thường hướng dẫn khá cụ thể về cách nộp khiếu nại, thông tin cần cung cấp, cũng như việc cơ quan giám sát các cấp phải xem xét và thông báo kết quả xử lý theo quy trình hợp lý. Nhìn tổng thể, các quyền này không chỉ là danh mục “quyền trên giấy”, mà còn là cơ chế buộc tổ chức phải xây dựng quy trình, hệ thống và dịch vụ theo hướng tôn trọng quyền riêng tư ngay từ đầu, giúp cá nhân có khả năng kiểm soát dữ liệu trong thực tế và tạo nền tảng niềm tin cho môi trường số [81].

Trong tiến trình xây dựng chính quyền số, Đức nhất quán với quan điểm rằng số hóa dịch vụ công chỉ bền vững khi được đặt trên nền tảng bảo vệ dữ liệu mạnh, qua đó tạo dựng và duy trì niềm tin xã hội đối với Nhà nước số. Ở cấp luật, Luật Tiếp cận trực tuyến đối với dịch vụ hành chính (Onlinezugangsgesetz - OZG) đặt ra nghĩa vụ thúc đẩy cung cấp các dịch vụ hành chính qua kênh số và kết nối các công dịch vụ của các cấp chính quyền trong một hệ thống liên thông tổng thể. Trên cơ sở đánh giá thực tiễn triển khai, Đức tiếp tục sửa đổi Luật Tiếp cận trực tuyến đối với dịch vụ hành chính thông qua Luật sửa đổi Luật Tiếp cận trực tuyến đối với dịch vụ hành chính (OZG 2.0). Trong mô hình của Đức, bảo vệ dữ liệu không được hiểu như một yêu cầu “tuân thủ hình thức”, mà là điều kiện cấu thành để triển khai các cấu phần cốt lõi của chính quyền số, như định danh số, công dịch vụ liên thông, và chia sẻ dữ liệu giữa cơ quan nhà nước trên nguyên tắc xử lý đúng mục đích, đủ dùng và kiểm soát được [75]. Từ góc độ hiệu quả chính sách, chính nền tảng bảo đảm quyền và kiểm soát này là yếu tố then chốt để nâng cao mức độ sẵn sàng chấp nhận và tỷ lệ sử dụng thực tế của người dân đối với dịch vụ công trực tuyến.

Tóm lại, mô hình liên bang, án lệ hiến pháp và sự kết hợp GDPR – BDSG như sau: (i) *Cấu trúc quyền lực Trung ương - Địa phương*: Đức là nhà nước liên bang. Cơ sở pháp lý được định hình từ phán quyết mang tính bước ngoặt Volkszählungsurteil (Census Judgment) ngày 15/12/1983 của Tòa án Hiến pháp Liên bang, xác lập quyền tự quyết thông tin (Informational Self-Determination) gắn liền với quyền nhân thân. (ii) *Khung pháp lý triển khai*: Vận hành trên hai trụ cột là GDPR (tạo khung chuẩn thống nhất cấp khu vực) và Luật Bảo vệ Dữ liệu Liên bang Đức (BDSG) (đạo luật hỗ trợ quốc gia tận dụng các “điều khoản mở” của GDPR để phù hợp với thể chế hành chính và tư pháp Đức). (iii) *Cơ chế giám sát và vận hành*: Cơ quan giám sát độc lập liên bang (BfDI) phối hợp với các cơ quan cấp bang. Trong xây dựng chính quyền số, Đức gắn kết chặt chẽ với Luật Tiếp cận trực tuyến (OZG và OZG 2.0), coi bảo vệ dữ liệu là điều kiện cấu thành để kết nối công dịch vụ công liên thông giữa các cấp chính quyền.

(2) Trung Quốc: Mô hình tập trung quyền lực và “Bộ ba” luật dữ liệu an ninh quốc gia

Trung Quốc đã xây dựng cơ chế bảo vệ DLCN dựa trên một “bộ ba” luật dữ liệu gồm Luật Bảo vệ Thông tin cá nhân (PIPL) kết hợp với Luật An ninh mạng (CSL) và Luật An ninh dữ liệu (DSL) để tạo khung quản trị dữ liệu theo hướng vừa bảo vệ quyền lợi cá nhân vừa gắn chặt với yêu cầu an ninh, an toàn dữ liệu. Luật Bảo vệ

Thông tin cá nhân (PIPL) được ban hành phù hợp với Hiến pháp nhằm bảo vệ quyền và lợi ích đối với thông tin cá nhân, điều chỉnh hoạt động xử lý và thúc đẩy việc sử dụng hợp lý đối với dữ liệu của cá nhân. Trong thực thi, Luật Bảo vệ Thông tin Cá nhân (PIPL) đặt nguyên tắc mục đích rõ ràng, tối thiểu hóa tác động và không thu thập quá mức, yêu cầu minh bạch khi xử lý và trách nhiệm bảo mật của bên xử lý [94]. Luật An ninh mạng (CSL) cũng nhấn mạnh các nguyên tắc như “*tính hợp pháp, tính chính đáng, tính cần thiết*” và yêu cầu công bố quy tắc thu thập/sử dụng, xin đồng ý khi thu thập thông tin cá nhân trong môi trường mạng [93].

Về quyền của chủ thể dữ liệu, Luật Bảo vệ Thông tin cá nhân (PIPL) quy định tập trung tại Chương IV (từ Điều 44 đến Điều 50), theo đó cá nhân có quyền được biết và quyết định đối với việc xử lý, quyền hạn chế hoặc từ chối xử lý (trừ trường hợp luật có quy định khác); quyền truy cập, tra cứu và sao chép dữ liệu; quyền yêu cầu chuyển dữ liệu sang bên xử lý khác khi đáp ứng điều kiện kỹ thuật do cơ quan quản lý đặt ra; quyền chỉnh sửa/bổ sung khi dữ liệu sai hoặc thiếu; quyền xóa trong các trường hợp như mục đích đã đạt, không còn cần thiết, hết thời hạn lưu trữ, rút lại đồng ý, hoặc bên xử lý vi phạm pháp luật hoặc thỏa thuận; quyền yêu cầu giải thích quy tắc xử lý [94]. Đi kèm là cách thức để bảo vệ quyền, đó là bên xử lý phải thiết lập cơ chế tiếp nhận và giải quyết yêu cầu, nếu từ chối phải nêu lý do và cá nhân có thể khởi kiện ra tòa khi yêu cầu bị bác.

Về nghĩa vụ của bên xử lý dữ liệu, Luật Bảo vệ Thông tin Cá nhân (PIPL) quy định dữ liệu nhạy cảm chỉ được xử lý khi có mục đích cụ thể, thật sự cần thiết và áp dụng biện pháp bảo vệ nghiêm ngặt; thường phải có “đồng ý riêng” (separate consent). Với các tổ chức xử lý dữ liệu đạt ngưỡng do cơ quan quản lý đặt ra, phải chỉ định người phụ trách bảo vệ thông tin cá nhân và công khai thông tin liên hệ [94]. Nhiều hoạt động có rủi ro cao phải làm đánh giá tác động bảo vệ thông tin cá nhân và lưu hồ sơ. Khi có (hoặc có nguy cơ) rò rỉ, sửa đổi, hoặc mất dữ liệu, bên xử lý dữ liệu phải khắc phục ngay và thông báo cho cơ quan có thẩm quyền và cá nhân liên quan theo nội dung luật định. Với chuyển dữ liệu ra nước ngoài, Luật Bảo vệ Thông tin Cá nhân (PIPL) đặt cơ chế kiểm soát chặt chẽ và yêu cầu thông báo rõ về bên nhận ở nước ngoài cũng như xin đồng ý riêng; một số chủ thể phải lưu trữ nội địa và chỉ được chuyển ra ngoài khi đáp ứng điều kiện.

Về cơ chế giám sát, khiếu nại, xử phạt, Luật Bảo vệ Thông tin cá nhân (PIPL) quy định hệ thống cơ quan quản lý không gian mạng chịu trách nhiệm điều phối tổng thể, cùng các cơ quan Nhà nước khác quản lý theo phạm vi chức năng; người dân có

quyền khiếu nại, tố giác hoạt động xử lý trái luật và cơ quan tiếp nhận phải xử lý, phản hồi kết quả, đồng thời công khai kênh liên hệ. Chế tài có thể rất cao: mức phạt hành chính có thể lên tới 50 triệu NDT hoặc 5% doanh thu năm trước trong trường hợp nghiêm trọng, kèm biện pháp đình chỉ hoặc thu hồi giấy phép và phạt cá nhân quản lý liên quan; ngoài ra còn có trách nhiệm bồi thường dân sự và cơ chế kiện vì lợi ích công cộng trong trường hợp xâm phạm diện rộng [94].

Về bảo vệ quyền đối với DLCN trong xây dựng chính quyền số, Luật Bảo vệ Thông tin cá nhân (PIPL) không chỉ quy định về khu vực tư mà còn có mục riêng về cơ quan nhà nước: khi xử lý dữ liệu để thực hiện nhiệm vụ pháp định phải đúng thẩm quyền, thủ tục, không vượt quá phạm vi cần thiết; dữ liệu do cơ quan nhà nước xử lý nhìn chung phải lưu trữ trong lãnh thổ và chuyển ra nước ngoài phải qua đánh giá an ninh khi thật sự cần. Vì vậy, nếu triển khai chính quyền số, nội dung của PIPL đưa ra các yêu cầu kèm theo như tối thiểu hóa dữ liệu, minh bạch mục đích, cơ chế để người dân truy cập, sửa và xóa theo luật, đánh giá tác động đối với hệ thống rủi ro cao, quy trình phản hồi sự cố, kiểm soát chuyển dữ liệu xuyên biên giới; đây chính là nền tảng để tăng niềm tin số và tính chính danh khi Nhà nước mở rộng cung cấp dịch vụ công trực tuyến ở quy mô lớn [94].

Tóm lại, mô hình tập trung quyền lực và “Bộ ba” luật dữ liệu an ninh quốc gia gồm: (i) *Cấu trúc quyền lực Trung ương - Địa phương*: Trung Quốc theo mô hình nhà nước đơn nhất tập trung cao độ từ trung ương xuống hệ thống hành chính địa phương (tỉnh, thành phố, huyện,...). Quản trị dữ liệu gắn chặt với yêu cầu an ninh quốc gia và kiểm soát không gian mạng. (ii) *Khung pháp lý*: Xây dựng “Bộ ba” luật đồng bộ gồm: Luật Bảo vệ Thông tin cá nhân (PIPL) kết hợp với Luật An ninh mạng (CSL) và Luật An ninh dữ liệu (DSL). PIPL có hẳn một chương riêng quy định về nghĩa vụ của cơ quan nhà nước khi xử lý dữ liệu phục vụ nhiệm vụ pháp định. (iii) *Cơ chế giám sát và chế tài*: Hệ thống cơ quan quản lý không gian mạng (CAC) điều phối tổng thể. Chế tài cực kỳ nghiêm khắc (phạt hành chính lên tới 50 triệu NDT hoặc 5% doanh thu năm trước đối với hành vi vi phạm nghiêm trọng).

(3) Liên bang Nga: Mô hình liên bang, nội địa hóa dữ liệu và liên thông liên ngành

Trong tiến trình xây dựng chính quyền số tại Liên bang Nga, bảo vệ DLCN được đặt trên nền tảng quyền hiến định về đời sống riêng tư và giới hạn quyền lực nhà nước đối với thông tin của công dân. Hiến pháp Liên bang Nga tại Điều 23 quy

định về bảo đảm quyền bất khả xâm phạm đời tư và bí mật cá nhân, gia đình; Điều 24 cũng đặt ra nguyên tắc về việc thu thập, lưu trữ, sử dụng và phổ biến thông tin về đời tư không được thực hiện nếu thiếu căn cứ hoặc sự đồng ý theo luật định; đồng thời cơ quan nhà nước có nghĩa vụ tạo điều kiện để công dân tiếp cận tài liệu, thông tin liên quan trực tiếp đến quyền và tự do của họ. Trên cơ sở đó, khung pháp lý liên bang về DLCN là Luật Liên bang số 152-FZ “Về Dữ liệu cá nhân”, kết hợp với Luật 149-FZ “*Về thông tin, CNTT và bảo vệ thông tin*”. Cùng với đó, Luật 210-FZ “*Về tổ chức cung cấp dịch vụ nhà nước và hành chính công*” cũng đưa ra thiết lập nguyên tắc và nghĩa vụ cung cấp dịch vụ công theo chuẩn hóa thủ tục, trong đó nhấn mạnh khả năng tiếp cận dịch vụ bằng phương thức điện tử như một lựa chọn hợp pháp của người dân (trừ trường hợp khác do luật định) [104].

Về phương diện nguyên tắc và căn cứ xử lý, Luật Liên bang số 152-FZ “Về Dữ liệu cá nhân” xác lập các nguyên tắc xử lý mang tính “hạn chế quyền lực dữ liệu” khi quy định xử lý phải có cơ sở hợp pháp và công bằng; mục đích xử lý phải cụ thể và hợp pháp; dữ liệu phải tương xứng với mục đích; bảo đảm độ chính xác, cập nhật; và bảo đảm an ninh dữ liệu. Điểm đáng chú ý trong bối cảnh chính quyền số là cơ chế xử lý không cần đồng ý, Điều 6 cho phép tiếp tục xử lý khi chủ thể rút lại đồng ý nếu tồn tại các căn cứ luật định như phục vụ thực thi nghĩa vụ pháp lý, thẩm quyền công, tư pháp [105]...

Từ góc độ quyền của chủ thể dữ liệu, Luật Liên bang số 152-FZ “Về Dữ liệu cá nhân” ghi nhận một hệ thống quyền tương đối đầy đủ để cá nhân kiểm soát dữ liệu trong quan hệ với “nhà vận hành dữ liệu”, bao gồm cả cơ quan nhà nước khi xử lý dữ liệu phục vụ quản trị và cung cấp dịch vụ công. Trọng tâm là quyền tiếp cận dữ liệu (Điều 14): công dân có quyền yêu cầu thông tin về việc dữ liệu của mình đang được xử lý (mục đích, căn cứ, nội dung dữ liệu, nguồn thu thập, thời hạn và các chủ thể nhận dữ liệu...), đồng thời có quyền yêu cầu làm rõ/cập nhật, hoặc chặn/hủy dữ liệu nếu dữ liệu không đầy đủ, lỗi thời, không chính xác, thu thập trái luật hoặc không còn cần thiết cho mục đích đã tuyên bố; Điều 16 đặt ra nguyên tắc cấm đưa ra các quyết định tạo hệ quả pháp lý hoặc ảnh hưởng đáng kể đến quyền/lợi ích hợp pháp của cá nhân chỉ dựa trên xử lý tự động, trừ trường hợp có đồng ý bằng văn bản hoặc do luật liên bang quy định kèm theo các biện pháp bảo đảm quyền. Để bảo đảm tính thực thi, Luật Liên bang số 152-FZ “Về Dữ liệu cá nhân” còn ghi nhận quyền khiếu nại

hoặckhởi kiện đối với hành vi hoặc sự không hành động của cơ quan quản lý trong xử lý dữ liệu [105].

Luật Liên bang số 152-FZ “Về Dữ liệu cá nhân” cũng đặt ra mô hình trách nhiệm của cơ quan quản lý theo hướng quản trị tuân thủ. Ngoài yêu cầu bảo mật và hạn chế tiết lộ dữ liệu nếu không có căn cứ hoặc không có sự đồng ý phù hợp, các nhà quản lý phải triển khai các biện pháp tổ chức, kỹ thuật nhằm bảo đảm tuân thủ, được cụ thể hóa tại Điều 18.1 về ban hành chính sách và tài liệu nội bộ về xử lý dữ liệu, thiết lập thủ tục ngăn ngừa, phát hiện, khắc phục vi phạm, phân định trách nhiệm và kiểm soát nội bộ. Đặc biệt trong xây dựng chính quyền số, quy định có tác động cấu trúc mạnh là yêu cầu nội địa hóa dữ liệu: theo khoản 5 Điều 18, khi thu thập DLCN (kể cả qua Internet), các thao tác cốt lõi như ghi nhận, hệ thống hóa, tích lũy, lưu trữ, cập nhật và trích xuất DLCN của công dân Nga không được thực hiện bằng cơ sở dữ liệu đặt ngoài lãnh thổ Nga, trừ các ngoại lệ do pháp luật quy định. Cơ chế giám sát và thực thi được xây dựng theo mô hình cơ quan chuyên trách khi cơ quan được ủy quyền bảo vệ quyền chủ thể dữ liệu thực hiện kiểm tra, thanh tra và giám sát tuân thủ [105]. Trên thực tế, vai trò này gắn với Dịch vụ Liên bang giám sát Truyền thông, Công nghệ thông tin và Truyền thông đại chúng trong hệ thống quản lý nhà nước về DLCN; cơ quan này có thẩm quyền yêu cầu cung cấp thông tin, tiến hành kiểm tra, đánh giá và áp dụng các biện pháp khắc phục đối với dữ liệu sai hoặc dữ liệu được thu thập trái luật.

Trong bối cảnh xây dựng chính quyền số tại Liên bang Nga, quy định được đưa ra là khi dữ liệu trở thành hạ tầng của dịch vụ công, cơ chế giám sát không chỉ nhằm xử lý sự cố đơn lẻ mà còn nhằm buộc các cơ quan quản lý và đơn vị cung ứng dịch vụ công nghệ cho nhà nước duy trì kỷ luật tuân thủ liên tục. Trong quá trình triển khai, quy định tại Luật Liên bang số 210-FZ đã xác lập quyền của người dân được nhận thông tin đầy đủ, cập nhật về thủ tục dịch vụ công và được lựa chọn nhận dịch vụ trên môi trường điện tử khi pháp luật không cấm; đồng thời đặt nghĩa vụ cho cơ quan cung cấp dịch vụ phải bảo đảm khả năng cung cấp dịch vụ ở dạng điện tử theo chuẩn thủ tục [106]. Cơ chế này được vận hành thực tế thông qua cổng dịch vụ công và hệ thống định danh-xác thực để truy cập dịch vụ số. Đồng thời, để hiện thực hóa nguyên tắc “không yêu cầu công dân nộp lại giấy tờ mà cơ quan nhà nước đã có”, mô hình chính quyền số Liên bang Nga chủ yếu dựa vào liên thông dữ liệu liên cơ quan thông qua Hệ thống tương tác điện tử liên ngành, liên bộ được đặt trên nền các nghị định của Chính phủ về hệ thống tương tác liên cơ quan.

Tóm lại, mô hình liên bang, nội địa hóa dữ liệu và liên thông liên ngành của Liên bang Nga như sau: (i) *Cấu trúc quyền lực Trung ương - Địa phương*: Liên bang Nga kết hợp giữa quyền lực liên bang và các chủ thể liên bang. Quyền đòi tư được hiến định tại Điều 23 và 24 Hiến pháp Liên bang Nga. (ii) *Khung pháp lý*: Dựa trên Luật Liên bang số 152-FZ (Về Dữ liệu cá nhân), Luật 149-FZ (Về thông tin, CNTT) và Luật 210-FZ (Về tổ chức cung cấp dịch vụ hành chính công). (iii) *Đặc thù vận hành*: Nổi bật với quy định nội địa hóa dữ liệu (khoản 5 Điều 18 Luật 152-FZ bắt buộc lưu trữ và xử lý dữ liệu cơ bản của công dân Nga trên lãnh thổ Nga). Việc cung cấp dịch vụ công và liên thông dữ liệu liên cơ quan được thực hiện qua Hệ thống tương tác điện tử liên ngành. Cơ quan giám sát chuyên trách Roskomnadzor thực hiện thanh tra, kiểm tra tuân thủ.

(4) Singapore: Mô hình Smart Nation, phân tách công - tư và đồng quy chuẩn mực

Mô hình kiến trúc pháp lý dữ liệu của Singapore (Chiến lược Quốc gia thông minh - Smart Nation): Singapore tiếp cận bảo vệ dữ liệu thông qua đạo luật nền tảng là Luật Bảo vệ Dữ liệu Cá nhân (PDPA 2012), được sửa đổi, bổ sung quy mô lớn vào các năm 2020 và 2024 nhằm thích ứng với môi trường trí tuệ nhân tạo (AI) và điện toán đám mây [112].

Về mặt cấu trúc quản trị công, điểm đặc thù mang tính lý luận của Singapore ban đầu là sự phân tách: PDPA chủ yếu điều chỉnh khu vực tư nhân và các tổ chức phi chính phủ, trong khi khu vực công (các cơ quan chính phủ và chính quyền hành chính địa phương) được điều chỉnh bởi Luật Chính phủ Điện tử và các Chỉ thị của Văn phòng Dữ liệu Chính phủ (SNDGO) thuộc Văn phòng Thủ tướng. Tuy nhiên, trong xu thế xây dựng Chính quyền số đồng bộ, các sửa đổi pháp lý gần đây đã thiết lập cơ chế “đồng quy chuẩn mực” (Standard Convergence). Theo đó, mặc dù khu vực công vận hành dưới một khuôn khổ quản trị công vụ riêng, nhưng các nguyên tắc cốt lõi về bảo vệ quyền chủ thể dữ liệu, như nguyên tắc minh bạch, giới hạn mục đích, bảo mật kỹ thuật và quyền tiếp cận, sửa đổi của công dân... đều được áp dụng tương đương nghiêm ngặt như khu vực tư nhân.

Cơ quan hành chính chuyên trách - Ủy ban Bảo vệ Dữ liệu Cá nhân (PDPC) - đóng vai trò điều phối, ban hành các hướng dẫn kỹ thuật áp dụng cho cả các doanh nghiệp công nghệ cung ứng giải pháp dịch vụ công và các mô hình hợp tác công - tư (PPP) của chính quyền địa phương. Chế tài xử phạt của Singapore có tính răn đe

mạnh về kinh tế, với mức phạt vi phạm có thể lên tới 10% doanh thu hàng năm của tổ chức hoặc 1 triệu đô la Singapore, tạo ra áp lực tuân thủ rất lớn cho toàn bộ hệ thống. [112]

Tóm lại, mô hình của Singapore: (i) *Cấu trúc quyền lực Trung ương - Địa phương*: Singapore là nhà nước đô thị đơn nhất. Ban đầu có sự phân tách rõ rệt: PDPA 2012 điều chỉnh khu vực tư nhân, trong khi khu vực công chịu sự điều chỉnh của Luật Chính phủ Điện tử và các chỉ thị của Văn phòng Dữ liệu Chính phủ (SNDGO). (ii) *Xu hướng hiện đại*: Các sửa đổi gần đây (2020, 2024) thiết lập cơ chế “đồng quy chuẩn mực” (Standard Convergence), theo đó các nguyên tắc cốt lõi về bảo vệ quyền chủ thể được áp dụng tương đối nghiêm ngặt giữa khu vực công và khu vực tư. Cơ quan PDPC điều phối chung và áp dụng chế tài tài chính rất nặng (lên tới 10% doanh thu hoặc 1 triệu đô la Singapore).

(5) Thái Lan: Mô hình luật hợp nhất công - tư và nội luật hóa GDPR tại Đông Nam Á

Mô hình chuyển dịch chuẩn mực quốc tế của Thái Lan (Khung cấu trúc PDPA 2019): Thái Lan ban hành Luật Bảo vệ Dữ liệu Cá nhân (PDPA 2019) và chính thức có hiệu lực toàn diện từ năm 2022 sau nhiều lần trì hoãn để bộ máy hành chính chuẩn bị hạ tầng kỹ thuật. Khác với Singapore, PDPA của Thái Lan được thiết kế như một đạo luật hợp nhất, áp dụng toàn diện cho cả khu vực tư nhân và các cơ quan nhà nước, bao gồm cả chính quyền địa phương và các tỉnh trưởng [113].

Về mặt lý luận bảo hộ quyền, PDPA Thái Lan được xem là sự “bản địa hóa” thành công nhất của GDPR châu Âu tại Đông Nam Á. Luật trao cho công dân Thái Lan đầy đủ các quyền năng mạnh mẽ để đối trọng với quyền lực dữ liệu của cơ quan công quyền: quyền được biết, quyền truy cập, quyền cải chính, quyền phản đối xử lý, quyền hạn chế xử lý, quyền chuyển đổi dữ liệu và đặc biệt là “quyền được quên” (xóa dữ liệu khi không còn mục đích công vụ pháp định).

Để vận hành, Thái Lan thành lập Ủy ban Bảo vệ Dữ liệu Cá nhân (PDPC) đóng vai trò là cơ quan tài phán độc lập. Trọng tâm trong xây dựng chính quyền số tại các tỉnh của Thái Lan theo PDPA 2019 là nghĩa vụ bắt buộc của các cơ quan hành chính địa phương trong việc chỉ định người phụ trách bảo vệ dữ liệu (DPO), thực hiện đánh giá tác động bảo vệ dữ liệu (DPIA) đối với các hệ thống dịch vụ công cốt lõi và tuân thủ các quy định nghiêm ngặt về chuyển dữ liệu xuyên biên giới khi sử dụng các dịch vụ lưu trữ đám mây quốc tế. Chế tài của Thái Lan kết hợp cả xử phạt hành chính

(lên tới 5 triệu Baht), trách nhiệm bồi thường dân sự mang tính trừng phạt (punitive damages, gấp đôi thiệt hại thực tế) và hình phạt hình sự (phạt tù lên đến 1 năm) đối với hành vi cố ý tiết lộ dữ liệu nhạy cảm trái phép [113].

Tóm lại, mô hình Thái Lan về mặt Cấu trúc quyền lực Trung ương - Địa phương thì Thái Lan là nhà nước đơn nhất. Khác với Singapore, Luật Bảo vệ Dữ liệu Cá nhân (PDPA 2019) của Thái Lan được thiết kế như một đạo luật hợp nhất, áp dụng toàn diện, đồng bộ cho cả khu vực tư nhân lẫn các cơ quan nhà nước, bao gồm cả chính quyền địa phương và các tỉnh trưởng. Về cơ chế vận hành, được xem là bản “nội luật hóa” GDPR thành công tại khu vực. Đạo luật trao cho công dân đầy đủ các quyền năng mạnh mẽ (truy cập, cải chính, phản đối, quyền được quên). Cơ quan tài phán độc lập PDPC giám sát việc thực thi; bắt buộc các cơ quan hành chính địa phương phải chỉ định DPO và thực hiện đánh giá tác động (DPIA).

Có thể thấy, từ những nghiên cứu pháp luật của Đức, Trung Quốc, Liên bang Nga, Thái Lan, Singapore cả năm quốc gia đều thiết lập đầy đủ và vận hành nhuần nhuyễn các nội dung và phương thức bảo vệ quyền tương đồng với hướng Việt Nam đang xây dựng:

Thứ nhất, hoàn thiện pháp luật thông qua bảo vệ quyền: Các quốc gia này không chỉ ban hành luật mà xây dựng một cấu trúc pháp luật đa tầng, đồng bộ: (1) Đức: Thiết lập mô hình “chuẩn - triển khai” gồm GDPR (khung chuẩn chung của EU) kết hợp với BDSG (Luật Bảo vệ dữ liệu liên bang Đức) đóng vai trò lớp quy phạm triển khai, tận dụng “điều khoản mở”. Đặc biệt, nền tảng quyền được định hình sớm từ Hiến pháp (Luật Cơ bản) và phán quyết của Tòa án Hiến pháp liên bang (Volkszählungsurteil 1983). (2) Trung Quốc: Xây dựng “bộ ba” luật dữ liệu đồng bộ bao gồm: Luật Bảo vệ Thông tin cá nhân (PIPL) + Luật An ninh mạng (CSL) + Luật An ninh dữ liệu (DSL). (3) Nga: Kết hợp luật chuyên ngành 152-FZ (Về DLCN) với Luật 149-FZ (Về thông tin, CNTT) và Luật 210-FZ (Về tổ chức cung cấp dịch vụ hành chính công). (4) Thái Lan: Bản địa hóa tiêu chuẩn cao (PDPA 2019 áp dụng chung công - tư).

Thứ hai, thông qua tổ chức bộ máy và cơ chế quản lý trong nội bộ từng cơ quan: Kết quả nghiên cứu chỉ ra xu hướng dịch chuyển từ quản lý thủ công sang quản trị tuân thủ nội bộ chủ động: (1) Đức, Trung Quốc và Thái Lan: Bắt buộc các cơ quan, tổ chức xử lý dữ liệu đạt ngưỡng quy định phải chỉ định người phụ trách bảo vệ DLCN (DPO - Data Protection Officer) và công khai thông tin liên hệ. (2) Nga: Điều 18.1

Luật 152-FZ buộc các cơ quan nhà nước phải ban hành chính sách, tài liệu nội bộ, thiết lập thủ tục ngăn ngừa, phát hiện, khắc phục vi phạm và phân định trách nhiệm kiểm soát nội bộ rõ ràng.

Thứ ba, bảo vệ bằng các biện pháp kỹ thuật, công nghệ: Phương thức này được coi là điều kiện cấu thành để triển khai chính quyền số: (1) Đức: Áp dụng nguyên tắc “Privacy by Design & by Default” (Tôn trọng quyền riêng tư ngay từ đầu trong thiết kế hệ thống). Dữ liệu liên thông phải bảo đảm đúng mục đích, đủ dùng và kiểm soát được thông qua các cổng dịch vụ liên thông và định danh số. (2) Nga: Hiện thực hóa nguyên tắc “không yêu cầu công dân nộp lại giấy tờ” bằng cách liên thông dữ liệu qua Hệ thống tương tác điện tử liên ngành, liên bộ, dựa trên nền tảng kỹ thuật ghi vết, mã hóa và kiểm soát truy cập.

Thứ tư, bảo vệ thông qua cơ chế thanh tra, kiểm tra: Tất cả các nước đều thành lập hoặc chỉ định Cơ quan chuyên trách độc lập/có thẩm quyền tối cao: (1) Đức (BfDI), Thái Lan (PDPC): Cơ quan chuyên trách độc lập giải quyết khiếu nại của công dân; giám sát khu vực công, hướng dẫn quy trình nộp khiếu nại. (2) Trung Quốc, Singapore: Chế tài tài chính cực nặng (tính theo phần trăm doanh thu) và phạt tù hình sự đối với cá nhân vi phạm; hệ thống cơ quan quản lý không gian mạng (CAC) chịu trách nhiệm điều phối tổng thể, có quyền phạt hành chính cực nặng (lên tới 50 triệu NDT hoặc 5% doanh thu). (3) Nga: Cơ quan chuyên trách Roskomnadzor (Dịch vụ Liên bang giám sát Truyền thông, Công nghệ thông tin và Truyền thông đại chúng) có toàn quyền thanh tra, kiểm tra và áp dụng biện pháp khắc phục hệ thống dữ liệu sai phạm.

Thứ năm, bảo vệ thông qua bảo đảm quyền chủ thể dữ liệu gắn với quyền con người: Đây là tư tưởng xuyên suốt, coi DLCN là quyền hiến định chứ không thuần túy là đối tượng quản lý hành chính: (1) Đức: Khẳng định tối cao “Quyền tự quyết thông tin” (từ án lệ năm 1983). Chương III GDPR trao cho người dân bộ công cụ: Quyền truy cập (Điều 15), Cải chính (Điều 16), Xóa dữ liệu/“Được quên” (Điều 17), Phản đối xử lý tự động/lập hồ sơ bằng thuật toán AI (Điều 22). (2) Trung Quốc: Chương IV PIPL bảo đảm quyền được biết, quyết định, hạn chế/từ chối xử lý, và quyền yêu cầu giải thích quy tắc thuật toán. (3) Nga: Điều 23, 24 Hiến pháp bảo đảm bất khả xâm phạm đời tư; Luật 152-FZ trao quyền tiếp cận, chặn/hủy dữ liệu lỗi thời và cấm áp đặt quyết định tự động tạo hệ quả pháp lý bất lợi (Điều 16). (4) Thái Lan,

Đức: Trao “bộ công cụ quyền năng” mạnh mẽ (quyền được quên, quyền phản đối thuật toán tự động của AI).

Thứ sáu, tuyên truyền, giáo dục: Tuy các tài liệu nghiên cứu không tách riêng một mục về giáo dục, nhưng phương thức này được thể hiện gián tiếp qua nghĩa vụ minh bạch hóa (Điều 12 GDPR của Đức, PIPL của Trung Quốc). Các cơ quan như BfDI (Đức) hay Roskomnadzor (Nga) đều có chức năng hướng dẫn công khai, dễ hiểu, dễ tiếp cận cho công dân về cách thức nộp khiếu nại, bảo vệ quyền, từ đó nâng cao nhận thức và “niềm tin số” của toàn xã hội khi tham gia dịch vụ công trực tuyến.

Thứ bảy, thông qua hợp tác quốc tế, chia sẻ thông tin và có kiểm soát giữa các chủ thể: (1) Đức: Bản thân việc áp dụng trực tiếp GDPR chính là đỉnh cao của hợp tác quốc tế, tạo ra không gian dữ liệu chung an toàn giữa Đức và các quốc gia thành viên Liên minh châu Âu. (2) Trung Quốc và Nga (Kiểm soát chuyển dữ liệu xuyên biên giới/Nội địa hóa): Đặt ra cơ chế kiểm soát rất ngặt nghèo. Khoản 5 Điều 18 Luật 152-FZ của Nga buộc nội địa hóa dữ liệu (các thao tác ghi nhận, lưu trữ dữ liệu công dân Nga phải thực hiện bằng cơ sở dữ liệu đặt trong lãnh thổ Nga). Trung Quốc quy định dữ liệu do cơ quan nhà nước xử lý phải lưu trữ nội địa, chuyển ra nước ngoài phải qua đánh giá an ninh của cơ quan quản lý.

2.3.3. Những kinh nghiệm rút ra trong bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh ở Việt Nam

Mô hình GDPR & Đức: Đề cập đến việc chuyển dịch từ cơ chế bảo vệ thụ động sang cơ chế kiểm soát tuân thủ chủ động thông qua định chế DPO nội bộ và Báo cáo đánh giá tác động dữ liệu (DPIA).

Mô hình Trung Quốc: Đề cập đến việc phân loại dữ liệu theo mức độ quan trọng (Cốt lõi, quan trọng, thông thường) để áp dụng các hàng rào kỹ thuật mã hóa và kiểm soát chuỗi cung ứng nhà thầu CNTT trong khu vực công.

Mô hình Nga: Đề cập đến việc thắt chặt chủ quyền dữ liệu quốc gia và quy trình lưu vết, nội địa hóa dữ liệu trên hệ thống điện toán đám mây công (Public Cloud) do Nhà nước kiểm soát việc luân chuyển dữ liệu.

Mô hình Singapore: Đề cập đến việc thiết lập cơ chế quản trị dữ liệu linh hoạt (Data Governance) và quy chuẩn hóa trách nhiệm giải trình của công chức thông qua cẩm nang thực thi khu vực công.

Mô hình Thái Lan: Đề cập đến việc mô hình hóa cơ quan giám sát độc lập (PDPC) và thách thức chuyển đổi đồng bộ giữa luật trung ương và năng lực thực thi hành chính của chính quyền địa phương

Từ góc độ lý luận, kinh nghiệm quốc tế cho thấy bảo vệ quyền đối với DLCN trong xây dựng chính quyền số không chỉ dừng ở liệt kê quyền, mà được tổ chức như một cơ chế bảo đảm quyền theo chu trình chuẩn tắc hóa - thể chế hóa - cưỡng chế hóa. Ở bình diện pháp luật quốc tế về QCN, quyền riêng tư và quyền được pháp luật bảo vệ trước sự can thiệp tùy tiện hoặc trái pháp luật vào đời sống riêng tư (bao gồm DLCN) là cơ sở quan trọng, qua đó đặt ra yêu cầu mọi hoạt động xử lý dữ liệu của khu vực công phải được giới hạn bởi các tiêu chí hợp pháp, không tùy tiện, cần thiết và tương xứng. Từ góc độ lý luận, kinh nghiệm quốc tế cho thấy bảo vệ quyền đối với DLCN trong chính quyền số không thể dựa đơn thuần vào tuyên ngôn về quyền, mà phải được xây dựng như một cơ chế thể chế hóa quyền gồm ba tầng liên kết: xác lập chuẩn mực; tổ chức thực thi; và cưỡng chế-khắc phục. Trên nền tảng đó, có thể rút ra hệ kinh nghiệm có giá trị tham chiếu cho Việt Nam ở cấp tỉnh như sau:

Thứ nhất, hoàn thiện thể chế pháp luật: Bảo vệ DLCN cần được đặt vững chắc trong khung QCN và nguyên tắc pháp quyền, theo đó mọi can thiệp vào dữ liệu công dân phải có căn cứ luật định, hướng tới mục tiêu chính đáng và đáp ứng yêu cầu cần thiết và tương xứng. Quyền được bảo vệ khỏi sự can thiệp tùy tiện hoặc trái pháp luật vào đời sống riêng tư và quyền được pháp luật bảo vệ trước các can thiệp đó đã được ghi nhận trong Điều 17 ICCPR. Trên nền tảng này, Cộng hòa Liên bang Đức là trường hợp tiêu biểu về hiến định hóa tư duy bảo vệ dữ liệu thông qua phán quyết “Census” (15/12/1983), phát triển quyền “tự quyết thông tin” như một nội dung cốt lõi của QCN trong xã hội dữ liệu. Kinh nghiệm trong xây dựng chính quyền số cấp tỉnh ở Việt Nam là phải pháp quyền hóa toàn bộ các hoạt động xây dựng cơ sở dữ liệu dùng chung, liên thông hồ sơ và định danh số, tránh nguy cơ chuyển dịch từ quản trị theo luật sang quản trị theo năng lực kỹ thuật với xu hướng thu thập dữ liệu tối đa.

Tóm lại, bài học cho Việt Nam đó là cần bảo đảm sự tương thích và đồng bộ giữa Luật Bảo vệ dữ liệu cá nhân với pháp luật chuyên ngành (Luật Lưu trữ, Luật Đất đai, Luật Căn cước). Ở cấp tỉnh, chính quyền cần chủ động ban hành các quy chế nội bộ, quy trình tác nghiệp chuẩn (SOP) để cụ thể hóa các quy định của trung ương phù hợp với thực tiễn quản lý địa phương.

Thứ hai, Tổ chức bộ máy và quản lý nội bộ cơ quan nhà nước: Các quốc gia có hệ thống bảo vệ dữ liệu phát triển đều coi việc chuẩn hóa nguyên tắc xử lý là xương sống của quản trị dữ liệu công, bởi nguyên tắc là cơ sở để xây dựng quy trình, phân định trách nhiệm và kiểm soát rủi ro. Trong bối cảnh xử lý dữ liệu đa trung tâm của chính quyền số, kinh nghiệm quan trọng là phải xây dựng cơ quan/đầu mối giám sát và cơ chế phối hợp đa cấp để bảo đảm áp dụng thống nhất và truy cứu trách nhiệm xuyên suốt chuỗi xử lý. Đức tổ chức giám sát theo mô hình liên bang với BfDI và các cơ quan giám sát ở các bang, đồng thời phối hợp qua DSK nhằm hình thành quan điểm áp dụng thống nhất. Ở bình diện chuẩn mực, Công ước 108+ nhấn mạnh vai trò nâng cao nhận thức và trách nhiệm của chủ thể xử lý, cũng như yêu cầu tham vấn cơ quan giám sát đối với các đề xuất pháp lý, hành chính liên quan xử lý dữ liệu. Từ đó, Việt Nam cần cơ chế phối hợp giám sát theo chuỗi liên thông, bảo đảm một cửa trách nhiệm khi xảy ra sự cố và có đầu mối đủ thẩm quyền ban hành hướng dẫn thống nhất trong phạm vi tỉnh.

Thay đổi từ tư duy “Thu thập tối đa” sang “Tối thiểu hóa dữ liệu” trong cải cách thủ tục hành chính. Hiện nay, khi làm thủ tục trực tuyến, các sở, ngành có xu hướng yêu cầu người dân khai báo rất nhiều thông tin trùng lặp để tiện cho việc quản lý. Tỉnh cần rà soát lại toàn bộ các biểu mẫu điện tử trên Cổng dịch vụ công theo chuẩn OECD và GDPR: Chỉ thu thập những trường dữ liệu bắt buộc phải có để giải quyết thủ tục. Nếu dữ liệu đó đã có ở cơ sở dữ liệu quốc gia (như Căn cước công dân), các sở tuyệt đối không được bắt dân khai báo lại (áp dụng triệt để nguyên tắc Tối thiểu hóa dữ liệu).

Có thể thấy, các quốc gia đều yêu cầu các cơ quan, tổ chức xử lý dữ liệu phải có người phụ trách chuyên trách (DPO) và hệ thống tài liệu quản trị nội bộ chặt chẽ (như mô hình Điều 18.1 Luật 152-FZ của Nga hay yêu cầu DPIA tại Thái Lan, Đức). Cấp tỉnh ở Việt Nam cần thể chế hóa rõ ràng mô hình DPO độc lập trong các cơ quan chuyên môn thuộc UBND cấp tỉnh.

Thứ ba, biện pháp kỹ thuật, công nghệ: Kinh nghiệm của Đức, cũng như của Liên minh châu Âu (EU) cho thấy quyền đối với DLCN chỉ vận hành thực chất khi được bảo đảm bằng điều kiện kỹ thuật và quản trị rủi ro, tiêu biểu là “bảo vệ dữ liệu ngay từ khâu thiết kế và theo mặc định” và cơ chế đánh giá tác động. GDPR quy định nghĩa vụ *data protection by design and by default* (Điều 25) và yêu cầu DPIA đối với

hoạt động xử lý có nguy cơ cao (Điều 35); các hướng dẫn của EDPB tiếp tục làm rõ đây là trụ cột của bảo vệ dữ liệu trong xã hội số. Cộng hòa Liên bang Đức còn phát triển các công cụ mô hình hóa nhằm chuyển hóa yêu cầu pháp lý thành biện pháp mang tính kỹ thuật và tổ chức.

Buộc áp dụng quy trình đánh giá tác động bảo vệ dữ liệu (DPIA) trước khi nghiệm thu các dự án CNTT của tỉnh. Tỉnh thường chú trọng nghiệm thu tính năng phần mềm (tốc độ, giao diện) mà bỏ qua việc thẩm định kiến trúc bảo mật dữ liệu ngay từ khâu thiết kế hệ thống. Học tập Điều 25, 35 GDPR (Privacy by Design), chính quyền tỉnh cần ban hành quy chế thể chế hóa: Mọi dự án xây dựng phần mềm công, hệ thống camera AI, kho dữ liệu dùng chung của các sở, ngành trước khi đưa vào vận hành bắt buộc phải trải qua bước Đánh giá tác động bảo vệ dữ liệu. Hệ thống phải có tính năng tự động ghi vết (Audit Logs) để xem cán bộ nào đã tra cứu dữ liệu của dân, ngăn chặn việc cán bộ làm lộ thông tin ra ngoài.

Kiểm soát chặt chẽ các điều khoản bảo mật khi thuê hạ tầng Cloud của doanh nghiệp công nghệ. Để tiết kiệm chi phí, nhiều tỉnh đang thuê hạ tầng lưu trữ (Cloud, Hosting) từ bên thứ ba hoặc các tập đoàn công nghệ. Áp dụng bài học về “Chuyển giao dữ liệu” của pháp luật quốc tế, khi ký hợp đồng với các doanh nghiệp công nghệ, UBND tỉnh phải đưa vào các điều khoản pháp lý chặt chẽ: Doanh nghiệp chỉ là bên xử lý dữ liệu thuê, quyền sở hữu thuộc về Nhà nước và công dân; doanh nghiệp phải cam kết lưu trữ dữ liệu tại máy chủ đặt đúng địa bàn, không được chuyển giao hay sử dụng dữ liệu đó để phân tích thị trường hoặc thương mại hóa.

Áp dụng bắt buộc nguyên tắc “Bảo vệ dữ liệu ngay từ khâu thiết kế” đối với tất cả các dự án hạ tầng số quốc gia (như VNeID, Cổng dịch vụ công quốc gia, hệ thống trực liên thông dữ liệu). Hệ thống công nghệ phải tích hợp sẵn các biện pháp kỹ thuật như: mã hóa dữ liệu ở trạng thái lưu trữ và truyền tải, tự động ẩn danh hóa/che mờ thông tin nhạy cảm trên màn hình làm việc của cán bộ, và triển khai giải pháp kiểm soát truy cập phân quyền nghiêm ngặt (RBAC).

Bảo vệ dữ liệu không chỉ là văn bản hành chính mà phải được mã hóa vào hạ tầng kỹ thuật (mã hóa đa trạng thái, phân quyền truy cập nghiêm ngặt, lưu vết bất biến - Audit Log) nhằm hiện thực hóa nguyên tắc liên thông dữ liệu an toàn nhưng vẫn kiểm soát được.

Thứ tư, bảo vệ quyền chủ thể dữ liệu (Quyền con người): Pháp luật các quốc gia được nghiên cứu đã nhấn mạnh rằng bảo vệ quyền đối với DLCN không chỉ nằm

ở nội dung quyền, mà còn ở cơ chế thực thi quyền theo hướng “dễ kích hoạt - dễ truy cứu - có thời hạn”. Điển hình như EU/Đức coi quyền khiếu nại tới cơ quan giám sát (GDPR Điều 77) là một trong những biện pháp quan trọng; Trung Quốc trong pháp luật quốc gia (PIPL) cũng ghi nhận quyền của cá nhân được biết và ra quyết định đối với xử lý dữ liệu và quyền yêu cầu truy cập/nhận bản sao trong thời hạn hợp lý. Việt Nam cần ưu tiên xây dựng quy trình thực thi quyền trên cổng dịch vụ công và cơ chế một cửa - là kênh tiếp nhận, xác thực, thời hạn phản hồi, và quy trình phối hợp liên thông để quyền đối với DLCN của cá nhân không bị hạn chế trong công tác phối hợp giữa các cơ quan có thẩm quyền của Nhà nước. Đồng thời, đối với kho dữ liệu dùng chung và nền tảng tích hợp cấp tỉnh, cần có cơ chế cấp quyền theo chức năng, nhật ký truy cập bắt buộc và quy tắc “mục đích nào - dữ liệu đó”, hạn chế tái mục đích hóa không kiểm soát.

Thiết lập giao diện “Minh bạch thông tin” và cơ chế “Rút lại sự đồng ý” trên các nền tảng số của tỉnh. Người dân Việt Nam hiện nay khi cài đặt các app chính quyền số (như app công dân số của tỉnh) thường chỉ nhấn “Đồng ý với điều khoản” một cách thụ động mà không biết dữ liệu mình bị dùng làm gì. Chính quyền tỉnh phải thiết kế lại giao diện tương tác số minh bạch. Trước khi công dân nộp hồ sơ hoặc dùng app, hệ thống phải hiển thị rõ ràng: Dữ liệu này sẽ lưu trong bao lâu? Ai được quyền tiếp cận? Đồng thời, phải thiết kế một nút bấm chức năng cho phép người dân: Yêu cầu sửa dữ liệu sai, hoặc rút lại quyền khai thác thông tin khi thủ tục hành chính đã hoàn thành.

Chuyển dịch tư duy quản lý từ “Nhà nước ban phát, thu thập để quản lý” sang “Tôn trọng quyền tự quyết thông tin của công dân”. Trên các cổng dịch vụ công, phải thiết kế các tính năng tương tác thực chất để người dân thực hiện “bộ công cụ quyền” của mình: quyền yêu cầu cơ quan nhà nước cải chính dữ liệu sai lệch, quyền được biết mục đích chia sẻ dữ liệu liên ngành, và đặc biệt là “quyền không bị áp đặt quyết định hoàn toàn tự động” bởi AI/thuật toán (theo Điều 22 GDPR và Điều 16 Luật của Nga) khi giải quyết các thủ tục hành chính liên quan đến lợi ích cốt lõi của công dân.

Có thể thấy, cần tăng cường thẩm quyền của Cơ quan chuyên trách bảo vệ DLCN; duy trì cơ chế thanh tra, kiểm tra chuyên ngành thường xuyên từ các cơ quan chuyên trách (như BfDI của Đức, Roskomnadzor của Nga, hay PDPC của Thái Lan, Singapore) kết hợp với các chế tài xử lý nghiêm minh (kỷ luật công vụ, xử phạt hành chính, bồi thường dân sự và truy cứu trách nhiệm hình sự) để tạo sức răn đe thực chất.

Thứ năm, tuyên truyền, giáo dục: Đơn giản hóa các “Điều khoản bảo mật” trên các ứng dụng chính quyền số (như VNeID hay app công dân số địa phương). Thay vì những văn bản pháp lý dài dòng, phức tạp, cơ quan nhà nước phải xây dựng các hướng dẫn ngắn gọn, trực quan (dạng infographic hoặc video ngắn) để người dân hiểu rõ quyền của mình và biết cách tự bảo vệ, cấu hình bảo mật tài khoản số cá nhân.

Tóm lại, cần xuyên suốt các mô hình quốc tế (đặc biệt là Đức, Thái Lan, Trung Quốc), quyền đối với DLCN luôn được định vị là sự cụ thể hóa của quyền riêng tư và quyền tự quyết thông tin (Informational Self-Determination), lấy con người làm trung tâm trong mọi chiến lược phát triển chính quyền số.

Thứ sáu, hợp tác quốc tế và kiểm soát luồng chảy dữ liệu: Kinh nghiệm quốc tế cho thấy, việc bảo đảm chủ quyền đối với dữ liệu cá nhân và kiểm soát chuyển dữ liệu xuyên biên giới cần được thiết kế theo hướng phân tầng rủi ro. Quy định chặt chẽ ranh giới bảo mật đối với các doanh nghiệp tư nhân tham gia dự án đô thị thông minh (PPP); kiểm soát vị trí lưu trữ máy chủ dịch vụ công trực tuyến.

Theo đó, Trung Quốc xây dựng cơ chế kiểm soát chuyển dữ liệu ra nước ngoài bằng các công cụ khác nhau (đánh giá an ninh, hợp đồng mẫu, chứng nhận), phản ánh cách tiếp cận quản trị rủi ro đối với luồng dữ liệu. Trong khi đó, Liên bang Nga nhấn mạnh yêu cầu nội địa hóa dữ liệu công dân theo sửa đổi có hiệu lực từ năm 2015. Trong bối cảnh cấp tính thường sử dụng nhà thầu và hạ tầng đám mây, bài học là cần phân loại dữ liệu (thường/nhạy cảm/đặc biệt quan trọng), xác lập quy tắc lưu trữ, xử lý trong nước cho nhóm rủi ro cao và đặt điều kiện nghiêm ngặt khi sử dụng dịch vụ xuyên biên giới.

Học tập kinh nghiệm nội địa hóa dữ liệu của Nga và Trung Quốc một cách có chọn lọc. Trong xây dựng chính quyền số, toàn bộ dữ liệu cốt lõi về định danh, hộ tịch, trắc sinh học và hành chính của công dân Việt Nam bắt buộc phải lưu trữ trên các máy chủ nằm trong phạm vi lãnh thổ Việt Nam. Khi cơ quan nhà nước sử dụng các dịch vụ điện toán đám mây (Cloud) của các tập đoàn quốc tế, phải có hàng rào kỹ thuật và điều khoản pháp lý kiểm soát nghiêm ngặt, không cho phép chuyển giao dữ liệu ra nước ngoài nếu chưa qua thẩm định an ninh quốc gia.

Thứ bảy, cơ chế thanh tra, kiểm tra: Các hệ thống pháp luật có hiệu quả bảo vệ cao đều dựa trên cơ chế chế tài và bồi thường đủ mạnh để nội hóa chi phí vi phạm, như EU đặt trọng tâm vào cơ chế khiếu nại và biện pháp khắc phục, Cộng hòa Liên bang Đức vận hành mạng lưới cơ quan giám sát dày đặc; trong khi đó, Trung Quốc

nhấn mạnh chế tài nghiêm khắc gắn với doanh thu, thể hiện tư duy rắn đẽ mạnh. Việt Nam cần bảo đảm cơ chế thanh tra - xử lý - bồi thường ở cấp tỉnh vừa kịp thời, vừa minh bạch, bởi nếu chế tài đối với các hành vi vi phạm không đủ sức rắn đẽ sẽ dễ dẫn đến tình trạng lạm dụng và xâm phạm đến DLCN cũng như quyền đối với DLCN của con người.

Thể chế hóa quy trình “Tiếp nhận khiếu nại” và “Bồi thường tổn thất tinh thần” tại địa phương. Khi xảy ra sự cố rò rỉ dữ liệu từ hệ thống công, người dân Việt Nam thường không biết khiếu nại với ai, và pháp luật hiện tại chủ yếu mới phạt hành chính cơ quan làm lộ chứ chưa có cơ chế đền bù cho dân. Học tập Điều 82 GDPR, tỉnh cần đi đầu trong việc thí điểm quy trình tiếp nhận phản ánh về lộ lọt dữ liệu tại Trung tâm Hành chính công hoặc qua tổng đài 1022. Đồng thời, xây dựng cơ chế phối hợp giữa Sở KHCN, Công an tỉnh và Tòa án nhân dân tỉnh để thiết lập hành lang xử lý dân sự: Nếu cơ quan công quyền để lộ thông tin nhạy cảm của dân (như hộ tịch, hồ sơ bệnh án) do lỗi chủ quan, chính quyền phải có trách nhiệm công khai xin lỗi và thực hiện đền bù thiệt hại (kể cả thiệt hại phi vật chất - tổn thất tinh thần) cho công dân.

Cần tăng cường thẩm quyền và năng lực hành động cho Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05 - Bộ Công an) hoặc thiết lập một Cơ quan giám sát dữ liệu độc lập (tương tự BfDI của Đức hay Roskomnadzor của Nga). Cơ quan này phải có quy trình tiếp nhận khiếu nại trực tuyến trực quan cho người dân và có chế tài xử phạt hành chính đủ sức rắn đẽ đối với cả các cơ quan công quyền nếu để xảy ra lộ lọt, rò rỉ dữ liệu do quản lý yếu kém.

Bảng ma trận: Quyền - nghĩa vụ nhà nước - Chỉ báo đánh giá - Bằng chứng thực tiễn - Kết quả bảo đảm quyền.

Nhóm Quyền năng của Công dân (Chương 2)	Nghĩa vụ Pháp lý - Kỹ thuật tương ứng của Chính quyền cấp tỉnh	Tiêu chí/Chỉ báo đánh giá thực trạng (Chương 3)	Bằng chứng thực tiễn minh chứng ở cấp tỉnh	Kết quả/Mức độ bảo đảm quyền thực tế
1. Quyền được biết & Minh bạch thông tin	Nghĩa vụ công khai quy trình, mục đích, phạm vi thu thập, lưu trữ, liên thông và thời hạn xử lý DLCN.	- Tỷ lệ Cổng Dịch vụ công (DVC) có <i>Chính sách bảo vệ DLCN</i> rõ ràng. - Mức độ công khai danh mục các bên thứ ba được chia sẻ dữ liệu qua LGSP.	- Giao diện Cổng DVC cấp tỉnh có/không có biểu mẫu thông báo bảo mật. - Khảo sát mức độ nhận biết của người dân về việc dữ liệu mình bị chia sẻ.	Thấp/Mang tính hình thức: Người dân bị thụ động; không được biết dữ liệu của mình đã được chuyển cho những sở/ngành nào sau khi nộp hồ sơ.
2. Quyền đồng ý & Rút lại sự đồng ý	Nghĩa vụ thiết lập cơ chế kỹ thuật cho phép công dân chủ động cấp/hủy quyền xử lý dữ liệu ngoài nghĩa vụ TTHC bắt buộc.	- Sự tồn tại của nút tính năng "Rút lại sự đồng ý" (Opt-out/Consent Withdrawal) trên Cổng DVC. - Quy trình xử lý khi dân rút sự đồng ý.	- Thiết kế phần mềm Cổng DVC cấp tỉnh (có/không có tùy chọn đồng ý riêng cho từng mục đích).	Chưa được bảo đảm: Hệ thống áp đặt cơ chế "đồng ý mặc định" (mã hóa cứng); không có tính năng kỹ thuật để rút lại sự đồng ý trên giao diện số.
3. Quyền truy cập, xem &	Nghĩa vụ cung cấp giao diện cho phép	- Tính năng "Lịch sử truy cập DLCN" (xem ai/cơ	- Trải nghiệm người dùng trên Cổng	Mức độ Trung bình - Thấp: Người dân xem được

Nhóm Quyền năng của Công dân (Chương 2)	Nghĩa vụ Pháp lý - Kỹ thuật tương ứng của Chính quyền cấp tỉnh	Tiêu chí/Chỉ báo đánh giá thực trạng (Chương 3)	Bằng chứng thực tiễn minh chứng ở cấp tỉnh	Kết quả/Mức độ bảo đảm quyền thực tế
Chỉnh sửa dữ liệu	công dân tra cứu toàn bộ dữ liệu cá nhân đang lưu trữ và yêu cầu cập nhật, sửa đổi.	quan nào đã tra cứu dữ liệu của mình). - Tỷ lệ yêu cầu chỉnh sửa dữ liệu được giải quyết đúng hạn.	DVC/VNeID cấp tỉnh. - Tồn tại tình trạng sai lệch thông tin nhân thân trên CSDL nhưng thủ tục đính chính phức tạp.	thông tin cá nhân cơ bản nhưng <i>không xem được nhật ký tra cứu công vụ</i> và thủ tục đính chính còn nặng về giấy tờ.
4. Quyền xóa dữ liệu & Hạn chế xử lý / Phản đối	Nghĩa vụ hủy bỏ/xóa DLCN khi hết thời hạn lưu trữ hoặc khi người dân yêu cầu (nếu không thuộc trường hợp miễn trừ pháp lý).	- Cơ chế kỹ thuật tự động xóa/ẩn dữ liệu khi hết thời hạn TTHC. - Quy trình tiếp nhận và phản hồi yêu cầu hạn chế/phản đối xử lý.	- Văn bản quy định thời hạn lưu trữ DLCN tại các Trung tâm Tích hợp dữ liệu (IDC) cấp tỉnh. - Sự tồn tại của nút “Xóa dữ liệu/Đóng tài khoản”.	Rất yếu: Tư duy quản lý hành chính vẫn là “lưu trữ vĩnh viễn/tích lũy tối đa”; hoàn toàn thiếu công cụ kỹ thuật để người dân bấm “Xóa” hoặc “Hạn chế xử lý”.
5. Quyền khiếu nại, tố cáo & Yêu cầu	Nghĩa vụ thiết lập kênh tiếp nhận sự cố, quy trình truy	- Tỷ lệ sự cố rò rỉ dữ liệu được chính quyền chủ động thông	- Báo cáo thanh tra/kiểm tra về an toàn thông tin tại tỉnh.	Chưa được bảo đảm: Khi xảy ra sự cố lộ lọt, chính quyền có xu hướng che

Nhóm Quyền năng của Công dân (Chương 2)	Nghĩa vụ Pháp lý - Kỹ thuật tương ứng của Chính quyền cấp tỉnh	Tiêu chí/Chỉ báo đánh giá thực trạng (Chương 3)	Bằng chứng thực tiễn minh chứng ở cấp tỉnh	Kết quả/Mức độ bảo đảm quyền thực tế
bồi thường	vết lỗi công vụ (Audit Log) và bồi thường thiệt hại khi lộ lọt DLCN.	báo cho công dân. - Số lượng vụ việc khiếu nại/bồi thường DLCN được thụ lý, giải quyết ở cấp tỉnh.	- Tình trạng không cung cấp được nhật ký hệ thống (Audit Log) làm bằng chứng cho dân.	giấu rủi ro; người dân thiếu bằng chứng kỹ thuật để khiếu kiện hoặc đòi bồi thường thiệt hại.
6. Quyền an toàn & Bảo mật dữ liệu	Nghĩa vụ áp dụng các giải pháp kỹ thuật bắt buộc (Mã hóa, Zero Trust, SOC) để chống truy cập trái phép từ bên trong lẫn bên ngoài.	- Mức độ đáp ứng mô hình bảo vệ 4 lớp và tiêu chuẩn ISO/IEC 27001. - Khả năng khoanh vùng và ngăn chặn nguy cơ lạm dụng dữ liệu nội bộ qua LGSP.	- Biên bản kiểm toán an ninh mạng; kết quả giám sát từ NCSC. - Số lượng tài khoản cán bộ bị phát hiện tra cứu dữ liệu vượt thẩm quyền.	Mức độ Trung bình: Làm tương đối tốt ở khía cạnh chống tấn công từ bên ngoài, nhưng bộc lộ nhiều lỗ hổng ở khía cạnh kiểm soát lạm dụng nội bộ.

Tiểu kết Chương 2

Chương 2 đã xây dựng cơ sở lý luận cho nghiên cứu bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh; khái quát các đặc điểm của bảo vệ quyền DLCN ở cấp tỉnh, gắn với bối cảnh dữ liệu được xử lý chủ yếu để giải quyết thủ tục hành chính và cung cấp dịch vụ công trực tuyến, đồng thời thường xuyên phát sinh hoạt động phối hợp liên ngành và liên thông dữ liệu.

Về nội dung và phương thức bảo vệ, luận án đã hệ thống hóa các nhóm quyền của chủ thể dữ liệu và yêu cầu bảo đảm khả năng thực thi quyền trong môi trường số; nghĩa vụ của các chủ thể tham gia xử lý dữ liệu; và cơ chế bảo đảm thực thi. Chương 2 cũng phân tích nhóm yếu tố ảnh hưởng đến hiệu quả bảo vệ quyền DLCN, bao gồm: mức độ hoàn thiện của khuôn khổ pháp luật; mô hình quản trị dữ liệu và phân định trách nhiệm giữa các cơ quan; mức độ sẵn sàng của hạ tầng số và năng lực bảo đảm an toàn thông tin; nguồn lực con người và văn hóa tuân thủ; cùng với mức độ minh bạch và cơ chế giám sát - giải trình trong hoạt động liên thông, chia sẻ dữ liệu. Luận án cũng nghiên cứu chuẩn mực pháp luật quốc tế và kinh nghiệm một số quốc gia (Đức, Liên bang Nga, Trung Quốc, Singapo, Thái Lan) để rút ra các gợi ý có giá trị tham khảo cho Việt Nam. Mặc dù khác biệt về thể chế và mô hình quản trị, các tiếp cận này đều nhấn mạnh những trụ cột chung như: giới hạn mục đích và kiểm soát tái sử dụng dữ liệu; trách nhiệm giải trình của chủ thể kiểm soát dữ liệu; minh bạch và cơ chế thực thi quyền của chủ thể dữ liệu; kiểm soát truy cập và truy vết; cùng cơ chế giám sát và chế tài xử lý vi phạm. Những kết quả trên là nền tảng lý luận để Chương 3 tiếp tục phân tích thực trạng pháp luật và thực tiễn triển khai ở Việt Nam, qua đó xác định khoảng trống, vấn đề đặt ra và định hướng giải pháp hoàn thiện trong các chương tiếp theo.

Chương 3

THỰC TRẠNG BẢO VỆ QUYỀN ĐỐI VỚI DỮ LIỆU CÁ NHÂN TRONG XÂY DỰNG CHÍNH QUYỀN SỐ CẤP TỈNH Ở VIỆT NAM

3.1. KHÁI QUÁT CHUNG THỰC TRẠNG VÀ CÁC YẾU TỐ TÁC ĐỘNG ĐẾN XÂY DỰNG CHÍNH QUYỀN SỐ CẤP TỈNH LIÊN QUAN ĐẾN DỮ LIỆU CÁ NHÂN

3.1.1. Chủ trương, chính sách của Đảng và Nhà nước về phát triển chính quyền số cấp tỉnh tại Việt Nam hiện nay

Chính quyền số cấp tỉnh là bộ phận cấu thành hữu cơ, quyết định sự thành bại của chiến lược chuyển đổi số quốc gia. Hệ thống chủ trương, chính sách của Đảng và Nhà nước về vấn đề này mang tính nhất quán, thúc đẩy đồng bộ cả lực lượng sản xuất số và quan hệ sản xuất số tại địa phương qua hai hệ thống văn bản cốt lõi:

3.1.1.1. Định hướng chiến lược của Đảng

Văn kiện Đại hội XIV của Đảng, coi chuyển đổi số là nhiệm vụ chính trị trọng tâm, là một trong những động lực chính đưa đất nước bước vào Kỷ nguyên mới - Kỷ nguyên vươn mình của dân tộc. Tư duy chiến lược dịch chuyển mạnh mẽ từ tin học hóa quy trình cũ sang “kiến tạo quyền lực số và thay đổi toàn diện phương thức quản trị quốc gia”. Đảng định hướng mô hình quan hệ giữa Nhà nước và Nhân dân trong môi trường số: Nhà nước sử dụng công nghệ, dữ liệu để nâng cao năng lực quản trị công và trao quyền ngược lại để Nhân dân làm chủ, giám sát. Mục tiêu then chốt là phát triển nhanh và bền vững dựa trên khoa học công nghệ, đổi mới sáng tạo và chuyển đổi số, xây dựng lực lượng sản xuất mới (hạ tầng, dữ liệu, nhân lực số, AI, bán dẫn) để đưa kinh tế số chiếm 30% GDP vào năm 2030 [25]. Trong mô hình chính quyền địa phương, Đảng nhấn mạnh chuyển đổi số đồng bộ từ cấp cơ sở xã, phường nhằm hình thành “công dân số, cộng đồng dân cư số”. Các định hướng này được cụ thể hóa qua các nghị quyết dẫn dắt như: Nghị quyết số 57-NQ/TW, ngày 22/12/2024 của Bộ Chính trị, yêu cầu thể chế số phải đi trước một bước; hạ tầng và dữ liệu số phải đầu tư tập trung, triệt tiêu tình trạng “cát cứ dữ liệu” giữa các bộ, ngành và địa phương; Nghị quyết số 52-NQ/TW, ngày 27/9/2019 của Bộ Chính trị, xác định mục tiêu hoàn thiện thể chế hành chính công, xây dựng kiến trúc Chính phủ số, bảo đảm an toàn mạng và bảo vệ bí mật đời tư của công dân; Văn kiện Đại hội XIII của Đảng khẳng định chuyển đổi số là phương thức quản trị quốc gia mới; yêu cầu cấp tỉnh phát triển mô hình chính quyền số phục vụ người dân, doanh nghiệp trên nền tảng dữ liệu mở, minh bạch và an toàn.

3.1.1.2. Chương trình hành động của Chính phủ:

Để cụ thể hóa tư duy của Đảng, Chính phủ đã ban hành các đề án hành động số hóa toàn diện từ Trung ương đến địa phương như: Quyết định số 749/QĐ-TTg, ngày 03/6/2020 của Thủ tướng Chính phủ, phê duyệt “Chương trình Chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030”, giao chỉ tiêu cứng cho các tỉnh hoàn thiện Cổng dịch vụ công, hình thành Nền tảng tích hợp, chia sẻ dữ liệu cấp tỉnh (LGSP) liên thông với quốc gia (NDXP); Quyết định số 942/QĐ-TTg, ngày 15/6/2021 của Thủ tướng Chính phủ phê duyệt “Chiến lược phát triển Chính phủ số giai đoạn 2021 - 2025, định hướng đến năm 2030”, chuyển dịch từ “Chính phủ điện tử” sang “Chính phủ số” dựa trên dữ liệu; trọng tâm cấp tỉnh là xây dựng hạ tầng dữ liệu dùng chung, kết nối Trung tâm điều hành thông minh (IOC) với các kho dữ liệu chuyên ngành; Quyết định số 06/QĐ-TTg, ngày 06/01/2022 của Thủ tướng Chính phủ (Đề án 06): Chiến lược cốt lõi tác động trực tiếp đến quyền dữ liệu cá nhân. Đề án 06 buộc chính quyền cấp tỉnh kết nối đồng bộ với Cơ sở dữ liệu quốc gia về dân cư qua định danh VNeID, tạo ra luồng dữ liệu cá nhân không lỏ vào hệ thống hành chính công, đặt ra yêu cầu cấp bách phải cân bằng giữa khai thác hiệu quả và bảo vệ quyền con người đối với dữ liệu. Đồng thời, dữ liệu số phải bảo đảm nghiêm ngặt tiêu chuẩn “đúng, đủ, sạch, sống” để phục vụ quản lý và ra quyết định.

Tóm lại, thể chế phát triển chính quyền số cấp tỉnh hiện nay vận hành theo 03 nguyên tắc cốt lõi: (1) Lấy người dân làm trung tâm, dịch vụ công thuận tiện, minh bạch; (2) Dữ liệu là tài nguyên, vận hành theo nguyên tắc (nộp một lần, tự liên thông); (3) Phát triển gắn liền với an toàn thông tin và bảo vệ quyền bảo mật dữ liệu của công dân theo Hiến pháp. Hành lang chính trị - pháp lý này đã khiến chính quyền cấp tỉnh trở thành chủ thể thu thập, lưu trữ và xử lý khối lượng DLCN khổng lồ của công dân.

3.1.2. Thực trạng xây dựng chính quyền số cấp tỉnh ở Việt Nam hiện nay

Trong những năm gần đây, việc xây dựng chính quyền số cấp tỉnh ở Việt Nam đã được triển khai trong tổng thể chiến lược chuyển đổi số quốc gia, trên cơ sở một hệ thống chủ trương, chính sách và văn bản pháp luật tương đối đầy đủ và ngày càng hoàn thiện. Các văn bản do Trung ương ban hành đã hình thành nền tảng pháp lý thống nhất, tạo cơ sở để các địa phương cụ thể hóa và tổ chức thực hiện nhiệm vụ xây dựng chính quyền số trên địa bàn, đặc biệt nhờ sự tăng tốc của Đề án 06 và chiến lược xây dựng hạ tầng dữ liệu số, cấu trúc DLCN tại các cơ quan hành chính nhà nước cấp tỉnh đã có sự dịch chuyển căn bản. Từ trạng thái “manh mún, thủ công, phân tán”, dữ liệu đã được quy tụ thành tài nguyên số có quy mô khổng lồ với những đặc điểm mang tính thời đại.

Quy mô DLCN do chính quyền cấp tỉnh (thông qua các sở, ban, ngành và UBND các cấp) nắm giữ hiện nay đạt đến độ lớn chưa từng có, thể hiện qua 3 khía

cạnh: Tỷ lệ số hóa hồ sơ công dân gần như tuyệt đối, hầu hết các tỉnh, thành phố đã hoàn thành việc số hóa sổ hộ tịch (khai sinh, kết hôn, khai tử), dữ liệu đất đai, nhà ở, và hồ sơ sức khỏe điện tử cho trên 90% cư dân trên địa bàn [9]. Mật độ thu thập đa kênh, thời gian thực, dữ liệu không chỉ đến từ việc người dân chủ động khai báo khi làm thủ tục hành chính, mà còn được thu thập tự động thông qua: Hệ thống camera giao thông, camera giám sát đô thị thông minh (IOC) có tích hợp công nghệ nhận diện khuôn mặt; dữ liệu định vị vị trí qua các ứng dụng (app) công dân số của địa phương. Sự hình thành Kho dữ liệu dùng chung (LGSP) cấp tỉnh, thay vì nằm rải rác ở các máy chủ đơn lẻ của từng sở như trước, DLCN hiện được tích hợp, “đổ” về Kho dữ liệu dùng chung của tỉnh, tạo thành một chỉnh thể dữ liệu không lồ liên kết trực tiếp với định danh VNeID của từng cá nhân.

DLCN ở cấp địa phương có những đặc trưng pháp lý và kỹ thuật rất riêng biệt so với dữ liệu của các doanh nghiệp thương mại (Big Tech), bao gồm dữ liệu cơ bản (Họ tên, ngày sinh, số định danh, địa chỉ thường trú...) và dữ liệu nhạy cảm (Hồ sơ bệnh án y tế; dữ liệu trắc sinh học; dữ liệu về tình trạng tài sản và dữ liệu về các mối quan hệ gia đình, lịch sử tư pháp, khiếu nại tố cáo...).

Dữ liệu cấp tỉnh không đứng yên; theo nguyên tắc “Once-Only” (chỉ nộp một lần), dữ liệu liên tục chảy qua Trục liên thông văn bản và dữ liệu quốc gia (NDXP), chia sẻ và dịch chuyển giữa các sở với nhau (dịch chuyển ngang), từ cấp xã lên cấp tỉnh và ngược lại (dịch chuyển dọc).

Khác với dữ liệu mạng xã hội (có thể dùng tài khoản ảo), dữ liệu do chính quyền tỉnh quản lý là dữ liệu “gốc”, gắn chặt với quyền công dân, nghĩa vụ pháp lý và lợi ích cốt lõi (an sinh xã hội, quyền sở hữu tài sản) của người dân nên có giá trị pháp lý và tính định danh cao.

3.1.2.1. Thực trạng pháp lý điều chỉnh quá trình xây dựng chính quyền số cấp tỉnh

Một trong những thành tựu quan trọng về thể chế trong giai đoạn hiện nay là việc Nhà nước đã ban hành các văn bản định hướng chiến lược làm cơ sở cho quá trình chuyển đổi từ Chính phủ điện tử sang Chính phủ số, chính quyền số. Nghị quyết số 17/NQ-CP, ngày 07/3/2019 của Chính phủ: Về một số nhiệm vụ, giải pháp trọng tâm phát triển Chính phủ điện tử giai đoạn 2019 - 2020, định hướng đến 2025, đã đặt nền móng cho phát triển Chính phủ điện tử, xác lập các nhiệm vụ, giải pháp trọng tâm về ứng dụng CNTT trong hoạt động của cơ quan nhà nước. Trên cơ sở đó, Quyết định số 749/QĐ-TTg, ngày 03/6/2020 phê duyệt Chương trình Chuyển đổi số quốc gia đã đánh dấu bước chuyển quan trọng về tư duy quản lý, chuyển trọng tâm từ điện tử hóa quy trình sang chuyển đổi số dựa trên dữ liệu và dịch vụ số, trở thành căn cứ trực tiếp để UBND các tỉnh, thành phố

trực thuộc Trung ương ban hành chương trình chuyển đổi số cấp tỉnh. Tiếp theo, Quyết định số 942/QĐ-TTg, ngày 15/6/2021 phê duyệt Chiến lược phát triển Chính phủ điện tử hướng tới Chính phủ số giai đoạn 2021 - 2025, định hướng đến năm 2030, tiếp tục hoàn thiện định hướng phát triển Chính phủ điện tử hướng tới Chính phủ số, tạo cơ sở để các địa phương điều chỉnh mục tiêu, nhiệm vụ và lộ trình xây dựng chính quyền số.

Trên nền tảng các văn bản định hướng chiến lược nêu trên, đa số các địa phương đã ban hành chương trình, kế hoạch chuyển đổi số, trong đó xác định mục tiêu phát triển chính quyền số gắn với cải cách hành chính, nâng cao hiệu lực, hiệu quả quản lý nhà nước và thúc đẩy phát triển kinh tế - xã hội. Đồng thời, các quy định pháp luật về vận hành thủ tục hành chính và dịch vụ công trực tuyến, đặc biệt là Nghị định số 45/2020/NĐ-CP của Chính phủ về thực hiện thủ tục hành chính trên môi trường điện tử, Nghị định số 42/2022/NĐ-CP của Chính phủ quy định về việc cung cấp thông tin và dịch vụ công trực tuyến của cơ quan nhà nước trên môi trường mạng và Thông tư số 01/2023/TT-VPCP, ngày 05/4/2023 Quy định một số nội dung và biện pháp thi hành trong số hóa hồ sơ, kết quả giải quyết thủ tục hành chính và thực hiện thủ tục hành chính trên môi trường điện tử, đã tạo cơ sở pháp lý trực tiếp cho việc triển khai thủ tục hành chính trên môi trường điện tử tại cấp tỉnh, góp phần chuẩn hóa quy trình, thúc đẩy cung cấp dịch vụ công trực tuyến và nâng cao tính công khai, minh bạch trong hoạt động của chính quyền địa phương.

Bên cạnh đó, hệ thống văn bản pháp luật về quản trị, kết nối và chia sẻ dữ liệu số, mà trọng tâm là Nghị định số 47/2020/NĐ-CP của Chính phủ về quản lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước, cùng với các quy định về định danh và xác thực điện tử theo Đề án 06, đã từng bước hình thành nền tảng pháp lý cho chính quyền số cấp tỉnh dựa trên dữ liệu. Trên cơ sở này, nhiều địa phương đã ban hành quy chế quản lý, chia sẻ dữ liệu, xây dựng nền tảng tích hợp, chia sẻ dữ liệu cấp tỉnh và triển khai tích hợp định danh điện tử trong cung cấp dịch vụ công, qua đó tạo điều kiện cho việc tái sử dụng dữ liệu và cá nhân hóa dịch vụ công.

Tuy nhiên, xét từ góc độ thực trạng, mặc dù khung pháp lý cho xây dựng chính quyền số cấp tỉnh đã tương đối đầy đủ, song ở một số địa phương, việc cụ thể hóa các quy định pháp luật vẫn còn chậm và chưa đồng bộ. Chính sách cấp tỉnh trong nhiều trường hợp mới dừng lại ở mức định hướng chung, thiếu quy định cụ thể về lộ trình thực hiện, phân bổ nguồn lực và cơ chế phối hợp liên ngành. Điều này dẫn đến hiệu quả triển khai chưa cao, thiếu tính bền vững và chưa phát huy đầy đủ vai trò của thể chế pháp luật trong việc dẫn dắt quá trình xây dựng chính quyền số ở địa phương.

3.1.2.2. Thực trạng hạ tầng số và nền tảng công nghệ trong xây dựng chính quyền số cấp tỉnh

Trong quá trình xây dựng chính quyền số cấp tỉnh, hạ tầng số và nền tảng công nghệ được xác định là yếu tố nền tảng, quyết định khả năng triển khai và vận hành hiệu quả các hoạt động quản lý nhà nước trên môi trường số. Thực tiễn cho thấy, hạ tầng CNTT tại cấp tỉnh ở Việt Nam đã từng bước được đầu tư, nâng cấp, tạo tiền đề quan trọng cho việc phát triển chính quyền số trong giai đoạn hiện nay. Nhiều địa phương trên cả nước đã chú trọng xây dựng và hoàn thiện trung tâm dữ liệu, mạng truyền số liệu chuyên dùng của các cơ quan nhà nước, đồng thời triển khai nền tảng tích hợp, chia sẻ dữ liệu cấp tỉnh (LGSP) nhằm phục vụ công tác quản lý, điều hành và kết nối, liên thông giữa các sở, ngành, địa phương. Việc hình thành các nền tảng hạ tầng dùng chung này góp phần chuẩn hóa môi trường kỹ thuật, nâng cao khả năng kết nối, chia sẻ thông tin và từng bước khắc phục tình trạng cát cứ dữ liệu trong hoạt động của chính quyền địa phương.

Bên cạnh đó, tại một số tỉnh, thành phố lớn và các địa phương có điều kiện kinh tế - xã hội thuận lợi, việc ứng dụng các công nghệ số mới như điện toán đám mây, trí tuệ nhân tạo, dữ liệu lớn đã được triển khai bước đầu trong quản lý nhà nước. Các ứng dụng này chủ yếu tập trung vào các lĩnh vực như giám sát, điều hành đô thị, phân tích dữ liệu phục vụ ra quyết định (Ví dụ như hệ thống camera giám sát giao thông của thành phố Hà Nội...), hỗ trợ cung cấp dịch vụ công và tương tác với người dân, doanh nghiệp, qua đó góp phần nâng cao hiệu quả hoạt động của chính quyền địa phương. Tuy nhiên, trên thực tế, sự chênh lệch về mức độ đầu tư và năng lực hạ tầng số giữa các địa phương còn khá rõ nét. Nhiều tỉnh, đặc biệt là các địa phương thuộc khu vực miền núi, vùng sâu, vùng xa, hải đảo, hạ tầng CNTT còn hạn chế, thiếu đồng bộ cả về mạng kết nối, thiết bị kỹ thuật và nền tảng công nghệ dùng chung. Điều này không chỉ ảnh hưởng đến khả năng triển khai các ứng dụng chính quyền số ở cấp tỉnh, mà còn làm gia tăng khoảng cách số giữa các địa phương, đặt ra thách thức lớn đối với mục tiêu xây dựng chính quyền số toàn diện, thống nhất trên phạm vi cả nước. Về hạ tầng, dữ liệu và năng lực triển khai ở cơ sở, giai đoạn 2020 - 2025 thể hiện sự kết hợp giữa đầu tư kỹ thuật và các giải pháp tổ chức - xã hội nhằm hỗ trợ người dân tiếp cận chính quyền số. Nhà nước thúc đẩy các chương trình gắn dữ liệu dân cư với định danh điện tử phục vụ chuyển đổi số theo Quyết định số 06/QĐ-TTg 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, đồng thời nhiều địa phương triển khai các hoạt động hỗ trợ kỹ năng số cho người dân. Ở cộng đồng, mạng lưới Tổ công nghệ số cộng đồng được mở rộng trên toàn quốc, với thống kê lên tới hơn 80.000 tổ tại 63 tỉnh, thành (cũ) trong các báo cáo giai đoạn 2023 - 2024 [9]. Đây là yếu tố quan trọng giúp chuyển dịch từ mức độ

“cung cấp dịch vụ công trực tuyến” sang sử dụng thực tế, đặc biệt tại khu vực nông thôn và áp dụng hiệu quả với nhiều nhóm yếu thế.

Tuy vậy, nếu đặt trong yêu cầu của mô hình chính quyền số dựa trên dữ liệu, thực trạng xây dựng chính quyền số cấp tỉnh ở nước ta vẫn bộc lộ nhiều hạn chế, khó khăn về mặt cấu trúc. Liên thông dữ liệu giữa các sở, ngành và giữa địa phương với trung ương chưa đồng bộ, dễ phát sinh tình trạng phân mảnh dữ liệu và trùng lặp thu thập thông tin. Chất lượng dữ liệu như độ đầy đủ, chính xác và cập nhật của dữ liệu chưa ổn định đã ảnh hưởng đến hiệu quả ra quyết định và cung cấp dịch vụ công. Năng lực bảo đảm an toàn thông tin và quản trị rủi ro đối với dữ liệu tại một số địa phương chưa tương xứng với mức độ mở rộng của nền tảng số. Đồng thời, sự chênh lệch về nhân lực số, ngân sách và mức độ chấp nhận công nghệ tiếp tục tạo ra phân hóa rõ rệt giữa các địa phương.

Bên cạnh đó, hạ tầng kỹ thuật số cấp tỉnh nhìn chung đã đạt chuẩn bảo mật nền tảng, cơ bản hoàn thiện mô hình bảo vệ 4 lớp theo hướng dẫn của Bộ chuyên ngành, triển khai Trung tâm điều hành an toàn thông tin (SOC) cấp tỉnh và kết nối với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), có khả năng ngăn chặn tương đối tốt các nguy cơ tấn công kỹ thuật từ bên ngoài (DDoS, mã độc, truy cập trái phép) vào Cổng Dịch vụ công và Trung tâm tích hợp dữ liệu (IDC) của tỉnh. Tuy nhiên, tính tự chủ công nghệ hạn chế, hạ tầng kỹ thuật phụ thuộc lớn vào các nhà thầu CNTT bên ngoài, thiếu công cụ kiểm toán mã nguồn độc lập. Năng lực ghi vết (Audit Log) chưa sâu, việc lưu vết kỹ thuật mới dừng ở cấp độ truy cập hệ thống chung, chưa ghi nhận chi tiết thao tác tác động đến từng trường dữ liệu cá nhân, gây khó khăn cho việc truy vết sự cố.

Những hạn chế này không chỉ dừng lại ở phương diện kỹ thuật, mà còn thể hiện qua các rủi ro về mặt thực tiễn liên quan đến quản lý đối với DLCN và bảo đảm quyền đối với DLCN trong quá trình vận hành chính quyền số cấp tỉnh. Thực tiễn giai đoạn 2020 - 2025 ghi nhận tình trạng công khai hoặc đăng tải quá mức DLCN trên cổng thông tin điện tử và các chuyên mục Hỏi - đáp, phản ánh kiến nghị, khi thông tin định danh và liên hệ của công dân được hiển thị vượt quá những nhu cầu mang tính minh bạch hành chính. Bên cạnh đó, các vụ việc xâm nhập hệ thống và lạm dụng quyền truy vấn cơ sở dữ liệu liên thông cho thấy rủi ro phát sinh khi cơ chế phân quyền, giám sát truy cập và phát hiện bất thường chưa được xây dựng tương xứng với mức độ kết nối dữ liệu. Ngoài ra, các sự cố an toàn thông tin tại hệ thống chuyên ngành, đặc biệt trong lĩnh vực y tế và an sinh xã hội, cho thấy dữ liệu nhạy cảm ở cấp tỉnh đang trở thành mục tiêu dễ tổn thương trước các hình thức tấn công mạng. Đặc biệt, việc lộ lọt hoặc bị khai thác dữ liệu còn kéo theo các hình thức lừa

đảo mạo danh, trong đó đối tượng xấu sử dụng chính thông tin cá nhân của nạn nhân để tạo độ tin cậy và thao túng hành vi của nạn nhân.

Thực trạng trên cho thấy, mặc dù hạ tầng số và nền tảng công nghệ tại cấp tỉnh đã có những bước phát triển đáng kể, song chưa đáp ứng đầy đủ yêu cầu của chính quyền số ở mức độ cao, đòi hỏi phải tiếp tục đầu tư có trọng tâm, trọng điểm, đồng thời có cơ chế hỗ trợ phù hợp đối với các địa phương còn khó khăn, nhằm bảo đảm tính đồng bộ và bền vững trong quá trình xây dựng chính quyền số cấp tỉnh ở Việt Nam hiện nay.

3.1.2.3. Về xây dựng và khai thác dữ liệu số trong xây dựng chính quyền số cấp tỉnh

Trong quá trình xây dựng chính quyền số cấp tỉnh, dữ liệu số ngày càng được xác định là nguồn lực quan trọng, giữ vai trò nền tảng cho hoạt động quản lý, điều hành và cung cấp dịch vụ công. Thực tiễn triển khai tại các địa phương ở nước ta cho thấy, công tác xây dựng và khai thác dữ liệu số đã được quan tâm và từng bước triển khai trong những năm gần đây.

Nhiều địa phương đã chú trọng xây dựng các cơ sở dữ liệu chuyên ngành trong các lĩnh vực như dân cư, đất đai, tài nguyên - môi trường, y tế, giáo dục, tài chính và an sinh xã hội; đồng thời từng bước kết nối, chia sẻ với các cơ sở dữ liệu quốc gia theo lộ trình chung. Việc hình thành các cơ sở dữ liệu này góp phần phục vụ công tác quản lý nhà nước, hỗ trợ quá trình giải quyết thủ tục hành chính và nâng cao chất lượng cung cấp dịch vụ công tại cấp tỉnh.

Bên cạnh đó, tại một số tỉnh, thành phố, kho dữ liệu dùng chung cấp tỉnh đã được hình thành và bước đầu đưa vào khai thác, phục vụ công tác chỉ đạo, điều hành của chính quyền địa phương, cũng như hỗ trợ cung cấp dịch vụ công trực tuyến. Điển hình như tại Thành phố Hồ Chí Minh, việc hình thành và khai thác kho dữ liệu dùng chung đã được thể chế hóa khá sớm thông qua Quyết định số 5086/QĐ-UBND, ngày 28/11/2019 ban hành Quy chế tích hợp, quản lý, vận hành, khai thác Kho dữ liệu dùng chung của thành phố. Quyết định này đã tạo khung pháp lý cho hoạt động kết nối, chia sẻ và sử dụng dữ liệu giữa các cơ quan nhà nước. Trên cơ sở đó, Cổng dữ liệu của thành phố được xác định là nơi khai thác tập trung kho dữ liệu dùng chung, phục vụ nhu cầu chia sẻ, khai thác dữ liệu và hỗ trợ cung cấp dịch vụ công trực tuyến. Hoặc như tỉnh Ninh Bình, hạ tầng dữ liệu phục vụ chính quyền số được triển khai theo hướng hình thành hệ sinh thái dữ liệu mở và kho dữ liệu dùng chung. Các văn bản, kế hoạch của tỉnh ghi nhận Cổng dữ liệu mở (data.ninhbinh.gov.vn) đã được đưa vào khai thác và giai đoạn 1 kho dữ liệu dùng chung đã hoàn thành với các chức năng cơ bản, tiếp tục mở rộng, tạo nền tảng cho tích hợp, chia sẻ dữ liệu liên ngành phục

vụ chỉ đạo, điều hành và dịch vụ công trực tuyến. Đặc biệt, hệ thống eCabinet được mô tả là “mắt xích” trong hệ sinh thái dữ liệu số của tỉnh nhờ kết nối, tích hợp và chia sẻ dữ liệu với kho dữ liệu dùng chung qua LGSP, góp phần chuyển dần sang điều hành dựa trên dữ liệu...[116]. Nói cách khác, việc xây dựng kho dữ liệu dùng chung giúp tạo điều kiện cho việc tổng hợp, phân tích thông tin liên ngành, từng bước chuyển từ quản lý theo quy trình sang quản lý dựa trên dữ liệu.

Tuy nhiên, những hạn chế trong xây dựng và khai thác dữ liệu số vẫn còn khá phổ biến. Tình trạng dữ liệu phân tán ở nhiều sở, ngành, thiếu liên thông, chuẩn hóa chưa đồng bộ; chất lượng dữ liệu chưa cao, thiếu tính đầy đủ và chính xác; cùng với việc cập nhật dữ liệu còn chậm so với yêu cầu thực tiễn đã ảnh hưởng trực tiếp đến hiệu quả vận hành chính quyền số cấp tỉnh.

Bên cạnh đó, các tỉnh đã thiết lập và vận hành LGSP làm nền tảng tích hợp, chia sẻ dữ liệu cấp tỉnh kết nối với Trục NDXP quốc gia, bước đầu loại bỏ các khoảng trống thông tin, cắt giảm thủ tục giấy tờ và nâng cao hiệu quả quản trị hành chính công tại địa phương. Tuy nhiên, điểm nghẽn lớn nhất là nguy cơ lạm dụng, vượt mục đích ban đầu (Function Creep) ở mức cao. Việc chia sẻ dữ liệu qua LGSP giữa các sở, ban, ngành và cấp xã, phường chủ yếu tuân theo yêu cầu nghiệp vụ hành chính, nhưng thiếu cơ chế kiểm soát mục đích sử dụng. Cán bộ công quyền có thể dễ dàng truy cập, tra cứu rộng hơn phạm vi cần thiết để giải quyết một thủ tục cụ thể. Có xung đột giữa “Tối ưu hóa quản lý” và “Kiểm soát quyền lực dữ liệu”, biểu hiện ở việc thiếu cơ chế phân quyền chi tiết và quy chế trách nhiệm cụ thể của người đứng đầu khi cho phép chia sẻ dữ liệu liên ngành, dẫn đến rủi ro “rò rỉ từ bên trong” (insider threat) chưa được kiểm soát triệt để bằng thể chế công vụ.

Những tồn tại, hạn chế này không chỉ làm giảm khả năng khai thác, tái sử dụng dữ liệu nói chung và DLCN nói riêng trong quản lý, điều hành, mà còn hạn chế việc phát triển các dịch vụ công dựa trên dữ liệu, đặt ra yêu cầu cấp thiết phải tiếp tục hoàn thiện cơ chế quản trị dữ liệu và nâng cao năng lực tổ chức thực hiện tại địa phương.

3.1.2.4. Về cung cấp dịch vụ công trực tuyến và cải cách thủ tục hành chính

Cung cấp dịch vụ công trực tuyến và cải cách thủ tục hành chính là nội dung trọng tâm, thể hiện trực tiếp mức độ phát triển của chính quyền số cấp tỉnh. Trong những năm qua, các địa phương đã có nhiều nỗ lực trong việc ứng dụng công nghệ số nhằm đổi mới phương thức giải quyết thủ tục hành chính, nâng cao chất lượng phục vụ người dân và doanh nghiệp.

Thực tiễn cho thấy, hầu hết các tỉnh, thành phố trực thuộc Trung ương đã xây dựng và vận hành Cổng dịch vụ công cấp tỉnh, đồng thời thực hiện tích hợp, kết nối

với Công Dịch vụ công quốc gia. Tỷ lệ thủ tục hành chính được cung cấp trực tuyến, đặc biệt là dịch vụ công trực tuyến mức độ cao, ngày càng tăng. Việc triển khai dịch vụ công trực tuyến đã góp phần rút ngắn thời gian giải quyết thủ tục, giảm chi phí tuân thủ, tăng cường tính công khai, minh bạch và hạn chế tiếp xúc trực tiếp trong quá trình giải quyết công việc hành chính. Bên cạnh đó, nhiều địa phương đã gắn việc cung cấp dịch vụ công trực tuyến với tái cấu trúc quy trình thủ tục hành chính, từng bước chuyển từ phương thức xử lý thủ công sang xử lý điện tử, hướng tới mô hình giải quyết thủ tục hành chính “toàn trình”. Một số tỉnh đã triển khai tiếp nhận, xử lý hồ sơ trên môi trường điện tử gắn với số hóa hồ sơ, kết quả giải quyết thủ tục hành chính, tạo tiền đề cho việc tái sử dụng dữ liệu trong giải quyết các thủ tục liên thông. Điển hình như tại Quảng Ninh, việc tiếp nhận và giải quyết thủ tục hành chính trên môi trường điện tử được gắn chặt với số hóa hồ sơ và trả kết quả điện tử thông qua Hệ thống thông tin giải quyết thủ tục hành chính và Trung tâm Phục vụ hành chính công tỉnh Quảng Ninh. Theo thông tin công bố, tỷ lệ số hóa hồ sơ, kết quả giải quyết thủ tục hành chính đạt 97,54%, đồng thời tỷ lệ khai thác, sử dụng lại dữ liệu đạt 95,64% [115], qua đó cho thấy nền tảng dữ liệu đã được hình thành và bước đầu hỗ trợ cơ chế tái sử dụng dữ liệu trong xử lý thủ tục hành chính, đặc biệt đối với các quy trình có tính liên thông; hoặc tại Đà Nẵng, thành phố đã triển khai số hóa hồ sơ và kết quả giải quyết thủ tục hành chính gắn với hệ thống một cửa điện tử; đồng thời hướng dẫn khai thác “Kho kết quả thủ tục hành chính số” để thay thế một số giấy tờ mà người dân/tổ chức thường phải nộp lại, qua đó tăng khả năng kế thừa và tái sử dụng dữ liệu khi thực hiện dịch vụ công trực tuyến và thủ tục hành chính liên thông.

Tuy nhiên, hiệu quả cung cấp dịch vụ công trực tuyến tại cấp tỉnh vẫn chưa đồng đều giữa các địa phương và giữa các lĩnh vực. Mức độ sử dụng dịch vụ công trực tuyến của người dân và doanh nghiệp còn hạn chế; nhiều thủ tục tuy đã được cung cấp trực tuyến nhưng vẫn yêu cầu nộp bổ sung hồ sơ giấy hoặc thực hiện các khâu đối chiếu thủ công. Trong khi đó, ở không ít trường hợp, dịch vụ công trực tuyến mới dừng lại ở việc số hóa khâu tiếp nhận hồ sơ, chưa thực sự thay thế phương thức giải quyết truyền thống.

Bên cạnh đó, người dân bước đầu được bảo đảm “Quyền được biết” ở khía cạnh công khai danh mục thủ tục hành chính, thành phần hồ sơ và kết quả xử lý dịch vụ công. Tuy nhiên, điểm nghẽn nghiêm trọng nhất là thiếu vắng hoàn toàn giao diện quản lý quyền của chủ thể dữ liệu. Công dịch vụ công cấp tỉnh hiện nay mới chỉ phục vụ chiều thu thập dữ liệu của cơ quan nhà nước, hoàn toàn thiếu hụt các tính năng kỹ thuật hỏi đáp để người dân thực thi đầy đủ 6 quyền được hiến định và luật định (quyền truy cập, xem lịch sử khai thác dữ liệu của mình, quyền chỉnh sửa, quyền xóa/quên,

quyền hạn chế xử lý, quyền phản đối và quyền rút lại sự đồng ý). Người dân không thể biết dữ liệu cá nhân của mình sau khi nộp vào hệ thống đã được chia sẻ cho những cơ quan nào, nhằm mục đích gì và ai đã tra cứu. Cơ chế hỗ trợ pháp lý khi có sự cố rò rỉ dữ liệu tại địa phương còn mang tính thủ tục hành chính truyền thống, thiếu cơ chế tự động cảnh báo rủi ro đến chủ thể dữ liệu.

Những hạn chế nêu trên cho thấy, cải cách thủ tục hành chính gắn với chuyển đổi số ở cấp tỉnh chưa đạt được tính toàn diện và thực chất, còn chịu tác động bởi nhiều yếu tố như chất lượng hạ tầng số, mức độ liên thông dữ liệu, năng lực vận hành của đội ngũ cán bộ, công chức và thói quen sử dụng dịch vụ của người dân. Điều này đặt ra yêu cầu tiếp tục hoàn thiện quy trình, nâng cao chất lượng dịch vụ công trực tuyến và thúc đẩy cải cách thủ tục hành chính theo hướng lấy người dân, doanh nghiệp làm trung tâm trong xây dựng chính quyền số cấp tỉnh.

3.1.2.5. Về tổ chức bộ máy và nguồn nhân lực trong xây dựng chính quyền số cấp tỉnh

Tổ chức bộ máy và nguồn nhân lực là điều kiện bảo đảm mang tính quyết định đối với hiệu quả xây dựng và vận hành chính quyền số cấp tỉnh. Thực tiễn triển khai cho thấy, trong những năm gần đây, các địa phương đã từng bước kiện toàn cơ chế tổ chức, phân công trách nhiệm và bố trí lực lượng phục vụ chuyển đổi số trong khu vực công.

Trước hết, về tổ chức bộ máy, đa số tỉnh, thành phố đã xác định rõ đầu mối tham mưu, quản lý nhà nước về chuyển đổi số (thường là cơ quan chuyên môn về thông tin và truyền thông hoặc bộ phận chuyên trách trong văn phòng UBND), đồng thời thành lập hoặc kiện toàn các ban chỉ đạo, tổ công tác chuyển đổi số nhằm tăng cường vai trò điều phối liên ngành. Cùng với đó, một số địa phương đã bước đầu hình thành cơ chế phối hợp giữa các sở, ngành trong triển khai hạ tầng số, nền tảng số, dịch vụ công trực tuyến và quản trị dữ liệu, qua đó tạo nền tảng tổ chức cho việc triển khai nhiệm vụ theo hướng đồng bộ.

Tuy nhiên, cơ cấu tổ chức phục vụ chính quyền số ở nhiều địa phương vẫn còn biểu hiện phân tán theo ngành, lĩnh vực; cơ chế điều phối liên thông chưa thực sự hiệu quả, dẫn đến tình trạng “mạnh ai nấy làm”, thiếu thống nhất về chuẩn dữ liệu, chuẩn kỹ thuật và quy trình vận hành hệ thống. Ở một số tỉnh, vai trò đầu mối điều phối chưa được trao đủ thẩm quyền hoặc chưa có cơ chế ràng buộc trách nhiệm giữa các cơ quan chuyên môn, làm giảm hiệu lực quản trị và tính nhất quán trong quá trình triển khai.

Về nguồn nhân lực, các địa phương đã quan tâm đào tạo, bồi dưỡng kỹ năng số cho đội ngũ cán bộ, công chức; từng bước triển khai các chương trình tập huấn về

sử dụng hệ thống thông tin giải quyết thủ tục hành chính, vận hành cổng dịch vụ công, số hóa hồ sơ, khai thác dữ liệu và bảo đảm an toàn thông tin. Một số địa phương có điều kiện đã chủ động thu hút nhân lực CNTT, hình thành bộ phận kỹ thuật vận hành hạ tầng và nền tảng số, góp phần nâng cao năng lực triển khai và duy trì hoạt động của chính quyền số.

Tuy nhiên, khó khăn hiện nay trong xây dựng chính quyền số cấp tỉnh là tình trạng thiếu hụt nhân lực chất lượng cao về CNTT trong khu vực công, đặc biệt ở cấp cơ sở và tại các tỉnh, địa phương còn khó khăn. Khảo sát thực chứng đối với 100 cán bộ, công chức trực tiếp vận hành Cổng dịch vụ công và Hệ thống thông tin giải quyết TTHC tại 03 tỉnh, thành phố (Hà Nội, Nghệ An, Đắk Lắk) cho thấy sự thiếu hụt nghiêm trọng về năng lực bảo vệ dữ liệu cá nhân theo tinh thần Nghị định 13/2023/NĐ-CP và Luật Bảo vệ dữ liệu cá nhân: (1) Về đào tạo chuyên môn: Có tới 68,5% công chức phản hồi “chưa từng tham gia bất kỳ khóa tập huấn chuyên sâu nào” về quy trình kỹ thuật và nghĩa vụ pháp lý trong bảo vệ dữ liệu cá nhân (chủ yếu mới dừng lại ở các lớp bồi dưỡng CNTT hoặc An toàn thông tin chung). (2) Về nhận thức ranh giới công vụ: 72% cán bộ cho rằng “chỉ cần hệ thống không bị ngắt kết nối hay bị hacker tấn công là đã bảo đảm an toàn”, hoàn toàn chưa nhận thức được hành vi tự ý tra cứu, sao chép dữ liệu công dân không phục vụ TTHC trực tiếp là hành vi vi phạm pháp luật. (3) Về xử lý sự cố: Chỉ có 14,5% cán bộ nắm rõ quy trình báo cáo sự cố lộ lọt dữ liệu cho Cục An toàn thông tin hoặc cơ quan chuyên trách trong vòng 72 giờ theo quy định. Bên cạnh đó, năng lực số và tư duy số hóa của một bộ phận cán bộ, công chức còn chưa theo kịp yêu cầu chuyển đổi mô hình quản trị từ thủ công sang dựa trên dữ liệu và quy trình số; kỹ năng vận hành, khai thác hệ thống còn hạn chế, dẫn đến hiệu quả ứng dụng công nghệ chưa tương xứng với mức độ đầu tư. Ở một số địa phương vẫn còn tình trạng phụ thuộc vào đơn vị cung cấp giải pháp trong vận hành, bảo trì, nâng cấp hệ thống, dẫn đến những rủi ro tiềm ẩn về tính chủ động kỹ thuật, tính liên tục của dịch vụ và an toàn thông tin đối với dữ liệu.

Tính đến hết năm 2025 và sang đầu năm 2026, quá trình xây dựng chính quyền số cấp tỉnh ở Việt Nam đã đạt được những tiến bộ rõ rệt nhưng chưa đồng đều giữa các địa phương. Cụ thể:

Trước hết, về kết quả đo lường và đánh giá tổng thể, giai đoạn 2020 - 2025 ghi nhận sự cải thiện rõ rệt của Việt Nam trong các chỉ số phản ánh mức độ phát triển chính quyền điện tử và chính quyền số. Trên phương diện quốc tế, theo Báo cáo khảo sát Chính phủ điện tử của Liên Hợp Quốc, Việt Nam đã tăng 15 bậc trong Chỉ số phát triển Chính phủ điện tử (EGDI) năm 2024, xếp thứ 71/193 quốc gia và được xếp vào nhóm các quốc gia có chỉ số EGDI ở mức “rất cao”. Kết quả này phản ánh xu hướng tích cực trong việc hoàn thiện hạ tầng số, dịch vụ công trực tuyến và năng lực thể chế

của khu vực công. Điều này tạo điều kiện thuận lợi để chính quyền tích hợp các giải pháp bảo mật nâng cao (mã hóa, giám sát an toàn thông tin 4 lớp, xác thực VNeID) và thực thi các quy trình kỹ thuật phục vụ quyền của công dân (như tra cứu, cập nhật dữ liệu) một cách đồng bộ, chính xác hơn so với quản lý thủ công (bản giấy). Tuy nhiên, mức độ số hóa càng cao không đồng nghĩa với việc quyền dữ liệu cá nhân được bảo đảm tốt hơn, thậm chí còn làm gia tăng nguy cơ xâm phạm quyền riêng tư nếu năng lực bảo vệ không phát triển tương xứng. Số hóa triệt để và tích hợp dữ liệu quy mô lớn (Big Data/Cloud) làm gia tăng tập trung dữ liệu nhạy cảm của hàng triệu công dân vào các Trung tâm dữ liệu. Sự cô lập từ đây sẽ gây hậu quả dây chuyền nghiêm trọng gấp nhiều lần rò rỉ hồ sơ giấy thông thường. Hạ tầng số phát triển giúp chính quyền thu thập, chia sẻ và kết nối dữ liệu dễ dàng hơn. Nếu thiếu cơ chế kiểm soát truy cập (Zero Trust/Least Privilege) và thiếu quy định bồi thường trong các hợp đồng dịch vụ Cloud với bên thứ ba, nguy cơ dữ liệu bị làm quyền lạm quyền (cán bộ tra cứu) hoặc bị thương mại hóa trái phép sẽ gia tăng tương ứng.

Ở góc độ trong nước, Chỉ số chuyển đổi số (DTI) quốc gia tiếp tục được cải thiện qua các năm. Theo công bố của Bộ Khoa học và Công nghệ, Chỉ số chuyển đổi số (DTI) của nước ta năm 2024 đạt 0,7955, tăng khoảng 8,6% so với năm 2023. Chỉ số chuyển đổi số cho thấy sự phân hóa đáng kể giữa các tỉnh, thành phố. Trong các bảng xếp hạng DTI giai đoạn 2023 - 2024, nhóm địa phương dẫn đầu thường xuyên bao gồm Đà Nẵng, Thành phố Hồ Chí Minh, Thừa Thiên Huế, Hà Nội, Hải Phòng, Thanh Hóa, trong khi nhiều địa phương khác duy trì ở mức trung bình hoặc thấp [9]. Điều này cho thấy chính quyền số cấp tỉnh đã trở thành một lĩnh vực có thể đo lường và so sánh, song khoảng cách về năng lực triển khai, nguồn lực và mức độ sẵn sàng giữa các địa phương vẫn tồn tại, tạo nên bức tranh không đồng đều trong xây dựng chính quyền số [8]. Sự phân hóa DTI giữa các địa phương lại đặt ra nguy cơ phân mảnh và bất bình đẳng trong việc bảo đảm quyền dữ liệu cá nhân của công dân. Việc liên thông dữ liệu giữa tỉnh có hạ tầng bảo mật cao (nhóm dẫn đầu) với tỉnh có hạ tầng yếu kém (nhóm DTI thấp) biến các tỉnh yếu hơn thành “lỗ hổng hệ thống” đe dọa an toàn dữ liệu toàn quốc. Do đó, nếu việc đánh giá DTI chỉ tập trung vào tỷ lệ số hóa mà thiếu đi chỉ báo đo lường mức độ tuân thủ pháp luật bảo vệ dữ liệu cá nhân, thì sự cải thiện DTI sẽ vô hình trung gia tăng rủi ro lộ lọt dữ liệu trên diện rộng.

Thứ hai, về dịch vụ công trực tuyến và định danh số, giai đoạn 2020 - 2025 có sự mở rộng nhanh chóng của hệ thống dịch vụ công số cả về thủ tục lẫn quy mô sử dụng. Cổng Dịch vụ công Quốc gia của Việt Nam từng bước tích hợp hàng nghìn thủ tục hành chính, trong đó riêng năm 2025 đã xử lý khoảng 11,5 triệu hồ sơ trực tuyến. Song song với đó, hệ thống định danh điện tử VNeID được triển khai trên phạm vi toàn quốc, với

khoảng 67 triệu tài khoản định danh số theo số liệu quản lý nhà nước, phản ánh sự gia tăng nhanh về tiếp cận định danh số của người dân [6]. Điều này tạo nền tảng quan trọng cho việc cá nhân hóa dịch vụ công, tái sử dụng dữ liệu và giảm giấy tờ hành chính. Tuy nhiên, điều này đồng thời làm gia tăng mức độ dễ bị tổn thương của quyền dữ liệu cá nhân ở quy mô toàn quốc. Việc tập trung hóa thông tin nhân thân của 67 triệu người dân vào một hệ thống duy nhất vô hình trung tạo ra rủi ro hệ thống đặc biệt nghiêm trọng nếu xảy ra sự cố an toàn thông tin. Do đó, nếu tiến trình số hóa dịch vụ công trực tuyến chỉ tập trung vào chỉ tiêu “tái sử dụng dữ liệu” và “tăng số lượng hồ sơ” mà bỏ qua việc trao công cụ kỹ thuật cho công dân tự kiểm soát quyền (như tính năng rút lại sự đồng ý, xem nhật ký tra cứu công vụ trên VNeID), thì sự mở rộng quy mô dịch vụ công trực tuyến sẽ vô hình trung biến người dân thành chủ thể thụ động, bị tước bỏ quyền tự quyết đối với dữ liệu cá nhân của chính mình.

Tuy nhiên, xét ở khía cạnh mức độ sử dụng thực chất, quá trình chuyển dịch sang môi trường số vẫn chưa đạt kết quả cao. Theo thống kê, riêng tháng 10/2025, tỷ lệ hồ sơ được giải quyết hoàn toàn trực tuyến trên tổng số hồ sơ thủ tục hành chính đạt khoảng 39,98%. Kết quả này cho thấy, mặc dù xu hướng sử dụng dịch vụ công trực tuyến gia tăng, mức độ sử dụng thực tế vẫn phụ thuộc đáng kể vào tính dễ sử dụng và mức độ thuận tiện của quy trình nghiệp vụ, năng lực liên thông dữ liệu, mức độ tích hợp thanh toán số, cũng như thói quen của người dân, doanh nghiệp. Một số địa phương đã phát triển hơn theo mô hình tiếp nhận trực tuyến toàn bộ danh mục thủ tục hành chính được phê duyệt (điển hình tại Thành phố Hà Nội triển khai từ tháng 9/2025), song việc mở rộng mô hình này đồng thời đặt ra yêu cầu cao hơn về năng lực quản trị dữ liệu và bảo đảm an toàn thông tin ở cấp tỉnh [6].

Từ thực trạng nêu trên có thể nhận thấy rằng, Việt Nam đã đạt được những bước tiến đáng kể trong xây dựng chính quyền số cấp tỉnh giai đoạn 2020 - 2025, đặc biệt về hạ tầng cung ứng dịch vụ công trực tuyến và định danh số. Tuy nhiên, quá trình này hiện vẫn chủ yếu tập trung vào số hóa thủ tục và mở rộng nền tảng, trong khi yêu cầu tái xây dựng quản trị dựa trên dữ liệu, gắn với bảo đảm quyền đối với DLCN và trách nhiệm giải trình, chưa được thực hiện đầy đủ và đồng đều ở các địa phương.

Sự bùng nổ về quy mô và tính chất nhạy cảm của dữ liệu cá nhân tại chính quyền cấp tỉnh thời gian qua vừa là thành tựu lớn của chuyển đổi số, đồng thời cũng là nguồn rủi ro pháp lý cực lớn đối với quyền con người.

Một mặt, nó giúp chính quyền tỉnh tỉnh gọn bộ máy, ra quyết định quản trị dựa trên dữ liệu và cung cấp dịch vụ công nhanh chóng. Mặt khác, khi một kho dữ liệu chứa đựng toàn bộ bí mật đời tư của hàng triệu công dân (từ sức khỏe, tài sản đến di

chuyên) được tập trung và liên thông liên tục, nó sẽ trở thành mục tiêu hấp dẫn cho các cuộc tấn công mạng, hoặc dễ dàng bị xâm phạm do sự bất cẩn, lạm dụng quyền tra cứu của đội ngũ cán bộ, công chức cấp cơ sở. Đây chính là lý do vì sao việc thiết lập các phương thức bảo vệ quyền dữ liệu cá nhân tại địa phương trở thành một yêu cầu cấp bách hơn bao giờ hết.

3.1.3. Nhận diện các nguy cơ, thách thức đối với quyền dữ liệu cá nhân trong môi trường số cấp tỉnh

Sự bùng nổ về quy mô tích tụ, tần suất khai thác và tính chất kết nối liên thông của DLCN tại chính quyền cấp tỉnh trong giai đoạn qua là một bước tiến lớn về mặt công nghệ quản trị. Tuy nhiên, dưới góc độ khoa học an ninh mạng hệ thống và lý thuyết quyền con người, tiến trình này đồng thời đặt quyền và lợi ích hợp pháp của chủ thể dữ liệu trước những rủi ro mang tính hệ thống. Qua nghiên cứu thực tiễn triển khai hành chính số, các nguy cơ và thách thức đối với quyền DLCN trong môi trường số cấp tỉnh hiện nay được nhận diện cụ thể qua 04 nhóm vấn đề cốt lõi sau đây:

Thứ nhất, nguy cơ từ sự lạm dụng quyền hạn công vụ và “lỗ hổng nhân sự” nội bộ; đây là nguy cơ xuất phát từ yếu tố con người bên trong bộ máy công quyền địa phương, thuộc nhóm rủi ro nội tại thường trực và khó kiểm soát nhất.

(1). Rủi ro từ việc “vượt cấp quyền hạn” (*Over-privileged Access*): Khi các cơ sở dữ liệu chuyên ngành (dân cư, đất đai, hộ tịch, y tế) được liên thông về Kho dữ liệu dùng chung của tỉnh, diện chủ thể được cấp tài khoản và quyền truy cập mở rộng một cách cơ học từ cấp sở đến cấp xã. Thực tế ghi nhận hiện tượng cán bộ, công chức tự ý tra cứu, khai thác thông tin của công dân vì mục đích cá nhân (kiểm tra nhân thân, tìm hiểu đời tư đối tác, người quen) mà không có yêu cầu hay lý do công vụ chính đáng. Hành vi này trực tiếp xâm phạm quyền tự quyết thông tin, nhưng hệ thống quản trị hành chính chưa có bộ lọc ngăn chặn tự động.

(2). Hạn chế trong nhận thức về an toàn số của đội ngũ thực thi cơ sở: Tại cấp xã, phường, ý thức về bảo mật DLCN của một bộ phận công chức chuyên trách còn rất hạn chế. Hiện tượng chụp ảnh màn hình chứa thông tin định danh công dân, chia sẻ tự do các tệp tin dữ liệu thô qua các ứng dụng OTT không mã hóa đầu cuối (Zalo, Viber) phục vụ trao đổi công việc diễn ra phổ biến. Nghiêm trọng hơn, việc lỏng lẻo trong quản lý tài khoản tạo kẽ hở cho các hành vi trục lợi, bắt tay với các đối tượng bên ngoài (môi giới bất động sản, bảo hiểm, tài chính) để tuồn dữ liệu thô ra ngoài thị trường đen.

Thứ hai, thách thức từ sự bất cập, phân mảnh của hạ tầng công nghệ và các hình thức tấn công mạng chuyên sâu. Hạ tầng kỹ thuật của chính quyền số cấp tỉnh hiện nay đang phải đối mặt với các thách thức an ninh công nghệ mang tính cấu trúc.

(1). Sự phân mảnh và các “điểm mù” giao tiếp hệ thống: Hệ thống thông tin giải quyết thủ tục hành chính, Trung tâm điều hành thông minh (IOC) và các cơ sở dữ liệu chuyên ngành phần lớn được xây dựng qua nhiều giai đoạn, bởi nhiều nhà thầu kỹ thuật khác nhau. Sự thiếu đồng bộ về mặt kiến trúc công nghệ tạo ra các “lỗ hổng kỹ thuật” tại các giao diện lập trình ứng dụng (API). Đây chính là các điểm mù mà tin tặc có thể khai thác để thực hiện hành vi tấn công chiếm quyền điều khiển hoặc trích xuất dữ liệu hàng loạt.

(2). Nguy cơ từ các chiến dịch tấn công có chủ đích (APT) và mã độc tống tiền (Ransomware): Hệ thống thông tin của chính quyền cấp tỉnh ngày càng trở thành mục tiêu trọng điểm của tội phạm công nghệ cao. Các cuộc tấn công mã hóa dữ liệu trái phép nhằm vào các kho dữ liệu nhạy cảm, như hồ sơ bệnh án điện tử, dữ liệu học bạ học sinh, thông tin mã số thuế cá nhân... nhằm mục đích tống tiền, bôi nhọ hoặc thao túng thông tin đang gia tăng cả về tần suất lẫn phương thức tinh vi, đe dọa trực tiếp đến tính toàn vẹn và bảo mật của dữ liệu công dân.

Thứ ba, nguy cơ "thương mại hóa dữ liệu ngầm" trong mô hình thuê ngoài dịch vụ công nghệ với bên thứ ba. Mối quan hệ giữa chính quyền địa phương và các doanh nghiệp công nghệ trong quá trình số hóa đang bộc lộ những rủi ro lớn về mặt kiểm soát chủ quyền dữ liệu.

(1). Sự bất đối xứng về mặt năng lực công nghệ: Do giới hạn về biên chế và trình độ chuyên môn của đội ngũ công chức CNTT tại địa phương, đại đa số các tỉnh hiện nay đều áp dụng mô hình “thuê dịch vụ công nghệ văn phòng số” từ các tập đoàn tư nhân. Hệ quả là toàn bộ quyền quản trị tối cao (Root access), quy trình bảo trì hệ thống và kiểm soát mã nguồn phần lớn bị phụ thuộc vào đội ngũ kỹ sư của doanh nghiệp.

(2). Rủi ro chiếm dụng dữ liệu và sao lưu thứ cấp: Mặc dù các hợp đồng kinh tế đều có điều khoản cam kết bảo mật, nhưng chính quyền cấp tỉnh hoàn toàn thiếu công cụ kỹ thuật và cơ chế pháp lý để kiểm tra, giám sát xem doanh nghiệp có thực hiện hành vi “sao lưu ngầm” dữ liệu của người dân hay không. Khối dữ liệu này có rủi ro bị sử dụng trái phép để làm giàu cho các mô hình trí tuệ nhân tạo (AI) riêng hoặc chuyển giao cho các công ty con kinh doanh thương mại, tạo ra nguy cơ thất thoát dữ liệu quy mô lớn dưới danh nghĩa hợp tác kỹ thuật.

Thứ tư, nguy cơ xâm phạm đời tư từ việc ứng dụng các công nghệ giám sát đô thị thông minh diện rộng. Việc hiện đại hóa quản trị đô thị thông qua các công nghệ thu thập dữ liệu sinh trắc học đang đặt ra thách thức gay gắt đối với quyền riêng tư hiến định.

(1). Sự bùng nổ của hệ thống Camera AI nhận diện khuôn mặt: Trong khuôn khổ các đề án Đô thị thông minh (Smart City), các địa phương đã đồng loạt lắp đặt hàng ngàn camera giám sát thông minh tại các tuyến đường trục và không gian công cộng. Công nghệ này liên tục quét, thu thập và phân tích dữ liệu sinh trắc học (đặc điểm khuôn mặt, hành vi, biển số xe, lịch trình di chuyển) của mọi công dân theo thời gian thực.

(2). Sự thiếu vắng căn cứ pháp lý kiểm soát công nghệ: Nguy cơ lớn nhất hiện nay là việc vận hành hệ thống này chưa có hành lang pháp lý ở tầm luật quy định chi tiết. Các câu hỏi cốt lõi về mặt quyền con người: Hệ thống được phép thu thập dữ liệu của ai? Thời hạn lưu trữ tối đa là bao lâu? Cơ quan nào được quyền trích xuất dữ liệu di chuyển của công dân? vẫn chưa được phân định rõ ràng. Sự tùy tiện trong trích xuất dữ liệu camera phục vụ mục đích ngoài an ninh công cộng đang đe dọa trực tiếp đến quyền bất khả xâm phạm về đời sống riêng tư và quyền tự quyết trên không gian mạng của cá nhân.

Tóm lại, tất cả các nguy cơ và thách thức nêu trên tựu trung đều phản ánh một hiện tượng xã hội học pháp luật: “Sự bất đối xứng quyền lực dữ liệu”. Trong bối cảnh chính quyền cấp tỉnh đang được trao cơ chế tối đa hóa việc thu thập dữ liệu để phục vụ mục tiêu quản lý và phát triển kinh tế, thì các công cụ pháp lý để người dân thực hiện quyền tự vệ (quyền rút lại sự đồng ý, quyền yêu cầu xóa dữ liệu, quyền truy cập kiểm tra việc dữ liệu của mình được chuyển đến đâu) trên thực tế lại rất yếu và mang tính hình thức. Người dân gần như ở thế “buộc phải chấp nhận rủi ro và cung cấp dữ liệu” nếu muốn tiếp cận các dịch vụ công thiết yếu của Nhà nước. Đây chính là vấn đề cốt lõi nhất cần phải giải quyết bằng các giải pháp đột phá về thể chế bảo đảm.

3.2. THỰC TRẠNG TRIỂN KHAI CÁC NỘI DUNG, PHƯƠNG THỨC BẢO VỆ QUYỀN ĐỐI VỚI DỮ LIỆU CÁ NHÂN TRONG XÂY DỰNG CHÍNH QUYỀN SỐ CẤP TỈNH Ở VIỆT NAM

3.2.1. Thực trạng quy định của pháp luật bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh ở Việt Nam

3.2.1.1. Thực trạng quy định về nội dung quyền đối với dữ liệu cá nhân

Trong bối cảnh chuyển đổi số và sự phát triển mạnh mẽ của CNTT, DLCN ngày càng trở thành một nguồn lực quan trọng, đồng thời cũng là đối tượng dễ bị xâm phạm, khai thác và lạm dụng. Quyền đối với DLCN vì vậy dần được nhìn nhận như một bộ phận cấu thành của QCN, gắn với quyền riêng tư, quyền bất khả xâm phạm về đời sống cá nhân và quyền được bảo vệ nhân phẩm, danh dự của mỗi cá nhân. Trên phương diện lý luận QCN, quyền đối với DLCN không chỉ mang ý nghĩa bảo vệ cá nhân trước sự can thiệp tùy tiện của Nhà nước và các chủ thể khác, mà còn thể

hiện yêu cầu trao cho cá nhân khả năng kiểm soát thông tin về chính mình trong môi trường số hóa.

Ở Việt Nam, mặc dù thuật ngữ “*dữ liệu cá nhân*” chỉ mới được chuẩn hóa và quy định tương đối hệ thống trong giai đoạn gần đây, song các nền tảng pháp lý cho việc bảo vệ quyền đối với DLCN đã được hình thành từ sớm. Hiến pháp năm 2013, thông qua việc ghi nhận quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân, bí mật gia đình, đồng thời bảo đảm quyền bảo vệ danh dự và nhân phẩm, đã xác lập cơ sở hiến định quan trọng cho sự phát triển của hệ thống quy phạm bảo vệ dữ liệu cá nhân. Trên nền tảng đó, nhiều đạo luật chuyên ngành như Bộ luật Dân sự, Luật An ninh mạng, Luật Bảo vệ quyền lợi người tiêu dùng và các văn bản có liên quan đã từng bước cụ thể hóa những yêu cầu pháp lý đối với việc thu thập, xử lý, sử dụng và bảo vệ thông tin và DLCN. Tuy nhiên, các quy định này còn phân tán, thiếu thống nhất, dẫn đến hạn chế nhất định về tính đồng bộ và hiệu lực thực thi.

Nghị định số 13/2023/NĐ-CP là bước ngoặt trong hoạt động hoàn thiện pháp luật Việt Nam về bảo vệ DLCN, trong đó quyền của chủ thể DLCN được xác định rõ ràng như một trụ cột trung tâm. Tuy nhiên, là một văn bản dưới luật, Nghị định 13/2023/NĐ-CP vẫn mang những giới hạn nhất định về hiệu lực pháp lý và tính ổn định lâu dài. Vì vậy, Luật Bảo vệ dữ liệu cá nhân năm 2025 đã kế thừa và phát triển các nội dung cốt lõi của Nghị định 13/2023/NĐ-CP, trong đó Điều 4 ghi nhận một cách có hệ thống các quyền của chủ thể DLCN, gồm:

- “a) Được biết về hoạt động xử lý DLCN;*
- b) Đồng ý hoặc không đồng ý, yêu cầu rút lại sự đồng ý cho phép xử lý DLCN;*
- c) Xem, chỉnh sửa hoặc yêu cầu chỉnh sửa DLCN;*
- d) Yêu cầu cung cấp, xóa, hạn chế xử lý DLCN; gửi yêu cầu phản đối xử lý DLCN;*
- đ) Khiếu nại, tố cáo, khởi kiện, yêu cầu bồi thường thiệt hại theo quy định của pháp luật;*
- e) Yêu cầu cơ quan có thẩm quyền hoặc cơ quan, tổ chức, cá nhân liên quan đến xử lý DLCN thực hiện các biện pháp, giải pháp bảo vệ DLCN của mình theo quy định của pháp luật”.*

Đồng thời, Chính phủ đã ban hành Nghị định số 356/2025/NĐ-CP quy định chi tiết một số điều và biện pháp thi hành Luật, tạo cơ sở cho việc tổ chức thực thi (mẫu biểu, thủ tục, cơ chế quản lý nhà nước...). Về mặt nội dung, các quyền đối với DLCN cơ bản như quyền được biết, quyền đồng ý, quyền truy cập, chỉnh sửa và yêu cầu xóa dữ liệu... được nhấn mạnh như các quyền trọng tâm của con người đối với DLCN; các cơ chế xử lý vi phạm cũng mang tính răn đe hơn nhằm tạo ra sự bảo vệ

phù hợp cho quyền đối với DLCN. Sự phát triển này không chỉ hoàn thiện khuôn khổ pháp lý về bảo vệ DLCN, mà còn khẳng định rõ hơn vị trí của quyền đối với DLCN như một QCN trong pháp luật Việt Nam hiện đại. Cụ thể như sau:

Thứ nhất, quyền được biết về hoạt động xử lý DLCN.

Theo đó chủ thể dữ liệu có quyền được thông tin về việc DLCN của mình có đang được xử lý hay không, cũng như các yếu tố cơ bản của hoạt động xử lý dữ liệu (điểm a khoản 1 Điều 4). Quy định này thể hiện rõ nguyên tắc minh bạch trong xử lý DLCN, đặt ra nghĩa vụ cho cơ quan, tổ chức, cá nhân xử lý dữ liệu phải cung cấp thông tin đầy đủ, kịp thời và dễ tiếp cận liên quan đến mục đích xử lý, phạm vi dữ liệu được thu thập, chủ thể tham gia xử lý và khả năng chia sẻ dữ liệu cho bên thứ ba. Về bản chất, quyền được biết không chỉ nhằm bảo đảm quyền tiếp cận thông tin của cá nhân, mà còn là tiền đề để chủ thể dữ liệu có thể thực hiện một cách hiệu quả các quyền tiếp theo như quyền đồng ý, quyền phản đối hay quyền yêu cầu xóa, hạn chế xử lý DLCN. Việc ghi nhận quyền được biết phản ánh yêu cầu trao cho cá nhân vị thế chủ động trong quan hệ xử lý dữ liệu, thay vì chỉ là đối tượng bị thu thập thông tin một cách thụ động. Quy định về quyền này đã có tính tương thích với nguyên tắc minh bạch được thừa nhận rộng rãi trong pháp luật bảo vệ dữ liệu quốc tế, đặc biệt là trong Công ước 108+ của Hội đồng châu Âu và các Hướng dẫn về bảo vệ DLCN của OECD, là những nội dung nhấn mạnh nghĩa vụ cung cấp thông tin rõ ràng, dễ hiểu cho cá nhân ngay từ thời điểm thu thập dữ liệu. Việc luật hóa quyền được biết trong Luật Bảo vệ dữ liệu cá nhân năm 2025 là bước phát triển quan trọng, góp phần nội luật hóa các chuẩn mực quốc tế về bảo vệ quyền riêng tư và DLCN tại Việt Nam nói chung và trong quá trình xây dựng chính quyền số cấp tỉnh nói riêng.

Thứ hai, quyền đồng ý hoặc không đồng ý và rút lại sự đồng ý cho phép xử lý DLCN.

Theo đó cá nhân có quyền quyết định việc cho phép hay không cho phép xử lý DLCN của mình, cũng như quyền rút lại sự đồng ý đã được đưa ra trước đó (điểm b khoản 1 Điều 4) [50]. Việc ghi nhận quyền này cho thấy pháp luật nước ta xác định sự đồng ý của chủ thể dữ liệu là một trong những căn cứ pháp lý quan trọng để hợp pháp hóa hoạt động xử lý DLCN, qua đó đặt ý chí của cá nhân vào vị trí trung tâm của cơ chế bảo vệ dữ liệu. Quyền đồng ý không chỉ bao gồm hành vi chấp thuận đơn thuần, mà còn đòi hỏi sự đồng ý đó phải được thể hiện trên cơ sở tự nguyện, có hiểu biết và không bị ép buộc, đồng thời gắn liền với khả năng rút lại sự đồng ý vào bất cứ thời điểm nào khi cá nhân không còn mong muốn tiếp tục việc xử lý dữ liệu.

Quy định này đã có tính tương thích với các chuẩn mực quốc tế về bảo vệ DLCN, đặc biệt là các quy định về căn cứ xử lý dữ liệu và điều kiện của sự đồng ý

trong Quy định bảo vệ dữ liệu chung của Liên minh châu Âu (Điều 6 và Điều 7) [101]. Qua đó, quyền đồng ý và rút lại sự đồng ý phản ánh khuynh hướng pháp quyền hiện đại trong việc bảo đảm cho cá nhân khả năng kiểm soát thực chất đối với dữ liệu riêng tư của chính mình, đồng thời góp phần cân bằng giữa QCN và nhu cầu khai thác, sử dụng dữ liệu trong đời sống kinh tế - xã hội.

Thứ ba, quyền xem, chỉnh sửa hoặc yêu cầu chỉnh sửa DLCN.

Chủ thể dữ liệu có quyền tiếp cận DLCN của mình đang được xử lý và yêu cầu chỉnh sửa khi dữ liệu không chính xác, không đầy đủ hoặc không còn phù hợp với mục đích xử lý (điểm c khoản 1 Điều 4). Quyền này thể hiện rõ nguyên tắc bảo đảm tính chính xác và cập nhật của DLCN, đồng thời khẳng định vai trò chủ động của cá nhân trong việc giám sát chất lượng thông tin liên quan đến bản thân. Quyền xem và chỉnh sửa DLCN là điều kiện cần thiết để bảo đảm các quyền khác của chủ thể dữ liệu được thực hiện một cách hiệu quả, bởi nếu cá nhân không có khả năng tiếp cận và kiểm tra dữ liệu thì việc đồng ý, phản đối hay yêu cầu xóa dữ liệu khó có thể mang ý nghĩa thực chất. Đây cũng là quyền được nhấn mạnh trong các văn bản pháp lý quốc tế như Quy định bảo vệ dữ liệu chung của Liên minh châu Âu. Việc luật hóa quyền xem và chỉnh sửa DLCN trong Luật Bảo vệ dữ liệu cá nhân năm 2025 cho thấy sự tiếp thu có chọn lọc các chuẩn mực quốc tế, đồng thời góp phần củng cố cơ sở pháp lý cho việc bảo vệ QCN trong bối cảnh xử lý dữ liệu ngày càng phổ biến và phức tạp.

Thứ tư, quyền yêu cầu cung cấp, xóa, hạn chế xử lý DLCN và quyền phản đối việc xử lý DLCN.

Theo đó, chủ thể dữ liệu không chỉ có quyền tiếp cận thông tin về DLCN của mình, mà còn có quyền yêu cầu bên xử lý cung cấp dữ liệu, xóa dữ liệu hoặc hạn chế việc xử lý trong những trường hợp nhất định, đồng thời gửi yêu cầu phản đối đối với hoạt động xử lý DLCN (điểm d khoản 1 Điều 4) [50]. Quy định này thể hiện sự mở rộng đáng kể phạm vi kiểm soát của cá nhân đối với vòng đời của DLCN, từ giai đoạn thu thập đến giai đoạn lưu trữ, sử dụng và chia sẻ dữ liệu. Về mặt lý luận, các quyền nêu trên phản ánh nguyên tắc tối thiểu hóa và giới hạn mục đích xử lý dữ liệu, theo đó DLCN chỉ được xử lý trong phạm vi cần thiết và phù hợp với mục đích đã xác định. Việc thừa nhận quyền xóa và hạn chế xử lý dữ liệu còn cho thấy sự tiếp cận của pháp luật Việt Nam đối với khái niệm “quyền được quên” trong pháp luật bảo vệ dữ liệu, dù vẫn được đặt trong những giới hạn nhất định nhằm bảo đảm lợi ích công cộng và nghĩa vụ pháp lý của bên xử lý dữ liệu. Nhóm quyền này trong pháp luật Việt Nam có mức độ tương thích nhất định với các quyền tương ứng trong Quy định bảo vệ dữ liệu chung của Liên minh châu Âu, đặc biệt là quyền xóa dữ liệu, quyền hạn chế xử lý và quyền

phản đối, qua đó phản ánh xu hướng hội nhập của pháp luật Việt Nam với các chuẩn mực quốc tế về bảo vệ DLCN và QCN trong kỷ nguyên số.

Thứ năm, quyền khiếu nại, tố cáo, khởi kiện và yêu cầu bồi thường thiệt hại của chủ thể DLCN.

Quy định này thiết lập cơ chế bảo vệ quyền mang tính tố tụng và khắc phục hậu quả, cho phép cá nhân sử dụng các công cụ pháp lý để bảo vệ quyền và lợi ích hợp pháp của mình khi DLCN bị xử lý trái pháp luật hoặc gây thiệt hại (điểm đ khoản 1 Điều 4). Quyền khiếu nại và tố cáo tạo điều kiện cho chủ thể dữ liệu yêu cầu cơ quan nhà nước có thẩm quyền xem xét, xử lý hành vi vi phạm, trong khi quyền khởi kiện và yêu cầu bồi thường thiệt hại gắn liền với cơ chế bảo vệ quyền bằng con đường tư pháp, bảo đảm nguyên tắc trách nhiệm pháp lý và bồi thường tương xứng với thiệt hại đã xảy ra. Việc ghi nhận nhóm quyền này thể hiện yêu cầu bảo đảm quyền tiếp cận công lý và quyền được bồi thường hiệu quả, vốn là những yếu tố không thể thiếu để các quyền thực chất được hiện thực hóa.

Thứ sáu, quyền yêu cầu áp dụng các biện pháp, giải pháp bảo vệ DLCN.

Chủ thể dữ liệu có quyền yêu cầu cơ quan nhà nước có thẩm quyền, cũng như các cơ quan, tổ chức, cá nhân liên quan đến hoạt động xử lý DLCN thực hiện các biện pháp cần thiết nhằm bảo vệ DLCN của mình (điểm e khoản 1 Điều 4). Quy định này thể hiện cách tiếp cận coi bảo vệ DLCN không chỉ là nghĩa vụ pháp lý đơn thuần của bên xử lý dữ liệu, mà còn là quyền chủ động của cá nhân trong việc yêu cầu thiết lập và duy trì các cơ chế bảo vệ phù hợp. Về mặt nội hàm, quyền này bao gồm khả năng yêu cầu áp dụng các biện pháp kỹ thuật, biện pháp quản lý và các giải pháp tổ chức nhằm phòng ngừa, phát hiện và khắc phục nguy cơ xâm phạm DLCN, đặc biệt trong các trường hợp có dấu hiệu mất an toàn hoặc vi phạm quy định về bảo vệ dữ liệu. Quyền yêu cầu bảo vệ DLCN phản ánh nghĩa vụ tích cực của Nhà nước trong việc bảo đảm quyền, không chỉ dừng lại ở việc không can thiệp trái pháp luật mà còn phải thiết lập cơ chế bảo vệ hiệu quả trước các rủi ro phát sinh từ hoạt động xử lý dữ liệu.

3.2.1.2. Thực trạng quy định về chủ thể bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh ở Việt Nam

Thứ nhất, cơ quan nhà nước ở cấp tỉnh với tư cách là chủ thể bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh ở Việt Nam.

Trong khuôn khổ pháp luật Việt Nam hiện hành, cơ quan nhà nước ở cấp tỉnh được xác định là chủ thể giữ vai trò trung tâm trong việc bảo vệ quyền đối với DLCN trong quá trình xây dựng và vận hành chính quyền số. Cơ sở pháp lý nền tảng cho vai trò này được xác lập tại Điều 21 Hiến pháp năm 2013, theo đó “mọi người có quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân, bí mật gia đình” và “thông

tin về đời sống riêng tư, bí mật cá nhân, bí mật gia đình được pháp luật bảo đảm an toàn” [43]. Quy định mang tính hiến định này đồng thời đặt ra nghĩa vụ cho Nhà nước trong việc tôn trọng, bảo vệ và bảo đảm QCN, qua đó xác định trách nhiệm của các cơ quan nhà nước, trong đó có UBND cấp tỉnh và các cơ quan chuyên môn trực thuộc, trong việc bảo vệ quyền đối với DLCN khi thực hiện chức năng quản lý nhà nước và cung ứng dịch vụ công trên môi trường số.

Cụ thể hóa nghĩa vụ hiến định nêu trên, Luật An toàn thông tin mạng năm 2015 đã quy định tương đối rõ trách nhiệm của cơ quan nhà nước trong việc bảo vệ thông tin cá nhân. Điều 16 của luật này xác định: *“Cơ quan, tổ chức, cá nhân xử lý thông tin cá nhân có trách nhiệm bảo đảm an toàn thông tin cá nhân do mình xử lý”*, đồng thời yêu cầu việc thu thập, sử dụng thông tin cá nhân phải *“được sự đồng ý của chủ thể thông tin”*, trừ các trường hợp luật có quy định khác [44]. Trong bối cảnh xây dựng chính quyền số cấp tỉnh, các sở, ban, ngành và UBND các cấp tại địa phương là chủ thể trực tiếp xây dựng, quản lý và vận hành các hệ thống thông tin, cơ sở dữ liệu chuyên ngành và liên thông, do đó được xác định là chủ thể có nghĩa vụ pháp lý trong việc bảo đảm an toàn và bảo mật DLCN của người dân. Tuy nhiên, cách tiếp cận của Luật An toàn thông tin mạng năm 2015 vẫn chủ yếu đặt trọng tâm vào khía cạnh kỹ thuật và an ninh thông tin, trong khi việc bảo vệ DLCN với tư cách là một QCN độc lập chưa được thể hiện một cách rõ nét.

Luật An ninh mạng năm 2018 tiếp tục khẳng định vai trò của các cơ quan nhà nước trong việc bảo vệ DLCN trên không gian mạng. Theo Điều 17 của luật này, cơ quan, tổ chức, cá nhân có trách nhiệm *“bảo vệ thông tin cá nhân, bí mật đời sống riêng tư”* khi tham gia hoạt động trên không gian mạng, đồng thời Nhà nước giao cho các cơ quan quản lý nhà nước và lực lượng chuyên trách nhiệm vụ phòng ngừa, phát hiện và xử lý các hành vi xâm phạm an ninh mạng, trong đó bao gồm các hành vi xâm phạm DLCN [46]. Ở cấp tỉnh, các cơ quan chuyên môn thuộc UBND cấp tỉnh vừa thực hiện chức năng quản lý nhà nước về an ninh mạng, vừa trực tiếp tham gia thu thập, lưu trữ và xử lý DLCN trong các hệ thống phục vụ chính quyền số. Sự đan xen này cho thấy mô hình bảo vệ quyền đối với DLCN ở Việt Nam vẫn mang tính quản lý hành chính tập trung, trong đó cơ quan nhà nước đồng thời là chủ thể bảo vệ quyền và là chủ thể nắm giữ, kiểm soát khối lượng lớn DLCN.

Bước phát triển đáng chú ý trong việc xác định tư cách pháp lý của các cơ quan nhà nước địa phương với vai trò chủ thể bảo vệ quyền đối với DLCN được thể hiện tại Nghị định số 13/2023/NĐ-CP về bảo vệ DLCN. Theo quy định của nghị định này, các cơ quan nhà nước ở cấp tỉnh khi thu thập, xử lý DLCN được xác định là *“bên kiểm soát dữ liệu”* hoặc *“bên kiểm soát và xử lý dữ liệu”*, đồng thời có nghĩa

vụ “tôn trọng và bảo đảm các quyền của chủ thể dữ liệu”, bao gồm quyền được biết, quyền đồng ý, quyền truy cập, quyền chỉnh sửa, quyền xóa và quyền yêu cầu bảo vệ DLCN [18]. Việc xác lập rõ tư cách và nghĩa vụ pháp lý này cho thấy sự dịch chuyển bước đầu từ mô hình quản lý hành chính thuần túy sang cách tiếp cận dựa trên quyền, phù hợp hơn với yêu cầu bảo vệ QCN trong bối cảnh chuyển đổi số ở cấp địa phương.

Bên cạnh đó, Luật Bảo vệ dữ liệu cá nhân năm 2025 được thông qua đã tiếp tục kế thừa và phát triển các quy định của Nghị định số 13/2023/NĐ-CP, đồng thời hướng tới việc xác lập khuôn khổ pháp lý thống nhất ở cấp luật. Theo các nội dung cơ bản của Luật 91, cơ quan nhà nước, bao gồm cơ quan nhà nước ở cấp tỉnh, được xác định rõ là chủ thể có nghĩa vụ đặc biệt trong việc bảo vệ DLCN khi thực hiện chức năng quản lý nhà nước và cung cấp dịch vụ công, với yêu cầu tăng cường trách nhiệm giải trình, minh bạch và bảo đảm quyền của chủ thể dữ liệu [50]. Cách tiếp cận này cho thấy xu hướng hoàn thiện pháp luật theo hướng tiếp cận QCN, tiệm cận hơn với các chuẩn mực quốc tế về bảo vệ DLCN trong bối cảnh xây dựng chính quyền số.

Thứ hai, chủ thể sở hữu DLCN với tư cách là chủ thể bảo vệ quyền đối với DLCN.

Trong cơ chế bảo vệ quyền đối với DLCN theo pháp luật Việt Nam hiện hành, cá nhân sở hữu DLCN không chỉ được xác định là chủ thể thụ hưởng quyền, mà còn được đặt vào vị trí là chủ thể trực tiếp tham gia bảo vệ quyền đối với chính DLCN của mình. Cách tiếp cận này phản ánh xu hướng tiếp cận QCN hiện đại, theo đó việc bảo vệ quyền riêng tư và DLCN không chỉ là nghĩa vụ của Nhà nước mà còn gắn với trách nhiệm chủ động của cá nhân trong việc thực hiện và bảo vệ các quyền của mình trong môi trường số. Điều 21 Hiến pháp năm 2013 khẳng định “mọi người có quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân, bí mật gia đình” và “thông tin về đời sống riêng tư, bí mật cá nhân, bí mật gia đình được pháp luật bảo đảm an toàn” [43]. Quy định này không chỉ xác lập quyền cơ bản của cá nhân đối với DLCN với tư cách là một bộ phận của quyền riêng tư, mà còn đặt nền tảng cho việc cá nhân có trách nhiệm tự bảo vệ phạm vi đời sống riêng tư của mình thông qua việc kiểm soát việc cung cấp, chia sẻ và sử dụng DLCN trong các quan hệ pháp lý phát sinh.

Luật Bảo vệ dữ liệu cá nhân năm 2025 đã cụ thể hóa rõ ràng hơn vai trò của cá nhân sở hữu DLCN với tư cách là chủ thể bảo vệ quyền đối với DLCN. Theo luật này, cá nhân được xác định là chủ thể dữ liệu, có quyền quyết định đối với việc xử lý DLCN của mình, đồng thời phải thực hiện các quyền đó theo đúng quy định của pháp luật. Luật quy định rõ rằng việc thực hiện quyền của chủ thể dữ liệu phải “tuân thủ quy định của Luật này và quy định khác của pháp luật có liên quan”, không được

“lạm dụng quyền về bảo vệ DLCN để xâm phạm lợi ích quốc gia, dân tộc, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác” [50]. Bên cạnh đó, Luật Bảo vệ dữ liệu cá nhân năm 2025 còn đặt ra những nghĩa vụ pháp lý cụ thể đối với cá nhân sở hữu DLCN trong quá trình tự bảo vệ quyền của mình. Theo đó, chủ thể dữ liệu có nghĩa vụ *“cung cấp thông tin chính xác, đầy đủ khi thực hiện các quyền của chủ thể dữ liệu”*, đồng thời có trách nhiệm *“phối hợp với bên kiểm soát dữ liệu, bên xử lý dữ liệu và cơ quan có thẩm quyền trong quá trình xác minh, giải quyết yêu cầu liên quan đến bảo vệ DLCN”* [50]. Quy định này thể hiện rõ quan điểm lập pháp coi cá nhân không chỉ là người được bảo vệ thụ động mà còn là chủ thể có trách nhiệm tích cực trong việc bảo đảm hiệu quả của cơ chế bảo vệ DLCN.

Ngoài ra, Luật Bảo vệ dữ liệu cá nhân năm 2025 còn đặt ra yêu cầu đối với cá nhân trong việc sử dụng DLCN của chính mình. Theo đó, cá nhân không được *“cho người khác sử dụng DLCN của mình để thực hiện hành vi trái quy định của pháp luật”*, cũng như không được *“sử dụng quyền đối với DLCN của mình để tiếp tay cho các hành vi vi phạm pháp luật”* [50]. Nghĩa vụ này cho thấy pháp luật Việt Nam tiếp cận quyền đối với DLCN như một QCN gắn liền với trách nhiệm xã hội, chứ không phải là một quyền tuyệt đối, biệt lập khỏi lợi ích công cộng. Trong bối cảnh xây dựng chính quyền số cấp tỉnh, nơi cá nhân thường xuyên tương tác với các hệ thống thông tin, cơ sở dữ liệu do cơ quan nhà nước quản lý, vai trò tự bảo vệ quyền của cá nhân sở hữu DLCN càng trở nên quan trọng. Việc pháp luật đặt ra nghĩa vụ cho cá nhân trong việc cung cấp thông tin chính xác, thực hiện quyền một cách thiện chí và phối hợp với cơ quan có thẩm quyền góp phần hình thành cơ chế bảo vệ DLCN đa tầng, trong đó trách nhiệm bảo vệ quyền được phân bổ giữa Nhà nước và cá nhân, phù hợp với cách tiếp cận QCN trong quản trị số nói chung.

Thứ ba, chủ thể xử lý vi phạm liên quan đến quyền đối với DLCN.

Trong mô hình bảo vệ quyền đối với DLCN theo pháp luật Việt Nam hiện hành, chủ thể thứ ba đảm nhiệm chức năng xử lý vi phạm liên quan đến quyền đối với DLCN đóng vai trò quan trọng trong việc bảo đảm QCN và tính hiệu lực của hệ thống pháp luật. Pháp luật xác định rõ các chủ thể này phải tuân thủ các nguyên tắc, thủ tục và biện pháp xử lý vi phạm nhằm bảo vệ quyền của chủ thể DLCN khi quyền đó bị xâm phạm trong quá trình xử lý dữ liệu, đặc biệt trong bối cảnh triển khai chính quyền số cấp tỉnh.

(1). Luật Bảo vệ dữ liệu cá nhân năm 2025 xác định cơ chế xử lý vi phạm về bảo vệ DLCN tại Điều 8, theo đó: *“Tổ chức, cá nhân có hành vi vi phạm quy định của Luật này và quy định khác của pháp luật có liên quan đến bảo vệ DLCN thì tùy*

theo tính chất, mức độ, hậu quả của hành vi vi phạm có thể bị xử phạt hành chính hoặc bị truy cứu trách nhiệm hình sự; nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật” [50]. Quy định này xác lập rõ rằng chủ thể xử lý vi phạm bao gồm các cơ quan, tổ chức có thẩm quyền được Nhà nước ủy quyền để thực hiện biện pháp xử lý tương ứng đối với hành vi vi phạm luật về DLCN - từ xử phạt vi phạm hành chính, truy cứu trách nhiệm hình sự đến buộc bồi thường thiệt hại.

(2). Quy định về các hành vi bị nghiêm cấm liên quan đến DLCN tại Điều 7, theo đó: *“Xử lý DLCN trái quy định của pháp luật; sử dụng DLCN của người khác, cho người khác sử dụng DLCN của mình để thực hiện hành vi trái quy định của pháp luật; mua, bán DLCN; chiếm đoạt, cố ý làm lộ, làm mất DLCN...” [50]* là các hành vi nghiêm cấm. Việc liệt kê rõ các hành vi bị nghiêm cấm này giúp phân định rõ đối tượng vi phạm và phạm vi xử lý của chủ thể có thẩm quyền, bảo đảm rằng hành vi xâm phạm quyền đối với DLCN được tiếp cận không chỉ dưới góc độ quản lý hành chính mà còn nhìn nhận như xâm phạm QCN, từ đó có biện pháp xử lý phù hợp.

(3). Quy định về nghĩa vụ và cơ chế báo cáo vi phạm. Theo đó, tại Điều 23, khi bên kiểm soát DLCN, bên kiểm soát và xử lý DLCN hoặc bên thứ ba phát hiện hành vi vi phạm quy định về bảo vệ DLCN có thể gây thiệt hại nghiêm trọng, thì phải *“thông báo cho cơ quan chuyên trách bảo vệ DLCN chậm nhất là 72 giờ kể từ khi phát hiện hành vi vi phạm” [50].* Đồng thời, các bên này có nghĩa vụ lập biên bản và phối hợp với cơ quan chuyên trách bảo vệ DLCN xử lý hành vi vi phạm quy định về bảo vệ DLCN. Quy định này không chỉ phân công vai trò chủ thể xử lý vi phạm mà còn đặt ra yêu cầu phối hợp chặt chẽ giữa các chủ thể, gồm đơn vị phát hiện, bên kiểm soát, bên xử lý dữ liệu và cơ quan chuyên trách bảo vệ DLCN, nhằm bảo đảm tính hiệu quả trong xử lý khiếu nại, phản ánh và vi phạm liên quan đến quyền đối với DLCN.

(4). Quy định trách nhiệm phối hợp và hỗ trợ giữa các chủ thể được giao chức năng xử lý vi phạm. Theo Điều 36 Luật Bảo vệ dữ liệu cá nhân năm 2025, trách nhiệm quản lý nhà nước về bảo vệ DLCN *“thuộc về Chính phủ; Bộ Công an là cơ quan đầu mối chịu trách nhiệm trước Chính phủ trong thực hiện quản lý nhà nước về bảo vệ DLCN... Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ thực hiện quản lý nhà nước về bảo vệ DLCN đối với ngành, lĩnh vực theo phân công” [50].* Quy định này xác định rõ cơ quan chuyên trách trong hệ thống xử lý vi phạm là một thiết chế không thể tách rời trong việc điều tra, xác minh và khởi xướng các biện pháp chế tài đối với hành vi xâm phạm DLCN, điều này đặc biệt quan trọng trong bối cảnh chính quyền số cấp tỉnh, nơi DLCN được thu thập và xử lý với khối lượng lớn và đa dạng.

Luật Bảo vệ dữ liệu cá nhân năm 2025 đã xây dựng hệ thống chủ thể xử lý vi phạm liên quan đến DLCN tương đối toàn diện, từ việc liệt kê hành vi bị nghiêm cấm, quy định về biện pháp xử lý vi phạm pháp luật, đến cơ chế báo cáo và phối hợp xử lý giữa các chủ thể có thẩm quyền. Cách tiếp cận này phản ánh nỗ lực chuyển hóa nghĩa vụ bảo vệ quyền đối với DLCN thành một cơ chế pháp lý có hiệu lực thực thi, trong đó QCN về quyền riêng tư và an toàn dữ liệu được đặt vào trọng tâm xử lý vi phạm.

Thứ tư, quy định pháp luật về trách nhiệm của các chủ thể xử lý DLCN.

Pháp luật Việt Nam hiện hành, đặc biệt là Luật Bảo vệ DLCN năm 2025, đã bước đầu tiếp cận mô hình phân định trách nhiệm của các chủ thể xử lý DLCN theo vai trò trong quá trình xử lý dữ liệu, thay vì phân biệt theo khu vực công hay khu vực tư. Cách tiếp cận này thể hiện rõ quan điểm coi việc bảo vệ DLCN là nghĩa vụ pháp lý gắn với mức độ quyết định và can thiệp của chủ thể đối với dữ liệu, phù hợp với lý luận và thông lệ pháp lý quốc tế về bảo vệ DLCN. Theo Luật Bảo vệ DLCN năm 2025, trách nhiệm của các chủ thể xử lý DLCN được xác lập dựa trên việc chủ thể đó có “*quyết định mục đích và phương thức xử lý DLCN*” hay “*thực hiện việc xử lý DLCN theo chỉ đạo*”. Cụ thể, bên kiểm soát DLCN được xác định là chủ thể “*quyết định mục đích và phương thức xử lý DLCN*” và có trách nhiệm “*bảo đảm việc xử lý DLCN có căn cứ pháp lý, đúng mục đích, trong phạm vi cần thiết và tôn trọng các quyền của chủ thể dữ liệu*” [50]. Luật đồng thời đặt ra nghĩa vụ cho bên kiểm soát trong việc “*áp dụng các biện pháp bảo vệ DLCN phù hợp*” và “*chịu trách nhiệm trước pháp luật về toàn bộ hoạt động xử lý DLCN do mình quyết định*”.

Đối với bên xử lý DLCN, Luật Bảo vệ dữ liệu cá nhân năm 2025 quy định đây là chủ thể “*thực hiện việc xử lý DLCN theo hợp đồng hoặc theo chỉ đạo của bên kiểm soát DLCN*”. Trách nhiệm của bên xử lý được xác định theo hướng tuân thủ, theo đó bên xử lý có nghĩa vụ “*xử lý DLCN đúng phạm vi, mục đích, nội dung và thời hạn theo thỏa thuận hoặc theo chỉ đạo của bên kiểm soát dữ liệu*”, đồng thời “*áp dụng các biện pháp kỹ thuật, tổ chức cần thiết để bảo đảm an toàn, an ninh DLCN trong quá trình xử lý*” [50]. Quy định này cho thấy pháp luật không coi bên xử lý là chủ thể thuần túy kỹ thuật, mà là chủ thể có trách nhiệm pháp lý độc lập trong phạm vi vai trò xử lý dữ liệu được giao.

Đối với bên vừa kiểm soát vừa xử lý DLCN, Luật Bảo vệ dữ liệu cá nhân năm 2025 xác định đây là trường hợp chủ thể “*đồng thời quyết định mục đích, phương thức xử lý và trực tiếp thực hiện việc xử lý DLCN*” [50]. Theo đó, chủ thể này “*phải thực hiện đầy đủ trách nhiệm của bên kiểm soát DLCN và bên xử lý DLCN theo quy định của pháp luật*”. Cách quy định này thể hiện nguyên tắc trách nhiệm tương xứng:

chủ thể nào nắm giữ nhiều quyền lực hơn đối với dữ liệu thì phải gánh vác nghĩa vụ pháp lý ở mức cao hơn.

Ngoài Luật Bảo vệ DLCN năm 2025, trách nhiệm bảo vệ quyền đối với DLCN của các chủ thể còn được ghi nhận rải rác trong các văn bản pháp luật có liên quan. Hiến pháp năm 2013 khẳng định “*mọi người có quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân*” và “*thông tin về đời sống riêng tư, bí mật cá nhân được pháp luật bảo đảm an toàn*” (Điều 21) [43], tạo cơ sở hiến định cho việc xác lập trách nhiệm của các chủ thể xử lý dữ liệu. Luật An toàn thông tin mạng năm 2015 quy định trách nhiệm của cơ quan, tổ chức, cá nhân trong việc “*bảo đảm an toàn thông tin cá nhân khi thu thập, xử lý và sử dụng thông tin trên mạng*” [44]. Luật An ninh mạng năm 2018 tiếp tục đặt ra nghĩa vụ đối với cơ quan, tổ chức trong việc “*bảo vệ thông tin cá nhân trên không gian mạng*” và phòng ngừa, xử lý hành vi xâm phạm DLCN [46].

Trong bối cảnh xây dựng chính quyền số cấp tỉnh, các quy định này là cơ sở pháp lý để xác định rằng cơ quan nhà nước địa phương thường giữ vai trò bên kiểm soát hoặc bên kiểm soát và xử lý DLCN đối với các hệ thống thông tin hành chính, công dịch vụ công và cơ sở dữ liệu do địa phương quản lý.

Việc pháp luật phân định rõ trách nhiệm theo vai trò xử lý dữ liệu tạo nền tảng pháp lý quan trọng cho việc đánh giá mức độ tuân thủ và hiệu lực bảo vệ quyền đối với DLCN trong thực tiễn triển khai chính quyền số ở cấp tỉnh, sẽ được phân tích cụ thể ở các mục tiếp theo.

Chúng ta thấy rằng, thể chế và quy chế nội bộ được coi là phương thức bảo vệ đầu tiên, tạo hành lang pháp lý và quy tắc ứng xử cho toàn bộ bộ máy công quyền cấp tỉnh trong việc xử lý dữ liệu cá nhân.

Tại cấp độ nội bộ địa phương, chính quyền cấp tỉnh đã bước đầu nỗ lực “*nội địa hóa*” các quy định pháp lý thành quy trình vận hành cụ thể. Nhiều tỉnh đã cập nhật, ban hành mới quy chế quản lý, vận hành Công dịch vụ công trực tuyến và Trung tâm Điều hành thông minh (IOC). Trong các quy chế này, bước đầu đã có các điều khoản quy định về mục đích thu thập dữ liệu, thời hạn lưu trữ và trách nhiệm bảo mật của cơ quan chủ quản; phân quyền và bảo mật thông tin nội bộ. Các sở chuyên ngành nắm giữ nhiều dữ liệu nhạy cảm (như Sở Y tế với hồ sơ bệnh án, Sở Tư pháp với sổ hộ tịch, Sở TN&MT với dữ liệu đất đai) đã ban hành các quy định nội bộ về phân quyền truy cập hệ thống. Công chức, viên chức được cấp tài khoản định danh riêng và quy định rõ phạm vi trường dữ liệu được phép khai thác tùy theo vị trí việc làm.

Thời gian qua, mặc dù hệ thống văn bản được ban hành khá nhiều, nhưng khi đi sâu phân tích thực trạng, phương thức thể chế và quy chế nội bộ tại cấp tỉnh vẫn

tồn tại những hạn chế lớn như: (1) Tính hình thức, “sao chép nguyên bản” văn bản cấp trên: Phần lớn các quy chế nội bộ của các sở, ban, ngành hoặc quyết định của UBND tỉnh hiện nay đều mang tính chất “sao chép lại” một cách cơ học các điều khoản của Nghị định 13/2023/NĐ-CP và Luật Bảo vệ dữ liệu cá nhân. Các văn bản này thiếu đi sự cụ thể hóa, chưa chỉ ra được quy trình kỹ thuật cụ thể: Cán bộ ở bước này phải làm gì để xin ý kiến người dân? Quy trình xử lý khi công dân yêu cầu rút lại sự đồng ý hoặc xóa dữ liệu trên hệ thống dịch vụ công của tỉnh sẽ diễn ra như thế nào? (2) Quy chế nội bộ chưa bắt kịp các công nghệ mới của Đô thị thông minh: Các quy chế hiện hành của các tỉnh hầu như mới chỉ bao quát được dữ liệu hành chính dạng văn bản (text) trên cổng dịch vụ công. Thực tiễn cho thấy, địa phương vẫn chưa ban hành quy chế hoặc còn tồn tại khoảng trống pháp lý đáng kể trong hệ thống quy chế nội bộ điều chỉnh việc quản lý, khai thác và bảo vệ các nhóm dữ liệu nhạy cảm, bao gồm: dữ liệu từ hệ thống camera AI giám sát đô thị, dữ liệu nhận dạng sinh trắc học khuôn mặt và dữ liệu định vị không gian từ các ứng dụng công dân số. (3) Sự lỏng lẻo trong quy chế ràng buộc với các nhà thầu công nghệ (Bên thứ ba): Khi UBND tỉnh ký hợp đồng thuê dịch vụ CNTT hoặc xây dựng phần mềm với các doanh nghiệp, các điều khoản về bảo vệ quyền DLCN của người dân trong hợp đồng thường rất chung chung. Thiếu các quy chế kỹ thuật, pháp lý nghiêm ngặt để giám sát, chế tài doanh nghiệp, dẫn đến nguy cơ dữ liệu công dân bị nhà thầu chiếm dụng ngầm.

3.2.1.3. Thực trạng bảo vệ quyền chủ thể dữ liệu gắn với quyền công dân

Bảo đảm quyền của chủ thể dữ liệu (người dân) gắn liền với quyền công dân, quyền con người theo Hiến pháp là thước đo cao nhất phản ánh tính chất “phục vụ Nhân dân” của chính quyền số cấp tỉnh. Phương thức này chuyển dịch trọng tâm từ tư duy quản lý hành chính thuần túy sang việc tôn trọng và hiện thực hóa quyền tự quyết thông tin của người dân. Qua thực tiễn triển khai thời gian qua, phương thức này ghi nhận những kết quả bước đầu nhưng cũng bộc lộ những bất cập trong khâu thực thi.

Những chuyển biến tích cực trong việc tôn trọng quyền công dân số: Kể từ khi có Nghị định 13/2023/NĐ-CP và Luật 91 có hiệu lực, trên giao diện của các Cổng dịch vụ công trực tuyến và hệ thống thông tin giải quyết thủ tục hành chính cấp tỉnh bước đầu đã xuất hiện các biểu mẫu, hộp thoại “Điều khoản sử dụng và chính sách bảo mật”. Chính quyền tỉnh đã thực hiện nghĩa vụ thông báo công khai cho người dân biết rõ loại dữ liệu nào sẽ bị thu thập, mục đích thu thập và cơ quan nào sẽ chịu trách nhiệm xử lý. Thông qua việc liên thông với Cơ sở dữ liệu quốc gia về dân cư và ứng dụng VNeID (Hệ thống định danh và xác thực điện tử -VNeID đã cán mốc trên 85 triệu tài khoản được kích hoạt) [9], người dân khi thực hiện dịch vụ công tại địa

phương đã có thể dễ dàng kiểm tra, đối soát thông tin cá nhân của mình. Khi phát hiện sai lệch (sai số định danh, sai lệch thông tin hộ tịch, đất đai), quy trình tiếp nhận và xử lý yêu cầu cải chính dữ liệu của công dân tại bộ phận “Một cửa” đã được chuẩn hóa và giải quyết nhanh chóng hơn so với phương thức thủ công trước đây.

Tuy nhiên, dù bộ quyền của công dân được luật hóa rất thấu đáo, nhưng cơ chế để người dân thực hiện các quyền này trong môi trường hành chính công cấp tỉnh hiện nay lại gặp phải rào cản mang tính hệ thống: (1) Thụ động trong cơ chế đồng ý: Theo lý luận, chủ thể dữ liệu có quyền đồng ý, không đồng ý hoặc rút lại sự đồng ý đối với việc xử lý dữ liệu của mình. Tuy nhiên, tại các cổng dịch vụ công cấp tỉnh, cơ chế này mang tính áp đặt một chiều. Người dân chỉ có một lựa chọn duy nhất là bấm vào nút “Tôi đồng ý với tất cả điều khoản” thì hệ thống mới cho phép tiếp tục nộp hồ sơ. Nếu công dân phản đối hoặc muốn rút lại sự đồng ý đối với một trường dữ liệu mà họ cho là không cần thiết, hệ thống sẽ từ chối giải quyết TTHC. Quyền tự quyết thông tin của người dân trong trường hợp này bị triệt tiêu trước mệnh lệnh hành chính. (2) Sự bất khả thi của “Quyền được xóa dữ liệu” trong khu vực công: Theo các quy định của luật, công dân có quyền yêu cầu xóa dữ liệu cá nhân. Tuy nhiên, đối với hệ thống chính quyền số, dữ liệu cá nhân của người dân (như hồ sơ tư pháp, dữ liệu thuế, đất đai, hộ tịch) lại là căn cứ để Nhà nước thực hiện chức năng quản lý và lưu trữ lịch sử theo Luật Lưu trữ. Thực tế, chính quyền cấp tỉnh chưa có quy trình kỹ thuật và hành lang pháp lý phân định rõ: Dữ liệu nào thuộc diện lưu trữ bắt buộc của Nhà nước, dữ liệu nào người dân có quyền yêu cầu xóa bỏ? Điều này khiến quyền được xóa dữ liệu của công dân hoàn toàn bị vô hiệu hóa khi đối diện với các cơ quan công quyền. (3) Thiếu công cụ phản đối các quyết định tự động bằng thuật toán (AI): Trong xu hướng xây dựng đô thị thông minh cấp tỉnh, nhiều hệ thống đã bắt đầu áp dụng thuật toán AI để phân loại hồ sơ, chấm điểm tín nhiệm doanh nghiệp, công dân, hoặc xử phạt nguội qua camera giám sát. Mặc dù công dân có quyền phản đối việc bị định danh, lập hồ sơ hoặc ra quyết định tự động gây bất lợi cho mình, nhưng các nền tảng chính quyền số hiện nay hoàn toàn không thiết kế bất kỳ một nút bấm, một tính năng hay một quy trình khiếu nại nào để người dân thực hiện quyền phản đối này. (4) Kênh khiếu nại và hỗ trợ pháp lý khi bị xâm phạm dữ liệu còn mờ nhạt: Khi người dân nghi ngờ dữ liệu cá nhân của mình bị lộ lọt từ hệ thống dịch vụ công của tỉnh (ví dụ: ngay sau khi làm thủ tục đất đai liền bị các cuộc gọi rác quấy rầy), họ hoàn toàn lúng túng, không biết phải nộp đơn khiếu nại bảo vệ dữ liệu ở đâu, quy trình giải quyết ra sao. Các tỉnh chưa thiết lập được một cổng tiếp nhận và phản hồi riêng biệt dành cho các khiếu nại liên quan đến vi phạm dữ liệu cá nhân.

Có thể đánh giá một cách tổng thể, phương thức bảo vệ thông qua bảo đảm

quyền chủ thể dữ liệu tại chính quyền số cấp tỉnh thời gian qua đang rơi vào tình trạng “hữu danh vô thực”. Chúng ta đã tạo ra một bộ quyền rất tiến bộ trên văn bản pháp lý, nhưng lại đặt nó vào một cơ chế vận hành hành chính nặng tính mệnh lệnh, áp đặt.

Trong mỗi quan hệ này, cần hoàn thiện cơ chế để người dân phát huy quyền làm chủ trong môi trường số. Chính quyền số không thể coi là thành công nếu nó chỉ mang lại sự tiện lợi về mặt kỹ thuật cho cơ quan nhà nước, mà lại làm suy giảm quyền tự quyết thông tin - một bộ phận cấu thành của quyền con người và quyền công dân trong kỷ nguyên số.

3.2.1.4. Thực trạng thu thập, xử lý dữ liệu cá nhân qua các nền tảng, cổng dịch vụ công cấp tỉnh

Trong mô hình chính quyền số cấp tỉnh, Cổng dịch vụ công và Hệ thống thông tin giải quyết thủ tục hành chính là đầu mối tiếp xúc chủ yếu giữa cá nhân, tổ chức với cơ quan hành chính, đồng thời là nơi phát sinh và vận hành quá trình xử lý DLCN theo vòng đời thủ tục hành chính điện tử: đăng ký/đăng nhập và xác thực - nộp hồ sơ (biểu mẫu, tệp đính kèm) - luân chuyển/thẩm định - thanh toán - trả kết quả - đồng bộ, lưu trữ và tái sử dụng. Thực tiễn giai đoạn năm 2020 - 2025 cho thấy quy mô giao dịch qua các nền tảng dịch vụ công tăng nhanh, khiến hoạt động xử lý DLCN chuyển từ trạng thái hỗ trợ sang trạng thái “hạ tầng vận hành thường xuyên” của quản trị công.

Trước hết, quy mô vận hành của các nền tảng dịch vụ công, xét trên các chỉ báo nền tảng (tài khoản, hồ sơ, trạng thái đồng bộ, thanh toán), tăng liên tục từ 2020 đến 2025, qua đó phản ánh mức độ mở rộng phạm vi xử lý DLCN ở khu vực công. Trên thực tế vận hành Cổng dịch vụ công quốc gia, hệ thống đã ghi nhận trên 390.000 tài khoản đăng ký, hơn 25 triệu hồ sơ đồng bộ trạng thái và trên 612.000 hồ sơ thực hiện trực tuyến từ Cổng. Đến năm 2023, quy mô tích lũy và tần suất giao dịch đã tăng mạnh: tính đến thời điểm tháng 9/2023, Cổng dịch vụ công quốc gia có hơn 9,1 triệu tài khoản; hơn 233 triệu hồ sơ đồng bộ; khoảng 24,5 triệu hồ sơ trực tuyến thực hiện từ Cổng; hơn 15,8 triệu giao dịch thanh toán trực tuyến với tổng giá trị hơn 7,142 nghìn tỷ đồng; trong năm 2023, chỉ riêng từ đầu năm đến 27/5/2023 đã có hơn 4,3 triệu hồ sơ trực tuyến và 3,8 triệu giao dịch thanh toán trực tuyến phát sinh từ Cổng, cho thấy nhịp độ xử lý dữ liệu gắn với hồ sơ/chi trả nghĩa vụ tài chính ngày càng nhiều [8]. Trong giai đoạn từ 20/5-20/6/2024 có hơn 831.000 tài khoản đăng ký; hơn 2,5 triệu hồ sơ trực tuyến; hơn 1,4 triệu giao dịch thanh toán trực tuyến với số tiền hơn 917 tỷ đồng; lũy kế 6 tháng đầu năm 2024 có hơn 4,8 triệu tài khoản đăng ký, hơn 13,9 triệu hồ sơ trực tuyến và hơn 7,4 triệu giao dịch thanh toán trực tuyến với số tiền hơn 4.620 tỷ đồng...[9]. Các số liệu này cho thấy DLCN được thu thập, cập nhật và lưu trữ không

chỉ từ “dữ liệu định danh” khi tạo tài khoản, mà còn mở rộng theo từng lần tương tác, từng hồ sơ, từng trạng thái xử lý và từng giao dịch thanh toán.

Tuy nhiên, mức độ xây dựng chính quyền số và cường độ phát sinh xử lý DLCN giữa các địa phương không đồng đều, tạo nên tình trạng phân hóa về cả hiệu quả cung cấp dịch vụ lẫn rủi ro quyền đối với DLCN. Một mặt, tồn tại nhóm địa phương đẩy mạnh toàn trình và tích lũy dữ liệu ở mức cao; mặt khác, nhiều địa phương có tỷ lệ hồ sơ trực tuyến toàn trình thấp, dễ phát sinh cơ chế vừa trực tuyến vừa trực tiếp, kéo theo thu thập trùng lặp, khó chuẩn hóa vòng đời dữ liệu và khó truy vết trách nhiệm khi có sự cố. Theo số liệu do Bộ Thông tin và Truyền thông công bố qua hệ thống EMC, trong năm 2024 chỉ có 8 cơ quan/địa phương đạt tỷ lệ hồ sơ trực tuyến toàn trình trên 50% (bao gồm một số bộ và các địa phương như Hà Nam, Đà Nẵng, Hà Giang, Nam Định (cũ))[9]. Sự phân hóa này cho thấy nơi “toàn trình hóa” cao thì lợi ích quản trị tăng nhưng phạm vi xử lý dữ liệu rộng hơn; ngược lại, nơi “toàn trình hóa” thấp có thể phát sinh rủi ro quản trị dữ liệu theo hướng thiếu nhất quán (đặc biệt ở khâu lưu trữ, cập nhật, chia sẻ dữ liệu qua kênh giấy - số).

Về cấu trúc dữ liệu thu thập, thực tiễn Hệ thống thông tin giải quyết thủ tục hành chính cấp tỉnh thường tạo ra ít nhất bốn nhóm DLCN cơ bản: dữ liệu định danh (họ tên, số định danh/CCCD, tài khoản); dữ liệu liên hệ (điện thoại, email, địa chỉ); dữ liệu giao dịch hành chính (tình trạng hồ sơ, lịch sử xử lý, kết quả, nhật ký tương tác); và dữ liệu thanh toán (trạng thái giao dịch, chứng từ điện tử). Đối với nhiều thủ tục theo lĩnh vực như y tế, an sinh xã hội, tư pháp, đất đai, hôn nhân gia đình..., tệp hồ sơ có thể bao gồm cả DLCN nhạy cảm. Khi khối lượng DLCN lớn, yêu cầu bảo vệ quyền đối với DLCN không thể chỉ quy về an toàn hệ thống, mà phải bao gồm kiểm soát mục đích, tối thiểu hóa, giới hạn truy cập nội bộ và quản trị vòng đời dữ liệu theo cơ chế giải trình.

Thực tiễn ở nhiều địa phương cho thấy, quy luật “dịch vụ công càng toàn trình, phạm vi xử lý dữ liệu càng mở rộng”, *điển hình như* thành phố Đà Nẵng, báo cáo tại hội nghị chuyên đề ngày 31/8/2024 cho thấy địa phương đạt 95% tỷ lệ dịch vụ công trực tuyến toàn trình và 65% tỷ lệ hồ sơ trực tuyến toàn trình [9]; đồng thời hình thành kho kết quả thủ tục hành chính số, phát triển tài khoản công dân số và thúc đẩy tái sử dụng kết quả để giảm thủ tục cấp lại; ngược lại, tỉnh Quảng Ngãi phản ánh thực trạng tỷ lệ dịch vụ công trực tuyến toàn trình ở mức trung bình, nhưng đã hình thành kho dữ liệu vận hành dịch vụ công trực tuyến cụ thể. Trong năm 2022, tỉnh Quảng Ngãi đã tiếp nhận, giải quyết hơn 48.000 hồ sơ trực tuyến; tích hợp 688 dịch vụ công trực tuyến lên Cổng dịch vụ công quốc gia; có gần 250 thủ tục có thể thanh toán trực tuyến [7].

Đặc biệt, nghĩa vụ minh bạch và thông báo quyền đối với DLCN trong vận hành công dịch vụ công còn chưa thật sự tương xứng với quy mô xử lý dữ liệu. Nhiều hệ thống tại các địa phương được xây dựng mới chỉ ưu tiên mục tiêu hoàn tất thủ tục hơn là bảo đảm quyền tự quyết thông tin của cá nhân; vì vậy thông báo xử lý thường dừng ở mức khái quát, khiến người dùng khó xác định loại dữ liệu nào đang được thu thập (đặc biệt với DLCN nhạy cảm), mục đích và căn cứ xử lý đối với dữ liệu, chủ thể nào sẽ được chia sẻ hoặc tiếp cận đối với dữ liệu mà họ đã cung cấp, thời hạn lưu trữ đối với các loại dữ liệu này và cách thức thực hiện các quyền đối với DLCN sau khi thủ tục kết thúc. Những vấn đề đặt ra này càng có tính cấp thiết hơn khi trên thực tế Công dịch vụ công quốc gia đã có 16,4 triệu tài khoản (Thông báo 369/TB-VPCP, ngày 09/8/2024 của Văn phòng Chính phủ). Đồng thời Nhà nước cũng đã đặt mục tiêu đến hết năm 2024 đạt 80% dịch vụ công trực tuyến toàn trình, 40% dân số trưởng thành sử dụng dịch vụ công trực tuyến và 90% hài lòng trong giải quyết thủ tục; đến năm 2025 hướng tới 100% hồ sơ giải quyết thủ tục hành chính được gắn định danh cá nhân [9]. Trong thực hiện công tác định danh đối với công dân, theo thông tin của Bộ Công an đến ngày 16/01/2026 ứng dụng VNeID đã kích hoạt hơn 67 triệu tài khoản và ghi nhận trên 500 triệu lượt truy cập, bình quân hơn 3 triệu lượt/ngày [6], điều này cho thấy quy mô truy cập và mức độ phụ thuộc vào các nền tảng số đang tăng nhanh, càng đặt ra yêu cầu đối với xử lý và bảo vệ quyền đối với DLCN của chủ thể dữ liệu.

Cùng với đó, thực tiễn xử lý DLCN trên các nền tảng dịch vụ công cấp tỉnh cho thấy những nguy cơ và rủi ro tấn công mạng và đánh cắp dữ liệu đang ngày càng gia tăng, xâm phạm nghiêm trọng đến DLCN và quyền đối với DLCN của chủ thể dữ liệu trong giai đoạn hiện nay. Báo cáo khảo sát an ninh mạng năm 2025 cho thấy trong năm 2025 các hệ thống thông tin tại Việt Nam phải đối mặt khoảng 552.000 cuộc tấn công mạng; 52,30% cơ quan, doanh nghiệp vẫn ghi nhận chịu những tổn thất do tấn công mạng [34].

3.2.2. Thực trạng tổ chức bộ máy và quản trị nhân sự, phân công trách nhiệm bảo vệ quyền đối với dữ liệu cá nhân tại cơ quan cấp tỉnh

Trong quá trình triển khai chính quyền số ở cấp tỉnh giai đoạn 2020 - 2025, đa số cơ quan chuyên môn thuộc UBND cấp tỉnh đã hình thành các bộ phận liên quan đến vận hành hệ thống thông tin, chuyển đổi số, kiểm soát thủ tục hành chính hoặc cải cách hành chính. Ở nhiều địa phương, các thiết chế như Trung tâm phục vụ hành chính công, Trung tâm giám sát - điều hành thông minh (IOC), bộ phận chuyển đổi số hoặc đơn vị vận hành công dịch vụ công đã được xác lập và đi vào hoạt động. Tuy nhiên, qua thực tiễn triển khai thời gian qua, phương thức bảo vệ quyền dữ liệu cá

nhân thông qua tổ chức bộ máy tại cấp tỉnh vẫn đang trong quá trình “vừa triển khai vừa hoàn thiện”, bộc lộ nhiều điểm bất cập về cả cấu trúc lẫn năng lực vận hành, bộ máy bảo vệ DLCN với tư cách một chức năng quản trị chuyên biệt vẫn chưa được xây dựng đầy đủ và thống nhất. Thực trạng này thể hiện rõ trên ba bình diện có tính cấu trúc: (i) Tổ chức đầu mối; (ii) Phân công trách nhiệm theo chuỗi xử lý dữ liệu; (iii) Cơ chế phối hợp, xử lý yêu cầu của chủ thể dữ liệu và ứng phó sự cố.

Thứ nhất, về tổ chức bộ máy, biểu hiện phổ biến tại nhiều địa phương là chính quyền cấp tỉnh chưa thiết lập một cơ quan chuyên trách độc lập, thiếu một đầu mối duy nhất chịu trách nhiệm về bảo vệ DLCN trong phạm vi từng cơ quan chuyên môn mà chủ yếu vận hành theo mô hình phối hợp liên ngành, kiêm nhiệm. Trách nhiệm bảo vệ dữ liệu hiện đang được phân tán cho ba đầu mối chính: (1) Sở KH-CN, chịu trách nhiệm về hạ tầng kỹ thuật, an toàn thông tin; (2) Công an tỉnh, chịu trách nhiệm về an ninh mạng và quản trị Cơ sở dữ liệu quốc gia về dân cư - Đề án 06; (3) Các sở chuyên ngành, chủ quản dữ liệu trực tiếp như: Y tế, Tư pháp, Tài nguyên và Môi trường... Ở cấp tỉnh và các sở đều thành lập Ban chỉ đạo chuyển đổi số. Tuy nhiên, Ban chỉ đạo của tỉnh chủ yếu tham mưu, giúp Ủy ban nhân dân tỉnh và Chủ tịch Ủy ban nhân dân tỉnh chỉ đạo, điều phối và đôn đốc thực hiện các chủ trương, chiến lược, chương trình và kế hoạch về chuyển đổi số, phát triển chính quyền số, kinh tế số và xã hội số; Ban chỉ đạo cấp sở, ngành chủ yếu bước đầu xây dựng app, số hóa hồ sơ, tăng tỷ lệ dịch vụ công... chưa tập trung nhiều vào các giải pháp bảo vệ quyền DLCN.

Nhiệm vụ liên quan đến bảo vệ DLCN thường được bố trí theo hướng kiêm nhiệm, giao rải rác cho cán bộ CNTT, văn phòng hoặc pháp chế, tùy điều kiện tổ chức và nhân sự của từng đơn vị. Sự phân tán này khiến việc bảo vệ DLCN chỉ phát sinh trong quá trình vận hành chính quyền số mà không được xác lập thành một chức năng quản trị thường xuyên với thẩm quyền, trách nhiệm và nguồn lực rõ ràng. Thực tiễn cho thấy, hoạt động bảo vệ DLCN thường được chú trọng trong giai đoạn triển khai dự án (xây dựng hoặc nâng cấp cổng dịch vụ công, hệ thống một cửa, cơ sở dữ liệu chuyên ngành), song khi hệ thống đi vào vận hành ổn định thì cường độ kiểm soát dữ liệu giảm đáng kể, thiếu cơ chế duy trì định kỳ theo vòng đời dữ liệu. Một số địa phương điển hình như Đà Nẵng hoặc Bình Dương (cũ) đã hình thành các mô hình vận hành dựa trên dữ liệu với kho kết quả thủ tục hành chính số, IOC cấp tỉnh hoặc nền tảng điều hành tập trung. Tuy nhiên, ngay trong các mô hình này, chức năng bảo vệ DLCN vẫn chủ yếu được lồng ghép vào nhiệm vụ vận hành hệ thống hoặc an toàn thông tin, chưa được xây dựng thành một thiết chế quản trị quyền đối với DLCN độc lập. Điều này cho thấy, việc có mô hình kỹ thuật tiên tiến không đồng nghĩa với việc đã hình thành đầy đủ bộ máy bảo vệ quyền đối với DLCN theo quy chuẩn về QCN.

Thứ hai, về phân công trách nhiệm giữa các bộ phận, thực tiễn cho thấy trách nhiệm bảo vệ DLCN có xu hướng bị lệch về phía kỹ thuật, trong khi trách nhiệm pháp lý - nghiệp vụ chưa được xác lập tương xứng. Bộ phận CNTT hoặc đơn vị vận hành hệ thống thường được nhìn nhận là chủ thể chịu trách nhiệm chính khi xảy ra sự cố dữ liệu, mặc dù nhiều rủi ro lại phát sinh từ chính quy trình nghiệp vụ: thu thập dữ liệu vượt mức cần thiết; chia sẻ dữ liệu không đúng mục đích; xuất dữ liệu theo yêu cầu tình huống; hoặc quản lý hồ sơ kết hợp giấy - số thiếu nhất quán. Trong khi đó, các phòng chuyên môn, nơi trực tiếp phát sinh yêu cầu thu thập và sử dụng DLCN theo từng thủ tục hành chính, trong nhiều trường hợp chưa được xác định rõ là chủ thể chịu trách nhiệm trực tiếp về tính hợp pháp của mục đích xử lý, sự tương xứng giữa dữ liệu và yêu cầu giải quyết thủ tục, cũng như việc tuân thủ nguyên tắc tối thiểu hóa dữ liệu. Hệ quả là có thể tồn tại tình huống hệ thống an toàn về mặt kỹ thuật, nhưng quy trình xử lý dữ liệu vẫn tiềm ẩn nguy cơ xâm phạm quyền, do thiếu cơ chế bảo đảm tuân thủ ở cấp độ nghiệp vụ. Thực tiễn tại các địa phương triển khai mô hình một cửa tập trung điển hình như Quảng Ninh cho thấy, dù đầu mối tiếp nhận và trả kết quả được tổ chức tương đối rõ, nhưng trách nhiệm đối với dữ liệu lại phân tán theo các khâu thụ lý phía sau. Nếu không có cơ chế phân công trách nhiệm gắn với từng mắt xích của chuỗi xử lý, mô hình tập trung về dịch vụ vẫn có thể dẫn đến phân tán về trách nhiệm bảo vệ quyền đối với DLCN.

Bên cạnh đó, bộ phận pháp chế và thanh tra nội bộ tại nhiều cơ quan chuyên môn vẫn chủ yếu tập trung vào kiểm soát văn bản, trình tự thủ tục hành chính và kỷ luật công vụ, chưa tham gia một cách thường xuyên và có hệ thống vào quản trị rủi ro dữ liệu. Các nội dung như rà soát điều khoản hợp đồng với nhà thầu công nghệ liên quan đến phạm vi truy cập DLCN, nghĩa vụ bảo mật, cơ chế sao lưu - hủy dữ liệu, hay đánh giá mức độ tương thích của quy trình chia sẻ dữ liệu với mục đích xử lý, thường chưa trở thành một quy trình kiểm soát chuẩn trong nội bộ cơ quan.

Thực tế cho thấy, trong cơ cấu chỉ tiêu biên chế tại các sở, ban, ngành cấp tỉnh hiện nay chưa có bố trí vị trí việc làm dành riêng cho chuyên viên bảo vệ dữ liệu. Trách nhiệm này thường được giao cho cán bộ công nghệ thông tin hoặc cán bộ văn phòng (quá tải hoặc thiếu kiến thức chuyên sâu về công nghệ số). Đa số cán bộ cấp địa phương mới chỉ dừng lại ở mức hiểu bảo vệ dữ liệu là bảo mật máy tính, chưa nhận thức đúng về bảo vệ “quyền” của chủ thể dữ liệu (quyền được rút lại sự đồng ý, quyền yêu cầu xóa dữ liệu...). Kỹ năng xử lý các tình huống xâm phạm DLCN của đội ngũ này còn hạn chế, chủ yếu dựa trên kinh nghiệm cảm tính.

Thứ ba, về phối hợp nội bộ và liên thông giữa các cơ quan, đặc điểm của chính quyền số là dữ liệu được xử lý theo chuỗi liên thông: *bộ phận tiếp nhận hồ sơ - phòng*

chuyên môn - nền tảng dùng chung cấp tỉnh - chia sẻ liên ngành. Tuy nhiên, cơ chế phối hợp bảo vệ DLCN trong chuỗi này còn bộc lộ nhiều hạn chế như thiếu quy trình thống nhất khi chia sẻ hoặc liên thông dữ liệu: việc cung cấp dữ liệu giữa các cơ quan đôi khi dựa trên những yêu cầu nghiệp vụ hoặc thói quen chứ chưa được chuẩn hóa theo các tiêu chí tối thiểu như mục đích chia sẻ, phạm vi trường dữ liệu, thời hạn sử dụng, quyền truy cập theo vai trò và cơ chế truy vết. Khi phát sinh nghi ngờ truy cập bất thường hoặc nguy cơ lộ lọt dữ liệu, quá trình xác định đầu mối xử lý, phân cấp quyết định và tổ chức khắc phục thường lúng túng do thiếu một cơ chế điều phối sự cố dữ liệu gắn với trách nhiệm giải trình rõ ràng.

Mặt khác, ở nhiều địa phương, dữ liệu thuộc quyền quản lý của Nhà nước nhưng khả năng truy cập và thao tác kỹ thuật lại nằm ở chủ thể ngoài cơ quan, trong khi cơ chế kiểm soát nhà thầu về phạm vi xử lý dữ liệu, quyền truy cập, lưu trữ, sao lưu và hủy dữ liệu chưa được vận hành như một quy trình quản trị rủi ro bắt buộc. Điều này tạo ra khoảng trống trách nhiệm trong chuỗi xử lý dữ liệu và làm phức tạp việc truy cứu trách nhiệm khi xảy ra vi phạm quyền đối với DLCN.

Bên cạnh đó, việc thiếu một quy trình chuẩn về quản trị DLCN trong nội bộ cơ quan nhà nước, dẫn đến tình trạng: Khi dữ liệu an toàn, các bên đều nhận quyền quản lý; nhưng khi xảy ra sự cố lộ lọt thông tin công dân, trách nhiệm thường bị đẩy qua lại giữa Sở chuyên ngành (chủ quản nội dung) và Sở KHCN (chủ quản hạ tầng). Việc phân công trách nhiệm cá nhân trong việc khai thác dữ liệu chưa đi kèm với cơ chế hậu kiểm chặt chẽ. Nhật ký truy cập (log hệ thống) tại nhiều cơ quan cấp tỉnh dù có tồn tại nhưng ít khi được kiểm tra, giám sát định kỳ để phát hiện các hành vi tra cứu dữ liệu bất thường của cán bộ. Nhiều cơ quan chưa thiết lập kênh hoặc đầu mối rõ ràng để cá nhân thực hiện các quyền đối với DLCN của mình (tra cứu, chỉnh sửa, phản ánh việc sử dụng sai mục đích, yêu cầu giải trình...). Khi phát sinh yêu cầu, việc xử lý thường mang tính tình huống, phụ thuộc vào cá nhân tiếp nhận, thiếu quy trình phối hợp giữa pháp chế - chuyên môn, CNTT và thiếu chuẩn thời hạn giải quyết.

Tóm lại, nhiều sở, ban, ngành đã ban hành quyết định thành lập bộ phận chuyển đổi số, nhưng trên thực tế đang thiếu hụt nguồn nhân sự làm việc chuyên trách, có kiến thức về CNTT, nhất là thiếu kiến thức chuyên sâu về bảo vệ quyền DLCN. Thậm chí ở cấp xã thiếu nhân lực có chuyên môn về khoa học, công nghệ, chuyển đổi số; do chế độ, chính sách chưa tương xứng để thu hút nhân lực [64]. Có sự bất đối xứng về nhân lực giữa chính quyền và doanh nghiệp công nghệ: trong khi các tập đoàn công nghệ (bên thứ ba cung cấp dịch vụ cho tỉnh) có đội ngũ chuyên gia bảo mật hùng hậu, thì bộ máy quản lý nhà nước cấp tỉnh lại thiếu những nhân sự có đủ trình độ để giám sát hành vi của các doanh nghiệp này, dẫn đến nguy cơ “bị động”

trong việc bảo vệ dữ liệu của công dân địa phương. Chưa có cơ chế bảo vệ cán bộ thực thi; cán bộ, công chức làm nhiệm vụ bảo vệ dữ liệu đang phải chịu áp lực lớn về trách nhiệm pháp lý nhưng lại thiếu các hướng dẫn nghiệp vụ chi tiết và các công cụ công nghệ hỗ trợ, dẫn đến tâm lý e ngại, né tránh khi triển khai các dịch vụ công có liên quan đến dữ liệu nhạy cảm.

3.2.3. Thực trạng hạ tầng kỹ thuật, công nghệ bảo đảm an toàn, an ninh mạng nhằm bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh

Trong quá trình xây dựng chính quyền số cấp tỉnh giai đoạn 2020 - 2025, hạ tầng kỹ thuật và công nghệ bảo đảm an toàn, an ninh mạng cho các hệ thống thông tin hành chính đã có bước phát triển đáng kể, cả về quy mô đầu tư lẫn mức độ bao phủ. Tuy nhiên, xét từ góc độ bảo vệ quyền đối với DLCN, thực trạng này cho thấy sự chênh lệch rõ rệt giữa mức độ mở rộng hệ thống xử lý dữ liệu và năng lực bảo vệ dữ liệu tương ứng, đặc biệt ở cấp địa phương, là nơi trực tiếp vận hành công dịch vụ công, hệ thống giải quyết thủ tục hành chính và các cơ sở dữ liệu chuyên ngành.

Thứ nhất, về mức độ đầu tư và phổ cập hạ tầng an toàn thông tin ở cấp tỉnh, giai đoạn 2020 - 2025 ghi nhận xu hướng tích cực trong việc triển khai các giải pháp kỹ thuật bảo đảm an toàn, an ninh mạng cho hệ thống thông tin của cơ quan nhà nước. Theo báo cáo của Bộ KHCN, đến năm 2024, 100% bộ, ngành, địa phương đã kết nối mạng truyền số liệu chuyên dùng của cơ quan Đảng và Nhà nước; phần lớn các tỉnh, thành phố đã triển khai trung tâm dữ liệu (hoặc thuê dịch vụ trung tâm dữ liệu), hệ thống sao lưu, tường lửa, giám sát truy cập và các giải pháp bảo đảm an toàn thông tin ở mức cơ bản. Nhiều địa phương đã thành lập hoặc giao nhiệm vụ cho Trung tâm Giám sát, điều hành an toàn thông tin (SOC) ở cấp tỉnh hoặc tích hợp chức năng này trong Trung tâm IOC [9].

Tuy nhiên, thực tiễn cho thấy việc đầu tư hạ tầng an toàn thông tin chưa đồng đều giữa các địa phương, cả về quy mô, trình độ công nghệ và mức độ vận hành thực chất. Một số tỉnh, thành phố lớn điển hình như Hà Nội, Thành phố Hồ Chí Minh, Đà Nẵng, Bình Dương (cũ) đã nhanh chóng triển khai Trung tâm Giám sát, điều hành an toàn thông tin (SOC), hệ thống giám sát tập trung, phân tích nhật ký và cảnh báo sớm sự cố. Tuy nhiên, cơ sở vật chất, hạ tầng số, trang thiết bị làm việc và hạ tầng công nghệ thông tin tại nhiều địa phương còn khó khăn, nhất là những địa bàn vùng sâu, vùng xa, làm ảnh hưởng trực tiếp đến hiệu quả, chất lượng quản lý, điều hành, cung ứng dịch vụ công và giải quyết thủ tục hành chính cho người dân, doanh nghiệp. Vẫn còn thực trạng nhiều địa phương khác mới trang bị các giải pháp bảo mật rời rạc,

thiếu khả năng giám sát tập trung, phản ứng sớm và phối hợp xử lý sự cố theo thời gian thực [64].

Sự chênh lệch này dẫn đến tình trạng phạm vi xử lý dữ liệu mở rộng nhanh hơn năng lực bảo vệ dữ liệu, làm gia tăng rủi ro xâm hại quyền đối với DLCN tại những địa phương có mức độ số hóa cao nhưng an toàn thông tin hạn chế.

Thứ hai, về khả năng bảo vệ các hệ thống thông tin trọng yếu gắn với xử lý DLCN, như Cổng dịch vụ công, Hệ thống thông tin giải quyết thủ tục hành chính, các cơ sở dữ liệu chuyên ngành và nền tảng tích hợp, chia sẻ dữ liệu, thực tiễn cho thấy trọng tâm bảo vệ hiện nay vẫn thiên về bảo đảm tính sẵn sàng và liên tục của hệ thống hơn là bảo vệ quyền đối với DLCN theo vòng đời dữ liệu. Nhiều hệ thống được xây dựng ưu tiên khả năng tiếp nhận hồ sơ, liên thông dữ liệu và xử lý giao dịch với lưu lượng lớn, trong khi các chức năng kiểm soát truy cập theo vai trò, ghi nhật ký chi tiết, phân tách môi trường dữ liệu, mã hóa dữ liệu nhạy cảm hoặc kiểm soát truy xuất dữ liệu sau khi hoàn tất thủ tục chưa được triển khai đồng bộ.

Ở những địa phương đẩy mạnh dịch vụ công trực tuyến toàn trình và tái sử dụng dữ liệu (như Đà Nẵng, Bình Dương), khối lượng DLCN được lưu trữ tập trung và kết nối liên thông ngày càng lớn. Tuy nhiên, việc bảo đảm rằng mỗi lần truy cập, khai thác hoặc tái sử dụng dữ liệu đều có căn cứ, có phân quyền và có khả năng truy vết vẫn là thách thức kỹ thuật - tổ chức đáng kể. Điều này làm phát sinh nguy cơ xâm hại quyền đối với DLCN trong nội bộ hệ thống, tức dữ liệu không bị tấn công từ bên ngoài nhưng có thể bị truy cập vượt thẩm quyền, sử dụng sai mục đích hoặc lưu trữ quá thời hạn cần thiết.

Thứ ba, về năng lực phòng ngừa, phát hiện và ứng phó sự cố an ninh mạng, các số liệu giai đoạn 2020 - 2025 cho thấy rủi ro tấn công mạng đối với hệ thống thông tin tại Việt Nam gia tăng nhanh cả về số lượng và mức độ tinh vi. Báo cáo khảo sát an ninh mạng năm 2025 ghi nhận Việt Nam phải đối mặt với khoảng 552.000 cuộc tấn công mạng trong năm, và trên 52% cơ quan, tổ chức được khảo sát cho biết đã chịu thiệt hại do tấn công mạng [34]. Trong bối cảnh đó, nhiều hệ thống thông tin cấp tỉnh vẫn chủ yếu vận hành theo mô hình phản ứng sau sự cố, thiếu năng lực giám sát chủ động, phân tích hành vi bất thường và phối hợp xử lý theo kịch bản định sẵn. Khi xảy ra sự cố, việc xác định phạm vi dữ liệu bị ảnh hưởng, cá nhân chịu tác động và nghĩa vụ thông báo, khắc phục thường gặp khó khăn do thiếu công cụ kỹ thuật và quy trình phối hợp liên ngành rõ ràng. Đặc biệt, những nguy cơ, rủi ro xâm hại quyền đối với DLCN lại đến từ các hình thức tấn công ngoài hệ thống nhưng khai thác thương hiệu và quy trình hành chính, như mạo danh cổng dịch vụ công, giả mạo ứng dụng hoặc cán bộ để đánh cắp thông tin đăng nhập, dữ liệu định danh và thông tin

thanh toán. Thực tiễn cho thấy nhiều vụ việc người dân bị lừa cài đặt ứng dụng giả mạo dịch vụ công, dẫn đến mất quyền kiểm soát thiết bị và thiệt hại tài sản lớn. Các hành vi này cho thấy bảo vệ quyền đối với DLCN không chỉ là vấn đề kỹ thuật nội bộ, mà còn gắn với năng lực truyền thông cảnh báo, xác thực kênh chính thức và bảo vệ người dùng khi tiếp xúc với hệ thống.

Thứ tư, về mối quan hệ giữa hạ tầng kỹ thuật và trách nhiệm giải trình trong bảo vệ quyền đối với DLCN, thực tiễn cho thấy nhiều địa phương vẫn tiếp cận an toàn, an ninh mạng chủ yếu như một yêu cầu kỹ thuật, tách rời khỏi cơ chế thực thi quyền của chủ thể dữ liệu. Các hệ thống có thể được trang bị tường lửa, phần mềm chống mã độc, sao lưu dữ liệu, nhưng lại thiếu các chức năng hỗ trợ trực tiếp cho việc thực hiện quyền đối với DLCN, như: truy vết lịch sử truy cập dữ liệu theo từng cá nhân; xác định dữ liệu nào của cá nhân đang được lưu trữ ở đâu; hỗ trợ kiểm soát thời hạn lưu trữ và xóa dữ liệu khi không còn mục đích xử lý. Khoảng trống này khiến việc chuyển hóa quyền đối với DLCN từ “quyền trên giấy” sang “quyền có thể thực thi” gặp nhiều hạn chế trong thực tiễn chính quyền số cấp tỉnh.

Từ các phân tích trên có thể thấy rằng, mặc dù hạ tầng kỹ thuật và công nghệ bảo đảm an toàn, an ninh mạng cho hệ thống thông tin cấp tỉnh đã có bước phát triển đáng kể trong giai đoạn 2020 - 2025, nhưng vẫn tồn tại khoảng cách đáng kể giữa yêu cầu bảo vệ quyền đối với DLCN và năng lực bảo vệ dữ liệu thực tế. Hạ tầng an toàn thông tin hiện nay nhìn chung mới đáp ứng yêu cầu bảo vệ hệ thống, chưa được xây dựng đầy đủ theo logic bảo vệ quyền đối với DLCN theo vòng đời và trách nhiệm giải trình. Trong bối cảnh Luật Bảo vệ dữ liệu cá nhân có hiệu lực từ ngày 01/01/2026, những hạn chế này đặt ra yêu cầu cấp thiết đối với chính quyền cấp tỉnh phải chuyển từ mô hình đầu tư an toàn thông tin mang tính phòng vệ kỹ thuật sang mô hình quản trị an toàn dữ liệu gắn với QCN, trong đó hạ tầng kỹ thuật phải trở thành công cụ hỗ trợ trực tiếp cho việc kiểm soát mục đích xử lý, phân quyền truy cập, truy vết trách nhiệm và bảo đảm khả năng thực thi quyền của chủ thể dữ liệu.

Thứ năm, về thực trạng triển khai các giải pháp công nghệ bảo mật tại các kho dữ liệu dùng chung của tỉnh. Hiện nay, các kho dữ liệu dùng chung và Nền tảng tích hợp, chia sẻ dữ liệu cấp tỉnh (LGSP) đã được hình thành, song qua khảo sát thực tiễn dưới góc độ bảo đảm quyền con người, việc triển khai các giải pháp công nghệ bảo mật (mã hóa, xác thực, tường lửa, hệ thống ghi vết) vẫn tồn tại nhiều lỗ hổng lớn, cụ thể:

(1). Về công nghệ mã hóa: Thực trạng hiện nay cho thấy tình trạng “mã hóa không đồng bộ” vẫn còn hiện hữu. Phần lớn dữ liệu chỉ được mã hóa trên đường truyền bằng các giao thức cơ bản, nhưng lại gần như bỏ trống việc mã hóa ở trạng

thái lưu trữ trong các cơ sở dữ liệu chuyên ngành (hộ tịch, đất đai, y tế). Dữ liệu trong cấu trúc bảng cơ sở dữ liệu của nhiều sở, ngành vẫn lưu dưới dạng văn bản thuần túy, chưa được mã hóa. Thực trạng này dẫn đến nguy cơ: chỉ cần hệ thống bị xâm nhập hoặc cán bộ quản trị hệ thống (Admin) có ý đồ xấu, toàn bộ DLCN định danh của hàng triệu công dân sẽ bị khai thác một cách dễ dàng mà không có rào cản kỹ thuật nào ngăn chặn.

(2). Về cơ chế xác thực: Mặc dù hệ thống một cửa điện tử đã triển khai cấp tài khoản riêng cho từng cán bộ, công chức, nhưng phương thức xác thực vẫn dừng lại ở mức yếu và lạc hậu (chỉ dùng mật khẩu tĩnh). Tình trạng cán bộ công vụ dùng chung tài khoản, chia sẻ mật khẩu để “làm hộ” hồ sơ khi quá tải, hoặc không đăng xuất tài khoản khi rời vị trí làm việc diễn ra phổ biến tại bộ phận một cửa cấp huyện, cấp xã trong thời gian qua. Việc thiếu vắng cơ chế xác thực mạnh đa nhân tố (MFA) đối với các tài khoản có quyền khai thác sâu vào kho dữ liệu là nguyên nhân trực tiếp dẫn đến nguy cơ lộ lọt tài khoản và bị kẻ xấu lợi dụng để thu thập DLCN trái phép.

(3). Về hệ thống tường lửa và giám sát an ninh: Hầu hết các tỉnh đều đã trang bị tường lửa ứng dụng web (WAF) và kết nối với Trung tâm Giám sát an toàn thông tin (SOC) tỉnh. Mặc dù vậy, năng lực của hệ thống tường lửa hiện tại chỉ dừng lại ở mức độ phòng chống các hình thức tấn công bề nổi như thay đổi giao diện (Defacement) hoặc từ chối dịch vụ (DDoS); chưa đạt đến khả năng kiểm soát và phân tích chuyên sâu (Deep Packet Inspection) để phát hiện các hành vi dò quét, trích xuất và đánh cắp dữ liệu (Data Exfiltration) mang tính tinh vi. Bên cạnh đó, Trung tâm Giám sát an toàn thông tin (SOC) tại một số địa phương còn vận hành mang tính hình thức, thiếu hụt đội ngũ chuyên gia phân tích mã độc và dữ liệu độc hại theo thời gian thực để thực hiện cơ chế cảnh báo sớm.

(4). Về hệ thống ghi vết tự động (Audit Logs): Đây là “khoảng trống” nguy hiểm nhất dưới góc độ trách nhiệm giải trình. Hệ thống nhật ký (Log) của phần mềm hành chính công hiện nay chỉ ghi nhận các tác vụ mang tính cơ học (như thời gian đăng nhập, đăng xuất, chuyển bước hồ sơ) nhưng không ghi vết chi tiết hành vi truy cập dữ liệu (Data Access Logs). Điển hình như: Một công chức tự ý tra cứu thông tin lý lịch tư pháp, địa chỉ nhà ở hoặc lịch sử tiêm chủng của một công dân (không thuộc hồ sơ mình đang xử lý) thì hệ thống không hề cảnh báo và không ghi lại bằng chứng cụ thể. Việc thiếu hệ thống nhật ký kiểm tra độc lập, không thể sửa xóa tệp tin khiến cho việc quy trách nhiệm công vụ khi xảy ra sự cố lộ lọt dữ liệu trở nên bất khả thi trong thực tiễn.

(5). Việc áp dụng nguyên tắc “Bảo vệ dữ liệu ngay từ khâu thiết kế” trong phần mềm công của địa phương còn hạn chế. Nguyên tắc này là một chuẩn mực quốc

tế cốt lõi (theo GDPR), đòi hỏi việc bảo vệ quyền riêng tư của công dân phải được tích hợp sẵn vào cấu trúc của công nghệ ngay từ khi lập trình hệ thống, chứ không phải là biện pháp chắp vá sau khi phần mềm đã hoàn thành. Qua đánh giá thực trạng các phần mềm dịch vụ công, cổng thông tin và ứng dụng di động công dân (App công dân của tỉnh), việc áp dụng nguyên tắc này tại Việt Nam hiện nay đang ở trạng thái rất mờ nhạt và bị xem nhẹ. Thay vì áp dụng nguyên tắc “Tối thiểu hóa dữ liệu” (Data Minimization), các biểu mẫu điện tử (E-form) trên cổng dịch vụ công của tỉnh được thiết kế theo tư duy cũ; bắt buộc công dân phải điền rất nhiều thông tin không liên quan trực tiếp đến thủ tục cần giải quyết, như: làm thủ tục cấp phép xây dựng nhưng biểu mẫu yêu cầu khai cả số điện thoại của người thân, nghề nghiệp, dân tộc, tôn giáo... Phần mềm công đang vận hành theo cơ chế “Mặc định công khai” thay vì “Mặc định bảo mật” (Privacy by Default). Sự thiếu vắng công cụ tự quyết cho chủ thể dữ liệu: Trong cấu trúc mã nguồn của các phần mềm công, các kỹ sư lập trình hoàn toàn không thiết kế giao diện hay nút chức năng nào để công dân thực hiện các quyền thực chất của mình (như đã phân tích tại lỗi hệ thống All-or-Nothing ở mục trước). Không có module chức năng nào cho phép người dân nhấn nút “Rút lại sự đồng ý xử lý dữ liệu” hoặc tự động theo dõi xem dữ liệu của mình đã được hệ thống chia sẻ cho những sở, ngành nào. Hệ thống được thiết kế hoàn toàn phục vụ cho mục đích đơn giản hóa thao tác quản lý của cơ quan nhà nước, bỏ quên quyền kiểm soát dữ liệu của người dân. Thiếu quy trình đánh giá tác động bảo vệ dữ liệu (DPIA) trước khi nghiệm thu: Thực tế tại các địa phương, khi nghiệm thu và đưa vào vận hành một phần mềm một cửa mới hoặc hệ thống camera thông minh IOC, Hội đồng nghiệm thu của tỉnh (gồm Sở KHCN, Sở Tài chính...) chỉ đánh giá phần mềm dựa trên các tiêu chí: chạy có mượt không, giao diện có đẹp không, có tích hợp được với cổng quốc gia không. Hoàn toàn không có bất kỳ bước đánh giá tác động đến quyền con người và quyền đối với DLCN nào được thực hiện. Việc bỏ qua bước thẩm định này khiến các phần mềm công cấp tỉnh còn khiếm khuyết về mặt bảo mật quyền riêng tư trước khi đến tay người dân.

Có thể thấy, nguy cơ kỹ thuật, hệ thống bị mã hóa độc hại (Ransomware) hoặc rò rỉ dữ liệu do lỗi bảo mật Cloud tác động đến Quyền con người; điều này trực tiếp xâm phạm Quyền an toàn dữ liệu và Quyền riêng tư của công dân, làm lộ diện các thông tin nhạy cảm (nhân thân, tài chính, y tế...), đẩy công dân vào rủi ro bị đe dọa, lừa đảo hoặc xúc phạm danh dự. Thực trạng này phản ánh sự thiếu hụt trong nghĩa vụ tuân thủ các chuẩn mực an toàn của cơ quan công quyền. Khi sự cố xảy ra, nếu chính quyền không có cơ chế cảnh báo tức thì cho công dân và không xác định được trách nhiệm bồi thường thiệt hại, cơ chế bảo vệ quyền sẽ bị đứt gãy.

3.2.4. Thực trạng về công tác thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm liên quan đến bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh

Trong giai đoạn từ năm 2020 đến năm 2025, công tác thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm đóng vai trò then chốt trong việc bảo đảm quyền được bảo vệ và quyền được khắc phục hiệu quả khi DLCN bị xâm hại. Tuy nhiên, thực tiễn triển khai cho thấy năng lực kiểm soát và chế tài trong lĩnh vực này vẫn chưa theo kịp tốc độ mở rộng của chính quyền số, đặc biệt ở cấp tỉnh - nơi trực tiếp phát sinh phần lớn các hoạt động xử lý dữ liệu.

Thứ nhất, về thẩm quyền và tổ chức thực thi, việc ban hành Nghị định số 13/2023/NĐ-CP đã tạo bước ngoặt quan trọng khi xác lập rõ vai trò chủ trì của Bộ Công an trong quản lý nhà nước về bảo vệ DLCN, bao gồm thanh tra, kiểm tra và xử lý vi phạm, đồng thời đặt cơ chế phối hợp với Bộ Thông tin và Truyền thông trong phạm vi an toàn thông tin mạng. Tuy nhiên, trong thực tiễn cấp tỉnh, cơ chế thực thi vẫn mang tính đa kênh: khi phát sinh hành vi xâm hại DLCN trong quá trình giải quyết thủ tục hành chính điện tử, người dân thường phản ánh thông qua các kênh chung như tiếp công dân, thanh tra hành chính, phản ánh kiến nghị về thủ tục hành chính hoặc tố giác tội phạm. Việc thiếu một cơ chế chuyên biệt, dễ tiếp cận và có tính dự đoán cao dành riêng cho khiếu nại về xử lý DLCN khiến quyền khiếu nại, tố cáo tồn tại về mặt hình thức nhưng khó được kích hoạt một cách hiệu quả trong thực tiễn.

Thứ hai, về hoạt động thanh tra, kiểm tra, giai đoạn 2020 - 2025 cho thấy trọng tâm kiểm tra liên quan đến DLCN vẫn chủ yếu đặt trong các cuộc thanh tra chuyên ngành hoặc thanh tra công vụ, thay vì thanh tra chuyên đề về quyền đối với DLCN. Ở cấp độ trung ương, các đợt thanh tra, kiểm tra của Bộ Thông tin và Truyền thông trong giai đoạn 2021 - 2023 tập trung nhiều vào doanh nghiệp viễn thông, nền tảng số và an toàn hệ thống, với các kết quả xử phạt hành chính hàng tỷ đồng đối với hành vi vi phạm nghĩa vụ quản lý thông tin thuê bao hoặc để xảy ra lộ lọt dữ liệu. Tuy nhiên, các kết luận thanh tra công bố công khai ít khi phân tích sâu các tiêu chí mang tính quyền đối với DLCN như mục đích xử lý, tối thiểu hóa dữ liệu, thời hạn lưu trữ hoặc cơ chế thực hiện quyền của chủ thể dữ liệu.

Ở cấp tỉnh, một số địa phương đã tiến hành thanh tra chuyên đề về trách nhiệm giải quyết thủ tục hành chính và vận hành cổng dịch vụ công, điển hình như trong giai đoạn 2022 - 2024, kết luận thanh tra tại một số tỉnh cho thấy tồn tại các sai sót trong việc số hóa hồ sơ, quản lý dữ liệu kết quả giải quyết thủ tục hành chính và phân quyền truy cập hệ thống. Tuy nhiên, các kết luận này thường dừng ở việc kiến nghị khắc phục về quy trình, kỷ luật hành chính hoặc trách nhiệm cá nhân trong chậm trễ,

sai sót thủ tục, mà chưa coi việc xử lý DLCN vượt phạm vi, lưu trữ kéo dài hoặc chia sẻ dữ liệu không rõ mục đích là một dạng vi phạm quyền cần được nhận diện và xử lý độc lập.

Thứ ba, về xử lý vi phạm, số liệu giai đoạn 2023 - 2025 cho thấy các cơ quan chức năng đã tăng cường phát hiện và xử lý các vụ việc mua bán, trao đổi trái phép DLCN với quy mô lớn. Trong năm 2025, lực lượng chức năng đã phát hiện hàng chục vụ việc liên quan đến mua bán trái phép dữ liệu, với tổng số bản ghi bị thu thập và giao dịch trái phép lên tới hàng trăm triệu [34]. Những vụ việc này cho thấy tính nghiêm trọng và tính hệ thống của hành vi xâm hại DLCN trong môi trường số. Tuy nhiên, phần lớn các vụ việc bị xử lý theo hướng hình sự hoặc xử phạt hành chính đối với các đường dây, tổ chức vi phạm, trong khi cơ chế khắc phục quyền cho cá nhân bị ảnh hưởng (thông báo vi phạm, xác định phạm vi dữ liệu bị xâm hại, bồi thường hoặc hỗ trợ khắc phục) chưa được thể hiện rõ ràng trong thực tiễn xử lý.

Thứ tư, về giải quyết khiếu nại, tố cáo và yêu cầu khắc phục của chủ thể dữ liệu, thực tiễn ở nhiều địa phương cho thấy số lượng khiếu nại, tố cáo trực tiếp liên quan đến DLCN trong hoạt động hành chính còn hạn chế so với quy mô xử lý dữ liệu thực tế. Điều này có thể xuất phát từ việc người dân thiếu thông tin về quyền đối với DLCN, thiếu kênh tiếp nhận chuyên biệt, hoặc không rõ cơ quan nào có thẩm quyền giải quyết. Tại các địa phương có tỷ lệ dịch vụ công trực tuyến toàn trình cao như Đà Nẵng hay Bình Dương, dù khối lượng hồ sơ trực tuyến và dữ liệu phát sinh rất lớn, nhưng chưa ghi nhận cơ chế công khai thông kê hoặc báo cáo riêng về khiếu nại, phản ánh liên quan đến xử lý DLCN. Điều này làm hạn chế khả năng đánh giá hiệu lực bảo vệ quyền trong thực tiễn và trách nhiệm giải trình của cơ quan nhà nước.

Thứ năm, công tác thanh tra và xử lý vi phạm liên quan đến DLCN còn chịu ảnh hưởng bởi sự phụ thuộc vào mô hình thanh tra truyền thống. Nhiều cuộc thanh tra được xây dựng để kiểm tra việc chấp hành pháp luật về thủ tục hành chính, cải cách hành chính hoặc kỷ luật công vụ, trong khi tiêu chí đánh giá về bảo vệ quyền đối với DLCN chưa được tích hợp một cách có hệ thống. Ngay cả tại các địa phương đã đầu tư mạnh cho hạ tầng số và IOC, việc giám sát truy cập dữ liệu, phát hiện truy cập bất thường và chuyển hóa kết quả giám sát thành căn cứ thanh tra - xử lý vi phạm vẫn còn hạn chế, khiến công cụ kỹ thuật chưa thực sự được khai thác như một phần của cơ chế bảo vệ quyền.

Có thể thấy trong giai đoạn 2020 - 2025, công tác thanh tra, kiểm tra và xử lý vi phạm liên quan đến DLCN ở Việt Nam đã có bước phát triển nhất định, đặc biệt trong việc phát hiện và xử lý các hành vi vi phạm nghiêm trọng, có tổ chức. Tuy nhiên, ở cấp tỉnh, cơ chế thanh tra và khắc phục quyền vẫn bộc lộ những hạn chế như

thiếu trọng tâm trong thanh tra; thiếu cơ chế tiếp nhận và xử lý yêu cầu của chủ thể dữ liệu; thiếu liên kết giữa giám sát kỹ thuật với trách nhiệm giải trình pháp lý. Trong bối cảnh Luật Bảo vệ DLCN có hiệu lực từ ngày 01/01/2026, những hạn chế này đặt ra yêu cầu cấp thiết phải tái cấu trúc công tác thanh tra, kiểm tra ở cấp tỉnh theo hướng chuẩn hóa tiêu chí thanh tra về quyền đối với DLCN; thiết lập cơ chế tiếp nhận, giải quyết khiếu nại về xử lý DLCN rõ ràng, dễ tiếp cận; và bảo đảm khả năng truy vết, giải trình và khắc phục hữu hiệu khi quyền đối với DLCN bị xâm hại trong toàn bộ vòng đời xử lý dữ liệu.

3.2.5. Thực trạng tuyên truyền, phổ biến và nâng cao nhận thức của cán bộ, công chức, người dân và xã hội về bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh

Trong bối cảnh chính quyền số cấp tỉnh giai đoạn 2020 - 2025, nhận thức của cán bộ, công chức và người dân về quyền và nghĩa vụ liên quan đến DLCN là yếu tố quan trọng, có tính quyết định hiệu lực bảo vệ quyền đối với DLCN trong thực tiễn.

Thứ nhất, đối với cán bộ, công chức, nhận thức về DLCN trong giai đoạn 2020 - 2025 nhìn chung vẫn được hình thành chủ yếu thông qua yêu cầu bảo đảm an toàn, an ninh hệ thống thông tin, thay vì được tiếp cận như một nghĩa vụ bảo vệ QCN phát sinh từ hoạt động công vụ. Các chương trình, kế hoạch nâng cao nhận thức về an toàn thông tin mạng của Nhà nước ta tập trung chủ yếu vào kỹ năng phòng, chống tấn công mạng, bảo vệ tài khoản, hệ thống và dữ liệu của cơ quan, trong khi nội dung về quyền của chủ thể dữ liệu, nghĩa vụ pháp lý của người xử lý dữ liệu và trách nhiệm giải trình khi xâm phạm quyền đối với DLCN chưa được tích hợp một cách hệ thống vào đào tạo công vụ. Tại nhiều cơ quan chuyên môn cấp tỉnh, cán bộ nghiệp vụ vẫn có xu hướng coi DLCN là thông tin phục vụ giải quyết thủ tục, còn trách nhiệm bảo vệ dữ liệu chủ yếu thuộc về bộ phận CNTT hoặc đơn vị vận hành hệ thống. Nhận thức này dẫn đến hệ quả là nhiều hành vi xử lý dữ liệu phát sinh trong thực tiễn nghiệp vụ (yêu cầu bổ sung trường thông tin; yêu cầu nộp tệp hồ sơ chứa thông tin nhạy cảm; truy xuất dữ liệu từ kho dùng chung; chia sẻ dữ liệu theo yêu cầu phối hợp liên ngành) chưa được đặt thường xuyên trong khung phân tích về căn cứ pháp lý, mục đích xử lý, mức độ cần thiết và giới hạn sử dụng.

Thứ hai, đối với cá nhân, nhận thức về DLCN trong giai đoạn 2020 - 2025 có xu hướng tăng lên cùng với việc mở rộng sử dụng dịch vụ công trực tuyến và định danh điện tử, song vẫn mang tính thực dụng và phòng vệ hơn là nhận thức đầy đủ về quyền. Nhiều người dân tiếp cận DLCN theo quan điểm “đổi dữ liệu lấy tiện ích hành chính” khi sẵn sàng cung cấp thông tin để được giải quyết thủ tục nhanh hơn, giảm giấy tờ, trong khi hiểu biết về các quyền đối với DLCN (quyền được biết, quyền kiểm

soát mục đích xử lý, quyền yêu cầu chỉnh sửa, phản ánh hoặc khắc phục khi dữ liệu bị xử lý sai) còn hạn chế. Thực tế này phần nào xuất phát từ việc thông báo về xử lý dữ liệu trên các cổng dịch vụ công và nền tảng số thường mang tính tổng quát, khó chuyển hóa thành khả năng thực hành quyền đối với người dùng phổ thông. Mặt khác, người dân có xu hướng quan tâm mạnh đến rủi ro “mất tiền, bị lừa” hơn là rủi ro “bị xử lý dữ liệu sai mục đích”, dẫn đến hành vi phòng vệ tập trung vào bảo mật OTP, tài khoản ngân hàng, trong khi ít nhận thức về các rủi ro dài hạn như bị khai thác dữ liệu nhạy cảm, bị theo dõi lịch sử giao dịch hành chính hoặc bị tái sử dụng dữ liệu ngoài mục đích ban đầu.

Khoảng trống về mặt nhận thức của người dân được phản ánh thông qua những số liệu về lừa đảo trực tuyến trong giai đoạn 2023 - 2025. Tỷ lệ người dùng bị lừa đảo trực tuyến chiếm tỷ lệ cao, đã gây thiệt hại lớn về kinh tế, với tổng giá trị thiệt hại ước tính hàng chục nghìn tỷ đồng mỗi năm [34]; nhiều vụ việc có đặc điểm chung là đối tượng phạm tội đã mạo danh cán bộ Nhà nước và cổng dịch vụ công hoặc ứng dụng định danh để yêu cầu cung cấp thông tin định danh, mã xác thực hoặc thao tác sinh trắc học. Điều này cho thấy rủi ro xâm hại DLCN trong bối cảnh chính quyền số không chỉ gắn với lộ lọt dữ liệu, mà còn trực tiếp đe dọa quyền tài sản và quyền được bảo vệ trước hành vi phạm pháp của cá nhân. Do đó, nhận thức về DLCN của người dân cần được nâng lên thành năng lực nhận diện rủi ro và thực hành quyền đối với DLCN (biết kênh chính thức, yêu cầu giải trình, phản ánh và khiếu nại khi có dấu hiệu bị xâm hại dữ liệu).

Ở cấp địa phương, các hoạt động tuyên truyền và phổ biến, giáo dục pháp luật và các phương thức, thủ đoạn của các đối tượng phạm tội được triển khai rộng rãi trong giai đoạn 2024 - 2025, tập trung vào việc nhận diện cổng dịch vụ công chính thức, ứng dụng định danh hợp pháp và thủ đoạn giả mạo phổ biến. Tuy nhiên, cách tiếp cận truyền thông vẫn chủ yếu dừng ở việc cảnh báo nguy hiểm, chưa chuyển hóa thành giáo dục quyền đối với DLCN theo nghĩa đầy đủ để giúp người dân hiểu rõ dữ liệu của mình được thu thập và sử dụng ra sao trong quy trình hành chính, họ có những quyền gì đối với dữ liệu đã cung cấp, và phải làm gì khi nghi ngờ dữ liệu bị xử lý trái mục đích hoặc bị xâm hại.

Qua tổng hợp, phân tích nội dung đối với 100 bài viết, tin tức và tài liệu tuyên truyền về Chuyển đổi số, Chính quyền số được đăng tải trên Cổng thông tin điện tử của 05 tỉnh/thành phố (Hà Nội, TP HCM, Đà Nẵng, Thanh Hóa, Nghệ An), trong giai đoạn 2023 - 2025 cho thấy sự lệch pha rõ rệt về mặt định hướng thông tin, nhất là tỷ lệ phân bổ nội dung: Khoảng 82% dung lượng tuyên truyền tập trung vào nội dung “thúc đẩy nộp hồ sơ trực tuyến, tiện ích của chính quyền số và chỉ tiêu hoàn thành

TTHC”; 13% tuyên truyền về “cảnh báo lừa đảo trên không gian mạng (An ninh mạng)”; và chỉ có dưới 5% dung lượng đề cập đến “quyền của công dân đối với dữ liệu cá nhân, quyền từ chối cung cấp thông tin ngoài quy định và quyền tự quyết thông tin”. Điều này dẫn đến thực trạng người dân bị cuốn vào tiến trình số hóa trong vị thế “thụ động chấp nhận”, hoàn toàn thiếu thông tin và kỹ năng để chủ động thực thi các quyền năng kỹ thuật (xem, sửa, xóa, rút sự đồng ý) trên các nền tảng số công quyền.

Khi nhận thức quyền đối với DLCN chưa được hình thành bền vững, người dân khó có thể đóng vai trò là chủ thể tích cực trong cơ chế bảo vệ quyền, mà chủ yếu ở vị thế bị động và phòng vệ. Điều này làm suy giảm hiệu lực thực thi quyền đối với DLCN trong chính quyền số cấp tỉnh, bởi quyền chỉ thực sự được bảo vệ khi được nhận thức đầy đủ và thực hành một cách có ý thức bởi cả chủ thể xử lý dữ liệu và chủ thể dữ liệu. Trong bối cảnh Luật Bảo vệ dữ liệu cá nhân có hiệu lực từ ngày 01/01/2026, thực trạng nêu trên đặt ra yêu cầu cấp thiết phải chuyển trọng tâm từ tuyên truyền an toàn thông tin sang giáo dục quyền đối với DLCN và trách nhiệm giải trình đối với cán bộ, công chức là đào tạo gắn với vòng đời xử lý dữ liệu và nghĩa vụ pháp lý cụ thể; đối với người dân là xây dựng cơ chế thông tin, hướng dẫn và phản hồi quyền đối với DLCN theo hướng dễ hiểu, dễ tiếp cận và có khả năng sử dụng trong thực tiễn.

Thứ ba, đối với xã hội: Tuyên truyền, phổ biến và giáo dục nâng cao nhận thức xã hội là phương thức mang tính phòng ngừa từ sớm, từ xa. Phương thức này nhằm thu hẹp “khoảng cách thông tin” giữa chính quyền và người dân, đồng thời trang bị bộ công cụ kỹ năng để công dân số tự bảo vệ quyền tự quyết thông tin của mình. Thực tiễn triển khai phương thức này tại các địa phương thời gian qua ghi nhận nhiều nỗ lực đổi mới: Đa dạng hóa mô hình và hướng về cơ sở, Chính quyền cấp tỉnh (chủ trì bởi Sở Thông tin và Truyền thông và nay là Sở KHCN phối hợp với Công an tỉnh) đã triển khai nhiều chiến dịch diện rộng với cách làm sáng tạo, phát huy vai trò của Tổ công nghệ số cộng đồng; đây là lực lượng nòng cốt tại cơ sở. Với mô hình “đi từng ngõ, gõ từng nhà”, các thành viên của tổ đã trực tiếp hướng dẫn người dân từ cấp xã đến thôn cách thức cài đặt, sử dụng tài khoản định danh điện tử VNeID, các app công dân số của tỉnh; đồng thời lồng ghép cảnh báo người dân không tự ý chia sẻ ảnh chụp Căn cước công dân, số điện thoại lên các hội nhóm mạng xã hội.

Đổi mới hình thức tuyên truyền trực quan, số hóa. Thay vì phát tờ rơi hay đọc loa phát thanh truyền thống, các tỉnh đã xây dựng các chiến dịch truyền thông đa phương tiện. Xuất hiện nhiều video ngắn (TikTok, Reels), bài viết đồ họa (Infographic) trực quan đăng tải trên các trang Zalo Official Account, fanpage của

chính quyền địa phương đề hướng dẫn cách nhận diện các đường link lừa đảo đánh cắp dữ liệu, cách bảo mật mật khẩu dịch vụ công và cách thiết lập quyền riêng tư trên thiết bị di động.

Các tuần lễ, chiến dịch chuyên đề như “Chiến dịch tháng hành động tuyên truyền về nhận diện và phòng chống lừa đảo trực tuyến” hay “Tuần lễ an toàn thông tin” được tổ chức đồng loạt tại nhiều tỉnh, thành (như TP.HCM, Đà Nẵng, Quảng Ninh...), tạo hiệu ứng truyền thông mạnh mẽ trong cộng đồng doanh nghiệp và người dân tại địa bàn.

Tuy nhiên, nội dung tuyên truyền còn nặng tính “chuyển đổi số một chiều”, chưa cân bằng với “bảo vệ quyền”. Hầu hết các chiến dịch tuyên truyền của tỉnh hiện nay mới chỉ tập trung thúc đẩy người dân cung cấp dữ liệu, vận động cài đặt ứng dụng, nộp hồ sơ trực tuyến (tức là tập trung vào mục tiêu quản lý của chính quyền). Ngược lại, nội dung hướng dẫn cho người dân biết về “quyền của mình theo Nghị định 13/2023/NĐ-CP và Luật 91 (như quyền yêu cầu xóa dữ liệu, quyền rút lại sự đồng ý, quy trình nộp khiếu nại khi phát hiện cơ quan nhà nước làm lộ thông tin...)” còn rất mờ nhạt và mang tính hình thức.

Tuyên truyền về kỹ năng số chưa theo kịp sự tinh vi của tội phạm công nghệ. Các nội dung phổ biến tại địa phương thường dừng lại ở mức căn bản (như nhắc nhở đổi mật khẩu, không bấm vào link lạ...). Trong khi đó, các hình thức thu thập dữ liệu bất hợp pháp như lừa đảo bằng công nghệ Deepfake (giả mạo khuôn mặt/giọng nói), chiếm quyền điều khiển điện thoại để rút sạch dữ liệu nền tảng lại phát triển quá nhanh, khiến nội dung tuyên truyền tại địa phương luôn rơi vào trạng thái “chạy theo sau”.

Khoảng cách nhận thức số giữa các vùng miền và nhóm đối tượng. Tại cùng một tỉnh, nhận thức về quyền DLCN có sự phân hóa sâu sắc. Trong khi người dân ở vùng đô thị đã có ý thức nhất định về bảo mật, thì người dân ở vùng nông thôn, vùng sâu vùng xa, đặc biệt là người cao tuổi và đồng bào dân tộc thiểu số là nhóm yếu thế về kỹ năng số. Nhóm đối tượng này rất dễ bị các đối tượng xấu lợi dụng, lừa gạt lấy thông tin cá nhân, mở tài khoản ngân hàng ảo mà không hề biết mình bị xâm phạm quyền lợi.

Tóm lại, thực trạng phương thức tuyên truyền tại các tỉnh thời gian qua cho thấy chúng ta đang gặt hái được những kết quả về “bề nổi” (tăng tỷ lệ người dân biết đến dịch vụ số) nhưng chưa đạt được chiều sâu về “chất” (nâng cao năng lực tự vệ pháp lý của người dân đối với dữ liệu). Người dân tham gia vào chính quyền số ở thể “thụ động”, họ giao nộp dữ liệu vì bắt buộc phải làm thế để giải quyết thủ tục hành chính, chứ chưa thực sự hiểu rõ dữ liệu của mình được bảo vệ ra sao.

Chuyển đổi số chỉ thực sự bền vững khi “niềm tin số” của người dân được củng cố; và niềm tin đó chỉ có được khi công tác truyền thông của chính quyền cấp tỉnh giúp người dân ý thức rõ rằng: Bảo vệ dữ liệu cá nhân không chỉ là nghĩa vụ an ninh mạng của Nhà nước, mà còn là quyền con người tối cao của mỗi công dân trong không gian số.

3.2.6. Thực trạng ký kết hợp đồng, ràng buộc trách nhiệm pháp lý giữa UBND tỉnh với các tập đoàn công nghệ (bên thứ ba) khi thuê hạ tầng đám mây (Cloud) hoặc mua giải pháp phần mềm hành chính công

Trong bối cảnh nguồn ngân sách và nhân lực kỹ thuật nội tại còn hạn chế, Ủy ban nhân dân các tỉnh, thành phố hiện nay chủ yếu lựa chọn mô hình “Thuê dịch vụ CNTT” hoặc hợp tác chiến lược với các tập đoàn công nghệ lớn, như VNPT, Viettel, FPT... để xây dựng hạ tầng đám mây (Cloud), Cổng dịch vụ công và Trung tâm điều hành thông minh (IOC). Phương thức hợp tác này giúp địa phương tăng tốc chuyển đổi số, nhưng lại đặt ra những thách thức chưa từng có trong việc kiểm soát việc luân chuyển dữ liệu và bảo vệ quyền dữ liệu cá nhân của người dân trước bên thứ ba.

Qua nghiên cứu, rà soát 25 hồ sơ mời thầu và hợp đồng cung cấp dịch vụ Điện toán đám mây (Cloud) thuộc các dự án CNTT/Chính quyền số cấp tỉnh giai đoạn 2021 - 2025 tại các địa phương khảo sát cho thấy một khoảng trống pháp lý - kỹ thuật đáng quan ngại: (1) Về trách nhiệm bồi thường: Có tới 84% (21/25) hợp đồng dịch vụ Cloud chỉ quy định nghĩa vụ tài chính ứng với giá trị dịch vụ hoặc phạt vi phạm hợp đồng (thường không quá 8% giá trị hợp đồng theo Luật Thương mại), hoàn toàn thiếu vắng điều khoản bồi thường thiệt hại về tài sản, danh dự cho công dân khi xảy ra sự cố rò rỉ dữ liệu cá nhân do lỗi của nhà cung cấp dịch vụ Cloud. (2) Về quyền truy cập của bên thứ ba: 100% các hợp đồng khảo sát dành cho kỹ sư của nhà thầu (bên cung cấp giải pháp Cloud/Software) tài khoản có đặc quyền quản trị hệ thống (Super Admin/Root). Tuy nhiên, 76% (19/25) đơn vị cấp tỉnh không thiết lập cơ chế giám sát hay ghi nhật ký độc lập (Independent Audit Log) đối với các thao tác của kỹ sư nhà thầu trên cơ sở dữ liệu. (3) Về sao lưu và xóa bỏ dữ liệu: 92% (23/25) hợp đồng không quy định chi tiết quy trình tiêu hủy dữ liệu (Data Destruction) sau khi thanh lý hợp đồng, cũng như không cam kết về việc xóa bỏ triệt để các bản sao lưu ngầm (Shadow/Implicit Backups) trên các cụm máy chủ phụ của nhà thầu.

(1). Thực trạng cơ chế ký kết hợp đồng và ràng buộc trách nhiệm pháp lý: Sự hình thành các “Hợp đồng mẫu” nặng về tính thương mại: Khi ký kết các hợp đồng kinh tế về thuê hạ tầng Cloud hoặc mua giải pháp phần mềm, nội dung hợp đồng chủ yếu tập trung vào các thông số kỹ thuật (bảng thông, dung lượng lưu trữ, thời gian duy trì hệ thống - SLA) và nghĩa vụ tài chính. Các điều khoản về bảo vệ DLCN của

người dân thường được xếp vào mục “Bảo mật thông tin chung” mang tính chất thủ tục, chưa được thiết kế thành một cấu phần pháp lý độc lập, chuyên sâu.

Bước đầu thể chế hóa vai trò theo Nghị định 13/2023/NĐ-CP: Kể từ khi Nghị định 13 có hiệu lực, các tỉnh đã bắt đầu đưa các thuật ngữ pháp lý vào hợp đồng, xác định rõ: UBND tỉnh (hoặc Sở TT&TT trước đây) là Bên kiểm soát dữ liệu, còn Doanh nghiệp CNTT là Bên xử lý dữ liệu. Các doanh nghiệp bị ràng buộc nghĩa vụ không được tự ý chuyển giao, mua bán dữ liệu công dân cho bên thứ tư nếu không có sự đồng ý bằng văn bản của chính quyền tỉnh.

(2). Những nút thắt và hạn chế cốt lõi: Mặc dù có sự ràng buộc trên văn bản, nhưng thực tế kiểm soát dữ liệu trao đổi giữa chính quyền tỉnh và nhà thầu công nghệ đang bộc lộ 3 khoảng trống lớn:

Thứ nhất, sự “bất lực” trong kiểm soát quyền truy cập tối cao (Root Access) của doanh nghiệp: Về mặt kỹ thuật, các tập đoàn công nghệ khi cho thuê hạ tầng Cloud hoặc bảo trì phần mềm hành chính công đều nắm giữ quyền quản trị tối cao hệ thống. Chính quyền cấp tỉnh hầu như không có công cụ độc lập để giám sát xem các kỹ sư hệ thống của doanh nghiệp có trích xuất, sao lưu ngầm (Backup trái phép) dữ liệu hộ tịch, đất đai, hay hồ sơ sức khỏe của người dân về máy chủ riêng của doanh nghiệp hay không. Việc kiểm soát dữ liệu hiện chỉ nằm ở phía nhà thầu.

Thứ hai, thiếu cơ chế ràng buộc trách nhiệm bồi thường thiệt hại dân sự cho người dân: Trong hầu hết các hợp đồng giữa UBND tỉnh và doanh nghiệp CNTT, nếu xảy ra sự cố rò rỉ dữ liệu, các bên chỉ quy định trách nhiệm bồi thường thiệt hại kinh tế lẫn nhau hoặc phạt vi phạm hợp đồng (thường giới hạn ở mức 8% giá trị hợp đồng theo Luật Thương mại). Hoàn toàn không có điều khoản nào quy định doanh nghiệp phải có trách nhiệm liên đới bồi thường thiệt hại về danh dự, uy tín và vật chất cho bên bị hại thực sự là người dân khi quyền DLCN của họ bị xâm phạm.

Thứ ba, mơ hồ trong xử lý dữ liệu sau khi chấm dứt hợp đồng: Hoạt động thuê dịch vụ CNTT tại các tỉnh thường diễn ra theo giai đoạn (giai đoạn 3 năm hoặc 5 năm). Thực tế, quy chế nội bộ và điều khoản hợp đồng của các tỉnh chưa quy định chi tiết quy trình bàn giao và hủy bỏ dữ liệu khi hết hạn hợp đồng: Doanh nghiệp có nghĩa vụ xóa bỏ vĩnh viễn toàn bộ dữ liệu người dân trên máy chủ của họ như thế nào? Cơ chế nào để chính quyền tỉnh kiểm tra, xác nhận doanh nghiệp đã xóa sạch dữ liệu hay chưa? Đây là “điểm mù” khiến dữ liệu của công dân có nguy cơ bị lưu lại vô thời hạn tại khu vực tư nhân.

Thực tiễn triển khai tại các đô thị lớn như Hà Nội và TP. Hồ Chí Minh cho thấy, hạ tầng kỹ thuật dịch vụ công trực tuyến vẫn chưa thực sự đáp ứng được áp lực xử lý từ lượng hồ sơ hành chính khổng lồ. Việc quá tải hạ tầng, kết hợp với các đợt

nâng cấp hoặc đồng bộ dữ liệu quy mô lớn; đặc biệt là trong giai đoạn cao điểm tích hợp giữa Cổng dịch vụ công địa phương với Cơ sở dữ liệu quốc gia về dân cư (Đề án 06) đã dẫn đến tình trạng hệ thống phản hồi chậm, lỗi hiển thị hoặc gián đoạn chức năng ký số điện tử của người dân. Quá tải cục bộ ở một số dịch vụ bức thiết, các phân hệ dịch vụ có nhu cầu đột biến như: Đăng ký cư trú, đăng ký đất đai, lý lịch tư pháp hay nộp thuế trước bạ đất đai, phương tiện thường xảy ra hiện tượng “xoay vòng” (timeout) vào các khung giờ hành chính, buộc các cơ quan chức năng phải tạm ngắt kết nối để bảo trì và nâng cấp băng thông. Để chấm dứt tình trạng cát cứ công nghệ và gián đoạn cục bộ, Chính phủ đã có lộ trình đóng giao diện Cổng Dịch vụ công cấp tỉnh để chuyển toàn bộ việc tiếp nhận, xử lý trực tuyến lên một nền tảng thống nhất duy nhất là Cổng Dịch vụ công quốc gia.

Ngoài ra, các sự cố an ninh mạng nguy hiểm nhắm vào hạ tầng số của các cơ quan chính phủ và các đơn vị cung cấp dịch vụ thiết yếu tại địa phương đang là mục tiêu tấn công hàng đầu của tội phạm mạng, như: Tấn công mã hóa dữ liệu tổng tiền; đây là vấn đề nhức nhối nhất khi hàng loạt doanh nghiệp lớn và cơ quan cung cấp dịch vụ hạ tầng then chốt (như năng lượng, tài chính, chứng khoán) liên tiếp bị tấn công mã hóa toàn bộ dữ liệu, gây tê liệt hệ thống giao dịch trực tuyến trong nhiều ngày. Cục An toàn thông tin - Bộ TT&TT (Bộ KHCN) liên tục phải phát đi các cảnh báo khẩn cấp về chiến dịch tấn công mã hóa dữ liệu quy mô lớn này. Hay vấn nạn chèn mã độc đánh bạc/lừa đảo vào website cơ quan nhà nước nhằm cài các đường link ẩn, mã độc quảng cáo cờ bạc, cá độ hoặc trang giả mạo nhằm lừa đảo chiếm đoạt tài sản. Hay tấn công từ chối dịch vụ (DDoS) vào các cơ quan báo chí, cổng thông tin điện tử lớn tại các thành phố. Diễn hình như các đợt tấn công làm tràn băng thông nhắm vào Báo điện tử VOV và một số cơ quan báo chí lớn, khiến độc giả không thể truy cập hoặc đường truyền bị ngắt quãng liên tục trong nhiều giờ...

Khi xảy ra sự cố an toàn thông tin, chính quyền địa phương thường rơi vào thế bị động và phụ thuộc lớn vào năng lực xử lý của nhà thầu công nghệ. Thực trạng này phản ánh nguy cơ suy giảm năng lực kiểm soát của cơ quan công quyền đối với hạ tầng lưu trữ và xử lý dữ liệu cá nhân của công dân khi ủy thác cho bên thứ ba.

Chẳng hạn, khi người dân đăng ký kinh doanh tại tỉnh, dữ liệu cá nhân của họ chảy qua phần mềm do Doanh nghiệp A xây dựng, lưu trữ trên Cloud do Doanh nghiệp B cung cấp, và được liên thông sang hệ thống thuế do Doanh nghiệp C bảo trì. Việc dữ liệu bị phân tán qua nhiều bên trung gian công nghệ mà thiếu một cơ chế mã hóa đầu cuối (End-to-End Encryption) khiến cho nguy cơ lộ lọt dữ liệu tăng lên theo cấp số nhân tại các điểm giao tiếp (API).

Theo số liệu khảo sát từ Hiệp hội An ninh mạng quốc gia (NCA) và các hãng công nghệ lớn, hiện có khoảng 52,89% doanh nghiệp, tổ chức tại Việt Nam chưa trang bị đầy đủ các giải pháp công nghệ cũng như nhân sự chuyên trách để ứng phó hiệu quả với sự cố an ninh mạng [34]. Trước thực trạng này, các địa phương lớn hiện đang ráo riết chuyển dịch mô hình bảo mật từ “phòng thủ thụ động” sang “phòng thủ chủ động đa tầng”, đồng thời triển khai nghiêm ngặt quy trình giám sát 4 lớp do Bộ Thông tin và Truyền thông quy định để bảo vệ an toàn cho dữ liệu của người dân (gồm: Lực lượng tại chỗ; Tổ chức hoặc doanh nghiệp giám sát, bảo vệ chuyên nghiệp; Tổ chức hoặc doanh nghiệp độc lập kiểm tra, đánh giá định kỳ; Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) thuộc Bộ TT&TT kết nối, chia sẻ thông tin) [13].

Thực trạng phương thức hợp tác với bên thứ ba tại các tỉnh thời gian qua phản ánh một xu hướng “Tư nhân hóa hạ tầng quản trị dữ liệu công” nhưng thiếu cơ chế kiểm soát quyền lực tương xứng.

Chính quyền cấp tỉnh đang thiếu sự tách bạch giữa chủ thể vận hành và chủ thể giám sát khi chuyển giao việc xử lý dữ liệu công dân cho doanh nghiệp, nhưng lại không có đủ năng lực kỹ thuật để giám sát việc thực thi cam kết bảo mật của chính doanh nghiệp đó. Để bảo vệ quyền công dân một cách thực chất, hợp đồng dịch vụ công nghệ không thể chỉ là một văn bản thương mại thuần túy, mà phải được nâng tầm thành một “Khế ước trách nhiệm số”, trong đó quyền tự quyết thông tin của người dân phải được đặt ở vị trí trung tâm, không thể bị đánh đổi bởi bất kỳ lợi ích kinh tế hay sự tiện lợi công nghệ nào.

3.3. ĐÁNH GIÁ THỰC TRẠNG VỀ BẢO VỆ QUYỀN ĐỐI VỚI DỮ LIỆU CÁ NHÂN TRONG XÂY DỰNG CHÍNH QUYỀN SỐ CẤP TỈNH

3.3.1. Kết quả đạt được về bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh ở Việt Nam

Phương thức bảo vệ quyền đối với DLCN tại các tỉnh, thành phố trực thuộc Trung ương thời gian qua đã có những bước chuyển dịch căn bản. Từ chỗ coi dữ liệu là công cụ quản lý hành chính thuần túy, chính quyền cấp tỉnh đã bắt đầu thiết lập các cơ chế, giải pháp kỹ thuật và pháp lý nhằm tôn trọng và bảo vệ quyền tự quyết thông tin của công dân trên môi trường số.

3.3.1.1. Pháp luật về bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh đã dần hoàn thiện và phù hợp với thực trạng hoạt động này ở Việt Nam

Thứ nhất, pháp luật về bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh ở Việt Nam đã thể hiện tính phù hợp trong việc thể chế hóa quan điểm, chủ trương của Đảng và tiệm cận các chuẩn mực pháp lý quốc tế về bảo vệ

DLCN. Trong các văn kiện của Đảng ta, đặc biệt là các nghị quyết, chiến lược về chuyển đổi số và xây dựng Nhà nước pháp quyền, yêu cầu bảo đảm QCN, quyền công dân, trong đó có quyền riêng tư và bảo vệ thông tin cá nhân, được đặt ra cùng với mục tiêu phát triển chính quyền số. Trên cơ sở đó, hệ thống pháp luật từng bước được hoàn thiện theo hướng bảo vệ quyền đối với DLCN. Các quy định này thể hiện sự tương thích nhất định với các nghĩa vụ của Việt Nam theo các công ước quốc tế về QCN mà Việt Nam là thành viên, đặc biệt là các chuẩn mực về bảo vệ đời sống riêng tư, ngăn ngừa sự can thiệp tùy tiện hoặc trái pháp luật vào thông tin cá nhân trong bối cảnh ứng dụng công nghệ số.

Đặc biệt, Việt Nam đã nhanh chóng thiết lập được hành lang pháp lý nền tảng là Nghị định 13/2023/NĐ-CP và Luật Bảo vệ dữ liệu cá nhân năm 2025 (có hiệu lực từ 01/01/2026). Cách tiếp cận này rất gần với mô hình ưu tiên an ninh chủ quyền dữ liệu quốc gia của Nga và Luật Bảo vệ thông tin cá nhân (PIPL) của Trung Quốc. Chính quyền cấp tỉnh đã nhận thức rõ dữ liệu công dân là tài nguyên quốc gia, từ đó hình thành các Kho dữ liệu dùng chung (LGSP) được bảo vệ nghiêm ngặt bằng các giải pháp kỹ thuật 4 lớp (mô hình tường lửa, giám sát tập trung SOC), ngăn chặn hiệu quả các làn sóng tấn công mạng xuyên biên giới.

Thứ hai, pháp luật về bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh đã hình thành được khung điều chỉnh đối với những vấn đề cơ bản của bảo vệ DLCN. Hệ thống quy phạm pháp luật hiện hành đã từng bước xác lập các nội dung cốt lõi như khái niệm DLCN; phân loại DLCN cơ bản và DLCN nhạy cảm; nguyên tắc xử lý dữ liệu; quyền của chủ thể dữ liệu; nghĩa vụ và trách nhiệm của cơ quan nhà nước với tư cách là bên kiểm soát và xử lý dữ liệu, cũng như các yêu cầu về bảo đảm an toàn, an ninh trong quá trình xử lý dữ liệu nói chung, DLCN nói riêng. Những nội dung này được ghi nhận và điều chỉnh trong nhiều văn bản pháp luật quan trọng như Hiến pháp năm 2013 (Điều 21); Luật An toàn thông tin mạng năm 2015; Luật An ninh mạng năm 2018; Luật An ninh mạng năm 2025; Nghị định số 13/2023/NĐ-CP về bảo vệ DLCN; và đặc biệt là Luật Bảo vệ dữ liệu cá nhân năm 2025. Trong bối cảnh chính quyền số cấp tỉnh, các quy định này tạo cơ sở pháp lý để kiểm soát hoạt động thu thập, xử lý, chia sẻ và lưu trữ DLCN trong các hệ thống thông tin hành chính, công dịch vụ công và cơ sở dữ liệu do địa phương quản lý.

Thứ ba, pháp luật về bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh bước đầu đã thể hiện được tính cụ thể thông qua việc xác lập một số phương thức bảo vệ DLCN. Bên cạnh việc ghi nhận quyền và nguyên tắc chung, pháp luật đã quy định về phương thức bảo vệ như: yêu cầu bảo đảm an toàn, an ninh hệ thống thông tin; quy định về phân quyền truy cập và trách nhiệm

quản lý dữ liệu; cơ chế kiểm tra, thanh tra và xử lý vi phạm; cũng như cơ chế tiếp nhận, giải quyết khiếu nại, tố cáo liên quan đến bảo vệ DLCN.

Thứ tư, pháp luật đã thiết lập khuôn khổ trách nhiệm pháp lý tương đối rõ ràng trong bảo vệ quyền đối với DLCN, tiếp cận theo hướng phân định vai trò và trách nhiệm trong chuỗi xử lý dữ liệu. Trách nhiệm này được xác lập cụ thể tại Luật Bảo vệ dữ liệu cá nhân năm 2025 trên hai bình diện: 1) Điều 36 quy định trách nhiệm quản lý nhà nước về bảo vệ DLCN, khẳng định vai trò của Nhà nước trong xây dựng, tổ chức thực hiện pháp luật, thanh tra, kiểm tra và xử lý vi phạm, gắn bảo vệ DLCN với nhiệm vụ bảo đảm QCN trong bối cảnh chuyển đổi số; 2) Điều 37 phân định rõ trách nhiệm của bên kiểm soát, bên xử lý và bên vừa kiểm soát vừa xử lý DLCN, bảo đảm nguyên tắc trách nhiệm tương xứng với mức độ quyết định và can thiệp vào dữ liệu.

Tóm lại, kể từ khi Nghị định số 13/2023/NĐ-CP và sau này là Luật 91 có hiệu lực, 100% các tỉnh, thành phố đã ban hành các văn bản cụ thể hóa, kế hoạch triển khai và rà soát hệ thống [5]. Vấn đề bảo vệ DLCN, an toàn thông tin không còn là nội dung thứ yếu mà đã được luật hóa, lồng ghép trực tiếp vào Kế hoạch chuyển đổi số hàng năm của tỉnh và làm tiêu chí bắt buộc để chấm điểm chỉ số cải cách hành chính (PAR INDEX), chỉ số chuyển đổi số (DTI) của các cơ quan cấp tỉnh, chỉ số đánh giá hiệu quả công việc (KPI) của cấp ủy và chính quyền các cấp.

3.3.1.2. Bước đầu quyền tiếp cận, tra cứu và cải chính thông tin của công dân được thực hiện

Thông qua việc liên thông hệ thống thông tin giải quyết thủ tục hành chính cấp tỉnh với cơ sở dữ liệu quốc gia về dân cư và ứng dụng VNeID, chính quyền các tỉnh đã cung cấp cho người dân công cụ để chủ động đối soát dữ liệu của chính mình. Khi phát hiện sai lệch thông tin cá nhân (về hộ tịch, cư trú, đất đai...), quy trình tiếp nhận và xử lý yêu cầu cải chính dữ liệu của công dân tại bộ phận “Một cửa” đã được vận hành nhanh chóng, minh bạch theo thời gian thực.

Thông qua việc tích hợp hệ thống định danh VNeID và Cổng dịch vụ công trực tuyến, chính quyền các tỉnh đã hiện thực hóa thành công quyền tiếp cận, tra cứu và cải chính thông tin của chủ thể dữ liệu. Kết quả này gần với tinh thần tôn trọng quyền tự quyết thông tin (Informational Self-Determination) từ phán quyết của Tòa án Hiến pháp Liên bang Đức (1983), (Tiệm cận mô hình Liên minh Châu Âu). Người dân không còn ở trạng thái “mù mờ” về thông tin của mình mà có thể chủ động đối soát dữ liệu hộ tịch, đất đai, thuế trực tiếp trên môi trường số.

3.3.1.3. Nâng cấp hạ tầng kỹ thuật, ứng dụng công nghệ và hình thành mô hình bảo mật dữ liệu nhiều lớp đã góp phần bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh

Trong quá trình xây dựng chính quyền số cấp tỉnh, việc ứng dụng và cập nhật liên tục các công nghệ bảo mật dữ liệu đã trở thành một kết quả nổi bật, góp phần quan trọng vào việc bảo vệ quyền đối với DLCN. Trong giai đoạn 2020 - 2025, Nhà nước ta đã có sự gia tăng đầu tư cho hạ tầng an toàn thông tin tại các địa phương, đặc biệt đối với cổng dịch vụ công, hệ thống thông tin giải quyết thủ tục hành chính và các cơ sở dữ liệu chuyên ngành. Những biện pháp kỹ thuật hiện đại như xác thực đa yếu tố, phân quyền truy cập theo vai trò, mã hóa dữ liệu, sao lưu và phục hồi dữ liệu, giám sát truy cập và phát hiện bất thường đã được triển khai tương đối đồng bộ.

Cùng với đó, việc kết nối các hệ thống địa phương với nền tảng giám sát an toàn thông tin ở cấp quốc gia đã nâng cao năng lực phát hiện sớm và ứng phó sự cố. Một số tỉnh, thành phố còn đầu tư trung tâm giám sát, điều hành thông minh (IOC), tích hợp chức năng giám sát an ninh mạng và an toàn dữ liệu, qua đó tăng cường khả năng kiểm soát rủi ro trong môi trường số. Đến nay, hầu hết các tỉnh, thành đã hình thành Trung tâm dữ liệu (Data Center) và Kho dữ liệu dùng chung của các tỉnh, hệ thống bảo mật đã được nâng cấp rõ rệt. Các địa phương đã phối hợp với các doanh nghiệp công nghệ lớn triển khai mô hình giám sát an toàn thông tin 4 lớp (mô hình SOC tập trung). Việc phân định vai trò giữa UBND tỉnh (Bên kiểm soát dữ liệu) và các nhà thầu công nghệ (Bên xử lý dữ liệu) trong các hợp đồng thuê dịch vụ đám mây (Cloud) bước đầu đã thiết lập được ranh giới kiểm soát việc chuyển giao dữ liệu cho khu vực tư nhân. Mặc dù mức độ hiện đại hóa còn khác nhau giữa các địa phương, nhưng những ứng dụng công nghệ bảo mật đã được thực hiện thường xuyên và cập nhật theo xu hướng mới, tạo nền tảng kỹ thuật quan trọng để bảo vệ quyền đối với DLCN trong vận hành chính quyền số cấp tỉnh ở nước ta.

3.3.1.4. Nhận thức và trách nhiệm của cán bộ, người dân trong bảo vệ quyền đối với dữ liệu cá nhân đã được nâng cao

Trong bối cảnh chính quyền số hiện nay đã có sự chuyển biến tích cực về nhận thức và trách nhiệm của cán bộ, công chức và người dân đối với việc bảo vệ quyền đối với DLCN. Trong giai đoạn từ năm 2020 - 2025, nội dung an toàn thông tin, bảo mật dữ liệu và bảo vệ DLCN ngày càng được lồng ghép vào các chương trình đào tạo, bồi dưỡng cán bộ, công chức ở trung ương và địa phương. Điều này góp phần hình thành ý thức trách nhiệm trong việc thu thập, xử lý và sử dụng DLCN của người dân khi thực hiện nhiệm vụ.

Đối với người dân, các hoạt động truyền thông về chuyển đổi số, định danh điện tử, sử dụng dịch vụ công trực tuyến an toàn và cảnh báo rủi ro lừa đảo trên không gian mạng đã góp phần nâng cao hiểu biết về giá trị của DLCN và nhu cầu tự bảo vệ thông tin của cá nhân. Việc triển khai rộng khắp mạng lưới Tổ công nghệ số cộng đồng tại các địa phương, với phương châm “đi từng ngõ, gõ từng nhà” đã đem lại hiệu quả thực chất, tạo kênh hỗ trợ trực tiếp, giúp người dân tiếp cận dịch vụ công số và nâng cao nhận thức về quyền, nghĩa vụ liên quan đến DLCN, nhất là đã trực tiếp hướng dẫn người dân cách bảo mật tài khoản dịch vụ công, nhận diện các hình thức lừa đảo mạng, chiếm đoạt dữ liệu; từ đó từng bước xóa dần vùng còn hạn chế về kỹ năng số tại các địa bàn nông thôn, miền núi. Nhìn chung, nhận thức xã hội về bảo vệ DLCN đã có bước tiến rõ rệt, tạo điều kiện thuận lợi cho việc thực thi pháp luật trong xây dựng chính quyền số cấp tỉnh.

3.3.1.5. Về phương thức bảo đảm các quyền thực chất của chủ thể dữ liệu

Đây là phương thức cốt lõi nhằm chuyển hóa các quy định pháp lý mang tính tuyên ngôn thành các tiện ích thực tế, giúp người dân thực thi "chủ quyền dữ liệu" của mình trong mối quan hệ với cơ quan công quyền địa phương. Với sự phổ biến của Căn cước công dân gắn chip và sự phủ sóng của tài khoản định danh điện tử VNeID, chính quyền số cấp tỉnh đã đạt được những kết quả như sau:

Thứ nhất, hiện thực hóa quyền tiếp cận, tra cứu và kiểm tra thông tin: Thông qua việc tích hợp trực liên thông văn bản quốc gia và Cổng dịch vụ công trực tuyến cấp tỉnh, người dân không còn ở thế “bị động” đối với thông tin của chính mình. Chỉ cần đăng nhập bằng tài khoản VNeID cấp độ 2, công dân có thể trực tiếp tra cứu, hiển thị trọn vẹn và kiểm tra tính chính xác của các trường dữ liệu cá nhân cốt lõi đang lưu trữ tại các kho dữ liệu dùng chung của tỉnh như: thông tin cư trú, lịch sử đóng thuế, dữ liệu giấy phép lái xe, và tiến độ xử lý hồ sơ hành chính theo thời gian thực.

Thứ hai, số hóa quy trình thực thi quyền cải chính, sửa đổi dữ liệu: Trước đây, khi phát hiện sai sót về thông tin hộ tịch, đất đai hay bảo hiểm, người dân phải di chuyển qua nhiều cấp chính quyền với các thủ tục giấy tờ phức tạp. Hiện nay, hệ thống thông tin giải quyết thủ tục hành chính cấp tỉnh đã thiết lập các module chức năng cho phép công dân gửi yêu cầu cải chính dữ liệu hoàn toàn trực tuyến. Hệ thống tự động phân luồng hồ sơ về đúng cơ quan chuyên môn như: Sở Tư pháp, Sở Tài nguyên và Môi trường... để thẩm định và cập nhật, bảo đảm nguyên tắc dữ liệu luôn “đúng, đủ, sạch, sống” mà không làm phát sinh chi phí hay phiền hà cho người dân.

Thứ ba, minh bạch hóa việc xử lý dữ liệu hành chính: Kênh tương tác số giữa chính quyền tỉnh và người dân đã bước đầu tạo lập được cơ chế giám sát hai chiều. Việc tiếp nhận các phản ánh, kiến nghị liên quan đến việc cán bộ tự ý hạch sách, yêu

cầu cung cấp thêm thông tin ngoài quy định đã được hệ thống hóa qua các ứng dụng Công dân số của địa phương (ví dụ: các ứng dụng dạng Bình Dương Số, iHanoi, Danang Smart City...). Điều này giúp công dân thực hiện quyền phản đối các hành vi thu thập dữ liệu bất hợp pháp hoặc vượt quá phạm vi cần thiết của các cơ quan cấp cơ sở.

Tóm lại, từ kết quả này chứng minh chính quyền số cấp tỉnh đã bước đầu xây dựng thành công công cụ thực thi quyền bảo đảm thực chất. Việc công nghệ hóa quy trình tiếp cận và sửa đổi dữ liệu không chỉ bảo đảm tính chính xác của hệ thống thông tin quốc gia, mà còn là bước tiến lớn trong việc bảo đảm quyền tự quyết thông tin ở mức độ nền tảng, tạo dựng nền móng vững chắc cho một xã hội số minh bạch và tôn trọng người dân.

3.3.1.6. Hoạt động phản hồi và xử lý vi phạm liên quan đến dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh được triển khai nhanh chóng, kịp thời

Trong thời gian qua, các cơ quan quản lý nhà nước đã tăng cường thanh tra, kiểm tra an toàn thông tin và xử lý các hành vi xâm phạm DLCN, đặc biệt đối với các hành vi thu thập, sử dụng hoặc mua bán dữ liệu trái phép. Một số vụ việc vi phạm quy mô lớn được phát hiện và xử lý trong giai đoạn 2023 - 2025 cho thấy năng lực phản ứng của cơ quan chức năng đã được cải thiện, góp phần nâng cao hiệu quả răn đe và bảo vệ quyền đối với DLCN. Ở cấp địa phương, các kênh tiếp nhận phản ánh, kiến nghị và khiếu nại liên quan đến thủ tục hành chính điện tử và an toàn thông tin từng bước được thiết lập và vận hành, tạo điều kiện để người dân phản ánh kịp thời khi có dấu hiệu xâm hại DLCN. Đồng thời, việc ban hành Luật Bảo vệ dữ liệu cá nhân năm 2025 đã củng cố cơ sở pháp lý cho hoạt động xử lý vi phạm, giúp các cơ quan có căn cứ rõ ràng hơn trong phản hồi và khắc phục. Có thể khẳng định rằng cơ chế phản hồi và xử lý vi phạm liên quan đến DLCN đã được hình thành và vận hành ngày càng hiệu quả, góp phần bảo vệ quyền đối với DLCN trong chính quyền số cấp tỉnh.

3.3.1.7. Về phương thức hợp tác và kiểm soát việc chia sẻ dữ liệu để bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh thời gian qua

Trong xu thế hội nhập sâu rộng, cùng với xây dựng chính quyền số, phương thức hợp tác công - tư thông qua thuê dịch vụ CNTT và hạ tầng điện toán đám mây (Cloud) là tất yếu. Thời gian qua, chính quyền cấp tỉnh đã có những bước tiến quan trọng trong việc chuyển đổi tư duy, từ chỗ “khoán trắng” hệ thống cho nhà thầu sang việc xác lập cơ chế kiểm soát có chủ quyền đối với dữ liệu, bảo vệ quyền đối với DLCN của công dân trước sự tiếp cận của bên thứ ba và đã đạt được một số kết quả như:

Thứ nhất, xác lập rõ ràng tư cách pháp lý của các bên trong hợp đồng công nghệ: Kể từ khi Nghị định 13/2023/NĐ-CP được ban hành, Ủy ban nhân dân các tỉnh và các sở chuyên ngành khi ký kết hợp đồng thuê dịch vụ phần mềm hành chính công đã không còn sử dụng các mẫu hợp đồng thương mại chung chung. Các địa phương đã bước đầu chuẩn hóa các điều khoản pháp lý, phân định rõ cơ quan nhà nước cấp tỉnh là bên kiểm soát dữ liệu và doanh nghiệp công nghệ là bên xử lý dữ liệu. Sự phân định này đã quy trách nhiệm pháp lý cao nhất đối với việc xử lý dữ liệu thuộc về chính quyền, ngăn chặn tình trạng doanh nghiệp tự ý khai thác dữ liệu công dân cho mục đích thương mại riêng.

Thứ hai, triển khai các giải pháp chia sẻ dữ liệu an toàn, bảo mật từ đầu cuối: Thông qua việc kết nối giữa nền tảng tích hợp, chia sẻ dữ liệu cấp tỉnh (LGSP) với nền tảng quốc gia (NDXP), các tỉnh đã kiểm soát tốt hơn việc liên thông dữ liệu. Việc chuyển giao dữ liệu giữa các sở, ngành và các hệ thống dịch vụ công không còn thực hiện thủ công, lỏng lẻo mà được thực hiện qua các giao diện lập trình ứng dụng (API) có mã hóa và định danh nghiêm ngặt, giúp ghi vết (Audit logs) chính xác luồng di chuyển của dữ liệu.

Thứ ba, ràng buộc trách nhiệm bảo mật thông tin sau khi chấm dứt hợp tác: Trong các thỏa thuận hợp tác chiến lược và hợp đồng thuê dịch vụ đám mây, chính quyền cấp tỉnh đã đưa vào các điều khoản nghiêm ngặt về quyền sở hữu dữ liệu. Theo đó, doanh nghiệp công nghệ chỉ được quyền lưu trữ tạm thời để vận hành hệ thống; khi chấm dứt hợp đồng, doanh nghiệp có nghĩa vụ bàn giao nguyên vẹn và thực hiện quy trình "xóa vĩnh viễn", không được lưu giữ bất kỳ bản sao lưu (backup) nào chứa DLCN của công dân địa phương trên máy chủ tư nhân.

3.3.2. Nguyên nhân của kết quả đạt được về bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh ở Việt Nam

Sự chuyển biến tích cực trong công tác bảo vệ quyền đối với dữ liệu cá nhân tại chính quyền số cấp tỉnh thời gian qua không diễn ra biệt lập, mà là kết quả mang tính hệ thống, triển khai đồng bộ dựa trên các nhóm nguyên nhân sau:

Thứ nhất, hoàn thiện thể chế và quy chế nội bộ: Sự nhất quán trong chỉ đạo chiến lược của Đảng và Chính phủ; sự quyết tâm chính trị từ Trung ương (Nghị quyết 52-NQ/TW, Văn kiện Đại hội XIII và định hướng Đại hội XIV...) đã tạo ra một sức ép hành chính đủ mạnh để các địa phương bắt buộc phải thay đổi tư duy quản trị truyền thống sang quản trị số.

Việc nội luật hóa văn bản Trung ương là nguyên nhân cốt lõi giúp các địa phương định hình được khung pháp lý bảo mật, nhờ sự bao quát, kịp thời của Nghị định 13/2023/NĐ-CP và Luật 91. Từ “bộ khung” này, Ủy ban nhân dân các tỉnh đã

nhANH chóng chuyển hóa thành các chỉ thị, quy chế vận hành Công dịch vụ công và Trung tâm IOC. Chính việc “luật hóa” nội bộ này đã buộc các thủ trưởng cơ quan cấp tỉnh phải đặt trách nhiệm bảo vệ bí mật thông tin của dân ngang hàng với chỉ tiêu hoàn thành nhiệm vụ chuyên môn.

Thứ hai, tổ chức bộ máy và quản trị nhân sự: Sự hình thành cơ chế phối hợp liên ngành, kiểm soát và xử lý sự cố theo trục ba bên vững chắc: Sở Thông tin và Truyền thông (cũ), nay là Sở KHCN (quản lý nhà nước) - Phòng An ninh mạng PA05 Công an tỉnh (thực thi pháp luật) - và Trung tâm CNTT-TT (vận hành kỹ thuật). Sự phân định vai trò này giúp bộ máy tại địa phương tuy còn kiêm nhiệm nhưng vẫn phản ứng nhanh chóng trước các nguy cơ mất an toàn dữ liệu.

Thứ ba, áp dụng biện pháp kỹ thuật và công nghệ: Sự phát triển của hạ tầng bảo mật nội địa là cơ sở bảo vệ an toàn các kho dữ liệu dùng chung (LGSP), phần lớn nhờ vào việc các tỉnh đã nghiêm túc áp dụng mô hình giám sát an toàn thông tin 4 lớp (mô hình SOC). Việc các địa phương phối hợp với các tập đoàn công nghệ lớn để triển khai công nghệ mã hóa dữ liệu đầu cuối, xác thực OTP và hệ thống ghi vết tự động (Audit Logs) đã tạo ra “bức tường lửa” kỹ thuật vững chắc ngăn chặn tin tặc.

Thứ tư, công tác thanh tra, kiểm tra và xử lý vi phạm: Tính răn đe từ hoạt động thanh tra, kiểm tra chuyên đề, chuyên ngành gắn với Đề án 06 giữa Sở Thông tin và Truyền thông (cũ), nay là Sở KHCN với Công an tỉnh được siết chặt. Việc kiểm tra đột xuất quy trình quản lý tài khoản công vụ tại bộ phận “Một cửa” cấp huyện (cũ), xã và việc xử lý nghiêm các trường hợp cán bộ lạm dụng quyền tra cứu thông tin dân cư đã tạo ra tính răn đe cao, buộc đội ngũ công chức phải tự chấn chỉnh ý thức bảo mật.

Thứ năm, bảo đảm quyền thực chất của chủ thể dữ liệu: Sự hỗ trợ từ hạ tầng định danh điện tử quốc gia về dân cư giữ vai trò nền tảng công nghệ; nhờ VNeID, người dân thực hiện được quyền tra cứu, tiếp cận và cải chính thông tin một cách thông suốt. Hạ tầng này giúp chính quyền cấp tỉnh có được nền tảng xác thực “gốc” chuẩn hóa, giúp người dân nắm quyền làm chủ dữ liệu cá nhân của mình khi thực hiện thủ tục hành chính trực tuyến tại địa phương, giảm thiểu tối đa tình trạng giả mạo danh tính để đánh cắp dữ liệu.

Thứ sáu, công tác tuyên truyền, phổ biến nâng cao nhận thức xã hội được nâng lên một bước là nhờ sự chuyển đổi phương thức truyền thông mạnh mẽ, từ “mệnh lệnh giấy tờ” sang “tương tác trực tiếp”. Việc các tỉnh phát huy tối đa năng lực của Tổ công nghệ số cộng đồng đã giải thích các quy tắc bảo mật phức tạp một cách bình dân cho người dân, góp phần nâng cao nhận thức tự bảo vệ ngay từ cơ sở.

Thứ bảy, hợp tác và kiểm soát dòng chảy dữ liệu (thuê dịch vụ công nghệ): Sự dịch chuyển từ “phó thác” sang “quản trị có chủ quyền”, giúp giữ an toàn dữ liệu công dân, không để rò rỉ ra thị trường chợ đen; cụ thể, chính quyền tỉnh đã đưa các điều khoản bóc tách vai trò (Bên kiểm soát và Bên xử lý) vào hợp đồng thương mại với doanh nghiệp. Việc ưu tiên thuê hạ tầng “Cloud Việt” của các tập đoàn lớn chịu sự quản lý của Nhà nước (Viettel, VNPT) giúp chính quyền tỉnh duy trì được quyền giám sát và tối ưu hóa an ninh dữ liệu, giúp các tỉnh giải được bài toán thiếu hụt hạ tầng công nghệ lõi mà không cần phụ thuộc vào các nền tảng Cloud nước ngoài, bảo đảm an toàn chủ quyền dữ liệu.

Tóm lại, nguyên nhân tổng hợp của các kết quả đạt được về bảo vệ quyền đối với DLCN tại chính quyền số cấp tỉnh thời gian qua là nhờ sự cộng hưởng đồng bộ giữa hai nhóm yếu tố: Kỹ thuật công nghệ và Mệnh lệnh thể chế. Hệ thống 6 phương thức này đã vận hành như một bộ máy khép kín, giúp chính quyền địa phương vừa khai thác tốt tài nguyên số phục vụ phát triển, vừa bảo đảm an toàn chủ quyền dữ liệu.

Tuy nhiên, các nguyên nhân thành công này chủ yếu mới giải quyết được bài toán bảo vệ từ phía Nhà nước. Để thấy rõ những khoảng trống khi nhìn từ góc độ bảo đảm quyền thực chất của người dân, chúng ta cần phải phân tích sâu các hạn chế, tồn tại được nêu tại mục tiếp theo.

3.3.3. Những hạn chế, nguyên nhân hạn chế về bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh ở Việt Nam

3.3.3.1. Hạn chế về bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh ở Việt Nam

Thứ nhất, hạn chế trong hoàn thiện thể chế, pháp lý và quy chế nội bộ.

(1). Khuôn khổ pháp luật về bảo vệ quyền đối với DLCN còn mang tính đa tầng, phân tán và thiếu sự đồng bộ, gây khó khăn cho việc áp dụng thống nhất trong quá trình xây dựng và vận hành chính quyền số cấp tỉnh. Hiện nay, các quy định liên quan đến DLCN và quyền đối với DLCN được quy định rải rác trong nhiều văn bản pháp luật khác nhau. Tuy nhiên, mối quan hệ giữa các văn bản này chưa được xây dựng theo hướng phân định rõ ràng phạm vi điều chỉnh, áp dụng và nguyên tắc ưu tiên, dẫn đến tình trạng chồng lấn về nghĩa vụ bảo vệ quyền dữ liệu nhưng lại chưa quy định rõ trách nhiệm pháp lý khi quyền của cá nhân bị xâm phạm.

(2). Pháp luật hiện hành còn thiếu sự cụ thể hóa các quyền đối với DLCN theo bối cảnh đặc thù của khu vực công, đặc biệt trong mô hình chính quyền số cấp tỉnh. Mặc dù các quyền cơ bản của chủ thể dữ liệu như quyền được biết, quyền đồng ý, quyền truy cập, chỉnh sửa, hạn chế xử lý hay xóa dữ liệu đã được ghi nhận ở mức

nguyên tắc, nhưng các quy định này chưa được chuyển hóa thành các tiêu chí vận hành cụ thể đối với các hệ thống kỹ thuật đang được sử dụng phổ biến ở địa phương. Pháp luật chưa quy định rõ trách nhiệm của cơ quan nhà nước trong việc đánh giá tác động xử lý DLCN, phân loại mức độ nhạy cảm của dữ liệu trong từng thủ tục hành chính, hay giới hạn việc tái sử dụng DLCN cho các mục đích mới. Đặc biệt, khi xảy ra hành vi xử lý dữ liệu vượt quá mục đích ban đầu hoặc gây phương hại đến quyền, lợi ích của cá nhân, các quy định hiện hành chưa thiết lập được chế tài đủ sức răn đe hoặc cơ chế bồi thường tương xứng.

(3). Cơ chế bảo đảm thực thi quyền đối với DLCN còn thiếu tính khả dụng và hiệu quả trong môi trường chính quyền số, nhất là khi dữ liệu được xử lý theo chuỗi và liên thông qua nhiều hệ thống khác nhau. Các nguyên tắc quan trọng như minh bạch, thông báo, sự đồng ý của chủ thể dữ liệu, giới hạn mục đích, tối thiểu hóa dữ liệu và giới hạn thời hạn lưu trữ tuy đã được pháp luật ghi nhận, nhưng chưa có hướng dẫn thống nhất về hình thức, quy trình và trách nhiệm thực hiện ở cấp tỉnh.

Pháp luật chưa quy định rõ biểu mẫu yêu cầu thực hiện quyền đối với DLCN, thời hạn giải quyết yêu cầu của công dân, cơ quan có thẩm quyền chịu trách nhiệm chính khi dữ liệu đã được chia sẻ qua nhiều hệ thống, cũng như nghĩa vụ giải trình trong trường hợp xảy ra vi phạm. Đặc biệt, chế tài xử lý hành vi xâm phạm quyền đối với DLCN trong khu vực công còn chưa tương xứng với mức độ rủi ro và hậu quả, chủ yếu dừng lại ở xử lý kỷ luật hành chính nội bộ hoặc các quy định mang tính nguyên tắc, thiếu cơ chế bảo vệ hữu hiệu cho cá nhân bị xâm phạm quyền. Điều này làm suy giảm tính răn đe của pháp luật và ảnh hưởng trực tiếp đến mức độ tin cậy của người dân đối với chính quyền số cấp tỉnh.

Việc cụ thể hóa các văn bản chỉ đạo và quy chế nội bộ tại một số địa phương theo tinh thần Nghị định 13/2023/NĐ-CP còn thiếu tính thực tiễn, chưa được chuyển hóa thành các quy trình nghiệp vụ cụ thể cho đội ngũ thực thi. Bên cạnh đó, khung pháp lý cấp tỉnh vẫn chưa được bổ sung, hoàn thiện các quy định quản lý đối với các mô hình dữ liệu mới phát sinh, điển hình như dữ liệu trắc sinh học khuôn mặt thu thập qua hệ thống camera giám sát đô thị thông minh (IOC).

Theo báo cáo chỉ số DTI năm 2024 của Bộ Thông tin và Truyền thông (cũ), nay là Bộ KH-CN về khung pháp lý nội bộ tại 63 tỉnh, thành phố (cũ) cho thấy, mặc dù 100% các tỉnh có văn bản chỉ đạo chung về triển khai Nghị định 13, nhưng chưa đến 15% số tỉnh ban hành được quy trình kỹ thuật riêng biệt để xử lý các yêu cầu của công dân về quyền dữ liệu (như quy trình rút lại sự đồng ý hoặc xóa dữ liệu trên hệ thống một cửa) [9].

Thứ hai, hạn chế trong tổ chức bộ máy và quản trị nhân sự

(1). Chưa hình thành được cơ chế tổ chức chuyên trách và thống nhất về bảo vệ quyền đối với DLCN trong bộ máy chính quyền số cấp tỉnh. Trong thực tiễn, các hoạt động xử lý DLCN phục vụ cung cấp dịch vụ công được phân tán ở nhiều cơ quan, đơn vị khác nhau, nhưng chưa có đầu mối chịu trách nhiệm xuyên suốt về bảo vệ quyền đối với DLCN. Điều này dẫn đến tình trạng quyền và nghĩa vụ liên quan đến DLCN bị chia nhỏ theo chức năng quản lý, trong khi quyền của chủ thể dữ liệu mang tính toàn diện và liên tục trong suốt vòng đời xử lý dữ liệu. Hạn chế này thể hiện rõ khi DLCN được liên thông, chia sẻ giữa nhiều hệ thống và cơ quan ở cấp tỉnh: không xác định rõ cơ quan nào chịu trách nhiệm chính trong việc bảo đảm quyền của cá nhân, đặc biệt khi phát sinh khiếu nại hoặc tranh chấp liên quan đến việc sử dụng dữ liệu. Việc thiếu một cơ chế tổ chức rõ ràng khiến quyền đối với DLCN khó được bảo vệ hiệu quả trên thực tế, dù đã được ghi nhận trong pháp luật.

(2). Việc bảo vệ quyền đối với DLCN chưa được tích hợp đầy đủ vào quy trình nghiệp vụ hành chính điện tử, mà chủ yếu dừng lại ở yêu cầu kỹ thuật hoặc thủ tục hành chính chung. Trong nhiều quy trình giải quyết thủ tục hành chính trực tuyến, việc thu thập và xử lý DLCN vẫn được xây dựng theo hướng phục vụ yêu cầu quản lý, chưa thể hiện rõ các điểm kiểm soát nhằm bảo đảm các quyền cụ thể của chủ thể dữ liệu, như quyền được biết, quyền truy cập, quyền chỉnh sửa hoặc quyền hạn chế xử lý dữ liệu.

(3). Chưa thiết lập được vị trí người phụ trách bảo vệ dữ liệu (DPO) chuyên trách theo đúng tinh thần thông lệ quốc tế. Bộ máy bảo vệ dữ liệu tại các sở, ban, ngành hiện nay hoàn toàn là kiêm nhiệm. Cán bộ kỹ thuật CNTT phải gánh thêm trách nhiệm pháp lý về quyền con người đối với dữ liệu trong khi không có chuyên môn sâu, dẫn đến tình trạng quá tải và lúng túng. Theo thống kê về nhân lực số tại khu vực công cấp tỉnh, hơn 80% cán bộ phụ trách an toàn thông tin tại các cơ quan chuyên môn cấp tỉnh hiện nay đang phải làm việc theo chế độ kiêm nhiệm [10]. Theo báo cáo tổng kết thực thi Nghị định 13 của Bộ Công an (Cục An ninh mạng và Phòng chống tội phạm sử dụng công nghệ cao - A05) thì tỷ lệ cán bộ tại bộ phận “Một cửa” cấp huyện (trước đây), xã được đào tạo bài bản, có chứng chỉ chuyên sâu về pháp luật bảo vệ dữ liệu cá nhân đạt dưới 5% [6].

Thứ ba, hạn chế trong áp dụng biện pháp kỹ thuật và công nghệ

(1). Hạ tầng kỹ thuật của chính quyền số cấp tỉnh chưa bảo đảm đầy đủ các điều kiện kỹ thuật cần thiết để thực thi quyền đối với DLCN một cách hiệu quả. Hạ tầng công nghệ của nhiều địa phương chấp vá, tồn tại nhiều “điểm mù” kỹ thuật tại

các điểm giao tiếp dữ liệu (API) liên thông. Hệ thống ghi vết (Audit Logs) của các phần mềm hành chính công còn lỏng lẻo, chưa tự động cảnh báo được các hành vi truy cập dữ liệu bất thường của cán bộ khi không đi kèm mã hồ sơ thủ tục hành chính. Theo đánh giá từ Cục An toàn thông tin (Bộ TT&TT) về xếp hạng chuyển đổi số (DTI) khối địa phương chỉ ra rằng: Chỉ có khoảng 30% các tỉnh, thành phố triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin theo Cấp độ (từ Cấp độ 3 trở lên) đối với các kho dữ liệu dùng chung. Hơn 60% cổng dịch vụ công cấp tỉnh còn tồn tại các lỗ hổng bảo mật cấu hình ở mức độ “Nguy hiểm” và “Cao”, dễ bị tin tặc khai thác [9].

(2). Các hệ thống thông tin và cơ sở dữ liệu hiện nay chủ yếu được xây dựng với mục tiêu kết nối, liên thông và chia sẻ dữ liệu, trong khi chức năng hỗ trợ thực hiện quyền của chủ thể dữ liệu còn thiếu hoặc chưa hoàn chỉnh. Nhiều hệ thống chưa cho phép cá nhân kiểm tra lịch sử truy cập dữ liệu, theo dõi việc chia sẻ dữ liệu giữa các cơ quan, hoặc chủ động yêu cầu chỉnh sửa, cập nhật thông tin cá nhân. Bên cạnh đó, việc áp dụng các biện pháp kỹ thuật bảo vệ dữ liệu như phân quyền truy cập chi tiết, ghi nhật ký xử lý dữ liệu, hay cơ chế kiểm soát truy cập theo mục đích xử lý chưa được triển khai đồng bộ giữa các địa phương và các hệ thống. Điều này làm gia tăng nguy cơ xâm phạm quyền đối với DLCN và hạn chế khả năng phát hiện, ngăn chặn kịp thời các hành vi xử lý dữ liệu không phù hợp.

Thứ tư, hạn chế trong công tác thanh tra, kiểm tra và xử lý vi phạm

(1). Cơ chế giám sát, thanh tra, kiểm tra và xử lý vi phạm liên quan đến DLCN trong xây dựng chính quyền số cấp tỉnh còn thiếu hiệu quả về mặt tổ chức và kỹ thuật. Việc giám sát tuân thủ các quy định về bảo vệ DLCN chưa được xây dựng như một quy trình độc lập, mà thường lồng ghép trong hoạt động kiểm tra an toàn thông tin hoặc thanh tra hành chính chung. Khi xảy ra sự cố liên quan đến DLCN, cá nhân bị ảnh hưởng chưa có kênh tiếp cận rõ ràng để yêu cầu bảo vệ quyền và lợi ích hợp pháp của mình, trong khi các cơ quan nhà nước liên quan thiếu cơ chế phối hợp hiệu quả để xử lý trách nhiệm. Đây là một hạn chế đáng kể về tổ chức - kỹ thuật, làm suy giảm tính thực chất của quyền đối với DLCN trong quá trình xây dựng chính quyền số cấp tỉnh.

(2). Hoạt động thanh tra chuyên ngành về bảo vệ DLCN tại địa phương còn hạn chế, chủ yếu mang tính chất “nhắc nhở hành chính” khi có sự cố xảy ra chứ chưa chủ động phòng ngừa. Cơ chế xử lý vi phạm trong nội bộ cơ quan nhà nước khi để lộ thông tin của dân chưa nghiêm, chưa có tiền lệ quy trách nhiệm bồi thường dân sự hay xử lý hình sự người đứng đầu cơ quan chính quyền cấp tỉnh. Theo báo cáo từ các Sở TT&TT gửi về Bộ TT&TT (cũ) hàng năm trong giai đoạn vừa qua, số cuộc thanh

tra chuyên đề chuyên sâu về việc chấp hành pháp luật bảo vệ dữ liệu cá nhân tại các sở, ngành và UBND các cấp còn rất ít (trung bình dưới 2 cuộc thanh tra/tỉnh/năm). Các hình thức xử lý chủ yếu dừng lại ở mức kiểm điểm rút kinh nghiệm nội bộ là chính.

Thứ năm, hạn chế trong bảo vệ quyền thực chất của chủ thể dữ liệu

Quyền tự quyết thông tin gắn với quyền công dân bị “vô hiệu hóa” bởi cơ chế đồng ý một chiều. Người dân bắt buộc phải bấm đồng ý cho hệ thống khai thác mọi thông tin thì mới được nộp hồ sơ TTHC trực tuyến. Các quyền cốt lõi như quyền rút lại sự đồng ý, quyền xóa dữ liệu hay quyền phản đối các quyết định tự động bằng thuật toán (AI) hoàn toàn không có tính năng kỹ thuật hay quy trình hành chính để người dân thực hiện trên thực tế. Theo báo cáo chỉ số hiệu quả quản trị và hành chính công cấp tỉnh tại Việt Nam (PAPI), qua khảo sát về trải nghiệm người dùng trên 20 cổng dịch vụ công cấp tỉnh tiêu biểu cho thấy: 100% các cổng dịch vụ công không thiết kế nút chức năng “Rút lại sự đồng ý” hoặc “Yêu cầu xóa dữ liệu” dành cho tài khoản của công dân sau khi thủ tục hành chính đã được hoàn thành [58].

Thứ sáu, hạn chế trong công tác tuyên truyền, phổ biến nâng cao nhận thức xã hội

Công tác truyền thông tại một số địa phương hiện đang tập trung chủ yếu vào việc thúc đẩy người dân tiếp cận các ứng dụng chính quyền số và số hóa dữ liệu, mà chưa chú trọng đúng mức việc phổ biến kiến thức về quyền lợi và các biện pháp tự bảo vệ thông tin cá nhân theo quy định pháp luật. Bên cạnh đó, chưa tập trung tuyên truyền để nâng cao năng lực số cho người dân khu vực nông thôn, miền núi và người cao tuổi nhằm giảm thiểu tối đa các rủi ro an ninh mạng đối với nhóm đối tượng này.

Nội dung truyền thông của các tỉnh bị lệch pha, nặng về tính “vận động một chiều” (vận động dân nộp dữ liệu, cài app chính quyền số) mà bỏ quên việc giáo dục cho dân biết về “bộ quyền tự vệ” của mình theo pháp luật. Tình trạng thiếu hiểu biết về kỹ năng số ở vùng nông thôn, miền núi, nhóm người cao tuổi tại địa phương vẫn chưa được khóa lấp, biến họ thành mục tiêu dễ bị tổn thương trước tội phạm công nghệ. Theo báo cáo đánh giá của Cục Phát thanh, Truyền hình và Thông tin điện tử (Bộ TT&TT) về “Hiệu quả công tác truyền thông, thông tin cơ sở phục vụ Chuyển đổi số” năm 2024 cho thấy: Các chương trình tuyên truyền tại địa phương hiện nay có đến 75% thời lượng và nội dung tập trung vào việc hướng dẫn thao tác kỹ thuật (cách cài VNeID, cách nộp hồ sơ trực tuyến), trong khi nội dung cảnh báo rủi ro pháp lý và hướng dẫn quyền tự quyết thông tin của công dân chỉ chiếm dưới 10% tổng lượng thông tin truyền thông [9].

Thứ bảy, hạn chế trong hợp tác và kiểm soát dòng chảy dữ liệu

Trong quá trình triển khai, mô hình hợp tác công - tư về hạ tầng dữ liệu còn bộc lộ một số bất cập trong phân định quyền quản trị thực tế. Do tính chất chuyên sâu về mặt kỹ thuật, việc kiểm soát và vận hành trực tiếp các kho dữ liệu đám mây (Cloud) hiện phụ thuộc lớn vào đội ngũ kỹ sư của đơn vị vận hành tư nhân. Đồng thời, khung pháp lý trong các hợp đồng dịch vụ CNTT hiện tại chưa bao quát hết các chế tài giám sát khách quan và quy trình đền bù thiệt hại trực tiếp cho người dân trong trường hợp phát sinh sự cố lộ lọt thông tin.

Theo Báo cáo tình hình an toàn thông tin mạng và nhiễm mã độc tại khu vực công của Cục An toàn thông tin - Bộ Thông tin và Truyền thông thì Việt Nam nằm trong nhóm các quốc gia có lượng dữ liệu cá nhân bị rao bán lớn nhất thế giới (với hàng tỷ dòng dữ liệu công dân bị rò rỉ). Đáng chú ý, hơn 70% các gói dữ liệu rao bán trên chợ đen (Telegram, các diễn đàn hacker) bị tối ưu hóa và phân loại theo địa giới hành chính cấp tỉnh (ví dụ: danh sách chủ xe, danh sách chủ đất tại các tỉnh/thành cụ thể), điều này chứng tỏ dữ liệu tại địa phương đang bị rò rỉ nghiêm trọng qua các bên thứ ba tham gia vận hành hệ thống [35].

Tóm lại, trong xây dựng chính quyền số cấp tỉnh hiện nay: Chính quyền địa phương đang đẩy mạnh làm sạch cơ sở dữ liệu trong toàn dân và trên tất cả các lĩnh vực, tuy nhiên, , nhưng năng lực và công cụ bảo vệ quyền lợi cho người dân trước các rủi ro công nghệ lại đang vận hành ở tốc độ rất thấp. Khoảng cách giữa văn bản pháp lý và thực tế thực thi tại các tỉnh không chỉ đe dọa đến quyền an toàn thông tin của công dân, mà về lâu dài sẽ làm xói mòn “niềm tin số” của Nhân dân vào tính chính danh và an toàn của mô hình chính quyền số. Đây là nút thắt thể chế và kỹ thuật lớn nhất, đòi hỏi phải có những giải pháp đột phá và đồng bộ ở chương tiếp theo.

3.3.3.2. Nguyên nhân của những hạn chế trong bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh ở Việt Nam

Thứ nhất, nguyên nhân khách quan:

(1). *Sự bất cập và xung đột pháp lý từ cấp Trung ương:* Nghị định 13/2023/NĐ-CP là văn bản dưới Luật nên chưa đủ hiệu lực pháp lý cao nhất để giải quyết xung đột với các luật chuyên ngành. Mặc dù sau khi Luật Bảo vệ dữ liệu cá nhân đã chính thức được Quốc hội ban hành và có hiệu lực, nâng tầm hành lang pháp lý lên cấp độ cao nhất, nhưng ở giai đoạn đầu thực thi, các cơ quan Trung ương vẫn chưa ban hành đầy đủ các thông tư hướng dẫn chi tiết về việc xử lý các điểm giao thoa pháp lý với các luật chuyên ngành khác. Điển hình là sự chồng chéo giữa “Quyền được xóa dữ liệu của công dân” (theo Luật Bảo vệ dữ liệu cá nhân) và “Nghĩa vụ lưu trữ hồ sơ, tài liệu hành chính vĩnh viễn” (theo Luật Lưu trữ, Luật Đất đai, Luật Hộ

tịch). Việc thiếu các văn bản hướng dẫn liên bộ quy định rõ trường dữ liệu nào thuộc diện bắt buộc lưu trữ quốc gia, trường dữ liệu nào công dân được quyền yêu cầu xóa bỏ đã khiến chính quyền cấp tỉnh rơi vào trạng thái lúng túng. Địa phương thiếu đi một căn cứ vĩ mô rõ ràng để thiết kế quy trình kỹ thuật và các nút chức năng hồi đáp trên hệ thống Một cửa cho người dân thực hiện quyền tự quyết thông tin.

(2). *Tốc độ phát triển siêu tốc của công nghệ số*: Sự bùng nổ của Trí tuệ nhân tạo (AI), dữ liệu lớn (Big Data) và các phương thức tấn công mạng tinh vi diễn ra theo cấp số nhân. Trong khi đó, quy trình phê duyệt ngân sách công và đấu thầu mua sắm trang thiết bị bảo mật tại địa phương phải tuân thủ Luật Đấu thầu rất nghiêm ngặt và mất nhiều thời gian. Sự lệch pha về mặt tốc độ này khiến công nghệ bảo mật của tỉnh luôn bị lạc hậu so với thực tế.

(3). *Tính chất ẩn danh của thị trường “chợ đen” xuyên biên giới*: Dữ liệu sau khi bị rò rỉ ngay lập tức được phân tán lên các nền tảng mã hóa, ẩn danh như Telegram hoặc các diễn đàn Dark Web. Việc truy tìm dấu vết, điều tra tận gốc các đối tượng này vượt quá năng lực kỹ thuật và thẩm quyền tư pháp của các cơ quan chức năng cấp tỉnh, đòi hỏi phải có sự can thiệp từ lực lượng an ninh quốc gia.

Thứ hai, nguyên nhân chủ quan:

(1). *Nguyên nhân về thể chế và quy chế nội bộ*:

Sự lệch pha về mặt chính sách và độ trễ pháp lý; khung pháp lý về Chính quyền số được xây dựng dựa trên tư duy quản lý nhà nước truyền thống, lấy chỉ tiêu hành chính và số hóa thủ tục làm trung tâm, coi dữ liệu cá nhân thuần túy là “nguồn lực phục vụ quản lý”. Trong khi đó, pháp luật bảo vệ DLCN lại tiếp cận dựa trên tư duy quyền con người và quyền riêng tư hiến định. Sự phát triển bùng nổ của các nền tảng số công quyền diễn ra trước khi khung pháp lý chuyên biệt về quyền dữ liệu được hình thành, tạo ra khoảng trống thể chế kéo dài. Lãnh đạo các cơ quan chuyên môn cấp tỉnh thiếu chủ động do tâm lý “chờ đợi hướng dẫn” thường ban hành văn bản mang tính chất “qua chuyện”, thậm chí sao chép nguyên bản Nghị định 13/2023/NĐ-CP mà không cụ thể hóa thành quy trình tác nghiệp cho cán bộ; đồng thời bỏ ngỏ việc ban hành quy chế quản lý đối với các mô hình dữ liệu nhạy cảm mới phát sinh (như dữ liệu trắc sinh học khuôn mặt từ hệ thống Camera AI/IOC đô thị thông minh).

Cơ chế tác động và áp lực chỉ tiêu thi đua về chuyển đổi số (như Chỉ số DTI, tỷ lệ hồ sơ trực tuyến, phủ sóng VNeID) buộc chính quyền cấp tỉnh phải ưu tiên tối đa cho tốc độ thu thập, số hóa và liên thông dữ liệu. Trong quy trình xây dựng thể chế và phát triển phần mềm, giải pháp bảo vệ dữ liệu chỉ được xem là yếu tố bổ sung sau thay vì được tích hợp ngay từ đầu. Đồng thời, cơ chế thẩm định pháp lý hiện nay hoàn toàn bỏ ngỏ bước đánh giá tác động xử lý DLCN (DPIA) trước khi đưa các hệ

thống vào vận hành. Thể hiện trên thực tế là 100% Công dịch vụ công cấp tỉnh áp dụng cơ chế “Đồng ý một chiều” (công dân bắt buộc phải đồng ý cho khai thác toàn bộ dữ liệu mới được nộp hồ sơ TTHC); chưa đến 15% số tỉnh ban hành được Quy trình kỹ thuật riêng biệt để giải quyết các yêu cầu thực thi quyền của công dân (như quy trình rút consent, xóa dữ liệu trên hệ thống Một cửa); các công nghệ giám sát đô thị thông minh (IOC/Camera AI) vận hành trong tình trạng thiếu quy chế quản lý dữ liệu trắc sinh học... Từ đó quyền năng của công dân bị ảnh hưởng; trực tiếp tước bỏ Quyền tự quyết thông tin (Quyền được biết/Minh bạch thông tin, và Quyền đồng ý/Rút lại sự đồng ý của chủ thể dữ liệu); biến công dân thành “chủ thể thụ động” trong môi trường số; tạo ra khoảng trống pháp lý vô hiệu hóa khả năng khiếu nại, tố cáo hoặc yêu cầu bồi thường thiệt hại của người dân khi xảy ra sự cố rò rỉ dữ liệu.

(2). Nguyên nhân về tổ chức bộ máy và nhân sự:

Sự xung đột giữa mô hình công vụ truyền thống và sự đứt gãy về năng lực chuyên môn. Cơ cấu bộ máy cấp tỉnh được thiết kế theo tư duy quản lý truyền thống (phân chia theo địa giới hành chính và chức năng sở/ngành), hoàn toàn chưa thích ứng với tính chất “phi địa giới và liên thông liên tục” của dữ liệu số. Bên cạnh đó, sự thiếu hụt nguồn lực chuyên trách và đãi ngộ chưa tương xứng. Pháp luật và chính sách hiện hành thiếu vắng quy định bắt buộc thành lập vị trí “Nhân sự phụ trách bảo vệ dữ liệu” (DPO) độc lập trong khu vực công. Ngân sách nhà nước ưu tiên chi cho mua sắm hạ tầng dịch vụ công mà chưa quan tâm đúng mức đến việc đầu tư cho nhân sự. Đồng thời, cơ chế tiền lương khu vực công không đủ sức hút, gây ra tình trạng “chảy máu chất xám” chuyên gia an toàn thông tin giỏi sang khu vực tư nhân. Ngoài ra, nhận thức của đội ngũ cán bộ, công chức còn mang nặng tư duy cũ, coi việc thu thập và chia sẻ dữ liệu là hoạt động nghiệp vụ nội bộ của cơ quan nhà nước thay vì là hoạt động xử lý thông tin gắn liền với quyền riêng tư của công dân. Do thiếu biên chế chuyên trách DPO và thiếu hụt nhân sự tinh nhuệ, các cơ quan cấp tỉnh buộc phải dùng bộ máy nhân sự kiêm nhiệm để giải quyết một bài toán quản trị dữ liệu hiện đại. Trách nhiệm bảo vệ dữ liệu (vốn đòi hỏi sự am hiểu sâu về pháp lý quyền con người) bị đùn đẩy sang cho cán bộ kỹ thuật CNTT hoặc cán bộ bộ phận “Một cửa”. Các nguyên tắc pháp lý không được chuyển hóa thành quy trình nghiệp vụ hàng ngày do thiếu các chương trình đào tạo chuyên sâu. Trên thực tế có hơn 80% cán bộ an toàn thông tin tại các cơ quan chuyên môn cấp tỉnh phải làm việc theo chế độ kiêm nhiệm (xem bảo vệ dữ liệu là “nhiệm vụ phụ”); có dưới 5% cán bộ tại bộ phận “Một cửa” được đào tạo bài bản hoặc có chứng chỉ chuyên sâu về pháp luật bảo vệ dữ liệu cá nhân; khi xảy ra sự cố lộ lọt dữ liệu liên thông qua LGSP, các đơn vị đổ lỗi lẫn nhau, trách nhiệm bị chia nhỏ, không cơ quan nào đứng ra chịu trách nhiệm chính. Từ đó một số quyền năng của công dân bị ảnh hưởng; trực tiếp xâm phạm Quyền truy

cập, chỉnh sửa, hạn chế xử lý dữ liệu và Quyền được phản hồi/giải trình của chủ thể dữ liệu. Dẫn đến bộ máy vận hành rơi vào trạng thái “quá tải và lúng túng”; quy trình giải quyết các yêu cầu về quyền dữ liệu bị đứt gãy trên thực tế; công dân hoàn toàn không có đầu mối công vụ chuyên trách để nộp yêu cầu thực thi quyền, khiếu nại hoặc yêu cầu bảo vệ khi quyền lợi bị xâm phạm.

(3). Nguyên nhân về biện pháp kỹ thuật và công nghệ:

Sự bất tương thích về kiến trúc hệ thống, thiếu hụt đầu tư và sự lệ thuộc vào hạ tầng tư nhân; kiến trúc phần mềm chắp vá, thiếu tiêu chuẩn ngay từ đầu: Các hệ thống phần mềm Dịch vụ công trực tuyến và CSDL công quyền cấp tỉnh được xây dựng qua nhiều thời kỳ, lắp ghép chắp vá từ nhiều nhà thầu khác nhau theo tư duy “vừa chạy vừa xếp hàng”. Hệ thống ưu tiên tính năng “kết nối - thu thập” thay vì được thiết kế theo tiêu chuẩn “Bảo vệ dữ liệu ngay từ khâu thiết kế” (Privacy by Design), hoàn toàn thiếu các module mã hóa dữ liệu nhạy cảm hay tự động ghi vết hành vi. Bên cạnh đó, sự thiếu hụt, phân tán nguồn vốn đầu tư an toàn thông tin; nhiều địa phương không tuân thủ nghiêm túc chỉ tiêu dành tối thiểu 10% ngân sách CNTT cho an toàn thông tin (theo Chỉ thị số 14/CT-TTg năm 2019). Nguồn vốn đầu tư mang tính “nhỏ giọt, dàn trải”, dẫn đến thiếu hụt trang thiết bị phòng thủ chuyên sâu (SOC, tường lửa thế hệ mới, phần mềm rà quét tự động). Sự lệ thuộc vào hạ tầng tư nhân (Cloud/Vendor Lock-in): Chính quyền cấp tỉnh thiếu hạ tầng công nghệ độc lập nên phụ thuộc lớn vào dịch vụ Cloud và đội ngũ kỹ sư của doanh nghiệp CNTT tư nhân. Dưới áp lực thúc đẩy chỉ số chia sẻ dữ liệu từ Trung ương, các tỉnh bùng nổ mở cổng kết nối API liên thông nhưng lại thiếu năng lực kiểm soát kỹ thuật nội tại và thiếu các biện pháp xác thực mạnh, tạo ra những “lỗ hổng công nghệ liên thông”. Đồng thời, các hợp đồng dịch vụ CNTT/Cloud ký kết với nhà thầu tư nhân bị điều chỉnh chủ yếu bởi pháp luật về đấu thầu và thương mại (vốn chỉ chú trọng đến giá cả và phạt vi phạm hợp đồng), hoàn toàn thiếu các tiêu chuẩn kỹ thuật bắt buộc về bảo vệ dữ liệu cá nhân cũng như cơ chế bồi thường cho bên thứ ba (công dân) khi xảy ra sự cố. Trên thực tế, có hơn 60% Cổng dịch vụ công cấp tỉnh tồn tại lỗ hổng bảo mật cấu hình ở mức “Nguy hiểm” và “Cao”; hệ thống ghi vết (Audit Log) lỏng lẻo, không tự động cảnh báo hành vi truy cập bất thường của cán bộ; kỹ sư nhà thầu tư nhân nắm đặc quyền quản trị cao nhất (Super Admin/Root) nhưng không có cơ chế kiểm toán độc lập từ phía cơ quan nhà nước; hơn 70% các gói dữ liệu cá nhân rao bán trên chợ đen bị phân loại, tối ưu hóa theo địa giới hành chính cấp tỉnh, chứng minh dữ liệu bị rò rỉ theo dây chuyền qua các “điểm mù” kết nối API và nhà thầu tư nhân [34]... Dẫn đến một số quyền năng của cá nhân bị ảnh hưởng; xâm phạm nghiêm trọng Quyền an toàn, bảo mật dữ liệu và vô hiệu hóa Quyền yêu cầu bồi thường thiệt hại của chủ thể dữ liệu. Từ đó, bộc lộ các “điểm mù” kỹ thuật khiến dữ liệu công dân bị rò rỉ trên quy mô lớn; chính quyền mất

khả năng tự chủ kỹ thuật, không thể cung cấp bằng chứng ghi vết để truy cứu trách nhiệm công vụ, dẫn đến sự đứt gãy nghiêm trọng “niềm tin số” của Nhân dân vào mô hình Chính quyền số.

(4). Nguyên nhân về công tác thanh tra, kiểm tra và xử lý vi phạm:

Hoạt động *thanh tra, kiểm tra và xử lý vi phạm* còn mang nặng tính hình thức, "vừa đá bóng vừa thổi còi" (Sở TT&TT trước đây, nay là Sở KHCN vừa vận hành vừa đi kiểm tra). Tâm lý nể nang, né tránh trong nội bộ khu vực công; khi xảy ra lộ lọt dữ liệu, hình thức xử lý chủ yếu là phê bình, rút kinh nghiệm nội bộ, chưa áp dụng các chế tài nghiêm khắc đối với người đứng đầu để tạo tính răn đe.

Cơ chế giám sát và trách nhiệm giải trình trong xử lý DLCN chưa được thiết lập đầy đủ, dẫn đến việc vi phạm quyền đối với DLCN khó bị phát hiện và xử lý kịp thời. Việc giám sát hiện nay chủ yếu tập trung vào an toàn, an ninh thông tin, trong khi các hành vi xâm phạm quyền đối với DLCN không phải lúc nào cũng gắn liền với sự cố kỹ thuật. Khi thiếu các cơ chế giám sát chuyên biệt và trách nhiệm giải trình rõ ràng, việc xử lý vi phạm thường mang tính hình thức, chưa tạo được sức răn đe cần thiết. Đây là một trong những nguyên nhân trực tiếp khiến các hạn chế trong bảo vệ quyền đối với DLCN kéo dài trong quá trình xây dựng chính quyền số cấp tỉnh.

(5). Nguyên nhân về bảo đảm quyền thực chất của công dân:

Dưới áp lực hoàn thành các chỉ tiêu chuyển đổi số (như tỷ lệ hồ sơ xử lý trực tuyến, tỷ lệ liên thông dữ liệu), quá trình phát triển các hệ thống phần mềm hành chính công cấp tỉnh thời gian qua chủ yếu tập trung vào việc tối ưu hóa chức năng thu thập, quản lý và chia sẻ dữ liệu phục vụ nghiệp vụ của cơ quan nhà nước, mà chưa quan tâm đúng mức đến các tính năng kỹ thuật tương tác trên giao diện dịch vụ công trực tuyến giúp người dân chủ động thực thi quyền của mình (như công cụ rút lại sự đồng ý, yêu cầu cập nhật hoặc xóa bỏ dữ liệu cá nhân theo quy định của pháp luật).

(6). Nguyên nhân về công tác tuyên truyền, nâng cao nhận thức của công dân:

Cơ quan chức năng tại địa phương chưa nhận thức đúng tầm quan trọng của việc nâng cao “năng lực tự vệ số” cho người dân, mà mới chỉ tổ chức truyền thông một chiều, chạy theo thành tích. Các chương trình truyền thông mới chỉ tập trung hướng dẫn thao tác kỹ thuật (cách cài app, nộp hồ sơ) để tăng tỷ lệ dịch vụ công, chứ không giáo dục sâu rộng cho công dân biết về bộ quyền của mình.

(7). Nguyên nhân về hợp tác và kiểm soát dòng chảy dữ liệu

Sự phụ thuộc kỹ thuật và lỏng lẻo trong cam kết với bên thứ ba, do năng lực công nghệ nội tại yếu, chính quyền tỉnh phải phụ thuộc hoàn toàn vào các kỹ sư của nhà thầu công nghệ. Đồng thời, trong các hợp đồng kinh tế thuê dịch vụ CNTT, tỉnh

thiếu các điều khoản pháp lý ràng buộc trách nhiệm bồi thường thiệt hại trực tiếp cho người dân khi nhà thầu làm rò rỉ dữ liệu.

Tóm lại, tổng hợp hệ thống nguyên nhân trên chỉ ra một nghịch lý rằng: Chính quyền số cấp tỉnh đang đẩy mạnh thu thập tối đa dữ liệu của công dân ở tốc độ rất cao, nhưng năng lực thể chế và kỹ thuật để bảo vệ quyền lợi cho người dân lại đang vận hành ở tốc độ rất thấp. Sự rạn nứt này nếu không được khóa lấp sẽ làm xói mòn niềm tin số của Nhân dân.

Tiểu kết Chương 3

Chương 3 đã phân tích thực trạng bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh trên hai bình diện chủ yếu: Khung pháp luật và cơ chế chính sách hiện hành liên quan đến xử lý DLCN trong khu vực công; và thực tiễn vận hành các hệ thống chính quyền số ở cấp tỉnh, đặc biệt trong cung cấp dịch vụ công trực tuyến, giải quyết thủ tục hành chính, liên thông và chia sẻ dữ liệu giữa các cơ quan.

Với những chủ trương, chính sách quyết liệt của Đảng và Nhà nước, nhất là đòn bẩy công nghệ từ Đề án 06, chính quyền số cấp tỉnh thời gian qua đã đạt được những bước chuyển dịch căn bản. Thể chế nội bộ tại địa phương bước đầu được định hình tương thích với hệ thống pháp lý mới; hạ tầng kỹ thuật các kho dữ liệu dùng chung (LGSP) được nâng cấp bảo mật theo mô hình nhiều lớp (SOC); quyền tiếp cận và cải chính thông tin của công dân bước đầu được hiện thực hóa thông qua trực định danh VNeID; phương thức truyền thông số đã hướng mạnh về cơ sở thông qua Tổ công nghệ số cộng đồng và việc chia sẻ dữ liệu với các nhà thầu công nghệ bước đầu đã xác lập được ranh giới kiểm soát pháp lý.

Tuy nhiên, qua thực trạng các phương thức bảo vệ quyền và thực tiễn tại các địa phương, vẫn còn tồn tại những “khoảng cách” rất lớn. Thể chế nội bộ tại các tỉnh còn mang tính sao chép, bỏ ngỏ quy định đối với các công nghệ thế hệ mới (như dữ liệu trắc sinh học từ Camera AI); bộ máy nhân sự trong các cơ quan hành chính trực tiếp phụ trách CNTT, chuyển đổi số vẫn đang còn kiêm nhiệm, thiếu các vị trí chuyên trách (DPO); hạ tầng phần mềm chắp vá tồn tại nhiều “điểm mù” bảo mật tại các cổng kết nối liên thông (API); hoạt động thanh tra, xử lý vi phạm còn nể nang, thiếu tính răn đe. Đặc biệt, việc thực thi các quyền của chủ thể dữ liệu (tiếp cận, chỉnh sửa, hạn chế xử lý, phản đối, rút lại sự đồng ý khi áp dụng...) và quyền tự quyết thông tin thực chất của người dân bị “vô hiệu hóa” bởi cơ chế đồng ý một chiều, trong khi nội dung truyền thông bị lệch pha khi quá chú trọng vào thao tác kỹ thuật bề nổi mà bỏ quên việc trang bị năng lực tự vệ pháp lý cho công dân. Dữ liệu cấp tỉnh vẫn đang đứng trước rủi ro rò rỉ nghiêm trọng do sự phụ thuộc và lỏng lẻo trong giám sát nhà thầu công nghệ. Chương 3 cũng làm rõ nhóm nguyên nhân của các hạn chế như: Sự mất cân bằng giữa năng lực thu thập dữ liệu và năng lực bảo vệ quyền công dân xuất phát từ cả yếu tố khách quan lẫn chủ quan. Bên cạnh những nút thắt khách quan như độ trễ của các văn bản hướng dẫn luật vĩ mô, tốc độ phát triển siêu tốc của công nghệ và tính chất ẩn danh xuyên biên giới của tội phạm mạng, nguyên nhân chủ quan giữ vai trò quyết định. Đó là tư duy quản lý còn nặng tính thành tích, mới chủ yếu ưu tiên số hóa dữ liệu phục vụ Nhà nước là chính, chưa coi trọng quyền tự vệ của công dân, trách nhiệm của

người đứng đầu; là sự bất cập trong chính sách đãi ngộ nhân lực số khu vực công và sự phó thác kỹ thuật cho các doanh nghiệp tư nhân.

Mặt khác, thực trạng bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh hiện nay đang tồn tại sự “lệch pha” và đứt gãy giữa 3 tầng (An toàn kỹ thuật, quản trị công vụ, quyền con người). Tỉnh có thể làm rất tốt tầng An toàn kỹ thuật để chống lại các nguy cơ tấn công từ bên ngoài, nhưng lại bộc lộ khoảng trống lớn ở tầng Quản trị công vụ, khi chưa kiểm soát được nguy cơ lạm dụng dữ liệu nội bộ qua nền tảng LGSP, và gần như “bỏ ngỏ” tầng Quyền con người, khi chưa kỹ thuật hóa các quyền năng pháp lý của công dân thành các công cụ tương tác trên Cổng dịch vụ công. Đây chính là nguyên nhân cốt lõi khiến hiệu quả bảo vệ quyền đối với dữ liệu cá nhân trên thực tế ở địa phương còn thấp, đòi hỏi phải có sự chuyển dịch đồng bộ về thể chế và giải pháp công nghệ trong giai đoạn tới.

Tóm lại, dữ liệu của công dân đang được tập trung với tốc độ rất cao bằng các mệnh lệnh hành chính, nhưng các công cụ pháp lý và kỹ thuật để bảo vệ quyền lợi hợp pháp cho người dân lại đang vận hành ở tốc độ rất thấp. Chính quyền số cần xây dựng "niềm tin số" đối với chủ thể dữ liệu. Đây là căn cứ để đưa ra các định hướng và giải pháp nâng cao hiệu quả bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh ở chương tiếp theo của luận án.

Chương 4

QUAN ĐIỂM, GIẢI PHÁP BẢO VỆ QUYỀN ĐỐI VỚI DỮ LIỆU CÁ NHÂN TRONG XÂY DỰNG CHÍNH QUYỀN SỐ CẤP TỈNH Ở VIỆT NAM HIỆN NAY

4.1. DỰ BÁO BỐI CẢNH VÀ CÁC YẾU TỐ TÁC ĐỘNG ĐẾN BẢO VỆ QUYỀN ĐỐI VỚI DỮ LIỆU CÁ NHÂN TRONG XÂY DỰNG CHÍNH QUYỀN SỐ CẤP TỈNH TRONG THỜI GIAN TỚI

4.1.1. Những yếu tố tác động tích cực

4.1.1.1. Yếu tố cộng hưởng từ sự hoàn thiện và thực thi của Luật Bảo vệ DLCN

Việc hoàn thiện thể chế với trọng tâm là tiến trình xây dựng và đưa Luật Bảo vệ dữ liệu cá nhân chính thức đi vào cuộc sống (sau giai đoạn chuyển tiếp từ Nghị định số 13/2023/NĐ-CP) tạo ra một hành lang pháp lý tối cao, đồng bộ. Đặc biệt, sự ra đời của Nghị định số 356/2025/NĐ-CP, ngày 31/12/2025 của Chính phủ quy định chi tiết thi hành một số điều của Luật Bảo vệ dữ liệu cá nhân đã tháo gỡ hoàn toàn các nút thắt chông chéo với các luật chuyên ngành (Luật Lưu trữ, Luật Đất đai...). Đây là khung pháp lý vững chắc để các địa phương cụ thể hóa quy chế nội bộ.

Sự hoàn thiện thể chế này xác lập rõ địa vị pháp lý và các quyền năng của chủ thể dữ liệu; phân định minh bạch nghĩa vụ của cơ quan nhà nước cấp tỉnh trong các vai trò: Bên Kiểm soát, Bên Xử lý hoặc Bên Đồng kiểm soát dữ liệu. Các nguyên tắc “xác định mục đích” và “tối thiểu hóa dữ liệu” buộc chính quyền cấp tỉnh phải chuyển dịch từ phương thức thu thập theo thói quen sang thu thập dựa trên mục tiêu, căn cứ pháp lý và mức độ cần thiết; đồng thời kéo hoạt động số hóa thủ tục hành chính vào khuôn khổ quản trị dữ liệu dựa trên quyền và trách nhiệm giải trình.

4.1.1.2. Yếu tố từ sự hoàn thiện và bao phủ tuyệt đối của hạ tầng định danh số (Đề án 06), xác thực điện tử (VNeID) và chuẩn hóa chia sẻ dữ liệu dùng chung

Tính đến đầu năm 2026, Đề án 06 đã hoàn thành mục tiêu số hóa cơ bản với việc phủ sóng tài khoản định danh điện tử VNeID đến hơn 85% công dân trưởng thành tại Việt Nam, tích hợp sâu vào Hệ thống thông tin giải quyết thủ tục hành chính của 34 tỉnh, thành phố [6]. Sự phát triển đồng bộ này giúp chuẩn hóa dữ liệu “gốc”, giảm thiểu việc công dân phải nộp bản giấy hay khai báo lặp đi lặp lại dữ liệu thô tại bộ phận Một cửa.

Về phương diện bảo vệ quyền, cơ chế “truy cập theo ủy quyền” qua Trục liên thông văn bản quốc gia và nền tảng tích hợp, chia sẻ dữ liệu cấp tỉnh (LGSP) giúp hiện thực hóa nguyên tắc tối thiểu hóa dữ liệu. Các nền tảng hiện đại này gắn chặt với việc kiểm soát luồng dữ liệu, quản lý truy cập theo vai trò (RBAC) và tự động ghi vết (Log-generation), tạo điều kiện cho kiểm toán dữ liệu và truy cứu trách nhiệm khi xảy ra vi phạm.

4.1.1.3. Năng lực an toàn thông tin mạng và chuẩn hóa quản trị bảo mật trong cơ quan nhà nước ngày càng được nâng cao

An toàn thông tin tại các địa phương có sự chuyển biến mạnh mẽ từ mô hình “phòng thủ thụ động” sang “bảo vệ chủ động 4 lớp” theo chỉ đạo của Bộ KHCN. Xu hướng tăng đầu tư thể hiện rõ ở việc các tỉnh hoàn thành phê duyệt hồ sơ đề xuất cấp độ an toàn hệ thống thông tin (đạt tỷ lệ trên 90% hệ thống lỗi vào năm 2025) [34].

Đồng thời, sự phát triển của các doanh nghiệp công nghệ số Việt Nam trong việc cung cấp dịch vụ Điện toán đám mây an toàn (Cloud Việt) và các giải pháp mã hóa dữ liệu nội địa với chi phí hợp lý đã giải bài toán áp lực ngân sách tại các tỉnh nghèo. Khi an ninh hạ tầng được nâng chuẩn, các quyền đối với DLCN như: quyền bí mật, quyền toàn vẹn thông tin... được bảo vệ thực chất bằng các công cụ kỹ thuật thay vì chỉ tồn tại trên văn bản cam kết.

4.1.1.4. Phát triển nguồn nhân lực số và năng lực quản trị dữ liệu ở địa phương

Trong bối cảnh xây dựng chính quyền số, các địa phương đang kiện toàn bộ máy theo hướng hình thành các vị trí chuyên trách về an toàn thông tin và bảo vệ DLCN (tương đương mô hình Nhân sự bảo vệ dữ liệu - DPO). Việc đào tạo, tập huấn chứng chỉ an toàn thông tin cho đội ngũ công chức trực tiếp xử lý hồ sơ tại cấp cơ sở giúp giảm thiểu rủi ro lộ lọt dữ liệu do lỗi vô ý (như chia sẻ tài khoản, sử dụng mạng xã hội không mã hóa để truyền file công vụ).

Song song đó, nhận thức của người dân về “chủ quyền dữ liệu” tại Việt Nam tăng mạnh. Áp lực từ dư luận và trải nghiệm của người dân trước các sự cố an ninh mạng buộc chính quyền cấp tỉnh phải chuyển dịch tư duy từ “quản trị mệnh lệnh” sang “phục vụ và bảo vệ”, tăng cường tính minh bạch và phát triển các công dịch vụ công có tính năng cho phép công dân tra cứu, yêu cầu chỉnh sửa, cập nhật dữ liệu cá nhân trực tuyến.

4.1.1.5. Hợp tác công - tư và khả năng tiếp cận công nghệ bảo vệ dữ liệu hiện đại

Xu hướng hợp tác công - tư trong triển khai nền tảng chính quyền số được dự báo tiếp tục gia tăng do nhu cầu rút ngắn thời gian triển khai và tận dụng năng lực công nghệ của doanh nghiệp. Nếu được đặt trong khuôn khổ tiêu chuẩn và hợp đồng rõ ràng, hợp tác công - tư có thể tác động tích cực theo hai chiều: (1) doanh nghiệp có thể đưa vào hệ thống các giải pháp quản trị định danh - truy cập, giám sát an toàn, mã hóa, phòng chống thất thoát dữ liệu và phát hiện bất thường, qua đó nâng chuẩn bảo vệ dữ liệu trên quy mô toàn tỉnh; (2) mô hình hợp tác buộc phải làm rõ trách nhiệm giữa các chủ thể tham gia xử lý dữ liệu, từ đó thúc đẩy nguyên tắc trách nhiệm giải trình và khả năng kiểm toán. Tuy nhiên, tác động tích cực chỉ được bảo đảm khi địa phương thiết lập hàng rào quản trị đủ mạnh như giới hạn mục đích và phạm vi truy cập, điều kiện lưu trữ - chuyển giao dữ liệu, cơ chế kiểm tra tuân thủ và quy trình xử lý sự cố. Khi đó, hợp tác công - tư không chỉ là giải pháp huy động nguồn lực công nghệ, mà còn là phương tiện thể chế hóa chuẩn mực bảo vệ dữ liệu trong toàn bộ chuỗi cung ứng dịch vụ số của địa phương.

4.1.2. Những yếu tố tác động tiêu cực

Trong những năm tới, xây dựng chính quyền số ở cấp tỉnh sẽ tiếp tục tăng tốc, bởi dịch vụ công trực tuyến mở rộng, dữ liệu được số hóa và liên thông sâu hơn, nhiều quyết định quản trị dựa trên phân tích dữ liệu và ứng dụng trí tuệ nhân tạo. Đây là xu hướng chung của thế giới và cũng là yêu cầu nội tại của cải cách hành chính ở nước ta. Tuy nhiên, đi cùng với lợi ích về tiện lợi và hiệu quả là những rủi ro mới đối với QCN trong môi trường số, đặc biệt là quyền đối với DLCN. Khi DLCN trở thành nhiên liệu của hệ thống số, nếu thiếu giới hạn và cơ chế kiểm soát phù hợp, người dân có thể rơi vào tình thế “được phục vụ nhiều hơn nhưng kiểm soát ít hơn” đối với chính thông tin của mình. Dưới đây là các yếu tố tiêu cực được dự báo sẽ tác động rõ rệt đến việc bảo vệ quyền đối với DLCN trong xây dựng chính quyền số cấp tỉnh.

4.1.2.1. Rủi ro gia tăng từ trí tuệ nhân tạo (AI) và phân tích dữ liệu lớn (Big Data) trong quản trị công

Trong thời gian tới, trí tuệ nhân tạo (AI) và phân tích dữ liệu lớn (Big Data) sẽ được ứng dụng ngày càng rộng rãi nhằm hỗ trợ hoạt động điều hành, nâng cao năng lực dự báo nhu cầu, phát hiện bất thường, tự động hóa quy trình và thậm chí tham gia vào một số khâu ra quyết định có tác động trực tiếp đến quyền và lợi ích của người dân. Tuy nhiên, khác với các hệ thống xử lý dữ liệu truyền thống chủ yếu ở chức năng lưu trữ và truy xuất thì AI còn thực hiện suy luận và rút trích tri thức từ dữ liệu. Trên

cơ sở kết hợp các dữ liệu tương như rời rạc, hệ thống có thể hình thành “chân dung số” của cá nhân như thói quen, mức độ rủi ro, xác suất vi phạm, mức độ ưu tiên..., qua đó làm phát sinh những nguy cơ mới đối với quyền đối với DLCN, như phân loại con người hoặc thiết lập xếp hạng mà chủ thể dữ liệu không biết cách thức hình thành.

Sự bùng nổ của tội phạm mạng sử dụng Trí tuệ nhân tạo (AI) và Deepfake (Tội phạm công nghệ cao) sẽ không còn dừng lại ở việc đánh cắp dữ liệu dạng văn bản thô. Sự phát triển của các công cụ AI thế hệ mới cho phép chúng thực hiện các cuộc tấn công dò quét lỗ hổng API tự động, hoặc sử dụng công nghệ Deepfake giọng nói/hình ảnh dựa trên dữ liệu trắc sinh học bị rò rỉ để lừa đảo. Theo báo cáo tổng kết của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05) - Bộ Công an và Cục An toàn thông tin, chỉ tính riêng trong năm 2025, Việt Nam ghi nhận hơn 18.000 cuộc tấn công mạng quy mô lớn nhằm vào các hệ thống thông tin trọng yếu, tăng 28.5% so với giai đoạn trước. Trong đó, các vụ lừa đảo trực tuyến sử dụng công nghệ Deepfake (giọng nói, hình ảnh giả mạo) để chiếm đoạt tài khoản định danh số tăng đột biến, chiếm hơn 65% tổng số vụ việc lừa đảo công nghệ cao trên cả nước [6]. Đây là áp lực kỹ thuật cực lớn vượt quá năng lực phòng thủ hiện tại của nhiều Sở KHCN. Trong trường hợp thiếu các cơ chế kiểm định, giải thích, đánh giá tác động và bảo đảm quyền khiếu nại, chỉnh sửa, quyền đối với DLCN có thể trở nên khó thực thi trên thực tế; chủ thể dữ liệu chịu tác động nhưng không xác định được chủ thể chịu trách nhiệm giải trình cũng như con đường pháp lý để yêu cầu bảo vệ quyền lợi.

4.1.2.2. Thách thức từ mô hình dữ liệu thế hệ mới; liên thông và tái sử dụng dữ liệu vượt mục đích, thiếu minh bạch trong vận hành dịch vụ công trực tuyến

Thách thức từ mô hình dữ liệu thế hệ mới trong Đô thị thông minh (IOC) thời gian tới sẽ tác động mạnh mẽ đến công tác quản trị, do các tỉnh sẽ đẩy mạnh tích hợp dữ liệu từ hệ thống Camera giám sát giao thông, thiết bị cảm biến IoT, dữ liệu định vị... Đây là những loại dữ liệu động, nhạy cảm, có tần suất thu thập theo thời gian thực. Nếu không có quy trình bảo vệ tương ứng, nguy cơ quyền riêng tư di chuyển và hình ảnh đời tư của công dân bị xâm phạm là rất lớn.

Liên thông dữ liệu là một trụ cột của chính quyền số vì giúp người dân không phải khai đi khai lại, hồ sơ được xử lý nhanh hơn, và các cơ quan nhà nước phối hợp hiệu quả hơn. Tuy vậy, liên thông càng sâu thì nguy cơ “trượt mục đích” càng lớn. Dữ liệu ban đầu người dân cung cấp để giải quyết một thủ tục cụ thể có thể dần bị

dùng cho những mục đích khác chỉ vì “đã có sẵn” hoặc “kết nối được thì khai thác”, vượt khỏi mục đích ban đầu.

Ở cấp tỉnh, nơi quản lý nhiều lĩnh vực gắn trực tiếp với đời sống như y tế, giáo dục, an sinh xã hội, đất đai, dân cư, việc tái sử dụng dữ liệu có thể làm mờ ranh giới giữa việc phục vụ người dân và nguy cơ tăng khả năng kiểm soát dựa trên dữ liệu. Một vấn đề khác là nhiều hệ thống dịch vụ công trực tuyến hiện nay chủ yếu tập trung vào việc “xong hồ sơ”, trong khi phần thông báo về dữ liệu cá nhân còn sơ sài. Khi các quyền chỉ được thể hiện dưới dạng chung chung hoặc biểu mẫu khó sử dụng, quyền đối với DLCN dễ bị hình thức hóa, nói cách khác tồn tại về mặt thủ tục nhưng không tạo ra khả năng kiểm soát thực chất cho người dân. Trong bối cảnh liên thông và tái sử dụng dữ liệu ngày càng gia tăng, thiếu minh bạch còn làm suy giảm niềm tin, dẫn đến người dân ngại tương tác với dịch vụ số, ngại cung cấp thông tin, hoặc buộc phải cung cấp trong trạng thái thiếu tin tưởng, không yên tâm.

4.1.2.3. Yếu tố năng lực tổ chức, nguồn nhân lực và rủi ro chuỗi cung ứng trong triển khai, vận hành nền tảng số khi lệ thuộc chủ thể xử lý dữ liệu cá nhân

Ở cấp tỉnh, năng lực tổ chức và chất lượng nhân lực số giữa các địa phương còn chênh lệch; đây có thể trở thành yếu tố làm suy giảm hiệu quả bảo vệ quyền đối với dữ liệu cá nhân trong thời gian tới. Khi không có bộ phận hoặc đầu mối chuyên trách, trách nhiệm giữa các cơ quan không được phân định rõ và quy trình xử lý dữ liệu chưa được chuẩn hóa, việc bảo vệ dữ liệu rất dễ rơi vào tình trạng nhiều người cùng tham gia nhưng không ai chịu trách nhiệm đến cùng. Thực tế, nhiều sự cố xuất phát từ sai sót nghiệp vụ như cấp quyền truy cập quá rộng, gửi nhầm dữ liệu, chia sẻ sai kênh, lưu trữ không đúng chuẩn hoặc chậm, không đáp ứng đúng yêu cầu của chủ thể dữ liệu.

Bên cạnh đó, trong chuyển đổi số cấp tỉnh, một số công đoạn hoặc hạng mục kỹ thuật thường được xã hội hóa, thuê doanh nghiệp công nghệ thực hiện do ngân sách tỉnh có hạn. Điều này giúp triển khai nhanh và tận dụng chuyên môn. Tuy nhiên, các doanh nghiệp công nghệ đứng sau vận hành hệ thống có nguy cơ khai thác trái phép dữ liệu công dân (hành vi tiêu dùng, sở hữu tài sản, lịch sử y tế...) để tối ưu hóa thuật toán kinh doanh hoặc bán cho bên thứ ba, tạo ra các luồng dữ liệu ngầm rất khó kiểm soát. Điều này tạo ra sự phụ thuộc rất lớn nếu thiếu cơ chế quản trị hợp đồng chặt chẽ, quyền đối với dữ liệu cá nhân của người dân có nguy cơ bị ảnh hưởng. Khi xảy ra sự cố, nếu thiếu các điều khoản ràng buộc và cơ

chế phối hợp, quá trình xác định chủ thể phải giải trình, chịu trách nhiệm và thực hiện khắc phục có thể kéo dài, làm giảm hiệu lực bảo vệ quyền trên thực tế.

4.1.2.4. Sự gia tăng khoảng cách về năng lực bảo mật, tấn công mạng, lộ lọt dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh

Sự gia tăng khoảng cách về năng lực bảo mật giữa các địa phương do chênh lệch về nguồn thu ngân sách và thu hút nhân lực số sẽ làm sâu sắc thêm sự chênh lệch giữa các tỉnh, thành phố lớn (như Hà Nội, TP.HCM, Quảng Ninh...) và các tỉnh miền núi, vùng sâu vùng xa. Các tỉnh nghèo còn hạn chế về kỹ năng số sẽ trở thành mục tiêu ưu tiên của các cuộc tấn công mạng đây chuyên vào hệ thống liên thông quốc gia.

Khi chính quyền số phát triển mạnh hơn, hệ thống có nhiều dịch vụ và nhiều kênh kết nối hơn thì nguy cơ bị tấn công mạng cũng tăng lên, trong khi dữ liệu của khu vực công ngày càng nhiều và có giá trị, nên dễ trở thành mục tiêu của tội phạm mạng. Ngoài tấn công từ bên ngoài, còn có rủi ro từ bên trong như cấp quyền truy cập quá rộng, dùng quyền truy cập sai mục đích, hoặc khó phát hiện bất thường nếu cơ chế ghi nhật ký, lưu vết chưa tốt. Khi sự cố xảy ra, thiệt hại không chỉ là tiền và thời gian để sửa hệ thống, mà còn ảnh hưởng trực tiếp đến người dân: mất kiểm soát dữ liệu cá nhân, tăng nguy cơ bị lừa đảo, mạo danh, bị xâm phạm danh dự và quyền riêng tư.

Quyền của chủ thể dữ liệu có thể bị suy giảm hiệu lực do các rào cản về thủ tục và tổ chức, như thủ tục phức tạp, kênh tiếp nhận không rõ ràng, thời hạn phản hồi kéo dài, hoặc cơ chế khiếu nại và khắc phục thiếu tính độc lập và thiếu hiệu quả. Trong những điều kiện đó, quyền đối với DLCN không phát huy được vai trò như một công cụ kiểm soát quyền lực thông tin, mà chủ yếu tồn tại ở dạng tuyên bố mang tính chuẩn tắc. Đối với chính quyền số, nơi dữ liệu được xử lý với tốc độ cao, quy mô lớn và mức độ liên thông sâu, nếu khoảng cách giữa quyền được ghi nhận và quyền được thực thi kéo dài, hệ quả tất yếu là suy giảm niềm tin số và làm giảm mức độ sẵn sàng của người dân trong việc sử dụng dịch vụ công trực tuyến.

4.2. QUAN ĐIỂM BẢO VỆ QUYỀN ĐỐI VỚI DỮ LIỆU CÁ NHÂN TRONG XÂY DỰNG CHÍNH QUYỀN SỐ CẤP TỈNH Ở VIỆT NAM

4.2.1. Bảo vệ quyền đối với dữ liệu cá nhân phải là nguyên tắc cốt lõi trong bảo đảm quyền con người, quyền công dân trong môi trường số

Dữ liệu cá nhân là những nhận thức, ký ức, cảm xúc, niềm tin và sự tự ý thức của một cá nhân về bản thân mình. Bảo vệ DLCN thực chất là bảo vệ nhân phẩm, sự riêng tư, tự do và sự phát triển toàn diện của con người trước nguy cơ bị kiểm soát, thao túng hành vi, là những giá trị đã được Hiến pháp bảo vệ (Điều 21 Hiến pháp 2013 [43], các điều ước quốc tế về quyền con người (như Điều 17 ICCPR) [109], Luật Bảo vệ dữ liệu cá nhân và các quy định pháp luật có liên quan). Bảo vệ DLCN trong xây dựng Chính quyền số không thuần túy là giải pháp kỹ thuật, mà là nhiệm vụ quản trị công nhằm thực thi Hiến pháp và pháp luật về quyền con người. Mọi chính sách và ứng dụng công nghệ cấp tỉnh phải lấy con người làm trung tâm; chuyển đổi triệt để từ tư duy quản lý dữ liệu để phục vụ công vụ sang tư duy quản trị dữ liệu để bảo vệ quyền lợi hợp pháp của công dân. Quan điểm này định hướng trực tiếp cho nhóm Giải pháp hoàn thiện thể chế, quy chế nội bộ và Giải pháp nâng cao nhận thức, trách nhiệm của bộ máy hành chính cấp tỉnh.

4.2.2. Bảo vệ quyền đối với dữ liệu cá nhân là điều kiện tiên quyết để tạo dựng “niềm tin số” và bảo đảm sự phát triển bền vững của Chính quyền số

“Niềm tin số” của Nhân dân là nền tảng quyết định sự thành bại của Chính quyền số. Bảo vệ DLCN không phải là lực cản hay chi phí phát sinh của sự phát triển, mà là nền tảng tâm lý và pháp lý vững chắc. Chỉ khi công dân yên tâm rằng thông tin nhân thân của mình không bị lạm dụng, theo dõi hay rò rỉ, họ mới chủ động chuyển sang tương tác trên môi trường số và trở thành chủ thể cùng tham gia tạo lập dữ liệu cùng chính quyền địa phương. Quan điểm này là cơ sở để đề ra những giải pháp bảo vệ quyền thực chất của chủ thể dữ liệu và giải pháp về truyền thông, giáo dục kỹ năng tự bảo vệ dữ liệu cho Nhân dân.

4.2.3. Khai thác dữ liệu để phát triển kinh tế - xã hội phải bảo đảm sự cân bằng hợp lý với nghĩa vụ bảo vệ quyền riêng tư của công dân

Quyền đối với DLCN không phải là một quyền tuyệt đối mà có thể bị giới hạn theo luật định vì lợi ích công cộng và an ninh quốc gia (theo Khoản 2 Điều 14 Hiến pháp 2013) [43]. Khai thác dữ liệu phục vụ quản trị và phát triển kinh tế số phải luôn song hành với các biện pháp bảo vệ quyền tương xứng. Chính quyền cấp tỉnh tuyệt đối không đánh đổi quyền riêng tư của người dân lấy tốc độ tăng trưởng số thuần túy, mà phải hướng tới tối ưu hóa “lợi ích kép”: phát triển kinh tế - xã hội đi đôi với bảo đảm an toàn dữ liệu cá nhân. Nội dung này cần được nghiên cứu kỹ nhằm đề xuất

giải pháp kiểm soát việc luân chuyển dữ liệu, quản trị hợp tác công - tư và xây dựng quy chế chia sẻ, phân tán hay ẩn danh dữ liệu.

4.2.4. Bảo vệ quyền đối với dữ liệu cá nhân phải chuyển dịch mạnh mẽ sang tư duy “tiếp cận rủi ro” và lấy “phòng ngừa chủ động” làm chính

Sự cố xâm phạm DLCN trong môi trường số thường diễn ra nhanh, diện rộng và để lại hậu quả rất khó khắc phục. Việc xử phạt hay bồi thường sau khi rò rỉ dữ liệu chỉ là giải pháp giải quyết hậu quả. Bảo vệ DLCN phải đi trước một bước, chủ động nhận diện, đánh giá và triệt tiêu các rủi ro tiềm ẩn đối với quyền con người ngay từ khâu thiết kế hệ thống (Privacy by Design) và trong suốt vòng đời xử lý dữ liệu. Điều này đòi hỏi phải có những giải pháp kỹ thuật - công nghệ bắt buộc trong đánh giá DPIA, tích hợp nhật ký kiểm tra, giám sát và quản trị an toàn thông tin theo cấp độ.

4.2.5. Thấm quyền quản trị dữ liệu của cơ quan nhà nước phải gắn liền với trách nhiệm giải trình và nghĩa vụ công khai, minh bạch

Trong mối quan hệ hành chính số, tồn tại sự bất đối xứng tự nhiên về thông tin và vị thế giữa công dân và cơ quan nhà nước. Với vai trò vừa là Bên kiểm soát vừa là Bên xử lý dữ liệu quy mô lớn, chính quyền cấp tỉnh phải chuyển nghĩa vụ tuân thủ pháp luật từ “cam kết bị động” sang “chứng minh chủ động” với những bằng chứng kỹ thuật và pháp lý cụ thể. Mọi hành vi xử lý dữ liệu vượt quá mục đích hoặc gây rò rỉ dữ liệu phải được làm rõ trách nhiệm công vụ và chịu sự giám sát công khai. Cần có giải pháp hoàn thiện và đổi mới công tác thanh tra, kiểm tra, quy trách nhiệm người đứng đầu và cơ chế bồi thường thiệt hại theo quy định.

4.2.6. Bảo vệ quyền đối với dữ liệu cá nhân phải bảo đảm tính thống nhất thể chế toàn quốc, nhưng linh hoạt và phù hợp với đặc thù phát triển địa phương

Tiêu chuẩn bảo vệ quyền DLCN do cấp Trung ương quy định là thống nhất và tối thượng, các quy chế nội bộ của cấp tỉnh không được phép trái hoặc hạ thấp các chuẩn mực này. Tuy nhiên, quá trình thực thi phải có lộ trình phân kỳ hợp lý, linh hoạt tương ứng với trình độ hạ tầng, tiềm lực ngân sách và mức độ sẵn sàng số của từng địa phương; trong đó đặc biệt ưu tiên bảo vệ chủ động cho các nhóm đối tượng yếu thế (vùng sâu, vùng xa, đồng bào dân tộc thiểu số) nhằm thu hẹp “khoảng cách số”. Cần có giải pháp phân kỳ lộ trình thực thi và cơ chế hỗ trợ đặc thù cho các địa phương và nhóm yếu thế.

4.2.7. Xây dựng hệ thống bảo vệ quyền dữ liệu cấp tỉnh phải chủ động tiếp cận và nội hóa các chuẩn mực quốc tế tiên tiến

Dữ liệu và không gian mạng không có địa giới hành chính. Trong bối cảnh hội nhập quốc tế và thu hút đầu tư chất lượng cao đối với các dự án nước ngoài (FDI), chính quyền cấp tỉnh phải chủ động tham chiếu, tích hợp các nguyên tắc quản trị dữ liệu tiên tiến trên thế giới (như GDPR) vào thực tiễn địa phương. Việc nâng chuẩn bảo vệ DLCN tiệm cận quốc tế vừa giúp bảo vệ tối đa cho công dân, vừa nâng cao uy tín và tạo môi trường pháp lý an toàn để thu hút các tập đoàn công nghệ toàn cầu. Điều này đòi hỏi phải có chiến lược trong chuẩn hóa hạ tầng kỹ thuật theo tiêu chuẩn quốc tế và đào tạo nguồn nhân lực quản trị dữ liệu chất lượng cao nhằm đáp ứng yêu cầu hội nhập trong giai đoạn mới.

4.3. GIẢI PHÁP VỀ BẢO VỆ QUYỀN ĐỐI VỚI DỮ LIỆU CÁ NHÂN TRONG XÂY DỰNG CHÍNH QUYỀN SỐ CẤP TỈNH Ở VIỆT NAM

4.3.1. Nhóm giải pháp hoàn thiện thể chế pháp luật và quy chế nội bộ cấp tỉnh trong bảo vệ quyền đối với dữ liệu cá nhân

Để khắc phục triệt để những khoảng trống pháp lý, sự chồng chéo và lúng túng trong thực thi tại địa phương, nhóm giải pháp về thể chế cần được triển khai đồng thời ở cả hai phương diện: Kiến nghị về công tác lập pháp, lập quy ở cấp trung ương và cụ thể hóa quy chế quản trị nội bộ ở địa phương. Cụ thể bao gồm 3 nội dung trọng tâm sau:

(1). Tham mưu, kiến nghị Trung ương ban hành các thông tư hướng dẫn tháo gỡ các điểm chồng chéo, bất cập giữa Luật Bảo vệ DLCN và các luật chuyên ngành (Luật Lưu trữ, Luật Đất đai...)

Trong bối cảnh hiện nay, việc khoa học, công nghệ, chuyển đổi số phát triển quá nhanh, trong khi đó, các văn bản luật chưa theo kịp với sự phát triển và chưa bảo đảm sự phù hợp, tương thích giữa các văn bản quy phạm pháp luật chuyên ngành khác nhau, dẫn đến xung đột về pháp lý. Chính vì thế, đội ngũ công chức cấp tỉnh đang đối mặt với những rào cản pháp lý chồng chéo. Điển hình như xung đột Luật Bảo vệ DLCN với Luật Lưu trữ: Luật Bảo vệ DLCN đề cao “quyền được quên”, quyền xóa dữ liệu hoặc giới hạn thời gian lưu trữ của công dân khi mục đích thu thập đã đạt được. Ngược lại, Luật Lưu trữ lại ràng buộc trách nhiệm lưu trữ vĩnh viễn hoặc có thời hạn rất dài đối với hồ sơ hành chính, bao gồm cả DLCN nhạy cảm. Hay như xung đột với Luật Đất đai: Việc công khai thông tin quy hoạch, chủ sở hữu quyền sử dụng đất để bảo đảm tính minh bạch, phòng chống tham nhũng theo Luật Đất đai vô hình trung lại làm lộ lọt thông tin tài sản, cư trú (DLCN nhạy cảm) của cá nhân trên

các cổng thông tin của Sở Tài nguyên và Môi trường mà chưa có cơ chế kiểm soát quyền truy cập trực tiếp...

Từ đó, giải pháp cốt lõi đó là: UBND tỉnh cần giao Sở Tư pháp chủ trì, phối hợp với Sở KHCN tổng hợp các vướng mắc trên thực tiễn, lập báo cáo tham mưu để UBND tỉnh kiến nghị Chính phủ, Bộ Công an, Bộ Nội vụ và Bộ Tài nguyên và Môi trường ban hành các thông tư liên tịch hướng dẫn cơ chế phối hợp quy định rõ: Về nguyên tắc ưu tiên áp dụng pháp luật, xác định rõ ranh giới khi nào hành vi xử lý dữ liệu phục vụ lợi ích công cộng (lưu trữ lịch sử, quản lý đất đai) được miễn trừ nghĩa vụ xin phép chủ thể dữ liệu, và khi nào bắt buộc phải áp dụng các biện pháp mã hóa, ẩn danh hóa dữ liệu trước khi công khai hoặc lưu trữ. Cần có cơ chế phân chia dữ liệu, hướng dẫn kỹ thuật bóc tách phần “thông tin định danh cá nhân” ra khỏi “thông tin tài sản/hồ sơ lưu trữ” để vừa bảo đảm mục đích quản lý, vừa không xâm phạm quyền riêng tư của công dân.

(2). Ban hành Quy trình tác nghiệp hành chính nội bộ về bảo vệ dữ liệu cá nhân áp dụng bắt buộc đối với đội ngũ cán bộ, công chức, viên chức cấp tỉnh đến cấp xã

UBND tỉnh ban hành Quyết định hành chính cá biệt kèm theo “Quy chế hay Sổ tay hướng dẫn Quy trình tác nghiệp chuẩn về bảo vệ DLCN trong hoạt động công vụ”. Văn bản này mang tính chất chỉ đạo, điều hành quản trị nội bộ của người đứng đầu cơ quan hành chính nhà nước cấp tỉnh, hoàn toàn không tạo ra quy phạm pháp luật mới đối với công dân. Phạm vi áp dụng bắt buộc đối với toàn bộ cán bộ, công chức, viên chức, người lao động tại các sở, ban, ngành, Bộ phận Một cửa các cấp và UBND cấp xã, phường trên địa bàn tỉnh. Quy trình này không thay thế Luật mà đóng vai trò là công cụ cụ thể hóa các nguyên tắc của Luật Bảo vệ DLCN và Luật Căn cước thành các thao tác nghiệp vụ hành chính hàng ngày, giúp khắc phục tình trạng “thờ ơ” hoặc “né tránh” của công chức cơ sở. Tại khâu tiếp nhận hồ sơ TTHC (Một cửa), bắt buộc sử dụng mẫu biểu điện tử tích hợp tính năng “Thông báo và yêu cầu xác nhận sự đồng ý” theo đúng Nghị định 13 và Luật Bảo vệ DLCN. Công chức có nghĩa vụ giải thích rõ mục đích, phạm vi, thời hạn lưu trữ dữ liệu trước khi công dân xác nhận. Tại khâu xử lý và lưu trữ dữ liệu nội bộ, quy định rõ thẩm quyền phân quyền truy cập; nghiêm cấm công chức chia sẻ file chứa DLCN của người dân qua các ứng dụng OTT cá nhân (Zalo, Telegram...) khi chưa qua hệ thống mã hóa công vụ. Đưa tiêu chí tuân thủ bảo vệ DLCN vào Quy chế đánh giá chỉ số cải cách hành chính (PAR INDEX) và KPI hằng năm của các cơ quan, đơn vị; xử lý trách nhiệm kỷ luật công vụ đối với người đứng đầu nếu để xảy ra vi phạm thuộc phạm vi quản lý.

(3). Ban hành Quy chế quản lý, vận hành nội bộ hệ thống Giám sát đô thị thông minh (IOC) và cơ chế báo cáo Đề án thí điểm trình cấp có thẩm quyền

Chủ tịch UBND tỉnh ban hành Quy chế vận hành nội bộ và an toàn thông tin Hệ thống IOC áp dụng cho các cơ quan chuyên môn, cán bộ được giao quản lý, vận hành và khai thác hệ thống và cán bộ công chức được cấp quyền truy cập dữ liệu camera AI thuộc quản lý của tỉnh. Quy chế nội bộ của tỉnh không tự quy định thẩm quyền điều tra hay thẩm quyền xử phạt (do Bộ luật Tố tụng hình sự và Luật Xử lý vi phạm hành chính điều chỉnh), mà chỉ quy định quy trình quản trị kỹ thuật và bảo vệ dữ liệu nội bộ đối với hình ảnh do hệ thống của tỉnh thu thập được. Quy định dữ liệu từ IOC chỉ phục vụ 02 mục đích công vụ hợp pháp: Giám sát, điều tiết giao thông, đô thị (thẩm quyền hành chính của tỉnh) và cung cấp dữ liệu làm chứng cứ khi có văn bản yêu cầu chính thức từ Cơ quan tiến hành tố tụng theo đúng Bộ luật Tố tụng hình sự. Nghiêm cấm dùng dữ liệu IOC để chấm điểm công dân, phân loại xã hội hoặc thương mại hóa. Cần áp dụng giải pháp kỹ thuật bảo vệ tự động như: Cài đặt thuật toán tự động làm mờ khuôn mặt, biển số xe của chủ thẻ không liên quan sau 72 giờ; giới hạn thời gian lưu trữ dữ liệu thô tối đa 30 ngày (trừ trường hợp phục vụ vụ án đang điều tra) [48].

UBND tỉnh thành lập Hội đồng giám sát vận hành IOC địa phương (gồm đại diện UBND, Sở KH-CN, Sở Tư pháp) để kiểm tra định kỳ nhật ký hệ thống (Audit Log), phát hiện và xử lý kỷ luật cán bộ tự ý trích xuất camera giám sát cá nhân vì mục đích riêng.

Đối với các cơ chế khai thác dữ liệu trắc sinh học thể hệ mới theo thời gian thực (Real-time Biometrics) liên quan đến giới hạn quyền con người mà pháp luật hiện hành chưa có quy định hoặc vượt quá thẩm quyền ban hành của cấp tỉnh: UBND tỉnh không tự ban hành Quy chế, mà có trách nhiệm xây dựng Đề án thí điểm trình Chính phủ xem xét ban hành Nghị quyết cho phép áp dụng cơ chế thử nghiệm có kiểm soát (theo quy định của Luật Ban hành văn bản QPPL).

4.3.2. Nhóm giải pháp nâng cao năng lực tổ chức bộ máy, quản trị nhân sự thực thi pháp luật trong bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh

Để bảo đảm quyền đối với DLCN không bị xâm phạm trong tiến trình xây dựng chính quyền số, việc thay đổi từ mô hình nhân sự, quản trị kiêm nhiệm, thiếu chặt chẽ như hiện tại sang mô hình cán bộ chuyên trách là một đòi hỏi cấp bách. Tổ chức bộ máy và nhân sự thực thi phải được tiếp cận theo hướng nâng cao tính độc lập chuyên môn và tính chuyên nghiệp kỹ thuật. Nội dung nhóm giải pháp này bao gồm hai trọng tâm sau:

(1). *Mô hình tổ chức Bộ phận chuyên trách Bảo vệ dữ liệu và cơ chế DPO cấp tỉnh; bảo đảm tính độc lập chuyên môn trong khuôn khổ chế độ thủ trưởng*

(i). *Mô hình tổ chức và vị trí pháp lý:*

Về mặt tổ chức: Không thành lập thêm cơ quan hành chính mới (để tránh làm tăng biên chế), UBND tỉnh quyết định kiện toàn, giao bổ sung nhiệm vụ chuyên trách cho Phòng Công nghệ thông tin hoặc Trung tâm Chuyển đổi số trực thuộc Sở Khoa học và Công nghệ. Bộ phận này đóng vai trò là Cơ quan tham mưu, thẩm định độc lập về an toàn dữ liệu cá nhân của UBND tỉnh.

Về nhân sự DPO: Giám đốc Sở quyết định phân công, bổ nhiệm 01 công chức, viên chức chuyên trách giữ vai trò cán bộ phụ trách bảo vệ dữ liệu (DPO). DPO đòi hỏi phải đáp ứng tiêu chuẩn kép: Am hiểu kỹ thuật an toàn thông tin và nắm vững pháp luật về quyền con người, bảo vệ quyền dữ liệu.

(ii). *Mối quan hệ công vụ và cơ chế giải quyết xung đột (Giải trình vị trí “Độc lập chuyên môn” và “Quyền báo cáo”):*

Để bảo đảm tính khả thi và không vi phạm nguyên tắc quản lý hành chính, mối quan hệ giữa DPO với các chủ thể trong bộ máy được xác định rõ:

Với Thủ trưởng cơ quan trực tiếp (Giám đốc Sở, lãnh đạo đơn vị xử lý dữ liệu): DPO vận hành theo nguyên tắc tham mưu độc lập - Quyết định thuộc về Thủ trưởng. DPO có trách nhiệm lập Báo cáo đánh giá tác động bảo vệ dữ liệu (DPIA) cho các dự án số hóa. Nếu phát hiện rủi ro xâm phạm quyền dữ liệu, DPO có quyền kiến nghị bằng văn bản về giải pháp khắc phục. Thủ trưởng cơ quan giữ quyền quyết định cuối cùng và chịu trách nhiệm pháp lý toàn diện trước Chủ tịch UBND tỉnh và trước pháp luật.

Cơ chế ý kiến bảo lưu (thay cho “báo cáo vượt cấp” cơ học): Trường hợp Thủ trưởng cơ quan vẫn quyết định triển khai quy trình số hóa bất chấp cảnh báo bằng văn bản của DPO, DPO có quyền ghi nhận ý kiến bảo lưu chính thức trong hồ sơ thẩm định DPIA. Báo cáo có ý kiến bảo lưu này bắt buộc phải được gửi đồng thời cho 03 đầu mối để theo dõi rủi ro: Chủ tịch UBND tỉnh (Chỉ đạo thanh tra khi cần thiết); Thanh tra tỉnh (Lưu hồ sơ phục vụ công tác thanh tra công vụ định kỳ, đột xuất); Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (PA05) - Công an tỉnh (Ghi nhận điểm yếu kỹ thuật để giám sát an ninh dữ liệu). Cơ chế này không làm suy giảm quyền quyết định của Thủ trưởng cơ quan, mà tạo ra trách nhiệm giải trình bắt buộc. Khi có sự cố rò rỉ dữ liệu xảy ra, văn bản bảo lưu của DPO là căn cứ pháp lý để cá thể hóa trách nhiệm người đứng đầu, tránh tình trạng đùn đẩy trách nhiệm cho cán bộ kỹ thuật.

Với Cơ quan Thanh tra tỉnh và Đơn vị An toàn thông tin (Phòng PA05- CA tỉnh): DPO không phải là cơ quan điều tra hay thanh tra, mà là đầu mối phối hợp chuyên môn. DPO cung cấp hồ sơ đánh giá rủi ro và nhật ký hệ thống (Audit Log) cho Thanh tra tỉnh và PA05 khi các cơ quan này thực hiện nhiệm vụ kiểm tra, giám sát tuân thủ theo thẩm quyền luật định.

(2). Đánh giá nguồn nhân lực, chi phí vận hành và khả năng áp dụng phân kỳ giữa các địa phương

Một giải pháp quản trị chỉ có giá trị khi giải được bài toán nguồn lực (nhân sự và ngân sách) và tính khả thi thực tiễn. Luận án phân tích rõ khả năng áp dụng theo đặc thù địa phương như sau:

(i). Bài toán nguồn nhân lực và công tác đào tạo

Giải pháp ngắn hạn: Không chờ tuyển dụng mới, tiến hành rà soát và chuyển đổi đội ngũ công chức hiện có. Bố trí công chức Pháp chế hoặc công chức CNTT tham gia các khóa đào tạo ngắn hạn cấp chứng chỉ DPO/DPIA do Bộ Khoa học và Công nghệ, Bộ Công an hoặc các Trung tâm đào tạo uy tín phối hợp tổ chức.

Giải pháp dài hạn (Thu hút nhân tài): Áp dụng Nghị định 179/2025/NĐ-CP của Chính phủ về chính sách đãi ngộ đặc thù đối với lực lượng an toàn, an ninh mạng [21]. HĐND tỉnh ban hành Nghị quyết trích nguồn kinh phí Chuyển đổi số địa phương để chi phụ cấp ưu đãi nghề, thu nhập tăng thêm (gấp 2 - 3 lần mức lương cơ sở) cho nhân sự DPO có chứng chỉ chuyên môn quốc tế (CIPP/E, CISM, CISSP...).

(ii). Bài toán chi phí và nguồn kinh phí vận hành:

Tối ưu hóa ngân sách hiện có: Chi phí cho DPO và công tác đánh giá tác động dữ liệu (DPIA) không sử dụng nguồn chi thường xuyên mới, mà được tính trực tiếp vào chi phí quản lý dự án, thẩm định an toàn thông tin (quy định tối thiểu 10% ngân sách CNTT theo Chỉ thị 14/CT-TTg) của từng dự án số hóa, đầu tư hạ tầng dịch vụ công cấp tỉnh.

Cơ chế thuê ngoài tư vấn độc lập: Đối với các dự án đô thị thông minh (IOC) hoặc CSDL nhạy cảm phức tạp, cho phép áp dụng cơ chế đấu thầu mua dịch vụ kiểm toán an toàn dữ liệu độc lập từ các doanh nghiệp, viện nghiên cứu chuyên ngành. Điều này giúp tỉnh giảm chi phí duy trì bộ máy thường xuyên nhưng vẫn có được báo cáo phản biện kỹ thuật khách quan.

(iii). Khả năng áp dụng đồng đều và lộ trình phân kỳ giữa các địa phương

Do sự chênh lệch lớn về tiềm lực kinh tế và trình độ hạ tầng giữa các tỉnh, thành, giải pháp không áp dụng cào bằng mà được thiết kế theo lộ trình phân kỳ:

Nhóm 1: Các đô thị lớn và tỉnh có chỉ số DTI, ngân sách cao (Hà Nội, TP.HCM, Đà Nẵng, Quảng Ninh...): Thực hiện ngay việc kiện toàn Bộ phận DPO

chuyên trách; ban hành ngay Nghị quyết HĐND về thu nhập đặc thù; bắt buộc 100% dự án CNTT phải có báo cáo thẩm định DPIA độc lập của DPO trước khi phê duyệt.

Nhóm 2: Các tỉnh miền núi, vùng khó khăn, ngân sách hạn chế (vùng Tây Bắc, Tây Nguyên...): Thực hiện mô hình phân kỳ linh hoạt; trong giai đoạn đầu, áp dụng Mô hình DPO kiêm nhiệm (giao Phòng CNTT thuộc Sở KH-CN phụ trách) kết hợp sử dụng nền tảng kỹ thuật dùng chung và các biểu mẫu đánh giá tác động (DPIA) đã chuẩn hóa từ Trung ương để giảm tải chi phí chuyên môn.

Hỗ trợ kỹ thuật tập trung; tận dụng tối đa hạ tầng Trung tâm dữ liệu quốc gia và lực lượng an ninh mạng của Bộ Công an, Bộ Quốc phòng hỗ trợ rà quét, giám sát rủi ro kỹ thuật, giúp địa phương khắc phục tình trạng thiếu hụt chuyên gia tại chỗ.

Tóm lại, nhân sự số và bộ máy chuyên trách CNTT có tính độc lập tương đối, có chuyên môn kỹ thuật sẽ có vai trò rất quan trọng, giúp hiện thực hóa nghĩa vụ tôn trọng, bảo vệ và thúc đẩy quyền con người của Nhà nước trong không gian số.

4.3.3. Nhóm giải pháp về thể chế hóa nghĩa vụ năng lực kỹ thuật và trách nhiệm pháp lý trong bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh

Trong quản trị hành chính công hiện đại, kỹ thuật an toàn thông tin không thuần túy là công cụ vận hành, mà là hình thái thể hiện của nghĩa vụ pháp lý nhà nước. Việc áp dụng các giải pháp kỹ thuật bắt buộc chính là cơ chế kiểm soát và giới hạn việc sử dụng quyền lực công trong không gian số. Để bảo đảm tính bền vững pháp lý (không phụ thuộc vào sự thay đổi nhanh chóng của các công nghệ cụ thể), các yêu cầu kỹ thuật được chuyển hóa thành 04 nguyên tắc và trách nhiệm pháp lý bắt buộc sau đây:

(1). Quy định bắt buộc về thẩm định rủi ro, kiểm toán an ninh định kỳ và cá thể hóa trách nhiệm phê duyệt hệ thống

Về nguyên tắc pháp lý: Sự an toàn của Kho dữ liệu dùng chung (LGSP) là điều kiện tiên quyết để bảo đảm quyền riêng tư và bí mật đời tư của công dân. Nhà nước có nghĩa vụ thiết lập mức bảo vệ an toàn tối thiểu tương ứng với quy mô dữ liệu quản lý.

Về trách nhiệm pháp lý: Chủ tịch UBND tỉnh ban hành Quyết định phê duyệt Hồ sơ cấp độ an toàn hệ thống thông tin (tối thiểu Cấp độ 3 đối với Kho dữ liệu LGSP) trước khi đưa vào vận hành chính thức. Người đứng đầu cơ quan phê duyệt chịu trách nhiệm pháp lý hành chính, hình sự nếu phê duyệt hệ thống chưa đạt chuẩn an toàn gây hậu quả rò rỉ dữ liệu diện rộng.

Về nghĩa vụ kiểm toán độc lập: Bắt buộc các hệ thống thông tin công phải trải qua kiểm toán an ninh mạng định kỳ (tối thiểu 01 lần/năm) bởi tổ chức kiểm toán độc

lập do cơ quan chuyên trách bảo vệ DLCN quốc gia cấp phép. Báo cáo kiểm toán là căn cứ pháp lý để nghiệm thu hoặc dừng vận hành hệ thống.

(2). Thể chế hóa nghĩa vụ minh bạch sự cố và quyền được thông báo tức thì của công dân

Về nguyên tắc pháp lý: Công dân có quyền được biết về các rủi ro xảy ra đối với dữ liệu cá nhân của mình để chủ động thực hiện các biện pháp tự vệ (khóa tài khoản, thay đổi thông tin xác thực).

Về trách nhiệm pháp lý và nghĩa vụ cảnh báo bắt buộc: Pháp luật hành chính quy định nghĩa vụ của cơ quan vận hành hệ thống phải tự động phát thông báo vi phạm, rò rỉ dữ liệu đến công dân qua Cổng Dịch vụ công hoặc ứng dụng định danh quốc gia (VNeID) ngay khi phát hiện sự cố (trong thời hạn luật định theo Nghị định 13/2023/NĐ-CP và Luật Bảo vệ DLCN).

Về chế tài pháp lý: Nghiêm cấm và xử lý kỷ luật, hình sự đối với hành vi che giấu sự cố an ninh mạng của người quản trị hệ thống nhằm né tránh trách nhiệm công vụ.

(3). Chuẩn hóa nghĩa vụ giải trình và cơ chế ghi vết không thể sửa xóa (Audit Trail) phục vụ bồi thường thiệt hại

Về nguyên tắc pháp lý: Mọi hành vi truy cập, khai thác dữ liệu của công chức đều là hoạt động thi hành công vụ, phải chịu sự giám sát pháp lý và không được phép ẩn danh.

Về trách nhiệm pháp lý, nghĩa vụ lưu vết pháp lý: Quy định bắt buộc hệ thống thông tin chính quyền số phải tự động ghi nhận nhật ký thao tác (Ai, truy cập dữ liệu nào, thời gian nào, theo căn cứ hồ sơ hành chính nào) trên công nghệ lưu trữ bất biến (chỉ ghi, không thể sửa, xóa).

Giá trị chứng cứ khi khiếu nại, khởi kiện: Nhật ký hệ thống (Audit Log) là chứng cứ pháp lý khách quan để công dân sử dụng khi thực hiện Quyền yêu cầu bồi thường thiệt hại theo Luật Trách nhiệm bồi thường của Nhà nước. Nếu hệ thống không cung cấp được nhật ký trích xuất, cơ quan nhà nước bị suy đoán là có lỗi công vụ.

(4). Luật hóa Giao diện tương tác quyền công dân - Biến quyền lý luận thành công cụ kỹ thuật

Về nguyên tắc pháp lý: Quyền tự quyết về thông tin chỉ thực sự có hiệu lực khi công dân được trang bị phương tiện kỹ thuật để chủ động kiểm soát dữ liệu của chính mình trong mối quan hệ với chính quyền.

Về trách nhiệm pháp lý, nghĩa vụ tích hợp giao diện: Bắt buộc tất cả các phần mềm hành chính công cấp tỉnh phải tích hợp Bảng điều khiển quyền dữ liệu (User

Power Dashboard). Bảng này cho phép công dân: (i) Tra cứu lịch sử các cơ quan công quyền đã truy cập dữ liệu của mình; (ii) Thực hiện các thao tác kỹ thuật để rút lại sự đồng ý, yêu cầu chỉnh sửa hoặc đóng, xóa dữ liệu khi không còn cần cứ pháp lý.

Về nghĩa vụ phản hồi tự động: Hệ thống hành chính phải có cơ chế tiếp nhận và xử lý tự động các yêu cầu thực thi quyền của công dân, chấn chỉnh tình trạng cơ quan nhà nước tự ý lưu giữ và khai thác dữ liệu vô thời hạn.

Tóm lại, các giải pháp về thể chế hóa nghĩa vụ năng lực kỹ thuật và trách nhiệm pháp lý trong bảo vệ quyền đối với dữ liệu cá nhân đóng vai trò thể chế hóa các cam kết pháp lý về quyền con người, biến quy định pháp luật thành các giới hạn kỹ thuật bất khả xâm phạm trên không gian số.

4.3.4. Nhóm giải pháp về thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo và phân định hệ thống trách nhiệm pháp lý trong bảo vệ quyền đối với dữ liệu cá nhân

Cơ chế hậu kiểm và hệ thống chế tài xử lý vi phạm là mắt xích quyết định tính hiệu lực thực tế của pháp luật bảo vệ dữ liệu cá nhân. Để bảo đảm tính nghiêm minh nhưng không tạo ra tâm lý sợ sai cho bộ máy hành chính, hệ thống kiểm soát và xử lý vi phạm cấp tỉnh cần được phân định rành mạch thành 02 trụ cột: Cơ chế kiểm tra - giám sát liên ngành và Hệ thống 5 tầng trách nhiệm pháp lý độc lập.

(1). Thiết lập cơ chế kiểm tra liên ngành độc lập, định kỳ và đột xuất

UBND tỉnh ban hành Quy chế phối hợp liên ngành thường trực giữa Cơ quan chuyên trách bảo vệ dữ liệu, CNTT (Sở Khoa học và Công nghệ) và Cơ quan bảo vệ pháp luật (Phòng PA05 - Công an tỉnh):

Thanh tra, kiểm tra định kỳ (tối thiểu 02 lần/năm): Rà soát toàn bộ việc phân quyền, cấp phát, thu hồi tài khoản công vụ tại Bộ phận Một cửa và các hệ thống chuyên ngành; kiểm tra nhật ký hệ thống (Audit Logs) để phát hiện kịp thời các truy cập bất thường.

Kiểm tra đột xuất và thử nghiệm xâm nhập: Đoàn liên ngành có thẩm quyền kiểm tra không báo trước, áp dụng kỹ thuật giả lập tình huống tấn công, thử nghiệm xâm nhập để đánh giá mức độ tuân thủ quy trình SOP và năng lực ứng phó thực tế của cơ quan, đơn vị.

Giám định kỹ thuật phục vụ giải quyết khiếu nại, tố cáo: Khi nhận được phản ánh của công dân về việc lộ lọt thông tin (như bị quấy rối ngay sau khi thực hiện Dịch vụ công), liên ngành lập tức trưng cầu giám định kỹ thuật, truy vết hệ thống để xác định chính xác địa chỉ điểm rò rỉ, làm căn cứ áp dụng các hình thức trách nhiệm pháp lý tương ứng.

(2). Phân định rành mạch các loại hình trách nhiệm pháp lý và căn cứ quy trách nhiệm cho người đứng đầu

Để khắc phục tình trạng cào bằng trách nhiệm, pháp luật cấp tỉnh cần thể chế hóa và phân định rõ 05 dạng trách nhiệm pháp lý riêng biệt:

(i). Trách nhiệm kỷ luật công vụ, thi đua và căn cứ quy trách nhiệm người đứng đầu: Căn cứ phát sinh trách nhiệm người đứng đầu (Dựa trên nguyên tắc lỗi chủ quan, không áp dụng trách nhiệm tuyệt đối); người đứng đầu cơ quan chỉ chịu trách nhiệm kỷ luật khi để xảy ra sự cố lộ lọt dữ liệu do lỗi quản lý chủ quan (thiếu trách nhiệm), bao gồm 04 hành vi cấu thành: Không phân công bộ phận, nhân sự phụ trách DPO theo quy định; không ban hành hoặc không chỉ đạo thực hiện Quy trình thao tác chuẩn (SOP) về an toàn dữ liệu; không tổ chức tập huấn, phổ biến nghĩa vụ bảo mật cho cán bộ dưới quyền; cố tình phớt lờ, không triển khai các phương án khắc phục theo cảnh báo bằng văn bản của Cơ quan chuyên trách (DPO, Sở KHCN, Công an tỉnh). Tuy nhiên, nếu người đứng đầu đã thực hiện đầy đủ các nghĩa vụ quản lý nêu trên nhưng hệ thống vẫn bị tấn công bởi các phương thức công nghệ mới hoàn toàn bất khả kháng thì người đứng đầu được miễn trừ trách nhiệm kỷ luật.

Chế tài xử lý: Đối với mức độ hành chính - thi đua: Hạ bậc xếp hạng Chỉ số cải cách hành chính (PAR INDEX) và Chỉ số chuyển đổi số (DTI) của đơn vị; người đứng đầu không được xếp loại Hoàn thành xuất sắc nhiệm vụ. Đối với mức độ kỷ luật chính quyền: Áp dụng từ khiển trách, cảnh cáo đến đình chỉ công tác hoặc điều chuyển vị trí tùy thuộc vào quy mô dữ liệu bị ảnh hưởng và mức độ lỗi chủ quan.

(ii). Trách nhiệm xử phạt hành chính: Áp dụng đối với cá nhân công chức, viên chức trực tiếp có hành vi vi phạm (như: chia sẻ tài khoản công vụ, mua bán, tự ý tra cứu DLCN của công dân ngoài phạm vi nhiệm vụ) hoặc tổ chức vi phạm các quy định về bảo vệ DLCN. Thẩm quyền xử phạt, mức phạt và hình thức phạt bổ sung được thực hiện nghiêm ngặt theo quy định tại Nghị định xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng và bảo vệ DLCN.

(iii). Trách nhiệm bồi thường của Nhà nước và cơ chế hoàn trả của công chức: Căn cứ bồi thường cho công dân; khi sự cố rò rỉ dữ liệu xuất phát từ lỗi công vụ gây thiệt hại vật chất hoặc tinh thần cho công dân, Nhà nước có nghĩa vụ bồi thường trực tiếp cho công dân theo quy định của Luật Trách nhiệm bồi thường của Nhà nước. Sau khi ngân sách nhà nước chi trả bồi thường cho người dân, cơ quan nhà nước có thẩm quyền bắt buộc phải xem xét, ra quyết định yêu cầu cán bộ, công chức có lỗi (trực tiếp cố ý hoặc vô ý nghiêm trọng) phải hoàn trả số tiền bồi thường cho ngân sách nhà nước theo đúng quy định pháp luật.

(iv). Trách nhiệm dân sự, trách nhiệm hợp đồng của Nhà thầu công nghệ (Bên thứ ba): Đối với các sự cố rò rỉ dữ liệu phát sinh từ lỗi hỏng phần mềm, hạ tầng Cloud hoặc lỗi bảo mật của doanh nghiệp cung cấp dịch vụ CNTT cho chính quyền; xác định đây là trách nhiệm dân sự, hợp đồng thương mại. Cơ quan nhà nước (Bên thuê dịch vụ) có quyền và nghĩa vụ khởi kiện nhà thầu ra Tòa án có thẩm quyền để yêu cầu bồi thường toàn bộ thiệt hại, phạt vi phạm hợp đồng và cấm tham gia các dự án CNTT của tỉnh, tách biệt hoàn toàn với trách nhiệm hành chính của cán bộ công quyền.

(v). Trách nhiệm hình sự: Chuyển toàn bộ hồ sơ sang Cơ quan Điều tra để truy cứu trách nhiệm hình sự trong các trường hợp: Cán bộ, công chức có hành vi cố ý chiếm đoạt, mua bán trái phép DLCN (Tội thu thập, công khai hoặc sử dụng trái phép thông tin mạng máy tính... theo Điều 288 BLHS). Người đứng đầu có hành vi cố tình bao che, dung túng hoặc che giấu sự cố rò rỉ dữ liệu nghiêm trọng, gây hậu quả đặc biệt lớn cho xã hội (Tội Thiếu trách nhiệm gây hậu quả nghiêm trọng theo Điều 360 BLHS) [17].

(vi). Thể chế hóa cơ chế khiếu nại, tố cáo và khởi kiện của công dân: Quy trình giải quyết khiếu nại hành chính; công dân có quyền nộp đơn khiếu nại trực tiếp đến Chủ tịch UBND tỉnh hoặc gửi phản ánh qua User Power Dashboard trên Cổng Dịch vụ công. Trong thời hạn luật định, cơ quan nhận đơn phải trả lời bằng văn bản kèm theo kết quả giám định kỹ thuật từ đoàn liên ngành. Trong trường hợp không đồng ý với giải quyết khiếu nại hoặc khi có thiệt hại thực tế phát sinh, công dân có quyền khởi kiện vụ án hành chính (yêu cầu hủy bỏ quyết định, hành vi hành chính trái pháp luật về dữ liệu) hoặc khởi kiện vụ án dân sự tại Tòa án nhân dân để bảo vệ quyền năng pháp lý của mình.

Có thể khẳng định, việc hoàn thiện cơ chế thanh tra liên ngành gắn liền với quy chế trách nhiệm của người đứng đầu không mang tính trừng phạt thuần túy, mà đóng vai trò xác lập hành lang pháp lý an toàn và các giới hạn công vụ bắt buộc. Việc áp dụng các chế tài pháp lý nghiêm minh sẽ tạo động lực thể chế, thúc đẩy đội ngũ công chức và chính quyền địa phương chuyển từ phương thức “tuân thủ bị động” sang “chủ động trách nhiệm” trong việc bảo vệ quyền và lợi ích hợp pháp của công dân trên môi trường số.

4.3.5. Nhóm giải pháp về bảo đảm các quyền thực chất của chủ thể dữ liệu dựa trên phân loại căn cứ pháp lý xử lý dữ liệu

Để các quyền của chủ thể dữ liệu vận hành thực chất, không bị rào cản kỹ thuật vô hiệu hóa nhưng cũng không làm đứt gãy hoạt động quản lý nhà nước, chính quyền số cấp tỉnh cần thay đổi căn bản tư duy thiết kế hệ thống Cổng Dịch vụ công. Quyền

của công dân không thể áp dụng cào bằng cơ học, mà phải được phân định chính xác dựa trên căn cứ pháp lý xử lý dữ liệu theo Luật Bảo vệ dữ liệu cá nhân.

(1). Phân loại 03 nhóm căn cứ pháp lý xử lý dữ liệu và cấu trúc quyền năng tương ứng của công dân

UBND tỉnh chỉ đạo Sở Khoa học và Công nghệ phối hợp với Sở Tư pháp tiến hành chuẩn hóa toàn bộ các quy trình xử lý dữ liệu trên Cổng Dịch vụ công theo 03 nhóm căn cứ:

Nhóm 1: Xử lý dữ liệu phục vụ thực thi nhiệm vụ, thẩm quyền do luật định. Phạm vi áp dụng là các thủ tục hành chính cốt lõi gắn liền với quản lý nhà nước như: Hộ tịch, căn cước, đất đai, thuế, xử phạt vi phạm hành chính... Cơ quan nhà nước xử lý dữ liệu dựa trên thẩm quyền luật định, không dựa trên sự đồng ý (Consent) của công dân. Tuyệt đối không thiết kế giao diện nút “Tôi đồng ý/Từ chối” đối với nhóm này (tránh tạo ra nhận thức sai lầm cho người dân rằng họ có quyền từ chối cung cấp dữ liệu bắt buộc).

Cấu trúc quyền năng thực chất của công dân: (i) Quyền được thông báo minh bạch (Notice); hệ thống tự động hiển thị thông tư hoặc điều luật quy định căn cứ thu thập dữ liệu. (ii) Quyền truy cập và tra cứu (Access); xem lại chính xác các dữ liệu cơ quan nhà nước đang lưu giữ về mình. (iii) Quyền yêu cầu chỉnh sửa, cập nhật (Rectification); yêu cầu đính chính khi thông tin bị sai lệch. (iv) Quyền khiếu nại và yêu cầu xem xét lại (Review/Objection); đề nghị cơ quan chức năng giải trình hoặc xem xét lại các quyết định xử lý dữ liệu tự động nếu phát hiện có sai sót công vụ.

Nhóm 2: Xử lý dữ liệu phục vụ nghĩa vụ lưu trữ lịch sử và hồ sơ công vụ. Phạm vi áp dụng là dữ liệu thuộc Kết quả thủ tục hành chính số hóa (Giấy khai sinh, Giấy chứng nhận quyền sử dụng đất, Văn bằng, Chứng chỉ...), các quyết định hành chính đã ban hành. Cơ chế vận hành là việc lưu trữ phải tuân thủ nghiêm ngặt Luật Lưu trữ và pháp luật chuyên ngành. Quyền xóa dữ liệu của công dân bị giới hạn tối đa nhằm bảo đảm tính toàn vẹn của hồ sơ lịch sử và giá trị chứng cứ hành chính.

Cấu trúc quyền năng và giải pháp kỹ thuật xử lý xung đột: (i) Khóa chức năng xóa đối với Dữ liệu cốt lõi; hệ thống tự động khóa tính năng xóa đối với các dữ liệu kết quả TTHC, hiển thị lý do pháp lý dẫn chiếu Luật Lưu trữ khi công dân tra cứu. (ii) Mở quyền xóa đối với dữ liệu phụ trợ, thành phần hồ sơ hết hạn; tách biệt tệp tin kết quả với các tệp tin phụ trợ đính kèm tạm thời (như bản quét sổ hộ khẩu cũ, ảnh chụp chân dung thô, giấy ủy quyền tạm thời). Sau khi thủ tục hoàn thành và hết thời hạn kiểm tra, hệ thống cho phép công dân kích hoạt Quyền yêu cầu xóa, loại bỏ dữ liệu phụ trợ để giảm thiểu rủi ro lộ lọt [50].

Nhóm 3: Xử lý dữ liệu dựa trên sự đồng ý tự nguyện của công dân (Consent-based Processing). Phạm vi áp dụng là các dịch vụ gia tăng, hoạt động khảo sát hài lòng, tiện ích Đô thị thông minh (IOC), nhận thông báo truyền thông, định vị vị trí mở rộng... Cơ chế vận hành là sự đồng ý tự nguyện của công dân (Consent) là căn cứ pháp lý duy nhất.

Cấu trúc quyền năng thực chất của công dân: (i) Áp dụng cơ chế tự do lựa chọn độc lập: Bắt buộc tách biệt các tùy chọn bằng các ô tích chọn (Checkbox) riêng biệt, mặc định để trống. Tuyệt đối không gộp chung vào điều khoản chung dạng “tất cả hoặc không có gì” (All-or-Nothing). (ii) Tích hợp Nút “Rút lại sự đồng ý” (Opt-out) và Nút “Xóa dữ liệu mở rộng”; cho phép công dân hủy bỏ sự đồng ý dễ dàng như khi cung cấp. Khi công dân bấm nút, hệ thống tự động ngắt kết nối API xử lý và xóa, ẩn danh hóa dữ liệu tương ứng trong vòng 72 giờ. (theo Điều 10 Luật Bảo vệ dữ liệu cá nhân năm 2025) [50].

(2). *Quy trình hành chính – kỹ thuật chuẩn hóa xử lý yêu cầu thực thi quyền của công dân và giải quyết các xung đột pháp lý.*

Để giải quyết các yêu cầu thực thi quyền (tra cứu, đính chính, phản đối, xóa dữ liệu phụ trợ) trực tiếp tại bộ phận Một cửa hoặc qua môi trường số, UBND tỉnh ban hành quy trình 03 bước:

Bước 1 - Tiếp nhận và định danh chủ thể: Tiếp nhận yêu cầu của công dân trên Cổng Dịch vụ công hoặc trực tiếp tại Bộ phận Một cửa. Bắt buộc xác thực danh tính điện tử qua VNeID cấp độ 2 hoặc Căn cước gắn chip để tránh tình trạng giả mạo yêu cầu can thiệp dữ liệu của người khác.

Bước 2 - Thẩm định điều kiện qua Bộ lọc Căn cứ pháp lý: Hệ thống phần mềm quản trị nội bộ tự động đối chiếu dữ liệu được yêu cầu xử lý thuộc Nhóm 1, Nhóm 2 hay Nhóm 3.

Trường hợp thuộc Nhóm 1 và Nhóm 2 (Thực thi luật định, Lưu trữ bắt buộc): Phần mềm tự động xuất văn bản, thông báo từ chối có căn cứ pháp lý cụ thể (trích dẫn rõ điều khoản của Luật chuyên ngành hoặc Luật Lưu trữ), đồng thời hướng dẫn công dân quyền khiếu nại nếu không đồng ý.

Trường hợp thuộc Nhóm 3 hoặc Dữ liệu phụ trợ hết thời hạn: Lệnh thực thi được chuyển tự động đến Cơ quan chủ quản dữ liệu để phê duyệt điện tử.

Bước 3 - Thực thi kỹ thuật và phản hồi kết quả: Trong thời hạn tối đa 03 ngày làm việc (theo quy định tại Nghị định hướng dẫn Luật Bảo vệ DLCN), cơ quan quản lý phải thực hiện thao tác kỹ thuật (đính chính, xóa, ngắt kết nối) và phát văn bản, thông báo điện tử xác nhận kèm Mã chứng thực cho công dân.

Giải pháp này thiết lập một trạng thái cân bằng hoàn hảo về mặt lý luận: Vừa bảo đảm tính liên tục, hiệu lực của quyền lực quản lý nhà nước và nghĩa vụ lưu trữ công quyền (tuân thủ Luật Lưu trữ và Luật chuyên ngành), vừa bảo vệ thực chất quyền tự quyết và quyền kiểm soát dữ liệu của công dân đối với các vùng dữ liệu không bắt buộc (tuân thủ Luật Bảo vệ dữ liệu cá nhân).

4.3.6. Nhóm giải pháp đổi mới công tác giáo dục, truyền thông nâng cao nhận thức và năng lực tự vệ pháp lý cho chủ thể dữ liệu

Bảo vệ quyền đối với dữ liệu cá nhân (DLCN) không thể đạt hiệu quả nếu chỉ dựa vào các biện pháp kỹ thuật và chế tài hành chính từ phía Nhà nước, mà phải bắt đầu từ việc nâng cao năng lực tự bảo vệ của chính chủ thể dữ liệu. Trong bối cảnh chuyển đổi số cấp tỉnh, công tác truyền thông pháp luật cần được tháo gỡ khỏi tư duy "tuyên truyền hành chính một chiều" để chuyển sang mô hình giáo dục nhận thức quyền năng và kỹ năng tự vệ số. Nội dung nhóm giải pháp được đổi mới toàn diện theo các hướng sau:

(1). Tái cấu trúc khung nội dung truyền thông: Chuyển từ hướng dẫn thao tác kỹ thuật sang giáo dục quyền năng và kỹ năng tự vệ pháp lý

Trọng tâm thay đổi tư duy: Các sản phẩm truyền thông về Dịch vụ công và Chuyển đổi số địa phương hiện nay thường quá tập trung vào hướng dẫn kỹ thuật (các bước bấm nút, quét mã, tải ứng dụng), vốn là yếu tố có thể tự động hóa bằng thiết kế giao diện thông minh. Nội dung truyền thông mới cần tăng cường hàm lượng giáo dục pháp luật về quyền con người, các nguy cơ mất an toàn thông tin và kỹ năng tự bảo vệ dữ liệu.

Xác lập Khung nội dung chuẩn hóa: UBND tỉnh chỉ đạo Sở Khoa học & Công nghệ phối hợp với Sở Tư pháp xây dựng Bộ tài liệu truyền thông chuẩn hóa về Quyền dữ liệu cá nhân, cấu trúc theo 03 trụ cột nội dung bắt buộc: *(i) Nhận diện Quyền năng pháp lý*: Tuyên truyền dễ hiểu về các quyền của công dân theo Luật Bảo vệ DLCN (Quyền được biết, quyền truy cập, quyền đính chính, quyền rút sự đồng ý và quyền yêu cầu bồi thường thiệt hại). *(ii) Cảnh báo nguy cơ và thủ đoạn xâm phạm*: Nhận diện các hình thức thu thập dữ liệu trái phép, lừa đảo trực tuyến, giả mạo danh tính, mua bán thông tin cá nhân và các rủi ro từ việc chia sẻ thông tin quá đà trên không gian mạng. *(iii) Hướng dẫn kỹ năng tự vệ số*: Cung cấp công cụ và quy trình thao tác để công dân tự bảo vệ (cách thiết lập mật khẩu mạnh, xác thực 2 lớp, cài đặt quyền riêng tư trên thiết bị, sử dụng User Power Dashboard trên Cổng Dịch vụ công, và quy trình phản ánh, khiếu nại khi bị lộ lọt dữ liệu).

(2). Phân hóa phương thức truyền thông theo nhóm đối tượng mục tiêu

Công tác truyền thông không áp dụng một công thức cào bằng mà phải thiết kế thông điệp phù hợp với đặc điểm xã hội, nhân khẩu học của từng nhóm công dân trên địa bàn tỉnh: (i) *Đối với nhóm yếu thế và dân cư vùng nông thôn, miền núi*: Phương thức hiệu quả là tận dụng tối đa hệ thống Truyền thanh cơ sở (loa phát thanh xã, phường), Bản tin sinh hoạt chi bộ, Ngày hội chuyển đổi số cộng đồng và lực lượng Tổ công nghệ số cộng đồng “đi từng ngõ, gõ từng nhà”. Thông điệp cần ngắn gọn, trực quan, dùng tình huống thực tế (ví dụ: “Không đưa thẻ Căn cước cho người lạ chụp ảnh”, “Không nhấp vào đường link lạ nhận tiền hỗ trợ”...). (ii) *Đối với đội ngũ cán bộ, công chức, viên chức trực tiếp xử lý hồ sơ*: Phương thức chủ yếu là lồng ghép bắt buộc vào các chương trình bồi dưỡng lý luận chính trị, đạo đức công vụ và đào tạo kỹ năng số định kỳ hằng năm. Thông điệp cần quán triệt nghĩa vụ bảo mật dữ liệu là đạo đức công vụ và trách nhiệm pháp lý bắt buộc, không chỉ là công việc kỹ thuật thuần túy. (iii) *Đối với nhóm học sinh, sinh viên và thanh thiếu niên*: Phương thức chủ yếu là tích hợp vào chương trình giáo dục công dân, ngoại khóa tại các trường phổ thông, đại học; truyền thông qua các nền tảng mạng xã hội (Video ngắn, Infographic, chiến dịch truyền thông tương tác...). Thông điệp chính là dạy kỹ năng “Sức khỏe số” (xây dựng mối quan hệ lành mạnh, cân bằng và có chủ đích với công nghệ trong cả công việc lẫn cuộc sống hằng ngày) và ý thức bảo vệ dấu vết kỹ thuật số (dữ liệu để lại khi hoạt động trên Internet) từ sớm.

(3). *Xây dựng cơ chế đánh giá hiệu quả truyền thông (KPIs) dựa trên khảo sát thực nghiệm và phản hồi xã hội*

Để bảo đảm tính khoa học, thay vì ấn định chỉ tiêu % thời lượng ban đầu, hiệu quả của công tác truyền thông bảo vệ DLCN được đo lường thông qua Bộ chỉ số đánh giá tác động thực tế do UBND tỉnh ban hành: (i) Chỉ số Nhận thức pháp lý của Công dân: Định kỳ hằng năm, Sở Tư pháp chủ trì điều tra, khảo sát xã hội học độc lập trên một mẫu đại diện cư dân tỉnh về mức độ hiểu biết đối với quyền DLCN và các thủ đoạn lừa đảo dữ liệu. (ii) Mức độ chủ động thực thi quyền tự vệ: Đo lường thông qua dữ liệu thống kê hệ thống về số lượng công dân chủ động truy cập User Power Dashboard, số lượng yêu cầu đính chính, xóa dữ liệu phụ trợ hoặc các phản ánh sự cố rò rỉ dữ liệu gửi đến chính quyền. (iii) Tỷ lệ vụ việc vi phạm giảm thiểu: Sự suy giảm số lượng các vụ án lừa đảo chiếm đoạt tài sản qua mạng có gốc rễ từ rò rỉ DLCN tại địa phương.

Có thể thấy, việc xây dựng khung nội dung chuẩn hóa, phân hóa đối tượng và đánh giá bằng khảo sát thực nghiệm giúp giải pháp truyền thông của luận án bảo đảm tính chặt chẽ về mặt khoa học, tuân thủ nguyên tắc quản trị dựa trên chứng cứ, đồng thời tạo động lực thực chất nâng cao năng lực tự vệ số cho nhân dân.

4.3.7. Nhóm giải pháp về quản trị dòng chảy dữ liệu và hợp tác công - tư và tiếp thu kinh nghiệm quốc tế

Hợp tác công - tư (PPP) và thuê dịch vụ công nghệ thông tin là giải pháp tối ưu nguồn lực trong xây dựng chính quyền số. Tuy nhiên, về mặt lý luận quyền con người, Nhà nước là chủ thể mang nghĩa vụ tối cao và bất khả chuyển nhượng trong việc bảo vệ quyền đối với dữ liệu cá nhân của công dân. Việc chuyển giao xử lý dữ liệu cho doanh nghiệp tư nhân không đồng nghĩa với chuyển giao trách nhiệm pháp lý. Nhóm giải pháp này tập trung thiết lập hành lang pháp lý quản trị việc xử lý, chuyển giao dữ liệu qua 03 trụ cột:

(1). Chuẩn hóa khung hợp đồng công - tư: Phân định rạch ròi địa vị pháp lý và ràng buộc nghĩa vụ đối với Nhà thầu

UBND tỉnh giao Sở Tư pháp chủ trì ban hành mẫu hợp đồng khung bắt buộc áp dụng cho tất cả các dự án thuê dịch vụ CNTT, đấu thầu chính quyền số, chuyển hóa các yêu cầu kỹ thuật thành các điều khoản nghĩa vụ pháp lý rành mạch theo Luật Bảo vệ DCLN:

(i) Phân định chính xác địa vị pháp lý của các chủ thể: Cơ quan nhà nước cấp tỉnh là “Bên kiểm soát dữ liệu”; giữ quyền quyết định mục đích, phạm vi và phương thức xử lý dữ liệu. Doanh nghiệp nhà thầu là “Bên xử lý dữ liệu”; chỉ được thao tác kỹ thuật trong phạm vi ủy quyền văn bản của Bên kiểm soát. Nghiêm cấm nhà thầu tự ý trích xuất, phân tích dữ liệu (kể cả dữ liệu đã ẩn danh hóa) cho các mục đích thương mại, nghiên cứu riêng hoặc chuyển giao cho bên thứ ba.

(ii) Chuyển hóa quy chế kiểm soát kỹ thuật thành các phạm trù nghĩa vụ hợp đồng:

Quy định giới hạn ủy quyền và quyền kiểm toán: Thay vì “cấm truy cập Root Access”, hợp đồng quy định: Mọi truy cập vào hạ tầng cốt lõi của nhà thầu phải tuân thủ Cơ chế ủy quyền có thời hạn, được phê duyệt theo từng tác vụ chuyên biệt và chịu sự giám sát, lưu vết tự động của công cụ kiểm toán độc lập do chính quyền quản lý.

Nghĩa vụ cảnh báo và báo cáo sự cố tức thì: Nhà thầu có nghĩa vụ pháp lý phải thông báo cho Bên kiểm soát (Cơ quan nhà nước) trong thời hạn tối đa 24 - 48 giờ kể từ khi phát hiện bất kỳ nguy cơ hoặc sự cố rò rỉ dữ liệu nào, đồng thời chịu sự chỉ đạo khắc phục trực tiếp từ chính quyền.

Nghĩa vụ hoàn trả và xóa vĩnh viễn dữ liệu: Khi kết thúc hoặc chấm dứt hợp đồng, nhà thầu có nghĩa vụ bàn giao toàn bộ dữ liệu, mã nguồn và trích xuất nhật ký xử lý cho Nhà nước; đồng thời thực hiện quy trình xóa vĩnh viễn, không lưu vết trên toàn bộ hạ tầng của doanh nghiệp dưới sự chứng kiến của Hội đồng giám định pháp lý - kỹ thuật.

Trách nhiệm bồi thường thiệt hại trực tiếp và liên đới: Hợp đồng kinh tế phải đưa vào điều khoản trách nhiệm dân sự: Nếu sự cố rò rỉ dữ liệu phát sinh do lỗi bảo mật hoặc vi phạm nghĩa vụ của nhà thầu, doanh nghiệp không chỉ chịu phạt vi phạm hợp đồng đối với Nhà nước mà phải chịu trách nhiệm bồi thường tài chính trực tiếp cho những công dân bị ảnh hưởng, đồng thời hoàn trả ngân sách nếu Nhà nước đã chi bồi thường theo Luật Trách nhiệm bồi thường của Nhà nước.

(2). Quản trị hạ tầng Điện toán đám mây (Cloud) dựa trên Phân loại cấp độ dữ liệu và Đánh giá rủi ro an ninh

Mục tiêu bảo vệ chủ quyền dữ liệu quốc gia là chính đáng, nhưng không đồng nhất đơn thuần vị trí máy chủ với độ an toàn dữ liệu. Việc lựa chọn hạ tầng Cloud phục vụ chính quyền số cấp tỉnh phải dựa trên nguyên tắc quản trị rủi ro, tiêu chuẩn kỹ thuật và khả năng kiểm soát pháp lý. Phân loại dữ liệu theo cấp độ an toàn để lựa chọn hạ tầng lưu trữ:

(i) Đối với dữ liệu cốt lõi, dữ liệu nhạy cảm công quyền (Hộ tịch, căn cước, đất đai, tài chính): Bắt buộc lưu trữ trên hạ tầng điện toán đám mây dùng riêng (Private Cloud) hoặc Đám mây Chính phủ (Government Cloud) đặt tại các Trung tâm dữ liệu nội địa đáp ứng tiêu chuẩn an toàn cấp độ cao nhất do Bộ KHCN thẩm định. Điều này bảo đảm triệt để Quyền tài phán quốc gia và khả năng cưỡng chế thi hành pháp luật của Nhà nước.

(ii) Đối với dữ liệu dịch vụ công dùng chung, dữ liệu không nhạy cảm: Cho phép đề xuất sử dụng hạ tầng Cloud thương mại (bao gồm các nhà cung cấp quốc tế) nhưng phải thỏa mãn 04 điều kiện pháp lý - kỹ thuật bắt buộc: (1) Đạt chứng nhận tiêu chuẩn an ninh mạng quốc gia, quốc tế; (2) Cam kết không chuyển dữ liệu thô ra khỏi lãnh thổ Việt Nam khi chưa được sự đồng ý của Bên kiểm soát; (3) Cho phép cơ quan chuyên trách Việt Nam thực hiện quyền kiểm toán định kỳ; (4) Có cơ chế pháp lý ràng buộc nhà cung cấp tuân thủ pháp luật Việt Nam.

(iii) Kiểm soát chặt chẽ cơ chế chuyển dữ liệu xuyên biên giới: Mọi hoạt động liên thông hoặc lưu trữ tạm thời dữ liệu ra ngoài lãnh thổ quốc gia phải trải qua đánh giá tác động chuyển dữ liệu (TIA) và được sự chấp thuận bằng văn bản của Cơ quan chuyên trách bảo vệ DLCN quốc gia theo Luật Bảo vệ DLCN năm 2025.

(3). Tiếp thu có chọn lọc kinh nghiệm quốc tế về quản trị dòng chảy dữ liệu

Khung quản lý rủi ro FedRAMP (Hoa Kỳ): Rút ra bài học về việc ban hành Bộ tiêu chuẩn an ninh tối thiểu chuẩn hóa đối với dịch vụ đám mây tư nhân. Chỉ những nhà thầu vượt qua quy trình thẩm định an ninh độc lập mới đủ điều kiện tham gia đấu thầu các dự án chính quyền số.

Mô hình GDPR (Liên minh Châu Âu - EU): Rút ra bài học về phân định rạch ròi trách nhiệm pháp lý giữa Bên kiểm soát và Bên xử lý dữ liệu; đặc biệt là cơ chế trách nhiệm liên đới và nghĩa vụ bồi thường trực tiếp cho chủ thể dữ liệu, buộc các tập đoàn công nghệ phải đặt việc bảo đảm quyền con người ngang hàng với mục tiêu lợi nhuận.

Chiến lược Chủ quyền số (Singapore và Vương quốc Anh): Rút ra bài học về việc khóa quyền kiểm soát hạ tầng cốt lõi. Nhà nước giữ quyền tài phán tuyệt đối đối với các cổng kết nối API và hệ thống xác thực định danh; mọi truy cập của nhà thầu đều phải được giới hạn theo thời gian thực (Real-time Session) và ghi vết phục vụ truy cứu trách nhiệm.

Kết luận: Nhóm giải pháp quản trị dòng chảy dữ liệu và hợp tác công - tư đã khẳng định nguyên lý nền tảng của Luật Hành chính hiện đại: “Mọi hình thức ủy quyền hay thuê khoán dịch vụ kỹ thuật đều không làm thay đổi hay miễn trừ nghĩa vụ bảo đảm quyền con người của Nhà nước”. Bằng việc chuẩn hóa hợp đồng công - tư, quản trị rủi ro hạ tầng Cloud và tiếp thu chuẩn mực quốc tế, chính quyền số cấp tỉnh vừa tối ưu hóa được nguồn lực doanh nghiệp, vừa bảo đảm chủ quyền số và an toàn pháp lý cho nhân dân.

5. Lộ trình thực hiện các giải pháp bảo đảm quyền đối với dữ liệu cá nhân (Đến năm 2030)

Để các nhóm giải pháp không dừng lại ở đề xuất lý thuyết, lộ trình triển khai được thiết kế theo 03 giai đoạn chiến lược, bảo đảm tính khả thi thông qua việc xác định rõ: Cơ quan chủ trì, nguồn lực thực hiện, điều kiện bảo đảm và cột mốc đo lường kết quả.

Giai đoạn 1: Chuẩn hóa thể chế nội bộ, quy trình kỹ thuật và tối ưu bộ máy (2026 - 2027)

Mục tiêu trọng tâm: Tháo gỡ nút thắt thể chế hành chính tại địa phương; chuẩn hóa các công cụ quản trị nội bộ mà không làm phát sinh chi phí lớn ngân sách đầu tư công.

Nội dung thực hiện: UBND tỉnh ban hành Quy chế bảo vệ DLCN nội bộ; giao nhiệm vụ kiêm nhiệm, định danh nhân sự phụ trách bảo vệ dữ liệu (DPO nội bộ) tại các sở, ngành và UBND cấp xã trên cơ sở biên chế hiện có. Tổ chức tập huấn bắt buộc về nghĩa vụ tuân thủ Luật Bảo vệ DLCN năm 2025 cho lực lượng công chức trực tiếp tiếp nhận, xử lý hồ sơ tại Bộ phận Một cửa. Xây dựng quy trình phân loại tự động tại Kho số hóa để tách biệt: Dữ liệu lưu trữ bắt buộc (theo Luật Lưu trữ) và Dữ liệu phụ trợ, dữ liệu hành vi (được phép xóa/rút lại đồng ý). Ban hành Mẫu hợp đồng

chuẩn hóa về bảo mật dữ liệu áp dụng cho tất cả các dự án thuê dịch vụ CNTT, đấu thầu của tỉnh.

Giao Sở Tư pháp chủ trì, phối hợp Sở Khoa học và Công nghệ, Công an tỉnh (PA05), Văn phòng UBND tỉnh. Bố trí nguồn lực từ Ngân sách chi thường xuyên về đào tạo, tuyên truyền pháp luật và ứng dụng CNTT hiện hành. Giao chỉ tiêu 100% đơn vị sở, ngành, UBND cấp xã ban hành Quy chế nội bộ và phân công DPO kiêm nhiệm; 100% hồ sơ mời thầu CNTT mới áp dụng Mẫu hợp đồng chuẩn hóa.

Giai đoạn 2: Số hóa quy trình kiểm soát chủ động và quản trị hợp tác công - tư (2028 - 2029)

Mục tiêu trọng tâm: Tự động hóa các công cụ tự vệ cho công dân trên Cổng dịch vụ công (DVC) và thiết lập cơ chế giám sát rủi ro kỹ thuật đối với hệ thống đô thị thông minh (IOC/AI).

Nội dung thực hiện: Tích hợp công cụ tự quyết số; vận hành các tính năng User Power Dashboard (Cho phép công dân kiểm tra nhật ký truy cập, rút lại sự đồng ý, yêu cầu đính chính, xóa dữ liệu phụ trợ) trên Cổng DVC tỉnh. Kiểm soát rủi ro từ công nghệ giám sát bằng việc triển khai giải pháp kỹ thuật tự động làm mờ khuôn mặt, biển số xe đối với dữ liệu từ camera IOC không thuộc hồ sơ xử lý sự cố an ninh, trật tự trong vòng 72 giờ. Cơ chế giám sát rủi ro AI là thành lập Hội đồng/Ban tư vấn Giám sát rủi ro dữ liệu số cấp tỉnh (gồm đại diện Sở KHCN, Công an tỉnh, Sở Tư pháp, chuyên gia độc lập) để đánh giá định kỳ tác động quyền con người đối với các thuật toán AI/IOC. Thực thi trách nhiệm hợp đồng khi áp dụng cơ chế kiểm toán độc lập đối với nhà thầu CNTT và thực thi điều khoản bồi thường thiệt hại trực tiếp cho công dân khi xảy ra sự cố do lỗi nhà thầu [50].

Giao Sở Khoa học và Công nghệ chủ trì, phối hợp Công an tỉnh, Sở Tư pháp và các doanh nghiệp công nghệ đối tác. Bố trí nguồn lực từ ngân sách đầu tư công trung hạn cho chuyển đổi số và nguồn kinh phí vận hành, bảo trì hệ thống hàng năm. Tích hợp hoàn thành các nút tương tác quyền tự vệ trên Cổng DVC; 100% hệ thống camera IOC đô thị tích hợp tính năng làm mờ dữ liệu không liên quan; ban hành báo cáo đánh giá tác động rủi ro AI/IOC định kỳ hàng năm.

Giai đoạn 3: Nâng cấp hạ tầng an toàn, thu hẹp khoảng cách số và kiến nghị hoàn thiện thể chế quốc gia (Đến năm 2030)

Mục tiêu trọng tâm: Kiên cố hóa hạ tầng bảo mật theo tiêu chuẩn pháp lý, nâng cao năng lực tự vệ thực chất cho nhóm yếu thế và đóng góp luận cứ thực tiễn cho hoàn thiện pháp luật trung ương.

Nội dung thực hiện: Phân loại và nâng cấp an toàn hệ thống. Rà soát, phân loại toàn bộ hệ thống thông tin chính quyền số cấp tỉnh; tập trung nguồn lực thẩm định,

phê duyệt và đầu tư kiên cố hóa các hệ thống cốt lõi đạt tiêu chuẩn an toàn Cấp độ 3 và Cấp độ 4 theo quy định pháp luật an toàn thông tin mạng. Chuyển dịch toàn bộ cơ sở dữ liệu công vụ dùng chung lên hạ tầng Điện toán đám mây an toàn thuộc tài phán quốc gia, kiểm soát chặt chẽ luồng kết nối API. Bảo vệ nhóm yếu thế dựa trên chứng cứ triển khai chương trình hỗ trợ trực tiếp của Tổ công nghệ số cộng đồng; định kỳ khảo sát chỉ số nhận thức pháp lý số nhằm thu hẹp khoảng cách số tại các vùng sâu, vùng xa, vùng đồng bào dân tộc thiểu số. Tổng kết mô hình thí điểm quy chế nội bộ, hợp đồng công - tư và cơ chế thử nghiệm tại địa phương; xây dựng báo cáo kiến nghị gửi Bộ Công an, Bộ Khoa học và Công nghệ phục vụ việc hoàn thiện Luật Bảo vệ DLCN và các văn bản hướng dẫn thi hành trên quy mô toàn quốc.

UBND tỉnh chủ trì chỉ đạo, Sở Khoa học và Công nghệ tổng hợp, phối hợp Công an tỉnh và các bộ, ngành Trung ương. Bố trí nguồn lực theo Kế hoạch đầu tư công trung hạn giai đoạn 2026 - 2030; Quỹ Dịch vụ viễn thông công ích và nguồn xã hội hóa hợp pháp. Phấn đấu 100% hệ thống thông tin cốt lõi cấp tỉnh được phê duyệt và triển khai phương án bảo đảm an toàn thông tin theo cấp độ; công bố báo cáo đánh giá Chỉ số nhận thức pháp lý số của tỉnh; hoàn thành báo cáo tổng kết thực tiễn kiến nghị hoàn thiện thể chế gửi các cơ quan Trung ương.

Tiểu kết chương 4

Qua kết quả nghiên cứu, các giải pháp và kiến nghị được đề xuất tại Chương 4 là sự vận dụng phù hợp hệ thống lý luận (ở Chương 1, Chương 2) và kết quả đánh giá thực trạng dựa trên sự phản hồi trực tiếp đối với các điểm nghẽn thực thi 6 nhóm quyền năng đã được chỉ ra ở Chương 3. Theo đó, mỗi kiến nghị về thể chế hay hạ tầng kỹ thuật đều hướng tới mục tiêu: trang bị công cụ kỹ thuật/pháp lý cụ thể để công dân thực thi 1 trong 6 quyền năng Hiến định, đồng thời buộc chính quyền cấp tỉnh phải thực hiện nghĩa vụ công vụ tương ứng; từ đó định hình một hệ thống giải pháp đồng bộ, có tính chiến lược và khả thi nhằm bảo vệ quyền đối với DLCN trong tiến trình xây dựng chính quyền số cấp tỉnh ở Việt Nam hiện nay. Trên cơ sở đó, Chương 4 đạt được các kết quả cốt lõi và rút ra một số kết luận mang tính học thuật sau:

Thứ nhất, về mặt nhận thức luận và hệ quan điểm chỉ đạo: Chương 4 đã luận giải và xác lập hệ thống 07 quan điểm chỉ đạo mang tính nền tảng. Hệ quan điểm này tái khẳng định một luận điểm quan trọng của lý luận luật học hiện đại: Bảo vệ quyền đối với DLCN không phải là lực cản, mà chính là nền tảng pháp lý và tâm lý, là điều kiện tiên quyết để xây dựng “niềm tin số” và thúc đẩy sự phát triển bền vững của chính quyền số. Toàn bộ các quan điểm đã chuyển dịch tư duy quản trị từ “kỹ trị”, vị công nghệ sang tư duy “nhân trị”, lấy con người làm trung tâm, bảo đảm sự tương xứng và cân bằng giữa yêu cầu quản lý nhà nước, phát triển kinh tế với nghĩa vụ bảo vệ, tôn trọng phẩm giá và quyền đời tư số của công dân.

Thứ hai, về hệ thống giải pháp hoàn thiện thể chế và bộ máy: Chương nghiên cứu đã thiết kế các giải pháp đột phá nhằm phá vỡ những “vùng chòng chèo” pháp lý giữa Luật Bảo vệ DLCN và các luật chuyên ngành (Lưu trữ, Đất đai) thông qua các kiến nghị lập quy đối với Trung ương. Đồng thời, ở cấp độ địa phương, giải pháp đã cụ thể hóa các văn bản vĩ mô thành Quy trình tác nghiệp hành chính bắt buộc (SOP) cho công chức cấp tỉnh, xã và đề xuất “Khung pháp lý thử nghiệm” cho dữ liệu thể hệ mới từ hệ thống IOC. Sự đột phá này được vận hành dựa trên một bộ máy tổ chức được kiện toàn: thí điểm vị trí Người phụ trách bảo vệ dữ liệu (DPO) độc lập và ứng dụng chính sách đãi ngộ đặc thù (Nghị định 179/2025/NĐ-CP) để thu hút nhân tài an ninh mạng vào khu vực công. Đây chính là việc hiện thực hóa nghĩa vụ của Nhà nước thông qua các chính sách ưu việt.

Thứ ba, về các biện pháp kỹ thuật và cơ chế thực thi: Chương 4 đã làm rõ mối quan hệ biện chứng giữa công nghệ và quyền con người. Các giải pháp công nghệ như: chuẩn hóa an toàn thông tin Cấp độ 3 đối với kho dữ liệu dùng chung (LGSP),

mã hóa tự động ở cả hai trạng thái (At-rest, In-transit), công kết nối API xác thực mạnh đa nhân tố (MFA), và đặc biệt là hệ thống kiểm toán ghi vết tự động (Audit Logs) không đơn thuần là công cụ kỹ thuật, mà chính là những “rào chắn kỹ thuật số” ngăn chặn sự lạm quyền của chủ thể quyền lực nhà nước. Song hành với đó, cơ chế thanh tra liên ngành độc lập (Sở KHCN - PA05 Công an tỉnh) và quy chế quy trách nhiệm công vụ pháp lý nghiêm khắc đối với người đứng đầu đã tạo ra chế tài đủ mạnh, bảo đảm các vi phạm không thể ẩn nấp sau bức màn công nghệ.

Thứ tư, về việc giải phóng năng lực cho các chủ thể xã hội: Luận án đã giải quyết bài toán gốc rễ về sự bất bình đẳng quyền lực dữ liệu thông qua hai giải pháp hướng về xã hội. Việc tái cấu trúc giao diện Công dịch vụ công để xóa bỏ cơ chế “đồng ý một chiều” (All-or-Nothing), tích hợp các nút quyền thực chất (rút lại sự đồng ý, yêu cầu xóa dữ liệu) đã chuyển dịch vị thế của người dân từ “đối tượng bị quản lý” thành “chủ sở hữu quyền lực dữ liệu”. Bên cạnh đó, việc đổi mới nội dung truyền thông theo hướng giáo dục năng lực tự vệ số và phát huy vai trò chiến lược của Tổ công nghệ số cộng đồng đã tạo ra xung lực mạnh mẽ để xóa bỏ hạn chế về nhận thức số, bảo vệ hiệu quả các nhóm yếu thế trong xã hội.

Thứ năm, về quản trị luồng dữ liệu công - tư: Nhìn nhận từ xu hướng xã hội hóa, luận án đã định hình các điều khoản pháp lý chuẩn hóa để ràng buộc tư cách “Bên kiểm soát dữ liệu” của Nhà nước và “Bên xử lý dữ liệu” của doanh nghiệp nhà thầu, kiên quyết cấm khoán trắng quyền Root Access và bảo vệ chủ quyền số bằng hạ tầng Cloud nội địa. Luận điểm này khẳng định: Dù Nhà nước có thuê khoán bao nhiêu dịch vụ công nghệ, thì nghĩa vụ bảo đảm quyền con người của Nhà nước vẫn là bất khả chuyển nhượng.

Tóm lại, các giải pháp được đề xuất trong Chương 4 không vận hành biệt lập mà gắn kết chặt chẽ, biện chứng với nhau tạo thành một chỉnh thể quản trị dữ liệu liên chính, đồng bộ và nhân văn. Hệ thống giải pháp này vừa giải quyết được các nút thắt thực tiễn mang tính cấp bách của các địa phương, vừa đóng góp một mô hình lý luận toàn diện cho khoa học pháp lý về quyền con người trong kỷ nguyên số tại Việt Nam. Kết quả của Chương 4 cũng chính là câu trả lời trọn vẹn cho mục đích nghiên cứu mà luận án đã đặt ra ngay từ phần mở đầu.

KẾT LUẬN

Công trình nghiên cứu ***“Bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh ở Việt Nam hiện nay”*** là một nỗ lực khoa học nghiêm túc nhằm giải quyết mối quan hệ biện chứng giữa phát triển công nghệ quản trị hành chính và bảo đảm quyền con người, quyền công dân trong không gian số. Qua quá trình nghiên cứu lý luận, khảo sát thực tiễn và định hình hệ thống giải pháp, luận án rút ra những kết luận tổng quát sau:

Thứ nhất, về mặt lý luận khoa học pháp lý: Luận án đã xây dựng thành công khung lý luận toàn diện và cập nhật về quyền đối với dữ liệu cá nhân dưới khía cạnh quyền con người, khẳng định DLCN là “bản ngã kỹ thuật số”, một phần không thể tách rời của nhân phẩm và quyền đời tư hiến định. Bảo vệ quyền đối với DLCN không thuần túy là một bài toán kỹ thuật an ninh mạng, mà là nghĩa vụ hiến định mang tính cốt lõi của Nhà nước pháp quyền. Luận án đã làm rõ cấu trúc mối quan hệ pháp lý đặc thù trong mô hình chính quyền số cấp tỉnh: Trong đó, cơ quan nhà nước đóng vai trò vừa là Bên kiểm soát, vừa là Bên xử lý dữ liệu quy mô lớn dựa trên vị thế quyền lực công; còn người dân vừa là chủ thể dữ liệu vừa là chủ thể quyền, luôn ở thế yếu về mặt công nghệ. Từ đó, luận án xác lập triết lý quản trị dữ liệu liên chính, khẳng định tính tối thượng của các nguyên tắc: giới hạn mục đích, tối thiểu hóa dữ liệu và đặc biệt là trách nhiệm giải trình của cơ quan công quyền.

Thứ hai, về mặt đánh giá thực trạng thực thi tại địa phương: Thông qua việc khảo sát, phân tích bức tranh thực tiễn xây dựng chính quyền số tại các địa phương thời gian qua, luận án đã chỉ rõ sự mâu thuẫn giữa tốc độ số hóa hạ tầng và năng lực bảo vệ quyền con người. Về thể chế: Tồn tại những khoảng trống, điểm xung đột, chồng chéo nghiêm trọng giữa các quy định mới về bảo vệ DLCN và các luật chuyên ngành cũ (như Luật Lưu trữ, Luật Đất đai), gây lúng túng cho công chức thực thi ở cơ sở. Về bộ máy và nhân sự: Mô hình quản trị dữ liệu mang tính kiêm nhiệm lỏng lẻo, thiếu hẳn một cơ quan giám sát chéo độc lập; khu vực công cấp tỉnh đối mặt với cuộc khủng hoảng thiếu hụt chuyên gia an ninh mạng do thiếu cơ chế đãi ngộ đặc thù. Về kỹ thuật và quản trị: Hệ thống thông tin một cửa và các kho dữ liệu dùng chung (LGSP) còn nhiều lỗ hổng; cơ chế kiểm toán ghi vết (Audit Logs) chưa được tối ưu hóa; việc kiểm soát quyền truy cập tối cao (Root Access) đối với các nhà thầu doanh

nghiệp bị buông lỏng. Về khía cạnh xã hội: Tồn tại hạn chế về kỹ năng số lớn, đặc biệt là ở các nhóm yếu thế như: người cao tuổi, người nghèo, khu vực nông thôn, miền núi..., kết hợp với giao diện dịch vụ công áp đặt cơ chế “đồng ý một chiều” (All-or-Nothing) đã vô hình trung hình thức hóa các quyền thực chất của người dân.

Thứ ba, về hệ thống giải pháp đề xuất: Trên cơ sở hệ thống 07 quan điểm chỉ đạo xuyên suốt lấy con người làm trung tâm, luận án đã thiết kế một hệ thống giải pháp đồng bộ, có tính khả thi cao, bao quát từ gốc rễ thể chế đến công nghệ và xã hội. Hoàn thiện thể chế và bộ máy: Kiến nghị ban hành các văn bản gỡ rối chồng chéo luật; cụ thể hóa các văn bản quy định chung thành Quy trình tác nghiệp hành chính chuẩn (SOP) cho công chức hai cấp; thí điểm thành lập vị trí Người phụ trách bảo vệ dữ liệu (DPO) độc lập; ban hành Khung thể chế thử nghiệm quản lý dữ liệu trắc sinh học tại các trung tâm IOC; áp dụng chính sách thu nhập đặc thù theo Nghị định 179/2025/NĐ-CP để thu hút nhân tài mạng. Lá chắn kỹ thuật và cơ chế bảo mật: Chuẩn hóa an toàn thông tin tối thiểu Cấp độ 3 cho hệ thống LGSP; áp dụng công nghệ mã hóa kép; triển khai hệ thống ghi vết tự động không thể sửa xóa; bảo mật API bằng xác thực mạnh đa nhân tố (MFA). Đồng thời, thiết lập cơ chế thanh tra liên ngành (Sở KHCN - PA05 Công an tỉnh), đi đôi với quy chế quy trách nhiệm công vụ nghiêm khắc cho người đứng đầu nếu để xảy ra sự cố do lỗi chủ quan. Hiện thực hóa quyền của công dân và quản trị công - tư: Tái cấu trúc giao diện Cổng dịch vụ công để xóa bỏ cơ chế All-or-Nothing; tích hợp các nút công cụ tương tác trực tiếp cho phép công dân “rút lại sự đồng ý” hoặc “yêu cầu xóa dữ liệu”; đổi mới nội dung truyền thông theo hướng nâng tỷ lệ giáo dục pháp luật tự vệ số lên tối thiểu 30%; phát huy vai trò Tổ công nghệ số cộng đồng để xóa dần khoảng cách số cho nhóm yếu thế. Đối với khu vực tư, chuẩn hóa điều khoản hợp đồng khung, cấm khoán trắng quyền Root Access và kiên quyết ưu tiên sử dụng hạ tầng Cloud nội địa nhằm giữ vững chủ quyền số quốc gia.

Thứ tư, đóng góp mới và ý nghĩa khoa học của Luận án: Luận án là một trong những công trình đầu tiên tại Việt Nam tiếp cận vấn đề bảo vệ DLCN trong xây dựng chính quyền số một cách hệ thống dưới góc độ luật học về quyền con người, thoát ly khỏi lối tiếp cận kỹ trị thuần túy. Kết quả nghiên cứu của luận án không chỉ làm phong phú thêm kho tàng lý luận khoa học pháp lý về quyền riêng tư số trong kỷ nguyên

Cách mạng công nghiệp lần thứ tư, mà còn là cầm nang thực tiễn có giá trị tham khảo cao cho các nhà hoạch định chính sách, Ủy ban nhân dân và các sở, ban, ngành cấp tỉnh trong việc xây dựng một chính quyền số liêm chính, nhân văn, phụng sự nhân dân.

Bảo vệ quyền đối với dữ liệu cá nhân không phải là điểm kết thúc của sự phát triển, mà chính là điều kiện của sự phát triển bền vững, nơi công nghệ được sinh ra để bảo vệ và thúc đẩy các giá trị cao quý của con người.

**DANH MỤC CÁC CÔNG TRÌNH KHOA HỌC ĐÃ CÔNG BỐ
CỦA TÁC GIẢ LIÊN QUAN ĐẾN LUẬN ÁN**

[1]. Cao Nguyên Hùng: “Thực trạng pháp luật về bảo vệ quyền đối với dữ liệu cá nhân trong xây dựng chính quyền số cấp tỉnh ở Việt Nam hiện nay”, Tạp chí Pháp luật về Quyền Con người, số 51 (12/2025).

[2]. Cao Nguyên Hùng: “Bảo vệ dữ liệu cá nhân trong xây dựng chính quyền số - Kinh nghiệm từ Liên minh châu Âu và gợi mở cho Việt Nam”, Tạp chí Cộng sản điện tử, ngày 23/01/2026.

[3]. Cao Nguyên Hùng: “Bảo vệ dữ liệu cá nhân trong Liên minh châu Âu và kinh nghiệm với Việt Nam”, Tạp chí Cộng sản điện tử, ngày 01/3/2026.

DANH MỤC TÀI LIỆU THAM KHẢO

I. Tài liệu tiếng Việt

1. Bế Trung Anh (chủ biên), Nguyễn Mạnh Hùng, Nguyễn Đình Quý, Dương Văn Ninh (2020), *Giáo trình Chính phủ điện tử (Dùng cho đào tạo đại học ngành Quản lý nhà nước)*, Nxb Bách khoa Hà Nội, Hà Nội.
2. Nguyễn Thị Quế Anh, Vũ Công Giao, Vũ Ngọc Anh, Nguyễn Thị Minh Hà (2019), *Chính phủ mở, chính phủ điện tử và quản trị nhà nước hiện đại*, Nxb Hồng Đức, 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 Chính trị (2024), *Nghị quyết số 57-NQ/TW, ngày 22/12/2024 về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia*, Hà Nội.
5. Bộ Chính trị (2025), *Nghị quyết số 66-NQ/TW, ngày 30/4/2025 về đổi mới công tác xây dựng và thi hành pháp luật đáp ứng yêu cầu phát triển đất nước trong kỷ nguyên mới*, Hà Nội.
6. Bộ Công an (2026), *Báo cáo tổng kết hoạt động năm 2025, triển khai nhiệm vụ năm 2026 của Ban Chỉ đạo 57 và Ban Chỉ đạo 158 Bộ Công an*, Hà Nội.
7. Bộ Khoa học và Công nghệ (2023), *Báo cáo Chỉ số chuyển đổi số (DTI) năm 2022*, Hà Nội.
8. Bộ Khoa học và Công nghệ (2024), *Báo cáo Chỉ số chuyển đổi số (DTI) năm 2023*, Hà Nội.
9. Bộ Khoa học và Công nghệ (2025), *Báo cáo Chỉ số chuyển đổi số (DTI) năm 2024*, Hà Nội.
10. Bộ Thông tin và Truyền thông (2015), *Khung Kiến trúc Chính phủ điện tử Việt Nam - Phiên bản 1.0 (ban hành kèm Văn bản số 1178/BTTTT-THH, ngày 21/4/2015)*, Hà Nội.
11. Hoàng Thị Kim Chi (2023), *Thực trạng và giải pháp xây dựng Chính phủ điện tử hướng tới Chính phủ số ở Việt Nam*, Tạp chí Tổ chức nhà nước, số 10/2023.
12. Chính phủ (2019), *Nghị quyết số 17/NQ-CP, ngày 07/3/2019 về một số nhiệm vụ, giải pháp trọng tâm phát triển Chính phủ điện tử giai đoạn 2019 - 2020, định hướng đến 2025*, Hà Nội.

13. Thủ tướng Chính phủ (2019), *Chỉ thị số 14/CT-TTg, ngày 07/06/2019 về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam*.

14. Chính phủ (2020), *Nghị định số 45/2020/NĐ-CP, ngày 08/4/2020 về thực hiện thủ tục hành chính trên môi trường điện tử*, Hà Nội.

15. Chính phủ (2020), *Nghị định số 47/2020/NĐ-CP, ngày 09/4/2020 về quản lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước*, Hà Nội.

16. Chính phủ (2022), *Nghị định số 42/2022/NĐ-CP, ngày 24/6/2022 quy định về việc cung cấp thông tin và dịch vụ công trực tuyến của cơ quan nhà nước trên môi trường mạng*, Hà Nội.

17. Chính phủ (2022), *Nghị định số 14/2022/NĐ-CP, ngày 27/01/2022, sửa đổi, bổ sung một số điều của Nghị định số 15/2020/NĐ-CP ngày 03/02/2020 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử và Nghị định số 119/2020/NĐ-CP, ngày 07/10/2020 của Chính phủ quy định xử phạt vi phạm hành chính trong hoạt động báo chí, hoạt động xuất bản*.

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

19. Chính phủ (2025), *Nghị định số 278/2025/NĐ-CP quy định về kết nối, chia sẻ dữ liệu bắt buộc giữa các cơ quan thuộc hệ thống chính trị*, Hà Nội.

20. Chính phủ (2025), *Nghị định số 356/2025/NĐ-CP quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ Dữ liệu cá nhân*, Hà Nội.

21. Chính phủ (2025), *Nghị định số 179/2025/NĐ-CP, ngày 01/7/2025, Quy định về mức hỗ trợ đối với người làm công tác chuyên trách về chuyển đổi số, an toàn thông tin mạng, an ninh mạng*.

22. Nguyễn Văn Cương (2020), *Thực trạng pháp luật về bảo vệ thông tin cá nhân ở Việt Nam hiện nay và hướng hoàn thiện*, Tạp chí Nghiên cứu Lập pháp, số 15 (415), Hà Nội.

23. Đỗ Văn Đại (2017), *Bình luận khoa học những điểm mới của Bộ luật Dân sự năm 2015*, Nxb Hồng Đức, Hà Nội.

24. Đảng Cộng sản Việt Nam (2021), *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, Nxb Chính trị quốc gia Sự thật, Hà Nội.

25. Đảng Cộng sản Việt Nam (2026), *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIV*, Nxb Chính trị quốc gia Sự thật, Hà Nội.

26. Hoàng Văn Đoàn, Mai Văn Thắng (2018), *Ảnh hưởng của pháp luật phương Tây đến pháp luật Nhật Bản trong lịch sử và những giá trị tham khảo đối với Việt Nam trong bối cảnh hiện nay*, Tạp chí Khoa học Đại học Quốc gia Hà Nội, Luật học, Tập 34, Số 3, Hà Nội.

27. Thái Thị Tuyết Dung (2012), *Quyền tiếp cận thông tin và quyền riêng tư ở Việt Nam và một số quốc gia*, Nxb Hồng Đức, Hà Nội.

28. Đinh Thị Hương Giang (2020), *Những rào cản trong xây dựng Chính phủ số ở Việt Nam hiện nay*, Tạp chí Lý luận chính trị, số 12, Hà Nội.

29. Vũ Công Giao, Lê Trần Như Tuyên (2020), *Bảo vệ quyền đối với dữ liệu cá nhân trong pháp luật quốc tế, pháp luật ở một số quốc gia và giá trị tham khảo cho Việt Nam*, Tạp chí Nghiên cứu Lập pháp, số 09 (409), Hà Nội.

30. Vũ Công Giao, Nguyễn Văn Quân (2019), *Chính phủ điện tử và quản trị nhà nước hiện đại*, VNU Journal of Science: Legal Studies, Vol. 35, No. 3, Hà Nội.

31. Nguyễn Tấn Hoàng Hải, Trần Võ Kiều Anh, Hoàng Thị Khánh Hiền, Nguyễn Phạm Thanh Hoa (2021), *Chủ thể dữ liệu, chủ thể kiểm soát dữ liệu và chủ thể xử lý dữ liệu trong pháp luật về bảo vệ dữ liệu cá nhân*, trong Kỷ yếu Hội thảo cấp quốc gia *Bảo đảm chủ quyền quốc gia trên không gian mạng*, tập 1, Nxb Chính trị quốc gia Sự thật, Hà Nội.

32. Trần Thị Hồng Hạnh (2018), *Hoàn thiện pháp luật về bảo vệ thông tin cá nhân ở Việt Nam hiện nay*, Luận án tiến sĩ, Học viện Chính trị Quốc gia Hồ Chí Minh, Hà Nội.

33. Bùi Ngọc Hiền (2021), *Xây dựng chính quyền số hiện nay*, Tạp chí Quản lý nhà nước, số 09/2021, Hà Nội.

34. Hiệp hội An ninh mạng quốc gia (2025), *Báo cáo khảo sát an ninh mạng Việt Nam năm 2025*, Hà Nội.

35. Cục An toàn thông tin - Bộ TT&TT (2024), *Báo cáo tình hình an toàn thông tin mạng tại Việt Nam năm 2024*.

36. Học viện Chính trị quốc gia Hồ Chí Minh (2022), *Phát triển chính quyền số trong bối cảnh cách mạng công nghiệp lần thứ tư*, Đề tài nghiên cứu cấp Bộ.

37. Bùi Duy Khánh, Trần Minh Phú, Dương Yến Nhi (2021), *Bảo vệ dữ liệu cá nhân trong giai đoạn cách mạng công nghiệp 4.0 - Bài học kinh nghiệm của các quốc gia trên thế giới*, Báo cáo tổng kết đề tài nghiên cứu khoa học, Trường Đại học Luật Hà Nội, Hà Nội.

38. Khoa Luật - Đại học Quốc gia Hà Nội (2016), *Giáo trình Lý luận và pháp luật về quyền con người*, Nxb Đại học Quốc gia Hà Nội, Hà Nội.

39. Bùi Quốc Lộc (2025), *Dịch vụ công trực tuyến đến chính quyền điện tử: một số yêu cầu và giải pháp*, Tạp chí Quản lý nhà nước, số tháng 6.

40. Bạch Thị Nhã Nam (2022), *Hướng tiếp cận và hoàn thiện pháp luật bảo vệ dữ liệu cá nhân tại Việt Nam trước tác động lập pháp của thế giới và khu vực*, Tạp chí Luật học, Hà Nội.

41. Lê Văn Năng (2024), “*Xây dựng Chính quyền điện tử - Thực trạng và đề xuất một số giải pháp*”, Trang thông tin điện tử Trung tâm Lưu trữ lịch sử tỉnh Đắk Lắk, ngày 24/8/2024 (Link truy cập: <https://ttlts.sonoivu.daklak.gov.vn/xay-dung-chinh-quyen-dien-tu-thuc-trang-va-de-xuat-mot-so-giai-phap-25.html>).

42. Nguyễn Đăng Hậu, Nguyễn Hoài Anh, Cao Thu Hoài (2010), *Chính phủ điện tử*, Nxb Thông tin và Truyền thông, Hà Nội.

43. Quốc hội (2013), *Hiến pháp nước Cộng hòa xã hội chủ nghĩa Việt Nam*.

44. Quốc hội (2015), *Luật An toàn thông tin mạng*, Luật số 86/2015/QH13.

45. Quốc hội (2015), *Luật tổ chức chính quyền địa phương năm 2015*, Luật 77/2015/QH13.

46. Quốc hội (2018), *Luật An ninh mạng*, Luật số 24/2018/QH14.

47. Quốc hội (2019), *Luật Tổ chức Chính phủ*, Luật số 76/2015/QH13 (được sửa đổi, bổ sung năm 2019 theo Luật số 47/2019/QH14).

48. Quốc hội (2024), *Luật Dữ liệu*, Luật số 60/2024/QH15.

49. Quốc hội (2025), *Luật An ninh mạng*, Luật số 116/2025/QH15.

50. Quốc hội (2025), *Luật Bảo vệ dữ liệu cá nhân*, Luật số 91/2025/QH15.

51. Phạm Hải Sơn (2024), *Nghiên cứu đề xuất một số giải pháp công nghệ trong xây dựng khung kiến trúc Chính phủ điện tử tại Việt Nam*, Luận án tiến sĩ, Viện Công nghệ Thông tin - Đại học Quốc gia Hà Nội, Hà Nội.

52. Đỗ Văn Thắng (chủ biên) (2023), *Giáo trình Chính phủ điện tử và văn phòng điện tử*, Nxb Đại học Quốc gia thành phố Hồ Chí Minh, thành phố Hồ Chí Minh.

53. Nguyễn Minh Thu, Đỗ Thị Kim Lương, Trần Thị Thanh Mai (2025), *Khung pháp lý về bảo vệ dữ liệu cá nhân trong bối cảnh xây dựng Chính phủ số tại Việt Nam*, Tạp chí Công Thương, số 9/2025.

54. 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.

55. Thủ tướng Chính phủ (2021), *Quyết định số 942/QĐ-TTg, ngày 15/6/2021 phê duyệt Chiến lược phát triển Chính phủ điện tử hướng tới Chính phủ số giai đoạn 2021- 2025, định hướng đến năm 2030*, Hà Nội.

56. Thủ tướng Chính phủ (2022), *Quyết định số 06/QĐ-TTg, ngày 06/01/2022 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*, Hà Nội.

57. Nguyễn Thị Thục (2025), *Hoàn thiện pháp luật về tổ chức và hoạt động của Chính phủ đáp ứng yêu cầu quản trị quốc gia hiện đại ở Việt Nam*, Luận án tiến sĩ, Học viện Chính trị Quốc gia Hồ Chí Minh, Hà Nội.

58. Trường Đại học Mở Hà Nội (2023), *Kỷ yếu Hội thảo “Pháp luật về bảo vệ dữ liệu cá nhân trong kỷ nguyên số: Những vấn đề lý luận và thực tiễn ở Việt Nam hiện nay”*, Nxb Công an nhân dân, Hà Nội.

59. Đặng Minh Tuấn (chủ biên) (2021), *Pháp luật trong bối cảnh cách mạng công nghiệp lần thứ tư*, Nxb Chính trị Quốc gia Sự thật, Hà Nội.

60. Lã Khánh Tùng (2017), *Một số vấn đề về bảo vệ quyền riêng tư trong không gian Internet*, Hà Nội.

61. Lê Xuân Tùng (2020), *Bảo vệ dữ liệu cá nhân tại Nhật Bản thông qua Đạo luật về bảo vệ thông tin cá nhân và một số khuyến nghị đối với Việt Nam*, Tạp chí Nghiên cứu Lập pháp, số 13 (413), Hà Nội.

62. Ủy ban nhân dân Thành phố Hồ Chí Minh (2019), *Quyết định số 5086/QĐ-UBND, ngày 28/11/2019 ban hành Quy chế tích hợp, quản lý, vận hành, khai thác Kho dữ liệu dùng chung của Thành phố*, TP. Hồ Chí Minh.

63. Văn phòng Chính phủ (2025), *Báo cáo tình hình tích hợp, cung cấp dịch vụ công trực tuyến trên Cổng Dịch vụ công quốc gia năm 2025*, Hà Nội.

64. Văn phòng Chính phủ (2025), *Báo cáo vận hành Cổng Dịch vụ công quốc gia*, Hà Nội.

65. Viện Khoa học pháp lý - Bộ Tư pháp (2014), *Quyền con người trong Hiến pháp năm 2013 - Quan điểm mới, cách tiếp cận mới và các quy định mới*, Nxb Chính trị quốc gia Sự thật, Hà Nội.

66. Lại Đức Vượng, Nguyễn Thị Sự (2024), *Chính phủ số và giải pháp xây dựng Chính phủ số ở Việt Nam hiện nay*, Tạp chí Tổ chức nhà nước, tháng 7/2024.

67. Văn phòng Chính phủ (2024), Thông báo số 369/TB-VPCP, ngày 09/8/2024 *thông báo kết luận của Thủ tướng Chính phủ tại Hội nghị Thường trực Chính phủ về chuyển đổi số*, Hà Nội.

68. Văn phòng Chính phủ (2023), Thông tư số 01/2023/TT-VPCP, ngày 05/4/2023 *quy định một số nội dung và biện pháp thi hành trong số hóa hồ sơ, kết quả giải quyết thủ tục hành chính và thực hiện thủ tục hành chính trên môi trường điện tử*, Hà Nội.

69. Ban Thường vụ Tỉnh ủy Nghệ An (6/2026), *Kết luận số 111-KH/TU, ngày 11/6/2026 về sơ kết 01 năm vận hành mô hình tổ chức tổng thể của hệ thống chính trị, mô hình chính quyền địa phương 2 cấp trên địa bàn tỉnh Nghệ An*.

II. Tài liệu tiếng nước ngoài

70. Alan F. Westin (1967), *Privacy and Freedom*, Atheneum, New York.

71. Andrey Ponkin (2021), *Digital Government: Concept, Structure and Functions*, Moscow.

72. APEC (2015), *APEC Privacy Framework*, Singapore.

73. Bernd W. Wirtz (2022), *Digital Government: Strategy, Government Models, and Technology*, Springer International Publishing, Cham.
74. Bundesrepublik Deutschland (2017), *Bundesdatenschutzgesetz (BDSG)*, Berlin.
75. Bundesrepublik Deutschland (2017), *Onlinezugangsgesetz (OZG)*, Berlin.
76. Bundesverfassungsgericht (1983), *Volkszählungsurteil (Census Judgment)*, 15 December 1983, BVerfGE 65, 1, Karlsruhe.
77. Cécile de Terwangne (2013), “*The Right to Be Forgotten and Informational Autonomy in the Digital Environment*”, European Parliament Study, Brussels.
78. Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds.) (2020), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford.
79. Council of Europe (1981, sửa đổi 2018), *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+)*, Strasbourg.
80. Daniel J. Solove, Paul M. Schwartz (2022), *Information Privacy Law* (7th ed.), Wolters Kluwer, New York.
81. Daniel Veit, Jan Huntgeburth (2013), *Foundations of Digital Government: Leading and Managing in the Digital Era*, Springer, Berlin.
82. Eleni Kosta, Dara Hallinan, Paul De Hert, Suzanne Nusselder (eds.) (2025), *Data Protection, Privacy and Artificial Intelligence*, Bloomsbury Publishing, London.
83. European Commission (2016), *EU eGovernment Action Plan 2016–2020: Accelerating the Digital Transformation of Government*, Brussels.
84. European Parliament and Council (1995), *Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data*, Official Journal of the European Communities, Brussels.
85. Florent Thouvenin (2021), “*Information Self-Determination: A Convincing Rationale for Data Protection Law?*”, *JIPITEC – Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, Vol. 12, No. 1, Munich.
86. Graham Greenleaf (2014, cập nhật các năm sau), *Asian Data Privacy Laws*, Oxford University Press, Oxford.
87. Haya Alenezi (2022), “*Digital Government Transformation: Organizational and Strategic Perspectives*”, *Government Information Quarterly*, Elsevier, Amsterdam.

88. Ian Walden (ed.) (2018), *Law, Policy and the Internet*, Hart Publishing, Oxford (Chương: “Data Protection and e-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling”).
89. Iwona Florek, Susran Erkan Eroglu (2019), “*The Need for Protection of Human Rights in Cyberspace*”, *Journal of Modern Science*, No. 3(42), Józefów.
90. Lee A. Bygrave (2002), *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Kluwer Law International, The Hague.
91. Marco Di Giulio, Giancarlo Vecchi (2023), “*A Digital Government Framework: Technology, Administration and Governance*”, *Public Management Review*, Taylor & Francis, London.
92. Maria Tzanou (2013), “*Data Protection as a Fundamental Right next to Privacy? ‘Reconstructing’ a Not So New Right*”, *International Data Privacy Law*, Vol. 3, No. 2, Oxford University Press, Oxford.
93. National People’s Congress of the People’s Republic of China (2017), *Cybersecurity Law (CSL)*, Beijing.
94. National People’s Congress of the People’s Republic of China (2021), *Personal Information Protection Law (PIPL)*, Beijing.
95. National People’s Congress of the People’s Republic of China (2021), *Data Security Law (DSL)*, Beijing.
96. OECD (1980, sửa đổi 2013), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD Publishing, Paris.
97. OECD (2014), *Recommendation of the Council on Digital Government Strategies*, OECD Publishing, Paris.
98. OECD (2020), *The OECD Digital Government Policy Framework*, OECD Publishing, Paris.
99. Patrick Dunleavy, Helen Margetts, Simon Bastow, Jane Tinkler (2006), “*New Public Management Is Dead-Long Live Digital-Era Governance*”, *Journal of Public Administration Research and Theory*, Vol. 16, No. 3, Oxford University Press, Oxford.
100. Paul M. Schwartz, Daniel J. Solove (2011), *Information Privacy Law*, Wolters Kluwer, New York.

101. Paul Voigt, Axel von dem Bussche (2017), *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer, Cham.
102. Puneet Bhasin (2024), *Practical Guide to Digital Personal Data Protection Act, 2023: Law and Compliance*, OakBridge Publishing, New Delhi.
103. Russian Federation (1993), *Constitution of the Russian Federation*, Moscow.
104. Russian Federation (2006), *Federal Law No. 149-FZ “On Information, Information Technologies and Protection of Information”*, Moscow.
105. Russian Federation (2006), *Federal Law No. 152-FZ “On Personal Data”*, Moscow.
106. Russian Federation (2010), *Federal Law No. 210-FZ “On the Organization of Provision of State and Municipal Services”*, Moscow.
107. Svenja Falk, Andrea Römmele, Michael Silverman (2016), *Digital Government: Leveraging Innovation to Improve Public Sector Performance and Outcomes for Citizens*, Springer, Cham.
108. Tomasz Janowski (2015), “Digital Government Evolution: From Transformation to Contextualization”, *Government Information Quarterly*, Vol. 32, No. 3, Elsevier, Amsterdam.
109. United Nations (1966), *International Covenant on Civil and Political Rights (ICCPR)*, New York.
110. United Nations (2024), *United Nations E-Government Survey 2024*, New York.
111. Yvonne McDermott (2017), “Conceptualising the Right to Data Protection in an Era of Big Data”, *Big Data & Society*, Sage Publications, London.
112. Đạo luật PDPA (Personal Data Protection Act 2012); Public Sector (Governance) Act 2018 (viết tắt là PSGA); (Public Sector (Governance) (Amendment) Bill) (2026).
113. Personal Data Protection Act, B.E. 2562 (2019) (viết tắt là PDPA).

III. Nguồn Internet

114. Báo Chính phủ (2024), *Đà Nẵng: Tỷ lệ dịch vụ công trực tuyến toàn trình đạt 95%, cao nhất cả nước* (link truy cập: <https://baochinhphu.vn/da-nang-ti-le-dich-vu-cong-truc-tuyen-toan-trinh-dat-95-cao-nhat-ca-nuoc-102240831095316816.htm>).
115. Bộ Khoa học và Công nghệ (2025), *Quảng Ninh tăng tốc số hóa, nâng cao hiệu quả giải quyết thủ tục hành chính* (link truy cập: <https://mst.gov.vn/quang-ninh-tang-toc-so-hoa-nang-cao-hieu-qua-giai-quyet-thu-tuc-hanh-chinh-197251119091827023.htm>).

116. Công dữ liệu và hệ sinh thái dữ liệu mở tỉnh Ninh Bình (link truy cập: <https://data.ninhbinh.gov.vn>).

117. Đỗ Hưng (2023), *Hơn 90 bộ, ngành, địa phương, tổ chức kết nối nền tảng tích hợp, chia sẻ dữ liệu quốc gia*, Tạp chí Khoa học & Công nghệ Việt Nam điện tử, ngày 30/6/2023 (link truy cập: <https://vjst.vn/hon-90-bo-nganh-dia-phuong-to-chuc-ket-noi-nen-tang-tich-hop-chia-se-du-lieu-quoc-gia-57769.html>).

118. Phúc Lâm (2024), *Kết nối và chia sẻ dữ liệu thông qua nền tảng tích hợp, chia sẻ dữ liệu quốc gia*, Tạp chí Ngân hàng điện tử, ngày 5/4/2024 (link truy cập: <https://tapchinganhang.gov.vn/ket-noi-va-chia-se-du-lieu-thong-qua-nen-tang-tich-hop-chia-se-du-lieu-quoc-gia-9535.html>).

119. Đỗ Thị Tâm (2023), “Cơ hội, thách thức trong xây dựng Chính phủ điện tử hướng tới Chính phủ số ở Việt Nam hiện nay”, *Tạp chí Quản lý nhà nước điện tử*, ngày 27/4/2023 (link truy cập: <https://www.quanlynhanuoc.vn/2023/04/27/co-hoi-thach-thuc-trong-xay-dung-chinh-phu-dien-tu-huong-toi-chinh-phu-so-o-viet-nam-hien-nay/>)