

CHỦ QUYỀN DỮ LIỆU QUỐC GIA VÀ ĐỀ XUẤT CHO VIỆT NAM



⇒ NGUYỄN MINH THU -
Cục An toàn thông tin - Bộ TT&TT

Dữ liệu đã và đang trở thành nguồn tài nguyên giá trị nhất, tạo nên sự thành công vượt bậc của các tập đoàn công nghệ số, trong khi người dân và quốc gia tạo ra dữ liệu không được hưởng lợi từ nguồn tài nguyên do họ tạo ra mà còn đứng trước nguy cơ lệ thuộc. Việc bảo vệ chủ quyền dữ liệu quốc gia trở thành vấn đề cấp thiết cần được các quốc gia quan tâm, đặc biệt là đối với nước đang phát triển.

Tóm tắt:

- Chủ quyền dữ liệu quốc gia là quyền của một quốc gia đối với việc thu thập, xử lý và quản lý dữ liệu trong phạm vi quản lý của mình.
- Các nước đang có những mô hình bảo vệ chủ quyền dữ liệu khác nhau.
- Đề xuất cho Việt Nam:
 - (1) Xác định mô hình bảo vệ dữ liệu quốc gia;
 - (2) Nghiên cứu, hoàn thiện hành lang pháp lý về dữ liệu;
 - (3) Hoàn thiện hạ tầng dữ liệu số quốc gia, phát triển hệ sinh thái đổi mới sáng tạo dựa trên dữ liệu;
 - (4) Bảo vệ chủ quyền dữ liệu quốc gia khi tham gia các hiệp định thương mại tự do về dữ liệu.

Bối cảnh quốc tế

Dữ liệu đã và đang trở thành nguồn tài nguyên giá trị nhất, tạo nên sự thành công vượt bậc của các tập đoàn công nghệ số, hiện chủ yếu đến từ Mỹ và Trung Quốc.

Các tập đoàn công nghệ số ngày càng hùng mạnh, giàu có, trong khi người dân và các quốc gia đóng góp dữ liệu ngày càng bị phụ thuộc vào các doanh nghiệp công nghệ số lớn. Khi “kỹ thuật số” lan rộng trong hầu hết kiến trúc kinh tế, việc truy cập, kiểm soát dữ liệu sẽ định vị, xác định sự độc lập và lợi nhuận kinh tế của các bên. Điều này đúng trong mối quan hệ giữa người dùng (ví dụ: tài xế Uber, Grab, thương nhân trên Amazon) với các tập đoàn công nghệ số; và quan hệ giữa các quốc gia. Các tập đoàn công nghệ số hưởng lợi bao nhiêu từ người dùng, sự tồn tại của các thành phần kinh tế nhỏ, quốc gia nào được thăng hạng, hay phải đối mặt với tình trạng thuộc địa số? Câu trả lời được xác định thông qua cách thức thiết lập việc truy cập và kiểm soát dữ liệu¹.

Các tập đoàn công nghệ số thu thập, chuyển giao và xử lý dữ liệu của người dùng trên khắp thế giới. Họ mặc định được độc quyền và toàn quyền sử dụng dữ liệu đó cho mục tiêu phát triển của chính họ. Đồng thời, họ tạo ra các sản phẩm, dịch vụ để cạnh tranh với chính các thành phần kinh tế nhỏ hoạt động trên nền tảng của mình². Dữ liệu đang được sử dụng để phát triển trí tuệ số về người dân, quốc gia đang phát triển. Từ đó, dữ liệu sẽ được sử dụng để kiểm soát, khai thác và thậm chí thao túng họ.

Trái ngược với quyền lực và sự giàu có của các tập đoàn công nghệ số, người dân và quốc gia tạo ra dữ liệu không được hưởng lợi từ nguồn tài nguyên do họ tạo ra, đứng trước nguy cơ lệ

thuộc. Tài xế taxi Uber, Grab đóng góp phần lớn dữ liệu đằng sau mạng lưới giao thông thông minh của Uber, Grab. Nhưng họ đang bị dồn vào tình thế thu nhập chỉ đủ sống, mất khả năng thương lượng, không được hưởng bảo hiểm y tế, nhận tiền làm thêm giờ theo quy định của pháp luật về lao động. Thương nhân hoạt động trên nền tảng thương mại điện tử Amazon, Shopee, Lazada... thì bị cạnh tranh với chính Amazon, Shopee, Lazada.... Trên bình diện quốc gia, ngoài hai siêu cường là Trung Quốc và Mỹ, các nước có thể sẽ bị phụ thuộc vào các nền tảng số của các tập đoàn công nghệ số lớn.

Cam kết thương mại điện tử về “dòng dữ liệu tự do toàn cầu” gia tăng sức mạnh của các tập đoàn công nghệ số

Để duy trì và gia tăng sức mạnh dữ liệu, các tập đoàn công nghệ số đã và đang vận động quy tắc thương mại có lợi cho mình. “Dòng dữ liệu tự do toàn cầu” có nghĩa là “bất kỳ ai thu thập dữ liệu sẽ sở hữu dữ liệu đó”. Nếu các quốc gia từ bỏ kiểm tra dữ liệu chia sẻ, không thiết lập quy tắc sở hữu dữ liệu thì sẽ chấm dứt cơ hội để có một nền kinh tế số công bằng. Đặc biệt là đối với các thành phần kinh tế nhỏ và quốc gia đang phát triển. USMCA³, TPCPP, RCEP⁴ v.v., đã đưa thể chế này vào chương Thương mại điện tử.

Thỏa thuận mới về Thương mại số (TiSA)⁵, trong khuôn khổ đa phương của WTO được các tập đoàn công nghệ số vận động từ năm 2013 đến nay. Các quy tắc đề xuất đang được đàm phán gồm: (i) thu thập dữ liệu, (ii) trách nhiệm pháp lý, (iii) quyền tiếp cận thị trường, (iv) không phân biệt đối xử, (v) công khai mã nguồn, (vi) thuế, (vii) an toàn thông tin mạng và hơn thế⁶.

3. US Mexico Canada Agreement.

4. Regional Comprehensive Economic Partnership.

5. Trade in Services Agreement (TiSA)..

6. Các quy tắc được các tập đoàn công nghệ số đề xuất củng cố mô hình kinh doanh: Giành quyền tiếp cận thị trường trên toàn cầu, tiếp cận và kiểm soát dữ liệu cá nhân, xã hội và kinh doanh trên thế giới; Buộc các quốc gia bãi bỏ các quy định pháp lý và trốn tránh trong tương lai; Tiếp cận nguồn lao động không giới hạn trong khi người lao động bị tước quyền; Mở rộng quyền lực của mình thông qua độc quyền và trốn tránh việc nộp thuế (Digital trade rules: a disastrous new constitution for global economy by and for the bigtech, Deborah James).

1. Economic Rights Over Data: A Framework for Community Data Ownership Parminder Jeet Singh, Jai Vipra,

© Society for International Development 2019, Pg.1.

2. Tính theo vốn hóa thị trường trong hơn 1 thập kỷ qua.

Hiện có 80 nước thành viên WTO tham gia đàm phán. Các quy tắc được quan tâm đặc biệt gồm:

Quyền tự do chuyên dữ liệu xuyên biên giới, cấm quy định bản địa hóa dữ liệu, cấm yêu cầu sử dụng máy chủ địa phương, cấm yêu cầu tiết lộ thuật toán và mã nguồn phần mềm.

Thông qua TiSA, các tập đoàn công nghệ số sẽ thu thập nhiều dữ liệu hơn, kiểm soát người dùng nhiều hơn, từ đó, tích lũy lợi nhuận quy mô lớn hơn. TiSA buộc các nước đang phát triển trao cho các tập đoàn công nghệ số quyền khai thác miễn phí nguồn tài nguyên dữ liệu quý giá⁷ mà không được ban hành quy định để bảo vệ mình.

Các quốc gia đặc biệt là các nước đang phát triển cần nêu quan điểm về chủ quyền dữ liệu trong quá trình đàm phán TiSA

TiSA tìm cách đẩy mạnh luồng dữ liệu miễn phí, thúc đẩy nghĩa vụ cung cấp dữ liệu nguồn mở của chính phủ các nước, đồng thời, tìm cách giữ độc quyền dữ liệu cho các công ty thu thập. Vì sao việc chia sẻ tài nguyên chỉ đi một chiều từ khu vực công sang khu vực tư?⁸ Uber, Grab dựa vào cơ sở hạ tầng vật lý của thành phố (đường xá, vỉa hè, đèn đường, thậm chí cả kết nối mạng, v.v..) để xây dựng một kho dữ liệu khổng lồ về cách di chuyển của công dân trong thành phố. Tại sao cơ quan nhà nước có thẩm quyền không có quyền truy cập vào kho dữ liệu này cho mục đích quản lý giao thông thông minh, quy hoạch và phát triển đô thị?

Thế giới đang phải đối mặt trước sự độc quyền dữ liệu của các tập đoàn công nghệ số. Giá trị kinh tế của dữ liệu được khai thác cho mục đích tư mà quên đi lợi ích của chính người dân và quốc gia tạo ra nguồn dữ liệu đó. Chủ quyền của từng quốc gia bị ảnh hưởng khi hành vi của người dân, tổ chức bị các nền tảng số xuyên quốc gia chi phối. Các nước cần nêu vấn đề chủ quyền dữ liệu

quốc gia trong quá trình đàm phán TiSA, đồng thời thể hiện trong các quy định, chính sách phát triển kinh tế - xã hội của mình.

Chủ quyền dữ liệu quốc gia

Chủ quyền dữ liệu là khả năng người dùng được toàn quyền kiểm soát dữ liệu của mình.

Chủ quyền dữ liệu quốc gia là quyền của quốc gia đối với việc thu thập và quản lý dữ liệu do cá nhân, tổ chức của quốc gia đó tạo ra⁹.

Về pháp lý, chủ quyền dữ liệu (Data sovereignty) là khái niệm chỉ việc dữ liệu phải tuân thủ quy định tại quốc gia mà dữ liệu đó được thu thập; dữ liệu đó phải được lưu trữ ở vị trí địa lý do chính phủ hoặc tổ chức quy định (Data residency). Đối với luồng dữ liệu xuyên biên giới - dữ liệu cần được quy định, bảo vệ, kiểm soát cho cá nhân, doanh nghiệp, chính phủ và tổ chức khi chúng chảy qua biên giới quốc gia (Trans-border/cross-border flow)¹⁰.

Về quyền đối với dữ liệu, không chỉ xem xét quyền riêng tư đối với dữ liệu. Một nền kinh tế số công bằng còn đòi hỏi người dân có quyền kinh tế đối với dữ liệu đó. Do vậy, dữ liệu phải thuộc quyền sở hữu của nhóm, cộng đồng và quốc gia nơi tạo ra dữ liệu. Dữ liệu cộng đồng là động lực đổi mới, sáng tạo công nghệ, đổi mới mô hình hoạt động, kinh doanh để khai thác, phân phối giá trị của dữ liệu cho tất cả người dân, nhóm và thành phần trong xã hội¹¹.

Như vậy, **chủ quyền dữ liệu quốc gia là quyền của một quốc gia đối với việc thu thập, xử lý và quản lý dữ liệu trong phạm vi quản lý của mình. Dữ liệu phải tuân thủ quy định tại quốc gia mà nó phát sinh.** Người dân, cộng đồng, nhóm và quốc gia có quyền được hưởng lợi từ giá trị kinh tế

9. *Economic Rights Over Data: A Framework for Community Data Ownership* Parminder Jeet Singh, Jai Vipra,

© Society for International Development 2019.

10. Terry F. Buss Đại học Carnegie Mellon.

11. *Economic Rights Over Data: A Framework for Community Data Ownership* Parminder Jeet Singh, Jai Vipra,

© Society for International Development 2019, Pg.1.

7. *Economic Rights Over Data: A Framework for Community Data Ownership* Parminder Jeet Singh, Jai Vipra,

© Society for International Development 2019, Pg.3.

8. *Digital trade rules: a disastrous new constitution for global economy by and for the bigtech,* Deborah James.

mà dữ liệu mang lại cho mục tiêu phát triển kinh tế - xã hội của chính quốc gia đó. Dữ liệu là hàng hóa công. Đây là quan điểm mới mà các nước, đặc biệt là nước đang phát triển, cần khẳng định để giành lại cho mình quyền kiểm soát dữ liệu, chống lại việc thu thập, xử lý dữ liệu không theo quy định của các tập đoàn công nghệ số hiện nay.

Mô hình bảo vệ chủ quyền dữ liệu

Các nước đang có những mô hình bảo vệ chủ quyền dữ liệu khác nhau, một số mô hình điển hình là châu Âu, Hoa Kỳ, Australia, Trung Quốc, Indonesia.

Châu Âu: Quy định chung về bảo vệ dữ liệu - GDPR¹² cho phép cá nhân bảo vệ dữ liệu của họ. Mục tiêu là cân bằng các quyền của cá nhân với các quyền khác (gồm cả lợi ích công cộng) và bảo đảm quy định pháp luật nhất quán đối với dữ liệu cá nhân ngoài EU. “GDPR đặt ra trật tự thế giới kỹ thuật số mới” bằng cách yêu cầu các ngành thay đổi quy trình kinh doanh cơ bản và cung cấp quyền riêng tư theo cơ chế mặc định và bảo vệ dữ liệu theo thiết kế. Thay vì thu thập càng nhiều dữ liệu càng tốt, doanh nghiệp được yêu cầu chỉ thu thập dữ liệu tối thiểu để cung cấp dịch vụ cụ thể. GDPR không phải là luật toàn cầu, nhưng có thể đang trên đường trở thành luật trên thực tế (de facto law) vượt ra ngoài ranh giới của châu Âu.

Hoa Kỳ: Thống trị nhiều khía cạnh về chủ quyền dữ liệu, 92% các công ty lưu trữ dữ liệu ở đây. Hoa Kỳ không có luật bảo mật dữ liệu người dùng cấp liên bang. Tuy nhiên, họ có một số luật bảo vệ dữ liệu liên bang theo ngành (vd. Đạo luật bảo vệ quyền riêng tư của người lái xe năm 1994 và Đạo luật bảo vệ quyền riêng tư của video¹³). Đạo luật Ủy ban Thương mại Liên bang là quy định pháp luật có thẩm quyền rộng nhất. Nó ngăn

chặn các hành vi thương mại không công bằng hoặc “lừa đảo”. Quy định bao gồm hành động chống lại các công ty vi phạm quyền riêng tư dữ liệu của người tiêu dùng bằng cách thu thập, xử lý hoặc chia sẻ thông tin người tiêu dùng.

Ngoài ra còn có Đạo luật yêu nước và Đạo luật CLOUD¹⁴. Theo Đạo luật yêu nước, chính phủ được quyền truy cập vào không chỉ dữ liệu cá nhân, mà tất cả dữ liệu tổ chức đáp ứng các yêu cầu theo quy định. Đạo luật CLOUD, mở rộng quy định nêu trên đối với dữ liệu nằm ngoài Hoa Kỳ của bất kỳ nhà cung cấp nào thuộc quyền tài phán của Hoa Kỳ (bao gồm tất cả các công ty điện toán đám mây lớn).

Tháng 6/2020, Tổng thống Biden ký lệnh hành pháp bảo vệ dữ liệu nhạy cảm của người Mỹ khỏi đối thủ nước ngoài¹⁵. Cụ thể, Lệnh: (i) cho phép Mỹ thực hiện các bước mạnh mẽ để bảo vệ dữ liệu nhạy cảm của người Mỹ; (ii) cung cấp các tiêu chí để xác định ứng dụng phần mềm có thể gây ra rủi ro không thể chấp nhận được (các giao dịch hỗ trợ hoạt động quân sự hoặc tình báo của đối thủ nước ngoài, hoặc có liên quan đến mạng độc hại hoặc ứng dụng thu thập dữ liệu cá nhân nhạy cảm); (iii) phát triển các tùy chọn khác để bảo vệ dữ liệu cá nhân nhạy cảm và giải quyết mối đe dọa tiềm ẩn từ các ứng dụng phần mềm được kết nối nhất định (bảo vệ khỏi tác hại từ việc bán, chuyển giao hoặc truy cập vào dữ liệu cá nhân nhạy cảm, bao gồm kho dữ liệu lớn lưu trữ).

Hoa Kỳ ban hành chính sách và bày tỏ lập trường về bản địa hóa dữ liệu thông qua cơ quan quản lý quốc tế và các hiệp định thương mại đa phương. Theo đó, cấm bản địa hóa dữ liệu và chính thức hóa luồng dữ liệu tự do giữa các quốc gia thành viên (Hiệp định Hoa Kỳ- Mexico - Canada); cấm yêu cầu bản địa hóa dữ liệu và hạn chế dòng dữ

14. Clarifying Law Overseas Use of Data

15. <https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/09/fact-sheet-executive-order-protecting-americans-sensitive-data-from-foreign-adversaries/>

12. General Data Protection Regulation

13. <https://www.capacitymedia.com/articles/3827968/into-the-grey-the-us-and-data-sovereignty>

liệu xuyên biên giới (*các hiệp định thương mại đa phương khu vực Châu Á - Thái Bình Dương*). Tuy nhiên dòng dữ liệu xuyên Đại Tây Dương giữa Hoa Kỳ và Liên minh châu Âu (*ít nhất là dữ liệu cá nhân*) hiện vẫn còn chưa rõ ràng.

Australia: Trong Khuôn khổ Chúng nhận lưu trữ¹⁶ tất cả dữ liệu chính phủ của Cơ quan chuyển đổi số cần được lưu trữ trong các trung tâm dữ liệu “**được chứng nhận bảo đảm**” hoặc “**được chứng nhận chiến lược**”. Động thái nhằm giải quyết những vấn đề của khu vực công đang phải đối mặt: chủ quyền dữ liệu, lỗ hổng trong chuỗi cung ứng và mối đe dọa về an ninh mạng. Điều này thể hiện sự quan ngại của Úc về độ tin cậy hoạt động của trung tâm dữ liệu ở nước ngoài; rủi ro can thiệp của chính phủ và các tổ chức tư nhân nước ngoài (*ví dụ: Đạo luật CLOUD của Mỹ*).

Australia coi bản địa hóa dữ liệu là giữ dữ liệu trong biên giới - không chỉ khi nó được lưu trữ mà còn khi nó được xử lý. Mua sắm có mục tiêu hoặc có chủ quyền là lựa chọn các nhà thầu đang hoạt động ở Úc và không chịu ảnh hưởng pháp lý của khu vực tài phán nước ngoài.

Trung Quốc: Trung Quốc kêu gọi cộng đồng quốc tế giải quyết vấn đề an ninh dữ liệu một cách toàn diện, khách quan và dựa trên bằng chứng. Đồng thời duy trì chuỗi cung ứng mở, an toàn và ổn định cho các sản phẩm và dịch vụ công nghệ thông tin truyền thông toàn cầu¹⁷. Luật Bảo mật dữ liệu được ban hành trong bối cảnh quốc tế này được kỳ vọng sẽ nâng cao khả năng cạnh tranh của Trung Quốc trong vấn đề chủ quyền dữ liệu và cung cấp các giải pháp thay thế cho quản trị



dữ liệu. Luật Bảo mật dữ liệu quy định một số điều khoản quan trọng:

- *Phân loại dữ liệu theo tầng (level):* dữ liệu quan trọng hơn phải chịu sự điều chỉnh nghiêm ngặt hơn. Nhà xử lý “dữ liệu quan trọng” phải tuân theo yêu cầu đánh giá rủi ro bổ sung và kiểm soát xuất khẩu. Các công ty chuyển “dữ liệu trạng thái cốt lõi¹⁸” ra nước ngoài phải có chấp thuận của cơ quan chức năng. Trường hợp vi phạm sẽ bị phạt nặng lên đến 1,5 triệu USD cho mỗi vi phạm và đóng cửa doanh nghiệp.

- *Tăng cường quyền truy cập của chính phủ vào dữ liệu:* yêu cầu các tổ chức và cá nhân “hợp tác” với cơ quan chức năng thu thập dữ liệu “khi cần thiết để bảo vệ hợp pháp an ninh quốc gia hoặc điều tra tội phạm”.

- *Hạn chế chuyển dữ liệu ra nước ngoài:* Người xử lý “dữ liệu quan trọng” sẽ phải tuân theo các quy định sắp tới và bắt buộc các tổ chức hoặc cá nhân trong nước không được cung cấp dữ liệu được lưu trữ tại Trung Quốc cho các cơ quan thực thi pháp luật hoặc tư pháp nước ngoài nếu không được chính phủ cho phép trước.

16. https://www.dta.gov.au.translate.goog/our-projects/hosting-strategy/hosting-certification-framework?_x_tr_sl=en&_x_tr_tl=vi&_x_tr_hl=en-US&_x_tr_pto=ajax,se,elem

17. Sáng kiến Toàn cầu về Bảo mật Dữ liệu (Global Initiative on Data Security).

18. “Dữ liệu cốt lõi core state data” được định nghĩa rất rộng, bao gồm: dữ liệu liên quan đến an ninh quốc gia, huyết mạch của nền kinh tế quốc gia, các khía cạnh quan trọng trong sinh kế của người dân và lợi ích công cộng chính.

- *Áp dụng ngoài lãnh thổ:* Ngoài việc xử lý dữ liệu bên trong Trung Quốc, Luật bảo mật dữ liệu áp dụng cho tất cả việc xử lý dữ liệu bên ngoài Trung Quốc. Điều này tạo ra những thách thức tiềm năng về tuân thủ đối với các công ty nước ngoài hoạt động tại Trung Quốc.

Indonesia: là một trong những nền kinh tế số phát triển nhanh nhất trong khu vực APAC¹⁹. Bảo vệ dữ liệu chủ yếu được điều chỉnh thông qua Luật Giao dịch và Thông tin Điện tử (EITL), Quy định về Hệ thống và Giao dịch Điện tử (GR-71) và Quy định số 20 về Bảo vệ Dữ liệu Cá nhân trong Hệ thống Điện tử (PDP). Hiện nước này đang dự thảo Luật về Bảo vệ Dữ liệu Cá nhân²⁰. Đây là luật bảo vệ dữ liệu toàn diện dựa theo GDPR, sẽ thay thế các luật/quy định hiện hành. Bốn yếu tố quan trọng trong dự thảo là: (i) chủ quyền và bảo mật dữ liệu; (ii) quy định về dữ liệu cá nhân và dữ liệu cá nhân nhạy cảm, tầm quan trọng của chất lượng và độ chính xác của dữ liệu; (iii) quy định các luồng dữ liệu xuyên biên giới.

Về chuyển dữ liệu xuyên biên giới: PDP cho phép truyền dữ liệu xuyên biên giới. Theo đó, doanh nghiệp phải trình kế hoạch thực hiện cho Bộ Thông tin và Tin học (gồm: thông tin chi tiết về quốc gia đến, người nhận, ngày chuyển và lý do chuyển). Sau khi hoàn thành phải báo cáo với Bộ trưởng về việc thực hiện.

Về bản địa hóa dữ liệu: theo GR 71, yêu cầu về bản địa hóa dữ liệu chỉ áp dụng đối với các doanh nghiệp nhà nước. Các doanh nghiệp tư nhân có thể lưu trữ dữ liệu của họ bên ngoài Indonesia, chịu sự giám sát của các cơ quan chính phủ vì mục đích thực thi pháp luật.

Các mô hình bảo đảm chủ quyền dữ liệu của Mỹ, châu Âu, Úc, Trung Quốc, Indonesia đáp ứng yêu cầu phát triển kinh tế - xã hội của từng quốc gia.

19. APAC: Châu Á - Thái Bình Dương (Asia-Pacific).

20. Bill on Protection of Private Personal Data.

Hoa Kỳ ủng hộ dòng dữ liệu tự do trong nước và toàn cầu. Hoa Kỳ có nền kinh tế tiêu dùng nên thúc đẩy trao đổi dữ liệu cá nhân giúp người tiêu dùng có sản phẩm tốt nhất. Đây cũng là điều kiện tạo ra nhiều công ty khởi nghiệp giá trị tại đất nước có nguồn vốn đầu tư dồi dào nhất thế giới.

Châu Âu áp dụng mô hình cân bằng giữa lợi ích phát triển kinh tế khu vực với quan hệ kinh tế với Hoa Kỳ, thiết lập biện pháp bảo vệ dữ liệu cá nhân di chuyển ra ngoài biên giới.

Trung Quốc có cách tiếp cận dựa trên kiểm soát. Trung Quốc có thị trường và nguồn lực đủ mạnh, vì vậy họ bảo vệ dữ liệu như nguồn tài nguyên mới cho phát triển, hạn chế dòng dữ liệu xuyên biên giới.

Đề xuất cho Việt Nam

Nhằm thực hiện bảo vệ chủ quyền dữ liệu, xây dựng nguồn lực phát triển kinh tế số, bốn nhiệm vụ, giải pháp được đề xuất như sau:

a. Xác định mô hình bảo vệ dữ liệu quốc gia

Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến 2035 xác định mục tiêu: phát triển chính phủ số, kinh tế số, xã hội số và hình thành các doanh nghiệp công nghệ số Việt Nam có năng lực đi ra toàn cầu; hình thành nền tảng dữ liệu có các ngành kinh tế trọng điểm dựa trên dữ liệu. Đồng thời, theo đánh giá của Nikkei Asia, Việt Nam luôn nằm trong top 10 các nước có lượng dữ liệu chuyển qua biên giới lớn nhất của châu Á²¹. Do vậy, bảo vệ chủ quyền dữ liệu quốc gia đóng vai trò quan trọng để thực hiện các mục tiêu nêu tại Chương trình chuyển đổi số.

Trên cơ sở phân tích một số mô hình chủ quyền dữ liệu tại mục 3, Việt Nam có thể tham khảo mô hình phát triển của Liên minh châu Âu. Chính sách, quy định bảo vệ dữ liệu dựa trên quyền riêng tư, lợi ích phát triển kinh tế của người dân, quốc gia. Đồng thời, xây dựng cơ chế bảo đảm dòng dữ liệu tự do nội địa, thiết lập cơ chế chia sẻ

21. <https://vneconomy.vn/viet-nam-la-1-trong-10-nuoc-co-luong-du-lieu-luan-chuyen-xuyen-bien-gioi-lon-nhat.htm>.

dữ liệu an toàn nhằm mở rộng nguồn tài nguyên mới cho phát triển kinh tế dựa trên dữ liệu.

b. Nghiên cứu, hoàn thiện hành lang pháp lý về dữ liệu

Tin cậy trong giao dịch dữ liệu được duy trì bởi khuôn khổ pháp lý quy định biện pháp bảo vệ (*ngăn chặn sử dụng sai, vi phạm dữ liệu ảnh hưởng tính bảo mật và toàn vẹn của dữ liệu cá nhân/phi cá nhân/hỗn hợp*), thúc đẩy (tạo điều kiện thuận lợi cho việc sử dụng, tái sử dụng, chia sẻ dữ liệu thông qua tính mở, khả năng tương thích và tính di động)²². Hiện nay, ở Việt Nam việc xây dựng, triển khai, giám sát thi hành quy định về dữ liệu được thực hiện theo nhiều luật. Pháp luật thường bị lạc hậu hơn so với sự phát triển của công nghệ. Do vậy, khi không có quy định mang tính nguyên tắc chung thì có thể dẫn đến việc thiếu biện pháp pháp lý bảo vệ, phát triển dữ liệu trong các ngành.

Nghiên cứu bổ sung quy định về chủ quyền dữ liệu tại Luật Công nghiệp công nghệ số tạo căn cứ pháp lý để quy định trong lĩnh vực chuyên ngành. Một số nội dung cơ bản đề xuất đưa vào dự thảo Luật Công nghiệp công nghệ số: (i) quy định khái niệm và phân loại dữ liệu; (ii) quy định về thu thập, lưu trữ, định dạng, xử lý, phân tích dữ liệu; (iii) bảo đảm an toàn dữ liệu; (iv) chia sẻ dữ liệu; (v) quản lý dòng dữ liệu xuyên biên giới (vi) phát triển doanh nghiệp, thị trường dịch vụ dữ liệu; (vii) phát triển nguồn nhân lực dữ liệu; v.v.

c. Hoàn thiện hạ tầng dữ liệu số quốc gia, phát triển hệ sinh thái đổi mới sáng tạo dựa trên dữ liệu

Xây dựng và thiết lập hệ thống các trung tâm dữ liệu quốc gia, các trung tâm dữ liệu vùng và địa phương đạt tiêu chuẩn đồng bộ và thống nhất; kết nối các trung tâm dữ liệu của cơ quan nhà nước và doanh nghiệp để triển khai đám mây dữ liệu, tạo thuận lợi cho việc lưu trữ, xử lý, chia sẻ và phân phối dữ liệu.

Triển khai nền tảng trao đổi, chia sẻ, tổng hợp, phân tích dữ liệu tập trung tại Trung ương và địa phương: Hoàn thiện Cổng dữ liệu quốc gia để tạo lập môi trường công khai, minh bạch về dữ liệu.

Phát triển không gian dữ liệu cộng đồng trên cơ sở phối hợp và đóng góp dữ liệu từ cơ quan nhà nước, doanh nghiệp và người dân để hình thành kho tài nguyên số dùng chung; phát triển tài nguyên dữ liệu mẫu phục vụ phát triển trí tuệ nhân tạo, dữ liệu lớn dùng chung.

Hình thành hệ sinh thái đổi mới sáng tạo dựa trên dữ liệu để thu hút các nhà đầu tư, doanh nghiệp cung cấp dịch vụ, doanh nghiệp khởi nghiệp và các chuyên gia hoạt động, phát triển sản phẩm, dịch vụ Make in Viet Nam phục vụ mục tiêu phát triển kinh tế số, xã hội số của đất nước.

d. Bảo vệ chủ quyền dữ liệu quốc gia khi tham gia các hiệp định thương mại tự do về dữ liệu

Như đã nêu tại phần trên Việt Nam hiện đã tham gia các cam kết về Thương mại điện tử tại một số FTAs. Trong khuôn khổ Hiệp định CPTPP, Việt Nam đã cam kết: (i) Cho phép việc lưu chuyển thông tin xuyên biên giới bằng các phương tiện điện tử bao gồm cả thông tin cá nhân phục vụ cho hoạt động kinh doanh; (ii) Không được yêu cầu sử dụng hoặc đặt hệ thống máy chủ trên lãnh thổ làm điều kiện kinh doanh; (iii) Không được yêu cầu chuyển giao hoặc truy cập mã nguồn như là điều kiện nhập khẩu, phân phối, bán trong lãnh thổ. Mặc dù vậy, Việt Nam có thể không áp dụng cam kết (i), (ii) để thực hiện mục tiêu chính sách công cộng chính đáng; và có thể yêu cầu sửa đổi mã nguồn của phần mềm (iii) để tuân thủ với quy định không phù hợp với Hiệp định.

Trong thời gian tới, việc tham gia đàm phán quốc tế liên quan đến dữ liệu số, thương mại số, hợp tác kinh tế số cần cân nhắc thận trọng, bảo đảm chủ quyền dữ liệu quốc gia. ■

22. Data to better lives, Worldbank Development report 2021.