IPS Institute for Policy Studies and Media Development

UNDP

QUẢN TRỊ VÀ THAM GIA

Loạt báo cáo nghiên cứu thảo luận chính sách

ĐÁNH GIÁ VIỆC BẢO VỆ DỮ LIỆU CÁ NHÂN TRÊN CÁC GIAO DIỆN TƯƠNG TÁC VỚI NGƯỜI DÂN CỦA CHÍNH QUYỀN ĐỊA PHƯƠNG

Tháng 07 năm 2022

Loạt bài nghiên cứu chính sách về Quản trị và Tham gia này do Nhóm Quản trị và Tham gia của UNDP Việt Nam thực hiện.

Đây là những nghiên cứu phân tích xu thế của tiến trình và biện pháp thực hiện cải cách hành chính công trong các lĩnh vực cụ thể của nền hành chính công Việt Nam. Để giải quyết những thách thức về kinh tế, xã hội, chính trị và môi trường mà Việt Nam đang phải đối mặt, các nhà hoạch định chính sách cần những luận cứ thực chứng. Những bài nghiên cứu này nhằm cung cấp một số nội dung cho những thảo luận hiện nay về đổi mới chính sách, từ đó góp phần thúc đẩy hơn nữa những nỗ lực phát triển của Việt Nam.

Ba nguyên tắc chủ đạo trong thực hiện những nghiên cứu chính sách này là: (i) nghiên cứu thực chứng, (ii) sâu sắc về học thuật và độc lập trong phân tích, và (iii) hợp lý về mặt xã hội và có sự tham gia của các bên liên quan. Để đạt được ba nguyên tắc đó đòi hỏi cách tiếp cận nghiên cứu chuyên sâu và xác định một cách hệ thống và cặn kẽ các biện pháp chính sách nhằm giải quyết các vấn đề liên quan đến cải cách hành chính và phòng, chống tham nhũng.

Tên trích dẫn nguồn: Viện Nghiên cứu Chính sách và Phát triển Truyền thông và Chương trình Phát triển Liên Hợp Quốc (2022). *Đánh giá việc bảo vệ dữ liệu cá nhân trên các giao diện tương tác với người dân của chính quyền địa phương*. Báo cáo nghiên cứu chính sách về Quản trị và Tham gia đồng thực hiện bởi Viện Nghiên cứu Chính sách và Phát triển Truyền thông (IPS) và Chương trình Phát triển Liên Hợp Quốc (UNDP) tại Việt Nam. Hà Nội, Việt Nam: Tháng 06 năm 2022

Ghi chú: Các quan điểm, phát hiện và kết luận đưa ra trong báo cáo này không nhất thiết phản ánh quan điểm chính thức của Chương trình Phát triển Liên Hợp Quốc (UNDP) tại Việt Nam.

Chương trình Phát triển Liên Hợp Quốc

304 Kim Mã, Hà Nội, Việt Nam
Tel: (84 024) 38 500 100
Fax: (84 024) 37 265 520
Email: registry.vn@undp.org
www.undp.org/vietnam

Viện Nghiên cứu Chính sách và Phát triển Truyền thông

Tầng 18, Tòa nhà VTC Online,
18 Tam Trinh, Hai Bà Trưng, Hà Nội
Tel: (84) 969 520 220
Email: contact@ips.org.vn
ips.org.vn

Nhóm nghiên cứu

Nguyễn Quang Đồng
Nguyễn Đức Lam
Tống Khánh Linh
(Viện Nghiên cứu Chính sách và Phát triển Truyền thông)

và

Đỗ Thanh Huyền
(Chương trình Phát triển Liên Hợp Quốc)

MỤC LỤC

Danh mục hộp

Danh mục hình

Danh mục bảng

Danh mục từ viết tắt

BVDLCN	Bảo vệ dữ liệu cá nhân
CCCD	Căn cước công dân
CMTND	Chứng minh thư nhân dân
CNTT	Công nghệ thông tin
CQNN	Cơ quan nhà nước
DLCN	Dữ liệu cá nhân
DVCTT	Dịch vụ công trực tuyến
FTC	Ủy ban thương mại liên bang Hoa Kỳ
GDPR	Quy định chung về bảo vệ dữ liệu của Liên minh Châu Âu EU
IPS	Viện Nghiên cứu Chính sách và Phát triển Truyền thông
LHQ	Liên Hợp Quốc
PIA	Đánh giá tác động quyền riêng tư
PII	Thông tin định danh cá nhân
TP HCM	Thành phố Hồ Chí Minh
TTĐT	Thông tin điện tử
TTTT	Thông tin và truyền thông
UBND	Ủy ban nhân dân
UNDP	Chương trình Phát triển Liên Hợp Quốc
ƯDTM	Ứng dụng thông minh

Lời cảm ơn

Báo cáo phân tích chính sách này là sản phẩm đầu tiên nằm trong chuỗi hoạt động nghiên cứu thảo luận chính sách về quản trị dữ liệu trong khu vực công do Viện Nghiên cứu Chính sách và Phát triển Truyền thông (IPS) phối hợp với Chương trình Phát triển Liên Hợp quốc (UNDP) tại Việt Nam thực hiện. Báo cáo nhằm đánh giá, phân tích thực tiễn triển khai việc bảo vệ dữ liệu cá nhân của chính quyền địa phương (63 tỉnh, thành phố trực thuộc trung ương) trên các giao diện tương tác trực tuyến với công dân tại Việt Nam.

Báo cáo được thực hiện bởi nhóm nghiên cứu gồm Ông **Nguyễn Quang Đồng**, Viện trưởng Viện IPS, Ông **Nguyễn Đức Lam**, Chuyên gia pháp luật của Văn phòng Quốc hội, Bà **Tống Khánh Linh**, Chuyên viên phân tích chính sách Viện IPS, và Bà **Đỗ Thanh Huyền**, Chuyên gia phân tích chính sách công, Chương trình Phát triển Liên Hợp Quốc tại Việt Nam.

Chúng tôi trân trọng cảm ơn các chuyên gia, các nhà nghiên cứu, đại diện các sở Thông tin và Truyền thông (TTTT) của 63 tỉnh, thành phố đã trao đổi và chia sẻ các quan điểm, phân tích cá nhân với nhóm nghiên cứu về các vấn đề liên quan đến việc bảo vệ dữ liệu cá nhân trong khu vực công tại Việt Nam. Nhóm nghiên cứu xin chân thành gửi lời cảm ơn đến các cá nhân:

Ông **Mai Thanh Hải** và Ông **Nguyễn Trọng Khánh**, Đại diện Cục Tin học hóa (Bộ TTTT) vì đã góp ý, phản biện kỹ thuật cho phương pháp nghiên cứu và tính khả thi của các khuyến nghị.

Ông **Nguyễn Dương Anh** và Ông **Trần Trọng Hiếu**, Đại diện Sở TTTT tỉnh Thừa Thiên Huế vì những chia sẻ về thực hành tốt của tỉnh Thừa Thiên Huế trong xây dựng quy định, quy chế về bảo vệ dữ liệu cá nhân và triển khai trên thực tiễn, bước đầu thành công trong xây dựng niềm tin của người dân vào chính phủ điện tử.

Ông **Trần Diễn Phúc,** Đại diện Sở TTTT tỉnh Quảng Bình vì những chia sẻ về thực tiễn khó khăn trong đầu tư phát triển hệ thống công nghệ thông tin khi nguồn kinh phí hạn hẹp, và những góp ý cụ thể về quy định cho hồ dữ liệu (data lakes) để bảo đảm bảo vệ dữ liệu cá nhân công dân.

Bà **Nguyễn Thị Kim Thoa**, nguyên Vụ trưởng Vụ pháp luật hình sự hành chính (Bộ Tư Pháp); Bà **Thái Tuyết Dung**, Giảng viên Trường Đại học kinh tế luật (ĐHQG TPHCM); Bà **Nguyễn Thị Long** (Đại học Luật Hà Nội); Bà **Lưu Hương Ly**, Trưởng phòng, Phòng Pháp luật dân sự, Vụ Pháp luật dân sự - kinh tế (Bộ Tư pháp) vì những góp ý liên quan đến khoảng trống pháp lý về bảo vệ dữ liệu cá nhân nói chung và trong khu vực công nói riêng.

Ông **Huỳnh Thiên Tứ**, Giảng viên Khoa Luật, Trường Kinh Tế, Luật và Quản lý Nhà nước (Đại học Kinh tế TPHCM) vì những góp ý về mặt triết lý nghiên cứu.

Ông **Đặng Đình Ngọc**, Chuyên gia Tổ chức CARE International, và Ông **Lê Nghiêm**, nguyên Cục trưởng Cục thông tin đối ngoại (Bộ TTTT) vì những góp ý về cấu trúc nghiên cứu và thực tiễn địa phương.

Ngoài ra, nhóm nghiên cứu đặc biệt cảm ơn đội ngũ nhân lực trẻ tuổi và nhiệt huyết, các bạn **Phùng Ngọc Trâm** và **Nguyễn Thị Thùy** (cộng tác viên của IPS đến từ Đại học Khoa học Xã hội và Nhân Văn Hà Nội) đã hỗ trợ công tác thu thập dữ liệu từ các giao diện tương tác và bạn **Trần Thị Tuyết** (cộng tác viên của IPS đến từ Đại học Ngoại thương) đã hỗ trợ công tác rà soát báo cáo và tổ chức hậu cần.

Cuối cùng, trân trọng cảm ơn Bộ Ngoại giao và Thương mại Úc (DFAT), Đại sứ quán Ai-len và Chương trình Phát triển Liên Hợp Quốc (UNDP) tại Việt Nam đã tài trợ cho nghiên cứu này.

Tóm tắt báo cáo

Hiến pháp năm 2013 và nhiều đạo luật khác đã ghi nhận quyền về đời sống riêng tư (sau đây gọi là quyền riêng tư) như một quyền con người cơ bản ở Việt Nam. Trong giai đoạn hiện nay, khi quá trình chuyển đổi số, xây dựng chính quyền số là một trong những mục tiêu quan trọng của quốc gia, việc bảo vệ, đảm bảo quyền riêng tư trên môi trường số có ý nghĩa quan trọng. Dữ liệu, thông tin cá nhân[1] được thu thập rất nhiều qua các công cụ trên môi trường số, điển hình như cổng thông tin điện tử, cổng dịch vụ công trực tuyến và ứng dụng thông minh của Ủy ban nhân dân cấp tỉnh. Tuy nhiên, việc bảo vệ dữ liệu cá nhân, đảm bảo quyền riêng tư trên các giao diện đó vẫn chưa được chú ý, vẫn còn những khoảng cách nhất định so với quy định pháp luật, nhất là so với các thực hành tốt.

Trong bối cảnh nói trên, đối chiếu với khung pháp luật hiện hành, nghiên cứu này đánh giá tổng quan ban đầu về thực tiễn bảo vệ dữ liệu cá nhân, đảm bảo quyền riêng tư, trên các cổng TTĐT, cổng DVCTT của 63 tỉnh, thành phố trực thuộc trung ương, ƯDTM của 50 tỉnh, thành. Từ đó, nghiên cứu đưa ra một số khuyến nghị phù hợp về mặt chính sách, pháp luật và thực thi pháp luật tới các cơ quan hữu quan ở trung ương và địa phương nhằm cải thiện việc bảo vệ dữ liệu cá nhân trên các giao diện tương tác giữa chính quyền và người dân trên mạng Internet. Việc đánh giá được thực hiện trên hai phương diện: (i) các chính sách bảo vệ quyền riêng tư của chính quyền địa phương ban hành (có nêu rõ cơ quan chịu trách nhiệm bảo vệ quyền riêng tư; những loại thông tin nào được thu thập; thông tin cá nhân được chia sẻ cho cơ quan nào; quyền riêng tư của trẻ em v.v.); (ii) các biện pháp kỹ thuật cụ thể để người dùng thực hiện các quyền của mình như quyền đồng ý hay không; quyền yêu cầu truy cập, chỉnh sửa; quyền hạn chế phạm vi thu thập thông tin.

Đồng thời, dựa trên các nguyên tắc của Liên Hợp quốc (LHQ),[2] báo cáo này đánh giá thực tiễn bảo vệ dữ liệu cá nhân và quyền riêng tư của các địa phương theo sáu tiêu chí: (i) tính công bằng, hợp pháp trong xử lý thông tin cá nhân; (ii) mục đích sử dụng thông tin cá nhân rõ ràng; (iii) tính tương xứng và cần thiết; (iv) nguyên tắc về lưu trữ thông tin; (v) tính minh bạch; và (vi) tính giải trình trong thu thập, xử lý dữ liệu cá nhân.

Thực trạng bảo vệ dữ liệu cá nhân, đảm bảo quyền riêng tư trên các giao diện tương tác giữa chính quyền và người dân trên mạng Internet ở cấp tỉnh

Một số địa phương đã và đang có sự nỗ lực trong xây dựng và triển khai các công cụ khác nhau để bảo vệ dữ liệu cá nhân, và rộng hơn là quyền riêng tư, trên các giao diện tương tác với người dân. Tuy nhiên, nói chung, chính quyền các tỉnh, thành phố chưa quan tâm nhiều đến vấn đề này. Không có địa phương nào thực hiện tốt việc bảo vệ dữ liệu cá nhân, đảm bảo quyền riêng tư trên các phương diện khác nhau, mà chỉ có một số cách làm tốt đối với một số khía cạnh riêng biệt. Chỉ có 4 trong số 63 cổng TTĐT và 3 trong số 63 cổng DVCTT có đăng tải văn bản quy định về bảo vệ dữ liệu cá nhân song với tên gọi chưa thống nhất (ví dụ: chính sách/quy định/thông báo về bảo vệ thông tin cá nhân; chính sách bảo mật; hoặc chính sách về quyền riêng tư).[3] Trong số 50 tỉnh, thành phố có vận hành ƯDTM để tương tác với công dân, 32 địa phương có đăng tải chính sách bảo vệ quyền riêng tư do yêu cầu của Google Play và Apple Store phải làm như vậy đối với ứng dụng.

---

[1] *Trong Báo cáo này, thuật ngữ "dữ liệu cá nhân" và "thông tin cá nhân" hầu hết được sử dụng với ý nghĩa tương đương. Xem định nghĩa cụ thể trong mục về nội dung nghiên cứu, Phần I – Giới thiệu tổng quan về nghiên cứu.*

[2] *Ủy ban cấp cao về quản lý của LHQ, Các nguyên tắc về bảo vệ dữ liệu cá nhân và quyền riêng tư, thông qua tại phiên họp thứ 36 ngày 11/10/2018. Có thể tải về từ: https://archives.un.org/sites/archives.un.org/files/_un-principles-on-personal-data-protection-privacy-hl-cm-2018.pdf*

[3] *Chính sách về quyền riêng tư thuật ngữ tiếng Anh là Privacy policy*

Có thể thấy, các chính sách, công cụ liên quan đến quyền riêng tư trên cổng TTĐT, cổng DVCTT và ƯDTM của các tỉnh, thành phố còn mang tính tự phát, mà chưa xuất phát từ nhận thức rõ ràng về tầm quan trọng của việc bảo vệ quyền riêng tư của công dân. Các địa phương chú ý nhiều đến các yêu cầu kỹ thuật nhằm đảm bảo an toàn, bảo mật của dữ liệu hơn là tính riêng tư của dữ liệu; phòng chống các mối nguy cơ, rủi ro đối với an ninh mạng hơn là quyền riêng tư của người sử dụng ba giao diện tương tác nêu trên. Có thể dễ dàng tiếp cận trực tuyến các văn bản của chính quyền địa phương về an toàn thông tin, nhưng không thể tìm thấy văn bản về bảo vệ dữ liệu cá nhân, đảm bảo quyền riêng tư trên 59 cổng TTĐT và 60 cổng DVCTT. Không chỉ thế, hầu như các giao diện hiện thời chỉ yêu cầu người sử dụng khẳng định thông tin họ cung cấp là chính xác, nhưng lại không có công cụ để người dùng lựa chọn để bảo vệ quyền riêng tư.

Bên cạnh đó, không một chính sách, công cụ nào nói trên đáp ứng đầy đủ yêu cầu của pháp luật liên quan đến quyền riêng tư trên môi trường số theo 17 chỉ tiêu nhỏ mà báo cáo này đánh giá,[4] cũng như theo 6 nguyên tắc của LHQ về bảo vệ dữ liệu cá nhân và quyền riêng tư như đã đề cập ở trên. Cụ thể, trong số 39 chính sách về quyền riêng tư được công khai, 16 chính sách chỉ bằng tiếng Anh, mà không có tiếng Việt, và 22 chính sách thì ngược lại. Những chính sách về quyền riêng tư hiện có trên các giao diện tương tác với công dân ở cấp tỉnh chưa có các điều khoản bảo vệ thông tin, quyền riêng tư của trẻ em; song, lại đưa ra điều khoản để thu thập nhiều loại thông tin vượt quá giới hạn được phép; không viện dẫn cơ sở pháp lý; không nêu rõ mục đích thu thập thông tin cá nhân; không thể hiện rõ quyền được đồng ý/không đồng ý của người dùng đối với việc thu thập thông tin cá nhân; thiếu công cụ để người dùng thực hiện quyền được tiếp cận, yêu cầu chỉnh sửa thông tin, khiếu nại, v.v.

Đặc biệt, trừ một trường hợp ƯDTM của tỉnh Hậu Giang, hầu hết các văn bản về chính sách quyền riêng tư trên các cổng và các ứng dụng thông minh khác đều không xác định rõ mối quan hệ pháp lý giữa cơ quan Nhà nước chịu trách nhiệm chính với người sử dụng các ứng dụng và các Cổng. Do không xác định rõ chủ thể quản lý dữ liệu, trách nhiệm pháp lý đối với dữ liệu cá nhân bị lẫn lộn giữa "cơ quan chủ quản" (Ủy ban nhân dân tỉnh, thành phố), "cơ quan/đơn vị vận hành" (Sở Thông tin và Truyền thông) và doanh nghiệp cung cấp dịch vụ xây dựng giao diện. Chỉ có 1 trong số 39 chính sách về quyền riêng tư được rà soát nêu rõ UBND tỉnh là cơ quan chịu trách nhiệm đối với việc thu thập, lưu trữ dữ liệu cá nhân; còn Sở TTTT là cơ quan thay mặt UBND vận hành, xử lý dữ liệu trên giao diện này. Thực trạng này đáng lưu ý ở chỗ, nó không chỉ tạo ra khoảng trống về trách nhiệm đối với thông tin cá nhân thu thập qua các giao diện nói trên, mà còn không chỉ rõ căn cứ để xác định chủ thể chịu trách nhiệm và xem xét trách nhiệm lưu trữ, quản lý, sử dụng, chia sẻ khối dữ liệu khổng lồ sau khi đã được thu thập từ người dùng qua các giao diện tương tác của chính quyền địa phương.

Ở mức độ tổng quan, nếu đặt việc bảo vệ quyền riêng tư trong toàn bộ quá trình tương tác của chính quyền địa phương với công dân trên môi trường số, có thể nói, các yếu tố đầu vào như cơ sở vật chất, hạ tầng kỹ thuật đã được quan tâm khá nhiều. Tuy nhiên, quá trình thực hiện các chính sách, pháp luật có liên quan đến bảo vệ thông tin, dữ liệu cá nhân của người dùng nói riêng, và quyền riêng tư nói chung cần được cải thiện nhiều hơn nữa. Đặc biệt, kết quả đầu ra gồm mức độ bảo vệ dữ liệu cá nhân và đáp ứng quyền riêng tư của người dân còn chưa được như mục tiêu mong muốn đã đề ra trong Hiến pháp năm 2013, Bộ luật Dân sự năm 2015, Luật An toàn thông tin mạng năm 2015, Luật Công nghệ thông tin năm 2006, Nghị định số 47/2020/NĐ-CP về quản lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước, Nghị định số 64/2007/NĐ-CP về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước, Nghị định số 43/2011/NĐ-CP[5] quy định về việc cung cấp thông tin và DVCTT trên trang TTĐT hoặc cổng TTĐT của cơ quan nhà nước, và Thông tư số 25/2010/TT-BTTTT quy định việc thu thập, sử dụng, chia sẻ thông tin cá nhân và các biện pháp đảm bảo an toàn và bảo vệ thông tin cá nhân trên trang TTĐT hoặc cổng TTĐT của cơ quan nhà nước.

[4] *Xem bảng 17 tiêu chí đánh giá ở phần Phụ lục.*
[5] *Nghị định số 43/2011/NĐ-CP được thay thế bởi Nghị định số 42/2022/NĐ-CP (ban hành ngày 24 tháng 6 năm 2022)*

Một số khuyến nghị

Hoàn thiện khung pháp luật quốc gia

Ở tầm quốc gia, các văn bản quy phạm pháp luật có liên quan cần điều chỉnh một số vấn đề sau đây liên quan đến bảo vệ dữ liệu cá nhân, quyền riêng tư:

Một là, cần xác định, phân loại rõ ràng dữ liệu cá nhân phù hợp với các xu hướng mới của chuyển đổi số, trong đó có các loại dữ liệu cá nhân được thu thập từ người sử dụng trên các giao diện tương tác của chính quyền. Đồng thời, cần phân biệt giữa tính riêng tư của dữ liệu và an toàn bảo mật dữ liệu, theo đó tính riêng tư quan tâm bảo vệ quyền riêng tư của người dân, còn an toàn bảo mật dữ liệu chú trọng bảo vệ hệ thống công nghệ thông tin và an ninh của cơ quan Nhà nước qua các công cụ kỹ thuật.

Hai là, cần phân biệt rõ ràng giữa chủ thể kiểm soát dữ liệu và chủ thể xử lý dữ liệu, từ đó xác định rõ trách nhiệm pháp lý của các chủ thể đó đối với chủ thể dữ liệu cá nhân. Cần thiết lập chế độ trách nhiệm pháp lý mặc nhiên của cơ quan Nhà nước khi đăng tải văn bản tuyên bố chính sách về quyền riêng tư của mình; hoặc khi họ cung cấp công cụ cho người dân thực hiện quyền của mình, ví dụ như quyền đồng ý hoặc không đồng ý cung cấp thông tin cá nhân trên ứng dụng thông minh. Tương tự, cần làm rõ mối quan hệ pháp lý giữa cơ quan Nhà nước thu thập dữ liệu cá nhân với doanh nghiệp cung cấp giao diện tương tác trên môi trường số.

Ba là, xác định rõ trách nhiệm của các cơ quan liên quan và chuẩn hóa quy trình, thủ tục minh bạch trong sử dụng, chia sẻ dữ liệu cá nhân trong các cơ quan Nhà nước và với các chủ thể bên ngoài. Điều này đặc biệt quan trọng trong bối cảnh một khối dữ liệu cá nhân khổng lồ được thu thập qua các giao diện tương tác của chính quyền với người dân, kéo theo mối quan tâm lớn để làm sao đảm bảo khối dữ liệu đó được bảo vệ, quyền riêng tư được đảm bảo trong quá trình lưu trữ, sử dụng, chia sẻ sau đó.

Bốn là, hoàn thiện các quy định liên quan đến xử lý vi phạm trong quá trình các cơ quan Nhà nước, cán bộ, công chức Nhà nước xử lý dữ liệu cá nhân, bao gồm: xác định rõ ràng, cụ thể các hành vi vi phạm kèm theo mức phạt phù hợp, kể cả bồi thường Nhà nước; quy trình, thủ tục xử lý vi phạm về mặt hành chính, hình sự, dân sự; cơ quan hoặc đơn vị đầu mối tiếp nhận, xử lý ban đầu các yêu cầu, khiếu nại liên quan đến dữ liệu cá nhân.

Năm là, đạo luật có liên quan cần có quy định về nhân sự phụ trách bảo vệ dữ liệu cá nhân và quyền riêng tư trong hoạt động của các cơ quan Nhà nước, ít nhất ở cấp tỉnh; công bố thông tin về nhân sự này để người dân liên hệ khi cần thiết. Người này có nhiệm vụ tham mưu cho lãnh đạo cơ quan Nhà nước về những vấn đề bảo vệ dữ liệu cá nhân và quyền riêng tư; theo dõi việc tuân thủ các quy định pháp luật, chuẩn mực chung và quy tắc nội bộ về bảo vệ dữ liệu cá nhân và quyền riêng tư; kết nối chủ thể dữ liệu với cơ quan Nhà nước kiểm soát dữ liệu.

Sáu là, trên phạm vi toàn quốc, để đạt được sự đồng nhất giữa các tỉnh/thành phố trong thực tiễn bảo vệ quyền riêng tư trên môi trường số, cần liên tục đánh giá, nghiên cứu các thông lệ, cách làm tốt, từ đó khái quát thành các quy định, hướng dẫn cụ thể để các địa phương nắm bắt được các chuẩn mực, dễ dàng bám sát, tuân theo; tạo cơ sở pháp lý để các tỉnh bảo vệ quyền riêng tư tốt hơn trên môi trường số. Bộ TTTT có thể chủ trì xây dựng các văn bản mẫu cho các cơ quan chính quyền địa phương sử dụng trong quá trình cung cấp các DVCTT, bảo đảm quyền riêng tư, bảo vệ dữ liệu cá nhân. Đó là Quy chế mẫu về quyền riêng tư; Thỏa thuận sử dụng mẫu; hoặc, Hợp đồng mẫu trong cung cấp các giao diện tương tác của chính quyền với người dân.

Cải thiện việc bảo vệ dữ liệu cá nhân và quyền riêng tư trên môi trường số của chính quyền địa phương

Trường hợp của các tỉnh/thành phố thực hiện tốt bảo vệ quyền riêng tư cho thấy, cần chú ý đến tất cả các yêu cầu: xây dựng các quy tắc của địa phương; chú trọng quá trình thực hiện; đáp ứng quyền, lợi ích của người dân. Các chính sách bảo vệ quyền riêng tư, các công cụ thực tế để thực hiện các chính sách đó trên các giao diện tương tác của chính quyền cần bám sát, đáp ứng tất cả các yêu cầu theo 17 nội dung pháp luật Việt Nam quy định mà báo cáo này đã đánh giá. Trong đó, cần chú ý xác định rõ chủ thể chịu trách nhiệm chính; các công cụ/kênh tiếp nhận ý kiến, khiếu nại về các vi phạm quyền riêng tư, phản hồi của người dân về chất lượng, hiệu quả của việc bảo vệ quyền riêng tư.

Đặc biệt, nghiên cứu này nhấn mạnh tầm quan trọng của việc đáp ứng quyền, lợi ích của người dân ở địa phương – là những người sử dụng các dịch vụ, sản phẩm, công cụ trên các cổng TTĐT, cổng DVCTT và các ƯDTM do chính quyền đưa vào sử dụng. Mức độ đáp ứng có thể được đánh giá dựa trên các tiêu chí của LHQ về bảo vệ dữ liệu cá nhân, quyền riêng tư. Qua đó, chính quyền địa phương các tỉnh/thành phố có thể nhận biết những yếu tố cần điều chỉnh, cải thiện để dữ liệu cá nhân, quyền riêng tư được bảo vệ tốt hơn. Cụ thể là, chính quyền địa phương có thể xây dựng các biện pháp, công cụ cụ thể để đảm bảo tính chính danh, hợp pháp trong xử lý thông tin cá nhân; thu thập, sử dụng thông tin cá nhân với mục đích rõ ràng; thu thập thông tin cá nhân một cách tương xứng với mục đích, căn cứ trên sự cần thiết; nêu rõ về thời hạn lưu trữ thông tin; tăng tính minh bạch, tính giải trình trong thu thập, xử lý, lưu trữ, sử dụng thông tin cá nhân.

Khuyến nghị về đánh giá việc bảo vệ dữ liệu cá nhân và quyền riêng tư trên môi trường số của các cấp chính quyền

Báo cáo khuyến nghị cần mở rộng hơn cách tiếp cận trong đánh giá việc bảo vệ thông tin, dữ liệu cá nhân và quyền riêng tư trên môi trường điện tử, môi trường số của chính quyền nói chung, cũng như chính quyền địa phương nói riêng. Báo cáo khuyến nghị xem xét bổ sung các chỉ số, chỉ tiêu quan trọng về bảo vệ dữ liệu cá nhân, quyền riêng tư vào mục tiêu chuyển đổi số quốc gia, đồng thời bổ sung các tiêu chí đánh giá việc bảo vệ dữ liệu cá nhân vào bộ Chỉ số chuyển đổi số Việt Nam (DTI) của Bộ TTTT, để bảo đảm chuyển đổi số được thành công cả về chất và lượng, đặc biệt, đạt được mục tiêu cuối cùng là bảo đảm quyền, lợi ích của người dân.

Đồng thời, có thể đầu tư nguồn lực lớn hơn để tiến hành khảo sát, tìm hiểu, đánh giá sâu hơn về thực tiễn bảo vệ dữ liệu cá nhân, quyền riêng tư không chỉ trên các cổng TTĐT, cổng DVCTT, các ƯDTM, mà còn trong các cơ sở dữ liệu do các cơ quan Nhà nước quản lý, nơi dữ liệu cá nhân được lưu trữ, sử dụng, chia sẻ sau khi được thu thập từ các giao diện tương tác với người dân của chính quyền.

I. GIỚI THIỆU TỔNG QUAN VỀ NGHIÊN CỨU

TỔNG QUAN PHƯƠNG PHÁP NGHIÊN CỨU

ĐÁNH GIÁ VIỆC BẢO VỆ DỮ LIỆU CÁ NHÂN TRÊN CÁC GIAO DIỆN TƯƠNG TÁC VỚI NGƯỜI DÂN CỦA CHÍNH QUYỀN ĐỊA PHƯƠNG

MỤC TIÊU NGHIÊN CỨU

Đánh giá thực trạng việc bảo vệ dữ liệu cá nhân trên các giao diện tương tác với người dân của chính quyền cấp tỉnh

PHẠM VI ĐÁNH GIÁ

* Chỉ đánh giá đối với thông tin công khai tiếp cận được. Không đánh giá toàn bộ dữ liệu cá nhân khu vực công

3 NỀN TẢNG

63 **Cổng thông tin điện tử tỉnh/thành phố trực thuộc trung ương**

78 kênh thu thập dữ liệu cá nhân qua **3** chuyên mục: (i) Hỏi đáp
(ii) Phản ánh kiến nghị
(iii) Lấy ý kiến xây dựng văn bản quy phạm pháp luật

63 **Cổng dịch vụ công trực tuyến**

50 **Ứng dụng thông minh**

Hỗ trợ tương tác giữa chính quyền với người dân
50 tỉnh/thành phố trực thuộc trung ương

ĐỐI TƯỢNG ĐÁNH GIÁ

1 **Chính sách về quyền riêng tư (Privacy Policy)**

2 **Công cụ kỹ thuật để bảo vệ dữ liệu cá nhân**

VỚI 17 TIÊU CHÍ

14 **Tiêu chí đánh giá chính sách về quyền riêng tư**

1. Bảo đảm **tính sẵn có** của các **chính sách về quyền riêng tư**
2. Bảo đảm **mức độ thân thiện của ngôn ngữ** với người dùng
3. Dẫn chiếu **cơ sở pháp lý** để thu thập và xử lý dữ liệu cá nhân
4. Xác định **trách nhiệm của cơ quan nhà nước** đối với việc bảo đảm quyền riêng tư dữ liệu của người dùng
5. Xác định **chủ thể dữ liệu** và các quyền tương ứng
6. Làm rõ thông tin cá nhân người dùng sẽ được **chia sẻ với ai**
7. Bảo đảm **quyền riêng tư của trẻ em**
8. Liệt kê và làm rõ **các loại thông tin cá nhân được thu thập**
9. Mô tả những **mục đích** thu thập và xử lý thông tin cá nhân
10. Thông báo về **thời gian lưu trữ** thông tin cá nhân
11. Thông báo về **rủi ro** quyền riêng tư và các **biện pháp** để ngăn chặn
12. Cam kết **thông báo về những thay đổi/cập nhật** trong chính sách về quyền riêng tư
13. Cung cấp **thông tin liên hệ** đối với các câu hỏi, yêu cầu, khiếu nại về thông tin cá nhân
14. Nêu rõ **thời hạn trả** lời các câu hỏi, yêu cầu, khiếu nại từ chủ thể dữ liệu

3 **Tiêu chí đánh giá công cụ kỹ thuật để bảo vệ dữ liệu cá nhân**

1. Quyền được **đồng ý và được biết**
2. Quyền **hạn chế phạm vi** sử dụng thông tin cá nhân
3. Quyền **đặt câu hỏi, yêu cầu truy cập/sửa chữa/xóa và gửi khiếu nại**

1.1. Bối cảnh nghiên cứu

Bảo vệ dữ liệu cá nhân và quyền riêng tư trong xu thế phát triển chính phủ số

Quyền bảo mật dữ liệu cá nhân, quyền bảo vệ thông tin cá nhân, quyền riêng tư được công nhận và quy định theo khuôn khổ pháp lý bảo vệ dữ liệu của Việt Nam hiện nay. Hiến pháp năm 2013 (tại Điều 21) đã quy định quyền riêng tư, bí mật cá nhân và bí mật gia đình, bảo vệ thông tin cá nhân là bất khả xâm phạm. Bộ luật Dân sự năm 2015 (tại Điều 38) coi sự đồng ý của một cá nhân là điều kiện tiên quyết để thu thập, lưu giữ, sử dụng và công bố thông tin về cuộc sống riêng tư của người đó. Bên cạnh đó, Luật Trẻ em năm 2016 (tại Khoản 11, Điều 6); Luật Giao dịch điện tử năm 2005 (tại Khoản 2 Điều 46); Luật An ninh mạng năm 2018 (tại Điều 17), cũng như các luật chuyên ngành khác đều đưa ra các quy định tương tự về bảo vệ dữ liệu cá nhân.

Đồng thời, Chính phủ Việt Nam đã cam kết tăng cường tiếp cận thông tin và cải thiện chất lượng dịch vụ công thông qua chuyển đổi số khu vực công. Cam kết này được thể hiện qua hai văn bản: (1) Quyết định số 749/QĐ-Ttg ngày 03/06/2020 phê duyệt "Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030" và (2) Quyết định số 942/QĐ-TTg ngày 15/06/2021 về "Chiến lược phát triển Chính phủ điện tử hướng tới Chính phủ số giai đoạn 2021 - 2025, định hướng đến năm 2030". Hai văn bản quan trọng này khẳng định chuyển đổi số là ưu tiên hàng đầu của quốc gia, trong đó đề ra các mục tiêu cụ thể được liệt kê trong Hộp 1.

Hộp 1: Định hướng và mục tiêu chuyển đổi số quốc gia đến 2030

Quyết định số 749/QĐ-Ttg ngày 03/06/2020 phê duyệt "Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030":

- 90% hồ sơ công việc tại cấp bộ, tỉnh; 80% hồ sơ công việc tại cấp huyện và 60% hồ sơ công việc tại cấp xã được xử lý trên môi trường mạng (trừ hồ sơ công việc thuộc phạm vi bí mật nhà nước).
- 100% cơ sở dữ liệu quốc gia được hoàn thành, kết nối và chia sẻ trên toàn quốc.

Quyết định số 942/QĐ-TTg ngày 15/06/2021 của Thủ tướng Chính phủ về "Chiến lược phát triển Chính phủ điện tử hướng tới Chính phủ số giai đoạn 2021 - 2025, định hướng đến năm 2030":

- 100% thủ tục hành chính đủ điều kiện theo quy định của pháp luật được cung cấp dưới hình thức dịch vụ công trực tuyến mức độ 4.
- 100% dịch vụ công trực tuyến được thiết kế, thiết kế lại nhằm tối ưu hóa trải nghiệm người dùng, khi sử dụng được điền sẵn dữ liệu mà người dùng đã cung cấp trước đó theo thỏa thuận, phù hợp với tiêu chuẩn chất lượng dịch vụ.
- 100% người dân và doanh nghiệp sử dụng dịch vụ công trực tuyến được định danh và xác thực thông suốt, hợp nhất trên tất cả các hệ thống của các cấp chính quyền từ trung ương đến địa phương.
- Tối thiểu 80% hồ sơ thủ tục hành chính được xử lý hoàn toàn trực tuyến, người dân chỉ phải nhập dữ liệu một lần.
- 100% cơ quan nhà nước cấp bộ, tỉnh tham gia mở dữ liệu và cung cấp dữ liệu mở phục vụ phát triển Chính phủ số, kinh tế số, xã hội số.

Quyết định số 06/QĐ-TTg ngày 06/01/2022 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 2030:

- Hoàn thành tích hợp, cung cấp dịch vụ xác thực thông tin về số Chứng minh nhân dân (9 số) với Căn cước công dân trên Cổng Dịch vụ công quốc gia để 100% tài khoản định danh điện tử của cá nhân đã được tạo lập bởi Cổng Dịch vụ công quốc gia, Cổng Dịch vụ công cấp bộ, cấp tỉnh thực hiện được việc xác thực với danh tính điện tử do Bộ Công an cung cấp.

Một trong những mấu chốt của việc phát triển chính phủ điện tử là phải tập hợp một giao diện dữ liệu công thống nhất. Kể từ năm 2015, Việt Nam đã nỗ lực gia tăng mức độ sẵn có của dữ liệu (data availability) bằng cách triển khai 6 cơ sở dữ liệu quốc gia, bao gồm: Cơ sở dữ liệu quốc gia về dân cư, Cơ sở dữ liệu đất đai quốc gia, Cơ sở dữ liệu quốc gia về đăng ký doanh nghiệp, Cơ sở dữ liệu quốc gia về thống kê tổng hợp về dân số, Cơ sở dữ liệu quốc gia về tài chính, và Cơ sở dữ liệu quốc gia về bảo hiểm.[6] Bên cạnh đó, Bộ TTTT đã xây dựng, đưa Giao diện tích hợp, chia sẻ dữ liệu quốc gia (NDXP-National Data Exchange Platform) vào sử dụng, kết nối với hơn 90 bộ, ngành, địa phương, doanh nghiệp, với 10 Cơ sơ sở dữ liệu, 08 hệ thống thông tin. Trong năm 2021, Giao diện đã đạt 180.919.031 giao dịch dữ liệu,[7] với khoảng 500 nghìn giao dịch mỗi ngày, giúp hạn chế kê khai thông tin nhiều lần, tăng cường sử dụng lại dữ liệu.[8]

Đồng thời, nhu cầu kết nối, chia sẻ, giao dịch dữ liệu từ khu vực công gia tăng. Ngày 26/04/2022, Thủ tướng Chính phủ ban hành Chỉ thị số 2/CT-TTg về về Phát triển Chính phủ điện tử hướng tới Chính phủ số, thúc đẩy chuyển đổi số quốc gia, xác định vấn đề chia sẻ dữ liệu là một trong những "điểm nghẽn" quan trọng cần tập trung tháo gỡ để phát triển Chính phủ điện tử, Chính phủ số. Đồng thời, đưa ra yêu cầu công khai danh mục cơ sở dữ liệu dùng chung, và đặc biệt là danh mục các dịch vụ chia sẻ dữ liệu. Tuy nhiên, để có thể chia sẻ dữ liệu thông suốt, hiệu quả, công tác bảo vệ dữ liệu cá nhân, bảo đảm quyền riêng tư của công dân là điều kiện tiên quyết.

Rủi ro đối với lộ lọt dữ liệu cá nhân trong khu vực công ở Việt Nam

Quá trình số hóa thông tin và các dịch vụ công dẫn tới các dữ liệu cá nhân nhạy cảm của công dân được thu thập và tập trung trên không gian số. Điều này có thể gây ra những rủi ro về an toàn dữ liệu và bảo vệ dữ liệu cá nhân (xem ví dụ ở Hộp 2). Chẳng hạn, xu hướng này thể hiện rõ trong giai đoạn đầu của đại dịch COVID-19, khi các phương tiện thông tin đại chúng và chính quyền thường tiết lộ thông tin cá nhân của người mắc COVID-19 bao gồm tên, địa chỉ, dữ liệu y tế và các mối quan hệ riêng tư. Còn theo thống kê của Bộ Công an, từ tháng 5 năm 2020 đến tháng 5 năm 2021, cả nước xảy ra gần 2.500 vụ lừa đảo trên không gian mạng, trong đó có 527 vụ việc đối tượng giả danh cơ quan tư pháp để lừa đảo, chiếm đoạt tài sản của người dân.[9] Bên cạnh đó, Bộ Công an cũng đưa ra cảnh báo về nguy cơ cổng TTĐT, website của cơ quan nhà nước bị các đối tượng mạo danh để lừa đảo, chiếm đoạt tài sản.[10] Mặc dù vẫn chưa chứng minh được mối liên hệ nhân quả giữa các vụ lừa đảo và hành vi xâm phạm dữ liệu cá nhân, nhưng có vẻ như hành vi trộm cắp danh tính,[11] liên quan đến việc làm giả hoặc sử dụng dữ liệu cá nhân sai mục đích, đang gia tăng. Trong bối cảnh các cơ sở dữ liệu dân cư quốc gia trở thành xương sống cho các giao dịch kỹ thuật số trong khu vực công, thì hành vi trộm cắp danh tính còn có thể gây ra nhiều tác động nghiêm trọng hơn.

---

[6] *Quyết định số 714/QĐ-TTg, ngày 22/05/2015 của Thủ tướng chính phủ ban hành Danh mục cơ sở dữ liệu quốc gia cần ưu tiên triển khai tạo giao diện phát triển chính phủ điện tử.*

[7] *Giao dịch dữ liệu là các giao dịch chia sẻ, sử dụng, kết nối dữ liệu.*

[8] *Công văn số 677/BTTTT-THH 2022 kết nối dữ liệu thông qua giao diện tích hợp*

[9] *Xem chi tiết tại bài viết "Mạo danh cơ quan điều tra để chiếm đoạt tài sản: Vì sao nhiều người sập bẫy?", truy cập tại: https://vov.vn/phap-luat/mao-danh-co-quan-dieu-tra-de-chiem-doat-tai-san-vi-sao-nhieu-nguoi-sap-bay-900621.vov*

[10] *Xem chi tiết tại bài viết "Giả danh website các cơ quan nhà nước để lừa đảo", truy cập tại: https://vtv.vn/kinh-te/gia-danh-website-cac-co-quan-nha-nuoc-de-lua-dao-20220714011026472.htm*

[11] *Hành vi trộm cắp danh tính (tiếng Anh là identity theft) là khi ai đó thu thập thông tin cá nhân của một chủ thể khác với mục đích thường là mạo danh, lừa đảo, đánh cắp tiền. Một ví dụ tiêu biểu cho hành vi trộm cắp danh tính chính là trộm cắp danh tính liên quan đến thuế, xảy ra khi ai đó đánh cắp thông tin cá nhân để thực hiện hành vi gian lận thuế. Tiền thuế của chủ thể bị trộm cắp danh tính có thể bị ảnh hưởng nếu số An sinh xã hội của chủ thể đó được sử dụng để khai báo gian lận, hoặc để yêu cầu tiền hoàn thuế, hoặc tín thuế. Một điển hình khác là khi một cá nhân có thể bị ngân hàng từ chối mở tài khoản vì căn cước công dân đã được dùng để mở một tài khoản không chính chủ khác. Tham khảo nguồn định nghĩa identity theft tại: https://www.investopedia.com/terms/i/identitytheft.asp*

Hộp 2: Trường hợp sử dụng sai mục đích dữ liệu cá nhân thu thập từ kênh phản ánh kiến nghị trực tuyến trên cổng TTĐT tỉnh Đồng Tháp

Ngày 19/05/2020, Chủ tịch UBND tỉnh Đồng Tháp ban hành Công văn 21/UBND-KSTTHC về phòng ngừa việc sử dụng thông tin cá nhân của người phản ánh, kiến nghị qua Tổng đài 1022 không đúng mục đích. Trong quá trình xử lý các phản ánh, kiến nghị, có những báo cáo về các hành vi sử dụng thông tin của người phản ánh, kiến nghị không đúng mục đích, ảnh hưởng đến cá nhân của người phản ánh, kiến nghị và quá trình giải quyết các phản ánh, kiến nghị này. Do đó, Chủ tịch UBND tỉnh Đồng Tháp yêu cầu các cơ quan, đơn vị, địa phương nâng cao ý thức về quản lý thông tin cá nhân của người phản ánh kiến nghị và dữ liệu phản ánh, kiến nghị trên Tổng đài 1022 và yêu cầu đơn vị cho thuê và khai thác hạ tầng Tổng đài 1022 (VNPT Đồng Tháp) đảm bảo các điều kiện kỹ thuật để bảo mật dữ liệu từ các dịch vụ công và thông tin cá nhân của người phản ánh kiến nghị.

Nguồn: *Cổng thông tin điện tử Đồng Tháp, 19/05/2020*

Trong khi Chính phủ Việt Nam nỗ lực chống hoạt động thương mại hóa dữ liệu cá nhân bất hợp pháp ở khu vực tư nhân thì ở khối công, việc bảo vệ dữ liệu cá nhân trên các giao diện tương tác giữa chính quyền và người dân như các cổng TTĐT, cổng DVCTT, hay các ƯDTM ít được quan tâm. Đơn cử, cổng TTĐT thành phố Đà Nẵng <hoidap.danang.gov.vn> hiện đang công khai các thông tin cá nhân như họ và tên, địa chỉ nhà riêng, số an sinh xã hội của công dân (xem Hình 1). Điều này là đáng quan ngại khi xem xét nguy cơ bị đánh cắp danh tính nhằm mục đích lừa đảo như những trường hợp được ghi nhận ở trên.

Hình 1: Ví dụ về hiện trạng tiết lộ thông tin cá nhân trên kênh hỏi đáp trực tuyến của chính quyền địa phương

Rủi ro đối với lộ lọt dữ liệu cá nhân trong khu vực công đang trở thành một nguy cơ hiện hữu không chỉ ở Việt Nam mà còn trên thế giới. Theo "Báo cáo về phí tổn do lộ lọt dữ liệu năm 2021"[12] của IBM, khu vực công đã chứng kiến một sự gia tăng đáng kể trong chi phí do vi phạm dữ liệu, với mức tăng 78,7% trong tổng chi phí trung bình từ 1,08 triệu lên 1,93 triệu đô la từ năm 2020 đến năm 2021. Thông tin nhận dạng cá nhân của khách hàng được cho là loại dữ liệu bị xâm phạm phổ biến nhất, chiếm 44% hồ sơ bị đánh cắp, đồng thời cũng là loại vi phạm dữ liệu tốn kém nhất với trung bình 180 đô la cho mỗi hồ sơ bị mất.

[12] *Xem chi tiết tại: https://www.ibm.com/security/data-breach*

Khoảng trống trong nghiên cứu

Tại sao cần tiến hành nghiên cứu về thực tiễn thực hiện bảo vệ dữ liệu cá nhân (từ đây gọi tắt BVDLCN) của chính quyền cấp tỉnh?

- Chưa có một chỉ số đánh giá toàn diện việc thực hành BVDLCN trên các cổng thông tin trực tuyến và ứng dụng tương tác với người dân của chính quyền cấp tỉnh. Hầu hết các chỉ số hiện có tập trung vào đánh giá hiệu quả thực hiện chính phủ điện tử, trong đó BVDLCN chỉ là một thành phần nhỏ, thường được bao hàm trong khái niệm "an toàn, an ninh thông tin". Do đó, rất khó để đánh giá hiệu quả hoạt động BVDLCN trong khu vực công và đưa ra các khuyến nghị phù hợp. Đây sẽ là đánh giá đầu tiên của loại hình này ở cấp chính quyền địa phương, cụ thể là cấp tỉnh tại Việt Nam.

- Các chỉ số hiện tại tập trung vào việc đánh giá năng lực của chính quyền cấp tỉnh trong việc cung cấp các dịch vụ điện tử, chứ chưa đánh giá việc tôn trọng bảo vệ các quyền của công dân (chẳng hạn như quyền tiếp cận các dịch vụ công, quyền bảo vệ dữ liệu cá nhân). Chưa có nghiên cứu đánh giá một cách hệ thống góc nhìn và trải nghiệm về BVDLCN của người dân – những người sử dụng cổng TTĐT, cổng DVCTT, hay các ƯDTM do chính quyền triển khai thực hiện. Nghiên cứu này sẽ đánh giá việc thực hiện các quyền đối với dữ liệu cá nhân của công dân trên các kênh tương tác trên môi trường trực tuyến của chính quyền cấp tỉnh.

- Mức độ hiểu biết và nhận thức về BVDLCN giữa các chính quyền địa phương là khác nhau. Vì vậy, cần tiến hành nghiên cứu này để có cơ sở đánh giá việc thực hiện BVDLCN và ghi lại các thông lệ tốt để xây dựng hướng dẫn quốc gia về BVDLCN trong khu vực công.

Do vậy, nghiên cứu này sẽ đánh giá thực trạng quản lý dữ liệu cá nhân thể hiện trên giao diện trực tuyến của các cơ quan nhà nước ở 63 tỉnh, thành phố với các mục tiêu:

1) Rà soát các quy định pháp luật liên quan đến bảo vệ DLCN và quyền riêng tư trên các giao diện trực tuyến của các cơ quan chính quyền địa phương.

2) Đánh giá hiện trạng thực thi pháp luật và thực hành bảo vệ DLCN trên các giao diện tương tác trực tuyến giữa chính quyền địa phương với người dân. Qua đó ghi nhận các thông lệ tốt, giúp định hướng xây dựng các tiêu chuẩn, hướng dẫn trên toàn quốc về bảo vệ DLCN trong khu vực công; đồng thời nhận diện những khoảng trống pháp lý liên quan đến vấn đề này cần được hoàn thiện.

3) Khuyến nghị các giải pháp nâng cao hiệu quả thực hành bảo vệ DLCN ở cấp độ chính quyền địa phương; hoàn thiện khung chính sách, pháp luật quốc gia về bảo vệ dữ liệu cá nhân và quyền riêng tư.

4) Đảm bảo quyền riêng tư về dữ liệu cá nhân được các chính quyền các cấp tôn trọng như một quyền con người; nâng cao nhận thức của các cơ quan nhà nước bảo vệ dữ liệu cá nhân trên môi trường số.

1.2. Nội dung và phương pháp nghiên cứu

Nghiên cứu này tập trung đánh giá việc bảo vệ dữ liệu cá nhân, bảo đảm quyền riêng tư trên các giao diện[13] tương tác của chính quyền cấp tỉnh với người dân, gồm cổng TTĐT; cổng DVCTT; ƯDTM.

Dữ liệu, thông tin cá nhân

Trên thế giới, mà cụ thể giữa Mỹ và châu Âu đang có hai cách tiếp cận trong định nghĩa về dữ liệu, thông tin cá nhân. Nói chung, ở châu Âu, dữ liệu cá nhân (personal data) có ý nghĩa mở rộng hơn so với thông tin cá nhân (personally identifiable information – PII) ở Mỹ.[14]

---

[13] Theo Nghị định số 42/2022/NĐ-CP (ngày 24/6/2022), kênh cung cấp thông tin và dịch vụ công trực tuyến của cơ quan nhà nước trên môi trường mạng (sau đây gọi là kênh cung cấp) là "kênh giao tiếp trên môi trường mạng được cơ quan nhà nước xác định và quản lý để kiểm soát việc cung cấp thông tin và dịch vụ công trực tuyến cho tổ chức, cá nhân." Theo đó, có 02 loại là kênh cung cấp thông tin và kênh cung cấp dịch vụ công trực tuyến. Trong báo cáo này, chúng tôi thống nhất gọi cổng TTĐT, cổng DVCTT, và các ƯDTM là ba kênh giao diện (tiếng Anh dùng từ interface) tương tác của chính quyền với người dân.

[14] IPS, Báo cáo thảo luận chính sách về bảo vệ dữ liệu cá nhân và quyền riêng tư trong bối cảnh nền kinh tế số, Hà Nội, 2020

Cụ thể, theo định nghĩa của Bộ Thương mại Mỹ, PII là những thông tin "có thể sử dụng để phân biệt hay nhận dạng một cá nhân như tên, số an sinh xã hội, hồ sơ sinh trắc, v.v. nói riêng, hoặc khi kết hợp với các thông tin cá nhân hay thông tin nhận dạng khác liên quan hoặc có thể liên quan với một người cụ thể như ngày và nơi sinh, tên khai sinh của mẹ".[15] Ở châu Âu, Quy định chung về bảo vệ dữ liệu (GDPR) định nghĩa về dữ liệu cá nhân là "bất kể thông tin gì liên quan đến một cá nhân đã được nhận dạng (identified person) hoặc có thể được nhận dạng (identifiable person); một cá nhân có thể được nhận dạng là người có thể được nhận dạng trực tiếp hay gián tiếp bằng việc tham chiếu số định danh hay một hoặc các yếu tố riêng về vật lý, sinh lý, tâm thần, kinh tế, văn hoá và xã hội".

Dù theo cách nào, dữ liệu/thông tin cá nhân là thông tin cho phép xác định/nhận dạng trực tiếp hoặc gián tiếp một con người cụ thể. Dữ liệu cá nhân được chia thành hai loại: (i) dữ liệu cá nhân cơ bản gồm những thông tin cụ thể cho phép xác định trực tiếp danh tính một con người như: tên, tuổi, giới tính, dân tộc, v.v.; và, (ii) dữ liệu cá nhân nhạy cảm gồm những thông tin liên quan trực tiếp đến quyền cơ bản và tự do của con người và khi xử lý những thông tin này có thể tạo ra rủi ro đối với quyền này, tác động đến danh dự, nhân phẩm của con người như quan điểm chính trị, quan điểm tôn giáo, tình trạng đời sống tình dục, đặc điểm di truyền học, v.v.[16] Thuật ngữ "dữ liệu cá nhân" theo nghĩa như vậy cũng được sử dụng trong dự thảo Nghị định quy định về bảo vệ dữ liệu cá nhân.[17]

Bên cạnh đó, hiện nay thuật ngữ "thông tin cá nhân" được sử dụng trong các văn bản quy phạm pháp luật có liên quan của Việt Nam.[18] "Thông tin cá nhân" có thể hiểu theo nghĩa rộng tại Khoản 15, Điều 3, Luật An toàn thông tin mạng, định nghĩa thông tin cá nhân là thông tin liên quan đến việc xác định danh tính của một cá nhân, hoặc cụ thể như trong Nghị định số 64/2007/NĐ-CP (Khoản 5, Điều 3) và Thông tư số 25/2010/TT-BTTTT (Khoản 3, Điều 3), trong đó xác định thông tin cá nhân là thông tin đủ để xác định danh tính của một cá nhân, bao gồm ít nhất một trong các thông tin như họ tên, ngày sinh, nghề nghiệp, chức danh, địa chỉ liên lạc, email, số điện thoại, số định danh cá nhân (ID), số hộ chiếu; thông tin liên quan đến bí mật cá nhân như hồ sơ sức khỏe, hồ sơ thuế, số an sinh xã hội, số tín dụng và các bí mật cá nhân khác.[19]

Mặt khác, Điều 5, Thông tư số 25/2010/TT-BTTTT quy định, hình thức thu thập thông tin cá nhân như (1) do người sử dụng cung cấp khi sử dụng dịch vụ công trực tuyến hoặc (2) được thu thập tự động trong quá trình người sử dụng truy cập cổng TTĐT. Theo ngôn ngữ của Điều 5, Thông tư số 25/2010/TT-BTTTT, thông tin cá nhân được bảo vệ và điều chỉnh vượt ra ngoài định nghĩa hẹp của Nghị định số 64/2007/NĐ-CP, tương đồng nhiều hơn với định nghĩa rộng trong Luật An ninh mạng.
Xét trong bối cảnh quá trình số hóa đang diễn ra mạnh mẽ hiện nay, nghiên cứu này sẽ đánh giá việc BVDLCN dựa trên định nghĩa rộng về thông tin cá nhân của pháp luật Việt Nam. Đồng thời, khi cần thiết, ví dụ như đề xuất kiến nghị, báo cáo này sử dụng thuật ngữ dữ liệu cá nhân và các thuật ngữ liên quan như chủ thể dữ liệu, chủ thể kiểm soát dữ liệu, xử lý dữ liệu v.v.

---

[15] *IPS, Báo cáo thảo luận chính sách về bảo vệ dữ liệu cá nhân và quyền riêng tư trong bối cảnh nền kinh tế số, Hà Nội, 2020*
[16] *IPS, Báo cáo thảo luận chính sách về bảo vệ dữ liệu cá nhân và quyền riêng tư trong bối cảnh nền kinh tế số, Hà Nội, 2020*
[17] *https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Du-thao-Nghi-dinh-quy-dinh-ve-bao-ve-du-lieu-ca-nhan-465185.aspx*
[18] *Gần đây nhất, ngày 24 tháng 6 năm 2022, Chính phủ đã ban hành Nghị định số 42/2022/NĐ-CP (thay thế Nghị định số 43/2011/NĐ-CP) quy định về việc cung cấp thông tin và dịch vụ công trực tuyến của cơ quan nhà nước trên môi trường mạng. Trong đó, Điều 26 có ghi "Cơ quan nhà nước có trách nhiệm cung cấp thông tin và dịch vụ công trực tuyến trên môi trường mạng, bảo đảm an toàn thông tin, bảo vệ thông tin cá nhân và bảo đảm an toàn hệ thống thông tin theo quy định của pháp luật về an toàn thông tin, an ninh mạng."*
[19] *Theo thực tế khảo sát, các chính sách/quy đinh/ thông báo về bảo vệ/ bảo mật thông tin/dữ liệu cá nhân được tìm thấy trên 3 Cổng DVCTT và 4 Cổng TTTT hiện đều đang sử dụng định nghĩa cụ thể này. Trong khi đó, phần đa các chính sách về quyền riêng tư (privacy policy) của các apps lại đang sử dụng định nghĩa rộng.*

Quyền và trách nhiệm của các bên

Với định nghĩa nói trên về thông tin cá nhân, các chủ thể dữ liệu có các quyền:

- Đồng ý sau khi được thông báo.[20]
- Yêu cầu tổ chức, cá nhân lưu trữ thông tin cá nhân của mình trên môi trường mạng thực hiện việc kiểm tra, đính chính hoặc hủy bỏ thông tin đó.[21]
- Yêu cầu cơ quan chủ quản thu thập, lưu trữ và xử lí thông tin cá nhân dừng cung cấp thông tin cá nhân cho bên thứ ba.[22]
- Yêu cầu bồi thường thiệt hại gây ra bởi hành vi vi phạm các quy định về thông tin cá nhân.[23]
- Yêu cầu những cơ quan chủ quản thu thập và xử lí thông tin cá nhân phải cung cấp quyền truy cập tới những thông tin đó.[24]
- Lựa chọn giới hạn nội dung và phạm vi sử dụng thông tin cá nhân.[25]

Trách nhiệm của các cơ quan chủ quản trong thu thập, xử lí và sử dụng thông tin cá nhân bao gồm:

- Nhận được sự đồng ý của chủ thể dữ liệu trước khi thu thập, xử lí và sử dụng thông tin cá nhân của họ, trừ trường hợp pháp luật có quy định khác.[26]
- Thông báo cho chủ thể dữ liệu về hình thức, phạm vi, địa điểm và mục đích của việc thu thập, xử lý và sử dụng thông tin cá nhân của họ;[27] xây dựng và công khai các biện pháp xử lý và bảo vệ thông tin cá nhân trong cơ quan mình;[28] các quy định về đảm bảo an toàn và bảo vệ thông tin cá nhân phải đáp ứng các yêu cầu: nội dung đơn giản, rõ ràng, dễ hiểu, phù hợp với tính chất, quy trình công việc liên quan và không chồng chéo; được tổ chức khoa học, có khả năng in ấn, hiển thị được về sau và có thể truy cập bằng phương pháp trực tuyến; được hiển thị rõ đối với người sử dụng trước thời điểm người sử dụng gửi thông tin cá nhân.[29]
- Chỉ sử dụng thông tin cá nhân cho các mục đích xác định trước và hạn chế lưu trữ thông tin cá nhân theo quy định của pháp luật hoặc thỏa thuận của hai bên.[30]
- Áp dụng các biện pháp quản lý và biện pháp kỹ thuật cần thiết để ngăn chặn thông tin cá nhân không bị mất, đánh cắp, tiết lộ hay thay đổi hoặc bị phá hủy.[31]
- Có các biện pháp cần thiết khi nhận được yêu cầu điều tra, sửa đổi hoặc xóa thông tin cá nhân từ chủ thể dữ liệu; không được cung cấp hoặc sử dụng thông tin cá nhân liên quan cho đến khi cập nhật xong,[32] xử lý các yêu cầu và thông báo cho chủ thể dữ liệu; cung cấp quyền truy cập để chủ thể dữ liệu có thể cập nhật, thay đổi hoặc xóa thông tin cá nhân của họ.
- Phải xóa thông tin cá nhân đã lưu trữ trước đó sau khi mục đích thu thập đã hoàn thành hoặc thời gian lưu trữ đã hết và thông báo cho chủ thể dữ liệu về việc xóa đó, trừ khi pháp luật có quy định khác.[33]
- Cung cấp cơ chế lựa chọn giới hạn nội dung và phạm vi sử dụng thông tin cá nhân.[34]

---

[20] *Khoản 1a, Điều 17, Luật an toàn thông tin mạng năm 2015 năm*
[21] *Khoản 1, Điều 22, Luật Công nghệ thông tin năm 2006*
[22] *Khoản 1, Điều 18, Luật an toàn thông tin mạng năm 2015*
[23] *Khoản 3, Điều 22, Luật Công nghệ thông tin năm 2006*
[24] *Khoản 3, Điều 17, Luật an toàn thông tin mạng năm 2015*
[25] *Khoản 2, Điều 6, Thông tư số 25/2010/TT-BTTTT*
[26] *Khoản 1, Điều 21, Luật Công nghệ thông tin năm 2006; Khoản 1a, Điều 17, Luật an toàn thông tin mạng năm 2015*
[27] *Khoản 2a, Điều 21, Luật Công nghệ thông tin năm 2006*
[28] *Khoản 3, Điều 16, Luật an toàn thông tin mạng Năm 2015*
[29] *Khoản 2, Điều 11, Thông tư số 25/2010/TT-BTTTT*
[30] *Khoản 2b, Điều 21, Luật Công nghệ thông tin năm 2006*
[31] *Điều 19, Luật an toàn thông tin mạng 2015*
[32] *Điều 18, Luật an toàn thông tin mạng 2015*
[33] *Khoản 3, Điều 18, Luật an toàn thông tin mạng năm 2015*
[34] *Điều 6, Thông tư số 25/2010/TT-BTTTT*

Quyền riêng tư

Quyền riêng tư là quyền của mỗi cá nhân được bảo vệ sự bí mật, không tiết lộ, không công khai hoá về đời sống riêng tư của mình. Quyền riêng tư gắn với con người là những cá nhân cụ thể, là chủ sở hữu đối với những gì gắn với bản thân mình, từ tên, tuổi, hình ảnh nhận dạng, cơ thể vật lý đến danh dự, uy tín và bí mật của đời sống riêng tư. Tựu trung, quyền riêng tư có thể được hiểu rằng mỗi cá nhân được độc quyền sở hữu một thế giới riêng bao gồm thân thể, nơi ở, tài sản, tư tưởng, tình cảm, bí mật và bản sắc liên quan đến mình.[35]

Nghiên cứu này tập trung đánh giá thực tiễn việc BVDLCN dưới góc độ bảo đảm quyền riêng tư trên các giao diện tương tác với người dân của chính quyền địa phương. Cụ thể, nghiên cứu đánh giá hai khía cạnh: (i) đánh giá đối với chính sách về quyền riêng tư trên các giao diện tương tác đó; và (ii) đánh giá về các biện pháp kỹ thuật bảo đảm các quyền riêng tư.

(i) Đánh giá đối với chính sách về quyền riêng tư

Trong khuôn khổ nghiên cứu này, chính sách về quyền riêng tư là một tuyên bố hay một văn bản của bên thu thập và xử lý dữ liệu được đăng tải trên cổng TTĐT, cổng DVCTT, các ứng dụng thông minh của chính quyền địa phương. Văn bản này mô tả cách thức cơ quan nhà nước thu thập, sử dụng, chia sẻ, xử lý, lưu trữ, và quản lý thông tin cá nhân của công dân/người dùng. Bởi người dùng sẽ được yêu cầu nhấn nút chấp thuận, đây có thể được xem như một dạng thỏa thuận điện tử giữa các cơ quan nhà nước thu thập thông tin cá nhân và chủ thể dữ liệu (công dân/người dùng). Nghiên cứu này đánh giá các thỏa thuận điện tử đó có thiết lập đầy đủ quyền của chủ thể dữ liệu và trách nhiệm của các cơ quan nhà nước thu thập và xử lý thông tin cá nhân, cũng như cung cấp cơ chế cho các chủ thể dữ liệu thực hành các quyền đối với dữ liệu cá nhân của mình, và yêu cầu các cơ quan nhà nước có trách nhiệm thực hiện các nghĩa vụ tương ứng.

Cụ thể, các chính sách về quyền riêng tư sẽ được đánh giá trên 14 tiêu chí như sau:

1.1. Sự tồn tại của chính sách về quyền riêng tư: Đây là một chỉ số tốt về sự tôn trọng từ các cơ quan nhà nước thu thập thông tin cá nhân đối với các chủ thể dữ liệu.

1.2. Khả năng tiếp cận về mặt ngôn ngữ: Chính sách về quyền riêng tư được cung cấp bằng tiếng Việt, tiếng Anh hay cả hai?

1.3. Cơ sở pháp lý để thu thập dữ liệu cá nhân: Chính sách về quyền riêng tư có viện dẫn các văn bản pháp luật để chủ thể dữ liệu tham khảo hay không?

1.4. Xác định các cơ quan nhà nước chịu trách nhiệm đối với các quyền của chủ thể dữ liệu: Chính sách về quyền riêng tư có xác định chính xác cơ quan nhà nước chịu trách nhiệm đối với các quyền của chủ thể dữ liệu? Trách nhiệm đó có được mô tả rõ ràng?

1.5. Xác định chủ thể dữ liệu: Chính sách về quyền riêng tư có mô tả chủ thể dữ liệu, các quyền của họ?

1.6. Quyền riêng tư của trẻ em: Chính sách về quyền riêng tư có đề cập tới quyền của trẻ em đối với thông tin cá nhân của trẻ hay không?

1.7. Những loại thông tin cá nhân nào được thu thập?

1.8. Có mô tả mục đích thu thập và xử lý thông tin cá nhân?

1.9. Có thông báo về thời gian lưu trữ thông tin cá nhân?

1.10. Có làm rõ thông tin cá nhân sẽ được chia sẻ với ai?

1.11. Có thông báo về rủi ro quyền riêng tư và các biện pháp để ngăn chặn?

1.12. Có cam kết thông báo về những thay đổi/cập nhật chính sách về quyền riêng tư?

1.13. Có thông tin liên hệ để nêu các câu hỏi, yêu cầu, khiếu nại về thông tin cá nhân?

1.14. Thời hạn trả lời các câu hỏi, yêu cầu, khiếu nại từ chủ thể dữ liệu có được nêu rõ?

[35] *IPS, Báo cáo thảo luận chính sách về bảo vệ dữ liệu cá nhân và quyền riêng tư trong bối cảnh nền kinh tế số, Hà Nội, 2020.*

(ii) Đánh giá về thực hiện kỹ thuật

Đồng thời, nghiên cứu này đánh giá cách thức thực hiện các quyền của chủ thể dữ liệu qua các công cụ kỹ thuật tích hợp trong các giao diện trực tuyến trên 3 tiêu chí:

2.1. Quyền được thông báo: Liệu giao diện của các cơ quan nhà nước về mặt kỹ thuật có cung cấp cho các chủ thể dữ liệu cơ hội lựa chọn có đồng ý hay không; liệu sự đồng ý này có được đưa ra với thông tin đầy đủ về phạm vi thu thập, lưu trữ, xử lý, chia sẻ và quản lý thông tin cá nhân dưới dạng liên kết đính kèm với chính sách về quyền riêng tư hay không.

2.2. Quyền hạn chế phạm vi sử dụng thông tin cá nhân: Liệu giao diện của các cơ quan nhà nước về mặt kỹ thuật có cung cấp cơ chế cho các chủ thể dữ liệu cơ hội lựa chọn hạn chế công khai/ẩn danh thông tin cá nhân.

2.3. Quyền đặt câu hỏi, yêu cầu truy cập/sửa chữa/xóa và gửi khiếu nại: Liệu thông tin liên hệ dưới hình thức email được cung cấp có thực sự hoạt động hiệu quả để bảo đảm các quyền của chủ thể dữ liệu.

(Xem cụ thể hơn về 17 nội dung nói trên trong Phụ lục).

Cách tiếp cận, phương pháp nghiên cứu

Cách tiếp cận

Nghiên cứu này áp dụng cách tiếp cận theo quá trình, theo đó có đầu vào – quá trình thực hiện – đầu ra với các nhóm nội dung như đã đề cập ở trên. Cách tiếp cận này giúp chỉ rõ, đối với từng phương diện của việc bảo vệ DLCN và quyền riêng tư, đâu là khâu chưa được thực hiện tốt: đầu vào và quá trình thực hiện (các chính sách về quyền riêng tư, các biện pháp kỹ thuật), hay đầu ra (đảm bảo quyền đối với dữ liệu cá nhân, quyền riêng tư). Từ đó, nghiên cứu đề ra khuyến nghị chính sách phù hợp.

Bên cạnh đó, việc đánh giá quyền riêng tư trên các giao diện tương tác với người dân của chính quyền cấp tỉnh ở Việt Nam có tham khảo một phần cách tiếp cận của đánh giá tác động về quyền riêng tư do Ủy ban Thương mại Liên bang Hoa Kỳ thực hiện (xem Hộp 3).

Hộp 3: Đánh giá tác động quyền riêng tư do Ủy ban Thương mại Liên bang Hoa Kỳ thực hiện

Đánh giá tác động quyền riêng tư (privacy impact assessments - PIA) cho thấy cách dữ liệu cá nhân được thu thập, sử dụng, chia sẻ và lưu trữ trong khu vực công. Các nhà quản lý chương trình và chủ sở hữu hệ thống được khuyến khích kiểm tra cẩn thận và xem xét các biện pháp bảo vệ quyền riêng tư trong các hoạt động liên quan đến dữ liệu cá nhân. PIAs tăng cường tính minh bạch của việc xử lý dữ liệu cá nhân của các tổ chức khu vực công, và do đó làm tăng niềm tin của công chúng vào các dịch vụ chính phủ số. PIAs được tiến hành hàng năm để đảm bảo độ chính xác và cập nhật. PIAs giúp đánh giá:

1. Loại dữ liệu, nguồn và cách sử dụng
2. Cơ chế truy cập và chia sẻ dữ liệu
3. Thông báo và đồng ý
4. Độ chính xác và bảo mật dữ liệu
5. Lưu giữ và xử lý dữ liệu
6. Mức độ bảo đảm quyền riêng tư của kênh.
7. Rủi ro về quyền riêng tư

Nguồn: Federal Trade Commission Privacy Impact Assessments *https://www.ftc.gov/policy-notices/privacy-policy/privacy-impact-assessments*

Đồng thời, dựa trên các nguyên tắc của LHQ, báo cáo này đánh giá thực tiễn bảo vệ dữ liệu cá nhân và quyền riêng tư của các địa phương theo 06 tiêu chí (trong số nhiều tiêu chí khác):[36] (i) tính công bằng, hợp pháp trong xử lý thông tin cá nhân; (ii) mục đích sử dụng thông tin cá nhân rõ ràng; (iii) tính tương xứng và cần thiết; (iv) nguyên tắc lưu trữ thông tin; (v) tính minh bạch; và (vi) tính giải trình trong thu thập, xử lý dữ liệu cá nhân.

Phương pháp nghiên cứu

Nghiên cứu này được thực hiện với các phương pháp sau đây:

Phân tích tài liệu: Nhóm nghiên cứu sử dụng dữ liệu thứ cấp gồm các văn bản quy phạm pháp luật, chương trình, đề án; chính sách về quyền riêng tư của các địa phương; các tài liệu về BVDLCN, bảo đảm quyền riêng tư trên thế giới (ví dụ như PIA của Hoa Kỳ, các nguyên tắc của LHQ; thực tiễn tốt từ một số quốc gia). Đây là cơ sở pháp lý, lý luận và thực tiễn để đối chiếu đánh giá việc BVDLCN trên các giao diện trực tuyến của chính quyền địa phương các tỉnh, thành phố trực thuộc trung ương.

Đánh giá trực tiếp: Nhóm nghiên cứu đã truy cập vào các cổng TTĐT, cổng DVCĐT và ƯDTM của các địa phương để đánh giá thực tiễn triển khai BVDLCN trên các giao diện đó, cụ thể bao gồm: 50 ứng dụng thông minh của 50 trong số 63 tỉnh, thành phố có đưa ƯDTM vào thực hiện; 63 cổng DVCTT; 63 cổng TTĐT với 78 kênh thu thập DLCN qua 3 chuyên mục gồm (i) Hỏi đáp, (ii) Phản ánh kiến nghị, và (iii) Lấy ý kiến xây dựng văn bản quy phạm pháp luật.

[36] *Ủy ban cấp cao về quản lý của LHQ, Các nguyên tắc về bảo vệ dữ liệu cá nhân và quyền riêng tư, thông qua tại phiên họp thứ 36 ngày 11/10/2018. Có thể tải về từ: https://archives.un.org/sites/archives.un.org/files/_un-principles-on-personal-data-protection-privacy-hlcm-2018.pdf*

Giới hạn của nghiên cứu: Bên cạnh những giá trị, ưu điểm đã được trình bày, nghiên cứu chỉ tập trung đánh giá việc BVDLCN trên các giao diện trực tuyến của chính quyền cấp tỉnh. Nhóm nghiên cứu chỉ đánh giá dựa trên thông tin công khai tiếp cận được trên các giao diện tương tác trực tuyến nói trên, không đánh giá toàn bộ dữ liệu cá nhân ở khu vực công. Đối với việc BVDLCN trong quá trình lưu trữ, sử dụng, chia sẻ khối lượng dữ liệu cá nhân rất lớn sau khi được thu thập từ các giao diện này, nghiên cứu mới chỉ đánh giá được một phần nhỏ, mà chưa có điều kiện tìm hiểu, phân tích sâu do chưa có đủ điều kiện về thời gian, nguồn lực con người và tài chính. Cũng vì các lý do này, một số phương pháp nghiên cứu chưa được sử dụng như phiếu điều tra xã hội học, thảo luận nhóm có trọng tâm, phỏng vấn sâu.

II. NHỮNG PHÁT HIỆN CHÍNH

CHÍNH SÁCH QUYỀN RIÊNG TƯ TRÊN CÁC KÊNH TƯƠNG TÁC

3 Cổng dịch vụ công trực tuyến có chính sách về quyền riêng tư

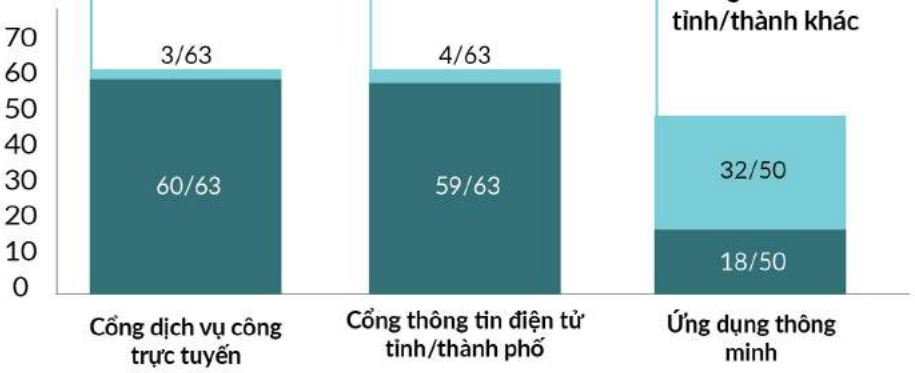
Thừa Thiên Huế
Đà Nẵng
Gia Lai

4 Cổng thông tin điện tử tỉnh/thành phố có chính sách về quyền riêng tư

Bình Định
Phú Thọ
Hà Nội
Thừa Thiên Huế

32 Ứng dụng thông minh có chính sách về quyền riêng tư

Bắc Kạn
Vĩnh Phúc
Đồng Tháp
Tiền Giang
và 28 Ứng dụng thông minh của các tỉnh/thành khác



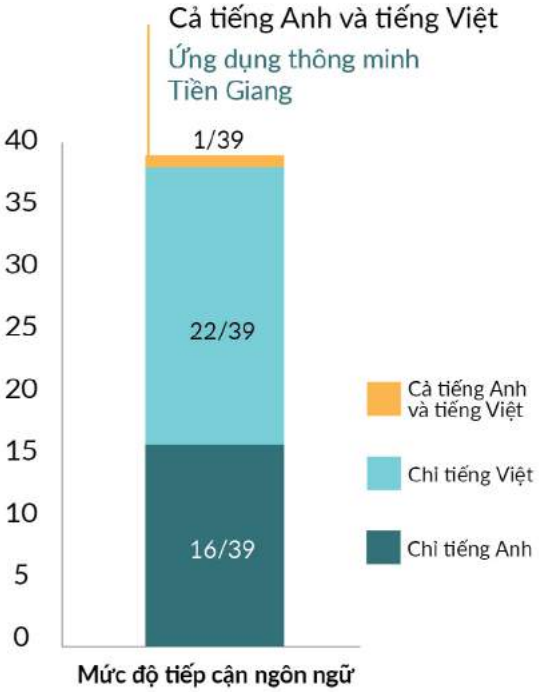
Trong 63 tỉnh/thành, **chỉ có duy nhất tỉnh Thừa Thiên Huế** có chính sách quyền riêng tư trên cả ba kênh tương tác với người dân:

(1) Cổng dịch vụ công trực tuyến

(2) Cổng thông tin điện tử

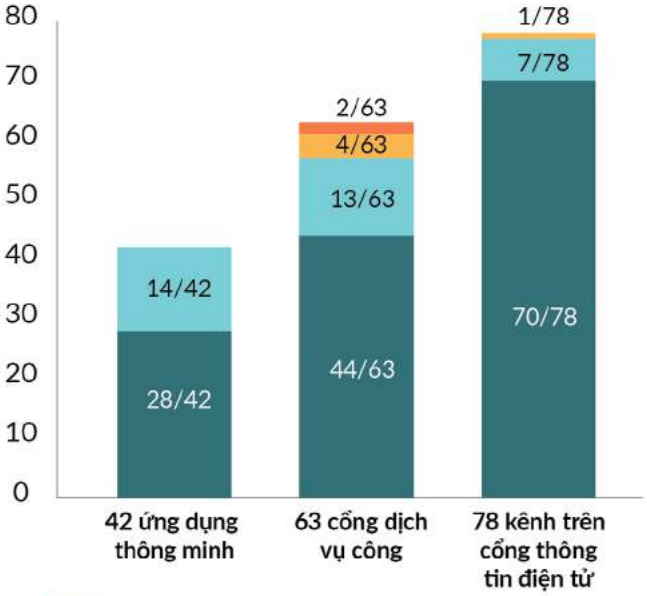
(3) Ứng dụng thông minh

MỨC ĐỘ THÂN THIỆN CỦA NGÔN NGỮ VỚI NGƯỜI DÙNG



Duy nhất **Ứng dụng thông minh tỉnh Tiền Giang** có chính sách về quyền tiêng tư có thể tiếp cận được ở cả tiếng Anh và tiếng Việt

QUYỀN ĐỒNG Ý VÀ ĐƯỢC BIẾT



** 42 Ứng dụng thông minh có hoạt động tại thời điểm đánh giá*

2.1. Một số nhận định chung

Về bảo vệ DLCN và quyền riêng tư trên các giao diện tương tác với người dân của chính quyền địa phương

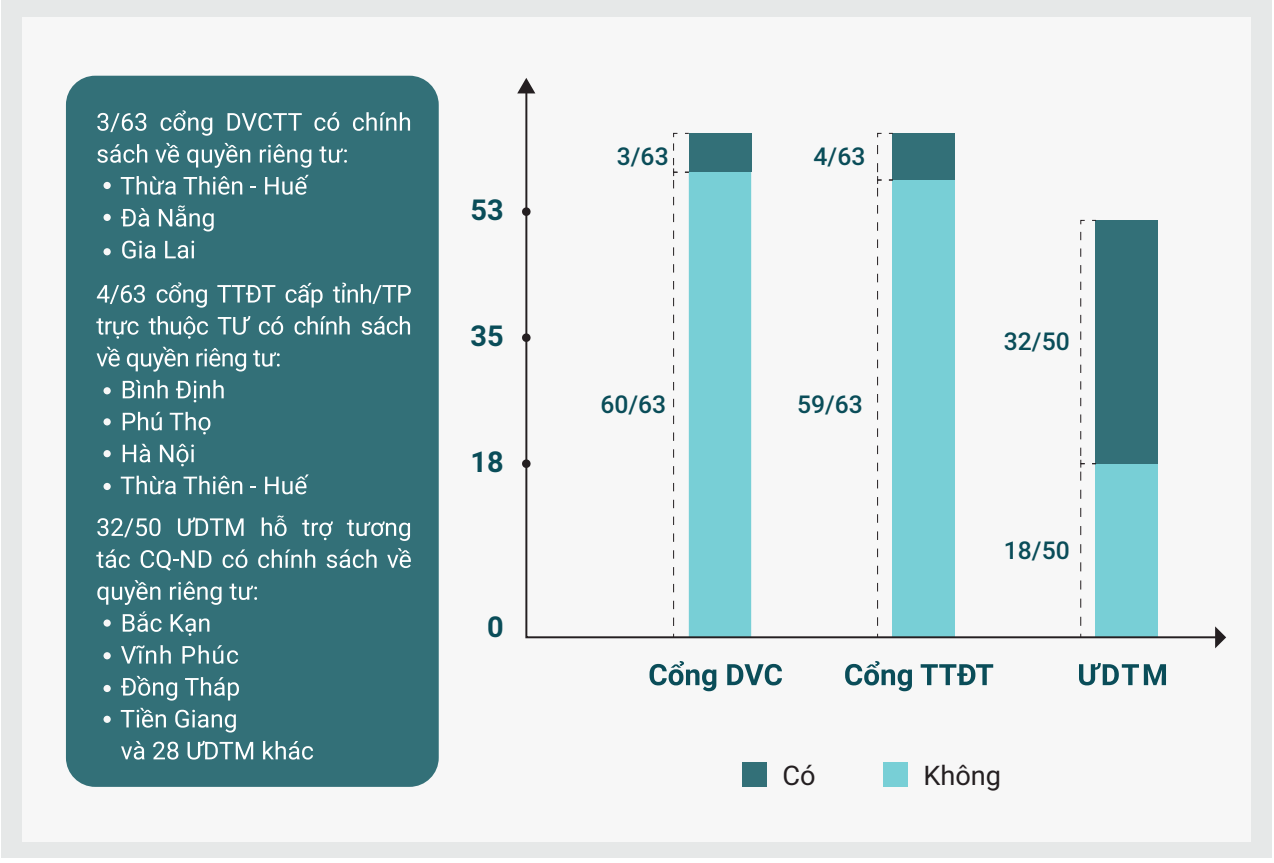
Một số địa phương đã và đang có sự nỗ lực trong xây dựng và triển khai các công cụ khác nhau để bảo vệ dữ liệu cá nhân, quyền riêng tư trên các giao diện tương tác với người dân. Tuy nhiên, nói chung, chính quyền các tỉnh, thành phố chưa quan tâm nhiều đến vấn đề này. Chưa có địa phương nào thực hiện tốt việc bảo vệ quyền riêng tư nói chung trên các phương diện khác nhau, mà chỉ có một số cách làm tốt đối với một số khía cạnh cụ thể.

Có thể thấy, các chính sách, công cụ liên quan đến quyền riêng tư trên cổng TTĐT, cổng DVCTT và ƯDTM của các tỉnh, thành phố còn mang tính tự phát, mà chưa xuất phát từ nhận thức rõ ràng về tầm quan trọng của việc bảo vệ quyền riêng tư. Các địa phương chú ý nhiều đến các yêu cầu kỹ thuật nhằm đảm bảo an toàn, bảo mật của dữ liệu hơn là tính riêng tư của dữ liệu; phòng chống các mối nguy cơ, rủi ro đối với an ninh mạng hơn là quyền riêng tư của người sử dụng dịch vụ. Có thể dễ dàng tiếp cận văn bản của chính quyền địa phương về an toàn thông tin, nhưng hầu như không thể tìm thấy văn bản về bảo vệ quyền riêng tư trên các cổng TTĐT và cổng DVCTT. Không chỉ thế, hầu như các giao diện chỉ yêu cầu người sử dụng khẳng định thông tin họ cung cấp là chính xác, nhưng lại không có công cụ để người dân thực hiện quyền riêng tư.

Ở mức độ tổng quan, nếu đặt việc bảo vệ quyền riêng tư trong toàn bộ quá trình tương tác của chính quyền địa phương với công dân trên môi trường số, có thể nói, các yếu tố đầu vào như cơ sở vật chất, hạ tầng kỹ thuật, con người đã được quan tâm khá nhiều. Tuy nhiên, quá trình thực hiện các chính sách, pháp luật có liên quan đến bảo vệ quyền riêng tư cần được cải thiện nhiều hơn nữa. Đặc biệt, kết quả đầu ra về mức độ bảo vệ dữ liệu cá nhân, đáp ứng quyền riêng tư của người dân còn chưa được như mục tiêu mong muốn.

Cụ thể, đánh giá sơ bộ trình bày ở Hình 2 và Bảng 1 cho thấy, các chính sách về quyền riêng tư chưa được quan tâm đúng mức, thể hiện ở cả số lượng và chất lượng của các chính sách về quyền riêng tư.

Hình 2: Mức độ công khai chính sách về quyền riêng tư trên các giao diện tương tác với người dân của chính quyền địa phương



Về số lượng, tổng cộng chỉ có 39 văn bản chính sách về quyền riêng tư được tìm thấy trên cả ba kênh giao diện trực tuyến của chính quyền địa phương 63 tỉnh, thành. Trong đó, chỉ có 3 trong số 63 cổng DVCTT (của Đà Nẵng, Gia Lai, Thừa Thiên Huế) và 4 trong số 63 cổng TTĐT (của Bình Định, Phú Thọ, Hà Nội, Thừa Thiên-Huế) công bố chính sách về quyền riêng tư. Trong số 50 tỉnh, thành phố có ƯDTM hoạt động, 32 ứng dụng đã công khai chính sách về quyền riêng tư, còn lại 18 ứng dụng không có chính sách về quyền riêng tư hoặc không thể truy cập được chính sách về quyền riêng tư. Tỷ lệ công bố chính sách về quyền riêng tư của ứng dụng cao hơn có thể là do các yêu cầu kỹ thuật tích hợp sẵn của Google Play và Apple Store, khiến các nhà phát triển ứng dụng bắt buộc phải công bố chính sách về quyền riêng tư khi ứng dụng ra mắt.

Về chất lượng, không có chính sách quyền riêng tư đáp ứng đầy đủ các điều kiện quy định trong Luật Công nghệ thông tin số 67/2006/QH11, Nghị định số 64/2007/NĐ-CP và Thông tư số 25/2010/TT-BTTTT, cũng như theo 6 nguyên tắc của LHQ về bảo vệ dữ liệu cá nhân và quyền riêng tư như đã đề cập ở trên. Đặc biệt, hầu hết các chính sách về quyền riêng tư hiện tại không thiết lập được thỏa thuận điện tử hiệu quả giữa cơ quan thu thập và xử lý dữ liệu (UBND cấp tỉnh) và chủ thể dữ liệu (người dùng ứng dụng thông minh, cổng DVCTT và cổng TTĐT). Định nghĩa không rõ ràng về quyền kiểm soát dữ liệu dẫn đến sự nhầm lẫn về trách nhiệm pháp lý của cơ quan thu thập và xử lý dữ liệu (UBND các địa phương) và đơn vị vận hành (Sở TTTT hoặc các đơn vị tư nhân).

Bảng 1: Tóm tắt các phát hiện nghiên cứu chính

Chính sách quyền riêng tư của các ƯDTM	Chính sách quyền riêng tư của các cổng TTĐT [37]	Chính sách quyền riêng tư của cổng DVCTT
1/32 tỉnh, thành phố (Hậu Giang) có ƯDTM đã ban hành chính sách về quyền riêng tư xác định Ủy ban nhân dân tỉnh là cơ quan thu thập và quản lý dữ liệu.	4 tỉnh/thành phố đã công bố chính sách quyền riêng tư trên cổng TTĐT (Bình Định, Phú Thọ, Hà Nội, Thừa Thiên - Huế) không xác định chính xác cơ quan thu thập và quản lý dữ liệu	1/3 (Đà Nẵng) chính sách quyền riêng tư[38] đã được công bố trên cổng DVCTT thiết lập thỏa thuận giữa Sở Thông tin và Truyền thông với người dùng.
5/32 tỉnh, thành phố (Bình Định, Đà Nẵng, Đồng Tháp, Thừa Thiên - Huế, Vĩnh Long) có ƯDTM đã ban hành chính sách về quyền riêng tư thiết lập thỏa thuận giữa Sở TTTT với người dùng;	• Bình Định • Hà Nội • Phú Thọ • Thừa Thiên - Huế	1/3 (Gia Lai) chính sách quyền riêng tư[39] đã công bố trên cổng DVCTT thiết lập thỏa thuận điện tử giữa tổ chức/doanh nghiệp cung cấp dịch vụ cho cơ quan nhà nước (WSO2 Identity Server) và người dùng.
11/32 tỉnh, thành phố (Bắc Kạn, Bạc Liêu, Bến Tre, Cần Thơ, Hòa Bình, Hưng Yên, Kon Tum, Long An, Quảng Nam, Quảng Ninh, Sóc Trăng) có ƯDTM đã ban hành chính sách về quyền riêng tư thiết lập thỏa thuận điện tử giữa tổ chức/doanh nghiệp cung cấp dịch vụ cho cơ quan nhà nước và người dùng.		1/3 (Thừa Thiên - Huế) chính sách quyền riêng tư đã được công bố trên cổng DVCTT không làm rõ cơ quan nào chịu trách nhiệm bảo vệ quyền riêng tư của các chủ thể dữ liệu.
15/32 tỉnh, thành phố (An Giang, Bà Rịa - Vũng Tàu, Cao Bằng, Hải Phòng, Kiên Giang, Lai Châu, Lạng Sơn, Ninh Bình, Phú Yên, Sơn La, Tây Ninh, Thái Bình, Thái Nguyên, Tiền Giang, Vĩnh Phúc) không làm rõ cơ quan nào chịu trách nhiệm bảo vệ quyền riêng tư của các chủ thể dữ liệu. Chỉ nêu rất chung chung là "Chúng tôi".		

[37] *Trên các cổng TTĐT, chính sách quyền riêng tư được ban hành thường được gọi với các tên khác như "Chính sách đảm bảo an toàn thông tin cá nhân," "Quy định về bảo vệ thông tin cá nhân," "Thông báo về thu thập và sử dụng thông tin cá nhân" hoặc "Quy định thu thập, chia sẻ thông tin cá nhân trên cổng TTĐT."*
[38] *Trên Cổng DVCTT thành phố Đà Nẵng, chính sách quyền riêng tư được gọi là "Chính sách bảo mật thông tin"*
[39] *Trên Cổng DVCTT tỉnh Gia Lai, chính sách quyền riêng tư được gọi là "Chính sách bảo mật", nhưng thực tế link dẫn đến "privacy policy"*

Chỉ có 1/39 chính sách về quyền riêng tư được đánh giá là ứng dụng thông minh của tỉnh Hậu Giang[40] xác định đúng Ủy ban nhân dân tỉnh Hậu Giang là đơn vị thu thập và quản lý thông tin cá nhân và Sở Thông tin và Truyền thông là đơn vị vận hành ứng dụng nhân danh UBND tỉnh (Hình 3).

Hình 3: Thực hành tốt từ chính sách về quyền riêng tư của ứng dụng thông minh của tỉnh Hậu Giang

Trường hợp điển hình

Thừa Thiên - Huế là tỉnh duy nhất đã công bố chính sách về quyền riêng tư trên cả 3 giao diện tương tác với người dân của chính quyền địa phương (cổng TTĐT, cổng DVCTT và ƯDTM). Trong đó, cổng TTĐT Thừa Thiên - Huế (thuathienhue.gov.vn) đã công bố bộ quy tắc BVDLCN riêng. Trong khi chính sách về quyền riêng tư thông thường sẽ thiết lập một thỏa thuận điện tử giữa bên thu thập và quản lý dữ liệu (Ủy ban nhân dân các địa phương) và chủ thể dữ liệu (người sử dụng cổng thông tin trực tuyến), thì quy định được công bố trên thuathienhue.gov.vn là mang tính chất quy tắc nội bộ, thông báo cách trang web thu thập, xử lý và bảo vệ dữ liệu cá nhân. Do đó, các quy tắc được công bố tập trung vào việc làm rõ các yêu cầu kỹ thuật đối với việc thu thập, xử lý và chia sẻ dữ liệu trong nội bộ Ban biên tập cổng TTĐT, hơn là cung cấp cho người dùng các cơ chế chỉnh sửa, hạn chế, khiếu nại hoặc thông báo về các thay đổi chính sách.

Mặt khác, loại "chính sách về quyền riêng tư" này có một số ưu điểm như:

- Xác định phạm vi thu thập dữ liệu cá nhân, cụ thể là xác định rõ các kênh thu thập dữ liệu cá nhân trên cổng TTĐT: 1) kênh Tiếp nhận, xử lý phản ánh, kiến nghị của cá nhân, tổ chức về quy định hành chính; 2) kênh Dân hỏi cơ quan chức năng trả lời; 3) kênh Đối thoại trực tuyến "Trao đổi và tháo gỡ"; 4) kênh Lấy ý kiến nhân dân về dự thảo văn bản pháp luật; 5) kênh Làm cho Huế đẹp hơn; 6) kênh Góp ý, hiến kế xây dựng tỉnh Thừa Thiên - Huế; và 7) kênh Hộp thư góp ý;

- Quy trình hành chính về thu thập, xử lý và chia sẻ dữ liệu được minh bạch, để người dùng nắm rõ các bước nội bộ và biết những gì sẽ xảy ra. Quy trình này có những điểm tương tự Đánh giá tác động quyền riêng tư do Ủy ban Thương mại Liên bang Hoa Kỳ thực hiện và là một cách làm tốt cần được khuyến khích.[41]

Về khoảng trống trong khung chính sách, pháp luật chung về bảo vệ dữ liệu cá nhân

Ở tầm quốc gia, qua những điểm bất cập trong thực tiễn BVDLCN, quyền riêng tư trên các giao diện tương tác với người dân của chính quyền địa phương, có thể nhận thấy một số vấn đề sau đây trong khung chính sách pháp luật liên quan đến bảo vệ dữ liệu cá nhân, quyền riêng tư:

Một là, Việt Nam chưa định nghĩa, phân loại rõ ràng dữ liệu cá nhân phù hợp với các xu hướng mới của chuyển đổi số, trong đó có các loại dữ liệu cá nhân được thu thập từ người sử dụng trên các giao diện tương tác của chính quyền. Luật An ninh mạng đưa ra định nghĩa về thông tin cá nhân quá rộng (vì vậy không rõ ràng); trong khi định nghĩa của Nghị định số 64/2007/NĐ-CP lại quá hẹp. Chỉ có Thông tư số 25/2010/TT-BTTTT đề cập đến thông tin cá nhân (không hẳn là dữ liệu cá nhân) được thu thập tự động trên cổng TTĐT.

[40] *Xem chi tiết tại https://app.haugiang.gov.vn/policy.html*
[41] *Privacy Impact Assessments | Federal Trade Commission*

Hai là, tính riêng tư của dữ liệu, quyền riêng tư chưa được chú ý phân định rõ, mà còn tập trung nhiều vào an toàn bảo mật dữ liệu. Do được xây dựng trước khi bảo vệ quyền riêng tư dữ liệu cá nhân trở thành một đề tài gây chú ý trong xã hội, khung pháp lý hiện hành tập trung nhiều hơn vào các yêu cầu kỹ thuật để đảm bảo an toàn, an ninh dữ liệu hơn là bảo vệ quyền riêng tư đối với dữ liệu cá nhân.

Ba là, không chỉ trong thực thi của chính quyền địa phương, mà ngay cả khung chính sách, pháp luật chưa phân định rõ ràng giữa chủ thể kiểm soát dữ liệu và chủ thể xử lý dữ liệu, từ đó xác định rõ trách nhiệm pháp lý của các chủ thể đó đối với chủ thể dữ liệu cá nhân. Ví dụ như khi cơ quan Nhà nước đăng tải văn bản chính sách về quyền riêng tư, liệu có thể coi đó là cơ sở để xác định chế độ trách nhiệm pháp lý của cơ quan đó? Bên cạnh đó, mối quan hệ pháp lý chưa được rõ giữa cơ quan Nhà nước thu thập dữ liệu cá nhân với doanh nghiệp cung cấp giao diện tương tác trên môi trường số.

Bốn là, còn có những nội dung chưa rõ ràng trong trách nhiệm của các cơ quan liên quan và quy trình, thủ tục minh bạch trong lưu trữ, sử dụng, chia sẻ khối lượng lớn dữ liệu cá nhân được thu thập trong các cơ quan Nhà nước và với các chủ thể bên ngoài, để làm sao quyền riêng tư được đảm bảo trong quá trình đó. Điển hình là khoảng trống quy định về thời gian lưu trữ dữ liệu, hay trách nhiệm thông báo tới người dùng khi có sự cố lộ lọt dữ liệu xảy ra.

Năm là, pháp luật chưa có quy định về nhân sự làm đầu mối bảo vệ dữ liệu cá nhân và quyền riêng tư trong hoạt động của các cơ quan Nhà nước với nhiệm vụ, quyền hạn cụ thể; công bố thông tin về nhân sự này để người dân liên hệ khi cần thiết.

Sáu là, cơ chế xử lý vi phạm, giải quyết khiếu nại, khiếu kiện, bồi thường thiệt hại, chế tài liên quan BVDLCN, quyền riêng tư trên môi trường số ở khu vực công chưa được quy định rõ ràng, cụ thể, phù hợp với sự phát triển của chuyển đổi số và thực tiễn hoạt động.

Bảy là, trên phạm vi toàn quốc, sở dĩ giữa các tỉnh/thành phố còn có sự thiếu thống nhất trong thực tiễn bảo vệ quyền riêng tư trên môi trường số một phần do còn thiếu các quy định, hướng dẫn cụ thể để các địa phương nắm bắt được các chuẩn mực, dễ dàng bám sát, tuân theo; tạo cơ sở pháp lý để các tỉnh bảo vệ quyền riêng tư tốt hơn trên môi trường số.

2.2. Bảo vệ dữ liệu cá nhân ở địa phương so với quy định pháp luật hiện hành

Từ việc đối chiếu thực tiễn BVDLCN trên môi trường số ở địa phương theo 17 tiêu chí như đã đề cập, phần này trình bày những phát hiện chính về thực tiễn BVDLCN trên các phương diện: (1) cung cấp thông tin về bảo vệ dữ liệu cá nhân trên các giao diện trực tuyến; (2) xác định quyền, trách nhiệm của các bên liên quan; (3) thông tin để liên hệ, phản hồi; và (4) các biện pháp đảm bảo quyền của người sử dụng.

2.2.1. Cung cấp thông tin về bảo vệ dữ liệu cá nhân trên các giao diện trực tuyến

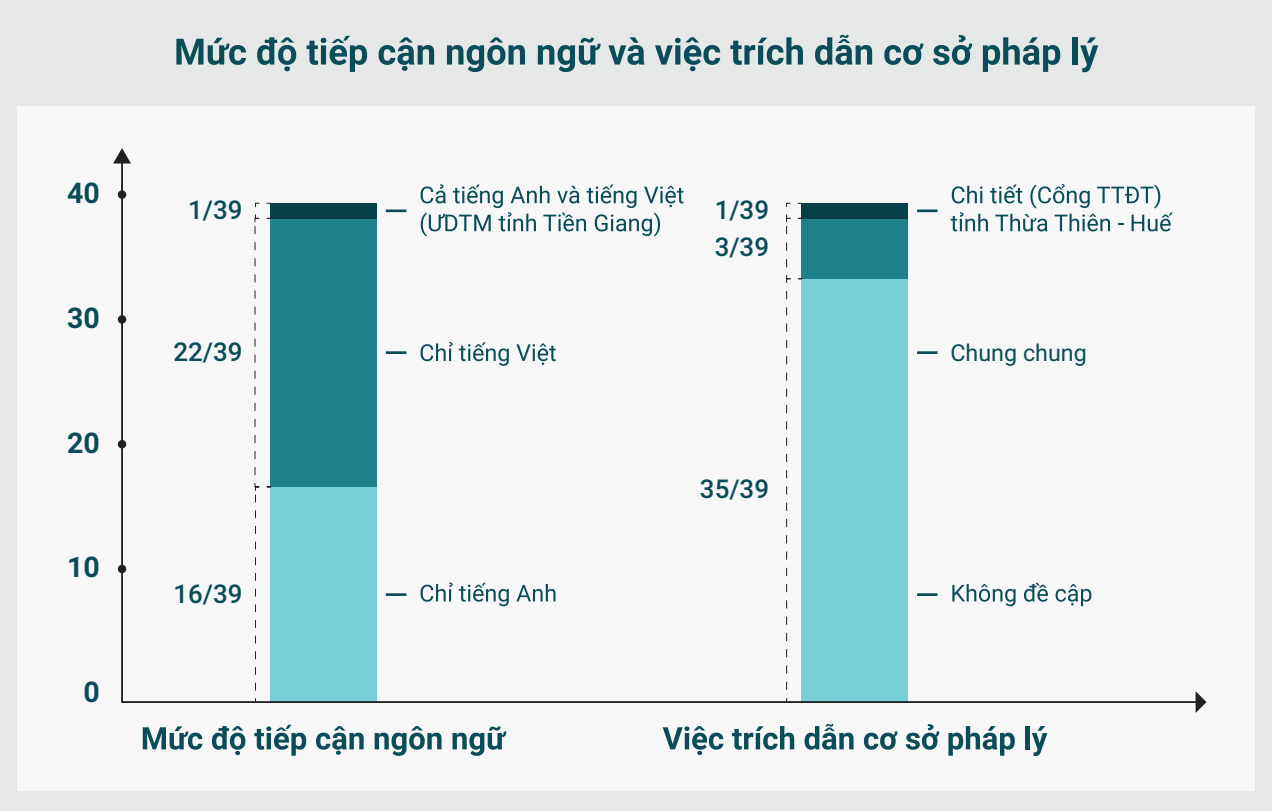
Ngôn ngữ được sử dụng

Ngôn ngữ được sử dụng trong chính sách về quyền riêng tư có thể tạo ra rào cản đối với người dùng các giao diện trực tuyến của chính quyền địa phương. Như trình bày ở Hình 4, trong số 39 bản chính sách về quyền riêng tư được tìm thấy và xem xét, chỉ có ứng dụng thông minh của Tiền Giang[42] cung cấp cả phiên bản tiếng Anh và tiếng Việt. Phần còn lại, 16/39 (15 từ ƯDTM, 1 từ cổng DVCTT) bằng tiếng Anh, 22/39 (16 từ ƯDTM, 4 từ cổng TTĐT, 2 từ cổng DVCTT) bằng tiếng Việt. Như vậy, có rất nhiều người không biết tiếng Anh không thể tự đọc các chính sách về quyền riêng tư bằng tiếng Anh, ngăn cản họ hiểu và thực hiện các quyền đối với DLCN của mình. Ngược lại, những người không biết tiếng Việt (như đại đa số khách du lịch nước ngoài) cũng không thể đọc các chính sách về quyền riêng tư bằng tiếng Việt khi truy cập cổng TTĐT và thực hiện các DVCTT trên cổng DVCTT. Nói cách khác, việc thực hiện quy định tại Điều 11, Thông tư số 25/2010/TT-BTTTT chưa được thực hiện đầy đủ.[43]

[42] *Xem chi tiết tại: https://sites.google.com/view/tiengiangs*

[43] *Điều 11: Công khai quy định đảm bảo an toàn và bảo vệ thông tin cá nhân - Cơ quan chủ quản có trách nhiệm thông báo rõ các quy định về đảm bảo an toàn và bảo vệ thông tin cá nhân trên trang chủ hoặc cung cấp một cơ chế để người sử dụng dễ dàng tiếp cận và tìm hiểu trên cổng TTĐT.*

Hình 4: Mức độ tiếp cận ngôn ngữ và việc trích dẫn cơ sở pháp lý của các chính sách về quyền riêng tư được đánh giá



Viện dẫn cơ sở pháp lý để xử lí dữ liệu

Các chính sách về quyền riêng tư được tìm thấy và xem xét hiếm khi nêu rõ cơ sở pháp lý để xử lý dữ liệu. Trong số 39 chính sách về quyền riêng tư được đánh giá, chỉ có 1 chính sách (từ cổng TTĐT tỉnh Thừa Thiên - Huế) trích dẫn các văn bản quy phạm pháp luật như Nghị định số 64/2007/NĐ-CP, Thông tư số 25/2010/TT-BTTTT, Quyết định số 851/QĐ-UBND, và tiêu chuẩn quốc gia TCVN ISO 9001: 2008 để chứng minh tính hợp pháp của việc xử lý dữ liệu cá nhân trên trang web. Chỉ có 3 trong số 39 chính sách về quyền riêng tư đề cập chung chung "luật pháp Việt Nam", 35 chính sách về quyền riêng tư còn lại không đưa ra căn cứ pháp lý cho việc thu thập và xử lý dữ liệu cá nhân trên giao diện tương tác với người dân.

Những loại dữ liệu cá nhân đang được thu thập

Theo quy định, cơ quan chủ quản có trách nhiệm phải công khai, minh bạch đối với chủ thể dữ liệu về các loại dữ liệu cá nhân được thu thập trên môi trường mạng.[44] Chính sách về quyền riêng tư của các tỉnh/thành đều cung cấp loại thông tin này, mặc dù ở các mức độ khác nhau,[45] tùy thuộc vào cách định nghĩa dữ liệu cá nhân. Có hai xu hướng rõ ràng:

Theo quy định, cơ quan chủ quản có trách nhiệm phải công khai, minh bạch đối với chủ thể dữ liệu về các loại dữ liệu cá nhân được thu thập trên môi trường mạng. Chính sách về quyền riêng tư của các tỉnh/thành đều cung cấp loại thông tin này, mặc dù ở các mức độ khác nhau, tùy thuộc vào cách định nghĩa dữ liệu cá nhân. Có hai xu hướng rõ ràng:

- Định nghĩa hẹp coi dữ liệu cá nhân là thông tin nhận dạng cá nhân theo quy định của pháp luật,[46] bao gồm ít nhất một trong các thông tin sau: họ tên, ngày sinh, nghề nghiệp, chức danh, địa chỉ thường trú, địa chỉ email, số điện thoại, số CMND, số hộ chiếu và thông tin thuộc phạm vi bí mật cá nhân cụ thể là hồ sơ sức khỏe, hồ sơ thuế, số an sinh xã hội, số thẻ tín dụng và các bí mật cá nhân khác.[47]

[44] *Điều 21, Luật CNTT (67/2006/QH11) và Điều 17, Luật An toàn thông tin mạng (86/2015/QH13)*
[45] *Xem Phụ lục*
[46] *Theo Luật Công nghệ thông tin 67/2006/QH11, Nghị định 64/2007/NĐ-CP và Thông tư số 25/2010/TT-BTTTT..*
[47] *Ví dụ như: Quy định về bảo vệ thông tin cá nhân | Cổng Thông Tin Điện Tử Phú Thọ hoặc Quy trình_thu_thap_su_dung_va_chia_se_thong_tin_ca_nhan_tren_Cong_TTDT.PDF*

• Định nghĩa rộng có tính đến sự phát triển của trí tuệ nhân tạo (AI) và phân tích dữ liệu lớn, do vậy mở rộng phạm vi định nghĩa dữ liệu cá nhân để bao gồm bất kỳ thông tin nào liên quan đến một cá nhân được xác định hoặc được nhận dạng.[48]

Định nghĩa về dữ liệu cá nhân có ý nghĩa rất lớn đối với việc thiết lập quyền và cơ chế thực hiện quyền của chủ thể dữ liệu. Trước mắt, cần đảm bảo rằng các loại thông tin nhận dạng cá nhân theo nghĩa hẹp được bảo vệ. Còn trong tầm nhìn dài hạn, rất cần bảo vệ quyền riêng tư dữ liệu cá nhân theo nghĩa mở rộng, khi ngày càng có nhiều can thiệp bởi các công nghệ mới nổi như AI và dữ liệu lớn, dẫn đến tình trạng dữ liệu cá nhân dễ bị lạm dụng/giám sát.

Mục đích xử lý dữ liệu cá nhân

Thông qua các chính sách về quyền riêng tư, người dùng có thể tìm hiểu xem dữ liệu cá nhân của họ có được sử dụng cho các mục đích hợp pháp hay không. Theo kiểm định của nhóm nghiên cứu, có 28 trong số 39 chính sách về quyền riêng tư thiếu chi tiết về nội dung này, thường chỉ đề cập chung chung các nội dung: (i) để có trải nghiệm tốt hơn, (ii) để xác định người dùng, (iii) để đáp ứng yêu cầu của người dùng; (iv) quản lý tương tác trực tuyến; và (v) liên hệ. Trong hầu hết các trường hợp này, thường không có phần riêng biệt giải thích mục đích xử lý dữ liệu, hoặc chỉ một phần mô tả ngắn cho mục đích xử lý dữ liệu cá nhân. Chưa đến một phần ba (11/39 văn bản) mô tả tương đối chi tiết về mục đích xử lý dữ liệu cá nhân thành một phần riêng biệt của văn bản.

Bên cạnh đó, một số chính sách về quyền riêng tư đề cập các mục đích xử lý dữ liệu cá nhân gây tranh cãi. Ví dụ, chính sách về quyền riêng tư của ƯDTM 'Smart Quảng Ninh' ghi: *"Khi đăng ký làm thành viên, bạn cần cung cấp cho chúng tôi một số thông tin cá nhân, ví dụ như họ tên, ngày sinh và các thông tin khác. Chúng tôi có thể kết hợp thông tin cá nhân do bạn cung cấp với các thông tin khác ngoài Dịch vụ hoặc từ các bên thứ ba để phân tích các nội dung mà bạn quan tâm. Chúng tôi có thể sử dụng thông tin cá nhân của bạn để xác định xem liệu bạn có thể quan tâm đến các sản phẩm hay dịch vụ của bên thứ ba nào không."*

Một trường hợp khác là cổng DVCTT của Thừa Thiên - Huế[49] với chính sách về quyền riêng tư ghi rõ số liệu thống kê của khách truy cập sẽ được chia sẻ với bên thứ ba, mà không làm rõ thêm các bên thứ ba này là ai. Tuy nhiên, mục đích này là chính đáng và hợp pháp hay không, ở mức độ nào, còn phụ thuộc vào quy định của pháp luật và cách mà chính sách về quyền riêng tư xác định khái niệm dữ liệu cá nhân.[50]

Thông báo về thời gian lưu trữ dữ liệu cá nhân

Vì dữ liệu cá nhân được sử dụng để quản lý dịch vụ công cộng, nó được coi là số liệu thống kê quan trọng và sẽ được lưu trữ dài hạn, trừ khi được cơ quan chủ quản quyết định khác. Tuy nhiên, hầu hết các chính sách về quyền riêng tư không cung cấp thông tin về thời gian lưu trữ dữ liệu cá nhân. Chỉ có 6 trong số 39 chính sách về quyền riêng tư thông báo cho người dùng về việc lưu trữ dữ liệu cá nhân. Trong đó, văn bản của tỉnh Hậu Giang[51] chỉ rõ: *"Dữ liệu cá nhân của người dùng sẽ được lưu trữ đến khi đơn vị chủ quản (UBND tỉnh Hậu Giang) có yêu cầu huỷ bỏ. Còn lại, trong mọi trường hợp thông tin người dùng sẽ được lưu trữ bảo mật trên máy chủ của cơ quan quản lý nhà nước."*

Thông báo được coi là sơ sài nếu không nêu rõ được điều kiện để hủy bỏ dữ liệu cá nhân và thời gian lưu trữ cụ thể. Ví dụ, chính sách về quyền riêng tư trong ứng dụng thông minh của tỉnh Bình Định chỉ giải thích chung chung: *"Dữ liệu sử dụng thường được lưu trữ trong một khoảng thời gian ngắn hơn, ngoại trừ khi dữ liệu này được sử dụng để tăng cường bảo mật hoặc cải thiện chức năng của Dịch vụ của chúng tôi hoặc Chúng tôi có nghĩa vụ pháp lý phải lưu trữ dữ liệu này trong thời gian dài hơn."*

---

[48] *Ví dụ như: Privacy Policy for 1022 Danang hoặc Privacy Policy for Smart City Bình Định*
[49] *Chính sách bảo vệ thông tin cá nhân*
[50] *Trích dẫn từ chính sách về quyền riêng tư của Cổng DVCTT tỉnh Thừa Thiên Huế: "Xin lưu ý rằng cổng DVCTT tỉnh Thừa Thiên - Huế có thể cung cấp các số liệu thống kê tổng hợp về các khách viếng thăm, hình thức kết nối vào Cổng và các thông tin liên quan đến Cổng cho những bên thứ ba có uy tín, nhưng những thống kê này không chứa các thông tin nhận diện cá nhân."*
[51] *Xem cụ thể ở đây: CHÍNH SÁCH VỀ QUYỀN RIÊNG TƯ THÔNG TIN*

Khi đọc mô tả chung chung như vậy, người dùng không biết được khoảng thời gian cụ thể để lưu trữ dữ liệu, liệu họ có quyền yêu cầu xóa dữ liệu hay không. Hoặc ở Gia Lai, dữ liệu cá nhân có thể bị xóa hay không được quyết định bởi hành động đơn giản là người dùng ngừng hoạt động trên hệ thống, như trong chính sách về quyền riêng tư được dẫn link có ghi.[52]

Thông báo rủi ro về quyền riêng tư và các biện pháp phòng ngừa

Trong số 39 tỉnh, thành phố có chính sách về quyền riêng tư, có 34 địa phương có thông báo cho người dùng về rủi ro quyền riêng tư thông qua 30 ứng dụng, 3 cổng TTĐT, và 1 cổng DVCTT. Đây là con số cao so với kết quả đánh giá ở các tiêu chí khác. Điều này thể hiện sự quan tâm đối với các rủi ro về quyền riêng tư và biện pháp bảo mật trong môi trường kỹ thuật số. Tuy nhiên, có vẻ như các cơ quan công quyền địa phương vẫn ngần ngại đối phó với hậu quả của các sự cố vi phạm hay lộ lọt dữ liệu.

Chỉ có chính sách về quyền riêng tư từ ƯDTM của tỉnh Hậu Giang công nhận và tuyên bố trách nhiệm của UBND tỉnh trong việc thông báo cho người dùng trong trường hợp hệ thống bị hacker tấn công. Cách tiếp cận này thể hiện mức độ trách nhiệm cao của UBND tỉnh Hậu Giang đối với các công dân số, và điều này có thể làm tăng niềm tin của công chúng vào chính phủ số.

Về mặt thực tiễn triển khai, nhóm nghiên cứu ghi nhận thực hành tốt từ tỉnh Đồng Tháp. Cụ thể, khi phát hiện tình trạng sử dụng thông tin cá nhân của người phản ánh, kiến nghị qua Tổng đài 1022 của tỉnh không đúng mục đích, Chủ tịch UBND tỉnh Đồng Tháp đã minh bạch thông tin về tình trạng này trên cổng TTĐT tỉnh, đồng thời công khai biện pháp xử lý qua ban hành Chỉ đạo số 21/UBND-KSTTHC.[53]

Đây là những cách tiếp cận mà báo cáo này khuyến khích chính quyền địa phương áp dụng, bởi qua đó đảm bảo tính minh bạch và chịu trách nhiệm trước các cuộc tấn công kỹ thuật số, thay vì hạn chế việc tiết lộ và né tránh xử lý hậu quả của các sự cố tấn công dữ liệu cá nhân người dùng.

Cam kết thông báo khi có thay đổi trong chính sách về quyền riêng tư

Trong khi phần lớn các chính sách về quyền riêng tư của 24 trong số 39 tỉnh, thành phố thể hiện cam kết thông báo cho người dùng khi có thay đổi về chín h sách về quyền riêng tư, số còn lại không thể hiện cam kết này. Trong số những chính sách thể hiện cam kết, chỉ có 5 chính sách chỉ rõ phương thức thông báo: email, thông báo nổi bật trên giao diện, hoặc cập nhật ngày “Cập nhật lần cuối” trong chính sách về quyền riêng tư.[54]

Những chính sách có mô tả được phân loại là sơ sài chỉ dừng lại ở việc hiển thị một câu chung chung như “chúng tôi sẽ thông báo cho bạn về bất kỳ thay đổi nào bằng cách đăng Chính sách về quyền riêng tư mới trên trang này”, mà không nêu chi tiết các cơ chế để cập nhật cho người dùng về các thay đổi trong chính sách về quyền riêng tư.[55] Ngay cả khi các chính sách về quyền riêng tư cam kết rõ về thông báo thay đổi, chẳng hạn như trong trường hợp cổng DVCTT của Thừa Thiên - Huế, vẫn bị đánh giá là không thể hiện cam kết, bởi lẽ chính sách này không giải thích cụ thể sẽ thông báo cho người dùng về những thay đổi nào và cũng không giải thích các phương thức thông báo đến người dùng.

[52] *Trích dẫn từ chính sách về quyền riêng tư của Cổng DVCTT tỉnh Gia Lai “WSO2 IS lưu giữ dữ liệu cá nhân của bạn miễn là bạn là người dùng tích cực của hệ thống của chúng tôi. Bạn có thể cập nhật dữ liệu cá nhân của mình bất cứ lúc nào bằng cách sử dụng cổng thông tin người dùng tự chăm sóc nhất định”.*
[53] *Thông tin chi tiết xem tại: CỔNG THÔNG TIN ĐIỆN TỬ TỈNH ĐỒNG THÁP*
[54] *Xem ví dụ chi tiết tại chính sách về quyền riêng tư của UDTM tỉnh Bình Định tại Privacy Policy for Smartcity Bình Định*
[55] *Xem ví dụ chi tiết tại chính sách về quyền riêng tư của UDTM Bạc Liêu tại Bac Lieu SmartCity*

Làm rõ dữ liệu cá nhân sẽ được chia sẻ với ai

Phần lớn (29/39) chính sách về quyền riêng tư có nêu dữ liệu cá nhân sẽ được chia sẻ với các tổ chức, cá nhân khác. Tuy nhiên, về mức độ rõ ràng, hầu hết các văn bản này (23/29) không cung cấp cho các chủ thể dữ liệu danh mục đầy đủ các chủ thể có quyền truy cập vào dữ liệu cá nhân của họ. Cụ thể, các chính sách về quyền riêng tư này tuyên bố: *"Chúng tôi có thể sử dụng các công ty và cá nhân bên thứ ba vì các lý do sau: 1) để tạo điều kiện thuận lợi cho dịch vụ của chúng tôi; 2) để cung cấp dịch vụ thay mặt chúng tôi; 3) thực hiện các dịch vụ liên quan đến dịch vụ; hoặc 4) để hỗ trợ chúng tôi trong việc phân tích cách dịch vụ của chúng tôi được sử dụng."* Chỉ có 5 trong số 39 chính sách về quyền riêng tư nêu rõ các bên thứ ba khác nhau (nhà cung cấp dịch vụ, chuyển nhượng doanh nghiệp, chi nhánh, đối tác kinh doanh, người dùng khác), cũng như mục đích chia sẻ tương ứng với các tổ chức, cá nhân đó.

2.2.2. Xác định quyền, trách nhiệm của các bên liên quan

Xác định cơ quan chủ quản và trách nhiệm của họ

Kết quả đánh giá theo tiêu chí này cho thấy, hầu hết các chính quyền địa phương đều chưa nhận thức hết các quan hệ pháp lý giữa cơ quan chịu trách nhiệm thu thập và xác định mục đích xử lý dữ liệu với chủ thể dữ liệu. Điều quan trọng nhất là các chính sách về quyền riêng tư cần phải thông báo cho các chủ thể dữ liệu biết cơ quan nào sẽ chịu trách nhiệm giải quyết các yêu cầu và khiếu nại của họ, cũng như cách thức liên hệ để yêu cầu thực hiện các quyền đối với dữ liệu của họ. Nếu các chính sách về quyền riêng tư không xác định chính xác các cơ quan nhà nước phụ trách, trách nhiệm của họ đối với các chủ thể dữ liệu sẽ không được thiết lập rõ ràng, có thể dẫn đến vướng mắc trong thực tiễn như phân tích trong Hộp 4 dưới đây.

Hộp 4: Một số vấn đề về trách nhiệm pháp lý đối với dữ liệu cá nhân

Làm rõ trách nhiệm pháp lý là rất quan trọng trong trường hợp vi phạm xảy ra đối với dữ liệu cá nhân và gây thiệt hại (có thể là tài chính hoặc tinh thần) cho các chủ thể dữ liệu. Trong trường hợp lạm dụng dữ liệu cá nhân được thu thập trên cổng TTĐT, như đã xảy ra ở Đồng Tháp chẳng hạn, trách nhiệm bồi thường đối với thiệt hại về dữ liệu thuộc về cơ quan nào, nếu công dân quyết định đưa vụ việc ra tòa án? Đó sẽ là Ủy ban nhân dân tỉnh Đồng Tháp, là cơ quan chủ quản của cổng TTĐT, hay là Sở Thông tin và Truyền thông, đơn vị vận hành nó? Một kịch bản khác là nếu có vi phạm liên quan đến dữ liệu hộ tịch, và công dân muốn đưa vụ việc ra Tòa án, họ sẽ khởi kiện Ủy ban nhân dân hay Sở Tư pháp?

Để trả lời những câu hỏi này, trách nhiệm pháp lý phải được xác định rõ không chỉ trong thỏa thuận với bên ngoài được thể hiện qua các chính sách về quyền riêng tư và hợp đồng thương mại với các nhà cung cấp dịch vụ. Trách nhiệm này còn phải được quy định trong các quy tắc và tiêu chuẩn nội bộ (như ISO 27701) nhằm bảo đảm an toàn cho các hoạt động chia sẻ dữ liệu giữa các bộ phận khác nhau của cùng một cơ quan nhà nước hoặc giữa các cơ quan nhà nước với nhau. Chỉ có như vậy, trách nhiệm pháp lý mới được phân định rõ ràng theo toàn bộ chu kỳ thu thập và xử lý dữ liệu.

Nguồn: *Đây là những câu hỏi do nhóm nghiên cứu đặt tình huống*

Mặc dù việc xác định đúng cơ quan thu thập và quản lý dữ liệu là rất quan trọng, chỉ có 1 trong số 39 chính sách về quyền riêng tư xác định chính xác UBND là cơ quan nhà nước chịu trách nhiệm. Trong số đó, 5 chính sách về quyền riêng tư nhầm lẫn, coi Sở TTTT là đơn vị chịu trách nhiệm, trong khi thực tế họ là bộ phận xử lý dữ liệu thay mặt cho UBND, 6 chính sách về quyền riêng tư coi các hệ thống CNTT (có thể là cổng TTĐT hoặc hệ thống chính phủ điện tử) là bên chính của thỏa thuận. Trong trường hợp đó, chính sách về quyền riêng tư được công bố như là các quy định nội bộ được chia sẻ với công chúng hơn là các chính sách về quyền riêng tư. Trong số 32 chính sách quyền riêng tư, 11 chính sách coi các chủ thể tư nhân như đơn vị chịu trách nhiệm quản lý dữ liệu trong khi họ là đơn vị cung cấp dịch vụ, và trên nguyên tắc sẽ không có quyền truy cập hoặc thay đổi dữ liệu cá nhân.

Trong trường hợp cổng DVCTT của tỉnh Gia Lai liên kết trực tiếp với chính sách về quyền riêng tư của đơn vị cung cấp dịch vụ giao diện WSO2, những điều khoản trong chính sách này không có nhiều ý nghĩa pháp lý với người dùng, bởi người dùng đồng ý thỏa thuận với cơ quan nhà nước chịu trách nhiệm chứ không phải đơn vị cung cấp dịch vụ. Gần một nửa (15/32) chính sách về quyền riêng tư được xem xét đưa ra nhận dạng mơ hồ về bên quản lý dữ liệu. Trong các trường hợp đó, đại từ "chúng tôi" được sử dụng, nhưng cụ thể "chúng tôi" là ai trong mối quan hệ với các chủ thể dữ liệu không được làm rõ.

Xác định chủ thể dữ liệu và quyền của họ

Nhìn chung, các giao diện trực tuyến của chính quyền địa phương xác định rõ chủ thể dữ liệu, không xảy ra nhầm lẫn như đối với cơ quan kiểm soát dữ liệu. Tuy nhiên, nhóm nghiên cứu đề xuất cách diễn đạt rõ ràng hơn, ví dụ như: *"Chính sách về quyền riêng tư này áp dụng đối với quý vị, nếu quý vị truy cập trang web của chúng tôi, đăng ký tài khoản hoặc sử dụng dịch vụ của chúng tôi"*. Một cách làm tốt là cổng TTĐT của tỉnh Phú Thọ,[56] với chính sách về quyền riêng tư phân biệt rõ giữa khách truy cập và người dùng. Sự phân biệt này là hữu ích vì dữ liệu của người dùng thường là dữ liệu đã đăng ký hoặc số liệu thống kê quan trọng, được các cơ quan nhà nước thu thập và lưu trữ dài hạn cho các mục đích quản lý hành chính và pháp lý của khu vực công; trong khi dữ liệu của khách truy cập thường là dữ liệu hành vi/hồ sơ được thu thập và phân tích để cải thiện DVCTT.

2.2.3. Cung cấp thông tin liên hệ, phản hồi

Thông tin về đầu mối liên hệ

Trong số 39 chính sách về quyền riêng tư, 21 chính sách của 17 ƯDTM, 1 cổng DVCTT và 3 cổng TTĐT cung cấp thông tin liên lạc là hòm thư điện tử (email) hoặc số điện thoại, hoặc cả hai. Trong số 21 email được cung cấp, chỉ có 7 là email công vụ chính thức và 13 là email cá nhân. Tất cả các địa chỉ email liên hệ được cung cấp trên các cổng TTĐT là email công vụ, trong khi chỉ có 4 email được cung cấp trong các chính sách về quyền riêng tư của các ƯDTM là email công vụ. Thực trạng này có thể được giải thích bởi thực tế là chính quyền địa phương thường thuê đơn vị cung cấp dịch vụ bên ngoài để phát triển ƯDTM. Trong phần lớn trường hợp đó, các đơn vị cung cấp dịch vụ thường sẽ kiêm nhiệm thiết kế các chính sách về quyền riêng tư trước khi xuất bản các ứng dụng trên các cửa hàng của Google và Apple.

Vì các chính sách về quyền riêng tư được phát triển như một phần của các yêu cầu kỹ thuật của các nền tảng phân phối ứng dụng kỹ thuật số trực tuyến, chứ không phải do yêu cầu chặt chẽ từ cơ quan chủ quản, các email liên hệ được cung cấp phần lớn là tài khoản cá nhân. Một mặt, những email cá nhân có rủi ro bảo mật lớn nếu công dân gửi yêu cầu liên quan đến dữ liệu cá nhân tới các tài khoản thuộc sở hữu tư nhân không được kiểm tra này. Trên thực tế, giả danh email công vụ của các cơ quan nhà nước để tiếp cận nạn nhân là một phương pháp phổ biến trong gian lận và trộm cắp danh tính. Theo báo cáo của IBM, xâm nhập thông tin nội bộ (compromised credentials) là phương thức tấn công ban đầu phổ biến nhất, gây ra 20% các vụ lộ lọt dữ liệu với tổng phí tổn trung bình là 4,37 triệu đô la.[57] Nếu tất cả các tài khoản email cá nhân này được thiết lập và công khai để sử dụng một lần, chúng có thể bị tấn công và sử dụng cho mục đích gian lận để tiếp cận với công dân và lấy thông tin cá nhân dưới danh nghĩa của các quan chức chính phủ. Mặt khác, việc công khai email cá nhân thay vì email công vụ của cơ quan nhà nước trong các chính sách về quyền riêng tư (hình thức thỏa thuận số giữa chính quyền địa phương và công dân) có thể làm giảm niềm tin của công chúng vào chính phủ số.

[56] *Truy cập tại: Quy định về bảo vệ thông tin cá nhân | Cổng Thông Tin điện tử Phú Thọ*
[57] *Trang 20, Báo cáo "IBM security report 2021".*

Làm rõ thời hạn trả lời yêu cầu/khiếu nại từ chủ thể dữ liệu

Không có chính sách về quyền riêng tư nào từ các ứng dụng thông minh và cổng DVCTT làm rõ thời hạn trả lời các câu hỏi/yêu cầu/khiếu nại từ các chủ thể dữ liệu, mặc dù email/điện thoại liên hệ được cung cấp. Chỉ có 4 chính sách về quyền riêng tư từ cổng TTĐT của Bình Định, Hà Nội, Phú Thọ, Thừa Thiên - Huế đề cập thời hạn phản hồi (24 giờ ở Hà Nội và Phú Thọ, và 48 giờ ở Bình Định), nhưng chỉ đối với việc cung cấp mật khẩu mới theo yêu cầu của chủ thể dữ liệu vì được coi là một dịch vụ công chính thức.

Cổng TTĐT tỉnh Thừa Thiên - Huế là một ví dụ tốt khi nêu rõ các mốc thời gian cụ thể trong Quy tắc thu thập, sử dụng và chia sẻ thông tin cá nhân:[58]

1. Để cập nhật thông tin cá nhân: các công chức phụ trách có nhiều nhất 2 ngày làm việc, kể từ khi nhận được thông tin cập nhật của cá nhân, để cập nhật dữ liệu cá nhân lên hệ thống.

2. Để sửa đổi thông tin cá nhân: các công chức nhà nước phụ trách có nhiều nhất 2 ngày làm việc, kể từ khi nhận được yêu cầu từ các cá nhân, để sửa đổi dữ liệu cá nhân được lưu trên hệ thống.

Tuy nhiên, không có chính sách về quyền riêng tư nào thiết lập cơ chế rõ ràng để giải quyết các khiếu nại về dữ liệu cá nhân. Quan sát các trường hợp đã khiếu nại cho thấy chính quyền địa phương hiện đang giải quyết các khiếu nại về dữ liệu cá nhân như một dạng phản ánh kiến nghị của công dân về vi phạm hành chính. Hiện vẫn chưa có nhân sự được phân công phụ trách việc tiếp nhận, xử lý các khiếu nại về dữ liệu cá nhân.

2.2.4. Các biện pháp đảm bảo quyền của người sử dụng

Quyền được đồng ý và được biết

Sự đồng ý của người dùng là một chỉ số quan trọng thể hiện tính hợp pháp của việc thu thập và xử lý dữ liệu cá nhân[59]. Việc bảo vệ dữ liệu cá nhân của các cơ quan chính quyền địa phương trên các giao diện tương tác về cơ bản dựa trên sự đồng ý bằng hình thức kỹ thuật số do không có sự tương tác hay cơ hội để đồng ý bằng văn bản. Trong trường hợp như vậy, theo Điều 11, Thông tư số 25/2010/TT-BTTTT, cơ quan nhà nước (Ủy ban nhân dân) cần yêu cầu sự đồng ý của chủ thể dữ liệu ở định dạng số theo một cách dễ hiểu và dễ tiếp cận. Hơn nữa, đó phải là sự đồng ý có hiểu biết, hay nói cách khác, các chủ thể dữ liệu cần biết rõ ràng về những gì họ đang đồng ý.[60]

Trên các ƯDTM và trang web của chính quyền địa phương, yêu cầu sự đồng ý của người dùng dựa trên sự hiểu biết có thể được thể hiện thông qua hộp "đồng ý" đính kèm chính sách về quyền riêng tư:

1. Hộp "đồng ý" cho phép chủ thể dữ liệu thực hiện quyền lựa chọn đồng ý hay không.

2. Các chính sách về quyền riêng tư kèm theo thông báo tới chủ thể dữ liệu để họ biết đang đồng ý với điều gì.

[58] *Xem chi tiết tại: QT_Thu_thap_su_dung_va_chia_se_thong_tin_ca_nhan_tren_Cong_TTDT.PDF*
[59] *Điều 21, Luật Công nghệ thông tin 2006; Điều 5, Nghị định 64/2007/NĐ-CP; Điều 4, Thông tư số 25/2010/TT-BTTTT.*
[60] *Khoản 3, Điều 4, Thông tư số 25/2010/TT-BTTTT quy định: "Việc thu thập và sử dụng thông tin cá nhân phải được sự đồng ý của cá nhân đó trừ những trường hợp pháp luật có quy định khác.". Điều 11, Thông tư số 25/2010/TT-BTTTT chỉ rõ: "Cơ quan chủ quản có trách nhiệm thông báo rõ các quy định về đảm bảo an toàn và bảo vệ thông tin cá nhân trên trang chủ hoặc cung cấp một cơ chế để người sử dụng dễ dàng tiếp cận và tìm hiểu trên cổng thông tin điện tử".*

Kết quả đánh giá cho thấy, dữ liệu cá nhân trên các giao diện trực tuyến của chính quyền địa phương hiện đang được tự động thu thập khi người dùng đăng ký. Nghĩa vụ cung cấp sự đồng ý có hiểu biết hiện ít được chú ý. Trong số 42 ứng dụng thông minh đang hoạt động và có thể truy cập, không có ứng dụng nào đính kèm chính sách về quyền riêng tư vào hộp "đồng ý". Kể cả đối với 14 ứng dụng yêu cầu xác nhận từ người dùng rằng *"Tôi đồng ý với các điều khoản sử dụng và chính sách về quyền riêng tư của ứng dụng này"*. Trong số 63 cổng DVCTT của tỉnh, thành phố trực thuộc trung ương, có 4 cổng yêu cầu sự đồng ý của người dùng khi đăng ký, nhưng không kèm theo chính sách về quyền riêng tư. Có 13 cổng DVCTT đã liên thông hệ thống đăng ký với Cổng Dịch vụ công quốc gia, liên kết trực tiếp đến các điều khoản sử dụng của Cổng Dịch vụ công quốc gia với một số điều khoản về bảo vệ dữ liệu cá nhân (xem Hộp 5).

Hộp 5: Điều khoản sử dụng có đề cập bảo vệ dữ liệu cá nhân của Cổng dịch vụ công quốc gia

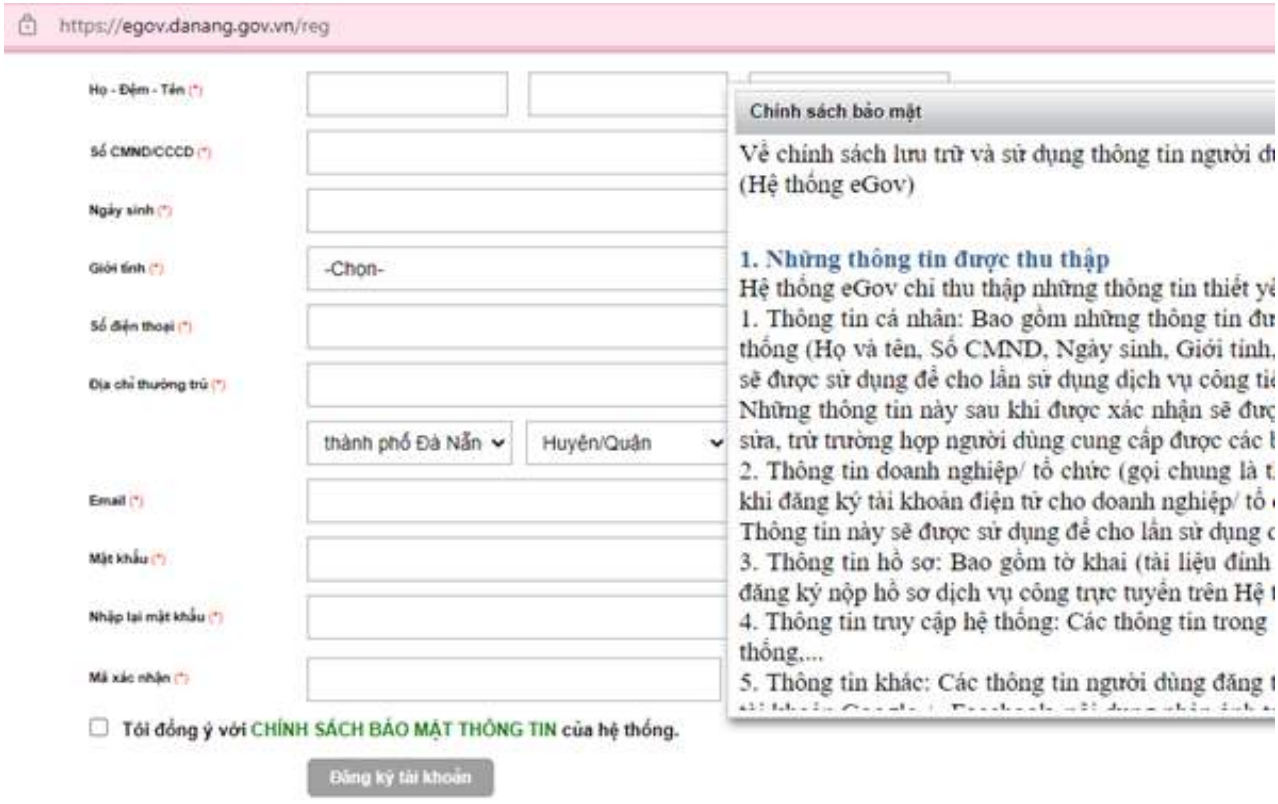
Cổng Dịch vụ công quốc gia **không** chia sẻ thông tin về người sử dụng với các cơ quan khác mà không có sự cho phép của người sử dụng, trừ các trường hợp:

- Việc cung cấp là cần thiết để giải quyết một thủ tục hành chính, dịch vụ công theo yêu cầu của người sử dụng;
- Việc cung cấp thông tin trong trường hợp cần thiết vì lợi ích công cộng, sức khỏe của cộng đồng theo quy định của luật có liên quan.

Nguồn: *Điều khoản và điều kiện sử dụng Cổng Dịch vụ công Quốc gia, truy cập tại: https://dichvucong.gov.vn/p/home/dvc-dieu-khoan-su-dung.html*

Chỉ có hai trường hợp[61] mà hộp "đồng ý" liên kết đến chính sách về quyền riêng tư. Cổng DVCTT của thành phố Đà Nẵng là một ví dụ tốt về thiết kế tích hợp để đảm bảo quyền được thông báo và quyền được đồng ý đầy đủ,[62] khi người dùng có thể đánh dấu vào hộp kiểm và đọc chính sách về quyền riêng tư đính kèm (xem Hình 5).

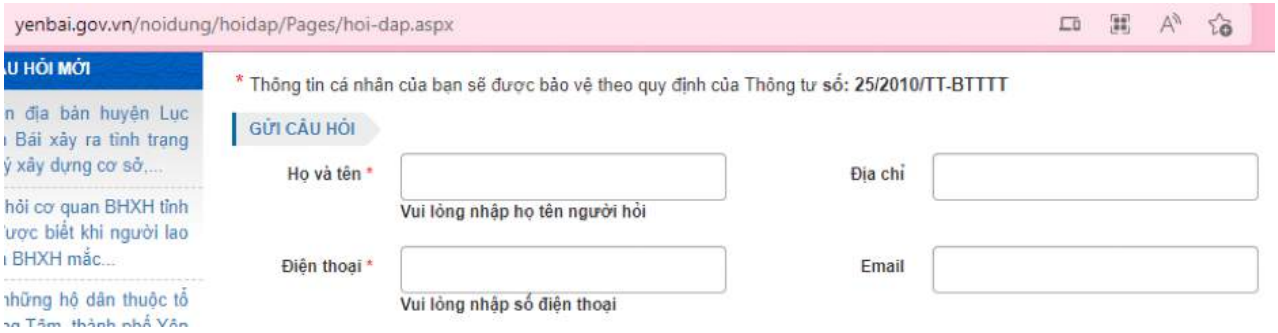
Hình 5: Thực hành tốt trong bảo đảm Quyền đồng ý và được biết – Đà Nẵng



[61] *Tham khảo chi tiết tại: Cổng DVCTT thành phố Đà Nẵng và tỉnh Gia Lai*
[62] *Ở đây chúng tôi chỉ đánh giá việc đáp ứng 2 yêu cầu kỹ thuật là có hộp đồng ý kèm theo chính sách về quyền riêng tư, mà chưa xem xét đến chất lượng của chính sách đó.*

Với cổng TTĐT, 78 kênh thu thập dữ liệu cá nhân trên 63 cổng TTĐT đã được nhóm nghiên cứu xem xét, trong đó 70 kênh không yêu cầu sự đồng ý khi thu thập dữ liệu cá nhân từ người dùng và 7 kênh yêu cầu sự đồng ý nhưng không cung cấp thông tin về chính sách về quyền riêng tư. Chỉ có 1 trường hợp trên cổng TTĐT của tỉnh Yên Bái[63] đính kèm một câu ở đầu phiếu gửi câu hỏi: "Thông tin cá nhân của bạn sẽ được bảo vệ theo quy định của Thông tư số 25/2010/TT-BTTTT" (Hình 6). Mặc dù không phải là chính sách về quyền riêng tư hoàn chỉnh, kênh này ít nhất đã cố gắng thông báo cho người dùng về cách dữ liệu cá nhân của họ sẽ được xử lý và bảo vệ.

Hình 6: Thực hành tốt trong bảo đảm Quyền đồng ý và được biết – Yên Bái



Tiêu chí này nhằm mục đích đo lường mức độ phản hồi của cơ quan Nhà nước bằng cách gửi yêu cầu đến email được cung cấp bởi các giao diện trực tuyến của chính quyền địa phương. Các email đặt ra hai câu hỏi: 1) Cách cập nhật số CMND (từ hệ thống 9 đến 12 số)/Cách khôi phục mật khẩu của tài khoản đã đăng ký; 2) Chia sẻ chính sách về quyền riêng tư dữ liệu của các giao diện trực tuyến/Giải thích cách thông tin cá nhân được bảo vệ khi xử lý thanh toán trực tuyến. Do đa số cổng TTĐT và cổng DVCTT không có chính sách về quyền riêng tư, nhóm nghiên cứu đã gửi:

- 17 thư điện tử đến 17 địa chỉ email liên lạc được cung cấp trong chính sách về quyền riêng tư của 17 ứng dụng thông minh (vì chỉ có 17 trong số 32 chính sách về quyền riêng tư cung cấp email liên hệ).
- 58 thư điện tử đến các địa chỉ email liên lạc được cung cấp trên 58 cổng TTĐT (5 cổng TTĐT của Cần Thơ, Đồng Nai, Hà Nam, Hòa Bình, Quảng Ninh không cung cấp email trên trang chủ).
- 55 thư điện tử đến các địa chỉ email liên lạc được cung cấp trên 55 cổng DVCTT (8 cổng DVCTT của Bạc Liêu, Bắc Ninh, Cà Mau, Cần Thơ, Cao Bằng, Đà Nẵng, Hà Nam, Hà Nội không cung cấp email trên trang chủ).

Trong số 130 email gửi đi, tính đến ngày 06.06.2022, chỉ có 9 email phản hồi: 2 email từ cổng TTĐT của Hải Phòng và Bình Dương, và 7 email từ cổng DVCTT của Kon Tum, Bến Tre, Thanh Hóa, Hưng Yên, Bình Dương, Tiền Giang, Lào Cai. Nhóm nghiên cứu không nhận được phản hồi từ các địa chỉ email được cung cấp trên các ứng dụng.[64] Thời gian phản hồi trung bình 2,22 ngày: nhanh nhất là ngay trong ngày và chậm nhất là 9 ngày. Có 4 thông báo về việc hệ thống không chấp nhận email (do cơ chế chống thư rác).

Bến Tre là ví dụ điển hình tốt vì đã phản hồi chi tiết, đầy đủ đối với tất cả các yêu cầu của chủ thể dữ liệu. Các tỉnh khác chỉ trả lời câu hỏi đầu tiên và thường bỏ qua việc cung cấp chi tiết về biện pháp nào được đưa ra để bảo vệ thông tin cá nhân.[65]

[63] *Tham khảo chi tiết tại: http://yenbai.gov.vn/noidung/hoidap/Pages/hoi-dap.aspx*

[64] *Cổng TTĐT của Hải Phòng và Bình Dương trả lời ngay trong ngày; Cổng DVCTT của Kon Tum trả lời trong 9 ngày làm việc, Bến Tre trong 5 ngày làm việc, Thanh Hóa, Hưng Yên, Lào Cai trong 2 ngày làm việc, Bình Dương trả lời ngay trong ngày.*

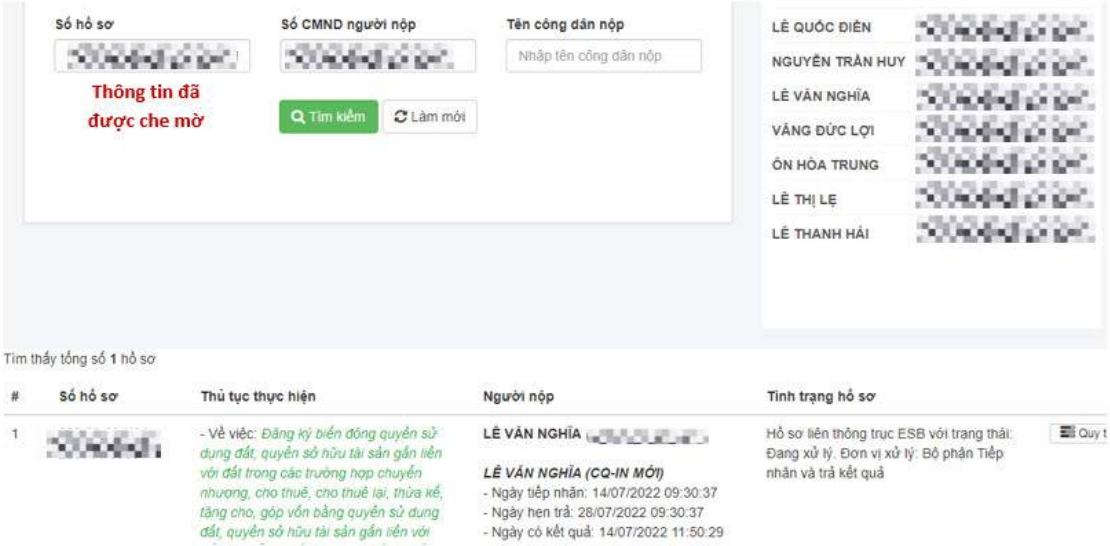
[65] *Xem chi tiết các thực hành tốt và chưa tốt tại Phụ lục*

Quyền hạn chế phạm vi sử dụng thông tin cá nhân

Tiêu chí này đánh giá mức độ quan tâm của chính quyền địa phương đối với việc ẩn danh như một biện pháp để bảo vệ dữ liệu cá nhân của người dùng. Tất cả 42 ứng dụng[66] được xem xét đều có cơ chế ẩn danh tích hợp. Trong đó, 36 ứng dụng có tính ẩn danh tốt[67] và 6 ứng dụng ẩn danh một phần.[68]

Trong số 63 cổng DVCTT, [69] 34 cổng có cơ chế ẩn danh tốt[70] để người dùng kiểm tra tình trạng xử lý các dịch vụ công được yêu cầu và 29 cổng có cơ chế ẩn danh một phần.[71] Ví dụ ở Hình 7 cho thấy, dữ liệu cá nhân như mã số hồ sơ, số định danh cá nhân (số CMND), họ và tên, và nội dung dịch vụ đều công khai. Mặc dù điều này là tốt cho mục đích minh bạch, nhưng lại chưa cân bằng với yêu cầu bảo vệ quyền riêng tư.

Hình 7: Thực hành chưa tốt về ẩn danh tự động



[66] *Đối với các ứng dụng thông minh, nhóm nghiên cứu khảo sát mức độ bảo đảm quyền hạn chế phạm vi sử dụng thông tin cá nhân thông qua biểu hiện kỹ thuật của ứng dụng trong công khai thông tin phản ánh, kiến nghị hiện trường.*

[67] *Thực hành ẩn danh được xếp loại "ẩn danh tốt" nếu thực hiện ẩn tất cả thông tin, ngoại trừ nội dung các khiếu nại và địa điểm xảy ra sự việc được công khai. Ẩn danh tốt được thực hiện theo nguyên tắc công khai tối thiểu.*

[68] *Thực hành ẩn danh được xếp loại "ẩn danh một phần" nếu có hiển thị công khai nhiều hơn các trường thông tin tối thiểu, bao gồm một hoặc nhiều hơn các trường thông tin như tên và họ, địa chỉ lưu trú, số điện thoại, email, ...*

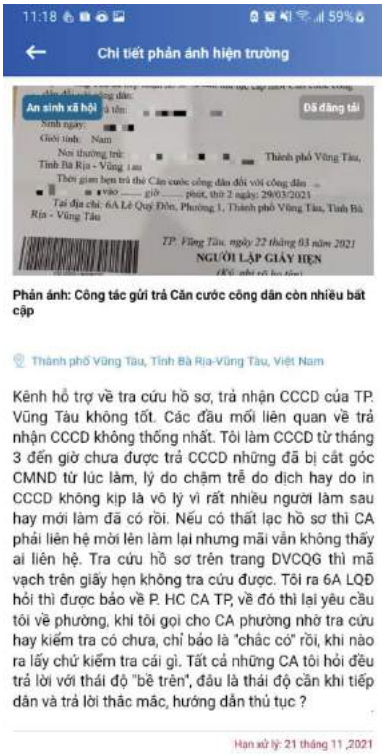
[69] *Đối với các cổng DVCTT, nhóm nghiên cứu khảo sát mức độ bảo đảm quyền hạn chế phạm vi sử dụng thông tin cá nhân thông qua biểu hiện kỹ thuật của cổng trong công khai thông tin tại mục tra cứu hồ sơ.*

[70] *Đối với các cổng DVCTT, thực hành ẩn danh được xếp loại "ẩn danh tốt" nếu thực hiện ẩn tất cả thông tin, bắt buộc người dùng phải nhập mã hồ sơ/ số biên nhận, hoặc các thông tin xác thực khác để truy cập.*

[71] *Đối với các cổng DVCTT, thực hành ẩn danh được xếp loại "ẩn danh một phần" nếu có hiển thị công khai số hồ sơ, tên, số CMND người nộp, và nội dung thủ tục trên cổng. (Như hình chụp)*

Đôi khi, người dùng có ý thức tự bảo vệ tốt (xem ví dụ tại Hình 8). Trong một số trường hợp khác, cơ quan nhà nước vô tình làm lộ thông tin cá nhân trong nội dung phản hồi phản ánh, kiến nghị được đăng tải (xem ví dụ tại Hình 9).

Hình 8: Bà Rịa Vũng Tàu – ví dụ về tự bảo vệ tốt dữ liệu cá nhân



Hình 9: An Giang – ví dụ về tự tiết lộ thông tin

Trong một số trường hợp, người dùng được cung cấp cơ hội để lựa chọn có nên để thông tin cá nhân của họ xuất hiện công khai hay không. Trong số 50 ứng dụng được đánh giá, 5 ứng dụng có tùy chọn bảo mật tích hợp này: Cần Thơ (Can Tho SC); Hòa Bình (Công dân Hòa Bình); Kon Tum (Kon Tum S); Quảng Nam (Smart Quang Nam); Sóc Trăng (Công dân tỉnh Sóc Trăng). Trong số 63 cổng DVCTT được rà soát, có 3 cổng có ưu tiên tích hợp này là Quảng Nam, Vĩnh Phúc và Thừa Thiên - Huế.

Có những thực hành tốt khác như ẩn một phần số điện thoại, đây cũng là một loại biện pháp kỹ thuật để đảm bảo bảo vệ quyền riêng tư có sẵn trên các ƯDTM như Smart Quang Ninh, Smart Nam Dinh, Smart Hai Duong.

Quyền riêng tư của trẻ em

Không có chính sách về quyền riêng tư nào được công bố trên các cổng DVCTT và cổng TTĐT đề cập đến quyền riêng tư của trẻ em. Trong khi đó, một nửa (16/32) chính sách về quyền riêng tư của các ƯDTM đề cập đến khía cạnh quan trọng này, có thể là do các yêu cầu kỹ thuật tích hợp sẵn của Google Play và Apple Store, và các mẫu chính sách về quyền riêng tư có sẵn. Đáng chú ý là các chính sách về quyền riêng tư có vẻ chưa thống nhất về định nghĩa độ tuổi được coi là trẻ em. Trong khi phần lớn đề cập đến bất kỳ ai dưới 13 tuổi, một số ứng dụng khác đề cập đến độ tuổi 18 và 7. Điều này đòi hỏi chính quyền các địa phương phải xem xét cẩn thận cách thức thu thập và xử lý dữ liệu cá nhân của những đối tượng dễ bị tổn thương như trẻ em.[72]

[72] *Xem chi tiết tại Phụ lục*

2.3. Thực tế địa phương so với các nguyên tắc của Liên Hợp quốc

Trong những năm gần đây, nhiều tổ chức quốc tế đã ban hành các quy định, nguyên tắc bảo vệ dữ liệu cá nhân và quyền riêng tư. Năm 2013, Tổ chức Hợp tác và phát triển kinh tế (OECD) đã thông qua *Các Nguyên tắc về quyền riêng tư,* cập nhật các nguyên tắc trước đó từ năm 1980, áp dụng đối với việc thu thập dữ liệu trong cả khối công và tư nhân. Vào tháng 4 năm 2016, Liên minh châu Âu đã thông qua *Quy định chung về bảo vệ dữ liệu* (GDPR), có hiệu lực vào tháng 5 năm 2018 và áp dụng đối với việc thu thập dữ liệu cả trong khối công và tư liên quan đến các nước thành viên EU.[73] Nhận thấy sự cần thiết phải bảo vệ dữ liệu cá nhân, Liên hợp quốc đã thông qua *Các nguyên tắc về dữ liệu cá nhân và quyền riêng tư* vào năm 2018, áp dụng cho tất cả dữ liệu cá nhân được lưu trữ hoặc xử lý bởi các tổ chức thuộc hệ thống của Liên hợp quốc hoặc nhân danh các tổ chức đó.

Mặc dù các văn bản này có nhiều điểm chung, với các khái niệm bảo vệ dữ liệu cá nhân và quyền riêng tư tương tự nhau, phần này dựa trên các nguyên tắc của LHQ để đánh giá việc bảo vệ dữ liệu cá nhân của chính quyền địa phương Việt Nam.[74] Bởi lẽ các nguyên tắc do LHQ đưa ra có nhiều nội dung sát với khung pháp luật và phù hợp với thực tiễn ở Việt Nam, cụ thể trong trường hợp này là thực tiễn bảo vệ dữ liệu cá nhân và quyền riêng tư trên môi trường số của chính quyền địa phương. Hơn nữa, đã có tiền lệ tốt trên thế giới, theo đó các nguyên tắc này đã được sử dụng để rà soát, đánh giá khuôn khổ pháp luật của quốc gia về bảo vệ dữ liệu cá nhân và quyền riêng tư trong hệ thống đăng ký, thống kê hộ tịch và quản lý định danh của chính phủ.[75] Trong khi LHQ đưa ra 10 nguyên tắc, báo cáo này tập trung vào 6 nguyên tắc phù hợp với phạm vi nghiên cứu và cách tiếp cận đánh giá thực thi BVDLCN trong khu vực công từ góc nhìn của công dân là người dùng.

Nguyên tắc công bằng và hợp pháp trong xử lý dữ liệu cá nhân

Theo nguyên tắc của Liên Hợp quốc, dữ liệu cá nhân cần được xử lý một cách công bằng trên cơ sở có sự đồng ý của chủ thể dữ liệu, hoặc theo quy định pháp luật. Mặc dù nguyên tắc xử lý công bằng và hợp pháp có thể được đảm bảo ở nhiều khía cạnh, nghiên cứu này tập trung vào việc đo lường sự công bằng và tính hợp pháp của việc xử lý dữ liệu cá nhân dựa trên các tiêu chí sau: sự đồng ý của người dùng; khả năng tiếp cận ngôn ngữ; và viện dẫn cơ sở pháp lý.

Pháp luật Việt Nam đã ghi nhận tầm quan trọng của việc có được sự đồng ý của chủ thể dữ liệu trước khi thu thập và xử lý dữ liệu cá nhân. Tuy nhiên, nguyên tắc này chưa nhận được sự quan tâm đầy đủ từ chính quyền địa phương trên các giao diện kỹ thuật số. Kết quả từ đánh giá này cho thấy các đối tượng dữ liệu hiếm khi được trao quyền đồng ý. Trong số 42 ứng dụng được xem xét, không có ứng dụng nào tạo điều kiện đầy đủ để người dùng thể hiện sự đồng ý có hiểu biết, bao gồm hộp kiểm đồng ý; và liên kết tới chính sách về quyền riêng tư.[76] Trong số 63 cổng DVCTT, chỉ có 2 tỉnh Đà Nẵng và Gia Lai cung cấp hộp kiểm đồng ý có liên kết tới chính sách về quyền riêng tư. Một xu thế tương tự có thể được quan sát thấy trên các cổng TTĐT: 70 trong số 78 kênh thu thập dữ liệu cá nhân không yêu cầu sự đồng ý của người dùng.

Ngôn ngữ cũng đặt ra rào cản đối với việc đảm bảo xử lý dữ liệu cá nhân được thực hiện công bằng và hợp pháp. Có tới 40% chính sách về quyền riêng tư hiện tại không có sẵn bằng tiếng Việt (chưa kể số lượng giao diện không có chính sách về quyền riêng tư). Bên cạnh đó, mặc dù đã có nhiều quy định cụ thể, nhưng chỉ có 1 trong số 39 chính sách về quyền riêng tư được rà soát trích dẫn các văn bản quy phạm pháp luật quan trọng (Nghị định số 64/2007/NĐ-CP và Thông tư số 25/2010/TT-BTTTT) để cung cấp cơ sở pháp lý cho việc thu thập và sử dụng dữ liệu cá nhân của các cơ quan nhà nước trên giao diện số.

---

[73] GDPR có đối tượng điều chỉnh gồm: 1) Cá nhân, pháp nhân, tổ chức EU thực hiện hành vi kiểm soát, xử lý dữ liệu cá nhân; 2) Cá nhân, pháp nhân, tổ chức ngoài EU thực hiện hành vi kiểm soát, xử lý dữ liệu cá nhân của người ở EU; 3) Cá nhân, pháp nhân, tổ chức không ở EU nhưng áp dụng theo nguyên tắc của công pháp quốc tế (cơ quan ngoại giao của quốc gia thành viên EU ở nước ngoài, tàu bay, tàu biển hoạt động ngoài EU có quốc tịch của quốc gia thành viên EU.

[74] Ủy ban cấp cao về quản lý của LHQ, Các nguyên tắc về bảo vệ dữ liệu cá nhân và quyền riêng tư, thông qua tại phiên họp thứ 36 ngày 11/10/2018. Có thể tải về từ: https://archives.un.org/sites/archives.un.org/files/_un-principles-on- personal-data-protection-privacy-hlcm-2018.pdf

[75]Liên Hợp quốc, Hướng dẫn xây dựng khung pháp lý về hệ thống đăng ký, thống kê hộ tịch và quản lý định danh, New York, 2019, trang 152 – 159; có thể tải về tại: https://unstats.un.org/unsd/demographic-social/Standards-and- Methods/files/Handbooks/crvs/CRVS_GOLF_Final_Draft-E.pdf

[76] Ở đây nhóm nghiên cứu chỉ đánh giá việc đáp ứng 2 yêu cầu kỹ thuật là có hộp đồng ý kèm theo chính sách về quyền riêng tư, mà chưa xem xét chất lượng của chính sách đó.

Nguyên tắc làm rõ mục đích thu thập, xử lý thông tin cá nhân

Theo nguyên tắc này của LHQ, dữ liệu cá nhân chỉ được xử lý cho mục đích đã được cụ thể hóa từ trước.[77] Tuy nhiên, như đã trình bày, hơn 70% chính sách về quyền riêng tư được rà soát không cung cấp đầy đủ chi tiết về mục đích và không đảm bảo một phần riêng biệt trong nội dung của chính sách về quyền riêng tư. Hầu hết chỉ dừng lại ở mô tả chung chung các mục đích như (i) để tạo trải nghiệm tốt hơn cho người dùng; (ii) để xác định người dùng; (iii) để đáp ứng yêu cầu của người dùng; (iv) để quản lý tương tác trực tuyến; và (v) để liên hệ.

Có trường hợp chính sách về quyền riêng tư đề cập mục đích không chính đáng trong xử lý dữ liệu cá nhân. Ví dụ như ƯDTM Smart Quảng Ninh, vì chính sách về quyền riêng tư được biên soạn bởi công ty có tên AIC thay vì chính quyền địa phương, cho nên AIC tuyên bố, có thể kết hợp dữ liệu cá nhân với thông tin từ bên ngoài hoặc bên thứ ba để phân tích nội dung nào người dùng quan tâm. Điều này vi phạm pháp luật, vì AIC là đơn vị cung cấp dịch vụ nên sẽ không có quyền truy cập vào dữ liệu cá nhân hoặc có bất kỳ quyền quyết định nào trong việc xác định mục đích xử lý dữ liệu cá nhân người dùng.

Nguyên tắc tương xứng và cần thiết

Theo nguyên tắc này, *"việc xử lý dữ liệu cá nhân phải có liên quan, có giới hạn, và phù hợp với những gì cần thiết liên quan đến các mục đích cụ thể của việc xử lý dữ liệu cá nhân"*. So với hai nguyên tắc nói trên, nguyên tắc này vẫn chưa được thể hiện rõ trong các quy định hiện hành ở Việt Nam, mặc dù Điều 6 của Thông tư số 25/2010/TT-BTTTT quy định rằng cơ quan chủ quản phải cung cấp cơ chế cho các chủ thể dữ liệu để hạn chế nội dung và phạm vi sử dụng dữ liệu cá nhân.

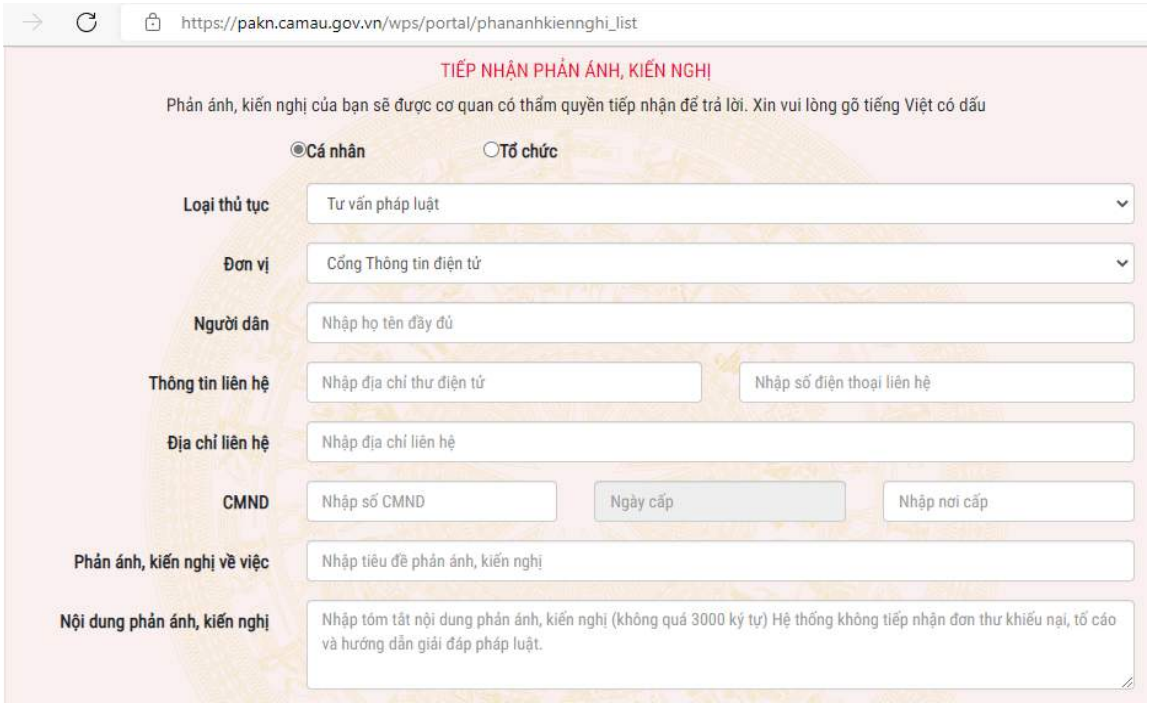
Trong thực tiễn, đánh giá này cho thấy chính quyền địa phương rất chú trọng đến việc ẩn danh như một biện pháp để bảo vệ dữ liệu cá nhân của người dùng. Tất cả 42 ứng dụng đang hoạt động và có thể truy cập được đều đã tích hợp cơ chế ẩn danh tự động. Chỉ có 34 trong số 63 cổng DVCTT có cơ chế ẩn danh tốt trong công khai tiến độ cung cấp dịch vụ công.

Tuy nhiên, nguyên tắc tương xứng và cần thiết vẫn có thể bị vi phạm theo hai hướng: (1) khi cổng thông tin/ứng dụng trực tuyến yêu cầu người dùng gửi nhiều thông tin hơn mức cần thiết cho một mục đích cụ thể; và (2) khi các cổng thông tin/ứng dụng trực tuyến công khai nhiều thông tin hơn mức cần thiết cho mục đích minh bạch.

[77] *Nguyên tắc này cũng được ghi nhận ở Việt Nam tại Điều 21 Luật Công nghệ thông tin và Điều 5 Thông tư số 25/2010/TT-BTTTT.*

Ví dụ điển hình 1: Trên cơ chế tiếp nhận phản ánh kiến nghị trực tuyến của Cà Mau (xem Hình 10), người dùng được yêu cầu cung cấp thông tin về ngày cấp và nơi cấp thẻ căn cước công dân. Những thông tin này không liên quan đến việc nộp đơn khiếu nại. Thêm vào đó, số thẻ căn cước cũng như các thông tin đi kèm dễ bị lạm dụng cho mục đích trộm cắp danh tính (xem chú thích số 11).

Hình 10: Thực hành chưa tốt về tính cần thiết – Yêu cầu điền ngày cấp và nơi cấp CMND



Ví dụ điển hình 2: Trong phần hỏi đáp của trang web thành phố Hồ Chí Minh (xem Hình 11), việc thu thập năm sinh và giới tính cho mục đích hỏi đáp là không liên quan và không cần thiết.

Hình 11: Thực hành chưa tốt của nguyên tắc thu thập thông tin tối thiểu

Ngược lại, có những ví dụ tốt từ Hòa Bình[78] và Hà Nội,[79] khi người dùng chỉ cần cung cấp họ tên và email khi gửi câu hỏi trên cổng thông tin trực tuyến

[78] *Gửi câu hỏi - Cổng thông tin điện tử Tỉnh Hòa Bình*
[79] *Cổng Giao tiếp điện tử Thành Phố Hà Nội*

Ví dụ điển hình 3: Trong trường hợp từ cổng TTĐT của Khánh Hòa (xem Hình 12), cơ quan chức năng đã vô tình công bố nhiều thông tin cá nhân hơn mức cần thiết. Trong trường hợp không thể trả lời mà không tiết lộ thông tin cá nhân, chính quyền địa phương có thể tóm tắt nội dung chính (bà Trinh có thể liên hệ với các phòng nghiệp vụ công an địa phương hoặc liên hệ với cơ quan công an thành phố Nha Trang để có được các tài liệu cần thiết) để công bố trên cổng TTĐT, đồng thời gửi email cá nhân, hoặc gọi điện thoại cho công dân để cung cấp thêm chi tiết, thay vì đăng tải công khai trên các cổng. Một phương án xử lý khác là làm mờ thông tin cá nhân trước khi công khai.

Hình 12: Thực hành chưa tốt – CQNN vô tình làm lộ thông tin cá nhân

Thời gian nhận được thẻ CCCD

09/09/2021 | 11:40 AM (GMT+7) Thích 0 Chia sẻ A+ A- A

Chứng minh nhân dân của tôi hết hạn tháng 4-2021. Tuy nhiên, tôi không làm được căn cước công dân do không có thông tin trên hệ thống. Ngày 8-7, tôi đã làm tại Công an TP. Nha Trang. Tôi muốn hỏi khoảng bao lâu tôi có thể nhận được? Do chứng minh nhân dân cũ đã hết hạn quá lâu và hiện giờ tôi rất cần căn cước công dân. Tôi không có 1 giấy tờ nào thay thế được. Chứng minh nhân dân cũ của tôi số: [redacted]

Cơ quan hành chính trả lời

Về vấn đề này, Công an TP. Nha Trang trả lời như sau:

Ngày 7-7-2021, Công an TP Nha Trang có thu nhận hồ sơ cấp căn cước công dân (CCCD) của công dân Phạm [redacted] sinh ngày [redacted] khẩu thường trú: [redacted] Nha Trang đã xử lý hồ sơ, chuyển dữ liệu lên Trung ương và đã được duyệt cấp thẻ, đang chờ Cục C06 trả thẻ về. Ngày sau khi nhận được thẻ, Công an TP. Nha Trang sẽ liên hệ công dân Phạm Thị Thu Trinh lên nhận thẻ CCCD.

Trong thời gian chưa được cấp CCCD, công dân Phạm Thị Thu Trinh có thể liên hệ Công an xã, phường để cấp giấy thông báo số định danh cá nhân hoặc liên hệ Công an TP. Nha Trang để cấp giấy xác nhận đang thực hiện cấp CCCD. Hai giấy tờ trên có giá trị thay thế căn cước công dân để thực hiện giao dịch cá nhân.

Ban Biên tập trân trọng cảm ơn Công an TP. Nha Trang đã có thông tin phản hồi công dân qua Cổng Thông tin điện tử tỉnh Khánh Hòa.

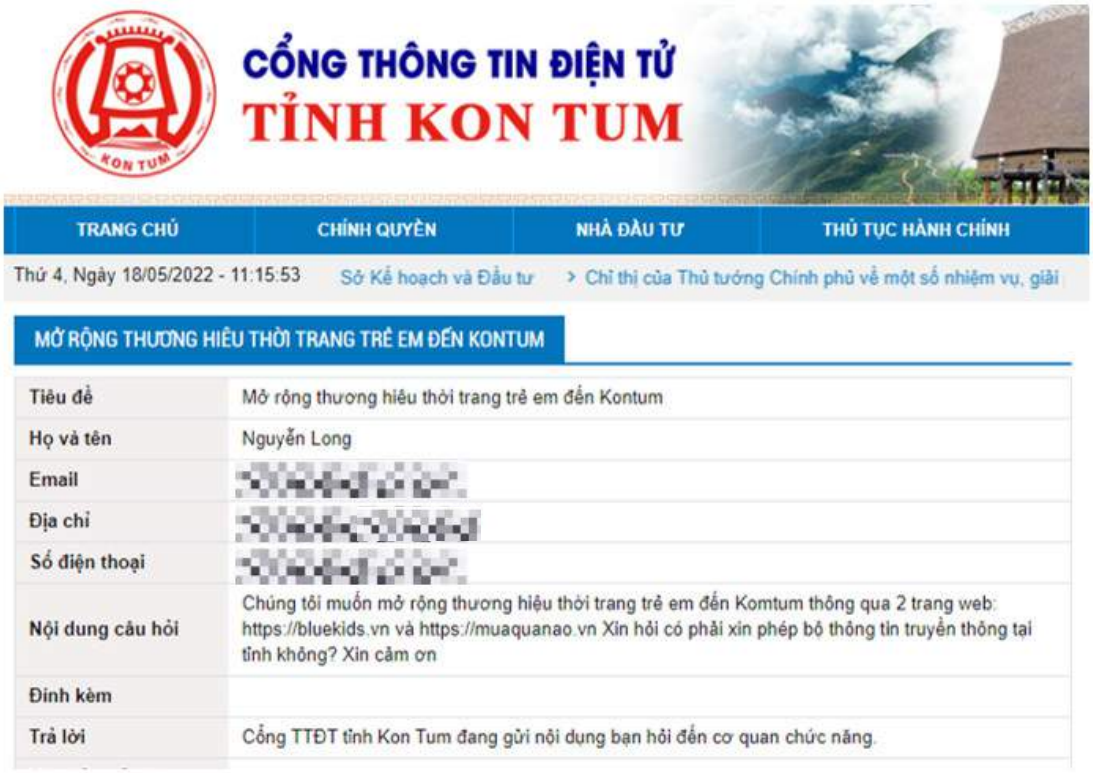
BBT

Ngày trả lời: 15/10/2021

Ví dụ điển hình 4: Trong phần hỏi đáp cổng TTĐT của Kon Tum (xem hình 13), không có cơ chế lọc để hạn chế nhận dạng người dùng. Có thể thấy từ hình dưới đây, cổng thông tin thu thập 4 trường dữ liệu cá nhân: (1) Họ và tên; (2) Email; (3) Địa chỉ; và (4) Số điện thoại. Tất cả bốn trường thông tin này được tự động công khai. Mặc dù có ý định tốt là minh bạch về câu hỏi và trả lời, việc tiết lộ thông tin là nhiều hơn cần thiết với mục đích cần được công khai. Theo một khiếu nại được tìm thấy trên cổng TTĐT của Đà Nẵng,[80] việc có được tên đầy đủ và số điện thoại di động là đã đủ để những kẻ lừa đảo có thể thực hiện giao dịch bất hợp pháp.

[80] *Xem chi tiết tại: http://hoidap.danang.gov.vn/CD_TraCuu.aspx*

Hình 13: Thực hành chưa tốt về thiếu cơ chế kỹ thuật làm ẩn thông tin



Nguyên tắc lưu trữ thông tin cá nhân

Nguyên tắc này yêu cầu dữ liệu cá nhân chỉ nên được lưu trữ trong thời gian cần thiết vì các mục đích được xác định rõ. Thời gian lưu trữ phụ thuộc vào mục đích thu thập và xử lý dữ liệu cá nhân. Trong nghiên cứu này, có hai dạng mục đích riêng biệt để xử lý dữ liệu cá nhân:

i. Đối với hồ sơ định danh công dân: Ví dụ như dữ liệu cá nhân được thu thập để đăng ký hộ tịch và quản lý định danh trên cổng DVCTT, theo luật định, các dạng dữ liệu cá nhân này sẽ được lưu trữ dài hạn nhằm mục đích pháp lý, thống kê và quản lý hành chính. Các cơ quan Nhà nước có trách nhiệm thông báo cho công dân về thời gian lưu trữ trong các chính sách về quyền riêng tư. Thông điệp lưu trữ dài hạn phải được truyền đạt rõ ràng trước khi công dân đồng ý cung cấp dữ liệu cá nhân của họ.

Ví dụ điển hình 1: Chính sách về quyền riêng tư trên ứng dụng thông minh Hậu Giang là một ví dụ tốt về thông báo thời gian lưu trữ. Theo đó, dữ liệu cá nhân của người dùng sẽ được lưu trữ đến khi đơn vị chủ quản có yêu cầu huỷ bỏ. Còn lại trong mọi trường hợp thông tin người dùng sẽ được lưu trữ bảo mật trên máy chủ của cơ quan quản lý nhà nước.[81]

[81] *CHÍNH SÁCH VỀ QUYỀN RIÊNG TƯ THÔNG TIN*

ii. Đối với mục đích khảo sát ngẫu nhiên: Dữ liệu cá nhân được thu thập khi các cơ quan Nhà nước thu thập ý kiến/quan điểm từ công dân về một vấn đề cụ thể. Chẳng hạn, tỉnh Thừa Thiên - Huế triển khai khảo sát Góp ý hiến kế xây dựng tỉnh Thừa Thiên - Huế (xem Hình 14).[82] Trong trường hợp này, cơ quan nhà nước thu thập thông tin cá nhân bao gồm họ tên đầy đủ, địa chỉ thường trú, điện thoại, email. Vì các số liệu thống kê này chỉ phục vụ cho một cuộc điều tra ý kiến, không phải là số liệu thống kê quan trọng, cơ quan nhà nước cần công khai thời gian lưu trữ, cung cấp cơ chế cho công dân thực hiện "quyền được lãng quên",[83] tức là có quyền yêu cầu xóa dữ liệu cá nhân của mình, và dữ liệu cá nhân sẽ bị xóa sau khi đạt được mục đích của cuộc khảo sát. Tuy nhiên, không dễ xác định rõ ràng, số liệu thống kê nào được coi là quan trọng vì có những trường hợp dữ liệu về người mắc COVID-19, khi xảy ra xung đột giữa quyền riêng tư và lợi ích công cộng, khi đó việc lưu trữ dữ liệu của bệnh nhân COVID-19 có thể được kéo dài hoặc chuyển sang được coi là số liệu thống kê quan trọng.

Hình 14: Ví dụ về thu thập DLCN qua khảo sát không thường xuyên ở địa phương

Nói chung, nguyên tắc về lưu trữ dữ liệu cá nhân vẫn chưa được giải quyết thỏa đáng trong các chính sách về quyền riêng tư của các tỉnh, thành. Chỉ có 6 trong số 39 chính sách về quyền riêng tư được rà soát thông báo cho người dùng về thời gian lưu trữ dữ liệu cá nhân và 5 trong số đó chỉ cung cấp mô tả ngắn gọn mà không chỉ rõ điều kiện để xóa dữ liệu cá nhân cũng như thời gian lưu trữ.

Nguyên tắc minh bạch

Nguyên tắc minh bạch yêu cầu *"Xử lý dữ liệu cá nhân phải được thực hiện minh bạch đối với các chủ thể dữ liệu một cách phù hợp và bất cứ khi nào có thể. Điều này nên bao gồm, ví dụ, cung cấp thông tin về việc xử lý dữ liệu cá nhân của họ, cũng như thông tin về cách yêu cầu truy cập, xác minh, chỉnh sửa và /hoặc xóa dữ liệu cá nhân đó."* Ở Việt Nam, nguyên tắc này cũng được ghi nhận rõ trong Luật Công nghệ thông tin (2006), Nghị định số 64/2007/NĐ-CP và Thông tư số 25/2010/TT-BTTTT.

[82] *Góp ý - Hiến kế xây dựng tỉnh Thừa Thiên Huế*
[83] *Điều 3 và Điều 16 của Dự thảo Nghị định quy định về BVDLCN của Việt Nam ghi nhận quyền được lãng quên khi cho phép chủ thể dữ liệu có quyền yêu cầu xóa dữ liệu cá nhân: https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Du-thao-Nghi-dinh-quy-dinh-ve-bao-ve-du-lieu-ca-nhan-465185.aspx*

Đánh giá về tính sẵn có và chất lượng của các chính sách về quyền riêng tư cho thấy nguyên tắc minh bạch chưa được chú trọng trên các giao diện kỹ thuật số của khu vực công Việt Nam. Trong số 63 cổng DVCTT, chỉ có 3 cổng công bố chính sách về quyền riêng tư của họ. Trong số 63 cổng TTĐT, chỉ có 4 cổng chia sẻ chính sách về quyền riêng tư. Trong số 50 tỉnh có ƯDTM hoạt động, không thể truy cập được các chính sách về quyền riêng tư của 18 ứng dụng. Về chất lượng, không có chính sách về quyền riêng tư được rà soát nào đảm bảo các yêu cầu minh bạch trong các quy định hiện hành. Đa số không chia sẻ đầy đủ thông tin về cách yêu cầu truy cập, xác minh, chỉnh sửa và/hoặc xóa dữ liệu cá nhân. Như đã đề cập trước đây, khoảng hai phần ba chính sách về quyền riêng tư thiếu các chi tiết cần thiết để làm rõ mục đích xử lý dữ liệu cá nhân.

Ngoài ra, nguyên tắc minh bạch khuyến khích cơ quan chủ quản (Ủy ban nhân dân) kịp thời cảnh báo rủi ro về quyền riêng tư và vi phạm dữ liệu cá nhân cho công chúng. Mặc dù hầu hết các cổng TTĐT và ứng dụng được rà soát chưa bảo đảm nguyên tắc này, nhưng có một số cách làm tốt. Chính sách về quyền riêng tư của các ứng dụng Bạc Liêu và Bình Định nêu rõ: *"Chúng tôi đánh giá cao sự tin tưởng của bạn khi cung cấp cho chúng tôi thông tin cá nhân của bạn, do đó chúng tôi đang cố gắng sử dụng các phương tiện được chấp nhận về mặt thương mại để bảo vệ thông tin đó. Tuy nhiên, cần lưu ý rằng, không có phương pháp truyền qua internet, hoặc phương pháp lưu trữ điện tử nào an toàn và đáng tin cậy 100%, và chúng tôi không thể đảm bảo an toàn tuyệt đối". Ứng dụng Hậu Giang cũng nêu rõ: "Trong trường hợp máy chủ lưu trữ thông tin người dùng bị hacker tấn công dẫn đến mất mát dữ liệu cá nhân, chúng tôi có trách nhiệm thông báo đến người dùng thông qua ứng dụng Hậu Giang."*

Nguyên tắc trách nhiệm giải trình

Theo đánh giá sơ bộ, thực tiễn các kênh tương tác trực tuyến của chính quyền địa phương chưa tuân thủ nguyên tắc trách nhiệm giải trình, vì hầu hết các chính sách về quyền riêng tư không xác định chính xác các cơ quan nhà nước chịu trách nhiệm. Chỉ có 1 trong số 39 chính sách về quyền riêng tư nêu rõ Ủy ban Nhân dân là cơ quan chịu trách nhiệm bảo vệ dữ liệu cá nhân. Gần một nửa (15/32) các chính sách về quyền riêng tư được rà soát trình bày mơ hồ, trong trường hợp đó đại từ *"chúng tôi"* được sử dụng mà không làm rõ *"chúng tôi"* là ai trong mối quan hệ hợp đồng bảo mật với các chủ thể dữ liệu. Các chính sách khác đề cập đến các đơn vị tư nhân hoặc Sở TTTT như các bên của chính sách về quyền riêng tư.

Chính sách về quyền riêng tư thiết lập thỏa thuận giữa chủ thể dữ liệu và cơ quan chủ quản. Do vậy, việc xác định sai các cơ quan có trách nhiệm sẽ dẫn đến khó khăn trong việc bảo vệ quyền của chủ thể dữ liệu như quyền truy cập, sửa chữa hoặc xóa dữ liệu khi được yêu cầu, giải quyết các khiếu nại hành chính và tư pháp, thông báo vi phạm dữ liệu cá nhân cho các chủ thể dữ liệu. Điển hình là trong cơ chế liên hệ, chỉ có 8 chính sách về quyền riêng tư cung cấp email công vụ của cơ quan nhà nước, trong khi 13 chính sách cung cấp email cá nhân/doanh nghiệp. Thậm chí, chính sách về quyền riêng tư trên các ƯDTM của Cần Thơ và Quảng Nam có chung địa chỉ email liên hệ *quanb1401083tggdev@gmail.com.*

Bên cạnh đó, trong các chính sách về quyền riêng tư của các ƯDTM, các nhà phát triển ứng dụng thường bị nhầm lẫn là một trong những bên của thỏa thuận với chủ thể dữ liệu. Theo quy định của pháp luật, các nhà cung cấp dịch vụ (nhà phát triển ứng dụng) cần ký hợp đồng với các cơ quan có trách nhiệm (Ủy ban nhân dân) để đảm bảo rằng họ không có quyền truy cập vào dữ liệu cá nhân. UBND có trách nhiệm giám sát xem các nhà cung cấp dịch vụ có thực sự tuân thủ các nghĩa vụ pháp lý của họ để bảo vệ bí mật và bảo mật dữ liệu cá nhân hay không. Về nguyên tắc, các nhà cung cấp dịch vụ không có quyền truy cập vào dữ liệu cá nhân và không thể đáp ứng các quyền truy cập và chỉnh sửa dữ liệu và các nhà cung cấp dịch vụ không nên được xác định là đầu mối liên lạc cho các chủ thể dữ liệu.

III. HÀM Ý CHÍNH SÁCH VÀ KHUYẾN NGHỊ

MỘT SỐ KHUYẾN NGHỊ CHÍNH

ĐÁNH GIÁ VIỆC BẢO VỆ DỮ LIỆU CÁ NHÂN TRÊN CÁC NỀN TẢNG TƯƠNG TÁC VỚI NGƯỜI DÂN CỦA CHÍNH QUYỀN ĐỊA PHƯƠNG

PHÂN BIỆT GIỮA AN TOÀN, BẢO MẬT DỮ LIỆU VÀ TÍNH RIÊNG TƯ

	AN TOÀN, BẢO MẬT DỮ LIỆU	TÍNH RIÊNG TƯ CỦA DỮ LIỆU
Đối tượng bảo vệ	Hệ thống công nghệ thông tin	Người dùng (công dân)
Nội hàm	Bảo vệ: ✓ Tính toàn vẹn dữ liệu ✓ Tính bảo mật dữ liệu ✓ Tính sẵn có của dữ liệu	Các quyền của người dùng: ✓ Quyền đồng ý ✓ Quyền yêu cầu cập nhật ✓ Sửa đổi, xoá ✓ Quyền tiếp cận ✓ ...
Công cụ bảo vệ/ thực thi	✓ Hướng dẫn kỹ thuật ✓ Quy định nội bộ ✓ Hợp đồng dịch vụ với các điều khoản bảo vệ dữ liệu cá nhân	✓ Chính sách về quyền riêng tư và cơ chế cho phép lựa chọn sự đồng ý ✓ Nghĩa vụ thông báo ✓ Nghĩa vụ pháp lý

HOÀN THIỆN KHUNG CHÍNH SÁCH, PHÁP LUẬT QUỐC GIA

1 Hoàn thiện quy định về định nghĩa, phân loại dữ liệu cá nhân

2 Hoàn thiện quy định về trách nhiệm của các bên

✓ Phân định rõ Chủ thể kiểm soát dữ liệu và **Chủ thể vận hành dữ liệu**
Chú trọng phát triển 03 công cụ trong thông tư hướng dẫn:
(1) Chính sách về quyền riêng tư mẫu
(2) Điều khoản sử dụng mẫu
(3) Hợp đồng mẫu với đơn vị vận hành

✓ Thừa nhận **chính sách về quyền riêng tư** như một dạng **thỏa thuận điện tử**

✓ Bổ sung **quy trình làm rõ trách nhiệm** giữa các cơ quan nhà nước trong **chia sẻ dữ liệu cá nhân**

3 Minh bạch hóa và đánh giá tác động quyền riêng tư

✓ Hoàn thiện các quy định về xử lý vi phạm

Quy định về chế tài đối với vi phạm liên quan đến dữ liệu cá nhân (bổ sung trong Luật Trách nhiệm bồi thường nhà nước năm 2017)

Thiết lập hệ thống tập trung để tiếp nhận, xử lý yêu cầu, khiếu nại về dữ liệu cá nhân

✓ Thiết chế hóa **đầu mối phụ trách bảo vệ dữ liệu cá nhân**

GIẢI PHÁP KỸ THUẬT

1 Hiện đại hóa điện toán đám mây

2 Quy định về trách nhiệm của cơ quan quản lý đối với hồ dữ liệu

✓ **Về mặt hình thức:**
Cam kết trách nhiệm trước khi đảm nhận vị trí công tác

✓ **Về mặt kỹ thuật:**
(1) Đưa ra yêu cầu chấp nhận đồng ý với bản cam kết đảm bảo thông tin, đồng thời ghi lại nhật ký khai thác dữ liệu công dân (có thể truy xuất khi cần thiết)

(2) Lưu lại các thao tác, hành vi truy cập khai thác thông tin để có căn cứ xử lý vi phạm (nếu có) theo quy định

(3) Áp dụng tiêu chuẩn ISO 27701 liên quan đến bảo vệ dữ liệu cá nhân

GIÁM SÁT ĐÁNH GIÁ THỰC HÀNH BẢO VỆ DỮ LIỆU CÁ NHÂN

1 Minh bạch về sự cố dữ liệu và đánh giá tác động tới quyền riêng tư dữ liệu cá nhân

2 Bổ sung tiêu chí Bảo vệ dữ liệu cá nhân vào bộ Chỉ số Đánh giá chuyển đổi số (DTI) của Bộ Thông tin và Truyền thông

✓ Chính sách về quyền riêng tư của giao diện trực tuyến có được công khai?

✓ Các cơ quan nhà nước đã áp dụng ISO 27701 hay chưa?

✓ Cơ quan Nhà nước đã tổ chức tập huấn về bảo vệ dữ liệu cá nhân chưa?

✓ Đánh giá tác động quyền riêng tư có thường xuyên được thực hiện?

✓ UBND cấp tỉnh đã bố trí nhân sự đầu mối về bảo vệ dữ liệu cá nhân?

3 Đánh giá độc lập mức độ thực thi bảo vệ dữ liệu cá nhân trong khu vực công của các hiệp hội doanh nghiệp và bảo vệ người tiêu dùng

HÀM Ý CHÍNH SÁCH VÀ KHUYẾN NGHỊ

ĐÁNH GIÁ VIỆC BẢO VỆ DỮ LIỆU CÁ NHÂN TRÊN CÁC GIAO DIỆN TƯƠNG TÁC VỚI NGƯỜI DÂN CỦA CHÍNH QUYỀN ĐỊA PHƯƠNG

XÁC ĐỊNH ĐÚNG CHỦ THỂ KIỂM SOÁT DỮ LIỆU

✅ **Nên xác định UBND tỉnh là Chủ thể kiểm soát dữ liệu**

Ví dụ từ Chính sách về quyền riêng tư của Ứng dụng thông minh tỉnh Hậu Giang

Địa chỉ của đơn vị thu thập và quản lý thông tin cá nhân
UBND tỉnh Hậu Giang
Địa chỉ: Số 2, Hòa Bình, TP. Vị Thanh, Hậu Giang
Điện thoại: 0293.3878840

❌ **Không nên xác định tổ chức/ doanh nghiệp cung cấp dịch vụ cho cơ quan nhà nước là Chủ thể kiểm soát dữ liệu**

Ví dụ từ Chính sách về quyền riêng tư của Ứng dụng thông minh Smart Quảng Ninh

Thỏa thuận sử dụng và bảo mật này được lập ra bởi giữa bạn và Công ty Cổ phần tiến bộ Quốc tế AIC về việc sử dụng bất kỳ hay tất cả các loại dịch vụ của ứng dụng Smart Quảng Ninh của bạn

❌ **Không nên xác định trang thông tin điện tử là Chủ thể kiểm soát dữ liệu**

Ví dụ từ Chính sách đảm bảo an toàn thông tin cá nhân của Cổng Thông tin Điện tử Thành phố Hà Nội

Nhằm bảo đảm an toàn cho Cổng giao tiếp điện tử thành phố Hà Nội, đồng thời bảo mật thông tin khách hàng, Trang thông tin điện tử của Thành phố Hà Nội (HNP) đưa ra Chính sách bảo mật thông tin cá nhân (Privacy Policy) dành cho các tổ chức và cá nhân truy cập HNP

BẢO ĐẢM QUYỀN ĐƯỢC ĐỒNG Ý VÀ ĐƯỢC BIẾT

✅ **Nên cung cấp:**
1) Hộp kiểm đồng ý
2) Chính sách về quyền riêng tư đính kèm

Ví dụ từ Cổng dịch vụ công điện tử Thành phố Đà Nẵng

❌ **Không nên chỉ cung cấp Hộp điểm đồng ý mà thiếu Chính sách về quyền riêng tư đính kèm**

Ví dụ từ Cổng dịch vụ công tỉnh Bình Thuận

❌ **hoặc không cung cấp cả hai**

Ví dụ từ Cổng dịch vụ công tỉnh Cao Bằng

❌ **Không nên chỉ đưa ra điều khoản yêu cầu cung cấp đúng thông tin, sự thật mà thiếu đi chính sách về quyền riêng tư cho người dùng**

Ví dụ từ Ứng dụng "VUNGTAUIOC-Civ (Công dân - Phản ánh hiện trường)"

THU THẬP THÔNG TIN CÁ NHÂN TƯƠNG XỨNG VỚI MỤC ĐÍCH, CĂN CỨ TRÊN SỰ CẦN THIẾT

✅ **Nên thu thập thông tin cá nhân trên nguyên tắc tối thiểu**

Ví dụ từ Cổng dịch vụ công điện tử tỉnh Lạng Sơn

❌ **Không nên thu thập thông tin nhiều hơn mức cần thiết**

Ví dụ từ Hệ thống tiếp nhận, trả lời phản ánh, kiến nghị của người dân tỉnh Cà Mau

❌ **Không nên công khai thông tin nhiều hơn mức cần thiết**

Ví dụ từ Mục hỏi - đáp Cổng thông tin điện tử tỉnh Kon Tum

HÀM Ý CHÍNH SÁCH VÀ KHUYẾN NGHỊ

ĐÁNH GIÁ VIỆC BẢO VỆ DỮ LIỆU CÁ NHÂN TRÊN CÁC GIAO DIỆN TƯƠNG TÁC VỚI NGƯỜI DÂN CỦA CHÍNH QUYỀN ĐỊA PHƯƠNG

QUY ĐỊNH RÕ THỜI GIAN PHẢN HỒI

✓ **Nên quy định cụ thể thời gian phản hồi cho người dùng**

Ví dụ từ Cổng thông tin điện tử tỉnh Thừa Thiên Huế

✗ **Không nên quy định thời gian chung chung**

Ví dụ từ Ứng dụng thông minh Lạng Sơn Trực tuyến

CÔNG KHAI SỰ CỐ DỮ LIỆU VÀ BIỆN PHÁP XỬ LÝ

✓ **Nên công khai cam kết chịu trách nhiệm với người dùng trước sự cố dữ liệu**

Cam kết bảo mật thông tin cá nhân người dùng

Ví dụ từ Ứng dụng thông minh tỉnh Hậu Giang

Trong trường hợp máy chủ lưu trữ thông tin người dùng bị hacker tấn công dẫn đến mất mát dữ liệu cá nhân, chúng tôi có trách nhiệm thông báo đến người dùng thông qua ứng dụng Hậu Giang

✓ **Nên công khai biện pháp xử lý sự cố lộ lọt thông tin**

Ví dụ từ Cổng Thông tin Điện tử tỉnh Đồng Tháp

✗ **Không nên phủ nhận trách nhiệm trước sự cố mất an toàn thông tin**

Bảo mật dữ liệu cá nhân của bạn

Ví dụ từ Ứng dụng thông minh Tiền Giang S

Việc bảo mật Dữ liệu Cá nhân của Bạn là quan trọng đối với Chúng tôi, nhưng hãy nhớ rằng không có phương thức truyền tải nào qua Internet hoặc phương pháp lưu trữ điện tử là an toàn 100%. Trong khi Chúng tôi cố gắng sử dụng các phương tiện được chấp nhận về mặt thương mại để bảo vệ Dữ liệu Cá nhân của Bạn. Chúng tôi không thể đảm bảo tính bảo mật tuyệt đối của Dữ liệu đó

LÀM RÕ THỜI GIAN LƯU TRỮ DỮ LIỆU

✓ **Nên làm rõ thời gian lưu trữ dữ liệu cá nhân của người dùng trên hệ thống**

Thời gian lưu trữ thông tin

Ví dụ từ Ứng dụng thông minh tỉnh Hậu Giang

Dữ liệu cá nhân của người dùng sẽ được lưu trữ đến khi đơn vị chủ quản có yêu cầu hủy bỏ. Còn lại trong mọi trường hợp thông tin người dùng sẽ được lưu trữ bảo mật trên máy chủ của cơ quan quản lý nhà nước

✗ **Không nên thiếu rõ ràng trong việc quy định thời gian lưu trữ dữ liệu**

Lưu giữ dữ liệu cá nhân của bạn

Ví dụ từ Ứng dụng thông minh Tiền Giang S

Công ty sẽ chỉ lưu giữ Dữ liệu Cá nhân của Bạn chừng nào cần thiết cho các mục đích được nêu trong Chính sách Bảo mật này. Chúng tôi sẽ lưu giữ và sử dụng Dữ liệu Cá nhân của Bạn trong phạm vi cần thiết để tuân thủ các nghĩa vụ pháp lý của chúng tôi (ví dụ: nếu chúng tôi được yêu cầu giữ lại dữ liệu của bạn để tuân thủ luật hiện hành), giải quyết tranh chấp và thực thi các thỏa thuận và chính sách pháp lý của chúng tôi.
Công ty cũng sẽ giữ lại Dữ liệu sử dụng cho các mục đích phân tích nội bộ. Dữ liệu sử dụng thường được lưu giữ trong một khoảng thời gian ngắn hơn, ngoại trừ khi dữ liệu này được sử dụng để tăng cường bảo mật hoặc để cải thiện chức năng của Dịch vụ của chúng tôi hoặc Chúng tôi có nghĩa vụ pháp lý phải lưu giữ dữ liệu này trong khoảng thời gian dài hơn

3.1. Hoàn thiện khung chính sách, pháp luật quốc gia

Nhìn tổng quan, việc hoàn thiện khung chính sách, pháp luật quốc gia về BVDLCN cần chú trọng tiếp cận từ góc độ quyền con người đã được hiến định, cụ thể là quyền đối với dữ liệu cá nhân, quyền riêng tư, nhất là đặt các quyền đó trong bối cảnh chuyển đổi số, xây dựng chính phủ số với những khía cạnh mới. Các văn bản cần hoàn thiện trong khung chính sách, pháp luật bao gồm: Hiến pháp; Chiến lược quốc gia về chuyển đổi số; các luật, nghị định có liên quan, nhất là cần nghiên cứu xây dựng Luật Bảo vệ dữ liệu cá nhân.[84]

Đối với một số nội dung cụ thể, báo cáo này đưa ra các khuyến nghị làm rõ một số khái niệm chủ chốt về dữ liệu cá nhân, quyền riêng tư đối với dữ liệu cá nhân; phân định trách nhiệm của cơ quan nhà nước và các đơn vị cung cấp dịch vụ đối với cá nhân – chủ thể dữ liệu; minh bạch hóa quá trình thu thập, sử dụng dữ liệu; và một số giải pháp kỹ thuật.

3.1.1. Hoàn thiện quy định về định nghĩa, phân loại dữ liệu cá nhân

Định nghĩa và phân loại rõ ràng về dữ liệu cá nhân

Luật về bảo vệ dữ liệu cá nhân hoặc văn bản luật có liên quan cần định nghĩa và phân loại dữ liệu cá nhân phù hợp với xu hướng chuyển đổi số hiện nay. Quá trình số hóa đang được đẩy mạnh với ngày càng nhiều dữ liệu được thu thập tự động từ hành vi của người dùng, kéo theo nhiều rủi ro đối với dữ liệu cá nhân. Dự thảo Nghị định về bảo vệ dữ liệu cá nhân đã phân loại dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm, bao gồm dữ liệu hành vi được thu thập tự động từ các hoạt động của người dùng trên giao diện trực tuyến. Tuy nhiên, những quy định này liên quan đến quyền của các cá nhân nên chúng cần được đưa vào luật. Định nghĩa dữ liệu cá nhân rõ ràng sẽ giúp thiết lập quyền kiểm soát dữ liệu cá nhân, quyết định quyền của chủ thể dữ liệu và trách nhiệm pháp lý của những bên liên quan trong việc thu thập, sử dụng, lưu trữ và chia sẻ dữ liệu.

Bên cạnh đó, báo cáo này khuyến nghị xây dựng một thông tư riêng về dữ liệu được thu thập và xử lý trong khu vực công, trong đó phân loại dữ liệu cá nhân thành dữ liệu cá nhân,[85] dữ liệu nhạy cảm[86] và thông tin riêng tư.[87] Một mặt, sự phân loại hiệu quả sẽ hỗ trợ quá trình hủy nhận dạng và thúc đẩy phát triển dữ liệu chính phủ mở bằng cách làm cho quyết định trường dữ liệu nào nên được đóng, chia sẻ hoặc mở cho công chúng trở nên dễ dàng hơn. Mặt khác, phân loại dữ liệu cá nhân hiệu quả sẽ đảm bảo rằng các cơ quan nhà nước có thể ứng dụng AI và tự động hóa để giám sát và ra quyết định mà không xâm phạm quyền riêng tư. Phân loại dữ liệu chuẩn hóa quốc gia (đạt tiêu chuẩn quốc tế) cũng sẽ phục vụ xu hướng phát triển các giao diện số quốc gia[88] và tập trung hóa dữ liệu, bởi đăng ký định danh số sẽ từng bước được tích hợp vào hệ thống cổng dịch vụ công quốc gia.

---

[84] *Tháng 3/2022, Chính phủ đã ban hành Nghị quyết số 27/NQ-CP thông qua hồ sơ xây dựng nghị định về bảo vệ dữ liệu cá nhân. Trong đó có giao Bộ Công an chủ trì, phối hợp với Bộ Tư pháp nghiên cứu, đề xuất xây dựng Luật Bảo vệ dữ liệu cá nhân.*

[85] *Dữ liệu cá nhân (Personal Data) được Điều 2 của Quy định chung về bảo mật thông tin của Liên minh Châu Âu EU (GDPR) định nghĩa là: "bất kì thông tin nào liên quan đến việc xác định hoặc có thể xác định một thể nhân ('chủ thể dữ liệu'). Một thể nhân là một cá nhân cụ thể có thể được nhận dạng trực tiếp hoặc gián tiếp thông qua một mã định dạng chẳng hạn như tên, số căn cước công dân, dữ liệu về địa điểm, mã định danh số hoặc thông qua một hoặc vài yếu tố đặc thù khác về về thể chất, sinh lý, di truyền, tinh thần, kinh tế, văn hóa hoặc xã hội của cá nhân đó."*

[86] *Dữ liệu nhạy cảm (Sensitive Data): là dữ liệu có thông tin mật, thông tin lưu hành nội bộ của đơn vị hoặc do đơn vị quản lý, nếu lộ lọt ra ngoài sẽ gây ảnh hưởng xấu đến danh tiếng, tài chính và hoạt động của đơn vị. Tham khảo Điều 2, Khoản 8 Thông tư 31/2015/TT-NHNN Quy định về đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin trong hoạt động ngân hàng do Thống đốc Ngân hàng Nhà nước ban hành*

[87] *Thông tin riêng tư (Private Information): là thông tin liên quan tới một pháp nhân hoặc thể nhân có thể nhận dạng được; không là trong phạm vi công cộng hoặc kiến thức chung; và nếu để lộ có thể gây cho họ thiệt hại, tổn thất hoặc đau khổ cho họ. Định nghĩa này là rất giống với những gì GDPR gọi là dữ liệu danh mục đặc biệt. Tham khảo:*
(i) Office for National Statistics (2009): National Statistician's Guidance on Confidentiality of Official Statistics: https://gss.civilservice.gov.uk/wp-content/uploads/2012/12/Confidentiality-of-Official-Statistics-National-Statisticians-Guidance.pdf
(ii) Information Commissioner's Office (2018), 'Guide to Data Protection': https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/#scd1

[88] *Như tại Quyết định 186/QĐ-BTTTT (ngày 11/ 02/2022) về Chương trình khuyến khích phát triển và ứng dụng giao diện số quốc gia phục vụ chuyển đổi số và phát triển Chính phủ số, kinh tế số, xã hội số.*

3.1.2. Phân biệt giữa quyền riêng tư của dữ liệu và an toàn bảo mật dữ liệu

Khung pháp lý quốc gia và kể cả việc thực hiện pháp luật cần phân định rõ sự khác biệt giữa bảo vệ quyền riêng tư của dữ liệu cá nhân (đặc trưng bởi trọng tâm bảo vệ quyền của người dùng) và bảo vệ an ninh dữ liệu (đặc trưng bởi trọng tâm bảo vệ an toàn, an ninh hệ thống CNTT và bảo mật của các cơ quan, tổ chức). Mặc dù an toàn dữ liệu là điều kiện tiên quyết của quyền riêng tư dữ liệu, nhưng hai khái niệm vẫn tách biệt. Như trình bày ở Bảng 2, trong khi bảo vệ an ninh dữ liệu chủ yếu liên quan đến các kỹ thuật tích hợp để đảm bảo an toàn cho hệ thống CNTT, bảo vệ quyền riêng tư chú ý bảo đảm quyền của các chủ thể dữ liệu đối với dữ liệu cá nhân của họ. Quyền riêng tư đối với dữ liệu đòi hỏi xử lý dữ liệu một cách cẩn trọng, cần có sự đồng ý của người dùng; thông báo khi có thay đổi, sự cố...; làm rõ dữ liệu được quản lý và chia sẻ với bên thứ ba như thế nào; cách dữ liệu được thu thập, lưu trữ và chuyển giao; sự tuân thủ các quy định và giới hạn pháp lý. Một trong những cách hiệu quả nhất để đảm bảo quyền của chủ thể dữ liệu là xây dựng và đăng tải chính sách về quyền riêng tư với đầy đủ quyền, trách nhiệm của các bên liên quan.

Bảng 2: Phân biệt giữa quyền riêng tư của dữ liệu và an toàn bảo mật dữ liệu

	An toàn, bảo mật dữ liệu	Tính riêng tư của dữ liệu
Đối tượng bảo vệ	**Hệ thống công nghệ thông tin**	**Công dân là người dùng**
Nội hàm	**Bảo vệ:** • Tính toàn vẹn dữ liệu • Tính bảo mật dữ liệu • Tính sẵn có của dữ liệu	• Các quyền của người dùng: quyền đồng ý, quyền yêu cầu cập nhật, sửa đổi, xóa, quyền tiếp cận, ...
Công cụ bảo vệ/ thực thi	• Hướng dẫn kỹ thuật • Quy định nội bộ • Hợp đồng dịch vụ với các điều khoản BVDLCN	• Chính sách về Quyền riêng tư và cơ chế cho phép lựa chọn sự đồng ý • Nghĩa vụ Thông báo • Nghĩa vụ pháp lý

3.1.3. Hoàn thiện các quy định về trách nhiệm của các bên

Phân định rõ chủ thể kiểm soát dữ liệu và chủ thể vận hành dữ liệu

Cần phân biệt rạch ròi giữa chủ thể kiểm soát dữ liệu và chủ thể vận hành dữ liệu. Khi quyền riêng tư đối với dữ liệu cá nhân nổi lên như một vấn đề toàn cầu và trở thành một thỏa thuận quan trọng của các hiệp định thương mại tự do đa phương và khi số hóa tăng tốc, sự phân định rõ ràng theo hướng kĩ thuật giữa bên kiểm soát dữ liệu và bên vận hành giúp xác định trách nhiệm pháp lý tương ứng của các chủ thể này đối với cá nhân (chủ thể dữ liệu).

Ngoài việc phân biệt rõ chủ thể kiểm soát dữ liệu và chủ thể vận hành dữ liệu ở cấp độ luật, điều quan trọng là phải có các công cụ để thiết lập trách nhiệm ràng buộc giữa cơ quan nhà nước kiểm soát dữ liệu và đơn vị vận hành đối với chủ thể dữ liệu, bao gồm: (1) chính sách về quyền riêng tư có tính chất như hợp đồng kỹ thuật số giữa chủ thể dữ liệu và bên kiểm soát dữ liệu (cơ quan nhà nước có trách nhiệm); (2) thỏa thuận giữa cơ quan nhà nước và đơn vị vận hành. Về vấn đề này, Bộ Thông tin và Truyền thông có thể chủ trì xây dựng: (1) chính sách về quyền riêng tư mẫu; (2) điều khoản sử dụng mẫu; và (3) thỏa thuận mẫu với đơn vị vận hành để đưa vào thông tư hướng dẫn.

Coi chính sách về quyền riêng tư như một dạng thỏa thuận điện tử có giá trị pháp lý

Trong bối cảnh khối lượng dữ liệu cá nhân được thu thập và xử lý thông qua hệ sinh thái của chính phủ số ngày càng tăng, cần xem xét nghiêm túc hơn về tác động pháp lý của các chính sách về quyền riêng tư, trong đó đặt ra trách nhiệm pháp lý của các cơ quan nhà nước (cơ quan chủ quản) đối với chủ thể dữ liệu. Khi người dùng đánh dấu vào ô đồng ý như một hình thức xác nhận điện tử thay cho chữ ký trên giấy thì họ có quyền được biết chi tiết về những nội dung họ đồng ý. Với việc Luật Giao dịch điện tử đang được sửa đổi cho phù hợp với các loại chữ ký điện tử, thanh toán kỹ thuật số, hóa đơn điện tử và các loại hình tương tự mới, dự thảo Nghị định về nhận dạng và xác thực điện tử đang được xây dựng, các chính sách về quyền riêng tư có thể trở thành một công cụ pháp lý để các chủ thể dữ liệu được bảo đảm quyền riêng tư của họ khi có tranh chấp xảy ra.

Quy trình và trách nhiệm giữa các cơ quan nhà nước trong chia sẻ dữ liệu cá nhân

Các văn bản quy phạm pháp luật có liên quan như Nghị định số 47/2020/NĐ-CP và Thông tư số 25/2010/TT-BTTTT cần bổ sung và làm rõ hơn trách nhiệm của các cơ quan nhà nước khi chia sẻ thông tin cá nhân của người dân trong nội bộ và ra bên ngoài. Một giải pháp tiềm năng cho vấn đề này là áp dụng ISO 27701 (xem Hộp 6),[89] một tiêu chuẩn quốc tế mới được công bố vào tháng 8 năm 2019, mở rộng từ ISO 27001 và 27002, bao gồm các tiêu chuẩn bảo vệ dữ liệu cá nhân sau khi GDPR có hiệu lực ở Liên minh Châu Âu EU. Tương tự như cách Thông tư số 22/2019/TT-BTTTT[90] khuyến khích các cơ quan chính phủ áp dụng IPv6, DNSSEC, https sử dụng TLS v1.2 với mã hóa an toàn nhận dạng và chia sẻ thông tin nhạy cảm của người dùng (dữ liệu cá nhân, dữ liệu giao dịch), việc thực thi ISO 27701 và các tiêu chuẩn BVDLCN tương ứng sẽ góp phần đáng kể vào việc cải thiện BVDLCN trong khu vực công Việt Nam.

Hộp 6: Yêu cầu ISO 27701 liên quan đến bảo vệ dữ liệu cá nhân

Để tăng cường bảo vệ dữ liệu cá nhân, ISO 27701 mở rộng các hệ thống quản lý bảo mật thông tin ISO, bao gồm các điểm đặc thù của việc xử lý dữ liệu cá nhân:

- Xác định vai trò của tổ chức với tư cách là bên kiểm soát dữ liệu và/hoặc bên vận hành, xử lý dữ liệu (trong 27701, "PII bên kiểm soát" và "PII bên vận hành, xử lý");
- Xây dựng cơ chế quản lý rủi ro đồng bộ đối với rủi ro cho tổ chức và đối với các chủ thể dữ liệu (trong 27701, "PII principals"), chỉ định một cán bộ bảo vệ dữ liệu (trong ISO 27701, "nhân viên bảo mật riêng tư");
- Nâng cao nhận thức của nhân viên, phân loại thông tin, bảo vệ phương tiện truyền thông có thể tháo rời, quản lý truy cập, mã hóa dữ liệu, sao lưu, ghi nhật ký sự kiện;
- Điều kiện truyền tải dữ liệu, quyền riêng tư theo thiết kế và theo mặc định, quản lý sự cố;
- Tuân thủ các yêu cầu pháp lý và hành chính, v.v.

ISO 27701 cung cấp các biện pháp cụ thể để xử lý dữ liệu cá nhân, liên quan đến vai trò của cơ quan, tổ chức (như chủ thể kiểm soát dữ liệu, chủ thể xử lý chính hoặc chủ thể xử lý thứ cấp):

- Nguyên tắc cơ bản: Nêu rõ mục đích xử lý, cơ sở pháp lý, có cơ chế cho phép người dùng cung cấp và cho phéo người dùng rút lại sự đồng ý, lưu giữ các hoạt động xử lý, đánh giá tác động quyền riêng tư;
- Quyền của chủ thể dữ liệu: được thông báo, truy cập, sửa chữa, xóa, đưa ra quyết định tự động;
- Quyền riêng tư theo thiết kế và theo mặc định: nguyên tắc tối thiểu, ẩn danh và xóa dữ liệu, lưu trữ dữ liệu;
- Hợp đồng phụ, truyền tải dữ liệu và chia sẻ dữ liệu.

[89] *ISO 27701, một tiêu chuẩn quốc tế giải quyết vấn đề bảo vệ dữ liệu cá nhân | CNIL*
[90] *Thông tư 22/2019/TT-BTTTT quy định tiêu chí chức năng, chức năng kỹ thuật của cổng dịch vụ công và hệ thống một cửa trực tuyến cấp bộ, cấp tỉnh.*

3.1.4. Minh bạch hóa vi phạm về DLCN và đánh giá tác động quyền riêng tư

Việc xử lý dữ liệu cá nhân phải được thực hiện với sự minh bạch đối với các chủ thể dữ liệu. Mọi người đều có quyền biết dữ liệu cá nhân của mình được thu thập, sử dụng, lưu trữ và chia sẻ như thế nào. Tất cả mọi người cũng có quyền chỉnh sửa và sửa đổi thông tin của mình, phản đối việc sử dụng dữ liệu không đúng cách theo quy định của pháp luật, có quy trình khiếu nại hành chính và khiếu kiện tư pháp giúp đảm bảo quyền minh bạch.

Đặc biệt, cần thúc đẩy việc minh bạch hóa các vi phạm về dữ liệu cá nhân trong các cơ quan nhà nước ở tất cả các cấp. Chủ thể dữ liệu có quyền nhận thông báo trong trường hợp sự cố lộ lọt dữ liệu xảy ra. Bên cạnh đó, các cơ quan nhà nước cần thường xuyên tiến hành đánh giá tác động quyền riêng tư và công khai thông tin kết quả đánh giá trên các giao diện trực tuyến. Tính minh bạch về vi phạm dữ liệu và công bố đánh giá tác động quyền riêng tư cần được chính thức coi như một nội dung trong chứng nhận bảo mật do Trung tâm Giám sát an toàn không gian mạng quốc gia, Bộ TTTT, cấp.

3.1.5. Hoàn thiện các quy định về xử lý vi phạm

Quy định về chế tài đối với vi phạm liên quan đến dữ liệu cá nhân

Hiện nay các văn bản quy phạm pháp luật điều chỉnh lĩnh vực quản lý hành chính, hoạt động tố tụng cần chú trọng bổ sung các quy định liên quan đến xử lý dữ liệu cá nhân, ví dụ như Luật Xử lý vi phạm hành chính, Bộ Luật Tố tụng hình sự, Bộ Luật Tố tụng dân sự, Luật Khiếu nại, v.v. Cần bổ sung quy định về bồi thường thiệt hại do dữ liệu cá nhân bị xâm phạm trong Luật Trách nhiệm bồi thường nhà nước năm 2017 đối với hành vi thu thập, xử lý dữ liệu cá nhân trái quy định pháp luật gây thiệt hại cho chủ thể dữ liệu và các chủ thể có liên quan.

Được biết Dự thảo Nghị định bảo vệ dữ liệu cá nhân quy định chế tài xử lý vi phạm hành chính được áp dụng cho hành vi xâm phạm dữ liệu cá nhân. Quy định này cần phải đủ sức "răn đe", mức phạt cần tương xứng với hậu quả mà những hành vi xâm phạm này gây ra.[91] Các quy định về vi phạm trong xử lý dữ liệu cá nhân và mức phạt đi kèm cần rõ ràng, cụ thể, ví dụ như thiếu cơ sở pháp lý khi xử lý dữ liệu; sử dụng dữ liệu không đúng mục đích hợp pháp; lạm dụng dữ liệu cá nhân v.v. Xem ví dụ tham khảo của Cộng Hòa Liên Bang Đức ở Hộp 7.

Hộp 7: Ví dụ về xử phạt hành chính đối với vi phạm về dữ liệu cá nhân ở Cộng hòa Liên Bang Đức

- Kênh theo dõi thực thi GDPR (GDPR Enforcement Tracker) ghi nhận 20 trường hợp xử phạt cảnh sát vì vi phạm Điều 5 và 6 của GDPR về Thiếu cơ sở pháp lý để xử lý dữ liệu.
- Mức phạt cao nhất: 1,800 euros - Lý do: Một cảnh sát liên tục tiếp cận dữ liệu cá nhân từ kho dữ liệu cảnh sát cho mục đích nghiên cứu cá nhân.
- Mức phạt 1,400 euros – Cảnh sát sử dụng hệ thống giao thông trung tâm để tra cứu thông tin đăng ký của nạn nhân tai nạn giao thông, và liên hệ với nạn nhân qua số điện thoại riêng và điện thoại nhà.
- Mức phạt: 800 euros – Cảnh sát sử dụng dữ liệu của nhân chứng để liên hệ vì mục đích cá nhân.
- Mức phạt: 400 euros – Cảnh sát lạm dùng dữ liệu cá nhân từ cơ sở dữ liệu cảnh sát để ép buộc người bán sách thanh toán online theo phương thức mong muốn.

Nguồn: *https://www.enforcementtracker.com/ETid-1205*

[91] *Tham khảo Điều 83, GDPR năm 2016.*

Thiết lập hệ thống tập trung để tiếp nhận, xử lý yêu cầu, khiếu nại về dữ liệu cá nhân

Cần thành lập hệ thống tập trung để tiếp nhận, xử lý yêu cầu, khiếu nại về dữ liệu cá nhân, có thể đặt ở Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin, Bộ TTTT. Từ kinh nghiệm của các cổng DVCTT cấp tỉnh đang tích hợp đăng ký tài khoản với hệ thống của Cổng dịch vụ công quốc gia, tất cả các giao diện trực tuyến của các cơ quan nhà nước có thể phát triển một định dạng tiêu chuẩn để tiếp nhận và xử lý các yêu cầu, khiếu nại liên quan đến bảo vệ quyền riêng tư đối với dữ liệu cá nhân và tập trung vào hệ thống này.[92]

Cơ quan chịu trách nhiệm quản lý hệ thống khiếu nại về BVDLCN có vai trò thúc đẩy tăng cường an toàn và tiêu chuẩn BVDLCN, giám sát thực tiễn BVDLCN, ban hành quyết định khi cần thiết và tư vấn/ tham khảo ý kiến các CQNN để thực hiện BVDLCN tốt hơn. Hệ thống tập trung như vậy sẽ nhằm 3 mục đích: (1) giảm gánh nặng tăng nguồn nhân lực[93] và hạn chế tác động từ thực trạng thiếu năng lực của cán bộ dữ liệu ở cấp địa phương; (2) đảm bảo rằng các hoạt động BVDLCN tại các cơ quan công quyền địa phương được theo dõi và tư vấn thường xuyên; và (3) nghiên cứu và nắm bắt xu hướng vi phạm BVDLCN trên toàn quốc và phối hợp với các bộ khác, nhất là Bộ Công an trong việc bảo vệ quyền riêng tư dữ liệu cá nhân.

Cùng với việc thiết lập hệ thống khiếu nại BVDLCN tập trung, việc giải quyết các khiếu nại và yêu cầu BVDLCN cần được coi là dịch vụ công chính thức, cần tuân theo các quy tắc phản hồi tiêu chuẩn và thời hạn trả lời. Trên thực tế, yêu cầu này đã được đề cập tại Điều 20[94] Luật An toàn thông tin mạng, nhưng chưa được triển khai đầy đủ.

3.1.6. Bố trí nhân sự về bảo vệ dữ liệu cá nhân

Có thể nghiên cứu bố trí nhân sự làm đầu mối về bảo vệ dữ liệu ở cấp tỉnh, tương tự như người phát ngôn và cung cấp thông tin cho báo chí được quy định bởi Nghị định số 09/2017/NĐ-CP. Tuy nhiên, trong bối cảnh tinh giảm biên chế hiện nay, chỉ nên bố trí công chức kiêm nhiệm về vấn đề này.

Trách nhiệm của công chức làm đầu mối về bảo vệ dữ liệu bao gồm: i) thông báo và tư vấn cho cơ quan nhà nước kiểm soát dữ liệu và đơn vị vận hành cũng như các cán bộ, công chức liên quan về nghĩa vụ của họ theo quy định của pháp luật hiện hành; ii) giám sát việc tuân thủ pháp luật về bảo vệ dữ liệu của Việt Nam và các chính sách nội bộ của cơ quan/tổ chức; iii) tư vấn về đánh giá tác động bảo vệ dữ liệu; iv) hợp tác với các cơ quan giám sát và đóng vai trò là đầu mối liên lạc cho họ về các vấn đề liên quan đến thu thập, xử lý dữ liệu; v) đóng vai trò là người đại diện cho quyền lợi của các chủ thể dữ liệu.

Về bản chất, công chức này là người bảo đảm các tiêu chuẩn bảo vệ dữ liệu và quyền riêng tư, đầu mối tương tác chính với các nhà quản lý và cơ quan giám sát và là người bảo vệ lợi ích của các chủ thể dữ liệu. Như vậy, thông tin liên lạc được cung cấp trong chính sách về quyền riêng tư phải là của công chức đầu mối về bảo vệ dữ liệu.

3.1.7. Một số giải pháp kỹ thuật

Hiện đại hóa điện toán đám mây

Hiện đại hóa điện toán đám mây có thể là một hàm ý chính sách quan trọng khác đối với BVDLCN trên môi trường số. Báo cáo của IBM[95] cho thấy tổn thất vi phạm dữ liệu cao hơn đáng kể đối với các tổ chức đang ở giai đoạn đầu của hiện đại hóa hạ tầng đám mây. Theo quan sát, mô hình đám mây hybrid có tổng phí tổn vi phạm dữ liệu trung bình thấp nhất, so với các mô hình đám mây công cộng, riêng tư và tại chỗ. Các tổ chức đã hoàn thiện triển khai điện toán đám mây đã có thể xác định và ngăn chặn các vi phạm nhanh hơn 77 ngày so với những đơn vị đang trong giai đoạn đầu của hiện đại hóa đám mây.[96]

---

[92] *Xem chi tiết tại: https://wso2.com/contact/*
[93] *Trong trường hợp việc bố trí một công chức bảo vệ dữ liệu cho mỗi cơ quan Nhà nước đòi hỏi nguồn nhân lực lớn không cần thiết, việc phát triển một hệ thống tập trung với một nhóm chuyên trách để giải quyết các yêu cầu và khiếu nại BVDLCN ở cấp trung ương có thể là một giải pháp tốt.*
[94] *Điều 20, Luật an toàn thông tin mạng 2015: Trách nhiệm của cơ quan quản lý nhà nước trong bảo vệ thông tin cá nhân trên mạng.*
1. Thiết lập kênh thông tin trực tuyến để tiếp nhận kiến nghị, phản ánh của tổ chức, cá nhân liên quan đến bảo đảm an toàn thông tin cá nhân trên mạng.
2. Định kỳ hằng năm tổ chức thanh tra, kiểm tra đối với tổ chức, cá nhân xử lý thông tin cá nhân; tổ chức thanh tra, kiểm tra đột xuất trong trường hợp cần thiết.
[95] *Xem chi tiết tại Báo cáo "Cost of a Data Breach Report 2021 | IBM"*
[96] *Xem chi tiết tại Báo cáo "Cost of a Data Breach Report 2021 | IBM"*

Phân loại dữ liệu cá nhân trên hệ thống đám mây giúp các cơ quan nhà nước dự báo, xác định và ngăn chặn rủi ro về quyền riêng tư hiệu quả hơn. Do đó, cần thúc đẩy xây dựng các chiến lược di chuyển đám mây hiệu quả, chú trọng đến phân loại dữ liệu, để quyết định xem trường dữ liệu nào sẽ được lưu trữ trên các đám mây công cộng hay riêng tư.

Quy định về hồ dữ liệu

Hồ dữ liệu (Data Lakes) là các "kho" dữ liệu thô dùng để chứa đựng thông tin không theo định dạng của các tổ chức/cá nhân. Mục đích của Data Lake là cho phép người dân tạo một không gian chứa dữ liệu riêng tư, cá nhân trên môi trường mạng. Khi cần, người dân có thể vào để sử dụng chính các dữ liệu này khai báo, cung cấp cho cơ quan nhà nước mà không cần phải upload hoặc nộp lại (ví dụ: hộ chiếu, căn cước công dân, giấy khai sinh, v.v.). Hiện nay, nhiều tỉnh đang xây dựng hồ dữ liệu phục vụ quản lý loại thông tin này, tuy nhiên quy mô có thể khác nhau (có tỉnh xây dựng Data Lake cho riêng hệ thống cổng dịch vụ công, tỉnh khác xây dựng cho tất cả các hệ thống).

Vấn đề đặt ra là phải có cơ chế quản lý, ràng buộc trách nhiệm của cơ quan quản lý đối với dữ liệu cá nhân của công dân. Có thể nghiên cứu quy định về trách nhiệm của cơ quan, cán bộ trực tiếp thụ lý/trả kết quả hồ sơ, xử lý hồ sơ trong việc bảo đảm bảo mật thông tin cá nhân của công dân, tổ chức. Hình thức có thể là cam kết trách nhiệm trước khi đảm nhận vị trí công tác. Về mặt kỹ thuật, khi mở/khai thác dữ liệu của công dân, có thể đưa ra yêu cầu chấp nhận đồng ý với bản cam kết đảm bảo thông tin đồng thời ghi lại nhật ký (log) khai thác dữ liệu công dân (có thể truy xuất khi cần thiết). Như vậy, có thể vừa nâng cao ý thức, vừa nhắc nhở thường xuyên cán bộ quản lý hồ sơ. Đồng thời cũng lưu lại được các thao tác, hành vi truy cập khai thác thông tin, để có hình thức xử lý vi phạm theo quy định.

3.2. Khuyến nghị về thực thi bảo vệ dữ liệu cá nhân của các địa phương

Dựa trên quy định của pháp luật, hướng dẫn của Chính phủ, chính quyền địa phương có thể xây dựng các biện pháp, công cụ cụ thể để đảm bảo tính chính danh, hợp pháp trong xử lý thông tin cá nhân; thu thập, sử dụng thông tin cá nhân với mục đích rõ ràng; thu thập thông tin cá nhân một cách tương xứng với mục đích, căn cứ trên sự cần thiết; rõ ràng về thời hạn lưu trữ thông tin; tăng tính minh bạch, tính giải trình trong thu thập, xử lý, lưu trữ, sử dụng thông tin cá nhân.

Để xử lý dữ liệu cá nhân một cách công bằng và hợp pháp

Để đảm bảo dữ liệu cá nhân được xử lý một cách công bằng và hợp pháp, tất cả các giao diện trực tuyến của chính quyền địa phương phải xây dựng chính sách về quyền riêng tư, tham khảo các văn bản pháp luật có liên quan như Luật CNTT, Luật An toàn thông tin mạng, Nghị định số 64/2007/NĐ-CP, Thông tư số 25/2010/TT-BTTTT (như trường hợp cổng TTĐT của Thừa Thiên - Huế) và công khai chính sách bằng ít nhất hai ngôn ngữ (tiếng Việt và tiếng Anh).

Nguyên tắc này cũng có thể được đảm bảo về mặt kỹ thuật thông qua việc cung cấp định dạng đồng ý đính kèm chính sách về quyền riêng tư, bao gồm 2 khía cạnh:

i) Hộp kiểm đồng ý cho phép chủ thể dữ liệu thực hiện quyền lựa chọn đồng ý hay không.

ii) Các chính sách về quyền riêng tư kèm theo thể hiện quyền của chủ thể dữ liệu để biết họ đang đồng ý vì điều gì.

Hơn nữa, sự đồng ý đầy đủ cần được cung cấp ở định dạng thông báo nổi bật và tại tất cả các kênh thu thập dữ liệu cá nhân, bất kể dữ liệu cá nhân được thu thập phục vụ mục đích gì. Hiện nay, hầu hết các giao diện trực tuyến chỉ chú ý đến việc thu thập dữ liệu cá nhân trong đăng ký tài khoản lần đầu tiên. Như đã khảo sát, nếu các chính sách về quyền riêng tư được cung cấp, chúng thường xuất hiện ở giai đoạn này. Tuy nhiên, có thể có nhiều hơn một kênh thu thập dữ liệu cá nhân quan trọng trên các giao diện trực tuyến và điều quan trọng là chính quyền địa phương phải xác định và giám sát tất cả tất cả các kênh này.

Để làm rõ mục đích thu thập, sử dụng dữ liệu cá nhân

Để bảo đảm nguyên tắc này, chính quyền địa phương phải đảm bảo một phần mô tả riêng biệt về mục đích trong các chính sách về quyền riêng tư. Chính sách về quyền riêng tư của ứng dụng Thành phố thông minh Bình Định, mặc dù chưa đầy đủ, là một ví dụ có thể tham khảo. Trong trường hợp này, chính sách về quyền riêng tư phân chia các mục đích thành các nhóm khác nhau phù hợp với các bên khác nhau liên quan đến việc thu thập và xử lý dữ liệu cá nhân.

Bên cạnh đó, chính quyền địa phương phải xem xét cẩn thận các chính sách về quyền riêng tư để đảm bảo rằng tất cả các mục đích đều hợp pháp theo luật hiện hành. Bất kỳ mục đích bất hợp pháp nào của việc thu thập và xử lý dữ liệu cá nhân như trong trường hợp của ƯDTM Smart Quảng Ninh có thể ảnh hưởng tiêu cực tới niềm tin của người dân vào chính phủ số.

Để bảo đảm tính tương xứng và cần thiết

Đây là một nguyên tắc mà hầu hết các giao diện trực tuyến của chính quyền địa phương đã có thực hành tốt, đặc biệt là về việc trao quyền cho người dùng chọn mức độ ẩn danh của họ. Tuy nhiên, đánh giá cho thấy cần tránh vi phạm nguyên tắc tương xứng và cần thiết trên hai phương diện: (i) không yêu cầu người dùng gửi nhiều thông tin hơn mức cần thiết cho một mục đích cụ thể; và (ii) không công khai nhiều thông tin cá nhân hơn mức cần thiết cho mục đích minh bạch. Để bảo đảm nguyên tắc này, chính quyền địa phương được khuyến nghị tiến hành đánh giá tác động quyền riêng tư thường xuyên và kỹ lưỡng trên giao diện trực tuyến theo Điều 15, Thông tư số 25/2010/TT-BTTTT. Điều này sẽ giúp cơ quan có trách nhiệm nhận thức được rằng, ví dụ, việc thu thập số CMND cùng với ngày và địa điểm cấp là không cần thiết đối với việc gửi ý kiến như trong trường hợp của Cà Mau.

Để lưu trữ dữ liệu cá nhân hợp pháp

Để thực hiện nguyên tắc này, chính quyền địa phương có thể phân biệt giữa hai loại mục đích riêng biệt để xử lý dữ liệu cá nhân:

i) Đối với dữ liệu định danh công dân, chính quyền địa phương cần thông báo cho người dùng rằng dữ liệu cá nhân của họ sẽ được lưu trữ an toàn trên hệ thống trừ khi có yêu cầu gỡ bỏ của cơ quan nhà nước có trách nhiệm như tỉnh Hậu Giang đã làm.

ii) Đối với mục đích khảo sát ngẫu nhiên, chẳng hạn như khi tỉnh Thừa Thiên - Huế thu thập các sáng kiến của công dân để phát triển Huế, chính quyền địa phương cần: 1) minh bạch về thời gian lưu trữ, 2) cung cấp cơ chế cho công dân thực hiện quyền được lãng quên[97] và 3) bảo đảm dữ liệu cá nhân sẽ bị xóa sau khi mục đích của cuộc khảo sát hoàn thành.

Trong trường hợp khó khăn như COVID-19, điều quan trọng là phải tổ chức thảo luận cởi mở và truyền thông rõ ràng với công chúng về thời gian lưu trữ.

Để đảm bảo minh bạch

Để thực hành nguyên tắc minh bạch, chính quyền địa phương được khuyến khích phát triển và công khai các chính sách về quyền riêng tư chính thức và thể hiện cam kết thông báo rủi ro về quyền riêng tư và vi phạm dữ liệu cá nhân cho người dùng. Một cách làm tốt có thể được học hỏi từ chính sách về quyền riêng tư trên ƯDTM của tỉnh Hậu Giang với cam kết: *"Trong trường hợp tin tặc tấn công dẫn đến vi phạm dữ liệu cá nhân, chúng tôi có trách nhiệm thông báo cho người dùng thông qua ứng dụng Hậu Giang."*

[97] *Xem giải thích tại chú thích số 82*

Để bảo đảm trách nhiệm giải trình

Để bảo đảm nguyên tắc trách nhiệm giải trình, chính quyền địa phương phải tránh xác định mơ hồ nghĩa vụ của các cơ quan có liên quan. Việc xác định rõ ràng trách nhiệm này cần được thể hiện trong (1) chính sách về quyền riêng tư đối với người dùng; và (2) các quy tắc và quy định nội bộ hoặc áp dụng ISO 27701 trong nội bộ cơ quan. Những biện pháp này sẽ trở nên đặc biệt hữu ích khi các sự cố về BVDLCN diễn ra.

Để đảm bảo sự thống nhất trong thực hiện

Trên phạm vi toàn quốc, để đạt được sự đồng nhất giữa các tỉnh/thành trong thực tiễn bảo vệ quyền riêng tư trên môi trường số, cần liên tục đánh giá, nghiên cứu các thông lệ, cách làm tốt, từ đó khái quát thành các quy định, hướng dẫn cụ thể để các địa phương nắm bắt được các chuẩn mực, dễ dàng bám sát, tuân theo; tạo cơ sở pháp lý để các tỉnh bảo vệ quyền riêng tư tốt hơn trên môi trường số. Bộ TTTT có thể chủ trì xây dựng các văn bản mẫu cho các cơ quan chính quyền địa phương sử dụng trong quá trình cung cấp các DVCTT, bảo đảm quyền riêng tư, bảo vệ dữ liệu cá nhân. Đó là Quy chế mẫu về quyền riêng tư; Thỏa thuận sử dụng mẫu; Hợp đồng mẫu trong cung cấp các giao diện tương tác giữa chính quyền với người dân.

3.3. Mở rộng đánh giá về bảo vệ dữ liệu cá nhân

Cần mở rộng hơn cách tiếp cận trong đánh giá việc bảo vệ DLCN và quyền riêng tư trên môi trường số của chính quyền nói chung, cũng như chính quyền địa phương nói riêng. Trước hết, có thể bổ sung các tiêu chí đánh giá BVDLCN vào Bộ chỉ số đánh giá chuyển đổi số quốc gia (DTI) tại địa chỉ https://dti.gov.vn/. Ví dụ, DTI có khảo sát:

- Chính sách về quyền riêng tư của giao diện trực tuyến có được công khai?
- Các cơ quan nhà nước đã áp dụng ISO 27701 hay chưa?
- Cơ quan Nhà nước đã tổ chức tập huấn về bảo vệ dữ liệu cá nhân chưa?
- Đánh giá tác động quyền riêng tư có thường xuyên được thực hiện?
- UBND cấp tỉnh đã bố trí nhân sự đầu mối về bảo vệ dữ liệu cá nhân?

Đồng thời, có thể đầu tư nguồn lực lớn hơn để tiến hành khảo sát, tìm hiểu, đánh giá sâu hơn về thực tiễn bảo vệ dữ liệu cá nhân, quyền riêng tư không chỉ trên các cổng TTĐT, cổng DVCTT, các ƯDTM, mà còn trong các cơ sở dữ liệu do các cơ quan Nhà nước quản lý, nơi dữ liệu cá nhân được lưu trữ, sử dụng, chia sẻ sau khi được thu thập từ các giao diện tương tác của chính quyền. Cần mở rộng đối tượng nghiên cứu sang 18 Bộ/ngành cung cấp dịch vụ công, cũng như 7 bộ/cơ quan ngang bộ thuộc Chính phủ (không cung cấp dịch vụ công).

Cuối cùng, nghiên cứu này khuyến nghị sự tham gia của các hiệp hội doanh nghiệp và hiệp hội người tiêu dùng trong đánh giá thực thi bảo vệ quyền riêng tư dữ liệu của các cơ quan nhà nước trên môi trường số. Điều này vừa giảm bớt gánh nặng giám sát từ các cơ quan quản lý và vừa cung cấp một nguồn thông tin độc lập, khách quan.

Tài liệu tham khảo

Các văn bản quy phạm pháp luật

- Hiến pháp Việt Nam năm 2013
- Luật Công nghệ thông tin 2006 số 67/2006/QH11
- Luật An ninh mạng 2018 số 24/2018/QH14
- Nghị định số 64/2007/NĐ-CP ngày 10/04/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước
- Nghị định số 43/2011/NĐ-CP ngày 13/06/2011 của Chính phủ quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử của cơ quan nhà nước
- Nghị định số 45/2020/NĐ-CP ngày 08/04/2020 của Chính phủ về thực hiện thủ tục hành chính trên môi trường điện tử
- Nghị định số 47/2020/NĐ-CP ngày 09/04/2020 của Chính phủ về Quản lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước
- Nghị định số 42/2022/NĐ-CP ngày 24/06/2022 của Chính phủ về việc cung cấp thông tin và dịch vụ công trực tuyến của cơ quan nhà nước trên môi trường mạng
- Dự thảo 2 Nghị định quy định về bảo vệ dữ liệu cá nhân năm 2021 của Bộ Công an
- Thông tư số 25/2010/TT-BTTTT ngày 15/11/2010 của Bộ TT&TT quy định việc thu thập, sử dụng, chia sẻ thông tin cá nhân và các biện pháp đảm bảo an toàn và bảo vệ thông tin cá nhân trên trang thông tin điện tử hoặc cổng thông tin điện tử của cơ quan nhà nước
- Quyết định số 749/QĐ-Ttg ngày 03/06/2020 của Thủ tướng Chính phủ phê duyệt "Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030"
- Quyết định số 942/QĐ-TTg ngày 15/06/2021 của Thủ tướng Chính phủ về "Chiến lược phát triển Chính phủ điện tử hướng tới Chính phủ số giai đoạn 2021 - 2025, định hướng đến năm 2030"
- Quyết định số 06/QĐ-TTg ngày 06/01/2022 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 2030
- Quyết định số 34/2021/QĐ-TTg ngày 08/11/2021 của Thủ tướng Chính phủ Quy định về định danh và xác thực điện tử trên giao diện Cơ sở dữ liệu quốc gia về dân cư, Cơ sở dữ liệu căn cước công dân và Cơ sở dữ liệu quốc gia về xuất nhập cảnh
- Quyết định số 31/2021/QĐ-TTg ngày 11/10/2021 của Thủ tướng Chính phủ ban hành quy chế quản lý, vận hành, khai thác cổng dịch vụ công quốc gia
- Quyết định số 714/QĐ-TTg ngày 22/05/2015 của Thủ tướng chính phủ ban hành Danh mục cơ sở dữ liệu quốc gia cần ưu tiên triển khai tạo giao diện phát triển chính phủ điện tử
- Chỉ thị số 02/CT-TTg ngày 26/04/2022 của Thủ tướng chính phủ về phát triển Chính phủ điện tử hướng tới Chính phủ số, thúc đẩy chuyển đổi số quốc gia
- Công văn số 677/BTTTT-THH ngày 03/03/2022 của Bộ TT&TT hướng dẫn kết nối dữ liệu thông qua giao diện tích hợp

Báo cáo nghiên cứu

- IBM. (2022). Báo cáo về phí tổn do lộ lọt dữ liệu năm 2021. https://www.ibm.com/security/data-breach
- IPS. (2020). Báo cáo thảo luận chính sách về bảo vệ dữ liệu cá nhân và quyền riêng tư trong bối cảnh nền kinh tế số. https://ips.org.vn/thu-vien/thao-luan-chinh-sach-hoan-thien-chinh-sach-va-khung-kho-phap-luat-ve-bao-ve-du-lieu-thong-tin-ca-nhan-va-quyen-rieng-tu-trong-nen-kinh-te-so-thao-lu an-va-khuyen-nghi-ct213.html
- Liên Hợp Quốc. (2019). Hướng dẫn xây dựng khung pháp lý về hệ thống đăng ký, thống kê hộ tịch và quản lý định danh, 152 – 159. https://unstats.un.org/unsd/demographic-social/Standards-and- Methods/files/Handbooks/crvs/CRVS_GOLF_Final_Draft-E.pdf
- Ủy ban cấp cao về quản lý của LHQ. (n.d). Các nguyên tắc về bảo vệ dữ liệu cá nhân và quyền riêng tư (thông qua tại phiên họp thứ 36 ngày 11/10/2018). https://archives.un.org/sites/archives.un.org/iles/_un-principles-on-personal-data-protection-privacy-hlcm-2018.pdf
- Uỷ ban thương mại liên bang Hoa Kỳ (FTC). (n.d.). Đánh giá tác động đến quyền riêng tư. https://www.ftc.gov/policy-notices/privacy-policy/privacy-impact-assessments

Phụ lục

Các ví dụ về lộ lọt thông tin cá nhân người dùng trên các giao diện tương tác trực tuyến

Mục hỏi đáp	Mục tiếp nhận phản ánh kiến nghị	Mục lấy góp ý của nhân dân đối với các văn bản quy phạm pháp luật
Ví dụ 1: Cổng TTĐT tỉnh Kon Tum, công khai họ tên, số điện thoại, địa chỉ email, và địa chỉ nhà riêng  Ví dụ 2: Cổng TTĐT Lai Châu, để lộ số CMTND, tên, và năm sinh 	Ví dụ: Cổng TTĐT tỉnh Thừa Thiên - Huế, công khai số điện thoại và địa chỉ email 	Ví dụ: Cổng TTĐT tỉnh Thừa Thiên – Huế, có công khai tên, địa chỉ email, số điện thoại, và địa chỉ nhà riêng 

Danh sách các Ứng dụng thông minh được đánh giá

Bên dưới là danh sách các ứng dụng thông minh được tìm thấy, có hyperlink. Danh sách hiện có dựa trên kết quả tìm kiếm của nhóm nghiên cứu từ tháng 3/2022 đến tháng 5/2022 (số liệu thực tế có thể nhiều hơn). Đây đều là các ứng dụng có chức năng phản ánh hiện trường, hỗ trợ tương tác giữa chính quyền và người dân. Về việc lựa chọn ứng dụng nào để đánh giá, chúng tôi ưu tiên các ứng dụng có nhiều lượt tải về hơn, vì lượt tải về đồng nghĩa với số lượt đăng ký của người dùng, cũng như số lượng thông tin cá nhân được thu thập và lưu trữ.

Đối với các tỉnh, thành phố có nhiều hơn một ứng dụng, chúng tôi khuyến nghị chính quyền địa phương rà soát lại cẩn thận các ứng dụng này, ứng dụng nào không còn sử dụng nữa thì nên xóa bỏ khỏi Google Play và Apple Store nhằm tránh sự bối rối cho người dân khi tìm kiếm ứng dụng phù hợp, cũng như bảo đảm người dân không cung cấp thông tin cá nhân cho các ứng dụng "ma".

STT	Tỉnh, thành phố trực thuộc trung ương	Ứng dụng thông minh được đánh giá	Các Ứng dụng khác được tìm thấy nhưng không được đánh giá
1	An Giang	*AG.ANTT (Công dân – Phản ánh ANTT An Giang) (1000+)*	*Không*
2	Bà Rịa – Vũng Tàu	*VUNG TAUIOC-Civ (10,000+)*	*Vũng tàu trực tuyến (1000+)*
3	Bắc Giang	*BacGiang TCT (100+)*	*Không*
4	Bắc Kan	*Bắc Kan trực tuyến (100+)*	*1022 Bắc Kan (1+) BacKan-S (100+)*
5	Bạc Liêu	*Bạc Liêu SmartCity (50+)*	*Không*

STT	Tỉnh, thành phố trực thuộc trung ương	Ứng dụng thông minh được đánh giá	Các Ứng dụng khác được tìm thấy nhưng không được đánh giá
6	Bắc Ninh	*Phản ánh kiến nghị (1000+)*	*Không*
7	Bến Tre	*TP Bến Tre Trực Tuyến (1000+)*	*1TP Bến Tre Smart (100+) Bến Tre SmartCity (100+)*
8	Bình Định	*Bình Định SmartCity (1000+)*	*Bình Định Egov (100+)*
9	Bình Dương	*1022 Bình Dương (10,000+)*	*Không*
10	Bình Phước	*IOC Bình Phước (500+)*	*Không*
11	Bình Thuận	*Không*	*Không*
12	Cà Mau	*Cà Mau G (1000+)*	*Không*
13	Cần Thơ	*Cần Thơ SC (500+)*	*Không*
14	Cao Bằng	*Cao Bằng Smart (100+)*	*Không*
15	Đà Nẵng	*Danang Smart City (100,000+)*	*Không*
16	Đăk Lăk	*Đăk Lak Trực tuyến (5,000+)*	*Đăk Lak SmartCity (100+)*
17	Đăk Nông	*Không*	*Không*
18	Điện Biên	*Điện Biên Smart (100+)*	*Không*
19	Đồng Nai	*Smart Đồng Nai (100+)*	*Không*
20	Đồng Tháp	*e-Đồng Tháp (1,000+)*	*Không*
21	Gia Lai	*Không*	*Không*
22	Hà Giang	*Smart Hà Giang (100+)*	*MyCity Hà Giang (50+)*
23	Hà Nam	*Không*	*Không*
24	Hà Nội	*Hà Nội SmartCity (app này đã bị xóa trên Google Play) – (100,000+)*	*Hà Nội Smart (500+)*
25	Hà Tĩnh	*Không*	*Không*
26	Hải Dương	*Smart Hải Dương (50,000+)*	*Phản ánh ANTT CA Hải Dương (10+)*
27	Hải Phòng	*Hải Phòng Smart (100+)*	*Không*
28	Hậu Giang	*Hải Phòng Smart (100+)*	*Không*

STT	Tỉnh, thành phố trực thuộc trung ương	Ứng dụng thông minh được đánh giá	Các Ứng dụng khác được tìm thấy nhưng không được đánh giá
29	Hòa Bình	*Công dân Hòa Bình (50+)*	*Không*
30	Hưng Yên	*1022 Hưng Yên (50+)*	*Không*
31	Khánh Hòa	*Không*	*Không*
32	Kiên Giang	*Kiên Giang TTHC (500+)*	*Không*
33	Kon Tum	*KonTumS (1,000+)*	*PATT KonTumCity (500+)*
34	Lai Châu	*Lai Châu Smart (100+)*	*Không*
35	Lâm Đồng	*Lâm Đồng Trực tuyến (1,000+)*	*Không*
36	Lạng Sơn	*Lạng Sơn trực tuyến (100+)*	*Không*
37	Lào Cai	*Lào Cai Smart (500+)*	*LaoCai S (100+)*
38	Long An	*LA.ANTT (Công dân – Phản ánh ANTT Long An) (1,000+)*	*Không*
39	Nam Định	*Smart Nam Định (1,000+)*	*Xã thông minh tỉnh Nam Định (100+)*
40	Nghệ An	*Không*	*Không*
41	Ninh Bình	*Ninh Bình Smart (100+)*	*My Ninh Bình (50+)*
42	Ninh Thuận	*NinhThuan-S (100+)*	*NinhThuan-C (100+)*
43	Phú Thọ	*Không*	*Không*
44	Phú Yên	*Phú Yên Smart (10+)*	*Không*
45	Quảng Bình	*Không*	*Không*
46	Quảng Nam	*Smart Quảng Nam (10,000+)*	*Không*
47	Quảng Ngãi	*Không*	*Không*
48	Quảng Ninh	*Smart Quảng Ninh (10,000+)*	*Không*
49	Quảng Trị	*QUANGTRI IOC (1,000+)*	*Không*
50	Sóc Trăng	*Công dân tỉnh Sóc Trăng (500+)*	*Không*
51	Sơn La	*Sơn La Smart (10,000+)*	*Không*

STT	Tỉnh, thành phố trực thuộc trung ương	Ứng dụng thông minh được đánh giá	Các Ứng dụng khác được tìm thấy nhưng không được đánh giá
52	Tây Ninh	*Tây Ninh Smart (1022 Tây Ninh) (100,000+)*	*Không*
53	Thái Bình	*Thái Bình trực tuyến (100+)*	*Smart Thái Bình (100+)* *Phản ánh ANTT Thái Bình (50+)*
54	Thái Nguyên	*C-Thái Nguyên (100,000+)*	*Thái Nguyên ID (10,000+)* *Thái Nguyên SmartCity (100+)*
55	Thanh Hóa	*Smart Thanh Hóa (5,000+)*	*Công dân số tỉnh Thanh Hóa (100+)* *Phản hồi Thanh Hóa (100+)*
56	Thừa Thiên Huế	*Hue-S (100,000+)*	*Không*
57	Tiền Giang	*TienGiangS (50,000+)*	*Không*
58	Thành phố Hồ Chí Minh	*Không*	*Không*
59	Trà Vinh	*1102 Trà Vinh (500+)*	*Không*
60	Tuyên Quang	*Không*	*Không*
61	Vĩnh Long	*Smart Vĩnh Long (5,000+)*	*Không*
62	Vĩnh Phúc	*Vĩnh Phúc Smart (5+)*	*Không*
63	Yên Bái	*Không*	*Không*

17 tiêu chí đánh giá

	14 tiêu chí đánh giá chính sách về quyền riêng tư (Privacy policy)	Cách đánh giá/chấm điểm
I	**Mức độ sẵn có và dễ tiếp cận**	
1.1	**Có công khai hay không chính sách về quyền riêng tư?**	• Không • Có
1.2	**Có hay không bản chính sách về quyền riêng tư bằng tiếng Việt?**	• Không • Có: tiếng Anh • Có: tiếng Việt • Có: cả tiếng Anh và tiếng Việt
1.3	**Chính sách quyền riêng tư có xác định cơ sở pháp lý để thu thập và xử lý dữ liệu?**	• Không • Có: nhắc sơ sài • Có: trích dẫn nguồn
I	**Xác định các chủ thể liên quan, và phân định rõ quyền, nghĩa vụ tương ứng**	
1.4	**Có hay không tuyên bố về chủ thể chịu trách nhiệm?** • Phải tuyên bố rõ ràng về chủ thể chịu trách nhiệm thu thập, xử lý dữ liệu cá nhân • Ví dụ: Ứng dụng này thuộc về Ủy ban nhân dân tỉnh X, được vận hành bởi Sở Thông tin và Truyền thông tỉnh X (còn việc Sở Thông tin và Truyền thông tự vận hành hay thuê đơn vị nào cung cấp dịch vụ thì đơn vị được thuê là nhà thầu). Việc giao kết các điều khoản về bảo vệ dữ liệu cá nhân là giao kết giữa một cá nhân - công dân Việt Nam với một Ủy ban nhân dân tỉnh X cung cấp dịch vụ công trực tuyến.	• Không • Có: là đơn vị cung cấp dịch vụ và vận hành - VD như AIC – Quảng Ninh, VNPT, ... • Có: là CQNN vận hành – sở TTTT, văn phòng IOC • Có: là CQNN chủ quản – UBND
1.5	**Chính sách về quyền riêng tư có nêu rõ chủ thể dữ liệu là ai?**	• Không • Có: nhắc tên, không giải thích • Có: giải thích sơ sài • Có: giải thích kĩ

	14 tiêu chí đánh giá chính sách về quyền riêng tư (Privacy policy)	Cách đánh giá/chấm điểm
1.6	**Tuyên bố về cam kết với dữ liệu cá nhân trẻ em** • Phải có nội dung về bảo vệ trẻ em trên môi trường mạng do trẻ em là chủ thể thuộc nhóm dễ bị tổn thương (chưa hoàn thiện về nhận thức về quyền và khả năng thực hiện quyền của mình) • Trẻ em là cá nhân có độ tuổi 16 tuổi trở xuống theo Luật trẻ em • Theo Luật trẻ em, điều 6(11) Công bố, tiết lộ thông tin về đời sống riêng tư, bí mật cá nhân của trẻ em mà không được sự đồng ý của trẻ em từ đủ 07 tuổi trở lên và của cha, mẹ, người giám hộ của trẻ em là một trong những hành vi bị nghiêm cấm • Tuyên bố ứng dụng có thu thập hay không thu thập dữ liệu của trẻ em Nếu có thu thập dữ liệu của trẻ em thì phải đảm bảo dữ liệu được thu thập khi có sự đồng ý của người giám hộ, thông báo cho người giám hộ, nói chung các quyền riêng tư dữ liệu của trẻ em được thực hiện theo yêu cầu của người giám hộ	• Không • Có: nhắc tên, không giải thích • Có: giải thích sơ sài • Có: giải thích kĩ
	Thông tin về dữ liệu:	
1.7	**Trong chính sách về riêng tư, có liệt kê các dạng thông tin được thu thập không?**	• Không Có: nhắc tên, nhưng • không giải thích • Có: giải thích sơ sài • Có: giải thích tương đối chi tiết
1.8	**Trong chính sách riêng tư, có liệt kê mục đích sử dụng của dữ liệu?**	• Không • Có: giải thích sơ sài • Có: giải thích cụ thể
1.9	**Có hay không thông báo về thời gian lưu trữ dữ liệu?**	• Không • Có: chỉ nhắc đến • Có: có nhắc và giải thích
1.10	**Trong chính sách riêng tư, có ghi rõ những ai/đơn vị/tổ chức nào được truy cập vào dữ liệu, hay dữ liệu được chia sẻ với ai?**	• Không • Có: nhắc tên, không giải thích • Có: giải thích sơ sài • Có: giải thích kĩ

	14 tiêu chí đánh giá chính sách về quyền riêng tư (Privacy policy)	Cách đánh giá/chấm điểm
1.11	**Trong chính sách về quyền tư, có liệt kê các dạng nguy cơ, công khai và giải thích các nguy cơ được hạn chế như thế nào?**	• Không • Có: nhắc tên, không giải thích • Có: giải thích sơ sài • Có: giải thích kĩ
1.12	**Chính sách về quyền riêng tư có thể hiện cam kết đối với Quyền được thông báo về các thay đổi hay không?**	• Không • Có: giải thích sơ sài • Có: giải thích kĩ
	Thông tin liên hệ (để yêu cầu tiếp cận, chỉnh sửa, cập nhật, khiếu nại, ...)	
1.13	**Chính sách về quyền riêng rư có cung cấp cơ chế liên hệ hay không?** • Phải tuyên bố rõ ràng về phương thức giải quyết tranh chấp, khiếu nại • Cụ thể hóa người dùng có thể khiếu nại đến những địa chỉ nào: • Sở Thông tin và Truyền thông tỉnh X do sở này là đơn vị vận hành: thông tin liên hệ • Bộ phận nhận khiếu nại của Ủy ban Nhân dân tỉnh X do Ủy ban là chủ thể quản lý chung ứng dụng này: thông tin liên hệ	• Không • Có: giải thích sơ sài • Có: giải thích kĩ
1.14	**Chính sách về quyền riêng tư có làm rõ thời gian cam kết sẽ xử lý câu hỏi/ khiếu nại?**	• Không • Có: chung chung sẽ xử lý trong thời gian nhanh nhất có thể • Có: cụ thể thời gian, cách thức, và nếu có trì hoãn, sẽ giải thích vì sao có trì hoãn
	3 tiêu chí đánh giá mức độ triển khai thực tế	
2.1	**Quyền đồng ý:** được trao quyền lựa chọn "Tôi đồng ý cung cấp dữ liệu" không? Có đính kèm chính sách về quyền riêng tư cùng quyền đồng ý?	• Không thông báo • Có thông báo nhưng không kèm chính sách về quyền riêng tư (thường dưới dạng 1 ô vuông cho người dùng tích vào) • Có thông báo và kèm điều khoản sử dụng có đề cập đến bảo vệ dữ liệu cá nhân • Có thông báo và có kèm theo chính sách về quyền riêng tư

	14 tiêu chí đánh giá chính sách về quyền riêng tư (Privacy policy)	Cách đánh giá/chấm điểm
2.2	Quyền tiếp cận (xem), liên hệ chỉnh sửa, xoá dữ liệu, khiếu nại bồi thường được thể hiện như thế nào?	Gửi emails đến các đầu mối liên hệ • Không hồi đáp • Có hồi đáp sơ sài • Có hồi đáp cụ thể
2.3	Quyền được giới hạn thông tin cá nhân được công khai hiển thị trên các ứng dụng hoặc các cổng như thế nào?	• Có ẩn danh tốt • Có ẩn danh 1 phần • Không ẩn danh • Chưa thể đánh giá:

PDPR2022

CÁC CƠ QUAN ĐỒNG THỰC HIỆN

IPS Institute for Policy Studies and Media Development

UNDP

CÁC CƠ QUAN ĐỒNG TÀI TRỢ

Ambasáid na hÉireann | Vítneam
Embassy of Ireland | Vietnam
Đại sứ quán Ireland | Việt Nam

AUS4REFORM

Australian Aid

UNDP

Chương trình Phát triển Liên Hợp Quốc

304 Kim Mã, Hà Nội, Việt Nam
Tel: (84 024) 38 500 100
Fax: (84 024) 37 265 520
Email: registry.vn@undp.org
www.undp.org/vietnam

Viện Nghiên cứu Chính sách và Phát triển Truyền thông

Tầng 18, Tòa nhà VTC Online,
18 Tam Trinh, Hai Bà Trưng, Hà Nội
Tel: (84) 969 520 220
Email: contact@ips.org.vn
ips.org.vn