

**XỬ LÝ DỮ LIỆU CÁ NHÂN TRONG TRƯỜNG HỢP KHẨN CẤP
THEO QUY ĐỊNH PHÁP LUẬT VIỆT NAM**

NGUYỄN THỊ LONG*

ĐOÀN XUÂN NGỌC**

Ngày nhận bài: 30/01/2026

Ngày phản biện: 24/02/2026

Ngày đăng bài: 25/6/2026

Tóm tắt:

Trong quản trị nhà nước dựa trên dữ liệu, việc xử lý dữ liệu cá nhân (DLCN) trong tình huống khẩn cấp cần đảm bảo cân bằng giữa quyền riêng tư của chủ thể DLCN và lợi ích chung của cộng đồng. Bài viết phân tích quy định của pháp luật Việt Nam, chỉ ra khó khăn khi xử lý DLCN trong tình trạng khẩn cấp. Nghiên cứu kết hợp giữa phân tích luật thực định và sử dụng nguyên tắc tương xứng làm căn cứ để đánh giá mức độ hợp lý khi hạn chế quyền chủ thể dữ liệu. Từ đó, đề xuất xây dựng các điều kiện cụ thể về phạm vi, thời gian xử lý và bắt buộc phải có quy trình kiểm tra lại sau khi tình huống khẩn cấp kết thúc. Điều này nhằm đảm bảo quyền con người chỉ bị hạn chế trong mức độ thực sự cần thiết và có căn cứ pháp lý rõ ràng.

Từ khóa:

Xử lý dữ liệu cá nhân, tình huống khẩn cấp, kiểm soát quyền lực, bảo vệ quyền riêng tư.

Abstract:

In data-driven public governance, the processing of personal data in emergency situations must strike a balance between the data subject's right to privacy and the collective interests of the community. This article analyzes the relevant provisions of Vietnamese law and identifies the legal challenges associated with the processing of personal data during states of emergency. The study combines doctrinal legal analysis with the principle of proportionality as a framework for assessing the legitimacy of restrictions on data subjects' rights. On that basis, the article proposes establishing specific conditions governing the scope and duration of personal data processing, together with mandatory review procedures following the end of an emergency. These measures are intended to ensure that restrictions on human rights are imposed only to the extent strictly necessary and on the basis of clear legal grounds.

Keywords:

Processing of personal data, emergency situation, control of power, privacy protection.

* TS., GVC, Khoa Pháp luật Dân sự, Trường Đại học Luật Hà Nội; Email: longnt@hlu.edu.vn

** SV., Khoa Pháp luật Kinh tế, Trường Đại học Luật Hà Nội; Email: ngocdoan12082005@gmail.com

1. Đặt vấn đề

Việc xử lý DLCN trong các tình huống khẩn cấp theo điểm b khoản 1 Điều 19 Luật Bảo vệ DLCN năm 2025 dù cần thiết cho lợi ích công cộng nhưng đang đối mặt với rủi ro xâm phạm quyền của chủ thể DLCN. Mặc dù Luật Tình trạng khẩn cấp năm 2025 đã được ban hành nhưng pháp luật Việt Nam vẫn còn thiếu các tiêu chí định lượng về “mức độ cần thiết”, dẫn đến nguy cơ lạm quyền xử lý DLCN. Các nghiên cứu hiện hành chủ yếu tập trung vào quyền chung của chủ thể DLCN mà chưa nghiên cứu thiết lập các tiêu chí giới hạn cụ thể bao gồm giới hạn về mục đích sử dụng, phạm vi dữ liệu tối thiểu và thời hạn lưu trữ sau khẩn cấp. Bài viết tập trung xác lập các điều kiện áp dụng và cơ chế hậu kiểm, từ đó đề xuất mô hình hoàn thiện pháp luật nhằm đảm bảo sự cân bằng thực chất giữa yêu cầu ứng phó khẩn cấp và bảo vệ quyền riêng tư.

2. Quy định pháp luật Việt Nam hiện hành về xử lý dữ liệu cá nhân trong trường hợp khẩn cấp

2.1. Nhận diện tình trạng khẩn cấp theo quy định pháp luật Việt Nam

Theo điểm b khoản 1 Điều 19 Luật Bảo vệ DLCN năm 2025, việc xử lý DLCN không cần sự đồng ý của chủ thể dữ liệu được cho phép trong các trường hợp liên quan đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội, thảm họa lớn, dịch bệnh nguy hiểm; khi tồn tại nguy cơ đe dọa an ninh, quốc phòng nhưng chưa đến mức ban bố tình trạng khẩn cấp; cũng như trong hoạt động phòng, chống bạo loạn, khủng bố, tội phạm và vi phạm pháp luật nghiêm trọng theo quy định của pháp luật. Về bản chất, quy định này thể hiện cách tiếp cận mở rộng căn cứ hạn chế quyền riêng tư dựa trên tiêu chí “nguy cơ” thay vì điều kiện pháp lý đã được xác lập chính thức. Cách tiếp cận này cho thấy pháp luật ưu tiên tính linh hoạt và bảo đảm khả năng phản ứng nhanh của Nhà nước trước các rủi ro mang tính hệ thống, xuất phát từ yêu cầu bảo vệ lợi ích công cộng¹ đồng thời đặt ra yêu cầu kiểm soát chặt chẽ để tránh lạm quyền.

Ở góc độ pháp luật chung, Luật Tình trạng khẩn cấp năm 2025 quy định tình trạng khẩn cấp “là trạng thái xã hội được cơ quan có thẩm quyền ban bố hoặc công bố khi xảy ra hoặc có nguy cơ xảy ra thảm họa, hoặc khi xuất hiện tình huống đe dọa nghiêm trọng đến tính mạng, sức khỏe con người, tài sản, quốc phòng, an ninh quốc gia và trật tự an toàn xã hội”². Điểm đáng chú ý là dù thừa nhận yếu tố “nguy cơ”, luật vẫn gắn việc áp dụng các biện pháp đặc biệt với một hành vi pháp lý chính thức

¹ Đặng Minh Tuấn (2024), *Pháp quyền trong tình trạng khẩn cấp: khung lý luận và thách thức pháp lý đặt ra*, Tạp chí Quản lý Nhà nước, Số 344, tháng 9/2024, truy cập tại <https://vi.quanlynhanuoc.vn/qlnn/article/view/946>, truy cập ngày 10/01/2026.

² Điều 2 Luật Tình trạng khẩn cấp năm 2025.

của cơ quan có thẩm quyền. Như vậy, tiêu chí “nguy cơ” trong luật này không vận hành độc lập mà được “thể chế hóa” thông qua quyết định công bố tình trạng khẩn cấp, qua đó tạo ra một ngưỡng pháp lý rõ ràng để kích hoạt các biện pháp hạn chế quyền. Luật quy định ba nhóm gồm: khẩn cấp về thảm họa; khẩn cấp về an ninh quốc gia, trật tự an toàn xã hội; và khẩn cấp về quốc phòng. Việc phân loại này giúp xác định rõ mục đích và phạm vi áp dụng các biện pháp can thiệp.

Từ góc độ pháp luật chuyên ngành, một số luật cũng đã có quy định nhận diện tình trạng khẩn cấp trong từng lĩnh vực. Luật Quốc phòng năm 2018 cho phép ban bố tình trạng khẩn cấp về quốc phòng khi xuất hiện nguy cơ trực tiếp bị xâm lược hoặc đã xảy ra hành vi xâm lược, bạo loạn vũ trang nhưng chưa đến mức tuyên bố tình trạng chiến tranh³. Trong lĩnh vực y tế, Luật Phòng, chống bệnh truyền nhiễm năm 2007 xác định tình trạng khẩn cấp khi dịch bệnh lây lan nhanh trên diện rộng, đe dọa nghiêm trọng đến tính mạng, sức khỏe con người và sự ổn định kinh tế - xã hội⁴. Tương tự, Luật Thú y năm 2015 quy định việc ban bố tình trạng khẩn cấp trong trường hợp dịch bệnh động vật lây lan rộng⁵... Những quy định này cho thấy tình trạng khẩn cấp thường được nhận diện thông qua ba dấu hiệu cốt lõi: (i) Mức độ đe dọa nghiêm trọng đến lợi ích công cộng; (ii) Phạm vi ảnh hưởng rộng; và (iii) Yêu cầu áp dụng các biện pháp can thiệp đặc biệt vượt ra ngoài cơ chế quản lý thông thường.

Đối chiếu Luật Bảo vệ DLCN năm 2025 của Việt Nam với quy định chung về bảo vệ dữ liệu của Liên minh châu Âu (GDPR) cho thấy GDPR cho phép xử lý DLCN nhạy cảm không cần sự đồng ý trong các trường hợp “vì lợi ích công cộng quan trọng, đặc biệt trong lĩnh vực y tế hoặc an toàn cộng đồng”, với điều kiện không lấn át quyền và tự do cơ bản của chủ thể dữ liệu⁶. GDPR phân biệt các căn cứ xử lý như “vital interests”, “public interest” và “legitimate interests”, gắn với các nguyên tắc như giới hạn mục đích, tối thiểu hóa dữ liệu và đặc biệt là kiểm tra tính cần thiết, tương xứng của biện pháp. GDPR không chỉ xác định “khi nào được xử lý” mà còn kiểm soát “mức độ và cách thức xử lý”, qua đó thu hẹp đáng kể nguy cơ lạm dụng. Theo quy định của Điều 19 Luật bảo vệ DLCN năm 2025, pháp luật Việt Nam cho phép xử lý DLCN từ giai đoạn “nguy cơ” trong khi GDPR kiểm soát chặt chẽ hơn bằng cách yêu cầu các căn cứ xử lý phải được diễn giải hẹp và luôn chịu sự giám sát về tính tương xứng.

Từ góc độ quyền con người, quyền của chủ thể DLCN là quyền con người, việc cho phép xử lý dữ liệu mà không cần sự đồng ý của chủ thể thực chất là một hình thức

³ Khoản 10 Điều 2 Luật Quốc phòng 2018.

⁴ Điều 42 Luật Phòng, chống bệnh truyền nhiễm năm 2007.

⁵ Khoản 6 Điều 26 Luật Thú y năm 2015.

⁶ European Parliament & Council (2016). *Regulation (EU) 2016/679 (GDPR)*, truy cập tại <https://gdpr-info.eu/art-9-gdpr/>, truy cập ngày 10/01/2026.

hạn chế quyền. Theo Điều 29 Tuyên ngôn Quốc tế về Nhân quyền năm 1948, cũng như Điều 14 Hiến pháp năm 2013, sửa đổi, bổ sung năm 2025 của Việt Nam, việc hạn chế quyền chỉ được đặt ra trong những trường hợp thật sự cần thiết, vì các lợi ích công cộng chính đáng, và phải được quy định bằng luật⁷. Do đó, việc xác định chính xác tình trạng khẩn cấp và ranh giới giữa “nguy cơ dự báo” và “khẩn cấp thực tế” là điều kiện quan trọng nhằm bảo đảm tính hợp hiến và chính đáng của hoạt động xử lý DLCN.

2.2. Chủ thể có quyền xử lý dữ liệu cá nhân trong trường hợp khẩn cấp

Theo Luật Bảo vệ DLCN năm 2025, việc xử lý DLCN không cần sự đồng ý của chủ thể trong tình huống khẩn cấp có thể được thực hiện bởi bốn nhóm chủ thể với vai trò và trách nhiệm khác nhau.

Thứ nhất, bên kiểm soát DLCN là chủ thể có thẩm quyền quyết định mục đích và phương tiện xử lý dữ liệu, qua đó giữ vai trò trung tâm và chi phối toàn bộ quá trình xử lý⁸. Trong các tình huống khẩn cấp, chủ thể này đánh giá mức độ rủi ro, xác định phạm vi dữ liệu cần xử lý và lựa chọn phương thức xử lý phù hợp.

Thứ hai, bên xử lý DLCN là chủ thể thực hiện các hoạt động xử lý dữ liệu theo yêu cầu và dưới sự chỉ đạo của bên kiểm soát dữ liệu⁹. Trong bối cảnh khẩn cấp, chủ thể này không được tự ý thay đổi mục đích xử lý hoặc mở rộng phạm vi DLCN được xử lý, đồng thời phải chịu trách nhiệm khi xảy ra sai sót kỹ thuật hoặc rò rỉ thông tin.

Thứ ba, bên kiểm soát và xử lý DLCN: Khoản 9 Điều 2 Luật Bảo vệ DLCN năm 2025 thừa nhận mô hình “chủ thể lai”, đồng thời là “Bên kiểm soát và Bên xử lý DLCN”, khác với cơ chế phân tách vai trò tương đối rõ của GDPR¹⁰. Khi hai chức năng này được tập trung vào cùng một chủ thể, nguy cơ nói lỏng hoặc mở rộng mục đích xử lý dữ liệu gia tăng do thiếu sự kiểm soát độc lập. Đây cũng là rủi ro đã một số nghiên cứu về GDPR cảnh báo¹¹. Mô hình này đồng thời có thể làm suy yếu nguyên tắc trách nhiệm giải trình, bởi rất khó xác định sai phạm phát sinh từ quyết định xử lý DLCN hay từ quá trình xử lý kỹ thuật.

⁷ Ventrella, E. (2020). *Privacy in emergency circumstances: data protection and the Covid-19 pandemic*. Truy cập tại <https://pmc.ncbi.nlm.nih.gov/articles/PMC7521575/>, truy cập ngày 10/01/2026.

⁸ Xem khoản 7, Điều 2 Luật Bảo vệ DLCN năm 2025.

⁹ Xem khoản 8, Điều 2 Luật Bảo vệ DLCN năm 2025.

¹⁰ EDBP, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Version 2.1)*, truy cập tại https://www.edpb.europa.eu/system/files_en?file=2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf, truy cập ngày 26/4/2026.

¹¹ van Binsbergen, L. T., Steketee, M. C., Kebede, M. G., Janssen, H. L., & van Engers, T. M. (2025). *Lawful and accountable personal data processing with GDPR-based access and usage control in distributed systems*. Truy cập tại https://www.researchgate.net/publication/389715228_Lawful_and_Accountable_Personal_Data_Processing_with_GDPRbased_Access_and_Usage_Control_in_Distributed_Systems, truy cập ngày 26/4/2026.

Thứ tư, bên thứ ba là chủ thể không thuộc ba nhóm chủ thể nêu trên nhưng tham gia vào quá trình xử lý DLCN theo quy định pháp luật¹². Luật Bảo vệ DLCN năm 2025 chưa quy định rõ ràng về quyền và nghĩa vụ cụ thể của bên thứ ba, dẫn đến nguy cơ phát sinh khoảng trống trách nhiệm pháp lý. Trong khi đó, GDPR quy định chặt chẽ việc bên thứ ba chỉ được xử lý dữ liệu trong phạm vi chỉ đạo của bên kiểm soát nhằm hạn chế xử lý vượt mục đích.

Mặc dù Luật Bảo vệ DLCN năm 2025 đã quy định về xử lý DLCN không cần sự đồng ý của chủ thể trong tình huống khẩn cấp, nhưng các quy định hiện hành về thẩm quyền xử lý dữ liệu trong trường hợp khẩn cấp vẫn mang tính khái quát, chưa xác định rõ chủ thể có quyền đưa ra quyết định cuối cùng trong những tình huống đòi hỏi phản ứng nhanh. Điều này không chỉ gây khó khăn trong thực tiễn áp dụng mà còn có thể làm suy giảm hiệu quả ứng phó trong thực tiễn.

2.3. Giới hạn về thời gian, phạm vi và mục đích xử lý dữ liệu cá nhân trong trường hợp khẩn cấp

Thứ nhất, quy định về thời hạn quy định xử lý DLCN trong trường hợp khẩn cấp

Theo điểm b khoản 1 Điều 19 Luật Bảo vệ DLCN năm 2025, pháp luật cho phép xử lý dữ liệu mà không cần sự đồng ý của chủ thể không đồng nghĩa với việc trao cho các chủ thể xử lý quyền tùy nghi không giới hạn về mặt thời gian. Ngược lại, yếu tố thời hạn phải được xác định và kiểm soát chặt chẽ nhằm bảo đảm tính cần thiết, tương xứng và tạm thời của hoạt động xử lý.

Thời điểm bắt đầu xử lý DLCN

Điểm b khoản 1 Điều 19 Luật Bảo vệ DLCN năm 2025 hiện nay chưa quy định cụ thể. Thực tiễn cho thấy các nhà lập pháp cần cân nhắc cụm từ “cần xử lý ngay” để xác định mốc khởi phát hoạt động xử lý dữ liệu. Việc xử lý dữ liệu có thể được triển khai ngay khi xuất hiện dấu hiệu thực tiễn cho thấy nguy cơ gây tổn hại nghiêm trọng nếu không có biện pháp can thiệp kịp thời, thay vì phải chờ một quyết định hành chính chính thức về tình trạng khẩn cấp.

Thời điểm kết thúc xử lý DLCN

Theo Điều 3 Luật Bảo vệ DLCN năm 2025, việc xử lý dữ liệu trong tình huống khẩn cấp mang tính tạm thời và chỉ tồn tại trong phạm vi cần thiết. Ví dụ: DLCN chỉ được xử lý nhằm phục vụ trực tiếp cho việc bảo vệ tính mạng, sức khỏe con người hoặc bảo đảm an ninh, trật tự xã hội. Khi mục đích xử lý không còn tồn tại, việc tiếp

¹² Xem khoản 10 Điều 2 Luật Bảo vệ DLCN năm 2025.

tục xử lý hoặc lưu trữ dữ liệu sẽ vượt quá giới hạn pháp luật cho phép. Trên thực tế, thời điểm kết thúc thường được xác lập thông qua quyết định của cơ quan nhà nước có thẩm quyền, như tuyên bố hết dịch, xác nhận chấm dứt mối đe dọa an ninh hoặc dỡ bỏ trạng thái khẩn cấp. Sau thời điểm này, việc tiếp tục khai thác dữ liệu thu thập trong giai đoạn khẩn cấp có thể dẫn đến xâm phạm quyền riêng tư và làm sai lệch mục đích ban đầu. Vì vậy, việc xác định rõ thời điểm kết thúc xử lý là điều kiện quan trọng.

Thứ hai, quy định về các loại DLCN được xử lý.

Luật Bảo vệ DLCN năm 2025 phân loại DLCN thành hai nhóm cơ bản là DLCN cơ bản và DLCN nhạy cảm. Trong tình huống khẩn cấp, khi cơ chế xử lý không cần sự đồng ý được áp dụng, các dữ liệu được phép xử lý chủ yếu là những thông tin cần thiết để bảo vệ tính mạng con người và an ninh quốc gia. Một số nhóm DLCN thường được xử lý bao gồm: (i) Dữ liệu vị trí và lịch trình di chuyển phục vụ truy vết, cứu nạn hoặc khoanh vùng rủi ro; (ii) Dữ liệu nhạy cảm về sức khỏe nhằm phục vụ cấp cứu hoặc phòng, chống dịch bệnh; và (iii) Dữ liệu định danh và thông tin liên hệ phục vụ cảnh báo, sơ tán hoặc xác minh danh tính. Việc miễn trừ yêu cầu đồng ý đối với các nhóm dữ liệu này được đặt trên cơ sở bảo vệ lợi ích sống còn của chủ thể dữ liệu và lợi ích cộng đồng. Tuy nhiên, hoạt động xử lý vẫn phải tuân thủ nguyên tắc cân xứng, chỉ giới hạn trong phạm vi cần thiết để giải quyết tình huống khẩn cấp và không được mở rộng sang các mục đích khác.

Thứ ba, quy định về nội dung và mục đích xử lý DLCN trong tình trạng khẩn cấp.

Theo khoản 6 Điều 2 Luật Bảo vệ DLCN năm 2025, xử lý DLCN bao gồm toàn bộ các hành vi tác động lên dữ liệu, từ thu thập, ghi nhận, phân tích, xác minh, lưu trữ cho đến công khai, truyền đưa, chia sẻ, chuyển giao, mã hóa, xóa bỏ hoặc hủy dữ liệu... Từ góc độ nguyên tắc tương xứng, việc Luật Bảo vệ dữ liệu cá nhân năm 2025 định nghĩa xử lý dữ liệu cá nhân theo hướng bao quát toàn bộ các hành vi tác động lên dữ liệu giúp mở rộng phạm vi kiểm soát đối với mọi hoạt động có khả năng ảnh hưởng đến quyền riêng tư của chủ thể dữ liệu. Tuy nhiên, pháp luật hiện hành mới dừng lại ở việc xác định các hành vi xử lý dữ liệu mà chưa quy định rõ giới hạn tương ứng đối với từng hoạt động xử lý trong tình trạng khẩn cấp. Điều này có thể dẫn đến nguy cơ cơ quan có thẩm quyền mở rộng phạm vi thu thập, chia sẻ hoặc lưu trữ dữ liệu vượt quá mức cần thiết cho mục tiêu ứng phó khẩn cấp. Do đó, cần tiếp tục cụ thể hóa các tiêu chí đánh giá tính cần thiết và tính tương xứng của từng hoạt động xử lý dữ liệu nhằm bảo đảm rằng việc hạn chế quyền bảo vệ dữ liệu cá nhân chỉ được thực hiện trong phạm vi thực sự cần thiết để bảo vệ lợi ích cộng đồng.

3. Thực tiễn xử lý dữ liệu cá nhân trong trường hợp tình trạng khẩn cấp và một số vấn đề đặt ra

Thứ nhất, thiếu cơ chế kiểm soát quyền xử lý DLCN trong tình trạng khẩn cấp - minh chứng từ đại dịch Covid-19 tại Việt Nam.

Thực tiễn ứng phó đại dịch Covid-19 tại Việt Nam cho thấy việc thu thập và sử dụng các loại DLCN như lịch sử di chuyển, tình trạng y tế, thông tin liên hệ cá nhân được triển khai rộng rãi để phục vụ công tác truy vết, khoanh vùng dịch tễ và ngăn chặn nguy cơ lây lan trên diện rộng¹³. Nhà nước cũng đã nỗ lực cân bằng giữa bảo vệ lợi ích công cộng và bảo đảm quyền riêng tư cá nhân. Tuy nhiên, thực tiễn cũng bộc lộ khoảng trống pháp lý về xử lý DLCN trong tình huống đặc biệt này.

- Xử lý DLCN không cần sự đồng ý thông qua ứng dụng truy vết điện tử Bluezone/NCovi.

Năm 2020, ứng dụng Bluezone đạt hơn 20 triệu lượt tải, còn NCovi ghi nhận khoảng 7,2 triệu lượt khai báo y tế. Bluezone sử dụng Bluetooth để ghi nhận tiếp xúc gần giữa người dùng nhằm hỗ trợ truy vết dịch tễ¹⁴. Về mặt chức năng, Bluezone sử dụng Bluetooth để ghi nhận tiếp xúc gần giữa người dùng nhằm hỗ trợ truy vết dịch tễ. Dù dữ liệu được cho là lưu cục bộ và ẩn danh, nhiều chuyên gia nhận định vẫn tồn tại nguy cơ tái nhận dạng khi kết hợp với nguồn dữ liệu khác¹⁵. Từ góc độ pháp lý, trường hợp Bluezone cho thấy Nhà nước có thể xử lý DLCN mà không cần sự đồng ý trong tình trạng khẩn cấp, nhưng chưa có quy định rõ về phạm vi dữ liệu được thu thập, thời hạn lưu trữ, cơ chế xóa dữ liệu sau dịch và trách nhiệm giải trình của cơ quan quản lý.

- Xử lý DLCN thông qua hoạt động truy vết người mang bệnh trong thực tiễn phòng, chống dịch Covid-19.

Trong làn sóng Covid-19 thứ tư năm 2021, cơ quan chức năng đã thu thập và xử lý lượng lớn dữ liệu cá nhân như lịch sử di chuyển, tình trạng sức khỏe và quan hệ tiếp xúc để phục vụ truy vết. Theo WHO, đến cuối năm 2021, Việt Nam ghi nhận hơn 1,65 triệu ca nhiễm và thực hiện khoảng 35,4 triệu xét nghiệm trên toàn quốc phục vụ truy vết dịch tễ¹⁶. Việt Nam áp dụng cơ chế phân loại F0-F4 và triển khai truy vết diện rộng

¹³ National Library of Medicine, “In the interest of public safety: rapid response to the Covid-19 epidemic in Vietnam”, truy cập tại https://pmc.ncbi.nlm.nih.gov/articles/PMC7839307/?utm_source, truy cập ngày 20/01/2026.

¹⁴ Exemplars in Global Health. (2021). *Digital Health Vietnam Narrative*, truy cập tại https://assets-us-01.kc-usercontent.com/f5df0764-22d9-0088-d50f-b04f28688d85/5a134e67-3603-4773-aded-c7c3d7ea69e7/ECR_Digital%20Health_Vietnam_Narrative_Vietnamese%20v2021_0628.pdf, truy cập ngày 26/4/2026.

¹⁵ Globe (2020), “Vietnam’s contact-tracing app: Public health tool or creeping surveillance?”, truy cập tại https://southeastasiaglobe.com/bluezone-contact-tracing-app/?utm_source, truy cập ngày 26/01/2026.

¹⁶ World Health Organization & Ministry of Health Viet Nam (2021, December 26), *Viet Nam coronavirus disease 2019 (Covid-19) situation report #74*, truy cập tại https://www.who.int/docs/default-source/wpro---documents/countries/viet-nam/covid-19/viet-nam-moh-who-covid-19-sitrep_26dec2021.pdf?sfvrsn=e1240a3f_5, truy cập ngày 26/4/2026.

nhằm kiểm soát lây nhiễm trong cộng đồng. Tuy nhiên, thực tiễn này cũng làm phát sinh nhiều vấn đề pháp lý như lộ lọt DLCN công khai lịch trình di chuyển của người nhiễm bệnh và chia sẻ dữ liệu vượt quá phạm vi cần thiết. Bộ Y tế và Bộ Thông tin và Truyền thông khi đó đã phải yêu cầu các địa phương không công khai danh tính bệnh nhân Covid-19 nhằm bảo vệ quyền riêng tư¹⁷. Điều này cho thấy quyền xử lý dữ liệu cá nhân trong tình trạng khẩn cấp đã được mở rộng đáng kể nhưng chưa đi kèm cơ chế giám sát và hậu kiểm tương xứng¹⁸.

Thứ hai, nguy cơ mở rộng quyền xử lý dữ liệu vượt quá mục đích khẩn cấp (nhìn từ vụ việc xử lý của Hoa Kỳ).

Thực tiễn quốc tế cho thấy vấn đề xử lý DLCN không cần sự đồng ý của chủ thể dữ liệu trong tình trạng khẩn cấp không chỉ đặt ra thách thức tại Việt Nam mà còn là bài toán chung của nhiều quốc gia. Một trong những ví dụ điển hình là vụ việc Apple từ chối hỗ trợ Cục Điều tra Liên bang Hoa Kỳ (FBI) mở khóa thiết bị của nghi phạm trong một vụ xả súng nghiêm trọng¹⁹, vụ việc này cho thấy xung đột giữa yêu cầu bảo đảm an ninh quốc gia và bảo vệ quyền riêng tư của chủ thể DLCN. Trong hoạt động của Apple - FBI, một số học giả cho rằng cơ quan thực thi pháp luật cần được phép truy cập dữ liệu trong các nhiệm vụ khủng bố hoặc tội phạm nghiêm trọng trên cơ sở pháp lý nhằm bảo vệ an ninh quốc gia. Ngược lại, phe phản đối cho rằng yêu cầu của FBI có thể tạo ra tiền nguy hiểm cho quyền riêng tư của người dùng. Giải pháp được các học giả đề xuất là cơ quan điều tra chỉ được yêu cầu truy cập DLCN trong: (i) Trường hợp thực sự cần thiết (như khủng bố) và phải có lệnh của tòa án; (ii) Giới hạn mục đích xử lý DLCN trong từng trường hợp cụ thể; (iii) Có hoạt động giám sát, đảm bảo minh bạch và trách nhiệm giải trình rõ ràng. Thực chất, giải pháp này dựa trên quy định của Hoa Kỳ trong Tu chính thứ Tư, yêu cầu khám khám và truy cập dữ liệu phải dựa trên căn cứ hợp lý và thường phải có lệnh, giám sát tòa án, đồng thời giới hạn công việc sử dụng dữ liệu. Tòa án Tối cao Mỹ trong vụ Riley v. California (2014) đã khẳng định việc khám nghiệm dữ liệu điện thoại di động phải có lệnh khám vì điện thoại chứa đựng số lượng lớn DLCN²⁰.

¹⁷ Giang, T. (2021), *Privacy of Covid-19 patients needs to be protected*. Vietnamnet, truy cập tại <https://vietnamnet.vn/en/privacy-of-covid-19-patients-needs-to-be-protected-741642.html?>

¹⁸ Le, T.-A. T., Vodden, K., Wu, J., & Atiweh, G. (2021). *Policy responses to the Covid-19 pandemic in Vietnam*. International Journal of Environmental Research and Public Health, 18(2), 559. Truy cập tại <https://pmc.ncbi.nlm.nih.gov/articles/PMC7828055/>, truy cập ngày 26/4/2026.

¹⁹ EBSCO, FBI-Apple encryption dispute, truy cập tại <https://www.ebsco.com/research-starters/law/fbi-apple-encryption-dispute>, truy cập ngày 25/01/2026.

²⁰ Riley v. California, 573 U.S. 373 (2014), Supreme Court of the United States, truy cập tại <https://supreme.justia.com/cases/federal/us/573/373/>, truy cập ngày 26/4/2026.

Thứ ba, xuất hiện thách thức đối với cơ chế giám sát việc tuân thủ pháp luật về dữ liệu cá nhân.

Việc mở rộng quyền xử lý dữ liệu trong tình trạng khẩn cấp cũng đặt ra thách thức đối với các thiết chế giám sát. Khi nhiều chủ thể cùng tham gia xử lý dữ liệu nhưng quy định về thẩm quyền và trách nhiệm chưa rõ ràng, việc kiểm soát tính hợp pháp, cần thiết và tương xứng của hoạt động xử lý trở nên khó khăn. Vì vậy, pháp luật cần thiết lập các cơ chế giám sát độc lập và hiệu quả nhằm bảo đảm quyền lực được thực thi đúng mục đích, tránh xâm phạm quá mức quyền và lợi ích hợp pháp của chủ thể DLCN.

Từ thực tiễn xử lý dữ liệu cá nhân trong các tình huống khẩn cấp cho thấy pháp luật cần thiết lập cơ chế cân bằng giữa hai yêu cầu tưởng chừng đối lập: một mặt bảo đảm Nhà nước có đủ thẩm quyền và công cụ để ứng phó kịp thời với các tình huống đe dọa tính mạng, sức khỏe cộng đồng, quốc phòng, an ninh quốc gia hoặc trật tự, an toàn xã hội; mặt khác phải ngăn ngừa nguy cơ lạm quyền, mở rộng quá mức phạm vi xử lý dữ liệu hoặc duy trì việc xử lý dữ liệu vượt quá thời gian cần thiết.

Trên cơ sở đó, tác giả đề xuất một số định hướng hoàn thiện pháp luật như sau:

Thứ nhất, cần cụ thể hóa cơ chế kiểm soát hoạt động xử lý dữ liệu cá nhân trong trường hợp khẩn cấp trong Nghị định số 356/2025/NĐ-CP hướng dẫn thi hành Luật Bảo vệ dữ liệu cá nhân năm 2025.

Mặc dù Luật Bảo vệ dữ liệu cá nhân năm 2025 cho phép xử lý dữ liệu cá nhân trong một số trường hợp khẩn cấp, song các quy định hiện hành chưa xác định rõ cơ chế kiểm soát đối với quá trình xử lý dữ liệu. Do đó, Nghị định số 356/2025/NĐ-CP cần được hoàn thiện theo hướng thiết lập cơ chế kiểm soát ba giai đoạn gồm: (i) Phê duyệt trước; (ii) Giám sát trong quá trình thực hiện; và (iii) Hậu kiểm bắt buộc. Cách tiếp cận này phù hợp với nguyên tắc trách nhiệm giải trình (accountability), nguyên tắc tương xứng (proportionality) và yêu cầu lưu giữ hồ sơ hoạt động xử lý dữ liệu được ghi nhận trong pháp luật bảo vệ dữ liệu của Liên minh châu Âu²¹.

Ở giai đoạn phê duyệt trước, pháp luật cần phân biệt giữa tình trạng khẩn cấp đã được công bố hoặc có thể dự báo trước với các tình huống khẩn cấp đột xuất. Đối với trường hợp thứ nhất, việc xử lý dữ liệu cá nhân phải được thực hiện trên cơ sở quyết định của cơ quan có thẩm quyền công bố hoặc chủ trì ứng phó tình trạng khẩn cấp; trong phạm vi quốc gia hoặc liên tỉnh, thẩm quyền này có thể thuộc Thủ tướng Chính phủ hoặc cơ quan được giao chủ trì ứng phó, còn trong phạm vi địa phương là Chủ

²¹ GDPR, Điều 5(2), 24, 30.

tịch Ủy ban nhân dân cấp tỉnh²². Quyết định phê duyệt cần xác định rõ mục đích xử lý, loại dữ liệu được phép thu thập, nhóm chủ thể dữ liệu bị ảnh hưởng, chủ thể được tiếp cận dữ liệu và thời hạn xử lý. Đối với các tình huống đột xuất đe dọa trực tiếp đến tính mạng, sức khỏe hoặc an toàn công cộng, chủ thể có thẩm quyền được phép xử lý dữ liệu ngay để bảo đảm hiệu quả ứng phó²³, nhưng phải lưu vết hoạt động xử lý và thực hiện nghĩa vụ giải trình, hậu kiểm trong thời hạn nhất định. Cách tiếp cận này vừa bảo đảm tính kịp thời của hoạt động ứng phó khẩn cấp, vừa thể hiện nguyên tắc tương xứng khi việc hạn chế quyền bảo vệ dữ liệu cá nhân chỉ được thực hiện trong phạm vi cần thiết và luôn đặt dưới cơ chế kiểm soát phù hợp.

Ở giai đoạn giám sát trong quá trình thực hiện, cần xác định rõ vai trò của các chủ thể tham gia xử lý dữ liệu theo Luật Bảo vệ dữ liệu cá nhân năm 2025. Theo đó, cơ quan nhà nước được giao nhiệm vụ ứng phó tình trạng khẩn cấp đóng vai trò là bên kiểm soát dữ liệu cá nhân; các doanh nghiệp viễn thông, cơ sở khám chữa bệnh, doanh nghiệp công nghệ hoặc đơn vị cung cấp hạ tầng kỹ thuật tham gia thu thập, lưu trữ hoặc phân tích dữ liệu được xác định là bên xử lý dữ liệu cá nhân; các cơ quan, tổ chức tiếp nhận dữ liệu để phục vụ hoạt động ứng phó khẩn cấp được xem là bên thứ ba. Tất cả hoạt động truy cập, thu thập, chia sẻ, chuyển giao hoặc xóa dữ liệu phải được ghi nhận trên hệ thống nhật ký điện tử (audit log) và lưu giữ trong suốt thời gian xử lý nhằm phục vụ hoạt động kiểm tra, thanh tra hoặc giải trình khi cần thiết²⁴.

Ở giai đoạn hậu kiểm bắt buộc, sau khi tình trạng khẩn cấp chấm dứt, bên kiểm soát dữ liệu phải lập báo cáo tổng hợp gửi cơ quan quản lý nhà nước về bảo vệ dữ liệu cá nhân để đánh giá tính hợp pháp, tính cần thiết và tính tương xứng của hoạt động xử lý dữ liệu. Báo cáo cần làm rõ căn cứ pháp lý của việc xử lý, loại dữ liệu đã thu thập, phạm vi chia sẻ dữ liệu, thời gian lưu trữ, biện pháp bảo mật đã áp dụng và kết quả xóa hoặc ẩn danh dữ liệu sau khi hoàn thành mục đích sử dụng. Trường hợp phát hiện việc xử lý dữ liệu vượt quá phạm vi cho phép hoặc không còn đáp ứng yêu cầu cần thiết của tình trạng khẩn cấp, cơ quan có thẩm quyền có thể yêu cầu chấm dứt hoạt động xử lý, xóa dữ liệu hoặc áp dụng các biện pháp xử lý trách nhiệm theo quy định của pháp luật²⁵.

Bên cạnh đó, văn bản sửa đổi Nghị định số 356/2025/NĐ-CP nên ban hành kèm theo danh mục dữ liệu mẫu tương ứng với từng loại tình huống khẩn cấp như y tế công

²² Khoản 2 Điều 12 Luật Tình trạng khẩn cấp năm 2025.

²³ Khoản 5 Điều 3 Luật Tình trạng khẩn cấp năm 2025.

²⁴ GDPR, Điều 30 về hồ sơ hoạt động xử lý dữ liệu (Records of Processing Activities).

²⁵ GDPR, Điều 35 về đánh giá tác động bảo vệ dữ liệu (Data Protection Impact Assessment - DPIA) và Điều 36 về tham vấn trước (Prior Consultation).

cộng, thiên tai, sự cố môi trường, an ninh quốc gia hoặc phòng, chống khủng bố. Việc xác định trước phạm vi dữ liệu được phép xử lý không chỉ góp phần hạn chế tình trạng thu thập dữ liệu tràn lan mà còn bảo đảm thực hiện nguyên tắc tối thiểu hóa dữ liệu (data minimisation), theo đó chỉ những dữ liệu thực sự cần thiết cho mục đích ứng phó tình trạng khẩn cấp mới được phép thu thập và sử dụng.²⁶

Thứ hai, tăng cường hiệu quả cơ chế hậu kiểm và trách nhiệm giải trình trong xử lý dữ liệu cá nhân

Tại Việt Nam, cơ quan chuyên trách về bảo vệ DLCN giữ vai trò trung tâm trong việc quản lý, thanh tra, kiểm tra và xử lý vi phạm. Vì vậy, cơ chế hậu kiểm và trách nhiệm giải trình cần được thiết kế phù hợp với thẩm quyền quản lý hành chính của cơ quan này, tránh chồng chéo hoặc làm sai lệch chức năng của các chủ thể khác. Theo đó, pháp luật cần quy định rõ nội dung hồ sơ giải trình bắt buộc, bao gồm: căn cứ pháp lý, mục đích xử lý, nhân sự phụ trách, loại dữ liệu thu thập²⁷, thời gian lưu trữ và biện pháp bảo mật.. Trên cơ sở đó, cơ quan quản lý có thể áp dụng bộ tiêu chí đánh giá như: (i) Tính cần thiết (dữ liệu có thực sự cần cho mục tiêu khẩn cấp hay không); (ii) Tính tương xứng (phạm vi xử lý có vượt quá mức cần thiết hay không); và (iii) Tính tuân thủ quy trình (có thực hiện đầy đủ các bước phê duyệt, lưu vết và báo cáo hay không). Kết quả hậu kiểm cần gắn với chế tài cụ thể, bao gồm cả trách nhiệm hành chính và trách nhiệm cá nhân của người ra quyết định, nhằm bảo đảm tính răn đe và hiệu quả thực thi.

4. Kết luận

Thông qua việc nghiên cứu quy định Luật Bảo vệ DLCN năm 2025 và Luật Tình trạng khẩn cấp năm 2025, bài viết cho thấy pháp luật Việt Nam đã bước đầu thiết lập cơ sở pháp lý cho việc xử lý dữ liệu không cần sự đồng ý của chủ thể dữ liệu trong các tình huống đặc biệt. Đồng thời, nghiên cứu chỉ ra những khoảng trống pháp lý về căn cứ xử lý DLCN, phạm vi xử lý dữ liệu và cơ chế trách nhiệm giải trình. Trên cơ sở đó, bài viết đề xuất định hướng hoàn thiện pháp luật theo hướng cân bằng giữa yêu cầu ứng phó khẩn cấp và bảo vệ quyền chủ thể DLCN. Tuy nhiên, nghiên cứu vẫn còn hạn chế do chưa đi sâu đánh giá thực tiễn áp dụng và kinh nghiệm quốc tế. Trong thời gian tới, các nghiên cứu tiếp theo cần mở rộng theo hướng so sánh pháp luật và đánh giá tác động của công nghệ số nhằm góp phần hoàn thiện cơ chế bảo vệ dữ liệu cá nhân trong bối cảnh khẩn cấp.

²⁶ GDPR, Điều 5 khoản 1 điểm c; OECD, *Hướng dẫn về bảo vệ quyền riêng tư và lưu chuyển dữ liệu cá nhân xuyên biên giới*, 2013.

²⁷ Lili Zhang, Perihan Elif Ekmekci, Virginia Murray, Burcak Basbug Erkan, Francis P. Crawley, Xueting Li & Yandi Li (2024), The 'PROTECT' Essential Elements in Managing Crisis Data Policies, *Data Science Journal*, truy cập tại <https://datascience.codata.org/articles/10.5334/dsj-2024-012>, truy cập ngày 30/01/2026.

DANH MỤC TÀI LIỆU THAM KHẢO

1. Đặng Minh Tuấn (2024), *Pháp quyền trong tình trạng khẩn cấp: Khung lý luận và thách thức pháp lý đặt ra*. Tạp chí Quản lý Nhà nước, Số 344 (9/2024).
2. EDBP, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Version 2.1)*.
3. Exemplars in Global Health. (2021). *Digital Health Vietnam Narrative*.
4. Gianclaudio Malgieri (2020), Data protection and research: A vital challenge in the era of Covid-19 pandemic, *Computer Law & Security Review*.
5. Lili Zhang, Perihan Elif Ekmekci, Virginia Murray, Burcak Basbug Erkan, Francis P. Crawley, Xueting Li & Yandi Li (2024), *The 'PROTECT' Essential Elements in Managing Crisis Data Policies*, Data Science Journal.
6. Le, T.-A. T., Vodden, K., Wu, J., & Atiwesh, G. (2021). *Policy responses to the Covid-19 pandemic in Vietnam*. International Journal of Environmental Research and Public Health, 18(2), 559.
7. World Health Organization & Ministry of Health Viet Nam. (2021, December 26). *Viet Nam coronavirus disease 2019 (Covid-19) situation report #74*.
8. van Binsbergen, L. T., Steketee, M. C., Kebede, M. G., Janssen, H. L., & van Engers, T. M. (2025). *Lawful and accountable personal data processing with GDPR-based access and usage control in distributed systems*.