

PHÒNG NGỪA TỘI PHẠM LỪA ĐẢO CHIẾM ĐOẠT TÀI SẢN BẰNG THỦ ĐOẠN “BẮT CỐC ONLINE”

NGUYỄN VĂN HẠNH*

Sự phát triển của công nghệ thông tin, viễn thông và các nền tảng số làm xuất hiện nhiều phương thức lừa đảo chiếm đoạt tài sản mới, trong đó có “bắt cóc online”. Thực tiễn cho thấy, thủ đoạn này không chỉ gây thiệt hại về tài sản mà còn đặt ra yêu cầu mới đối với công tác quản lý nhà nước về phòng ngừa tội phạm trên không gian mạng. Bài viết làm rõ đặc điểm của lừa đảo chiếm đoạt tài sản bằng thủ đoạn “bắt cóc online”, phân tích thực trạng, hạn chế và nguyên nhân trong quản lý nhà nước, từ đó, đề xuất một số giải pháp nhằm nâng cao hiệu quả phòng ngừa trong tình hình hiện nay.

Từ khóa: Quản lý nhà nước; bắt cóc online; lừa đảo chiếm đoạt tài sản; tội phạm mạng; phòng ngừa tội phạm.

The development of information technology, telecommunications, and digital platforms has given rise to new forms of property appropriation fraud, including the so-called “online kidnapping” scheme. In practice, this scheme not only causes property losses but also poses new requirements for state management of crime prevention in cyberspace. This article clarifies the characteristics of property appropriation fraud involving “online kidnapping,” analyzes the current situation, limitations, and causes in state management, and proposes several solutions to improve the effectiveness of preventing this type of crime in the current context.

Keywords: State management; online kidnapping; property appropriation fraud; cybercrime; crime prevention.

NGÀY NHẬN: 18/8/2026 NGÀY PHẢN BIỆN, ĐÁNH GIÁ: 22/9/2026 NGÀY DUYỆT ĐĂNG: 06/10/2026

Email: hanhloan1993@gmail.com

DOI: <https://doi.org/10.59394/qlnn.370.2026.1652>

1. Đặt vấn đề

Sự phát triển của công nghệ thông tin, viễn thông và quá trình chuyển đổi số đã mang lại nhiều thuận lợi trong đời sống. Tuy nhiên, cùng với đó, không gian mạng ngày càng bị các đối tượng lợi dụng để thực hiện hành vi lừa đảo chiếm đoạt tài sản với nhiều phương thức, thủ đoạn tinh vi, khó nhận diện. Trong đó, “bắt cóc online” là thủ đoạn đáng

chú ý, không chỉ gây thiệt hại về tài sản, ảnh hưởng đến tâm lý nạn nhân mà còn đặt ra yêu cầu mới đối với công tác phòng ngừa, đấu tranh và quản lý nhà nước. Các đối tượng thường giả danh cơ quan có thẩm quyền, tạo dựng tình huống giả để đe dọa, thao túng tâm lý, yêu cầu nạn nhân giữ bí mật và cắt liên lạc

* ThS, Học viện Cảnh sát nhân dân

với người thân. Khi đã kiểm soát được tâm lý và hành vi của nạn nhân, chúng buộc nạn nhân chuyển tiền hoặc tạo dựng hình ảnh, video giả để tiếp tục gây sức ép với gia đình nhằm chiếm đoạt tài sản. Đáng chú ý, nhiều nạn nhân dù đã tiếp cận thông tin cảnh báo vẫn bị các đối tượng thao túng.

Thực trạng trên cho thấy, “bắt cóc online” không đơn thuần là sự thay đổi về thủ đoạn lừa đảo mà còn đặt ra những vấn đề mới đối với quản lý nhà nước (QLNN) trên không gian mạng. Vì vậy, công tác phòng ngừa không thể chỉ dừng ở phát hiện, điều tra và xử lý vụ việc mà cần chú trọng quản lý các điều kiện, phương tiện và môi trường mà đối tượng có thể lợi dụng. Điều này đòi hỏi sự phối hợp giữa lực lượng Công an với các cơ quan QLNN, tổ chức tín dụng, doanh nghiệp viễn thông, cơ sở giáo dục và chính quyền địa phương.

2. Nhận diện lừa đảo chiếm đoạt tài sản bằng thủ đoạn “bắt cóc online”

“Bắt cóc online” là một thủ đoạn lừa đảo chiếm đoạt tài sản, trong đó các đối tượng sử dụng phương tiện viễn thông, mạng xã hội và công nghệ số để tạo dựng tình huống giả, thao túng tâm lý và điều khiển hành vi của nạn nhân. Nạn nhân chủ yếu bị cô lập thông tin, gây áp lực tâm lý và buộc thực hiện các yêu cầu của đối tượng. Vì vậy, nhận diện thủ đoạn này qua một số đặc điểm sau:

Thứ nhất, đối tượng chủ yếu khống chế nạn nhân bằng cách thao túng tâm lý và cô lập thông tin. Các đối tượng thường giả danh cán bộ Công an, Viện kiểm sát, Tòa án hoặc người có thẩm quyền, thông báo nạn nhân liên quan đến các vụ án nghiêm trọng như rửa tiền, mua bán ma túy để gây hoang mang, lo sợ. Sau đó, chúng yêu cầu nạn nhân giữ bí mật, rời khỏi nơi ở, cắt liên lạc với gia đình hoặc tham gia các phòng họp trực tuyến nhằm duy trì sự kiểm soát. Khi bị cô lập khỏi người thân và các nguồn thông tin bên ngoài, nạn nhân khó kiểm chứng thông tin, dễ bị chi phối và thực hiện các yêu cầu của đối tượng.

Thứ hai, thủ đoạn được thực hiện thông qua sự kết hợp của nhiều phương tiện và dịch vụ. Trong một vụ việc, các đối tượng có thể sử dụng điện thoại, mạng xã hội, ứng dụng nhắn tin, gọi video, tài khoản ngân hàng và các nền tảng trực tuyến để tiếp cận, duy trì liên lạc với nạn nhân và thực hiện giao dịch. Việc sử dụng nhiều phương tiện, dịch vụ khiến công tác phòng ngừa, phát hiện và xử lý liên quan đến nhiều lĩnh vực quản lý khác nhau.

Thứ ba, phương thức phạm tội có tính xuyên biên giới và sử dụng công nghệ cao. Các đối tượng có thể hoạt động từ nước ngoài, thường xuyên thay đổi phương thức liên lạc, tài khoản nhận tiền và kịch bản lừa đảo. Một số trường hợp còn sử dụng AI, deepfake để giả giọng nói, ghép hình ảnh hoặc tạo video giả nhằm tăng tính thuyết phục. Những đặc điểm trên cho thấy “bắt cóc online” là thủ đoạn lừa đảo có sự kết hợp của nhiều yếu tố, phương tiện và dịch vụ.

QLNN trong phòng ngừa lừa đảo chiếm đoạt tài sản bằng thủ đoạn “bắt cóc online” là tổng thể hoạt động của các cơ quan có thẩm quyền trong xây dựng, tổ chức thực hiện pháp luật; quản lý các lĩnh vực liên quan; tổ chức phối hợp, tuyên truyền và hợp tác quốc tế nhằm hạn chế những điều kiện mà đối tượng có thể lợi dụng để phạm tội. Trước hết, QLNN tạo cơ sở pháp lý và xác định trách nhiệm của các cơ quan, tổ chức trong phòng ngừa.

Do “bắt cóc online” liên quan đến nhiều lĩnh vực, như: viễn thông, tài chính - ngân hàng, dữ liệu cá nhân, nền tảng số và phòng, chống tội phạm, hệ thống pháp luật và cơ chế quản lý là căn cứ để tổ chức kiểm tra, giám sát, trao đổi thông tin và xử lý vi phạm. Bên cạnh đó, QLNN góp phần kiểm soát các phương tiện, dịch vụ có thể bị lợi dụng để phạm tội. Việc quản lý thuê bao viễn thông, tài khoản thanh toán, dữ liệu cá nhân và tài khoản trên môi trường số có ảnh hưởng trực tiếp đến khả năng che giấu danh tính, tiếp cận nạn nhân và thực hiện giao dịch của đối tượng. Quản lý

nhà nước còn giữ vai trò tổ chức phối hợp giữa các cơ quan, tổ chức có liên quan.

Trong một vụ “bắt cóc online”, thông tin phục vụ xác minh thường nằm ở nhiều chủ thể, như: Công an, doanh nghiệp viễn thông, ngân hàng, gia đình và cơ sở giáo dục. Việc trao đổi thông tin kịp thời có ý nghĩa quan trọng trong xác định vị trí nạn nhân, ngăn chặn giao dịch và hạn chế hậu quả xảy ra. Đồng thời, QLNN có vai trò tổ chức tuyên truyền, giáo dục và nâng cao kỹ năng phòng ngừa cho người dân.

3. Thực trạng lừa đảo chiếm đoạt tài sản bằng thủ đoạn “bắt cóc online” và công tác quản lý nhà nước trong phòng ngừa

Thời gian gần đây, lừa đảo chiếm đoạt tài sản bằng thủ đoạn “bắt cóc online” có xu hướng gia tăng, tập trung chủ yếu vào học sinh, sinh viên. Theo số liệu của Công an TP. Hồ Chí Minh, năm 2025, trên địa bàn Thành phố ghi nhận 77 vụ việc, trong đó lực lượng chức năng đã giải cứu thành công 52 vụ (chiếm 67,5%). Riêng tháng 01/2026, tiếp tục phát sinh 16 vụ mới, trung bình khoảng hai ngày xảy ra một vụ. Phần lớn nạn nhân từ 16 - 22 tuổi, nữ giới chiếm khoảng 90%. Đáng chú ý, nhiều nạn nhân đã từng tiếp cận thông tin cảnh báo nhưng vẫn bị thao túng khi trực tiếp rơi vào tình huống do đối tượng tạo dựng (Công an TP. Hồ Chí Minh, 2025). Nhiều đối tượng hoạt động từ nước ngoài, như: Campuchia, Philippines, Malaysia. Các đối tượng này thường xuyên thay đổi kịch bản, thậm chí các đối tượng đã khai thác thông tin về gia đình nạn nhân để tăng sức ép tâm lý. Một số trường hợp còn sử dụng AI, deepfake để giả giọng nói, ghép hình ảnh hoặc tạo video giả, làm cho tình huống lừa đảo khó nhận diện hơn. Trước diễn biến phức tạp của tội phạm lừa đảo chiếm đoạt tài sản trên không gian mạng, công tác quản lý nhà nước đã được tăng cường cả về chỉ đạo, hoàn thiện cơ sở pháp lý và tổ chức phòng ngừa, xử lý, như việc ban hành Công điện số 29/CD-TTg ngày 03/4/2025 của Thủ tướng Chính phủ (Thủ

tướng Chính phủ, 2025), trong đó, yêu cầu các bộ, ngành, địa phương tăng cường phòng ngừa, xử lý hoạt động lừa đảo chiếm đoạt tài sản, nhất là hành vi sử dụng công nghệ cao trên không gian mạng.

Bên cạnh đó, Nghị định số 02/2025/NĐ-CP ngày 18/02/2025 của Chính phủ xác định trách nhiệm của Bộ Công an trong chủ động phòng ngừa, phát hiện, đấu tranh chống tội phạm, đồng thời kiến nghị khắc phục nguyên nhân, điều kiện phát sinh tội phạm (Chính phủ, 2025). Chỉ thị số 03/CT-BCA ngày 28/02/2025 cùng các văn bản nghiệp vụ có liên quan tiếp tục tạo cơ sở để lực lượng Công an triển khai các biện pháp phòng ngừa, phát hiện và đấu tranh với các phương thức, thủ đoạn phạm tội mới. Công tác phát hiện, ngăn chặn và giải cứu nạn nhân đã đạt những kết quả nhất định. Năm 2025, lực lượng chức năng đã giải cứu thành công 52 vụ cho thấy, việc phát hiện sớm, tiếp nhận thông tin và can thiệp kịp thời có ý nghĩa quan trọng trong bảo vệ nạn nhân (Nguyễn Minh, 2026). Việc quản lý thuê bao viễn thông, tài khoản ngân hàng, ví điện tử, dữ liệu cá nhân và hoạt động trên các nền tảng mạng xã hội ngày càng được quan tâm nhằm hạn chế khả năng đối tượng lợi dụng để thực hiện hành vi lừa đảo. Đặc biệt, hợp tác quốc tế trong phòng, chống tội phạm mạng tiếp tục được tăng cường. Công ước của Liên Hợp quốc về chống tội phạm mạng được mở ký tại Hà Nội ngày 25/10/2025 đã tạo cơ sở cho hợp tác trong thu thập dữ liệu điện tử xuyên biên giới, dẫn độ và truy thu tài sản.

Những kết quả trên cho thấy, công tác QLNN trong phòng ngừa lừa đảo trên không gian mạng đã có chuyển biến theo hướng chủ động hơn. Tuy nhiên, số vụ việc còn phát sinh, thủ đoạn liên tục thay đổi và việc ứng dụng công nghệ mới của các đối tượng cho thấy vẫn còn những hạn chế, bất cập cần khắc phục.

(1) Công tác quản lý còn gặp khó khăn trước sự thay đổi nhanh của công nghệ và phương thức phạm tội. AI, deepfake và các

công cụ tạo nội dung giả, giả mạo giọng nói, hình ảnh, video rất khó nhận diện và phát hiện.

(2) Việc quản lý các nền tảng xuyên biên giới và thu thập dữ liệu phục vụ xác minh, xử lý còn nhiều khó khăn. Một số nền tảng chưa thực hiện đầy đủ trách nhiệm pháp lý tại Việt Nam; việc gỡ bỏ nội dung vi phạm, thu thập chứng cứ và phối hợp xử lý còn hạn chế.

(3) Cơ chế phối hợp giữa các chủ thể có liên quan chưa đáp ứng đầy đủ yêu cầu xử lý nhanh. Một vụ “bắt cóc online” thường liên quan đến dữ liệu viễn thông, giao dịch ngân hàng và hoạt động trên các nền tảng trực tuyến. Hiệu quả tuyên truyền cũng còn hạn chế. Nhiều nạn nhân dù đã từng tiếp cận thông tin cảnh báo nhưng vẫn bị thao túng khi rơi vào tình huống cụ thể.

(4) Vai trò của gia đình và cơ sở giáo dục trong phòng ngừa chưa phát huy hiệu quả.

4. Một số giải pháp

Thứ nhất, tiếp tục hoàn thiện cơ sở pháp lý và tăng cường quản lý các lĩnh vực có nguy cơ bị lợi dụng. Trong đó, cần tiếp tục rà soát, hoàn thiện và thực hiện hiệu quả các quy định về an ninh mạng, viễn thông, an toàn thông tin, tài chính - ngân hàng, bảo vệ dữ liệu cá nhân và hoạt động của các nền tảng số; chẳng hạn: tăng cường quản lý việc đăng ký, kích hoạt và sử dụng thuê bao viễn thông; quản lý việc mở, sử dụng tài khoản ngân hàng, ví điện tử; ngăn chặn tình trạng thuê, mượn, mua bán tài khoản phục vụ hoạt động phạm tội. Bên cạnh đó, cần tăng cường bảo vệ dữ liệu cá nhân, xử lý nghiêm hành vi thu thập, mua bán, chia sẻ trái phép thông tin cá nhân. Đây là nguồn dữ liệu có thể bị các đối tượng khai thác để xây dựng kịch bản lừa đảo, gây sức ép đối với nạn nhân và gia đình.

Chú trọng, nâng cao trách nhiệm của các nền tảng mạng xã hội, ứng dụng OTT và doanh nghiệp cung cấp dịch vụ trên môi trường mạng trong xử lý tài khoản, nội dung vi phạm và cung cấp thông tin phục vụ xác minh. Cùng với hoàn thiện pháp luật, cần xác

định rõ trách nhiệm của từng cơ quan, tổ chức, tăng cường kiểm tra, giám sát và tổ chức thực hiện, qua đó, kịp thời khắc phục những sơ hở trong quản lý mà các đối tượng có thể lợi dụng.

Thứ hai, nâng cao năng lực công nghệ và chuyên môn của lực lượng trực tiếp thực hiện nhiệm vụ. Trong đó, tiếp tục đầu tư, nâng cấp hạ tầng công nghệ thông tin, viễn thông và các hệ thống kỹ thuật phục vụ truy vết số, giám định dữ liệu điện tử, phân tích giao dịch và dòng tiền bất thường. Đồng thời, hỗ trợ xác định phương tiện liên lạc, tài khoản và các dấu vết điện tử liên quan đến hành vi phạm tội.

Bên cạnh đó, cần tăng cường đào tạo, tập huấn cho cán bộ trực tiếp thực hiện nhiệm vụ về thu thập, bảo quản, phân tích chứng cứ điện tử, dữ liệu cuộc gọi, địa chỉ IP, thông tin giao dịch và nội dung số giả mạo. Đặc biệt, chú trọng kỹ năng nhận diện, xử lý hình ảnh, âm thanh, video được tạo hoặc chỉnh sửa bằng AI, deepfake. Việc kết hợp này sẽ giúp lực lượng chức năng chủ động hơn trong phát hiện, xác minh và xử lý các thủ đoạn phạm tội mới.

Thứ ba, hoàn thiện cơ chế phối hợp liên ngành và nâng cao khả năng phản ứng nhanh. “Bắt cóc online” là loại hành vi có liên quan đồng thời đến nhiều chủ thể, trong đó cơ quan Công an, doanh nghiệp viễn thông, tổ chức tín dụng, cơ sở giáo dục và chính quyền địa phương đều có vai trò nhất định trong phát hiện, ngăn chặn và xử lý vụ việc. Vì vậy, cần tiếp tục hoàn thiện cơ chế phối hợp liên ngành theo hướng rõ đầu mối, nhanh chóng và đồng bộ; xây dựng cơ chế phản ứng nhanh, hướng tới phong tỏa kịp thời tài khoản nhận tiền và cung cấp nhanh dữ liệu thuê bao, cuộc gọi, giao dịch phục vụ xác minh, xử lý. Bên cạnh đó, cần duy trì việc chia sẻ thông tin về phương thức, thủ đoạn mới giữa các cơ quan, đơn vị. Những kịch bản lừa đảo mới phát hiện cần được cập nhật, phổ biến kịp thời để phục vụ cảnh báo, nhận diện và phòng ngừa. Việc thiết lập cơ chế liên hệ nhanh khi học sinh, sinh viên mất

liên lạc, rời nơi ở hoặc có biểu hiện bất thường sẽ góp phần rút ngắn thời gian phát hiện và can thiệp.

Thứ tư, đổi mới công tác tuyên truyền, giáo dục theo hướng hình thành kỹ năng ứng phó. Tài liệu đã đề xuất xây dựng hoạt động tuyên truyền chuyên biệt về phòng, chống “bắt cóc online”, trong đó nhấn mạnh nguyên tắc cơ quan Công an, Viện kiểm sát, Tòa án không làm việc với người dân theo phương thức yêu cầu chuyển tiền qua tài khoản ngân hàng; đồng thời, tăng cường sử dụng các kênh như mạng xã hội, báo chí, tin nhắn SMS và hệ thống truyền thanh cơ sở để phổ biến thông tin cảnh báo. Bên cạnh cung cấp thông tin, cần hướng dẫn người dân cách xử lý khi nhận cuộc gọi giả danh cơ quan nhà nước, bị yêu cầu giữ bí mật, rời khỏi nơi ở, cung cấp thông tin tài khoản hoặc chuyển tiền. Đối với học sinh, sinh viên, nội dung tuyên truyền cần được thiết kế phù hợp với đặc điểm tâm lý và thói quen sử dụng mạng xã hội của nhóm này. Có thể chú trọng các tình huống giả định, hướng dẫn kỹ năng kiểm chứng thông tin, cách liên hệ với gia đình, nhà trường hoặc cơ quan chức năng khi xuất hiện dấu hiệu nghi vấn. Việc phối hợp với ngành giáo dục để đưa nội dung cảnh báo và kỹ năng phòng tránh vào các hoạt động ngoại khóa cũng cần tiếp tục được tăng cường.

Thứ năm, tăng cường hợp tác quốc tế trong phòng, chống tội phạm mạng. Tính chất xuyên biên giới làm gia tăng khó khăn trong phòng, chống “bắt cóc online”. Do đó, cần tiếp tục tăng cường hợp tác quốc tế trong trao đổi thông tin, thu thập dữ liệu điện tử, xác minh và truy tìm đối tượng, cũng như thu hồi tài sản có liên quan đến hành vi phạm tội. Công ước của Liên Hợp quốc về chống tội phạm mạng tạo cơ sở cho tăng cường hợp tác đa phương trong những nội dung như thu thập dữ liệu điện tử xuyên biên giới, dẫn độ và truy thu tài sản. Bên cạnh đó, cần tiếp tục duy trì và tăng cường các kênh trao đổi thông tin với Interpol, ASEANAPOL và các quốc gia trong khu vực, nhất là những quốc gia được

xác định có liên quan đến hoạt động của các nhóm tội phạm lừa đảo trên không gian mạng. Đồng thời, thúc đẩy các cơ chế tương trợ tư pháp song phương và đa phương nhằm tạo điều kiện thuận lợi hơn cho việc thu thập chứng cứ, truy tìm đối tượng và xử lý các vụ việc có yếu tố nước ngoài.

5. Kết luận

Sự phát triển nhanh của công nghệ, tính chất xuyên biên giới, hạn chế trong phối hợp và kỹ năng tự phòng vệ của người dân vẫn đặt ra nhiều khó khăn. Do đó, nâng cao vai trò của QLNN trong phòng ngừa lừa đảo chiếm đoạt tài sản bằng thủ đoạn “bắt cóc online” cần được thực hiện theo hướng chủ động, đồng bộ và thích ứng với sự thay đổi của công nghệ. Trọng tâm là hoàn thiện cơ chế quản lý các lĩnh vực có nguy cơ bị lợi dụng, nâng cao năng lực công nghệ và chuyên môn của lực lượng chức năng, tăng cường phối hợp liên ngành, đổi mới công tác tuyên truyền theo hướng hình thành kỹ năng ứng phó và đẩy mạnh hợp tác quốc tế. Qua đó, từng bước nâng cao khả năng phòng ngừa từ sớm, phát hiện kịp thời và hạn chế thiệt hại do loại tội phạm này gây ra □

Tài liệu tham khảo:

- Chính phủ (2025). *Nghị định số 02/2025/NĐ-CP ngày 18/02/2025 quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Công an*.
- Công an TP. Hồ Chí Minh (2025). *Báo cáo tình hình tội phạm bắt cóc online năm 2025*.
- Nguyễn Minh (22/01/2026). Thoát chiêu trò “bắt cóc online”. *Báo Tuổi trẻ*. <https://tuoitre.vn/thoat-chieu-tro-bat-coc-online-20260122084019118.htm>
- Thủ tướng Chính phủ (2025). *Công điện số 29/CD-TTg ngày 03/4/2025 về việc đẩy mạnh công tác phòng ngừa, xử lý hoạt động sử dụng công nghệ cao trên không gian mạng để lừa đảo chiếm đoạt tài sản*.
- United Nations (2024). *Công ước của Liên Hợp quốc về chống tội phạm mạng (Công ước Hà Nội), mở ký ngày 25/10/2025*.