

HÌNH PHẠT ĐỐI VỚI TỘI LỪA ĐẢO CHIẾM ĐOẠT TÀI SẢN BẰNG THỦ ĐOẠN KHÔNG CHẾ NGƯỜI QUA MẠNG THEO PHÁP LUẬT HÌNH SỰ VIỆT NAM

SV. KHỔNG NGUYỄN MINH TRÂM
SV. NGUYỄN THỊ ANH THƯ
SV. NGUYỄN HUỖNH MINH THƯ
SV. TRẦN TUYẾT NHÌ
HÀ THỊ HỒNG THẨM
LÊ VĨNH SƠN

Trường Đại học Công thương Thành phố Hồ Chí Minh

Nhận bài ngày 15/8/2026. Sửa chữa xong 15/9/2026. Duyệt đăng 10/10/2026.

Abstract

The proliferation of generative artificial intelligence and online platforms has facilitated scams involving psychological manipulation, particularly the impersonation of judicial authorities and “online kidnapping” schemes used to coerce victims into transferring property. This article examines the application of Article 174 of Vietnam’s 2015 Penal Code, as amended in 2017, including its penalty framework and qualifying circumstances, and distinguishes fraudulent appropriation from the offenses regulated under Articles 170 and 290. Drawing on international standards and Singapore’s experience, the study recommends clarifying offense-classification guidelines, accelerating the freezing of illicit financial flows, strengthening asset recovery mechanisms, and enhancing cross-border cooperation. It also emphasizes that technologies such as deepfakes and voice cloning constitute means of committing an offense and should not be equated with its statutory elements.

Keywords: Article 174 of the Penal Code, deepfake, fraudulent appropriation of property, online kidnapping, online psychological coercion, penalties.

1. Đặt vấn đề

Không gian mạng đã trở thành môi trường thiết yếu của đời sống kinh tế - xã hội nhưng đồng thời cũng tạo điều kiện cho các hành vi lừa đảo thay đổi nhanh về quy mô, cách thức tiếp cận và mức độ che giấu danh tính. Trong nhóm hành vi xâm phạm sở hữu, thủ đoạn giả danh cơ quan nhà nước, dựng tình huống khẩn cấp, giả mạo hình ảnh hoặc giọng nói và cô lập nạn nhân đang đặt ra nhiều vấn đề mới cho hoạt động định tội danh và quyết định hình phạt. Thực tiễn cho thấy đã xuất hiện các vụ “bắt cóc online” mà đối tượng từ xa thao túng nạn nhân, yêu cầu nạn nhân tự cách ly, đồng thời gây sức ép để gia đình chuyển tiền; có vụ gia đình đã chuyển gần 3 tỷ đồng trước khi nạn nhân được cơ quan công an giải cứu (Công an Thành phố Hồ Chí Minh, 2025b). Đặc điểm đáng chú ý của dạng hành vi này là sự kết hợp giữa gian dối và tác động tâm lý cường độ cao. Người phạm tội có thể giả danh Công an, Viện kiểm sát, Tòa án hoặc cơ quan tài chính; đưa ra thông tin nạn nhân liên quan đến ma túy, rửa tiền, tài khoản bất hợp pháp; yêu cầu giữ bí mật, duy trì liên lạc liên tục và làm theo chỉ dẫn. Ở một số trường hợp, công nghệ Deepfake hoặc công nghệ tổng hợp giọng nói có thể được sử dụng để làm tăng mức độ thuyết phục của kịch bản lừa đảo. Bộ Công an trong năm 2026 tiếp tục cảnh báo việc lợi dụng AI và Deepfake để tạo dựng, phát tán thông tin giả, cho thấy yêu cầu cấp thiết phải hoàn thiện công cụ pháp lý và kỹ thuật phòng ngừa (Bộ Công an, 2026).

Về phương diện luật hình sự, khó khăn không nằm ở việc “có sử dụng công nghệ hay không” mà ở

Email: sonlv@huit.edu.vn

việc xác định đúng bản chất hành vi khách quan và cơ chế chiếm đoạt. Nếu tài sản được giao do nạn nhân tin vào thông tin gian dối thì Điều 174 Bộ luật Hình sự là điểm xuất phát quan trọng để xem xét. Nếu việc giao tài sản chủ yếu xuất phát từ sự đe dọa nhằm uy hiếp tinh thần thì cần đặt vấn đề về Điều 170 Bộ luật Hình sự. Trong khi đó, Điều 290 Bộ luật Hình sự hướng tới nhóm hành vi chiếm đoạt được thực hiện thông qua những phương thức gần trực tiếp với mạng máy tính, mạng viễn thông hoặc phương tiện điện tử theo cấu trúc điều luật. Do đó, việc định tội phải dựa trên các dấu hiệu pháp lý cụ thể, không thể chỉ dựa trên phương tiện mà người phạm tội sử dụng.

Bài viết sử dụng phương pháp phân tích quy phạm, hệ thống hóa và so sánh pháp luật. Nguồn nghiên cứu gồm Bộ luật Hình sự Việt Nam, một số tài liệu khoa học luật hình sự, thông tin chính thức của cơ quan nhà nước và các văn bản quốc tế có liên quan. Đối với các thông tin thực tiễn chưa có số liệu thống kê toàn quốc được công bố đầy đủ, bài viết chỉ sử dụng các vụ việc hoặc cảnh báo đã có nguồn công khai, không suy rộng thành tỷ lệ chung. Cách tiếp cận này nhằm bảo đảm các nhận định thực tiễn có khả năng kiểm chứng và hạn chế việc sử dụng số liệu không truy xuất được nguồn gốc.

2. Nội dung nghiên cứu

2.1. Bản chất pháp lý của thủ đoạn khống chế tâm lý qua mạng

Thuật ngữ “khống chế người qua mạng” hoặc “bắt cóc online” hiện chủ yếu được sử dụng trong truyền thông và thực tiễn phòng, chống tội phạm để mô tả một kịch bản thao túng từ xa; đây chưa phải là một thuật ngữ định tội độc lập trong Bộ luật Hình sự. Vì vậy, khi sử dụng thuật ngữ này trong nghiên cứu khoa học pháp lý cần hiểu đó là cách mô tả phương thức thực hiện hành vi, còn trách nhiệm hình sự phải được xác định theo các cấu thành tội phạm cụ thể.

Về mặt cơ chế, có thể nhận diện ba nhóm hành vi thường nối tiếp nhau: 1) Người phạm tội thu thập dữ liệu và lựa chọn mục tiêu, khai thác thông tin cá nhân, quan hệ gia đình, đặc điểm tâm lý hoặc thói quen sử dụng mạng; 2) Người phạm tội thiết lập bối cảnh gian dối: giả danh người có thẩm quyền, dựng văn bản, hình ảnh hoặc cuộc gọi giả, tạo cảm giác về một vụ án hoặc sự kiện khẩn cấp; 3) Người phạm tội duy trì áp lực tâm lý, yêu cầu nạn nhân liên hệ với người khác, chuyển nơi ở, bật camera liên tục hoặc thực hiện các giao dịch tài chính theo chỉ dẫn. Thực tế các vụ việc đã công bố cho thấy việc cô lập nạn nhân và gây sức ép đối với người thân là đặc trưng thường gặp của “bắt cóc online” (Công an Thành phố Hồ Chí Minh, 2025b; 2025a).

Điểm pháp lý then chốt là phải xác định vì sao nạn nhân chuyển giao tài sản. Trong lừa đảo chiếm đoạt tài sản, hành vi gian dối phải có quan hệ nhân quả với việc người bị hại giao tài sản hoặc tạo điều kiện để người phạm tội chiếm đoạt. Cũng cần phân biệt thao túng con người với can thiệp kỹ thuật vào hệ thống. Công ước Budapest về tội phạm mạng quy định “computer-related fraud” ở Điều 8 chủ yếu gắn với việc nhập, thay đổi, xóa, ngăn chặn dữ liệu máy tính hoặc can thiệp vào hoạt động của hệ thống để gây thiệt hại tài sản (Council of Europe, 2001). Báo cáo giải thích của Công ước cũng cho thấy nếu pháp luật quốc gia đã có tội danh truyền thống bao quát hành vi thì không nhất thiết phải tạo ra tội danh mới chỉ vì có yếu tố công nghệ (Council of Europe, 2001). Đây là gợi ý quan trọng cho việc xử lý trường hợp tại Việt Nam, cần nhìn vào cơ chế chiếm đoạt, không đồng nhất “thực hiện qua mạng” với “tội phạm máy tính”.

2.2. Hệ thống hình phạt tại Điều 174 Bộ luật Hình sự và khả năng áp dụng

2.2.1. Khung hình phạt cơ bản

Khoản 1 Điều 174 Bộ luật Hình sự quy định hình phạt cải tạo không giam giữ đến 03 năm hoặc phạt tù từ 06 tháng đến 03 năm đối với hành vi lừa đảo chiếm đoạt tài sản đạt ngưỡng luật định; đồng thời cho phép xử lý một số trường hợp giá trị tài sản dưới ngưỡng khi có các điều kiện bổ sung do điều luật quy định (Quốc hội, 2017). Cấu trúc này phản ánh nguyên tắc phân hóa trách nhiệm hình sự theo giá trị tài sản, nhân thân và mức độ tác động xã hội.

Đối với các vụ lừa đảo qua mạng, không nên mặc định rằng khoản 1 “ít được áp dụng” nếu không

có thống kê tư pháp đáng tin cậy. Việc áp dụng khung nào phụ thuộc vào giá trị tài sản, tình tiết định khung và chứng cứ của từng vụ án. Vì vậy, bài viết không sử dụng nhận định định lượng về tần suất áp dụng các khoản khi chưa có cơ sở dữ liệu bản án đủ lớn.

2.2.2. Khung tăng nặng tại khoản 2 Điều 174

Khoản 2 Điều 174 quy định mức phạt tù từ 02 năm đến 07 năm khi có các tình tiết định khung tăng nặng, trong đó một số tình tiết có khả năng xuất hiện trong lừa đảo trực tuyến như “có tổ chức”, “có tính chất chuyên nghiệp”, “lợi dụng danh nghĩa cơ quan, tổ chức” và “dùng thủ đoạn xảo quyệt” (Quốc hội, 2017). Việc áp dụng từng tình tiết phải dựa trên nội hàm pháp lý đã được pháp luật và thực tiễn xét xử thừa nhận, không thể chỉ suy ra từ việc hành vi có sử dụng AI hoặc được thực hiện qua Internet.

Tình tiết “có tổ chức” cần được xem xét khi có sự cấu kết chặt chẽ, phân công vai trò giữa nhiều người theo các dấu hiệu của đồng phạm có tổ chức. Trong các đường dây lừa đảo xuyên biên giới, có thể tồn tại các nhóm phụ trách dữ liệu, kịch bản, liên lạc, nhận tiền và tẩu tán tài sản. Tuy nhiên, việc mô tả một đường dây như “doanh nghiệp tội phạm” chỉ có giá trị minh họa; kết luận pháp lý vẫn phải dựa trên chứng cứ về sự cấu kết và phân công cụ thể.

Đối với tình tiết “có tính chất chuyên nghiệp” cần áp dụng trên cơ sở hướng dẫn mới tại Nghị quyết số 04/2025/NQ-HĐTP ngày 30/9/2025 của Hội đồng Thẩm phán Tòa án nhân dân tối cao. Khoản 2 Điều 4 Nghị quyết xác định “phạm tội có tính chất chuyên nghiệp” là trường hợp người phạm tội thực hiện hành vi phạm tội từ 05 lần trở lên (không phân biệt đã bị truy cứu trách nhiệm hình sự hay chưa bị truy cứu trách nhiệm hình sự, với điều kiện chưa hết thời hiệu truy cứu trách nhiệm hình sự hoặc chưa được xóa án tích) và lấy khoản lợi bất chính thu được từ việc phạm tội làm nguồn thu nhập (Hội đồng Thẩm phán Tòa án nhân dân tối cao, 2025). Mặc dù quy định này được đặt trong phần hướng dẫn tình tiết tăng nặng trách nhiệm hình sự tại điểm b khoản 1 Điều 52 Bộ luật Hình sự, khoản 3 Điều 5 Nghị quyết đồng thời ghi nhận, tùy từng trường hợp cụ thể, người phạm tội từ 05 lần trở lên có thể bị áp dụng tình tiết định khung “có tính chất chuyên nghiệp”. Vì vậy, khi xem xét điểm b khoản 2 Điều 174 Bộ luật Hình sự đối với hành vi lừa đảo chiếm đoạt tài sản qua mạng, cơ quan tiến hành tố tụng cần chứng minh đồng thời tính lặp lại của hành vi theo ngưỡng nêu trên và việc người phạm tội lấy khoản lợi bất chính từ hoạt động phạm tội làm nguồn thu nhập; không thể chỉ dựa vào số lượng cuộc gọi, số tài khoản sử dụng hoặc tính chất có tổ chức của đường dây để mặc nhiên xác định tình tiết này.

Tình tiết “lợi dụng danh nghĩa cơ quan, tổ chức” có ý nghĩa đặc biệt đối với thủ đoạn giả danh Công an, Viện kiểm sát, Tòa án, ngân hàng hoặc cơ quan nhà nước để tạo niềm tin và uy lực giả. Khi chứng minh được người phạm tội đã chủ động khai thác danh nghĩa của cơ quan, tổ chức như một phương tiện tạo ra sự nhầm tưởng của nạn nhân, đây là căn cứ cần được xem xét theo đúng cấu trúc Điều 174 (Quốc hội, 2017).

Tình tiết “dùng thủ đoạn xảo quyệt” cần được áp dụng thận trọng. Deepfake, Voice Cloning, giả mạo số điện thoại, giao diện, văn bản điện tử hoặc tin nhắn thương hiệu có thể làm cho thủ đoạn trở nên khó phát hiện; tuy nhiên công nghệ tự thân không đương nhiên đồng nghĩa với “xảo quyệt”. Cơ quan tiến hành tố tụng cần chứng minh mức độ tinh vi, khả năng che giấu, gây khó khăn đáng kể cho việc nhận biết hoặc đối phó của người bị hại và cho hoạt động phát hiện tội phạm. Cách tiếp cận này tránh biến một tình tiết định khung thành “nhân công nghệ” áp dụng tự động.

2.2.3. Khoản 3, Khoản 4 và yêu cầu lượng hình tương xứng

Khoản 3 và khoản 4 Điều 174 thiết lập các khung hình phạt nghiêm khắc hơn, chủ yếu dựa vào giá trị tài sản và một số tình tiết đặc biệt do điều luật quy định; mức cao nhất có thể đến tù chung thân (Quốc hội, 2017). Việc Bộ luật Hình sự không còn quy định tử hình đối với tội lừa đảo chiếm đoạt tài sản thể hiện xu hướng thu hẹp hình phạt tử hình trong chính sách hình sự. Tuy vậy, không nên diễn đạt rằng tù chung thân “loại bỏ vĩnh viễn” người phạm tội khỏi xã hội, bởi pháp luật thi hành án hình sự vẫn có cơ chế giảm thời hạn chấp hành hình phạt và các chế định khác khi đủ điều kiện. Cách diễn đạt phù hợp hơn là khung hình phạt cao bảo đảm khả năng xử lý nghiêm các hành vi gây thiệt hại đặc biệt lớn.

2.2.4. Hình phạt bổ sung và vấn đề thu hồi tài sản

Khoản 5 Điều 174 cho phép áp dụng phạt tiền, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định và tịch thu một phần hoặc toàn bộ tài sản theo điều kiện của luật (Quốc hội, 2017). Đối với tội phạm vụ lợi, hiệu quả của chế tài kinh tế phụ thuộc rất lớn vào khả năng truy nguyên, phong tỏa và thu hồi tài sản. Nếu tài sản đã nhanh chóng được chia nhỏ, chuyển qua nhiều tài khoản hoặc chuyển hóa thành tài sản số, việc tuyên hình phạt tiền hoặc tịch thu sẽ khó đạt hiệu quả nếu biện pháp tố tụng bảo toàn tài sản triển khai chậm. Vì vậy, cần tách biệt hai vấn đề: 1) Quyết định hình phạt bổ sung của Tòa án; 2) Khả năng bảo đảm thi hành thông qua các biện pháp tố tụng, truy vết tài sản và phối hợp với tổ chức tín dụng. Nhận định rằng hình phạt bổ sung “gần như bị tê liệt” chỉ nên đưa ra khi có dữ liệu thi hành án đủ rộng. Trong phạm vi bài viết, có thể khẳng định thận trọng hơn rằng tốc độ luân chuyển dòng tiền trên môi trường số làm tăng đáng kể nguy cơ tài sản bị tẩu tán trước khi cơ quan có thẩm quyền kịp áp dụng biện pháp bảo toàn.

2.3. Các vấn đề pháp lý nổi bật trong định tội danh

2.3.1. Phân định Điều 174 và Điều 290 Bộ luật Hình sự

Một sai lệch dễ xảy ra trong nhận thức là cho rằng cứ sử dụng mạng máy tính hoặc mạng viễn thông để chiếm đoạt tài sản thì phải áp dụng Điều 290 Bộ luật Hình sự. Cách hiểu này không phù hợp với yêu cầu phân tích cấu thành tội phạm. Cần xác định hành vi cụ thể thuộc nhóm phương thức mà Điều 290 mô tả hay chỉ là việc sử dụng Internet như phương tiện liên lạc để thực hiện gian dối đối với con người.

Trong trường hợp đối tượng gọi điện, nhắn tin, gửi hình ảnh hoặc video giả để làm nạn nhân tin vào một sự kiện không có thật và nạn nhân tự thực hiện chuyển tiền, dấu hiệu gian dối đối với con người có thể đưa vụ việc về phạm vi Điều 174. Ngược lại, nếu người phạm tội can thiệp trái phép vào hệ thống dữ liệu hoặc phương tiện điện tử theo phương thức cấu thành Điều 290, việc định tội phải xem xét điều luật chuyên biệt đó. Công ước Budapest cũng phân biệt hành vi gian lận liên quan máy tính dựa trên sự thao tác dữ liệu hoặc hệ thống (Council of Europe, 2001), qua đó củng cố yêu cầu phân định theo cơ chế gây thiệt hại, không chỉ theo “không gian” xảy ra hành vi.

2.3.2. Phân định Điều 174 và Điều 170 Bộ luật Hình sự

Ranh giới giữa lừa đảo và cưỡng đoạt trở nên phức tạp khi người phạm tội vừa dựng thông tin giả vừa đưa ra lời đe dọa. Ví dụ, đối tượng dựng video giả cho thấy người thân đang bị bắt giữ và yêu cầu chuyển tiền hoặc giả danh cơ quan công quyền rồi đe dọa bắt giữ nếu nạn nhân không “chứng minh tài sản”. Trong các trường hợp này cần phân tích trạng thái nhận thức và động cơ trực tiếp dẫn đến việc giao tài sản.

Nếu nạn nhân chuyển tiền vì tin rằng thông tin gian dối là thật, chẳng hạn tin rằng người thân thực sự gặp nạn hoặc tin rằng việc chuyển tiền là yêu cầu hợp pháp của cơ quan chức năng thì yếu tố gian dối giữ vai trò trung tâm. Nếu nạn nhân biết hoặc không tin câu chuyện nhưng chuyển tiền để tránh một thiệt hại mà người phạm tội đe dọa sẽ gây ra, yếu tố uy hiếp tinh thần có thể là cơ sở xem xét tội cưỡng đoạt. Cách tiếp cận “nguyên nhân chi phối quyết định giao tài sản” giúp hạn chế việc định tội chỉ bằng cách đếm số lượng thủ đoạn được sử dụng.

2.3.3. Bổ sung tình tiết định khung riêng cho Deepfake và AI

Đề xuất này có ý nghĩa cảnh báo nhưng cần cân nhắc kỹ về kỹ thuật lập pháp. Công nghệ thay đổi rất nhanh; nếu liệt kê đích danh từng công nghệ, điều luật có nguy cơ nhanh chóng lạc hậu. Mặt khác, không phải mọi hành vi sử dụng AI đều nguy hiểm hơn một thủ đoạn gian dối truyền thống được chuẩn bị công phu.

Phương án hợp lý hơn là trước mắt ban hành hướng dẫn giải thích tiêu chí “thủ đoạn xảo quyệt” theo hướng trung lập về công nghệ, trong đó nêu các dấu hiệu như: khả năng giả mạo danh tính hoặc bằng chứng ở mức khó nhận biết; khả năng cá nhân hóa kịch bản dựa trên dữ liệu cá nhân; việc kết hợp nhiều lớp che giấu và thao túng; khả năng gây nhầm tưởng đặc biệt nghiêm trọng; hoặc làm tăng đáng kể khó khăn cho việc phát hiện, ngăn chặn. Deepfake và Voice Cloning có thể được dùng làm ví dụ, không nên là điều kiện duy nhất.

2.3.4. Thu hồi tài sản và “tốc độ” của phản ứng pháp lý

Trong lừa đảo trực tuyến, giá trị của biện pháp phong tỏa tài sản phụ thuộc rất lớn vào thời điểm. Dòng tiền có thể được chuyển qua nhiều tài khoản trong thời gian ngắn, sau đó đổi thành tài sản số hoặc chuyển ra nước ngoài. Điều này tạo ra khoảng cách giữa tốc độ giao dịch và tốc độ xử lý theo thủ tục truyền thống. Do đó, hoàn thiện cơ chế phối hợp tức thời giữa cơ quan điều tra và tổ chức tín dụng là một hướng cần ưu tiên.

Kinh nghiệm của Singapore cho thấy một hướng tiếp cận đáng tham khảo, Singapore trao quyền cho cảnh sát, trong những điều kiện luật định, ban hành restriction order yêu cầu ngân hàng tạm thời hạn chế một số giao dịch hoặc khả năng sử dụng tín dụng của người đang có nguy cơ chuyển tiền cho kẻ lừa đảo (Singapore, 2025). Cơ quan thực thi đã triển khai từ ngày 16/12/2024 xác định nghĩa vụ phòng ngừa của tổ chức tài chính và doanh nghiệp viễn thông đối với một số loại phishing scam; khi vi phạm nghĩa vụ có thể phát sinh cơ chế chi trả cho nạn nhân theo khuôn khổ này (Monetary Authority of Singapore, & Infocomm Media Development Authority, 2024).

2.4. Tham chiếu chuẩn mực quốc tế và kinh nghiệm nước ngoài

Công ước Budapest về tội phạm mạng là một nguồn tham chiếu quan trọng khi phân biệt tội phạm truyền thống được thực hiện qua môi trường số với hành vi trực tiếp xâm nhập, thao tác dữ liệu hoặc hệ thống. Điều 8 Công ước yêu cầu các quốc gia thành viên hình sự hóa việc cố ý gây thiệt hại tài sản cho người khác bằng việc nhập, thay đổi, xóa, ngăn chặn dữ liệu máy tính hoặc can thiệp vào chức năng hệ thống, với mục đích gian lận hoặc bất chính để thu lợi (Council of Europe, 2001). Nội dung này không cho phép suy luận rằng mọi hành vi “thao túng tâm lý qua phương tiện điện tử” phải cấu thành một tội độc lập hay đương nhiên bị tăng hình phạt 1,5-2 lần. Vì vậy, phần so sánh pháp luật của bản thảo được chỉnh lại để tránh gán cho EU hoặc Công ước Budapest những quy định không có trong nguồn.

Ở Liên minh châu Âu, Directive (EU) 2019/713 về chống gian lận và làm giả phương tiện thanh toán không dùng tiền mặt yêu cầu hình sự hóa một số hành vi gian lận liên quan hệ thống thông tin, trong đó nhấn mạnh việc thực hiện hoặc gây ra chuyển tiền bằng cách can thiệp hệ thống hoặc dữ liệu trái phép (European Parliament and Council of the European Union, 2019). Cách tiếp cận này tiếp tục cho thấy yếu tố công nghệ được gắn với phương thức can thiệp cụ thể, thay vì chỉ với việc giao tiếp trực tuyến.

Kinh nghiệm của Singapore lại đáng chú ý ở góc độ phòng ngừa thiệt hại và phân bổ trách nhiệm trong hệ sinh thái số. Cho phép can thiệp tạm thời để ngăn nạn nhân tiếp tục thực hiện giao dịch trong một số trường hợp; đặt ra những nghĩa vụ cụ thể đối với tổ chức tài chính và doanh nghiệp viễn thông trong phạm vi phishing scam (Singapore, 2025; Monetary Authority of Singapore, & Infocomm Media Development Authority, 2024). Đối với Việt Nam, giá trị tham khảo chính nằm ở cơ chế phản ứng nhanh, chia sẻ dữ liệu và bảo vệ nạn nhân chứ không phải sao chép nguyên mẫu chế tài.

3. Kết luận và kiến nghị

3.1. Kết luận

Dù là phương thức phạm tội mới, thủ đoạn khống chế tâm lý qua mạng không nhất thiết đòi hỏi tội danh mới. Trọng tâm định tội vẫn là xác định hành vi khách quan, nhận thức của nạn nhân, mối quan hệ nhân quả khi giao tài sản và phương thức can thiệp hệ thống để áp dụng đúng Điều 174, Điều 170 hoặc Điều 290 Bộ luật Hình sự. Dù Điều 174 Bộ luật Hình sự đã phân hóa tốt hình phạt theo thiệt hại và mức độ nguy hiểm, thách thức thực tiễn nằm ở việc giải thích thống nhất các tình tiết định khung và bảo đảm hiệu quả thu hồi tài sản. Đối với AI, Deepfake hay Voice Cloning cần tiếp cận theo hướng trung lập về công nghệ: đánh giá tính chất xảo quyệt và nguy hiểm thực tế thay vì tự động tăng nặng hình phạt chỉ vì có yếu tố công nghệ mới.

3.2. Kiến nghị

Hội đồng Thẩm phán Tòa án nhân dân tối cao cần sớm ban hành hướng dẫn áp dụng thống nhất

đối với hành vi kết hợp giữa gian dối số và uy hiếp tinh thần. Cần phân định Điều 174 với Điều 170 Bộ luật Hình sự dựa trên nguyên nhân chi phối việc giao tài sản; đồng thời phân biệt với Điều 290 Bộ luật Hình sự dựa trên việc tác động vào ý chí con người hay trực tiếp can thiệp dữ liệu, hệ thống.

Hướng dẫn rõ nội hàm tình tiết “dùng thủ đoạn xảo quyệt” theo hướng trung lập về công nghệ. Các công cụ như Deepfake hay Voice Cloning chỉ là ví dụ minh họa; việc áp dụng phải căn cứ vào mức độ che giấu, khả năng gây nhầm tưởng và tính chất phức tạp thực tế của hành vi, tránh gán nhãn công nghệ một cách máy móc.

Thiết lập cơ chế phản ứng nhanh đối với dòng tiền lừa đảo qua kênh phối hợp 24/7 giữa cơ quan Công an, Ngân hàng Nhà nước và các tổ chức tín dụng để phong tỏa, tạm dừng giao dịch khẩn cấp. Cơ chế này phải đi kèm tiêu chí kích hoạt chặt chẽ, thời hạn ngắn và quyền khiếu nại để tránh lạm quyền, xâm phạm quyền tài sản.

Nâng cao năng lực truy vết dòng tiền qua tài khoản trung gian, ví điện tử, tài sản mã hóa và xử lý chứng cứ điện tử cho cán bộ tố tụng. Mục tiêu hình sự cần hướng mạnh vào việc triệt tiêu lợi ích kinh tế và tối đa hóa tỷ lệ thu hồi tài sản cho nạn nhân.

Mở rộng hợp tác quốc tế và tương trợ tư pháp nhằm kịp thời phong tỏa tài sản, thu thập chứng cứ điện tử xuyên biên giới. Cần chuẩn hóa quy trình tiếp nhận thông tin khẩn cấp và tham chiếu các chuẩn mực quốc tế như Công ước Budapest để nâng cao hiệu quả xử lý tội phạm có yếu tố nước ngoài.

Nâng cao tính chuẩn xác trong nghiên cứu khoa học pháp lý về tội phạm mạng. Các thông tin về số vụ, thiệt hại hay thực tiễn xét xử cần dựa trên nguồn dữ liệu, bản án có thể kiểm chứng; tránh suy rộng các nhận định chưa có số liệu chính thức thành kết luận thực tiễn chung.

Chú thích

(*) Bài báo là kết quả từ Hợp đồng thực hiện đề tài nghiên cứu khoa học số 498/HĐ-DCT ngày 15/12/2026 của Trường Đại học Công thương Thành phố Hồ Chí Minh.

Tài liệu tham khảo

Bộ Công an (2026). *Xây dựng chế tài đủ mạnh để ngăn chặn tình trạng sử dụng AI, Deepfake để lan truyền tin giả* [Tham luận]. Tọa đàm chính sách về các dự thảo văn bản quy phạm pháp luật năm 2026.

Công an Thành phố Hồ Chí Minh (2025a). *Phòng Cảnh sát hình sự giải cứu nạn nhân bị “bắt cóc online”*.
https://congan.hochiminhcity.gov.vn/wps/portal/Home/trang-chu/loi-dung-chi-tiet/anninhtrattu/tin+tuc+an+ninh+trat+tu/phong+cshs+giai+cuu+nan+nhan+bi+bat+coc?WCM_Page.CATP_Menu_TinTucChiTiet_Related=3, ngày 11/6/2025.

Công an Thành phố Hồ Chí Minh (2025b). *Công an Thành phố Hồ Chí Minh giải cứu nam sinh viên bị “bắt cóc online”, gia đình bị lừa gần 3 tỷ đồng*.
https://congan.hochiminhcity.gov.vn/wps/portal/Home/trang-chu/loi-dung-chi-tiet/anninhtrattu/tin+tuc+an+ninh+trat+tu/catphcm+giai+cuu+nam+sinh+vien+bi+bat+coc+online%2C+gia+ding+bi+lua+gan+3+ty+dong?WCM_Page.CATP_Menu_TinTucChiTiet_R, ngày 22/8/2025.

Council of Europe. (2001). *Convention on cybercrime* (ETS No. 185) and *Explanatory report*.

European Parliament and Council of the European Union. (2019). Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA. *Official Journal of the European Union*, L 123, 18-29.

Hội đồng Thẩm phán Tòa án nhân dân tối cao (2025). *Nghị quyết số 04/2025/NQ-HĐTP ngày 30/9/2025 hướng dẫn áp dụng các tình tiết giảm nhẹ trách nhiệm hình sự, các tình tiết tăng nặng trách nhiệm hình sự quy định tại Điều 51 và Điều 52 Bộ luật Hình sự*.

Monetary Authority of Singapore, & Infocomm Media Development Authority. (2024). *Shared responsibility framework for phishing scams*.

Quốc hội (2017). *Luật Sửa đổi, bổ sung một số điều của Bộ Luật hình sự số 100/2015/QH13*. Luật số 12/2017/QH14, ngày 20/6/2017.

Singapore (2025). *Protection from Scams Act 2025* (Act No. 1 of 2025).