Tội phạm buôn lậu trên không gian mạng và một số kiến nghị nâng cao hiệu quả phòng, chống

15:07 05/02/2026

(Pháp lý). Trong bối cảnh chuyển đổi số mạnh mẽ, tội phạm buôn lậu đã và đang lợi dụng không gian mạng để thực hiện hành vi phạm tội với phương thức và thủ đoạn ngày càng tinh vi. Bài viết này phân tích thực trạng, những khó khăn trong công tác phòng ngừa và đề xuất các giải pháp nhằm nâng cao hiệu quả đấu tranh phòng, chống tội phạm buôn lậu trên không gian mạng tại Việt Nam.

1. Thực trạng tội phạm buôn lậu trên không gian mạng

Sự phát triển của công nghệ thông tin và thương mại điện tử đã mang đến nhiều tích cực cho phát triển kinh tế xã hội. Tuy nhiên mặt trái của vấn đề đã "tạo điều kiện thuận lợi" cho các đối tượng buôn lậu hoạt động trên không gian mạng. Theo báo cáo của Ban Chỉ đạo 389 quốc gia, trong năm 2023, các lực lượng chức năng đã xử lý hơn 14.600 vụ vi phạm buôn lậu, gần 130.000 vụ gian lận thương mại và hơn 5.400 vụ sản xuất, mua bán hàng giả. Trong 9 tháng đầu năm 2024, các lực lượng chức năng đã phát hiện, bắt giữ và xử lý 39.017 vụ vi phạm liên quan đến buôn lậu, gian lận thương mại và hàng giả, giảm 32,7% so với cùng kỳ năm 2023. Trong đó, buôn bán, vận chuyển trái phép hàng cấm, hàng lậu là 6.118 vụ (giảm 18,3%); gian lận thương mại, gian lận thuế là 31.473 vụ (giảm 21,7%); hàng giả, hàng vi phạm quyền sở hữu trí tuệ là 1.426 vụ (tăng 13,7%). Đặc biệt, hoạt động buôn lậu qua hình thức thương mại điện tử ngày càng phổ biến, với các đối tượng lợi dụng nền tảng trực tuyến để thực hiện hành vi vi phạm.

2. Khó khăn trong công tác phòng, chống

Thực trạng trên xuất phát từ một số khó khăn, hạn chế của các lực lượng chức năng trong công tác phòng chống tội phạm trên không gian mạng nói chung và công tác phòng, chống tội phạm buôn lậu nói riêng. Cụ thể là:

Tính ẩn danh trên mạng

Các đối tượng thường xuyên thay đổi tài khoản, sử dụng danh tính giả, công nghệ VPN để che giấu địa điểm thật. Ẩn danh trên mạng là một trong những thủ đoạn phổ biến và ngày càng tinh vi của tội phạm buôn lậu trong giai đoạn hiện nay. Việc lợi dụng tính ẩn danh, khó truy vết và thiếu kiểm soát chặt chẽ trên không gian mạng giúp các đối tượng dễ dàng thực hiện hành vi phạm tội mà không bị phát hiện ngay lập tức. Một số thủ đoạn ẩn danh phổ biến như các đối tượng tạo nhiều tài khoản trên mạng xã hội (Facebook, TikTok, Zalo...) với danh tính giả, ảnh đại diện giả, số điện thoại đăng ký không chính chủ, khi bị nghi ngờ hoặc truy vết, chúng có thể dễ dàng xóa tài khoản, đổi tên, chuyển nền tảng hoặc lập tài khoản mới.

Các đối tượng cũng có thể ẩn danh bằng thủ đoạn giao dịch qua nền tảng mã hóa có tính bảo mật cao như Telegram, Signal, WhatsApp, Viber, cho phép mã hóa đầu cuối, không lưu trữ tin nhắn. Một số đối tượng thậm chí sử dụng mạng ẩn danh (như Tor, VPN, Dark Web) để che giấu địa chỉ IP và vị trí thực. Cùng với đó, các đối tượng có thể ẩn danh trong khâu thanh toán thông qua việc dùng ví điện tử không định danh hoặc thanh toán bằng tiền mã hóa (crypto) như Bitcoin, USDT để tránh bị theo dõi giao dịch hoặc trung gian thanh toán hoặc "người vận chuyển" để làm mờ dấu vết.

Ngoài ra, các gian hàng buôn lậu thường không ghi rõ địa chỉ liên hệ trên các nền tảng bán hàng online. Chỉ giao hàng qua chuyển phát nhanh, dịch vụ trung gian và tránh tiếp xúc trực tiếp với khách.

Sự phối hợp giữa các cơ quan chức năng còn hạn chế

Sự phối hợp giữa các cơ quan chức năng như lực lượng Cảnh sát kinh tế, Hải quan, Quản lý thị trường, lực lượng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao và các nền tảng công nghệ chưa thực sự chặt chẽ: Phân tán chức năng, chồng chéo nhiệm vụ các đơn vị thực hiện độc lập, thiếu đầu mối chỉ đạo thống nhất dẫn đến trùng lặp hoặc bỏ sót; Thiếu cơ sở dữ liệu dùng chung cho các hệ lực lượng; Chưa có hệ thống liên thông giữa dữ liệu giao dịch mạng, đối tượng vi phạm, tài khoản ảo… khiến việc truy vết bị gián đoạn, khó tổng hợp, nắm tình hình và đánh giá một cách chính xác; Chưa đồng bộ giữa trung ương và địa phương. Nhiều địa phương chưa chủ động trong việc xử lý vi phạm TMĐT, còn ỷ lại vào chỉ đạo từ trung ương; Thiếu quy định pháp lý cụ thể về phối hợp trên không gian mạng; Pháp luật chưa quy định rõ ràng về quy trình chia sẻ thông tin, điều tra tội phạm mạng giữa các lực lượng chức năng.

Chính sách, quy định pháp luật còn thiếu sót

Một số quy định pháp luật chưa cập nhật kịp với sự phát triển nhanh chóng của công nghệ và hình thức vi phạm mới. Một trong những thách thức lớn nhất trong công tác phòng ngừa tội phạm buôn lậu trên không gian mạng hiện nay là hành lang pháp lý chưa theo kịp tốc độ phát triển nhanh chóng của công nghệ số và các phương thức phạm tội mới. Hiện nay, mặc dù Việt Nam đã ban hành nhiều văn bản pháp luật như Luật An ninh mạng 2018, Bộ luật Hình sự 2015 (sửa đổi 2017), Luật Thương mại điện tử, và một số nghị định hướng dẫn liên quan đến xử lý vi phạm trong môi trường mạng, song vẫn tồn tại khoảng trống pháp lý ở các khía cạnh:

- Thiếu quy định rõ ràng về truy vết, thu thập chứng cứ điện tử, đặc biệt với các giao dịch xuyên biên giới, sử dụng ví điện tử không định danh hoặc tiền mã hóa.

- Các hình thức buôn lậu qua livestream, mạng xã hội, app di động, dark web... chưa được quy định cụ thể trong luật, gây khó khăn cho công tác xử lý.

- Chưa có quy định rõ ràng về trách nhiệm pháp lý của các nền tảng công nghệ, sàn thương mại điện tử và mạng xã hội trong việc ngăn chặn, gỡ bỏ nội dung buôn lậu, hàng cấm.

- Luật hiện hành chưa phân biệt rõ ràng giữa hành vi vi phạm hành chính và hành vi hình sự khi buôn bán hàng lậu qua mạng, dẫn đến việc xử lý chưa nhất quán.

Hệ quả là nhiều đối tượng lợi dụng các "vùng xám pháp lý" này để thực hiện hành vi phạm tội mà cơ quan chức năng khó xử lý triệt để, hoặc việc điều tra kéo dài do thiếu cơ sở pháp lý rõ ràng.

Nguồn nhân lực chưa đáp ứng được các yêu cầu thực tiễn

Hiện nay, lực lượng chức năng như An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao, Cảnh sát kinh tế, Quản lý thị trường, Hải quan hay Thanh tra thông tin đều đang trong quá trình chuyển đổi từ mô hình truyền thống sang môi trường số, nhưng tốc độ đào tạo và thích ứng chưa đáp ứng được yêu cầu thực tiễn. Theo Hiệp hội An toàn thông tin Việt Nam (VNISA), tổng số nhân sự cho an toàn thông tin tại Việt Nam năm 2023 chỉ là 3.601 người, tăng 11,6% so với năm 2022. Tuy nhiên, con số này vẫn còn quá ít để đáp ứng khối lượng công việc khổng lồ trước các xu thế tấn công mạng ngày càng gia tăng. Trong khi đó, tại Singapore, quốc gia nhỏ hơn nhiều so với Việt Nam cả về diện tích và dân số, ước tính có hơn 77.400 nhân viên an ninh mạng, nhưng vẫn thiếu hụt hơn 6.000 nhân viên trong lĩnh vực này.

Ngoài ra, một thách thức khác là sự thiếu hụt nguồn nhân lực có trình độ cao trong lĩnh vực an ninh mạng. Số lượng chuyên gia bảo mật hiện tại chưa đáp ứng đủ nhu cầu cấp thiết, đặc biệt trong bối cảnh các cuộc tấn công mạng ngày càng phức tạp cả về quy mô và tính chất. Những hạn chế về nguồn nhân lực thể hiện trên các mặt như: Số lượng cán bộ có chuyên môn sâu về công nghệ thông tin, an ninh mạng và phân tích dữ liệu điện tử để phát hiện, truy vết các giao dịch buôn lậu trực tuyến

còn ít; Kỹ năng điều tra số (digital forensics) – như phục hồi dữ liệu, truy xuất IP, phân tích blockchain của các cơ quan chuyên trách như Hải quan, Quản lý thị trường hay Cảnh sát kinh tế – vẫn còn hạn chế, trong khi đối tượng phạm tội sử dụng thủ đoạn ngày càng tinh vi; Sự phối hợp giữa lực lượng có trình độ công nghệ thông tin cao và các cơ quan chức năng thiếu hiệu quả…

Thực tế này khiến cho công tác phòng ngừa, phát hiện và xử lý vi phạm buôn lậu trên không gian mạng gặp nhiều khó khăn, đồng thời tạo ra khoảng trống để các đối tượng lợi dụng, gây thiệt hại nghiêm trọng về kinh tế và trật tự xã hội.

3. Giải pháp

Xuất phát từ những khó khăn, hạn chế trên đây, để nâng cao hiệu quả công tác phòng ngừa, đấu tranh với tội phạm buôn lậu trên không gian mạng, cần thực hiện tốt một số giải pháp như sau:

Một là hoàn thiện pháp luật và cơ chế quản lý

Việc hoàn thiện pháp luật và cơ chế quản lý trong phòng, chống buôn lậu trên không gian mạng là yêu cầu cấp bách trong bối cảnh số hóa toàn diện và hội nhập kinh tế quốc tế. Để nâng cao hiệu quả phòng ngừa và xử lý, Việt Nam cần tiến hành đồng bộ giữa cải cách pháp luật – hiện đại hóa công nghệ – đào tạo nhân lực – tăng cường hợp tác đa ngành. Trước hết cần rà soát, bổ sung các quy định pháp luật về quản lý hoạt động thương mại điện tử, xử lý hành vi buôn lậu qua mạng. Đồng thời, cũng cần tăng cường trách nhiệm của các nền tảng công nghệ trong việc kiểm soát nội dung và xử lý tài khoản vi phạm.

- *Hoàn thiện hệ thống pháp luật chuyên ngành*

+ Bổ sung quy định pháp luật về buôn lậu trên không gian mạng như: Xây dựng các điều khoản riêng trong Bộ luật Hình sự để quy định rõ về hành vi buôn lậu sử dụng công nghệ cao, mạng xã hội, ví điện tử, tiền mã hóa hay phân loại rõ tội

phạm kinh tế truyền thống và tội phạm công nghệ cao liên quan đến buôn lậu, tránh bỏ sót trách nhiệm pháp lý.

+ Sửa đổi Luật Giao dịch điện tử, Luật Thương mại điện tử và Luật An ninh mạng, trong đó cần làm rõ trách nhiệm của nền tảng TMĐT, mạng xã hội trong việc kiểm soát hàng hóa và thông tin buôn bán, cũng như quy định cơ chế thu thập, giám định chứng cứ điện tử đảm bảo giá trị pháp lý, hỗ trợ điều tra và truy tố.

+ Ban hành Luật hoặc Nghị định riêng về tội phạm công nghệ cao trong lĩnh vực kinh tế để tạo khuôn khổ pháp lý trong hoạt động điều tra, xử lý các hành vi buôn bán hàng lậu, hàng cấm, hàng giả qua mạng.

- *Tăng cường cơ chế giám sát, kiểm tra và xử lý vi phạm*

+ Thiết lập hệ thống giám sát giao dịch điện tử xuyên biên giới: Kết nối dữ liệu giữa Tổng cục Hải quan, Bộ Công thương, Bộ Công an và các sàn TMĐT. Đồng thời ứng dụng AI, Big Data trong phân tích giao dịch đáng ngờ.

+ Tăng quyền cho lực lượng Quản lý thị trường và lực lượng Cảnh sát kinh tế như: Cho phép truy cập, thu thập, đóng băng dữ liệu điện tử liên quan đến hoạt động buôn lậu trực tuyến hay cải tiến thủ tục hành chính liên ngành để rút ngắn thời gian điều tra và xử lý.

+ Quy định nghĩa vụ phối hợp bắt buộc của doanh nghiệp công nghệ bằng cách ràng buộc pháp lý với các nền tảng thương mại trực tuyến Facebook, TikTok, Shopee, Lazada trong việc gỡ nội dung vi phạm, cung cấp thông tin tài khoản theo yêu cầu pháp luật.

Hai là ứng dụng công nghệ hiện đại trong giám sát và điều tra

Trong bối cảnh tội phạm buôn lậu ngày càng lợi dụng các nền tảng số như sàn thương mại điện tử, mạng xã hội, ví điện tử và tiền mã hóa để thực hiện hành vi phạm

tội, việc ứng dụng công nghệ hiện đại vào công tác giám sát và điều tra là yêu cầu cấp thiết. Có thể áp dụng một số giải pháp như:

- *Ứng dụng trí tuệ nhân tạo (AI) và học máy (Machine Learning)*

Để phân tích hành vi người dùng: Sử dụng AI để phát hiện các mô hình bất thường trong hành vi đăng bán, giao dịch, vận chuyển hàng hóa trái phép.

Có thể tự động nhận diện sản phẩm vi phạm: Áp dụng nhận dạng hình ảnh và xử lý ngôn ngữ tự nhiên (NLP) để phát hiện hàng giả, hàng cấm qua hình ảnh sản phẩm và mô tả trên sàn TMĐT hoặc mạng xã hội.

Dự đoán xu hướng phạm tội: AI có thể học từ các vụ việc trong quá khứ để cảnh báo sớm nguy cơ tội phạm tại các khu vực, nền tảng hoặc thời điểm nhất định.

Ví dụ: Một số hệ thống tại Trung Quốc và Singapore đã tích hợp AI để phát hiện buôn lậu qua các từ khóa, hình ảnh và dấu hiệu bất thường trong logistics.

- *Triển khai công nghệ phân tích dữ liệu lớn (Big Data):*

Kết nối và tổng hợp dữ liệu từ nhiều nguồn: Từ các sàn thương mại điện tử, ngân hàng, hải quan, mạng xã hội, hệ thống kho vận…

Truy vết chuỗi cung ứng: Sử dụng công cụ phân tích để phát hiện mối liên hệ giữa người bán – người mua – trung gian vận chuyển – tài khoản thanh toán.

Tích hợp hệ thống dữ liệu dùng chung liên ngành: Tạo kho dữ liệu phục vụ cho các cơ quan như công an, hải quan, quản lý thị trường cùng khai thác.

- *Phát triển các công cụ điều tra số (Digital Forensics)*

Khôi phục và giám định dữ liệu điện tử: Các công cụ forensics giúp truy xuất nội dung tin nhắn, giao dịch, tập tin đã xóa.

Theo dõi địa chỉ IP và vị trí định danh: Sử dụng hệ thống định vị để xác định nguồn gốc của các hành vi buôn lậu ẩn danh.

Giám sát hoạt động trên darknet, chợ đen trực tuyến: Các phần mềm chuyên dụng có thể xâm nhập và theo dõi hành vi buôn bán hàng cấm ẩn danh.

- *Sử dụng công nghệ blockchain trong truy vết và lưu trữ giao dịch*

Minh bạch hóa chuỗi giao dịch hàng hóa: Ứng dụng blockchain để theo dõi đường đi của hàng hóa, từ khâu xuất kho đến khâu giao nhận.

Phát hiện giao dịch đáng ngờ bằng tiền mã hóa: Phân tích địa chỉ ví điện tử và các giao dịch blockchain để phát hiện hoạt động tài trợ buôn lậu.

- *Tăng cường hệ thống cảnh báo sớm và giám sát tự động*

Hệ thống giám sát 24/7: Triển khai nền tảng quét nội dung, hàng hóa vi phạm trên mạng xã hội, sàn TMĐT theo thời gian thực.

Cảnh báo tự động đến các cơ quan quản lý: Khi phát hiện hành vi đáng ngờ, hệ thống có thể gửi cảnh báo đến lực lượng chức năng.

- *Xây dựng trung tâm điều phối và phân tích công nghệ cao*

Trung tâm phân tích số liệu chống buôn lậu số: Với sự tham gia của nhiều cơ quan: Bộ Công an, Hải quan, QLTT, Bộ TT&TT.

Đầu tư thiết bị công nghệ chuyên sâu: Mua sắm phần mềm giám sát, forensics, máy chủ lưu trữ và hệ thống xử lý chuyên dụng.

Ba là đào tạo, nâng cao năng lực chuyên môn cho đội ngũ cán bộ thuộc các lực lượng chức năng

Để ứng dụng công nghệ hiện đại vào giám sát và phòng, chống tội phạm buôn lậu trên không gian mạng cần có sự hỗ trợ bởi nguồn nhân lực chuyên sâu, cơ sở pháp lý đầy đủ và cơ chế liên ngành chặt chẽ để phát huy hiệu quả toàn diện. Nâng cao năng lực cho lực lượng chức năng là nền tảng then chốt để phòng ngừa, phát hiện và xử lý hiệu quả tội phạm buôn lậu trên không gian mạng. Việc này đòi hỏi cải cách

đồng bộ về đào tạo, tổ chức, công nghệ và cơ chế đãi ngộ, cùng với việc xây dựng lực lượng chuyên trách mạnh, hiện đại và chủ động trước những thay đổi nhanh chóng của tội phạm mạng trong thời đại số. Do đó, việc nâng cao năng lực là yêu cầu cấp bách với các giải pháp cụ thể như sau:

- *Đào tạo và bồi dưỡng chuyên sâu về công nghệ số và điều tra mạng*

Tổ chức các khóa đào tạo chuyên biệt cho công an kinh tế, hải quan, quản lý thị trường, thanh tra thông tin… về: Điều tra số (digital forensics); Kỹ thuật truy vết địa chỉ IP, định vị giao dịch trực tuyến; Phân tích dữ liệu lớn (big data) và phát hiện hành vi buôn lậu qua mạng xã hội, sàn TMĐT; Nhận diện giao dịch bằng tiền mã hóa và sử dụng ví điện tử bất hợp pháp.

Hợp tác với các trường đại học, viện nghiên cứu và doanh nghiệp công nghệ để xây dựng chương trình huấn luyện gắn với thực tiễn, cập nhật công nghệ mới.

Khuyến khích đào tạo chuyên sâu ở nước ngoài thông qua các chương trình hợp tác quốc tế như INTERPOL, ASEANPOL, hoặc với các quốc gia có kinh nghiệm như Singapore, Hàn Quốc, EU.

- *Xây dựng lực lượng chuyên trách về phòng chống tội phạm buôn lậu trên không gian mạng*

Thành lập các đơn vị nghiệp vụ chuyên trách trong các lực lượng: Cảnh sát kinh tế, Hải quan, Bộ Công thương, Quản lý thị trường… có khả năng tác chiến độc lập hoặc phối hợp liên ngành trong không gian mạng.

Bổ sung biên chế phù hợp với tính chất công việc mới, ưu tiên tuyển dụng nhân sự có kiến thức nền tảng về CNTT, an toàn thông tin, luật mạng.

Giao nhiệm vụ cụ thể và thiết lập cơ chế phối hợp liên thông giữa các lực lượng qua cổng thông tin chung hoặc nền tảng chia sẻ dữ liệu.

- *Trang bị phương tiện, công cụ kỹ thuật hiện đại*

Cung cấp thiết bị giám sát mạng, phần mềm phát hiện hành vi buôn lậu trực tuyến, công cụ phân tích blockchain, công cụ phục hồi dữ liệu điện tử.

Đầu tư hệ thống lưu trữ dữ liệu lớn, phục vụ điều tra kéo dài và truy vết tội phạm ẩn danh.

Tăng cường kết nối mạng an toàn nội bộ giữa các lực lượng để đảm bảo chia sẻ thông tin điều tra hiệu quả, bảo mật.

- Cơ chế bảo vệ và đãi ngộ hợp lý

Xây dựng chính sách ưu tiên về đãi ngộ, tuyển dụng và giữ chân nhân sự công nghệ cao làm việc trong lĩnh vực phòng chống tội phạm công nghệ số.

Áp dụng chính sách khen thưởng theo hiệu quả công tác đối với các cá nhân, tập thể phát hiện và xử lý các vụ việc buôn lậu trên không gian mạng phức tạp, có yếu tố xuyên quốc gia.

- Tăng cường hợp tác quốc tế và trao đổi kinh nghiệm

Tham gia các chương trình chia sẻ kinh nghiệm, tập huấn và chuyển giao công nghệ với các tổ chức như UNODC, INTERPOL, ASEANAPOL.

Thiết lập các đầu mối liên lạc quốc tế để xử lý vụ việc xuyên biên giới, đặc biệt trong các trường hợp sử dụng nền tảng mạng xã hội, tiền mã hóa, dịch vụ cloud đặt tại nước ngoài.

Bốn là tăng cường phối hợp liên ngành và hợp tác công - tư

Với việc tội phạm buôn lậu trên không gian mạng thường diễn ra dưới dạng ẩn danh, đa nền tảng, xuyên biên giới, gây khó khăn trong phát hiện, điều tra và xử lý. Trong khi đó, các lực lượng chức năng tại Việt Nam (như Cảnh sát kinh tế, Hải quan, Quản lý thị trường, Bộ TT&TT, Bộ Công thương...) vẫn thiếu cơ chế phối hợp thường xuyên, liên thông và hiệu quả. Đồng thời, khu vực doanh nghiệp công nghệ

và sàn TMĐT đang nắm giữ phần lớn dữ liệu, nền tảng và công nghệ hiện đại, nhưng mức độ phối hợp với các lực lượng chức năng còn hạn chế. Do vậy, việc tăng cường phối hợp liên ngành và thúc đẩy hợp tác công – tư (PPP) là một giải pháp chiến lược mang tính nền tảng. Cụ thể:

- *Thiết lập cơ chế điều phối tập trung liên ngành*

Thành lập "Trung tâm điều phối chống buôn lậu số quốc gia" dưới sự chỉ đạo của Chính phủ hoặc Ban Chỉ đạo 389 quốc gia.

Trung tâm này cần tập hợp các lực lượng: Công an, Hải quan, Quản lý thị trường, Bộ TT&TT, Bộ Tài chính, Bộ Công thương và các đơn vị công nghệ thông tin liên quan.

- *Xây dựng cơ sở dữ liệu dùng chung và liên thông thông tin*

Xây dựng hạ tầng chia sẻ dữ liệu liên ngành về: Danh sách đối tượng, tài khoản nghi vấn; Dữ liệu hàng hóa, vận chuyển, giao dịch điện tử; Hành vi vi phạm trên sàn thương mại điện tử hoặc mạng xã hội; Tích hợp hệ thống cảnh báo sớm, phân tích rủi ro tự động, từ đó ra quyết định xử lý hoặc chuyển điều tra.

- *Ban hành quy chế phối hợp cụ thể giữa các lực lượng*

Rà soát, hoàn thiện quy chế phối hợp giữa Bộ Công an – Bộ Công thương – Bộ TT&TT – Tổng cục Hải quan – Cục QLTT trong điều tra, xử lý và chia sẻ dữ liệu.

Quy định rõ trách nhiệm đầu mối, cơ chế phản ứng nhanh và thời hạn phối hợp xử lý.

- *Thiết lập cơ chế hợp tác chính thức giữa cơ quan Nhà nước và doanh nghiệp công nghệ*

Ký biên bản ghi nhớ (MOU) hoặc hiệp định hợp tác giữa các cơ quan quản lý với các sàn thương mại điện tử: Shopee, Lazada, Tiki…các nền tảng mạng xã hội: Facebook, TikTok, Zalo…và các công ty vận chuyển, trung gian thanh toán điện tử, ví điện tử.

- *Quy định nghĩa vụ cung cấp thông tin và phối hợp phòng ngừa, điều tra*

Sửa đổi, bổ sung luật để ràng buộc trách nhiệm pháp lý của doanh nghiệp trong: Gỡ bỏ nội dung vi phạm; Cung cấp thông tin người dùng, giao dịch, đơn hàng, IP… theo yêu cầu của lực lượng chức năng; Tham gia hệ thống cảnh báo sản phẩm, tài khoản vi phạm.

- *Khuyến khích đầu tư công nghệ điều tra từ các doanh nghiệp*

Khuyến khích doanh nghiệp công nghệ tham gia phát triển: Hệ thống quét và giám sát nội dung buôn lậu; Phần mềm phân tích giao dịch bất thường; Các mô hình dự báo và đánh giá rủi ro buôn lậu qua mạng; Có thể áp dụng mô hình "sandbox" (vùng thử nghiệm pháp lý) để các công ty công nghệ phối hợp cùng cơ quan công quyền thử nghiệm giải pháp điều tra tội phạm mạng.

- *Tham gia các mạng lưới chia sẻ dữ liệu và cảnh báo sớm như:*

Mạng lưới thu hồi tài sản khu vực châu Á – Thái Bình Dương (INTERPOL's Cybercrime Directorate; ASEANPOL, ARIN-AP); Ký kết hiệp định chia sẻ thông tin với các nền tảng xuyên quốc gia như Meta, Google, TikTok... thông qua đại diện pháp lý tại Việt Nam.

Đây là giải pháp có tính cấu trúc và dài hạn, đòi hỏi cách tiếp cận phù hợp với xu thế quản trị hiện đại, đòi hỏi sự chủ động, linh hoạt và minh bạch từ cả phía nhà nước và doanh nghiệp.

Năm là đẩy mạnh tuyên truyền, nâng cao nhận thức của người tiêu dùng

Trong bối cảnh rất nhiều người tiêu dùng không nhận thức được việc mua – bán hàng lậu, hàng giả, hàng không rõ nguồn gốc trên không gian mạng là hành vi vi phạm pháp luật. Người tiêu dùng thường bị thu hút bởi giá rẻ, thiếu hiểu biết về các quy định pháp luật và dễ bị lôi kéo vào hoạt động tiếp tay cho buôn lậu mà không nhận thức được mức độ nguy hiểm. Vì vậy, việc nâng cao nhận thức, tuyên truyền và phổ biến kiến thức pháp luật là giải pháp phòng ngừa cơ bản, giúp tạo "vaccine pháp lý" trong toàn xã hội. Cụ thể cần:

- *Đa dạng hóa hình thức và nội dung tuyên truyền*

Tổ chức các chiến dịch truyền thông đa phương tiện qua: Truyền hình, phát thanh, báo điện tử, báo giấy; Các nền tảng mạng xã hội (Facebook, TikTok, YouTube, Zalo); Ứng dụng TMĐT và ví điện tử (như Shopee, Tiki, MoMo, ZaloPay).

Tạo nội dung gần gũi, dễ tiếp cận, dễ hiểu, như: Video ngắn, infographics, phim tài liệu mini; Tình huống giả định, phỏng vấn chuyên gia, chia sẻ người bị hại.

Tổ chức các cuộc thi trực tuyến tìm hiểu pháp luật liên quan đến buôn lậu mạng.

Chủ động truyền thông những hậu quả pháp lý và kinh tế nghiêm trọng của việc buôn bán, tiếp tay, tiêu dùng hàng lậu: phạt hành chính, truy cứu hình sự, mất uy tín cá nhân/doanh nghiệp.

- *Phối hợp giữa các cơ quan và doanh nghiệp trong tuyên truyền*

Bộ TT&TT (nay là Bộ KHCN), Bộ Công an, Bộ Công thương, Cục QLTT… cần chủ trì các chiến dịch truyền thông quốc gia phối hợp với: Các sàn TMĐT; doanh nghiệp công nghệ, ngân hàng số, ví điện tử hoặc các KOLs, influencer có ảnh hưởng đến giới trẻ.

Tăng cường hợp tác với nhà trường, tổ chức đoàn thể, hiệp hội ngành nghề để đưa kiến thức pháp luật và kỹ năng nhận diện vi phạm vào các chương trình phổ biến

pháp luật tại các trường học (đặc biệt trung học, cao đẳng, đại học); các doanh nghiệp (tập huấn cho nhân viên bán hàng online) và trong cộng đồng dân cư (thông qua tổ dân phố, hội phụ nữ, đoàn thanh niên).

- *Ứng dụng công nghệ vào công tác tuyên truyền*

Xây dựng nền tảng tuyên truyền số: Trang web, ứng dụng di động, kênh YouTube hoặc chatbot cung cấp kiến thức pháp luật liên quan đến buôn lậu, thương mại điện tử.

Phát triển bộ công cụ nhận diện hàng lậu và cảnh báo sớm: Cho phép người tiêu dùng kiểm tra mã vạch, nguồn gốc hàng hóa, tài khoản bán hàng đáng ngờ…

- *Đo lường hiệu quả và cập nhật liên tục nội dung*

Thường xuyên khảo sát nhận thức người dân, từ đó điều chỉnh nội dung truyền thông cho phù hợp từng nhóm đối tượng (học sinh, sinh viên, tiểu thương, người lao động…).

Cập nhật các thủ đoạn mới, hình thức vi phạm mới để truyền thông kịp thời, chống lại sự "bình thường hóa" hành vi buôn lậu trên không gian mạng.

Khi người dân nhận thức rõ rằng hành vi buôn bán, tiếp tay tiêu thụ hàng lậu là vi phạm pháp luật và gây tổn hại nghiêm trọng đến kinh tế, sức khỏe và an ninh quốc gia, thì hiệu quả phòng chống tội phạm buôn lậu trên không gian mạng sẽ được nâng cao đáng kể.

4. Kết luận

Tội phạm buôn lậu trên không gian mạng là thách thức lớn đối với công tác quản lý nhà nước và bảo vệ quyền lợi người tiêu dùng. Để phòng ngừa hiệu quả, cần có sự vào cuộc đồng bộ của cả hệ thống chính trị, sự hợp tác chặt chẽ giữa các cơ quan chức năng, doanh nghiệp công nghệ và người dân. Việc kết hợp giữa giải pháp

công nghệ, pháp lý và tuyên truyền sẽ tạo ra một môi trường mạng lành mạnh, an toàn và minh bạch hơn.

Tài liệu tham khảo:

1. Ban Chỉ đạo 389 quốc gia. (2023). Báo cáo tổng kết công tác phòng, chống buôn lậu, gian lận thương mại và hàng giả năm 2023.

2. Tạp chí Dân chủ Pháp luật. (2023). Một số giải pháp nâng cao hiệu quả phòng, chống buôn lậu, gian lận thương mại tại Việt Nam.

3. Tạp chí Cộng sản. (2024). Chống buôn lậu, gian lận thương mại và hàng giả - Biện pháp bảo vệ sản xuất và tiêu dùng.

4. Tạp chí Mặt trận. (2024). Cần giải pháp toàn diện để phòng ngừa, ngăn chặn lừa đảo trên không gian mạng.

Nguyễn Văn Doanh (Thạc sỹ, Giảng viên Học viện Cảnh sát nhân dân)