**Bàn về pháp luật phòng, chống rửa tiền sử dụng công nghệ cao**

**Công nghệ cao, một mặt, mang lại nhiều giá trị hơn cho cuộc sống của con người; mặt khác, lại bị lạm dụng cho những hoạt động phạm tội; nhưng cũng chính công nghệ cao lại được cơ quan chức năng sử dụng để phòng, chống tội phạm này**  
 **1. Tội phạm công nghệ cao, rủi ro rửa tiền sử dụng công nghệ cao tại Việt Nam**  
 Công nghệ cao, một mặt, mang lại nhiều giá trị hơn cho cuộc sống của con người; mặt khác, lại bị lạm dụng cho những hoạt động phạm tội; nhưng cũng chính công nghệ cao lại được cơ quan chức năng sử dụng để phòng, chống tội phạm này. Ngày càng nhiều tội phạm lạm dụng công nghệ cao để tiến hành các hoạt động phạm tội và rửa những khoản thu này cũng bằng công nghệ cao. Với tính bảo mật cao và tài sản dưới dạng số, những thông tin về người thực hiện giao dịch và chủ sở hữu hưởng lợi thực sự đằng sau các giao dịch không tìm được dễ dàng là những điểm mà công nghệ cao bị lạm dụng để rửa tiền. Rửa tiền sử dụng công nghệ cao bao giờ cũng gắn kết với vai trò của những trung gian, những tổ chức, cá nhân cung ứng dịch vụ đóng vai trò kết nối, truyền dẫn và cả thanh toán, chuyển giá trị giữa các loại tài sản khác nhau.    
 Trong Báo cáo đánh giá đa phương năm 2009 của Nhóm Châu Á - Thái Bình Dương về chống rửa tiền (APG) đối với Việt Nam có nhận định liên quan đến tội phạm sử dụng công nghệ cao như sau: “Các hoạt động gian lận khác: Ngày càng có nhiều báo cáo về các hình thức kinh doanh gian lận/lừa đảo trên mạng (online ponzi) nơi mà các nhà đầu tư cả tin bị lừa đảo chiếm đoạt các khoản tiền tiết kiệm”. Cho tới nay, loại hình phạm tội này càng trở nên phức tạp và tinh vi hơn, với số lượng vụ án nhiều và nhiều nạn nhân bị lừa đảo. Đặc biệt, có những hành vi tội phạm công nghệ cao lần đầu xuất hiện như lập website để tổ chức huy động vốn, trả lãi suất cao, nhằm chiếm đoạt tài sản hoặc tấn công ví điện tử lấy tiền của khách hàng1. Các băng nhóm tội phạm cũng lập và tạo ra nhiều sàn giao dịch các loại tiền điện tử hoạt động theo mô hình đa cấp như: Onecoin, Bitcoin, ILcoin, Gemcoin... để thu hút các nhà đầu tư nhằm chiếm đoạt tài sản hoặc kinh doanh tiền điện tử trái phép để rửa tiền, ship hàng, trả tiền cá độ bóng đá... Nhiều vụ án, trong đó, tội phạm sử dụng công nghệ cao để thực hiện hành vi phạm tội và có những khoản thu không hề nhỏ, bị các cơ quan có thẩm quyền điều tra, truy tố, xét xử, nhưng hiếm khi được xét xử song song với vụ án rửa tiền; chưa có hành vi rửa tiền sử dụng công nghệ cao nào được phát hiện và xử lý theo quy định của pháp luật.  
 Theo Cyber Security Intelligence, hằng năm, có đến khoảng 200 tỷ đô la Mỹ có nguồn gốc phạm tội được tội phạm công nghệ cao rửa qua việc sử dụng tổng thể những cách thức khác nhau thông qua tiền kỹ thuật số, tiền đánh bạc và những tổ chức thanh toán nhỏ lẻ, vi mô. Tội phạm mạng, lúc đầu, thường không sử dụng tiền ảo như một phương thức rửa những khoản thu phạm tội, mà sử dụng những đồng tiền trong các trò chơi điện tử hoặc các thỏi vàng quy ước trong các trò chơi như Minecraft, FIFA, World of Warcraft hay GTA 5 vì trong đó, cho phép những người chơi chuyển đổi, mua bán đồng tiền chơi với nhau, sau đó, chuyển đổi ra đồng tiền pháp định và hàng hóa2. Theo các chuyên gia tính toán, có đến 10% tội phạm công nghệ cao sử dụng PayPal; 35% sử dụng các hệ thống thanh toán khác như Skrill, Dwoll, Zoom và các hệ thống thanh toán bằng mobile như M-Pesa để rửa tiền. Những phương thức như ʺrửa ít một“ được sử dụng, khi mà hàng nghìn giao dịch thanh toán điện tử nhỏ lẻ được thực hiện qua các nền tảng như Paypal nhằm tránh bị lần ra dấu vết ngày càng được sử dụng nhiều hơn và khó phát hiện hơn. Một phương thức thường được sử dụng khác nữa là việc sử dụng các giao dịch thanh toán trực tuyến qua các trang mạng như eBay để thực hiện rửa tiền. Nhiều tội phạm công nghệ còn sử dụng tiền ảo để mua những tài sản có giá trị cao như bất động sản, vàng,... và bằng cách đó, chuyển đổi tiền kiếm được từ hoạt động phạm tội sang tài sản hoặc tiền mặt hợp pháp. Những trang web như Bitcoin Real Estate cho phép người sở hữu đồng tiền này mua bán bất động sản trong khi đồng tiền này chưa được quản lý bởi bất cứ quốc gia hay ngân hàng trung ương nào.

Năm 2018, Bộ Tư pháp đã có Báo cáo tổng quan về pháp luật về tài sản ảo, thực tiễn về tài sản ảo, tiền ảo ở Việt Nam và trên thế giới. Tại Báo cáo này có nhận định: “Tại Việt Nam, mặc dù khung pháp lý cho tài sản mã hóa, tiền mã hóa chưa rõ ràng như đã phân tích, tài sản mã hóa, tiền mã hóa vẫn được giao dịch công khai và rất nhiều người tham gia giao dịch, đầu tư kinh doanh. Người tham gia mua bán các loại tài sản mã hóa, tiền mã hóa chủ yếu mang tính đầu cơ”3. Theo đó, ước tính có khoảng 1 triệu người sở hữu và tham gia giao dịch tài sản mã hóa với số tiền giao dịch hàng ngày khoảng 200 - 300 tỷ đồng, phần lớn giao dịch qua các tài khoản ngân hàng4. Đồng thời, đồng Việt Nam là một trong 8 đồng tiền pháp định được sử dụng nhiều nhất trong giao dịch tài sản mã hóa, tiền mã hóa thực tế trên toàn thế giới. Tài sản mã hóa còn được một số cá nhân, tổ chức sử dụng để chuyển giá trị ra nước ngoài mà không qua hệ thống ngân hàng, mạng lưới thanh toán chính thức hiện hành. Báo cáo này đã nhận định về nguy cơ rửa tiền và tài trợ khủng bố từ các giao dịch tài sản mã hóa, tiền mã hóa, do tính chất ẩn danh của các giao dịch này. Báo cáo nêu: một số tổ chức nước ngoài thay đổi cách tài trợ truyền thống thông qua tiền mặt, chuyển khoản hoặc hợp pháp hóa thành các khoản đầu tư, từ thiện bằng cách chuyển tài sản mã hóa, tiền mã hóa cho các nhóm chống phá trong nước. Việc quy đổi tài sản mã hóa, tiền mã hóa thành tiền mặt tại Việt Nam vẫn có thể diễn ra do khái niệm tiền mã hóa, tài sản mã hóa chưa được xác định, khuôn khổ pháp lý chưa rõ ràng, đồng bộ để quản lý, xử lý các hoạt động liên quan đến tài sản mã hóa, tiền mã hóa. Ngoài ra, tiền mã hóa còn được sử dụng để ẩn danh giao dịch thanh toán cho các hành vi vi phạm pháp luật khác như: mua bán thông tin thẻ tín dụng; thuê máy chủ không cần xác thực chủ thể, dùng để truyền bá văn hóa phẩm đồi trụy; thuê tấn công DDoS (thuế tấn công từ chối dịch vụ phân tán); chiếm quyền điều khiển máy tính tống tiền; buôn bán ma túy; buôn bán vũ khí và nhiều loại tội phạm khác5. Đây cũng là báo cáo đầy đủ nhất có đánh giá về nguy cơ tội phạm gắn với các giao dịch tài sản ảo và tiền ảo, tức là gắn với công nghệ cao hay công nghệ 4.0 hiện nay.  
 **2. Chuẩn mực quốc tế về phòng, chống rửa tiền sử dụng công nghệ cao**  
 Năm 2012, cùng với sự phát triển của những phương thức thanh toán mới, những loại tiền ảo, những sản phẩm, dịch vụ gắn liền với công nghệ mới, Lực lượng đặc nhiệm tài chính quốc tế (FATF) đã đưa ra Khuyến nghị 14 và 156 như sau:

*“14. Các dịch vụ chuyển tiền hoặc giá trị*

Các quốc gia cần phải tiến hành các biện pháp để đảm bảo rằng, cá nhân hay pháp nhân cung cấp dịch vụ chuyển tiền hoặc giá trị được cấp phép hoặc đăng ký và là đối tượng của hệ thống hiệu quả về giám sát và bảo đảm tuân thủ các biện pháp phù hợp đề cập trong các khuyến nghị của FATF. Các quốc gia cần phải có những hành động nhằm nhận biết các cá nhân và pháp nhân cung cấp dịch vụ chuyển tiền hoặc giá trị không được cấp phép hoặc đăng ký với cơ quan có thẩm quyền, và áp dụng các hình phạt phù hợp. Bất cứ cá nhân hay pháp nhân nào hoạt động như một đại lý cũng phải được cấp phép hoặc đăng ký với cơ quan có thẩm quyền, hoặc nhà cung cấp dịch vụ chuyển tiền hoặc giá trị cần phải duy trì một danh sách các đại lý của mình mà các cơ quan có thẩm quyền có thể truy cập được tại quốc gia mà nhà cung cấp dịch vụ đó cũng như các đại lý của mình hoạt động".  
 *“15. Các quốc gia và các tổ chức tài chính cần phải nhận dạng và đánh giá rủi ro rửa tiền và tài trợ khủng bố có thể phát sinh gắn liền với: (a) sự phát triển của các sản phẩm mới và thực tiễn kinh doanh mới, bao gồm cả những cơ chế giao nhận mới; và (b) việc sử dụng mới hay phát triển những công nghệ cho cả những sản phẩm mới và sản phẩm tồn tại trước đó. Đối với các tổ chức tài chính, việc đánh giá rủi ro như vậy cần phải làm trước khi đưa ra những sản phẩm hay công việc kinh doanh mới hoặc sử dụng hay phát triển những công nghệ mới. Những tổ chức này phải thực hiện những biện pháp thích hợp nhằm quản lý và giảm thiểu những rủi ro như vậy. Để quản lý và giảm thiểu những rủi ro nổi lên từ các tài sản ảo, các quốc gia phải đảm bảo rằng những nhà cung cấp dịch vụ liên quan tiền ảo phải được quản lý cho mục tiêu chống rửa tiền và chống tài trợ khủng bố, được cấp phép hoặc đăng ký, và là đối tượng của những hệ thống hiệu quả về giám sát và bảo đảm sự tuân thủ những biện pháp phù hợp đưa ra trong các khuyến nghị của FATF”.*  
 Đồng thời với 40 chuẩn mực quốc tế về phòng, chống rửa tiền, chống tài trợ khủng bố và chống phổ biến vũ khí hủy diệt được thông qua tháng 10/2013 và được cập nhật, bổ sung định kỳ, mới nhất vào tháng 10/2019, khuyến nghị 15 hay còn gọi là chuẩn mực quốc tế số 15 được FATF giải nghĩa như sau:  
 *“1. Nhằm mục đích áp dụng các Khuyến nghị của FATF, các quốc gia phải xem tài sản ảo như “tài sản”, “thu nhập”, “quỹ”, “quỹ hoặc tài sản khác” hoặc “giá trị tương đương” khác. Các quốc gia phải áp dụng các biện pháp phù hợp theo các Khuyến nghị của FATF đối với tài sản ảo và các nhà cung cấp dịch vụ tài sản ảo (VASPs) .*  
 *2. Phù hợp với Khuyến nghị 1, các quốc gia phải xác định, đánh giá và hiểu về rủi ro rửa tiền và tài trợ khủng bố phát sinh từ các hoạt động tiền ảo và hoạt động/hành động của VASPs. Dựa trên cơ sở đánh giá đó, các quốc gia phải áp dụng phương pháp tiếp cận trên cơ sở rủi ro để đảm bảo rằng những biện pháp phòng ngừa và ngăn chặn rửa tiền và tài trợ khủng bố tương ứng với mức độ rủi ro được xác định. Các quốc gia phải yêu cầu các VASPs xác định, đánh giá và tiến hành những hoạt động có hiệu quả nhằm ngăn chặn những rủi ro rửa tiền và tài trợ khủng bố của họ.*

*3. VASPs yêu cầu phải được cấp phép hoặc đăng ký. Ít nhất, VASPs cần phải được yêu cầu cấp phép hoặc đăng ký tại các quốc gia mà chúng được tạo nên. Trong trường hợp VASP là cá nhân thì họ phải được yêu cầu được cấp phép hoặc đăng ký tại quốc gia nơi mà trụ sở kinh doanh của họ đặt tại đó. Các quốc gia cũng có thể yêu cầu các VASPs đang cung cấp sản phẩm hay dịch vụ cho các khách hàng trong, hoặc thực hiện hoạt động từ quốc gia của họ, phải được cấp phép hoặc đăng ký tại quốc gia mình. Các cơ quan chức năng cần phải có những biện pháp về mặt pháp lý và quản lý cần thiết để tránh việc tội phạm và đồng bọn của chúng nắm giữ hoặc trở thành chủ sở hữu hưởng lợi, hoặc có quyền lợi chi phối hay kiểm soát, hoặc nắm giữ chức năng quản lý tại một VASP nào đó. Các quốc gia cần phải hành động nhằm xác định những cá nhân hay pháp nhân thực hiện hoạt động của một VASP mà không được cấp phép hay đăng ký trước đó, và áp dụng các biện pháp trừng phạt phù hợp.*

*4. Một quốc gia không cần phải có hệ thống cấp phép hay đăng ký riêng biệt liên quan tới các cá nhân hay pháp nhân đã được cấp phép hay đăng ký như những tổ chức tài chính (như được xác định theo Các khuyến nghị của FATF) trong quốc gia mà theo giấy phép và đăng ký thì những tổ chức này được phép thực hiện những hoạt động của VASPs và cũng đã là đối tượng thực hiện đầy đủ nghĩa vụ theo các Khuyến nghị của FATF.*  
 *5. Các quốc gia cần phải đảm bảo rằng, VASPs là đối tượng quản lý và giám sát, kiểm soát đầy đủ về chống rửa tiền và chống tài trợ khủng bố và thực hiện một cách có hiệu quả những khuyến nghị thích hợp của FATF nhằm ngăn chặn những rủi ro rửa tiền và tài trợ khủng bố gắn với tài sản ảo. VASPs phải là đối tượng của một hệ thống giám sát hiệu quả và đảm bảo sự tuân thủ với các yêu cầu về AML/CFT của quốc gia. VASPs phải được giám sát và quản lý bởi cơ quan có thẩm quyền (không phải tổ chức tự quản), mà cơ quan này phải tiến hành giám sát và quản lý trên cơ sở rủi ro. Các giám sát viên cần phải có quyền lực phù hợp để giám sát và quản lý và đảm bảo các VASPs tuân thủ với những yêu cầu chống rửa tiền và chống tài trợ khủng bố, bao gồm cả quyền thực hiện thanh tra, buộc cung cấp thông tin, và áp đặt những hình phạt. Các giám sát viên phải có quyền áp đặt rộng rãi các hình phạt từ hành chính đến tài chính, kể cả quyền rút, cấm hay tạm ngừng cấp phép hoặc đăng ký cho các VASPs, khi có thể áp dụng.*

*6. Các quốc gia phải đảm bảo rằng có khung hình phạt hiệu quả, thích đáng và có tính răn đe, cho dù đó là hình sự, dân sự hay hành chính, có thể giải quyết được những VASPs không tuân thủ những yêu cầu về AML/CFT, phù hợp với Khuyến nghị 35. Các hình phạt phải được áp dụng không những chỉ đối với các VASPs, mà còn đối với giám đốc hay ban quản lý cấp cao của những tổ chức này.*  
 *7. Liên quan tới các biện pháp phòng ngừa, những yêu cầu nêu tại Khuyến nghị 10 đến 21 áp dụng cho VASPs, tùy thuộc vào những tiêu chí sau: (a) Khuyến nghị 10 - Ngưỡng giao dịch vãng lai mà nếu trên mức đó, các VASPs phải thực hiện CDD là USD/EUR 1.000; (b) Khuyến nghị 16 - Các quốc gia cần phải đảm bảo rằng VASPs khởi tạo phải có được và lưu giữ thông tin một cách cẩn trọng và theo yêu cầu về người khởi tạo và thông tin về người thụ hưởng trong các giao dịch chuyển tài sản ảo (tất cả các giao dịch tài sản ảo đều được coi là các giao dịch xuyên biên giới), chuyển thông tin này tới VASPs thụ hưởng hoặc tổ chức tài chính (nếu có) ngay lập tức và đảm bảo an toàn, và sẵn sàng cung cấp cho cơ quan chức năng khi được yêu cầu. Các quốc gia phải đảm bảo rằng, các VASPs thụ hưởng phải có được và nắm giữ thông tin người khởi tạo theo yêu cầu và thông tin về người thụ hưởng một cách cẩn trọng và theo yêu cầu trong các giao dịch tài sản ảo và sẵn sàng cung cấp cho cơ quan thích hợp khi được yêu cầu. Những yêu cầu khác của Khuyến nghị 16 (bao gồm cả việc quản lý tính khả dụng của thông tin cũng như việc tiến hành các hành động phong tỏa và cấm giao dịch với những tổ chức, cá nhân chỉ định) áp dụng trên cùng một cơ sở như đưa ra trong Khuyến nghị 16. Những nghĩa vụ như vậy cũng áp dụng cho các tổ chức tài chính khi chuyển hay nhận các giao dịch tài sản ảo thay mặt cho khách hàng.*  
 *8. Các quốc gia phải cung cấp phạm vi hợp tác quốc tế rộng nhất có thể, một cách nhanh chóng, có tính xây dựng và hiệu quả, liên quan đến rửa tiền, tài trợ khủng bố, các tội phạm nguồn liên quan đến tài sản ảo, trên cơ sở được nêu tại các Khuyến nghị từ 37 đến 40. Đặc biệt, các giám sát viên đối với các VASPs phải trao đổi thông tin ngay lập tức và có tính xây dựng với các đối tác nước ngoài của mình mà không tính đến bản chất hay vị trí của các cơ quan giám sát và cả sự khác biệt trong tên gọi hay loại hình/vị trí của các VASPs7.*  
 Và để có thể thực hiện được những khuyến nghị này, FATF đã có những nghiên cứu và hướng dẫn để thống nhất triển khai thực hiện và làm cơ sở cho các đánh giá viên đánh giá mức độ tuân thủ và tính hiệu quả việc thực hiện chuẩn mực quốc tế tại các quốc gia liên quan.  
 Như vậy, phần lớn các giải nghĩa của FATF liên quan đến công nghệ mới gắn với hoạt động của những tổ chức cung ứng dịch vụ liên quan đến tiền ảo. Theo đó, tài sản ảo là một hình thức giá trị số có thể mua bán, chuyển nhượng bằng công nghệ số và có thể được sử dụng cho những mục đích thanh toán hoặc đầu tư. Tài sản ảo không bao gồm hình thức bằng kỹ thuật số của tiền thật, chứng khoán hay các tài sản tài chính khác đâu đó đã được nhắc đến trong các Khuyến nghị của FATF. Nhà cung cấp dịch vụ tài sản ảo (VASPs) được hiểu là bất cứ cá nhân hay pháp nhân nào chưa bao gồm trong các Khuyến nghị của FATF, và như là một nhà kinh doanh, thực hiện một hoặc nhiều hơn những hoạt động hoặc hành động sau cho hoặc thay mặt cho những thể nhân hay pháp nhân khác: (i) chuyển đổi giữa tài sản ảo và những đồng tiền thực hiện nay; (ii) chuyển đổi giữa một hoặc nhiều dạng tài sản ảo; (iii) chuyển tài sản ảo; (iv) canh giữ hoặc quản lý tài sản ảo hoặc công cụ ảo tạo điều kiện cho việc kiểm soát các tài sản ảo; (v) tham gia vào hoặc cung cấp dịch vụ tài chính liên quan đến việc cung ứng hoặc bán tài sản ảo của người phát hành8.

**3. Pháp luật Việt Nam về phòng, chống rửa tiền sử dụng công nghệ cao trong bối cảnh cách mạng công nghiệp 4.0**  
 Trong bối cảnh khung pháp lý nói chung tại Việt Nam hiện nay còn đang được các cấp, các ngành nghiên cứu để bổ sung, chỉnh sửa, hoàn thiện để đáp ứng được trong điều kiện cuộc cách mạng công nghiệp 4.0 thì pháp luật về phòng, chống rửa tiền cũng không phải là ngoại lệ.  
 Điều 15 Luật Phòng, chống rửa tiền năm 2012 quy định về trách nhiệm của các đối tượng báo cáo trong các giao dịch liên quan tới công nghệ mới như sau:  
 *“Điều 15. Các giao dịch liên quan tới công nghệ mới*

*1. Đối tượng báo cáo phải ban hành quy trình nhằm mục đích sau đây:*

*a) Phát hiện, ngăn chặn việc sử dụng công nghệ mới vào việc rửa tiền;*

*b) Quản lý rủi ro về rửa tiền khi thiết lập giao dịch với khách hàng sử dụng công nghệ mới và không gặp mặt trực tiếp.*

*2. Quy trình quy định tại khoản 1 Điều này phải bảo đảm việc cập nhật thông tin khách hàng có hiệu quả như việc cập nhật thông tin khách hàng gặp mặt trực tiếp.”*  
 *Điều 8 Nghị định 116/2013/NĐ-CP ngày 11/10/2013 hướng dẫn thi hành một số điều của Luật Phòng, chống rửa tiền hướng dẫn thêm về quy định trên của Luật Phòng, chống rửa tiền như sau:*

*“Điều 8. Giao dịch liên quan tới công nghệ mới*

*1. Giao dịch liên quan tới công nghệ mới là giao dịch sử dụng công nghệ cho phép khách hàng thực hiện giao dịch mà không cần gặp mặt trực tiếp nhân viên của đối tượng báo cáo.*

*2. Đối tượng báo cáo khi cung cấp dịch vụ theo quy định tại Khoản 1 Điều này phải thực hiện các yêu cầu sau:*

*a) Gặp mặt trực tiếp khách hàng khi lần đầu thiết lập mối quan hệ và yêu cầu khách hàng cung cấp thông tin theo quy định tại Điều 4 Nghị định này;*

*b) Xây dựng quy trình đánh giá rủi ro về rửa tiền khi cung cấp dịch vụ sử dụng công nghệ mới. Quy trình này tối thiểu phải bao gồm các nội dung sau: Xác định và mô phỏng các rủi ro về rửa tiền có thể phát sinh đối với các giao dịch áp dụng công nghệ mới; đưa ra các biện pháp phù hợp để phòng ngừa và giảm thiểu các rủi ro phát sinh”.*  
 Thực hiện các quy định nêu trên, trong những năm 2013 - 2019, các đối tượng báo cáo là các tổ chức tài chính và các tổ chức, cá nhân kinh doanh ngành nghề phi tài chính có liên quan đã cố gắng triển khai, áp dụng các biện pháp khác nhau nhưng chỉ có thể đảm bảo ban hành được quy trình nội bộ liên quan, sử dụng các chi nhánh và bên thứ ba để có thể tiếp xúc được khách hàng lần đầu.    
 Để khắc phục khó khăn này và để thích ứng với những thay đổi gắn với công nghệ mới, Điểm a Khoản 2 Điều 8 nêu trên đã được sửa đổi bởi Khoản 5 Điều 1 Nghị định số 87/2019/NĐ-CP ngày 14/11/2019 sửa đổi, bổ sung một số điều của Nghị định 116/2013/NĐ-CP ngày 11/10/2013 hướng dẫn thi hành một số điều của Luật Phòng, chống rửa tiền như sau:  
 “*a) Yêu cầu khách hàng cung cấp thông tin theo quy định tại Điều 4 Nghị định này và được quyết định gặp mặt trực tiếp hoặc không gặp mặt trực tiếp khách hàng khi lần đầu thiết lập mối quan hệ. Trường hợp không gặp mặt trực tiếp khách hàng, đối tượng báo cáo phải đảm bảo có các biện pháp, hình thức và công nghệ để nhận biết và xác minh khách hàng.”*  
 Về đối tượng báo cáo, Khoản 1 Điều 1 Nghị định số 87/2019/NĐ-CP ngày 14/11/2019 đã sửa đổi Khoản 2 và bổ sung Khoản 3 vào Điều 2 Nghị định số 116/2019/NĐ-CP ngày 04/10/2013 như sau:

*“2. Tổ chức, cá nhân khác liên quan đến phòng, chống rửa tiền, bao gồm:*

*a) Tổ chức cung ứng dịch vụ trung gian thanh toán;*

*b) Tổ chức, cá nhân nước ngoài hoặc người không có quốc tịch không hoạt động hoặc không sinh sống trên lãnh thổ Việt Nam nhưng có các giao dịch tài chính, giao dịch tài sản khác với tổ chức, cá nhân quy định tại khoản 1 Điều này.”*  
*“3. Tổ chức cung ứng dịch vụ trung gian thanh toán phải áp dụng các biện pháp phòng, chống rửa tiền theo quy định của pháp luật phòng, chống rửa tiền như đối với các đối tượng báo cáo là các tổ chức tài chính được quy định tại khoản 3 Điều 4 Luật Phòng, chống rửa tiền”.*  
 Như vậy, trung gian thanh toán cũng là đối tượng điều chỉnh của Luật Phòng, chống rửa tiền.  
 Trong pháp luật hình sự, tội rửa tiền được quy định tại Điều 251 và Điều 252 Bộ Luật Hình sự năm 1999. Điều 324 Bộ Luật Hình sự năm 2015, sau khi được sửa đổi, bổ sung bởi Khoản 122 Điều 1 Luật số 12/2017/QH14 ngày 20/6/2017 sửa đổi, bổ sung một số điều của Bộ Luật Hình sự năm 2015 quy định về tội Rửa tiền, nhưng không có khoản nào quy định về hành vi rửa tiền sử dụng công nghệ cao. Tuy nhiên, điểm đ, Khoản 2 Điều 254 quy định “Dùng thủ đoạn tinh vi, xảo quyệt” là tình tiết tăng nặng của tội Rửa tiền. Về điểm này, khoản 4 Điều 5 Nghị quyết số 03 của Hội đồng thẩm phán Tòa án Nhân dân tối cao ngày 24/5/2019 giải thích điểm đ, Khoản 2 Điều 324 như sau:  
 *“4. Dùng thủ đoạn tinh vi, xảo quyệt quy định tại điểm đ Khoản 2 Điều 324 của Bộ luật Hình sự là trường hợp người phạm tội sử dụng công nghệ cao, móc nối với người có chức vụ, quyền hạn trong cơ quan Nhà nước hoặc thủ đoạn gian dối, mánh khóe khác để tiêu hủy chứng cứ, che giấu hành vi phạm tội, gây khó khăn cho việc phát hiện, điều tra, xử lý tội phạm”.*

Như vậy, sử dụng công nghệ cao được coi là tình tiết tăng nặng khi thực hiện hành vi rửa tiền.    
 *So sánh với Chuẩn mực quốc tế liên quan đến rửa tiền sử dụng công nghệ cao, các quy định của pháp luật Việt Nam còn chưa bao quát được một số nội dung, cụ thể:*  
 *Một là,* còn thiếu vắng những quy định pháp luật điều chỉnh các giao dịch liên quan đến tiền ảo, tài sản ảo.    
 *Hai là,* pháp luật về phòng, chống rửa tiền chưa bao quát hết những yêu cầu trong các chuẩn mực quốc tế liên quan đến việc phòng ngừa hoạt động rửa tiền sử dụng công nghệ cao. Đối tượng điều chỉnh của Luật Phòng, chống rửa tiền hiện tại mới chỉ bao gồm những tổ chức tài chính được cấp phép thực hiện các hoạt động liên quan đến thanh toán, tiền điện tử.    
 *Ba là,* mặc dù pháp luật về phòng, chống rửa tiền có điều khoản quy định chung về công nghệ mới, nhưng chưa có quy định hay hướng dẫn cụ thể; trách nhiệm của các đối tượng báo cáo cũng chưa được đề cập cụ thể trong văn bản pháp luật hiện hành.  
 *Bốn là,* còn có những nội dung chưa thống nhất trong các văn bản hiện hành liên quan đến nội dung xử phạt vi phạm hành chính đối với những hành vi vi phạm pháp luật về phòng, chống rửa tiền trong các ngành khác nhau, một số hành vi được quy định trong pháp luật xử lý vi phạm hành chính của ngành này nhưng lại không được quy định trong pháp luật xử lý vi phạm hành chính của ngành khác.  
 *Năm là,* để thực hiện được những chuẩn mực quốc tế về chống rửa tiền liên quan đến công nghệ mới, cần hoàn thiện việc quy định trách nhiệm, quyền hạn của các đối tượng báo cáo; trách nhiệm, quyền lực của các cơ quan chức năng; những giải pháp mang tính bổ trợ như nguồn nhân lực, kỹ thuật, tài chính,… nhằm hỗ trợ cho các bên tuân thủ được các quy định của pháp luật một cách hiệu quả.  
 *Sáu là,* ý thức về tầm quan trọng của công tác bảo mật cơ sở dữ liệu, hệ thống thông tin của nhiều doanh nghiệp, người dân còn chủ quan, lơ là, dẫn đễn dễ bị tội phạm sử dụng công nghệ cao lạm dụng thực hiện hành vi phạm tội và rửa tiền.

**4. Một số đề xuất hoàn thiện pháp luật về phòng, chống rửa tiền sử dụng công nghệ cao**  
 Trong bối cảnh Cách mạng công nghiệp 4.0, cần phải tăng cường hoàn thiện công tác phòng, chống rửa tiền sử dụng công nghệ cao, đặc biệt là hoàn thiện một cách đồng bộ, thống nhất và nhanh chóng những văn bản pháp luật có liên quan, cụ thể:

*Thứ nhất,* bổ sung, sửa đổi Luật Phòng, chống rửa tiền năm 2012 và các nghị định, thông tư hướng dẫn kèm theo theo hướng: (i) bổ sung Khoản 3 Điều 4 theo hướng quy định “tổ chức tài chính” là những tổ chức thực hiện hoặc cung cấp dịch vụ cho những hoạt động như được liệt kê (không chỉ bao gồm những tổ chức được cấp phép); đồng thời, đưa hoạt động “cung ứng dịch vụ thanh toán, trung gian thanh toán, nền tảng công nghệ số, cung ứng dịch vụ liên quan tiền điện tử, tiền kỹ thuật số, tiền ảo, tài sản ảo” trong điểm đ của Khoản này để đưa các đối tượng cung ứng dịch vụ thanh toán hoặc cung ứng hạ tầng thanh toán cho các loại tài sản ảo, tiền ảo, tiền kỹ thuật số, thanh toán qua mạng phải báo cáo, cung cấp thông tin cho các cơ quan chức năng của Việt Nam; (ii) bổ sung quy định về việc những đối tượng báo cáo theo quy định của Luật Phòng, chống rửa tiền phải được cấp phép hoặc phải đăng ký nếu có hoạt động theo Khoản 3 và 4 Điều 4 Luật Phòng, chống rửa tiền với cơ quan quản lý; (iii) ban hành các hướng dẫn về các tiêu chí, chuẩn mực, công nghệ để làm cơ sở cho các đối tượng báo cáo thực hiện nội dung “phải đảm bảo có các biện pháp, hình thức và công nghệ để nhận biết và xác minh khách hàng” nếu không gặp mặt khách hàng trực tiếp theo Khoản 1 Điều 8 Nghị định 116/2013/NĐ-CP được bổ sung, sửa đổi bởi Nghị định số 87/2019/NĐ-CP; (iv) bổ sung điều khoản quy định về 20 loại tội phạm nguồn phù hợp với chuẩn mực quốc tế.

*Thứ hai,* bổ sung, sửa đổi, ban hành mới các văn bản pháp luật liên quan để đảm bảo tính thống nhất với pháp luật về phòng, chống rửa tiền theo hướng: (i) nghiên cứu, xem xét, sửa đổi, bổ sung Bộ Luật Hình sự để quy định thống nhất hành vi rửa tiền trong 01 điều luật; (ii) nghiên cứu, chỉnh sửa điều khoản quy định về trách nhiệm hình sự của pháp nhân để đảm bảo không chỉ pháp nhân thương mại, mà pháp nhân nói chung phải chịu trách nhiệm hình sự về tội rửa tiền; (iii) nghiên cứu, bổ sung, sửa đổi Điều 105 Bộ Luật Dân sự theo hướng quy định tiền, tài sản bao gồm cả tiền ảo, tài sản ảo; (iv) nghiên cứu, bổ sung, sửa đổi pháp luật nội dung liên quan đến tiền ảo, tài sản ảo; bao gồm cả những quy định về việc quản lý tiền ảo, tài sản ảo; chức năng, nhiệm vụ của các cơ quan có thẩm quyền; trách nhiệm của các tổ chức, cá nhân cung ứng dịch vụ liên quan đến tiền ảo, tài sản ảo; (v) nghiên cứu, bổ sung điều khoản trong pháp luật tố tụng hình sự về trách nhiệm của các cơ quan điều tra trong việc điều tra tài chính song song, có nghĩa là, điều tra tội phạm rửa tiền song song với điều tra các tội phạm nguồn; (vi) nghiên cứu, bổ sung điều khoản quy định về việc tịch thu dân sự, bao gồm cả việc tịch thu các tài sản ảo, tiền ảo theo chuẩn mực quốc tế; (vii) nghiên cứu, ban hành mới Nghị định xử lý vi phạm hành chính trong lĩnh vực phòng, chống rửa tiền, chống tài trợ khủng bố để áp dụng thống nhất trong tất cả các ngành.  
 *Thứ ba,* tăng cường những biện pháp hỗ trợ cho việc triển khai quy định của pháp luật, cụ thể: (i) nghiên cứu việc thiết lập trong Cục Phòng, chống rửa tiền một bộ phận chuyên về công nghệ cao với chức năng, nhiệm vụ cụ thể để có thể chủ động lần theo dấu vết được các khoản tiền ảo, tài sản ảo trong các nền tảng công nghệ mới; (ii) tăng cường đào tạo đội ngũ cán bộ của các cơ quan bộ, ngành, đặc biệt là cán bộ thuộc đơn vị tình báo tài chính về khả năng phân tích các giao dịch liên quan công nghệ mới và các cán bộ điều tra, truy tố, xét xử những tội phạm liên quan công nghệ cao; tăng cường đào tạo cho các đối tượng báo cáo giúp họ có thể nhận biết dễ dàng hơn những giao dịch có dấu hiệu đáng ngờ liên quan đến hành vi rửa tiền sử dụng công nghệ cao.  
 Cuộc cách mạng công nghệ 4.0 mang lại những lợi ích to lớn cho xã hội và nền kinh tế nói chung, nhưng cũng đặt ra nhiều thách thức cho chính các cơ quan chức năng trong việc bảo vệ những thành tựu đó, ngăn chặn tội phạm lạm dụng chính cuộc cách mạng này để thực hiện các hành vi phạm tội, trong đó có hành vi rửa tiền. Việc hoàn thiện khuôn khổ pháp lý liên quan đến phòng, chống rửa tiền sử dụng công nghệ cao là việc làm cấp bách do tính vượt trội về mặt thời gian của công nghệ số.

\_\_\_\_\_\_\_\_\_\_\_\_

1. https://baodautu.vn/toi-pham-cong-nghe-cao-bung-phat-tro-lai-d101631.html

2. https://www.cybersecurityintelligence.com /blog/cyber-criminals-have-ingenious-money-laundering-methods-3280.html

3. Báo cáo việc rà soát, đánh giá toàn diện thực trạng pháp luật, thực tiễn về tài sản ảo, tiền ảo ở Việt Nam và quốc tế; nhận diện, đề xuất các định hướng hoàn thiện; tr.94. Bộ Tư pháp - 2018

4. Theo số liệu của Cục PCTPCNC-NCA cung cấp tại Hội thảo do BTP tổ chức tại TP.HCM ngày 25/5/2018

5. Báo cáo việc rà soát, đánh giá toàn diện thực trạng pháp luật, thực tiễn về tài sản ảo, tiền ảo ở Việt Nam và quốc tế; nhận diện, đề xuất các định hướng hoàn thiện; tr.95. Bộ Tư pháp-2018

6. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

7. https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

8. https://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets.html?hf=10&b=0&s=desc(fatf\_releasedate).  
  
**ThS. Nguyễn Thị Thúy Ngọc**  
  
*Theo Tạp chí Ngân hàng số 14/2020*