



Original Article

# Safe Harbor Mechanism for Intermediary Service Providers in the World and Recommendations for Improving Vietnamese Law

Bui Dinh Nghia\*

*Academy of Justice, No. 9 Tran Vy, Mai Dich, Cau Giay, Hanoi*

Received 11 March 2023

Revised 18 August 2023; Accepted 15 December 2023

**Abstract:** Intermediary Service Providers (ISPs) are entities that play a crucial role in the modern world, providing Internet services to users. However, violations of the law by users are very common and not only negatively affect cyberspace but also cause ISPs to face legal issues. To address this problem, numerous countries have applied Safe Harbor to protect ISPs from users' violations and remove these violations from the Internet environment. This paper focuses on reviewing the regulations relating to Safe Harbor in the world and evaluating the potential to apply this mechanism to improve Vietnamese law.

**Keywords:** Safe Harbor; ISPs; exempt from liability; violation.

---

\* Corresponding author.

E-mail address: [hlu.4318.dinhnghia@gmail.com](mailto:hlu.4318.dinhnghia@gmail.com)

<https://doi.org/10.25073/2588-1167/vnuls.4545>

# Cơ chế Safe Harbor cho nhà cung cấp dịch vụ trung gian trên internet trên thế giới và gợi ý hoàn thiện pháp luật Việt Nam

Bùi Đình Nghĩa\*

*Học viện Tư pháp, số 9 Trần Vỹ, Mai Dịch, Cầu Giấy, Hà Nội*

Nhận ngày 11 tháng 3 năm 2023

Chỉnh sửa ngày 18 tháng 8 năm 2023; Chấp nhận đăng ngày 15 tháng 12 năm 2023

**Tóm tắt:** Nhà cung cấp dịch vụ trung gian trên Internet (Intermediary Service Providers, viết tắt “ISPs”) là các thực thể có vai trò quan trọng trong thế giới hiện đại, thực hiện cung cấp các dịch vụ Internet cần thiết cho người sử dụng. Tuy nhiên, tình trạng vi phạm pháp luật của người dùng trên các dịch vụ của các đơn vị này diễn ra rất phổ biến, không chỉ làm ảnh hưởng tiêu cực đến không gian mạng mà còn khiến các đơn vị cung cấp dịch vụ trung gian đối mặt với các rắc rối pháp lý. Để giải quyết tình trạng này, nhiều quốc gia trên thế giới đã áp dụng cơ chế Safe Harbor (Cảng an toàn) để bảo vệ các nhà khai thác khỏi vi phạm của người dùng, đồng thời loại bỏ vi phạm khỏi môi trường mạng. Bài viết này tập trung xem xét các quy định liên quan đến cơ chế Safe Harbor trên thế giới, đồng thời đánh giá tiềm năng áp dụng cơ chế này tại Việt Nam nhằm đưa ra một số đề xuất hoàn thiện pháp luật Việt Nam.

*Từ khóa:* Safe Harbor; ISPs; miễn trừ trách nhiệm; vi phạm pháp luật.

## 1. Khái quát về cơ chế Safe Harbor

### 1.1. Khái quát chung

Internet ngày càng đóng vai trò quan trọng trong cuộc sống của con người và các hoạt động của con người như kinh doanh, xây dựng quan hệ,... trên mạng đều được hỗ trợ bởi các nhà cung cấp dịch vụ trung gian thông qua các nền tảng của họ như Facebook, LinkedIn, các trang thương mại điện tử. Trong số các hoạt động này, bên cạnh nhiều chủ thể tuân thủ pháp luật, có rất nhiều cá nhân lợi dụng những dịch vụ này nhằm thực hiện hành vi vi phạm pháp luật trên nhiều lĩnh vực: hình sự, dân sự, sở hữu trí tuệ,... Hiện nay, để xử lý và ngăn chặn những hành vi phạm pháp luật trên không gian mạng, bên cạnh việc xử phạt trực tiếp những chủ thể vi phạm bằng chế tài hình sự, hành chính, một số trường hợp các

ISPs có thể đối mặt với trách nhiệm pháp lý ở mức độ khác nhau căn cứ trên hậu quả do để xảy ra vi phạm gây ra bởi người dùng như vụ việc giữa VNG và Tiktok ở Việt Nam [1].

Tuy nhiên, cách giải quyết xử phạt nhà cung cấp dịch vụ trung gian Internet không phải một giải pháp tối ưu để giải quyết vấn đề vi phạm đang tràn lan. Hiện nay, một số quốc gia đã đưa ra một cơ chế pháp lý là Safe Harbor (tạm dịch là Cảng an toàn). Về cơ bản, đây là một cơ chế miễn trừ trách nhiệm cho các nhà cung cấp dịch vụ trung gian trên Internet với các hành vi vi phạm quyền tác giả do người dùng thực hiện. Cơ chế này lần đầu tiên xuất hiện trong Đạo luật Bản quyền thiên niên kỷ kỹ thuật số (Digital Millennium Copyright Act) năm 1998 của Hoa Kỳ và sau đó được phát triển tại nhiều quốc gia khác. Theo các nhà làm luật tại Hoa Kỳ, cơ chế

\* Tác giả liên hệ.

Địa chỉ email: hlu.4318.dinhnghia@gmail.com

<https://doi.org/10.25073/2588-1167/vnuls.4545>

này ra đời nhằm đảm bảo xây dựng một hành lang pháp lý chắc chắn cho các Nhà cung cấp dịch vụ trung gian và trực tuyến; đồng thời thiết kế để các chủ sở hữu bản quyền có một cơ chế giải quyết tranh chấp nhanh chóng [2].

## 1.2. Đặc điểm

*Thứ nhất*, về đối tượng, cơ chế Safe Harbor bảo vệ những nhà cung cấp dịch vụ trung gian trên Internet. Nhà cung cấp dịch vụ trung gian trên Internet được hiểu là những đơn vị kết nối hoặc tạo điều kiện kết nối giữa các bên trên Internet, mà họ đóng vai trò là người cấp quyền truy cập, lưu trữ, truyền và tạo lập nội dung, sản phẩm và dịch vụ hoặc cung cấp các dịch vụ Internet cho bên thứ ba [3]. Những đơn vị này được coi là “người gác cổng” để tiếp cận với thế giới Internet [4], do đó, sự phát triển và hoạt động bình thường của những đơn vị này đóng một vai trò quan trọng trong thế giới hiện đại. Pháp luật Việt Nam chưa có định nghĩa cụ thể về những đơn vị này, nhưng hiện nay đã có những dạng hoạt động của đơn vị này cung cấp các dịch vụ trên như sau: dịch vụ viễn thông, dịch vụ Internet, dịch vụ mạng xã hội trực tuyến, dịch vụ tìm kiếm thông tin số, dịch vụ cho thuê chỗ lưu trữ thông tin số bao gồm cả dịch vụ cho thuê chỗ lưu trữ thông tin điện tử. Có thể kể tới một số đại diện tiêu biểu như VNPT, FPT, VNG, Viettel ở Việt Nam; hay Youtube, Facebook, Google, Alibaba, Baidu,... trên thế giới.

*Thứ hai*, cơ chế Safe Harbor bảo vệ các nhà cung cấp dịch vụ trên Internet khỏi các hành vi vi phạm của người dùng. Người sử dụng dịch vụ - đối tượng hướng tới của các nhà cung cấp, là người trực tiếp trải nghiệm, sử dụng dịch vụ theo cách riêng. Bên cạnh những hành vi tuân thủ pháp luật, vẫn còn nhiều cá nhân lợi dụng để thực hiện những hành vi vi phạm pháp luật như phát tán, chia sẻ nhạc xâm phạm bản quyền thông qua giao thức mạng ngang hàng [5], hay đăng tải video trái phép [6], bán hàng giả mạo, kém chất lượng [7],... Với việc đang ngày càng nhiều người được tiếp cận với Internet hiện nay, thì việc kiểm soát hành vi sử dụng dịch vụ của người dùng là rất khó khăn, khó đảm bảo loại bỏ được

tất cả các vi phạm của người dùng trên nền tảng dịch vụ của các ISPs cung cấp. Hướng đi này là nhằm giúp các ISPs tránh phải chịu các “trách nhiệm gián tiếp” (vicarious liability), Theo đó, ý nghĩa của trách nhiệm này yêu cầu ISPs cần phải chứng minh rằng đã cố gắng loại bỏ các hành vi vi phạm và không nhận được bất cứ lợi ích phát sinh nào từ hành vi vi phạm của người dùng. Nội dung về hưởng lợi ích phát sinh này đã được nhấn mạnh trong phán quyết của Tòa án Hoa Kỳ trong vụ việc A&M Records, Inc. v. Napster, Inc [5]. Trong vụ kiện, Napster, một đơn vị cung cấp dịch vụ chia sẻ nhạc ngang hàng trên Internet đã hưởng lợi bằng việc thu hút người dùng mới từ việc tạo thuận lợi cho các vi phạm bản quyền của người dùng về các tác phẩm âm nhạc, trong đó có các sản phẩm của A&M Record. Vì vậy, Tòa án quyết định rằng Napster phải chịu trách nhiệm gián tiếp bởi họ hưởng lợi gián tiếp từ vi phạm của người dùng cũng như mặc dù có khả năng ngăn chặn, hạn chế vi phạm nhưng đã không thực hiện nó. Do đó, cơ chế Safe Harbor được xây dựng như một tấm khiên bảo vệ các công ty công nghệ trước các vi phạm gây ra bởi người dùng của mình cũng như đảm bảo rằng các công ty công nghệ sẽ chú trọng hơn vào việc kiểm soát người dùng sử dụng dịch vụ lành mạnh, tuân thủ pháp luật.

*Thứ ba*, các nhà cung cấp dịch vụ trung gian trên Internet cần tuân thủ một số điều kiện chung để đảm bảo được miễn trừ theo cơ chế Safe Harbor. Về các điều kiện này, pháp luật trên thế giới có sự khác nhau ở một số điểm, nhưng nhìn chung, sẽ có một vài điều kiện cần tuân thủ như sau:

- Không can thiệp vào quá trình sử dụng dịch vụ của người dùng; trừ trường hợp vi phạm tiêu chuẩn của nhà cung cấp và pháp luật;

- Xoá bỏ/ vô hiệu hoá thông tin vi phạm trong thời gian ngắn khi nhận được báo cáo về thông tin vi phạm từ người dùng.

Quy định đảm bảo loại trừ hoặc hạn chế trách nhiệm đóng góp (contributory liability) của các ISPs. Lý thuyết về “trách nhiệm đóng góp” chỉ ra rằng, các ISPs sẽ phải chịu các ràng buộc pháp lý bất lợi nếu họ biết hoặc có bất cứ hành

động/không hành động nào mà có thể dẫn tới các vi phạm hoặc tạo điều kiện để người dùng thực hiện các vi phạm trên nền tảng dịch vụ của họ cung cấp. Vì vậy, các điều kiện trên đóng vai trò quan trọng trong việc thực hiện cơ chế Safe Harbor tại Hoa Kỳ, Liên minh châu Âu nhằm duy trì vị thế “thụ động/trung lập” của các nhà cung cấp dịch vụ trung gian trên Internet, đảm bảo họ sẽ chỉ cung cấp dịch vụ đơn thuần và tách bạch trách nhiệm trước bất cứ vi phạm nào của người dùng trên nền tảng của họ.

## 2. Cơ chế Safe Harbor trên thế giới và đánh giá tính khả thi khi áp dụng tại Việt Nam

### 2.1. Hoa Kỳ

Safe Harbor là một cơ chế bắt nguồn từ Hoa Kỳ, được quy định tại Chương II “Giới hạn trách nhiệm vi phạm bản quyền trực tuyến” trong Đạo luật Bản quyền Thiên niên kỷ Kỹ thuật số (Digital Millennium Copyright Act - DMCA) trước hết nhằm bảo vệ sự phát triển của các công ty, tập đoàn công nghệ Mỹ và quyền sở hữu trí tuệ của các chủ sở hữu.

#### 2.1.1. Nguồn gốc

Cơ chế Safe Harbor lần đầu được đưa ra khi có nhiều trường hợp vi phạm pháp luật sở hữu trí tuệ trên các dịch vụ số của các công ty công nghệ Mỹ. Để xác định các lỗi này, bên cạnh chủ thể vi phạm chính, Toà án Hoa Kỳ sẽ phải phát hiện ra người vi phạm thứ cấp, là chủ thể mà “có kiến thức về hoạt động vi phạm, gây ra hoặc góp phần quan trọng vào hành vi vi phạm” [8]. Nếu các công ty cung cấp dịch vụ trung gian trên mạng này được xác định là “có quyền và khả năng giám sát hoạt động vi phạm và cũng có lợi ích tài chính trực tiếp tới các hoạt động vi phạm đó” thì có thể đối mặt với các trách nhiệm pháp lý. Điều này đã được thể hiện thông qua phán quyết của Toà án Tối cao Hoa Kỳ tại vụ kiện Metro-Goldwyn-Mayer Studios, Inc v Grokster như sau:

“Ai phân phối thiết bị với mục đích quảng bá việc sử dụng thiết bị để vi phạm bản quyền, thể hiện bằng cách diễn đạt rõ ràng hoặc các cách tích cực khác thể hiện thúc đẩy hành vi vi phạm,

sẽ phải chịu trách nhiệm về các hành vi vi phạm do bên thứ ba gây ra,...” [9].

Hiện nay, những hành vi của những người dùng trên không gian mạng rất đa dạng từ nội dung đến cách thức thể hiện, không ít những hành vi trong đó vô tình hoặc cố ý vi phạm các quy định của pháp luật, không chỉ riêng pháp luật sở hữu trí tuệ. Do đó, qua phán quyết trên, có thể thấy các nhà cung cấp dịch vụ trung gian trên Internet là những đối tượng có đầy đủ yếu tố để chịu các trách nhiệm pháp lý gây ra bởi người dùng của họ nếu không có được bảo vệ từ pháp luật. Vì vậy, cơ chế Safe Harbor ra đời đã góp phần bảo vệ những công ty công nghệ Mỹ khỏi việc gánh chịu những trách nhiệm pháp lý; và đã đóng góp không nhỏ vào sự phát triển của các công ty công nghệ của Hoa Kỳ.

#### 2.1.2. Quy định về cơ chế Safe Harbor trong Đạo luật Bản quyền Thiên niên kỷ Kỹ thuật số

Không phải tất cả ISPs đều được bảo vệ bởi cơ chế Safe Harbor, mà chỉ những chủ thể đáp ứng các điều kiện là một “nhà cung cấp dịch vụ trung gian” theo DMCA thì mới được hưởng sự miễn trừ. Dựa vào cách thức hoạt động, DMCA xác định có bốn chủ thể được giới hạn trách nhiệm trong các vấn đề bản quyền, gồm: Cung cấp đường dẫn; Lưu trữ hệ thống; Lưu trữ thông tin trên mạng hoặc hệ thống theo điều hướng người dùng; và Công cụ định vị thông tin và phải tuân thủ các điều kiện khác nhau:

##### i) Nhà cung cấp dịch vụ truyền thông tin mạng

Đây là chủ thể đóng vai trò truyền tải dữ liệu kỹ thuật số từ một điểm trên mạng tới một điểm khác cho người khác (Transitory Digital Network Communications), thực hiện hoạt động truyền tải dữ liệu đơn thuần và không có làm thay đổi nội dung thông tin truyền tải. Và để bảo vệ các nhà cung cấp này, pháp luật Hoa Kỳ đặt ra yêu cầu như sau:

- Việc truyền tải dữ liệu phải diễn ra thông qua một quy trình kỹ thuật tự động mà không có sự can thiệp của nhà cung cấp.

- Người nhận được đảm bảo vô danh.

- Các bản sao trung gian, tạm thời được lưu trữ trên hệ thống hoặc mạng của nhà cung cấp

không được phép truy cập cho bất kỳ ai khác ngoài người nhận được chỉ định và các bản sao không được lưu trên hệ thống một cách lâu hơn mức cần thiết.

- Nhà cung cấp không được sửa đổi nội dung của tài liệu trực tuyến.

#### ii) Lưu trữ hệ thống

Đối tượng tiếp theo nhận được sự bảo vệ của cơ chế Safe Harbor là Lưu trữ hệ thống (System Caching), một dạng dịch vụ lưu trữ tạm thời và tự động các bản sao trong một thời gian giới hạn của tài liệu, được tải lên hay cung cấp bởi người dùng và được truyền tới bên khác. Dịch vụ này khác với đối tượng đầu tiên là nhà cung cấp được phép lưu trữ lại bởi một quá trình kỹ thuật tự động (an automatic technical process) các tập tin tài liệu, âm thanh, nội dung hình ảnh trong một khoảng thời gian lâu hơn cho tới khi người nhận tiếp cận với tài liệu. Điều này khiến các Lưu trữ hệ thống có khả năng nhận biết hoặc hiểu về các nội dung được truyền tải thông qua trí tuệ nhân tạo, hoặc các công nghệ mà ISPs phát triển. Do đặc điểm vận hành khác nhau, các ISPs cung cấp dịch vụ Lưu trữ hệ thống sẽ phải chịu một số điều kiện tại Điều 512 (b)(2) mang tính nghiêm ngặt hơn so với ISPs cung cấp dịch vụ truyền thông tin mạng. Đồng thời, họ phải thực hiện các biện pháp can thiệp trực tiếp vào quá trình sử dụng dịch vụ của người dùng nếu như nội dung đó vi phạm pháp luật. Cụ thể:

- ISPs không được sửa đổi nội dung của tài liệu, không được can thiệp vào tài liệu.

- Giới hạn quyền truy cập dữ liệu lưu trữ, vốn dành cho người truyền và nhận thông tin;

- Phải nhanh chóng phản hồi để xóa hoặc vô hiệu hoá quyền truy cập vào tài liệu mà bên thứ ba cung cấp khi bên thứ ba tạo ra hoặc thực hiện mà không cho phép chủ sở hữu bản quyền thông qua việc thông báo về vi phạm.

#### iii) Lưu trữ thông tin trên mạng hoặc hệ thống theo điều hướng người dùng

Đối tượng thứ ba hưởng cơ chế Safe Harbor theo DMCA của Hoa Kỳ là các ISPs cung cấp dịch vụ lưu trữ thông tin trên mạng hoặc hệ thống điều hướng của người dùng (Information

residing on systems or networks at direction of users). Ở đây, thuật ngữ “residing” (trú ngụ/lưu trú) ngụ ý về thời gian lưu trữ tài liệu dài hơn so với hai dịch vụ của ISPs đã đề cập. Tương tự như System Caching, ISPs sẽ có khả năng tốt hơn trong việc nắm các thông tin, học hỏi, cập nhật thay đổi từ những thông tin được tải lên trên mạng nên phải đáp ứng một số yêu cầu như sau:

- Không có các kiến thức nào, tài liệu nào trên hệ thống mạng của họ là vi phạm.

- Trong trường hợp không có nhận thức và thông tin về tài liệu vi phạm, phải hành động khẩn cấp để xóa thông tin hoặc vô hiệu hóa quyền truy cập vào tài liệu.

- Không nhận lợi ích tài chính trực tiếp từ hoạt động vi phạm đối với thông tin.

- Áp dụng những quy trình thông báo và gỡ bỏ cho người sở hữu bản quyền khi muốn khai báo về hành vi vi phạm.

#### iv) Công cụ định vị thông tin

Cuối cùng, Safe Harbor bảo vệ những ISPs cung cấp dịch vụ liên quan đến công cụ định vị thông tin của người dùng (Information Location Tools). Đây là các dịch vụ cung cấp cho người dùng quyền truy cập vào các trang web chứa các tài liệu vi phạm bằng cách sử dụng các công cụ định vị thông tin như siêu văn bản, thư mục, v.v. Các điều kiện để áp dụng Safe Harbor cho các ISPs này cũng tương tự như đối với ISPs thứ ba, cung cấp dịch vụ Lưu trữ hệ thống, như không thu lợi ích tài chính, áp dụng quy trình thông báo và gỡ bỏ.

Nhìn chung, các điều kiện trên đang loại bỏ các hành vi can thiệp vào thông tin, tài liệu của người dùng của ISPs. Khi đó, họ sẽ đảm bảo đúng bản chất là vai trò trung gian (intermediaries), chỉ thực hiện cung cấp dịch vụ cho người sử dụng và không can thiệp nội dung. Việc can thiệp chỉ xảy ra khi người dùng đã vi phạm quy định pháp luật thông qua cơ chế “thông báo và gỡ bỏ” (Notice and takedown), nhằm không để cho các hành vi vi phạm này được tiếp diễn và lan truyền trên không gian mạng. Điều này giúp các ISPs thúc đẩy cải tiến kỹ thuật để hiện đại hoá và làm đơn giản và hiệu quả quá trình xử lý các vi phạm của

người dùng, tránh phải đối mặt với các rắc rối pháp lý.

### 2.1.3. Thủ tục “Thông báo và gỡ bỏ”

Cốt lõi của cơ chế Safe Harbor nằm ở việc các ISPs sẽ xử lý như thế nào về các hành vi xâm phạm bản quyền trên không gian mạng được xác định theo DMCA. Theo đó, các nhà làm luật thiết lập một quy trình, được gọi là “Thông báo và gỡ bỏ”, để các ISPs có thể kịp thời ngăn chặn các hành vi vi phạm trước khi vi phạm trở nên nghiêm trọng hơn. Theo thủ tục “Thông báo và gỡ bỏ”, chủ sở hữu bản quyền của các thông tin bị vi phạm bản quyền trên mạng sẽ phải thực hiện thông báo cho các ISPs, gồm các thông tin cơ bản như tài sản bị vi phạm, ở dạng vật lý hay dữ liệu điện tử (ảnh, văn bản, file ghi âm,...), thẩm quyền phản ánh là chủ sở hữu, hay người được uỷ quyền có văn bản có chữ ký hợp pháp. Khi tiếp nhận thông tin, ISPs sẽ khẩn trương xác minh, thực hiện gỡ bỏ/vô hiệu hoá truy cập vào các tài khoản, nội dung thông tin vi phạm bản quyền.

Các nhà làm luật đặt ra yêu cầu các công ty công nghệ cung cấp dịch vụ này đặt ra một cơ quan để tiếp nhận các phản hồi từ các chủ sở hữu bản quyền. Cơ quan này có thể là một phần của ISPs đó, hoặc một bên thứ ba được quyền tiếp nhận các phản hồi này, như các Trung tâm trợ giúp, Trung tâm khiếu nại và trợ giúp trên một số website. Theo Điều 512 (c) (2), các cơ quan này phải cung cấp thông tin như tên, địa chỉ, số điện thoại, địa chỉ email và phải gửi các thông tin này cho cơ quan quản lý về bản quyền để họ tiếp nhận đầu mối làm việc. Ở đây, nhà làm luật đã san sẻ trách nhiệm phát hiện các sai phạm cho chủ sở hữu bản quyền như một cách để giảm trách nhiệm của các nhà cung cấp dịch vụ trung gian trên Internet. Như đã giải thích, việc đặt trách nhiệm giám sát vi phạm cho các ISPs sẽ khó phát huy hiệu quả bởi sự phát triển của Internet hiện nay cùng với sự gia tăng không ngừng của người dùng trên rất nhiều các nền tảng nên các ISPs khó có thể đảm bảo nguồn lực để có thể rà soát và loại bỏ các nội dung trái quy định pháp luật sở hữu trí tuệ.

Có thể thấy, đối với cơ chế Safe Harbor, tiêu chí “có nhận thức” là một yếu tố quan trọng để xem xét đến trách nhiệm của ISPs và việc cung cấp thông tin cho ISPs về hành vi vi phạm bản quyền được hiểu như cung cấp kiến thức cho ISPs về những hành vi vi phạm, từ đó, ISPs sẽ có trách nhiệm ngăn chặn những hành vi tương tự trong tương lai. Đặt trong bối cảnh tại Hoa Kỳ, khi đạo luật này ra đời, chủ sở hữu bản quyền hợp tác với ISPs, tức là chủ sở hữu bản quyền cung cấp các phát hiện về hành vi vi phạm qua các đơn vị tiếp nhận thông tin, ISPs được coi là đã nhận thức về hành vi vi phạm, và sẽ có nghĩa vụ phải chặn các thông tin xâm phạm quyền sở hữu trí tuệ trong lần thông báo của chủ sở hữu và trong các lần khác trong tương lai. Quan điểm này một lần nữa được củng cố thông qua vụ án *Viacom International Inc. v Youtube, Inc* [6]. Theo đó, Viacom, một đơn vị sản xuất phim và chương trình truyền hình đã cáo buộc Youtube vi phạm bản quyền với các đoạn clip của hãng này bị đăng lên mà không có sự cho phép từ 2005 tới 2008, và yêu cầu bồi thường. Tuy nhiên, theo Toà án, DMCA thiết lập sự miễn trách nhiệm mà theo đó, ISPs phải có nhận thức cụ thể về hành vi vi phạm, mới có thể thực hiện gỡ bỏ thông tin vi phạm theo thủ tục “Thông báo và gỡ bỏ”. Trong vụ việc này, Toà án không có bằng chứng nào về việc Youtube thực sự biết về các vi phạm của người dùng hay “tham gia, thúc đẩy và xúi giục” người dùng đăng tải các video của Viacom, nên không thể kết luận rằng Youtube tham gia vào hành vi vi phạm và thực tế Youtube cũng đã gỡ xuống rất nhiều video của Viacom vào năm 2007. Vì vậy, Toà đã bác bỏ các so sánh của Viacom về vụ *Metro-Goldwyn-Mayer Studios Inc. v. Grokster* và tuyên bố Youtube đã tuân thủ đúng quy định tại Điều 512 (c) của DMCA.

Sau quá trình nhận thông tin và xác minh, ISPs xoá thông tin vi phạm phải thông báo ngay cho người dùng, tức là người bị xác định là xâm phạm bản quyền, rằng họ đã xoá hoặc vô hiệu hoá quyền truy cập thông tin. Ngược lại, ISPs phải phục hồi trạng thái của thông tin hoặc ngừng vô hiệu hoá quyền truy cập nếu nhận được thông báo phản đối từ người dùng về việc xoá thông tin là không đúng.

## 2.2. Liên minh châu Âu

### 2.2.1. Nguồn gốc

Đầu thế kỷ 21, trong bối cảnh sự xuất hiện và phát triển của thương mại điện tử, những nhà lập pháp châu Âu nhìn nhận lĩnh vực này cần được điều chỉnh bởi một hành lang pháp lý thống nhất trong toàn khối, đồng thời để củng cố sự phát triển tự do của thị trường thương mại mới này giữa các quốc gia thành viên. Những dự thảo ban đầu xác định trách nhiệm của những nhà cung cấp dịch vụ trung gian là rất quan trọng bởi họ liên quan trực tiếp tới sự phát triển của các dịch vụ xuyên biên giới, bao gồm cả lưu và chuyển dữ liệu. Do đó, Chỉ thị số 2000/31/EC về Thương mại điện tử (E- Commerce Directive hay “ECD”) ra đời, nhằm đưa ra một hướng đi chung cho sự phát triển của thương mại điện tử trong khối và có những quy định đề cập trực tiếp tới hoạt động của các ISPs và những cơ chế đặc thù dành cho họ. Tuy nhiên, ECD là một Chỉ thị có phạm vi điều chỉnh khá mở, nên đã để ngỏ khả năng toà án và chính quyền yêu cầu các ISPs chấm dứt hoặc ngăn chặn hành vi vi phạm và thẩm quyền xác định tính hợp pháp của thông tin đăng tải trên các dịch vụ của ISPs [10].

### 2.2.2. Quy định Safe Harbor trong Chỉ thị 2000/31 về Thương mại Điện tử

ECD là một chỉ thị có phạm vi điều chỉnh khá mở. Khái niệm “Nhà cung cấp dịch vụ trung gian” có phạm vi rất rộng, được hiểu chung là nhà cung cấp dịch vụ xã hội thông tin (Information Society Service Providers), hay được gọi chung là gọi “Online Intermediaries” [11], là bên cung cấp bất kỳ dịch vụ nào có trả thù lao theo yêu cầu của cá nhân và được thực hiện bằng phương thức điện tử. Theo khái niệm này, những đơn vị là ISPs chịu sự điều chỉnh của ECD là rất rộng, không chỉ giới hạn trong lĩnh vực sở hữu trí tuệ, mà còn bao trùm lên các vấn đề hình sự, quyền riêng tư, v.v. [12]. Đồng thời, ISPs vẫn sẽ tuân thủ một số điều kiện để có thể nhận được sự miễn trừ theo ECD, cụ thể:

#### i) Đường truyền dẫn thuần túy

Đối tượng đường truyền dẫn thuần túy (Mere Conduit) được quy định tại Điều 12, gồm hai

nhóm cơ bản: i) truyền dẫn trong mạng thông tin nội bộ cung cấp bởi người nhận dịch vụ; và ii) cấp quyền truy cập vào một mạng truyền thông. Theo mô hình này, thông tin được chuyển đi trong một mạng máy tính, sau đó được lưu trữ lại trong một thời gian ngắn trên bất cứ máy nào, và cách hoạt động tương tự như một đường truyền dẫn đơn thuần, tương tự như Nhà cung cấp dịch vụ Truyền thông tin mạng của Hoa Kỳ.

Các yêu cầu đối với ISPs cung cấp dịch vụ dẫn truyền như sau: i) Không phải là người khởi xướng việc chia sẻ thông tin; ii) không lựa chọn/thay đổi người nhận thông tin; iii) không lựa chọn hoặc chỉnh sửa thông tin chia sẻ.

#### ii) Lưu trữ tạm thời trên hệ thống

Lưu trữ tạm thời trên hệ thống (Caching) được quy định tại Điều 13. Đây là hoạt động cung cấp dịch vụ của ISPs trong trường hợp thông tin được tự động lưu trữ tạm thời và trung gian trên mạng với mục đích là đảm bảo hiệu quả hơn trong việc truyền thông tin đi tới những người khác. Bằng cách này, ISPs cho phép các tài liệu, tập tin nhạc, ... được lưu trữ trong một thời hạn hợp lý để để chủ sở hữu có thể chia sẻ nhiều lần và hiệu quả trong quá trình truyền thông tin. Vì vậy, những ISPs cung cấp dịch vụ lưu trữ tạm thời trên hệ thống sẽ phải đáp ứng yêu cầu như:

- Không sửa đổi thông tin trong quá trình lưu trữ và truyền thông tin;

- Đảm bảo quyền tiếp cận thông tin theo yêu cầu của người chủ sở hữu thông tin;

- Tạo điều kiện cho chủ sở hữu cập nhật đầy đủ thông tin;

- Không sử dụng những lợi thế công nghệ, được ngành công nghệ chấp nhận và sử dụng rộng rãi, để lấy dữ liệu và sử dụng thông tin;

- Phải hành động ngay lập tức khi thông tin tải lên sai lệch, không chính xác, đã vô hiệu hoá hoặc có lệnh vô hiệu hoá bởi cơ quan nhà nước.

Những quy định trên yêu cầu ISPs vừa phải đảm bảo quyền tiếp cận của người dùng, và cũng không được tự ý thay đổi quyền truy cập của những đối tượng mà chủ sở hữu thông tin cho phép tiếp cận. Đây là nội dung phổ biến trong

các đạo luật về quyền riêng tư và an toàn thông tin mạng của châu Âu, để đảm bảo người dùng được bảo vệ trên môi trường mạng.

iii) Lưu trữ trên máy chủ

Lưu trữ trên máy chủ (Hosting), tương tự với Lưu trữ thông tin trên mạng theo DMCA, cung cấp cho người dùng không gian lưu trữ trên mạng ổn định trong thời gian dài. Các nhà làm chính sách của châu Âu cũng lo ngại việc lưu giữ tài liệu, thông tin, v.v trên không gian mạng trong thời gian dài sẽ tạo điều kiện để các công ty công nghệ có thể tiếp cận, sử dụng, và cải tiến các thông tin sẵn có đó, để sở hữu cho riêng mình và trục lợi, nên đã đặt ra các điều kiện họ phải tuân thủ. Đó là:

- Nhà cung cấp không nhận thức được các kiến thức, thông tin mà tại đó vi phạm xảy ra, hoặc gây ra thiệt hại;

- Nhà cung cấp, khi nhận thức được sự việc đã hành động kịp thời để loại bỏ hoặc vô hiệu hoá việc truy cập vào thông tin.

Theo đó, điều kiện đầu tiên xác định việc họ sẽ không phải chịu trách nhiệm khi họ không hề biết tới các thông tin vi phạm hoặc các hành vi vi phạm. Điều kiện này thiết lập tiêu chuẩn cho việc miễn trách nhiệm hình sự cho các ISPs nếu có thông tin hoặc vi phạm pháp luật hình sự được đưa lên hệ thống lưu trữ của họ. Điều kiện thứ hai gắn với các trách nhiệm dân sự khi có hành vi vi phạm từ thông tin được lưu trữ trên mạng, nhưng tương tự với điều kiện đầu tiên, họ cũng không nhận thức được về các sự việc này. Tức là họ đã tuân thủ nghiêm ngặt các quy tắc của ECD đặt ra trong việc đảm bảo tính trung lập, không can thiệp hoặc tiết lộ, tìm hiểu và sử dụng thông tin, chỉ thực hiện duy nhất chức năng lưu trữ như cam kết với người dùng. Ngoài ra, nếu các ISPs bằng cách nào đó biết được các thông tin vi phạm trên, họ phải có trách nhiệm xử lý chúng, gỡ bỏ và vô hiệu hoá quyền truy cập, để “ngăn chặn truy cập trái phép vào đối tượng được bảo vệ hoặc ít nhất là gây khó khăn và ngăn cản những người dùng truy cập vào đối tượng sở hữu trí tuệ”, hay được xác định rằng “đã thực hiện “tất cả các biện pháp cần thiết” để ngăn chặn” thì họ sẽ được loại trừ trách nhiệm, Điều này đã được

thể hiện thông qua phán quyết của Toà án Công lý Liên minh châu Âu trong vụ kiện UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH & Wega Filmproduktionsgesellschaft mbH [13].

### 2.3. Đánh giá tính khả thi của cơ chế Safe Harbor tại Việt Nam

Dịch vụ trung gian trên Internet là một dịch vụ quan trọng trong xã hội hiện đại nhưng cũng tiềm ẩn nhiều rủi ro pháp lý bởi người dùng của mình. Vì vậy, cơ chế Safe Harbor ra đời để hạn chế phần nào hoặc toàn bộ trách nhiệm cho các đơn vị trung gian này là một điều cần thiết, để đảm bảo các doanh nghiệp cung cấp dịch vụ trung gian được hoạt động bình thường, vận hành ổn định và tập trung vào phục vụ nhu cầu xã hội.

Hiện nay, pháp luật mới chỉ bước đầu xác lập các chủ thể với các chức năng được coi như những đơn vị cung cấp dịch vụ trung gian Internet. Cụ thể, theo Luật Công nghệ thông tin 2006, nhà cung cấp dịch vụ trung gian trên Internet được phân loại theo 4 nhóm: truyền đưa thông tin số, lưu trữ tạm thời thông tin số, cho thuê chỗ lưu trữ thông tin số, và công cụ tìm kiếm thông tin số. Theo đó, trong một số lĩnh vực như mạng xã hội Việt Nam có Gapo, Zalo; truyền thông tin số có VNPT, FPT, Viettel, hay cho thuê chỗ lưu trữ thông tin số có CMC. Những đơn vị trên chiếm vai trò quan trọng trong hoạt động công nghệ thông tin tại Việt Nam, là những nhà cung cấp dịch vụ Internet lớn của Việt Nam, với rất nhiều người dùng từ cá nhân đến doanh nghiệp. Tuy nhiên, các ISPs tại Việt Nam có vai trò khá thụ động, chưa có nhiều hành động cụ thể và hành lang pháp lý để các công ty này ngăn chặn hiệu quả các nội dung vi phạm pháp luật trên không gian mạng.

Cụ thể, mặc dù Việt Nam đã và đang hoàn thiện hệ thống pháp luật về ngăn ngừa, xử phạt các vi phạm trên không gian mạng, nhưng về cơ bản, quy định để bảo vệ các ISPs chưa nhiều và còn chưa hiệu quả, mới chỉ được quy định trong Thông tư liên tịch số 07/2012/TTLT-TTLT-BTTTT-BVHTTDL của Bộ Văn hoá, Thể thao



và Du lịch và Bộ Thông tin và Truyền thông về quy định trách nhiệm của doanh nghiệp cung cấp dịch vụ trung gian trong việc bảo hộ quyền tác giả và quyền liên quan trên môi trường mạng Internet và mạng viễn thông (Thông tư liên tịch số 07/2012/TTLT-BTTTT-BVHTTDL). Thông tư này điều chỉnh một số ISPs có mô hình với nhiều nét tương đồng với ISPs theo quy định của Hoa Kỳ và châu Âu. Tuy nhiên, các nghĩa vụ họ phải tuân thủ được quy định có sự khác biệt so với cơ chế Safe Harbor, như: gỡ bỏ và xoá nội dung khi có yêu cầu của cơ quan có thẩm quyền nhưng không có quy định thông báo cho người vi phạm; hay phải chịu bồi thường trực tiếp cho chủ sở hữu bản quyền khi trực tiếp vi phạm mà không phải vi phạm từ người dùng;... Ngoài ra, Thông tư 07/2012/TTLT-BTTTT-BVHTTDL còn quy định trách nhiệm cho ISPs nếu hoạt động như nguồn phân phối thứ cấp nội dung vi phạm quyền tác giả, nhưng pháp luật sở hữu trí tuệ Việt Nam hiện nay chưa có định nghĩa rõ ràng nào về một “nguồn phân phối thứ cấp”. Có thể thấy, những quy định này chưa thực sự tạo thành một hành lang pháp lý rõ ràng để giới hạn trách nhiệm của nhà cung cấp dịch vụ trung gian mà chỉ đang kiểm soát hoạt động của ISPs bằng cách gắn họ với các trách nhiệm trực tiếp, khiến họ vẫn có nguy cơ chịu các cáo buộc vi phạm trong khi vẫn có thể bỏ lọt hành vi của người sử dụng [14].

Trong nhiều năm qua, không khó để bắt gặp các vi phạm pháp luật Việt Nam, không chỉ trong lĩnh vực sở hữu trí tuệ như quảng cáo cá độ, bán hàng giả,... trên các nền tảng dịch vụ của các ISPs trên như sàn thương mại điện tử, website, mạng xã hội. Phải cho tới thời gian gần đây, khi có sự phản ánh của một bộ phận người dùng và sự vào cuộc của Bộ Thông tin và Truyền thông và các cơ quan hữu quan khác, những nội dung độc hại, vi phạm pháp luật trên mới dần bị gỡ bỏ và chặn truy cập tại Việt Nam. Theo đó, Nhà nước đã ban hành một số quy định mới nhằm ngăn ngừa các vi phạm trên không gian mạng và đã bước đầu có sự tiếp cận tới các chủ thể cung cấp dịch vụ trung gian trên không gian mạng. Cụ thể, Điều 21 Luật An ninh mạng 2018, quy định khi có tình huống nguy hiểm về an ninh mạng

xảy ra, thực hiện các biện pháp như triển khai phương án phòng ngừa, ứng phó với vi phạm, sau đó cần phải thông báo tới cơ quan, tổ chức có liên quan. Trách nhiệm của các công ty công nghệ, công ty viễn thông cũng được đề cập tới trong quy định này. Hoặc như quy định tại Điều 100 Nghị định 15/2020/NĐ-CP của Chính phủ về xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, công nghệ thông tin đã chỉ rõ các doanh nghiệp công nghệ vận hành mạng xã hội có hành vi hỗ trợ, lưu trữ, truyền, phát tán các hành vi, thông tin xấu độc sẽ phải chịu các mức xử phạt nghiêm khắc của pháp luật. Mặc dù vậy, hiệu quả của các quy định này đang ở mức tương đối. Ngoài lĩnh vực sở hữu trí tuệ, hiện nay còn tồn tại rất nhiều website vi phạm khác website cá độ bóng đá [15], kinh doanh sản phẩm trái pháp luật [16], hện hò trực tuyến [17],... đã lừa đảo rất nhiều người dùng. Có thể thấy những vi phạm trên không gian mạng đang diễn ra rất phổ biến và với quy mô cũng rất lớn, không chỉ riêng lĩnh vực sở hữu trí tuệ, mà còn cả hình sự, dân sự, thương mại. Tuy nhiên, các hành động trên đều xảy ra khi sự việc đã diễn ra được một thời gian, như đối với Phimmoi.com là một thời gian rất dài, nhưng phía các đơn vị trung gian đều không hề có các hành động nào thực sự quyết liệt cho tới khi bị các cơ quan, tổ chức nước ngoài nhắc tới và có sự vào cuộc của cơ quan Nhà nước. Việc pháp luật Việt Nam đang thiếu cơ chế để tự các đơn vị cung cấp dịch vụ trung gian trên Internet kiểm soát vi phạm không chỉ khiến thông tin vi phạm được phát tán, lan truyền rộng rãi hơn mà còn vô tình tác động tới những người dùng thiếu hiểu biết, nhẹ dạ cả tin trước các nguy hiểm trên mạng.

Trước thực trạng trên, việc tiếp cận cơ chế Safe Harbor theo hướng là một biện pháp ngăn chặn hành vi trái pháp luật trực tiếp và từ xa sẽ mang lại nhiều lợi ích cho các ISPs Việt Nam, cho người dùng và cơ quan nhà nước trong hoạt động quản lý không gian mạng. Các lợi ích này bao gồm:

*Thứ nhất*, các đơn vị cung cấp dịch vụ trung gian trên Internet sẽ tập trung vào tăng cường chất lượng trải nghiệm cho người dùng, nâng cao

chất lượng nội dung thông tin, các sản phẩm số để đảm bảo người dùng có một kênh thông tin chất lượng, lành mạnh để tương tác hay thực hiện các hoạt động trên không gian mạng. Ngược lại, nếu không duy trì điều này, các ISPs tại Việt Nam có thể đối mặt với các rủi ro pháp lý.

*Thứ hai*, các đơn vị này sẽ được miễn trừ trước các tranh chấp pháp lý hay quyết định xử phạt hành chính. Như phân tích đã đề cập, khi đáp ứng các điều kiện, cơ chế Safe Harbor cho phép các đơn vị cung cấp dịch vụ trung gian Internet không phải chịu trách nhiệm pháp lý đối với một số hành vi sai trái của người dùng trên nền tảng số của mình. Không chỉ vậy, khi mở rộng phạm vi, cơ chế Safe Harbor còn bao trùm lên các lĩnh vực pháp luật khác, không chỉ riêng trong phạm vi thương mại, sở hữu trí tuệ, mà còn cả dân sự, hình sự tương tự như Chỉ thị Thương mại điện tử của Ủy ban châu Âu. Do đó, với thực tế là sự phổ biến của những vi phạm trên các mạng xã hội, các trang thương mại điện tử, các đơn vị vận hành các nền tảng số trên có thể tránh khỏi các quyết định pháp lý bất lợi từ phía cơ quan nhà nước, vốn có thể làm ảnh hưởng đến uy tín, hình ảnh thương hiệu và cản trở sự phát triển của họ. Điều này sẽ có ý nghĩa giúp nâng cao uy tín trên thị trường của các công ty công nghệ viễn thông, giúp họ đảm bảo việc phát triển cũng như mở rộng thị phần, kêu gọi đầu tư, v.v

*Thứ ba*, để được hưởng cơ chế Safe Harbor, ISPs cần có ý thức trong việc phổ biến các kiến thức pháp luật cho người dùng để thực hiện. Điều này khiến họ giảm sự thụ động, tăng cường tính chủ động của họ đối với các dịch vụ mình cung cấp cho người dùng. Như ví dụ từ đạo luật DMCA, các ISPs sẽ thực hiện cơ chế “Notice and Take down” khi có phản hồi về việc vi phạm tới cơ quan tiếp nhận phản ánh của họ và ngăn ngừa được các vi phạm. Áp dụng với các trang thương mại điện tử, khi một nhà cung cấp độc quyền hàng chính hãng, do được phổ biến kiến thức về quyền của mình trên nền tảng của ISPs, phát hiện có bên khác bán hàng nhái, hàng giả, họ có thể phản ánh vấn đề này tới Trung tâm giải quyết khiếu nại của website đó và cung cấp bằng chứng, từ đó trang thương mại điện tử sẽ thực hiện kiểm tra và ngăn chặn vi phạm trước khi cơ

quan chức năng vào cuộc. Điều này giúp lành mạnh hoá không gian mạng và tăng cường sự hiệu quả trong công tác quản lý các vi phạm của cơ quan nhà nước.

Có thể thấy, Safe Harbor không loại bỏ hoàn toàn trách nhiệm pháp lý của ISPs, mà còn làm tăng trách nhiệm của những đơn vị này cùng với người dùng trong việc ngăn chặn hiệu quả những vi phạm trên nền tảng số từ xa, để làm lành mạnh môi trường mạng Việt Nam.

### 3. Kiến nghị hoàn thiện pháp luật Việt Nam

*Thứ nhất*, xây dựng chế định hoàn chỉnh về Safe Harbor. Theo đó, quy định về Safe Harbor cần tập trung vào những nội dung sau:

Một là, thống nhất phân loại đối tượng “Nhà cung cấp dịch vụ trung gian trên Internet”. Về cơ bản, các hoạt động của các đơn vị trung gian tập trung ở 4 nhóm, mà đạo luật DMCA đã khái quát bao gồm: i) Truyền tải tạm thời mạng kỹ thuật số, ii) Lưu trữ hệ thống trung gian và tạm thời, iii) Lưu trữ thông tin trên mạng hoặc hệ thống theo điều hướng của người dùng, iv) Công cụ định vị thông tin. Hiện nay, Luật Công nghệ thông tin đang không có quy định rõ ràng về những đối tượng cung cấp dịch vụ trung gian, mà chỉ quy định chức năng, công việc của các chủ thể này tại Chương II nên khiến người dân khó nắm bắt đầy đủ quy định pháp luật. Do đó, cần tiến hành rà soát lại các quy định, để đưa ra định nghĩa cụ thể về ISPs, hạn chế giảm sự trùng lặp phạm vi và khái quát cơ chế hoạt động của các chủ thể trên.

Hai là, phạm vi bảo vệ của cơ chế này sẽ bao quát tương đối nhiều lĩnh vực, từ dân sự, hình sự, thương mại tới sở hữu trí tuệ. Như quy định của Liên minh châu Âu, ta có thể thấy cơ chế Safe Harbor có thể loại trừ trách nhiệm cho các ISPs không chỉ trong một số vụ việc sở hữu trí tuệ, mà còn có cả vụ việc về quyền dân sự. Vì vậy, Việt Nam có thể học tập và xây dựng một cơ chế Safe Harbor với phạm vi mở rộng hơn, vượt ra ngoài khuôn khổ của pháp luật sở hữu trí tuệ, để bảo vệ không gian mạng khỏi các vi phạm hình sự, thương mại khác nhau.

Ba là, cần xác định các điều kiện tuân thủ để các chủ thể trên được hưởng cơ chế miễn trừ của Safe Harbor. Theo người viết, phụ thuộc vào từng loại đơn vị trung gian, những điều kiện này có thể khác nhau, nhưng cần bám sát các nguyên tắc sau:

- Tôn trọng, bảo vệ thông tin, dữ liệu của người dùng;

- Giữ vai trò “trung lập” trong toàn bộ quá trình sử dụng dịch vụ, lưu trữ, truyền thông tin của người dùng, trừ trường hợp vi phạm pháp luật;

- Gỡ bỏ kịp thời những thông tin, những dữ liệu của người dùng vi phạm quy định pháp luật trong phạm vi dịch vụ quản lý;

Các nguyên tắc trên đảm bảo các đơn vị cung cấp dịch vụ trung gian sẽ giữ nguyên vai trò trung lập của mình trong quá trình cung cấp dịch vụ cho người dùng, đảm bảo thông tin của người dùng sẽ được an toàn, không bị can thiệp và thay đổi, chỉnh sửa, làm mất đi tính nguyên vẹn của thông tin. Tuy nhiên, các nhà cung cấp dịch vụ này sẽ được quyền tiếp cận, hay “có nhận thức”, về hành vi vi phạm và can thiệp khi có những nội dung trái pháp luật trong thời gian kịp thời, hạn chế thông tin bị lan truyền trên không gian mạng.

Bốn là, thiết lập hành lang pháp lý rõ ràng cho cơ chế gỡ bỏ thông tin, dữ liệu của người dùng vi phạm pháp luật. Như các phân tích trên, quyền gỡ bỏ thông tin kịp thời là trọng tâm của cơ chế Safe Harbor, do đó, việc thiết lập một quy trình đầy đủ cho cơ chế này là điều cần thiết. Pháp luật Hoa Kỳ và Liên minh châu Âu đều thống nhất rằng thủ tục này gồm 2 bước chính: thông báo và gỡ bỏ.

Đối với thủ tục thông báo, người chịu trách nhiệm chính cho hoạt động này chính là người dùng. Khi phát hiện các hành vi có dấu hiệu vi phạm pháp luật, vi phạm bản quyền, lừa đảo, v.v thì người dùng sẽ là đầu mối báo cáo các thông tin này cùng với bằng chứng tới các đơn vị cung cấp dịch vụ trung gian. Theo đó, các đơn vị trung gian cần có các trung tâm tiếp nhận khiếu nại, phản ánh để tiếp nhận thông tin về các vi phạm trên và đưa ra quy trình xử lý nội bộ, và việc tiếp cận với các trung tâm này phải dễ dàng, thuận tiện để việc báo cáo diễn ra hiệu quả, chính xác.

Đối với thủ tục gỡ bỏ, người chịu trách nhiệm chính trong việc thực hiện hoạt động này là các nhà cung cấp dịch vụ trung gian. Việc gỡ bỏ trước hết cần có tinh thần tự giác và chấp hành pháp luật và quy định nghiêm chỉnh của người dùng. Tuy nhiên, vẫn cần có quy định để các nhà cung cấp ban hành và thực thi thủ tục gỡ bỏ của riêng mình để đảm bảo cơ chế này được thực hiện hiệu quả. Theo đó, thủ tục gỡ bỏ cần đảm bảo các nội dung quan trọng: i) sau khi nhận được khiếu nại, phải tiến hành xác minh kịp thời thông tin; ii) khi hoàn tất bước xác minh và có cơ sở về việc vi phạm quy định pháp luật, cần có thông báo cho người vi phạm và tiến hành gỡ bỏ thông tin; iii) có thể có những biện pháp giải quyết bổ sung: cấm hoạt động; gửi hồ sơ tới cơ quan Nhà nước,... Những thủ tục này cho phép nhà cung cấp sẽ có các chế tài áp dụng với đúng người và đúng lỗi, đảm bảo thông tin khiếu nại vẫn được kiểm tra 2 chiều, hạn chế được vụ khống bịa đặt, nhằm hạ thấp uy tín của bên thứ ba, điều này là đặc biệt quan trọng trên các sàn thương mại điện tử. Nhìn chung, việc hiện thực hoá quy trình trên có thể đem lại lợi ích cho cả người dùng và nhà cung cấp dịch vụ trung gian. Bên cạnh đó, cũng cần cho phép các đơn vị cung cấp dịch vụ trung gian trong nước áp dụng các chế tài có tính răn đe mạnh đối với người dùng của mình vi phạm quy định pháp luật, điều mà Facebook, Youtube đã thực hiện với vi phạm về sở hữu trí tuệ, điều khoản dịch vụ trên nền tảng của mình [18].

Tuy nhiên, một vấn đề cần quan tâm là thời gian để gỡ bỏ thông tin trái pháp luật. Mặc dù Chỉ thị 2000/31 về thương mại điện tử quy định rằng nhà cung cấp phải “khẩn trương” gỡ bỏ hoặc vô hiệu hoá truy cập thông tin trái phép, nhưng ngay Liên minh châu Âu (EU) cũng chưa có cách giải thích cụ thể về thời gian gỡ bỏ. Theo Bộ Quy tắc của EU về chống phát ngôn thù địch trên Internet, thời gian gỡ bỏ là 24 giờ; trong khi đó, luật của Hà Lan lại cho phép kéo dài hơn, nhưng không quá 5 ngày làm việc [11]. Trong thời đại mà vấn nạn tin giả đang trở nên nhức nhối, việc duy trì một khoảng thời gian cho sự tồn tại của các thông tin sai lệch, vi phạm pháp luật trên không gian mạng sẽ có hậu quả hết sức

khó lường. Vì vậy, người viết đề xuất nhà làm luật quy định thời gian này căn cứ vào các yếu tố: mức độ vi phạm pháp luật của thông tin đó; thời gian xác minh thông tin; thời gian gửi thông báo tới người dùng; điều kiện khoa học kỹ thuật của nhà cung cấp. Bên cạnh đó, cần quán triệt chủ trương cần phải loại bỏ sớm các hành vi, thông tin vi phạm khỏi không gian mạng, tránh để các thông tin này có điều kiện tồn tại lâu và phát tán ra xã hội. Điều này tạo sự công bằng cho các chủ thể, đồng thời cả người vi phạm và nhà cung cấp dịch vụ trung gian đều có thể theo dõi và nắm bắt được thời gian gỡ bỏ, nên có thể phát huy hiệu quả của việc thực hiện gỡ bỏ này.

Năm là, nhà làm luật cần có thiết chế để các cơ quan và người dùng phối hợp giám sát hoạt động thực hiện cơ chế Safe Harbor của các đơn vị cung cấp dịch vụ trung gian trên Internet tại Việt Nam. Điều này là cần thiết bởi cơ chế Safe Harbor về bản chất là sự tự gỡ bỏ thông tin trái pháp luật của các công ty công nghệ để được hưởng sự miễn trừ trách nhiệm pháp lý của Nhà nước, nên việc tự thực hiện này nếu không được giám sát sẽ khó phát huy hiệu quả. Do đó, một cơ quan nhà nước đảm trách nhiệm vụ thực hiện cơ chế Safe Harbor của các chủ thể có dịch vụ được cung ứng trên Internet là cần thiết và cũng là đầu mối để tiếp nhận phản ánh của người dùng sau khi đã phản ánh tới doanh nghiệp nhưng không được thực hiện. Ở đây, căn cứ theo phạm vi kiểm soát, môi trường có thể diễn ra các hành vi vi phạm của người dùng này, người viết đề xuất Cục Phát thanh, Truyền hình và Thông tin điện tử thuộc Bộ Thông tin và Truyền thông tiếp tục thực hiện giám sát, kiểm soát hoạt động pháp luật của các nhà cung cấp dịch vụ trung gian trên.

*Thứ hai*, cần ứng dụng mạnh mẽ các công nghệ mới như trí tuệ nhân tạo, blockchain, v.v vào việc xác minh các hành vi, nội dung thông tin vi phạm để tối ưu hoá quá trình Thông báo và Gỡ bỏ. Hiện nay, Youtube đã có những thuật toán rất hiện đại để họ có thể tự loại bỏ những bài hát, những video vi phạm bản quyền trong thời gian ngắn sau khi người dùng tải lên [19]. Đây là một công nghệ rất cần được học hỏi và ứng dụng tại Việt Nam, không chỉ ngoài phạm vi luật sở hữu trí tuệ, mà còn các lĩnh vực khác như

pháp luật khác. Với sự phát triển của công nghệ hiện nay, việc phát triển trí tuệ nhân tạo hay các thuật toán để hỗ trợ con người trong giám sát thực hiện pháp luật là rất có tiềm năng, và cơ chế Safe Harbor sẽ được hưởng lợi trực tiếp từ sự phát triển này.

*Thứ ba*, cần tiếp tục giáo dục, nâng cao ý thức sử dụng Internet của người dùng Việt Nam. Điều quan trọng nhất trong việc xây dựng một môi trường mạng lành mạnh, tuân thủ pháp luật vẫn là ý thức người dùng. Nếu tỉ lệ người dùng hiểu rõ các quy định pháp luật khi sử dụng Internet cao, thì tỉ lệ các hành vi vi phạm trên không gian mạng chắc chắn sẽ giảm xuống. Do đó, cần tiếp tục đẩy mạnh các chương trình truyền thông, tuyên truyền, giáo dục tại các cấp về các quy định, quy tắc sử dụng Internet ở tất cả khía cạnh có liên quan trực tiếp như pháp luật hình sự, dân sự, sở hữu trí tuệ. Điều này có thể đem lại lợi ích cho không chỉ riêng những nhà cung cấp dịch vụ trung gian trên Internet muốn hưởng cơ chế Safe Harbor, mà còn giúp củng cố hơn nữa môi trường mạng văn minh, lành mạnh, tuân thủ quy định pháp luật.

### Tài liệu tham khảo

- [1] N. L. Sỹ, N. T. L. Anh, Vụ VNG kiện TikTok: kinh nghiệm cho Việt Nam từ cơ chế ‘Safe harbour’ của Hoa Kỳ, Liên minh châu Âu và New Zealand, <http://lapphap.vn/Pages/tintuc/tinchitiet.aspx?tintucid=210759>, ((accessed on: December 17<sup>th</sup>, 2023).
- [2] M. Sag , Internet Safe Harbor and the Transformation of Copyright Law, *Notre Dame L.Rev.*, 2018, pp. 503
- [3] OECD, Internet Intermediaries: Definition, Economic Models and Role in the Value Chain, in: OECD, *The Role of Internet Intermediaries in Advancing Public Policy Objectives*, OECD Publishing, Paris, 2011, pp. 20-36.
- [4] S. Hunter, What Is An ISP (Internet Service Provider)?, <https://www.forbes.com/home-improvement/internet/what-is-an-isp/>, (accessed on: December 13<sup>th</sup>, 2022).
- [5] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9<sup>th</sup> Cir. 2001), <https://www.copyright.gov/fair-use/summaries/a&mrecords-napster-9thcir2001.pdf> (accessed on: December 13<sup>th</sup>, 2022).

- [6] *Viacom International Inc. v. Youtube, Inc.*, Dist. Court, SD New York 2013, [https://scholar.google.com/scholar\\_case?case=13644579048975596329&q=Viacom+International+Inc.+v.+YouTube,+Inc.&hl=en&as\\_sdt=6,39&as\\_vis=1](https://scholar.google.com/scholar_case?case=13644579048975596329&q=Viacom+International+Inc.+v.+YouTube,+Inc.&hl=en&as_sdt=6,39&as_vis=1), (accessed on: December 13<sup>th</sup>, 2022).
- [7] *L'Oréal SA and Others v eBay International AG and Others*, <https://globalfreedomofexpression.columbia.edu/cases/loreal-sa-v-ebay-international-ag/>, (accessed on: December 13<sup>th</sup>, 2022).
- [8] Legislative Attorney, Safe Harbor for Online Service Providers Under Section 512(c) of the Digital Millennium Copyright Act, [https://www.everycrsreport.com/files/20140326\\_R43436](https://www.everycrsreport.com/files/20140326_R43436), (accessed on: December 13<sup>th</sup>, 2022).
- [9] D. H. Souter, Supreme Court of The United States. U.S. Reports: *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913. [Periodical] Retrieved from the Library of Congress, <https://www.loc.gov/item/usrep545913/>, (accessed on: December 13<sup>th</sup>, 2022).
- [10] van Hoboken, J. Legal Space for Innovative Ordering: on the Need to Update Selection Intermediary Liability In The EU, *International Journal of Communications Law and Policy*, 13, pp. 55. [http://www.ijclp.net/files/ijclp\\_web-doc\\_3-13-2009.pdf](http://www.ijclp.net/files/ijclp_web-doc_3-13-2009.pdf), (accessed on: December 13<sup>th</sup>, 2022).
- [11] T. Madiaga & Members' Research Service, EPRS, Reform of the EU Liability Regime for Online Intermediaries - Background on the Forthcoming Digital Services Act, Brussels, 2020.
- [12] T. Dangngam, Internet Service Provider Liability for Third - Party Copyright Infringement - A Comparative Study Between US and EU Approaches, Master Thesis, Tilburg University, 2009.
- [13] Case C-314/12 giữa UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH & Wega Filmproduktionsgesellschaft mbH. Xem thêm tại: <https://curia.europa.eu/juris/document/document.jsf?jsessionid=70C4CC9705296A06EC06CB046EC31097?text=&docid=149924&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=16811>, (accessed on: December 15<sup>th</sup>, 2022).
- [14] N. T. Quân, T. P. Anh, Trách nhiệm pháp lí của nhà cung cấp dịch vụ trung gian với vi phạm quyền tác giả trên Internet, *Tạp chí Luật học*, Số 1, 2019, tr. 29-43.
- [15] V. Anh, Công bố tiếp 48 website có dấu hiệu vi phạm pháp luật, <https://ictnews.vietnamnet.vn/bo-tt-tt-cong-bo-48-website-co-dau-hieu-vi-pham-phap-luat-5001860.html>, (accessed on: December 13<sup>th</sup>, 2022).
- [16] Q. Luru, Tiếp tục xử lý 3 website vi phạm kinh doanh thương mại điện tử, <https://moit.gov.vn/quan-ly-thi-truong/tiep-tuc-xu-ly-3-website-vi-pham-kinh-doanh-thuong-mai-dien-2.html>, (accessed on: December 13<sup>th</sup>, 2022).
- [17] Ban Thời sự, Nguy hiểm bẫy tình "hẹn hò" online, <https://vtv.vn/xa-hoi/nguy-hiem-bay-tinh-hen-ho-online-20220709180129354.htm>, (accessed on: December 13<sup>th</sup>, 2022).
- [18] Youtube Support, Chấm dứt kênh hoặc tài khoản, <https://support.google.com/youtube/answer/2802168?hl=vi>, (accessed on: December 13<sup>th</sup>, 2022).
- [19] Youtube Support, Thông tin cơ bản về cảnh báo vi phạm bản quyền, <https://support.google.com/youtube/answer/2814000?>, (accessed on: December 13<sup>th</sup>, 2022).