PHÁP LUẬT VIỆT NAM VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN TRONG KỶ NGUYÊN SỐ DƯỚI TÁC ĐỘNG CỦA CÔNG NGHỆ DEEPFAKE

NGUYỄN THỊ TRÚC MAI[*]
LÊ MINH HẢI[**]
PHAN KHÁNH CHI[***]

Ngày nhận bài:27/07/2024
Ngày phản biện:15/08/2024
Ngày đăng bài:30/09/2024

Tóm tắt:

Dữ liệu cá nhân ngày càng trở thành tài sản quý giá, đồng thời là mục tiêu tiềm ẩn của các cuộc tấn công mạng và các hành vi lạm dụng trong kỷ nguyên số hiện nay. Công nghệ Deepfake, với khả năng tạo ra hình ảnh, âm thanh và video giả mạo thông qua trí tuệ nhân tạo (AI), đã mở ra nhiều cơ hội nhưng cũng đi kèm với các nguy cơ lớn đối với quyền riêng tư và an ninh cá nhân. Thông tin, hình ảnh của cá nhân bị thu thập, thông qua thuật toán máy tính có thể giả mạo danh tính người dùng nhằm mục đích lừa đảo hoặc nhằm bôi nhọ danh dự, uy tín của người đó. Bài viết này, trên cơ sở tiếp cận phương thức hoạt động của công nghệ Deepfake và những thách thức trong việc bảo vệ dữ liệu cá nhân dưới tác động của Deepfake, từ đó đề xuất các giải pháp pháp lý và kỹ thuật nhằm nâng cao hiệu quả bảo vệ dữ liệu và quyền riêng tư cá nhân trong môi trường số.

Từ khóa:

Bảo vệ dữ liệu cá nhân; Công nghệ Deepfake; tác động; kỷ nguyên số.

Abstract:

Personal data is increasingly becoming a valuable asset, as well as a potential target for cyberattacks and abuse in today's digital era. Deepfake technology, with its ability to create fake images, sounds and videos through artificial intelligence (AI), has opened up many opportunities but also comes with great risks to privacy and security. personal security. Information and images of individuals are collected through computer algorithms that can fake the user's identity for the purpose of fraud or to defame that person's honor and reputation. This article, based on the approach to how Deepfake technology works and the challenges in protecting personal data under the influence of Deepfake, proposes legal and technical solutions to improve personal data. effectively protect data and personal privacy in the digital environment.

Keywords:

Protect personal data; Deepfake technology; impact; digital era.

[*] Sinh viên lớp Luật K46B; Trường Đại học Luật, Đại học Huế; *Email: trucmai202312@gmail.com*
[**] Sinh viên lớp Luật K46A; Trường Đại học Luật, Đại học Huế; *Email:leminhhai.tk3@gmail.com*
[***] Khoa Luật Kinh tế, Trường Đại học Luật, Đại học Huế; *Email: chipk@hul.edu.vn*

1. Đặt vấn đề

Sự phát triển một cách nhanh chống của AI và Bigdata đã làm xuất hiện nên một nguy cơ mới đối với những người dùng mạng internet, đó chính là Deepfake. Công nghệ Deepfake sử dụng các thuật toán học sâu để tạo ra các video, âm thanh giả mạo có độ chính xác cao, khiến người xem khó phân biệt giữa thực và giả. Thông tin, hình ảnh cá nhân bị thu thập để tạo ra các sản phẩm Deepfake với mục đích xấu như lừa đảo, phá hoại danh dự hay thậm chí là các hoạt động tội phạm. Điều này dẫn đến việc xâm phạm quyền riêng tư cá nhân khi dữ liệu cá nhân bị thu thập một cách trái phép. Pháp luật Việt Nam đã có sự can thiệp và điều chỉnh từ rất sớm đối với hoạt động của người dùng trên không gian mạng nói chung. Tuy nhiên, cơ chế quản lý, xử lý đối với các sản phẩm từ công nghệ Deepfake vẫn chưa được xây dựng và kiểm soát hoạt động một cách có hệ thống.

2. Khái quát về dữ liệu cá nhân

Kỷ nguyên số là quá trình chuyển đổi số toàn cầu nhằm thay đổi tổng thể và toàn diện phương thức phát triển của xã hội, lối sống và hoạt động trên nền tảng số.[10] Thời kỳ này, công nghệ thông (CNTT) phát triển đã tạo ra một loại "tài sản" mới cho mỗi cá nhân, đó chính là "dữ liệu cá nhân" (DLCN). Theo Điều 4(1) quy định về bảo vệ dữ liệu chung GDPR (General Data Protection Regulation) của Liên minh châu Âu thì "dữ liệu cá nhân" nghĩa là: bất kỳ thông tin nào liên quan đến một người tự nhiên được xác định hoặc có thể nhận diện trực tiếp hoặc gián tiếp thông qua tham chiếu đến một định danh từ tên, số nhận dạng, thông tin vị trí số, định danh trực tuyến một hoặc nhiều nhân tố liên quan đến thể chất, sinh lý di truyền, tinh thần, kinh tế, văn hóa xã hội của người đó.

Pháp luật Việt Nam đã ghi nhận Nghị định số 13/2023/NĐ-CP ngày 17/04/2023 về bảo vệ dữ liệu cá nhân với một số điểm tương đồng về phạm vi điều chỉnh và đối tượng áp dụng với GDPR của EU. Nghị định định nghĩa: *"Dữ liệu cá nhân là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể. Dữ liệu cá nhân bao gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm".*

Như vậy, DLCN trong kỷ nguyên số là tất cả những gì về bí mật cá nhân, thông tin gia đình gắn liền với cá nhân cụ thể bao gồm: (i) dữ liệu cá nhân cơ bản (họ tên, ngày tháng năm sinh, giới tính, quốc tịch, quê quán, nơi thường trú,biển số xe, số định danh cá nhân...) và (ii) dữ liệu cá nhân nhạy cảm (quan điểm chính trị, quan điểm tôn giáo, thông tin về đời sống tình dục, đời sống tình dục, tình trạng sức khỏe, đời tư được ghi trong hồ sơ bệnh án…) được đăng tải và lưu trữ trên môi trường số.

Đặc điểm của "dữ liệu cá nhân" có thể chỉ ra:

[10]Tạp chí Cộng sản (2021), *Hội nhập quốc tế trong "kỷ nguyên số" và một số vấn đề đặt ra đối với Việt Nam*, https://www.tapchicongsan.org.vn/web/guest/quoc-phong-an-ninh-oi-ngoai1/-/2018/823137/hoi-nhap-quoc-te-trong-%E2%80%9Cky-nguyen-so%E2%80%9D-va-mot-so-van-de-dat-ra-doi-voi-viet-nam.aspx, truy cập 5/7/2024

Thứ nhất, DLCN của mỗi cá nhân mang tính cá biệt của chủ thể dữ liệu

DLCN là tập hợp những thông tin của một con người cụ thể, gắn liền với người đó từ khi sinh ra. Các thông tin đơn lẻ của mỗi người có thể giống nhau như: tên, ngày sinh, nhóm máu, giới tính. Nhưng nếu xác định trên tổng thể là một cá nhân cụ thể thì thông tin hình thành DLCN lại không thể trùng lặp hoàn toàn nên từ đó có thể phân biệt giữa các cá nhân với nhau.

Thứ hai, DLCN tồn tại dưới nhiều nội dung và hình thức thể hiện

DLCN không chỉ bao gồm các thông tin cơ bản như họ tên, địa chỉ, nhóm máu ngày sinh, quốc tịch,.... các thông tin này được chứa đựng dưới nhiều hình thức khác nhau bao gồm văn bản, hồ sơ trực tuyến, hình ảnh, bản ghi âm, ghi hình hoặc các dạng khác theo quy định của pháp luật.

Thứ ba, DLCN mang đặc điểm của một loại tài sản

Dưới góc độ tài sản, DLCN có thể chiếm hữu thông qua phạm vi hệ thống thông tin[11], có thể trở thành đối tượng của sự trao đổi vì có thể được truyền đưa, chia sẻ và nếu khai thác chúng có thể mang lại các giá trị cho người có quyền.

3. Công nghệ Deepfake và những rủi ro xâm phạm quyền của cá nhân của công nghệ Deepfake

Công nghệ Deepfake là một dạng trí tuệ nhân tạo sử dụng thuật toán máy tính thông minh để tạo ra nội dung đa phương tiện bao gồm âm thanh, hình ảnh, video không có thật trên cơ sở thu thập từ con người hay vật thể nào đó, sau đó sử dụng các thuật toán máy tính để sản xuất ra những gì không có thật. Kết quả của quá trình này là tạo ra sản phẩm hoàn toàn giả mạo phục vụ cho những mục đích nhất định.

Tại cuộc trao đổi với chủ đề "Cảnh giác với công nghệ "siêu lừa" Deepfake" trên kênh VOA Tiếng Việt, Tiến sĩ Bùi Trung Hiếu – Giảng viên Đại học Công giáo Hoa Kỳ cho rằng: Deepfake là một thông tin truyền thông được tạo ra mà người xem không thể dễ dàng phân biệt được thật hay giả, nó đánh lừa các giác quan của con người mà đa phần tập trung vào thị giác và thính giác của chúng ta. Deepfake được tạo ra bởi kỹ thuật chỉnh sửa âm thanh và thuật toán máy tính AI thông minh. Các thuật toán máy tính này sẽ tự học và tự phân tích các dữ liệu về âm thanh hình ảnh từ những cá nhân hay vật thể được chọn. Kết quả cuối cùng là người, hay vật được chọn đó bị thay thế bằng chân dung người khác hoặc vật khác mà người xem sẽ không dễ dàng nhận ra sự hoán đổi đó.

Nhìn chung, công nghệ Deepfake là một dạng trí tuệ nhân tạo sử dụng thuật toán máy tính thông minh để tạo ra nội dung đa phương tiện bao gồm âm thanh, hình ảnh, video không có thật trên cơ sở thu thập từ con người hay vật thể nào đó, sau đó sử dụng các thuật toán máy tính để sản xuất ra những gì không có thật. Kết quả của quá trình này là tạo ra sản phẩm hoàn toàn giả mạo phục vụ cho những mục đích nhất định.

[11]Nguyễn Minh Hiếu, Lâm Vũ Từ Nghi, Đặng Lan Anh, Nguyễn Đình Việt Hưng, Nguyễn Thị Anh (2023), *Dữ liệu cá nhân – Nên xem là hàng hóa hay không?*, Kỷ yếu Khoa học Hội thảo Quốc gia – Dòng chảy Dữ liệu cá nhân trong kỷ nguyên số, tr71

Những rủi ro xâm phạm quyền của cá nhân của công nghệ Deepfake bao gồm:

Thứ nhất, rủi ro xâm phạm quyền riêng tư

Một trong những rủi ro lớn nhất mà công nghệ Deepfake mang lại là khả năng xâm phạm quyền riêng tư của cá nhân. Công nghệ này có thể tạo ra những hình ảnh và video giả mạo trong đó cá nhân bị làm giả mà không có sự đồng ý.

Vào tháng 12 năm 2020, Sensity - một công ty có trụ sở tại Amsterdam chuyên phát hiện và theo dõi các video Deepfake trực tuyến, đã tìm thấy 85.047 video Deepfake trên các trang web phát trực tuyến và con số này tăng gấp đôi sau mỗi 6 tháng. Trước đó, tháng 9 năm 2019, Sensity đã phát hiện ra rằng 96 % video giả mạo liên quan đến nội dung khiêu dâm không có sự đồng thuận.[12]

Tại Việt Nam, các sản phẩm từ Deepfake xuất hiện ngày một nhiều. Theo thống kê năm 2023, Bộ Công an đã phải cảnh báo, xử lý hàng chục triệu các vụ việc có liên quan đến xâm phạm cơ sở dữ liệu cá nhân. Các dữ liệu này đã được rao bán giá rẻ trên các diễn đàn, thậm chí rao bán trên cả trên cả các hội nhóm Telegram. Đầu năm 2024, vụ việc VnDirect & 2 công ty liên quan bị tấn công mạng dẫn tới sự gián đoạn các giao dịch gây thiệt hại cho nhà đầu tư; thông tin cá nhân, thông tin tài khoản bị lộ lọt…

Thứ hai, xâm phạm danh dự và uy tín

Công nghệ Deepfake cũng có thể gây ra những thiệt hại nghiêm trọng đối với danh dự và uy tín của cá nhân. Những video hoặc âm thanh giả mạo có thể được tạo ra để làm giả phát ngôn, hình ảnh video khiêu dâm, tình dục, hành động hoặc sự kiện mà người bị làm giả không hề thực hiện. Những lời nói hoặc hành động sai lệch có thể dẫn đến sự hiểu lầm, gây tổn hại danh tiếng, uy tín của cá nhân, đặc biệt trong các lĩnh vực như chính trị, kinh doanh hoặc truyền thông.

Tại Hàn Quốc, số nạn nhân liên quan đến tội phạm công nghệ Deepfake chỉ trong năm 2024 đạt mức khoảng 800 người. Trong số đó, gần 200 vụ phạm tội liên quan đến Deepfake nhắm vào học sinh và giáo viên, đặc biệt là các nữ sinh. Vấn nạn Deepfake đã gây nhức nhối và bị lên án suốt nhiều năm qua ở Hàn Quốc.

Thứ ba, rủi ro trong lừa đảo và gian lận

Ngoài việc xâm phạm quyền cá nhân, công nghệ Deepfake còn tạo ra những nguy cơ lớn đối với an ninh và tài chính. Các cuộc tấn công lừa đảo qua việc sử dụng giọng nói giả mạo đã trở nên phổ biến, với các kẻ tấn công sử dụng giọng nói giả mạo của người có thẩm quyền trong một tổ chức để thực hiện hành vi gian lận tài chính hoặc thu thập thông tin nhạy cảm.

Đầu tháng 9/2024, anh Lê Mạnh Cường ở 71 Nguyễn Chí Thanh, Đống Đa (Hà Nội) đã bị lừa đảo số tiền 100 triệu đồng sau khi nhận được tin nhắn và cuộc gọi video giả mạo của người bạn thân qua Facebook. Các đối tượng đã đọc rất kỹ những tin nhắn

[12] An Observatory Report from the Europol Innovation Lab (2022), Facing reality? Law enforcement and the challenge of deepfakes

cũ của anh và bạn để có kịch bản lừa đảo hợp lý, kết hợp với công nghệ Deepfake để tạo ra cuộc gọi video mà anh không thể phát hiện[13].

Thứ tư, xâm phạm quyền sở hữu trí tuệ

Một vấn đề đáng chú ý khác là sự vi phạm quyền sở hữu trí tuệ. Các video hoặc hình ảnh được tạo ra thông qua công nghệ Deepfake có thể làm giả tác phẩm của các nghệ sĩ, nhà sản xuất hoặc các cá nhân nổi tiếng mà không có sự chấp thuận. Việc tạo ra các sản phẩm giả mạo mà không được cấp phép là hành vi xâm phạm quyền sở hữu trí tuệ, đặc biệt trong ngành công nghiệp giải trí và nghệ thuật, nơi hình ảnh và âm thanh của các cá nhân nổi tiếng là tài sản quý giá. Điều này không chỉ vi phạm quyền lợi tài chính của các chủ sở hữu mà còn làm suy yếu sự bảo vệ quyền sáng tạo cá nhân trong nền kinh tế sáng tạo.

Các mối đe dọa từ công nghệ Deepfake ngày càng trở nên nghiêm trọng, khi các cá nhân và tổ chức không kiểm soát được việc dữ liệu của họ bị lợi dụng, từ đó tạo ra các video giả mạo mà không được sự đồng ý. Việc nhận diện và xác minh video, hình ảnh thực hay giả cũng trở nên khó khăn khi các công cụ Deepfake ngày càng tinh vi.

4. Đánh giá thực tiễn thực hiện pháp luật về bảo vệ dữ liệu cá nhân dưới tác động của công nghệ Deepfake tại Việt Nam

Pháp luật Việt Nam liên quan đến bảo vệ dữ liệu người dùng can thiệp và điều chỉnh từ khá sớm. Những tác động của công nghệ Deepfake được điều chỉnh qua một số văn bản pháp lý quan trọng, chủ yếu là các quy định liên quan đến bảo vệ quyền cá nhân, quyền riêng tư và phòng chống các hành vi phạm tội mạng.

Thứ nhất, quy định về bảo vệ dữ liệu cá nhân

Một là, các quy định đối với hành vi xâm phạm dữ liệu cá nhân trái phép

Luật An ninh mạng có hiệu lực từ ngày 1/1/2019, có các quy định liên quan đến bảo vệ an ninh, an toàn thông tin mạng và bảo vệ quyền lợi của cá nhân trên không gian mạng. Điều 26 của Luật này quy định về việc cấm hành vi lợi dụng không gian mạng làm giả thông tin, xâm phạm đời tư, danh dự và uy tín để xâm phạm quyền lợi hợp pháp của tổ chức, cá nhân bao gồm: cấm hành vi sử dụng mạng xã hội, phương tiện truyền thông để phát tán thông tin sai lệch, xuyên tạc, bịa đặt nhằm làm mất uy tín của cá nhân, tổ chức và cấm hành vi tấn công, xâm phạm các hệ thống mạng, làm rò rỉ hoặc sử dụng trái phép thông tin cá nhân. Điều này có nghĩa là các hành vi sử dụng công nghệ Deepfake để tạo ra video, hình ảnh giả mạo nhằm tấn công danh dự, uy tín của cá nhân sẽ vi phạm quy định của Luật An ninh mạng.

Đồng thời, Luật Công nghệ thông tin 2006 (sửa đổi bổ sung 2018) cũng có các quy định về bảo vệ dữ liệu cá nhân trước các hành vi thu thập, sử dụng và phát tán

[13] Báo Quân đội Nhân dân (2024), *"Ngăn chặn tình trạng lừa đảo qua không gian mạng - Bài 2: Hiểm họa từ AI",* truy cập tại https://www.qdnd.vn/phap-luat/cac-van-de/ngan-chan-tinh-trang-lua-dao-qua-khong-gian-mang-bai-2-hiem-hoa-tu-ai-802704, truy cập ngày 11/7/2024

thông tin cá nhân trái phép.[14] Do đó, khi quyền riêng tư của cá nhân, tổ chức bị xâm phạm bởi công nghệ Deepfake thì có thể bị xử lý theo quy định của Luật này.

Hai là, các quy định về quyền của chủ thể dữ liệu và các chủ thể có liên quan

Nghị định 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân đã đánh dấu bước tiến quan trọng trong việc bảo vệ dữ liệu cá nhân tại Việt Nam. Nghị định này đưa ra các quy định chi tiết về việc thu thập, sử dụng và bảo vệ thông tin cá nhân của công dân. Đặc biệt, các quy định trong Nghị định này yêu cầu các tổ chức, doanh nghiệp phải có biện pháp bảo vệ dữ liệu cá nhân, đảm bảo rằng dữ liệu không bị lạm dụng hoặc sử dụng sai mục đích.

Các nguyên tắc hàng đầu của Nghị định này là: Tính hợp pháp, công bằng và minh bạch với chủ thể dữ liệu; trách nhiệm của chủ thể thu thập dữ liệu về hoạt động thu thập, lưu trữ và chịu trách nhiệm trong hoạt động của mình. Đồng thời, Điều 9 của NghỊ định này đã trao cho chủ thể dữ được các quyền: Quyền được biết, quyền đồng ý, quyền truy cập, quyền rút lại sự đồng ý, quyền xóa dữ liệu, quyền hạn chế xử lý dữ liệu, quyền cung cấp dữ liệu, quyền phản đối xử lý dữ liệu, quyền khiếu nại, tố cáo, yêu cầu bồi thường và quyền tự bảo vệ của Nghị định này được thực hiện theo Điều 11 Bộ Luật dân sự 2015.

Bên cạnh đó, Luật Giao dịch điện tử năm 2023 có hiệu lực từ 01/7/2024 quy định nghiêm ngặt về việc thu thập, lưu trữ và xử lý dữ liệu cá nhân của các tổ chức doanh nghiệp nhằm bảo vệ quyền riêng tư của cá nhân bao gồm: (i) sự đồng ý của chủ dữ liệu hoặc theo các quy định pháp luật; (ii) thực hiện một cách an toàn, sử dụng các biện pháp mã hóa và bảo mật để ngăn chặn truy cập trái phép, mất mát hoặc rò rỉ dữ liệu và (iii) tuân thủ các nguyên tắc bảo mật và chỉ được thực hiện cho các mục đích đã được người dùng chấp thuận. Đồng thời, người dùng có quyền truy cập, chỉnh sửa và yêu cầu xóa bỏ dữ liệu cá nhân của mình. Các quy định này có phần tương tự các quy định tại Nghị định 13/2023/NĐ-CP đã có hiệu lực trước đó.

Quyền được biết của chủ thể cũng được quy định tại Điều 32 Bộ Luật dân sự 2015 về việc sử dụng hình ảnh của cá nhân phải được người đó đồng ý. Pháp luật trao cho chủ thể quyền được biết và quyền quyết định đối với hình ảnh cá nhân của mình. Đối với hành vi ghép ảnh người khác vào sản phẩm khiêu dâm khi chưa được đồng ý và khoản 1 Điều 584 Bộ Luật dân sự năm 2015, người có hành vi xâm phạm danh dự, nhân phẩm, uy tín của người khác mà gây thiệt hại thì phải bồi thường. Khi đó, những chủ thể bị ghép vào hình ảnh khiêu dâm có quyền khởi kiện dân sự yêu cầu người có hành vi vi phạm chấm dứt hành vi xâm phạm, buộc xin lỗi, cải chính công khai và yêu cầu bồi thường thiệt hại.

Thứ hai, các quy định về xử lý hành vi xâm phạm dữ liệu cá nhân trái phép

[14] Điều 12 Luật Công nghệ Thông tin 2006 (sửa đổi bổ sung 2018)

Chính phủ đã ban hành Nghị định số 15/2020/NĐ-CP quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử, trong đó các mức xử phạt tương ứng đối với từng nhóm hành vi vi phạm thông tin trên mạng sau đây:

- Hành vi đưa thông tin sai sự thật, xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự và nhân phẩm của cá nhân của các trang tin điện tử vi phạm sẽ bị phạt tiền từ 20 triệu đến 30 triệu đồng (điểm a, khoản 3, Điều 99).

- Hành vi chủ động lưu trữ, truyền đưa thông tin giả mạo, thông tin sai sự thật, vu khống, xuyên tạc, xúc phạm uy tín của tổ chức và danh dự, nhân phẩm của cá nhân; chủ động lưu trữ, truyền đưa thông tin bịa đặt, gây hoang mang trong nhân dân sẽ phạt tiền từ 50 triệu đến 70 triệu đồng (điểm a, khoản 3, Điều 100).

- Hành vi cung cấp, chia sẻ thông tin giả mạo, thông tin sai sự thật, xuyên tạc, vu khống, xúc phạm uy tín của cơ quan, tổ chức, danh dự, nhân phẩm của cá nhân (điểm a, khoản 1, Điều 101); cung cấp, chia sẻ thông tin bịa đặt, gây hoang mang trong nhân dân (điểm d, khoản 1, Điều 101) sẽ bị phạt tiền từ 10 triệu đến 20 triệu đồng.

- Hành vi mua bán trái phép dữ liệu cá nhân có thể bị xử phạt vi phạm hành chính từ 50.000.000 đồng đến 70.000.000 đồng theo quy định tại Điều 102 Nghị định này.

Các vi phạm về dữ liệu cá nhân có thể bị xử phạt hình sự, với án tù giam cao nhất là 07 năm. Cụ thể: Điều 159 Bộ Luật Hình sự 2015 quy định, việc "xâm phạm bí mật hoặc an ninh thư tín, điện thoại, điện tín hoặc hình thức trao đổi thông tin riêng tư của người khác" có thể bị phạt tù tới 03 năm. Điều 288 quy định về "Tội đưa hoặc sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông" với mức hình phạt cao nhất là 07 năm tù giam.

Đối với các tội liên quan đến việc xâm phạm quyền lợi cá nhân, trong đó có các hành vi sử dụng công nghệ thông tin để phạm tội, bao gồm cả sử dụng công nghệ Deepfake để lừa đảo hoặc xâm phạm danh dự, uy tín của cá nhân. Điều 122 về tội vu khống cũng có thể áp dụng trong trường hợp công nghệ Deepfake được sử dụng để phát tán thông tin sai lệch gây tổn hại đến danh dự và uy tín của cá nhân.

Hành vi sử dụng mạng máy tính hoặc mạng viễn thông, phương tiện điện tử bịa đặt hoặc loan truyền những điều biết rõ là sai sự thật, nhằm xúc phạm nghiêm trọng nhân phẩm, danh dự hoặc gây thiệt hại đến quyền, lợi ích hợp pháp của người khác, có thể bị truy cứu trách nhiệm hình sự về tội vu khống theo Điều 156 Bộ luật Hình sự năm 2015. Khung hình phạt cao nhất đối với người phạm tội có thể đến 07 năm tù và có thể bị áp dụng hình phạt bổ sung là phạt tiền từ 10 triệu đồng đến 50 triệu đồng; cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ 01 năm đến 05 năm.

Dù đã có những nỗ lực trong việc xây dựng các quy định pháp lý để bảo vệ dữ liệu cá nhân và quyền lợi người sử dụng trong môi trường mạng, nhưng thực tế cho thấy pháp luật Việt Nam vẫn chưa hoàn thiện và không đủ đáp ứng được các thách thức do công nghệ Deepfake mang lại.

Một là, chưa có quy định chuyên biệt về Deepfake

Pháp luật Việt Nam hiện tại không có một quy định rõ ràng về công nghệ Deepfake từ định nghĩa cho đến các hành vi hay các biện pháp xử lý, điều này dẫn đến sự khó khăn trong việc xác định hành vi vi phạm và áp dụng chế tài xử lý. Các quy định về bảo vệ quyền lợi cá nhân, như quyền được bảo vệ danh dự, nhân phẩm, trong Bộ luật Dân sự 2015 và Bộ luật Hình sự 2015, chủ yếu áp dụng đối với hành vi xâm phạm quyền lợi cá nhân mà không đề cập trực tiếp đến các hành vi sử dụng công nghệ Deepfake.

Hai là, trách nhiệm của các nền tảng mạng xã hội chưa rõ ràng

Các nền tảng mạng xã hội như Facebook, YouTube, TikTok vẫn chưa chịu trách nhiệm rõ ràng về việc phát hiện và xử lý các video Deepfake. Mặc dù các nền tảng này có các chính sách để xử lý nội dung vi phạm, nhưng việc kiểm soát và ngừng phát tán các video Deepfake vẫn là một thách thức lớn. Điều này gây khó khăn trong việc bảo vệ quyền lợi của người sử dụng khi các video giả mạo vẫn dễ dàng được phát tán và lan truyền.

Ba là, chế tài xử lý còn yếu và không đồng bộ

Mặc dù pháp luật Việt Nam đã có các chế tài xử phạt trong Bộ luật Dân sự 2015 và Bộ luật Hình sự 2015 đối với các hành vi xâm phạm quyền lợi cá nhân, nhưng những chế tài này chưa đủ nghiêm khắc để đối phó với các vi phạm liên quan đến công nghệ Deepfake. Các mức xử phạt chưa đủ sức răn đe và không đủ hiệu quả trong việc ngăn chặn các hành vi lạm dụng công nghệ này.

Các bất cập trong việc thực thi pháp luật Việt Nam đối với công nghệ Deepfake có thể được lý giải bởi một số nguyên nhân chủ yếu:

Thứ nhất, sự phát triển nhanh chóng của công nghệ

Công nghệ Deepfake phát triển rất nhanh và thường xuyên thay đổi hình thức, chất lượng. Các sản phẩm từ công nghệ này có thể khiến cho khả năng phân biệt giữa thật và giả; đồng thời gây khó khăn trong việc xây dựng và cập nhật các quy định pháp lý để đối phó với những mối đe dọa.

Thứ hai, khả năng cảnh giác của người dùng internet còn hạn chế

Các cơ quan thực thi pháp luật và người dân còn thiếu nhận thức đầy đủ về những tác động của công nghệ Deepfake và các nguy cơ tiềm ẩn từ nó. Điều này dẫn đến sự thiếu hụt trong việc xây dựng các chiến lược và biện pháp phòng ngừa.

Sự chủ quan khi tiếp cận các nền tảng công nghệ và việc đăng tải thông tin, hình ảnh cá nhân lên các nền tảng này cũng tạo cơ hội cho các đối tượng lợi dụng vào các mục đích xấu như lừa đảo, xúc phạm danh dự, nhân phẩm...

Thứ ba, thiếu cơ chế phối hợp đồng bộ giữa các cơ quan

Việc xử lý các vụ việc liên quan đến công nghệ Deepfake đòi hỏi sự phối hợp chặt chẽ giữa các cơ quan chức năng như Bộ Thông tin và Truyền thông, Bộ Công an và các

nền tảng mạng xã hội. Tuy nhiên, sự phối hợp này vẫn chưa được thực hiện một cách đồng bộ và hiệu quả.

5. Một số giải pháp hoàn thiện pháp luật và nâng cao hiệu quả thực thi pháp luật Việt Nam về bảo vệ dữ liệu cá nhân trong kỷ nguyên số dưới tác động của công nghệ deepfake

Thứ nhất, bổ sung các quy định chuyên biệt về Deepfake

Cần xác định rõ khái niệm công nghệ Deepfake, những hành vi sử dụng Deepfake nào là hành vi vi phạm pháp luật, đặc biệt là khi tạo ra và phát tán các video, hình ảnh giả mạo nhằm xâm phạm quyền lợi cá nhân. Một trong những biện pháp cần thiết là bổ sung các quy định trong Bộ luật Hình sự 2015 để hình sự hóa hành vi sử dụng công nghệ Deepfake với mục đích bôi nhọ, lừa đảo, hoặc phá hoại danh dự của người khác. Việc quy định rõ ràng các hành vi vi phạm và mức xử phạt sẽ giúp cơ quan chức năng dễ dàng truy cứu và xử lý khi xảy ra vụ việc, đồng thời tạo ra một hành lang pháp lý minh bạch và có hiệu quả.

Thứ hai, tăng cường trách nhiệm của các nền tảng mạng xã hội

Với sự phát triển của các nền tảng như Facebook, YouTube, TikTok, việc phát tán các video Deepfake trở nên nhanh chóng và rộng rãi. Chính phủ cần yêu cầu các nền tảng mạng xã hội có nghĩa vụ phát hiện và gỡ bỏ các video Deepfake trong thời gian ngắn nhất, ít nhất là trong vòng 24 giờ kể từ khi nhận được báo cáo từ người dùng hoặc cơ quan chức năng. Ngoài ra, cần có các quy định yêu cầu các nền tảng này chủ động hợp tác với các cơ quan chức năng khi có yêu cầu cung cấp thông tin về nguồn gốc và người phát tán video giả mạo.

Để thực thi điều này, cần áp dụng các chế tài mạnh mẽ đối với các nền tảng không tuân thủ quy định, bao gồm các hình thức phạt hành chính nặng hoặc yêu cầu ngừng hoạt động trong một khoảng thời gian nhất định.

Thứ ba, nâng cao nhận thức và năng lực của cơ quan thực thi pháp luật

Để thực hiện điều này, cần thiết phải tổ chức các khóa đào tạo chuyên biệt về công nghệ Deepfake cho các cán bộ công an, kiểm sát viên, thẩm phán và các cơ quan liên quan. Những khóa đào tạo này không chỉ tập trung vào các khía cạnh kỹ thuật của công nghệ mà còn hướng đến việc hiểu rõ các phương thức và phương tiện mà tội phạm có thể sử dụng để lạm dụng công nghệ Deepfake trong các hành vi vi phạm pháp luật như bôi nhọ danh dự, lừa đảo hay phát tán thông tin sai sự thật. Cán bộ thực thi pháp luật cần được trang bị kiến thức về cách thức nhận diện các video giả mạo, các công cụ AI hỗ trợ phát hiện Deepfake, và các quy trình xử lý khi gặp phải các trường hợp này.

Bên cạnh việc đào tạo, cần thiết lập các cơ chế phối hợp giữa các cơ quan chức năng và các tổ chức, chuyên gia trong lĩnh vực công nghệ thông tin, nhằm tạo ra các nhóm chuyên trách để xử lý các vụ việc liên quan đến Deepfake. Điều này giúp cơ quan chức năng không chỉ ứng phó kịp thời mà còn xây dựng được đội ngũ chuyên gia có khả năng đối phó với những thách thức ngày càng gia tăng từ công nghệ mới này.

Thứ tư, xây dựng chế tài xử lý mạnh mẽ hơn

Bên cạnh các chế tài hình sự, cũng cần bổ sung các hình thức xử phạt hành chính đối với các hành vi phát tán video Deepfake trên mạng xã hội mà không được xử lý kịp thời. Các nền tảng mạng xã hội như Facebook, YouTube cần phải chịu trách nhiệm nếu không gỡ bỏ nhanh chóng các video Deepfake vi phạm khi được người dùng báo cáo, hoặc nếu không hợp tác với cơ quan chức năng trong việc điều tra và xác minh nguồn gốc của video.

Ngoài ra, việc yêu cầu các tổ chức phát tán video Deepfake phải bồi thường thiệt hại cho nạn nhân cũng là một giải pháp quan trọng. Các nạn nhân bị xâm phạm quyền lợi từ công nghệ Deepfake cần được bảo vệ, và việc bồi thường thiệt hại phải bao gồm cả các thiệt hại về tài chính và tinh thần.

6. Kết luận

Kỷ nguyên số là thời đại của khoa học máy tính và sự ra đời của công nghệ Deepfake ra đời là quy luật tất yếu. Những sản phẩm của công nghệ Deepfake trở thành vấn đề nhứt nhối trong việc bảo vệ dữ liệu cá nhân một cách an toàn khi mà hình ảnh cá nhân, xu hướng tình dục cá nhân thường xuyên trở thành đối tượng bị Deepfake xâm phạm, lợi dụng. Bị xâm phạm là thế, nhưng pháp luật Viêt Nam hiện nay chỉ dừng lại ở việc quy định về các trường hợp xâm phạm dữ liệu cá nhân thông thường, chưa có quy định cụ thể trong trường hợp cá nhân bị xâm phạm bởi công nghệ Deepfake. Công nghệ Deepfake, dù mang lại nhiều tiện ích, cũng đe dọa nghiêm trọng đến an ninh cá nhân và quyền riêng tư của người dùng. Cần có sự phối hợp giữa các quốc gia, các tổ chức công nghệ và cộng đồng trong việc phát triển các công cụ bảo mật, đồng thời hoàn thiện các chính sách pháp lý để bảo vệ dữ liệu cá nhân trong kỷ nguyên số. Việc duy trì sự kiểm soát và bảo vệ dữ liệu cá nhân trong bối cảnh công nghệ Deepfake phát triển mạnh mẽ là điều cần thiết để đảm bảo an ninh và quyền lợi của từng cá nhân.

DANH MỤC TÀI LIỆU THAM KHẢO

1. Quốc hội, 2015, Bộ luật Dân sự năm 2015;
2. Quốc hội, 2015, Bộ luật Hình sự năm 2015 (sửa đổi, bổ sung năm 2017);
3. Quốc hội, 2006, Luật Công nghệ thông tin 2006 (sửa đổi bổ sung 2018);
4. Quốc hội, 2023, Luật Giao dịch Điện tử năm 2023;
5. Chính phủ, 2013, Nghị định số 72/2013/NĐ – CP ngày 15/7/2013 về Quản lý, cung cấp dịch vụ internet và thông tin trên mạng;
6. Chính phủ, 2020, Nghị định số 15/2020/NĐ-CP ngày 03/02/2020 quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử;
7. Chính phủ, 2023, Nghị định số 13/2023/NĐ – CP ngày 17/4/2023 về Bảo vệ dữ liệu cá nhân;

8. Ngân hàng Nhà nước Việt Nam, 2024, Quyết định số 2345/QĐ-NHNN về triển khai các giải pháp an toàn, bảo mật trong thanh toán trực tuyến và thanh toán thẻ ngân hàng;

9. Law enforcement and the challenge of deepfakes, *"An Observatory Report from the Europol Innovation Lab (2022), Facing reality?"*;

10. Mdshohel Rana, Mohammad Nur Nobi, Beddhu Murali, Andrew H. Sung (2022), *Deepfake Detection: A Systematic Literature Review;*

11. Mullen, Molly (2022), *A New Reality: Deepfake Technology and the World Around Us*, Mitchell Hamline Law Review;

12. MikaWesterlund (2019), *The Emergence of Deepfake Technology: A , https://www.proquest.com/docview/2329154005?sourcetype=Scholarly%20Journals*;

13. Nguyễn Thị Chinh & Phan Thị Thu*, "Bảo vệ dữ liệu cá nhân trong bối cảnh cuộc cách mạnh công nghệ 4.0"*, Kỷ yếu Hội thảo khoa học Quốc gia: "Dữ liệu cá nhân trong dòng chảy kinh tế số Việt Nam";

14. Nguyễn Minh Hiếu, Lâm Vũ Từ Nghi, Đặng Lan Anh, Nguyễn Đình Việt Hưng, Nguyễn Thị Anh (2023), "*Dữ liệu cá nhân – Nên xem là hàng hóa hay không?"*, Kỷ yếu Khoa học Hội thảo Quốc gia – Dòng chảy Dữ liệu cá nhân trong kỷ nguyên số;

15. Tạp chí Cộng sản (2021), *Hội nhập quốc tế trong "kỷ nguyên số" và một số vấn đề đặt ra đối với Việt Nam*, truy cập tại https://www.tapchicongsan.org.vn/web/guest/quoc-phong-an-ninh-oi-ngoai1/-/2018/823137/hoi-nhap-quoc-te-trong-%E2%80%9Cky-nguyen-so%E2%80%9D-va-mot-so-van-de-dat-ra-doi-voi-viet-nam.aspx, truy cập ngày 5/7/2024.