

PHÁP LUẬT VỀ BẢO HỘ DỮ LIỆU CÁ NHÂN TRONG BỐI CẢNH PHÁT TRIỂN
TRÍ TUỆ NHÂN TẠO VÀ CÁC CÔNG NGHỆ SỐ MỚI NỔI KHÁC

NGUYỄN QUỲNH TRANG*

Ngày nhận bài: 29/01/2022

Ngày phản biện: 09/02/2022

Ngày đăng bài: 30/03/2022

Tóm tắt:

Cuộc cách mạng công nghiệp 4.0 với sự phát triển mạnh mẽ của các công nghệ như trí tuệ nhân tạo, tự động hoá, điện toán lượng tử, thực tế ảo, internet vạn vật... đã thay đổi thế giới và nhận thức của con người. Trong đó, trí tuệ nhân tạo được nhắc đến thường xuyên trên các phương tiện truyền thông đã ảnh hưởng đến hầu hết các ngành, lĩnh vực của đời sống kinh tế - xã hội, nhất là về dữ liệu cá nhân. Bên cạnh những lợi ích mà AI và các công nghệ số khác đem đến chúng ta không thể phủ nhận, vẫn còn tồn tại các vấn đề ảnh hưởng trực tiếp đến cuộc sống của con người, trong đó có quyền riêng tư, dữ liệu cá nhân. Bài viết tìm hiểu về trí tuệ nhân tạo và các công nghệ số mới nổi khác; các quy định của pháp luật về bảo hộ dữ liệu cá nhân như pháp luật Hoa Kỳ, Châu Âu (EU), pháp luật Việt Nam, từ đó đánh giá những lợi ích và rủi ro đối với các quy định bảo hộ dữ liệu cá nhân, đề xuất một số kiến nghị hoàn thiện pháp luật trong sự phát triển của AI và các công nghệ số.

Từ khoá:

Trí tuệ nhân tạo, dữ liệu cá nhân, pháp luật, bảo hộ

Abstract:

The fourth industrial revolution has flourished with emerging digital technologies like Artificial Intelligence (AI), automation, quantum computing, virtual reality (VR), Internet of Things (IoT), etc that change the world eternally. In there, the most mentioned term in the mass media was AI, which truly influent to almost every area of our social-economic life, especially personal data. It is undeniable that the benefits from AI are magnificent, however, we also need to objectively evaluate the seriousness of personal rights, personal data's violation during AI application in order to build a legal framework regulating the issue in detail. The paper explores the context of developing AI and other emerging digital technologies, benefits and challenges for personal data protection, current laws and proposes some recommendations in the future.

Keywords:

Artificial Intelligence (AI), emerging digital technologies, personal data, law, protection

* ThS., Viện Nhà nước và Pháp luật, Học viện Chính trị quốc gia Hồ Chí Minh;
Email: ngquynhtrang340450@gmail.com.

• Ghi chú: Tải bài viết toàn văn tại địa chỉ: <http://tapchi.hul.edu.vn>.

1. Khái quát về trí tuệ nhân tạo và các công nghệ số mới nổi

1.1. Trí tuệ nhân tạo

Trí tuệ nhân tạo (AI) đang dần trở thành thuật ngữ phổ biến trong công chúng nói chung và các lĩnh vực cụ thể nói riêng với những lợi ích mà nó mang lại cho con người. Người khai sinh ra khái niệm này là Alan Turing trong một nghiên cứu năm 1950¹ đã đưa ra câu hỏi “máy móc có thể suy nghĩ không” và tìm đáp án thông qua một thí nghiệm (ngày nay được gọi là “thí nghiệm Turing”) mà người hỏi sẽ cố gắng phân biệt đâu là câu trả lời của máy tính và đâu là câu trả lời của con người. Từ đó ông định nghĩa: “AI là hệ thống có khả năng hành động như con người”. Stuart Russell và Peter Norvig tiếp tục cho ra đời cuốn sách được ví như giáo trình của mọi học sinh ngành AI², trong đó đào sâu nghiên cứu bốn mục tiêu tiềm năng hay khái niệm của AI, phân biệt hệ thống máy tính dựa trên nền tảng tư duy hợp lý và hành động: Với cách tiếp cận của con người, đó là hệ thống nghĩ như con người, hành động như con người-

Kế thừa những thành quả của các nghiên cứu đi trước, John McCarthy cho rằng AI là khoa học và kỹ thuật chế tạo ra các máy thông minh, nhất là các chương trình máy tính thông minh. Tương tự như nhiệm vụ sử dụng máy tính để hiểu trí tuệ con người, nhưng AI không giới hạn bản thân nó trước những phương thức có thể quan sát bằng cơ chế sinh học thông thường³.

Dưới dạng đơn giản nhất, AI là một lĩnh vực kết hợp giữa khoa học máy tính và tập dữ liệu chuẩn mạnh (robust datasets) nhằm giải quyết vấn đề. Nó còn bao hàm liên ngành học máy (machine learning) và học sâu (deep learning) thường được nhắc đến khi liên kết với AI. Những kỹ thuật này cùng với thuật toán AI tạo ra hệ thống chuyên gia dự đoán hoặc phân loại dựa trên dữ liệu đầu vào⁴.

Để dễ hình dung, có thể kể đến rất nhiều ứng dụng thực tế của hệ thống AI hiện nay như:

- Nhận diện giọng nói: Còn được biết đến là nhận diện giọng nói tự động (ASR), nhận diện giọng nói máy tính, hay dịch từ giọng nói sang văn bản trong đó ứng dụng quá trình xử lý ngôn ngữ tự nhiên (NLP) – một kỹ thuật khó của AI. Nhiều thiết bị di động tích

¹ A. M. Turing (1950), *Computing Machinery and Intelligence*, Mind 49: p.433-460.

² Stuart Russell, Peter Norvig (1994), *Artificial Intelligence: A Modern Approach*, Englewood Cliffs, NJ: Prentice Hall.

³ John McCarthy (2004), *What is Artificial intelligence?*, Stanford University, Stanford.

⁴ IBM (2019), What is artificial intelligence, <https://www.ibm.com/cloud/learn/what-is-artificial-intelligence>, truy cập ngày 30/6/2021.

hợp nhận diện giọng nói vào phần mềm hệ thống như cho phép tìm kiếm bằng giọng nói (Siri) hoặc cung cấp nhiều khả năng tương tác khi đang gõ văn bản.

- Dịch vụ khách hàng: Robot trò chuyện trực tuyến (online chatbots) đang thay thế con người trong chăm sóc khách hàng, trả lời các câu hỏi thường gặp xung quanh vấn đề như vận chuyển hàng hoá hoặc đưa ra tư vấn đối với từng khách hàng, bán chéo (cross-selling) hoặc gợi ý kích cỡ cho người sử dụng. Chatbots đang thay đổi cách chúng ta nghĩ về sự cam kết của khách hàng thông qua website và các nền tảng mạng xã hội khác. Ví dụ robot trả lời tự động trên các trang web thương mại trực tuyến với Tổng đài trợ lý ảo, ứng dụng tin nhắn như Slack hoặc Facebook Messenger, trong đó các thao tác thường được thực hiện bởi trợ lý ảo và trợ lý giọng nói.

- Thị giác máy tính: Công nghệ AI này cho phép máy tính và hệ thống chuyển hoá thông tin có nghĩa từ các hình ảnh, video kỹ thuật số và các dữ liệu đầu vào trực quan khác, và thực hiện hoạt động khác dựa trên dữ liệu đó. Với các mạng thần kinh xoắn, thị giác máy tính ứng dụng trong gắn thẻ ảnh trên mạng xã hội, chụp X-quang trong y tế, và ô tô tự lái trong công nghiệp ô tô.

- Hệ thống gợi ý: Sử dụng tổng hợp dữ liệu hành vi trong quá khứ, thuật toán AI giúp tìm kiếm các xu hướng dữ liệu nhằm phát triển các bước bán chéo hiệu quả. Nó được dùng để tạo các gợi ý chương trình bổ sung cho khách hàng trong quá trình thanh toán cho các nhà bán lẻ trực tuyến.

- Giao dịch chứng khoán tự động: Được thiết kế để tối ưu hoá danh mục đầu tư chứng khoán, nền tảng giao dịch tần suất cao điều khiển bằng AI có thể tạo ra hàng nghìn, thậm chí hàng triệu giao dịch một ngày mà không cần sự can thiệp của con người.

1.2. Các công nghệ số khác

Cuộc cách mạng công nghiệp 4.0 đã mở ra cách tiếp cận mới chưa từng có đến sự phát triển của kinh tế, văn hoá, xã hội với các công nghệ số mới nổi như tự động hoá, điện toán lượng tử, dữ liệu lớn, thực tế ảo, internet vạn vật...

- Tự động hoá là một thuật ngữ chỉ việc ứng dụng máy móc để hạn chế tối đa sự can thiệp của con người. Tự động hoá góp phần nâng cao hiệu suất, độ tin cậy và tốc độ thực hiện nhiều việc một lúc do con người đảm nhiệm trước đây. Tự động hoá được sử dụng trong nhiều lĩnh vực như sản xuất, vận chuyển, tiện ích, quốc phòng, phương tiện, tính toán và gần nhất là công nghệ thông tin. Ví dụ:

+ Nhà thông minh sử dụng tổ hợp phần cứng và phần mềm công nghệ cho phép điều khiển mọi thiết bị trong nhà một cách tự động mà không cần sự có mặt của con người.

+ Kiểm tra trang web tự động: sắp xếp và tiêu chuẩn hoá website thông qua các thay đổi về thông số cấu hình trong quá trình phát triển.

+ Trung tâm dữ liệu tự động hoá cho phép các chương trình phần mềm thực hiện tính toán khối lượng lớn dữ liệu bao gồm hệ thống hoạt động tự động.

- Điện toán lượng tử là một công nghệ mới nổi có thể tăng sức mạnh máy tính hiện có theo cấp số mũ giúp giải quyết vấn đề mà chúng ta không thể làm được với máy tính thông thường. Công nghệ này sẽ bẻ khoá các phần mềm một cách dễ dàng và phá vỡ các biện pháp bảo mật hiện hành sử dụng dữ liệu mã hoá trong ngân hàng và các ngành công nghiệp khác. Ngoài ra, điện toán lượng tử còn được ứng dụng trong ngành khoa học, giúp trả lời những câu hỏi gây tranh cãi giữa các nhà khoa học suốt nhiều năm qua.

- Big data đã tạo ra sự tích lũy dữ liệu khổng lồ từ nhiều nguồn khác nhau, rất khác với cách thu thập, lưu trữ và phân tích dữ liệu truyền thống. Thông thường, nguồn dữ liệu bao gồm mạng nội bộ, bảng tính, cơ sở dữ liệu, tuy nhiên, ngày nay cả email, tài liệu PDF, ảnh, video, âm thanh, bài đăng trên mạng xã hội, kết quả thu được từ hoạt động và giao dịch của doanh nghiệp trên hàng tỷ trang web cũng nằm trong đó. Các nguồn dữ liệu trên sau đó được phân phối nhưng liên kết với nhau, phụ thuộc lẫn nhau tạo ra một nền tảng để chia sẻ tất cả dữ liệu có liên quan. Điều này khiến big data trở nên thiết yếu, quan trọng và giá trị trong giải quyết vô số vấn đề, tạo ra các cơ hội mới từ việc phân tích dữ liệu⁵.

- Thực tế ảo chỉ sự mô phỏng được tạo ra bởi máy tính trong đó con người có thể tương tác với môi trường 3D nhân tạo khi sử dụng thiết bị điện tử, như kính hoặc găng tay cảm biến. Điều đặc biệt là người dùng có khả năng cảm nhận mọi thứ như thật trong thế giới ảo. Ví dụ đơn giản nhất của thực tế ảo là phim 3D, khi đeo kính 3D, người xem có cảm giác mình là một phần của bộ phim ngay tại chỗ với hình ảnh và âm thanh sống động. Ngoài ra, thực tế ảo còn được áp dụng vào huấn luyện thể thao, bán hàng, du hành vũ trụ, thực hành y khoa⁶...

- Internet vạn vật chỉ việc tăng cường sử dụng các cảm biến để ghi lại sự vật hiện tượng như âm thanh, xúc giác, chuyển động, nhiệt độ, thậm chí cấu tạo hoá học nhằm tự động thu thập dữ liệu về con người, môi trường, đối tượng và chuyển giao những thông tin

⁵ UNESCO IITE and TheNextMinds (2020). *Artificial Intelligence: Media and Information Literacy, Human Rights and Freedom of Expression*.

⁶ Investopedia (2020), *Virtual reality*, <https://www.investopedia.com/terms/v/virtual-reality.asp>, truy cập ngày 30/6/2021.

đó trên internet⁷. Ứng dụng công nghệ này được lý giải bởi các cảm biến ngày càng rẻ và tốt hơn, cũng như kết nối internet và khả năng tính toán tăng lên. Ví dụ về những tiện ích mà internet vạn vật mang lại cho cộng đồng bao gồm:

+ Các thiết bị chăm sóc sức khỏe thông minh có thể giám sát bệnh nhân và cảnh báo cơ quan y tế nếu được yêu cầu.

+ Các cảm biến trong cơ sở hạ tầng về năng lượng và nước cho phép các nhà cung cấp theo dõi và quản lý bảo trì.

+ Các cảm biến trong lòng đất có thể đo lường độ ẩm giúp nông dân quản lý sử dụng nước và cải thiện mùa màng.

2. Quy định của pháp luật về bảo hộ dữ liệu cá nhân

2.1. Quy định của pháp luật một số quốc gia trên thế giới

Thứ nhất, theo pháp luật của châu Âu, cụ thể Điều 4 Quy định chung về bảo vệ dữ liệu của Liên minh châu Âu (GDPR), dữ liệu cá nhân được hiểu là “*bất kỳ thông tin nào liên quan đến việc nhận dạng trực tiếp hay gián tiếp một người hoặc một thực thể tự nhiên như tên, số chứng minh thư/căn cước công dân, nơi ở, mã định danh online hoặc một/một vài yếu tố xác định về hình dáng, gen, tâm thần, hoàn cảnh kinh tế, văn hoá, xã hội của người đó*”⁸.

Khái niệm dữ liệu cá nhân (personal data) của châu Âu rộng hơn khái niệm thông tin cá nhân (personally identifiable information) ở Mỹ theo hướng dẫn của Viện an ninh công nghệ máy tính quốc gia là “*bất cứ thông tin nào được dùng để phân biệt, nhận dạng danh tính của một cá nhân như tên, số an sinh xã hội, thông tin sinh trắc học nói riêng hay kết hợp với các thông tin nhận dạng khác như ngày sinh hoặc nơi sinh*”⁹.

Việc bảo vệ thông tin riêng cũng như thông tin cá nhân là vấn đề nóng không chỉ ở Việt Nam mà còn ở nhiều nước trên thế giới. Hiện nay, có khoảng 40 quốc gia đã ban hành các quy định pháp luật về bảo vệ thông tin cá nhân trên mạng. Trong đó, Liên minh châu Âu là hình mẫu bảo hộ dữ liệu cá nhân với GDPR có tầm ảnh hưởng đến nhiều quốc gia và khu vực, đặc biệt là các tổ chức xử lý bất kỳ dữ liệu cá nhân nào của công dân EU và mức phạt lên đến 20 triệu EUR, cao hơn nữa là 4% doanh thu toàn cầu nếu một doanh nghiệp

⁷ Department of Industry, Science, Energy and Resources, Australia Government, Understanding emerging technologies, <https://www.industry.gov.au/data-and-publications/australias-tech-future/introduction/understanding-emerging-technologies>, truy cập ngày 30/6/2021.

⁸ EU (2016), General Data Protection Regulation, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>, truy cập ngày 1/7/2021.

⁹ National Institute of Standards and Technology, U.S. Department of Commerce, <https://csrc.nist.gov/glossary/term/PII>, truy cập ngày 8/11/2021.

nào đó vi phạm về việc bảo vệ dữ liệu cá nhân (Điều 83 GDPR). Ngày nay, với những quy định quốc tế về kiểm soát an ninh và bảo vệ dữ liệu, tương lai sẽ còn tiếp tục xuất hiện các quy định khắt khe hơn, chế tài mạnh hơn và tổn hại danh tiếng nhiều hơn đối với chủ thể cố tình không tuân thủ.

Thứ hai, theo pháp luật Hoa Kỳ, không có luật chung trên phạm vi liên bang mà chỉ một số bang ban hành quy định bảo vệ thông tin cá nhân như bang Virginia, Colorado, California với Đạo luật quyền riêng tư của người tiêu dùng (CCPA) tôn trọng quyền riêng tư và bảo vệ người tiêu dùng. Điều 105, 110, 115, 120 Phần 3 Đạo luật cho phép các cư dân của bang thiết lập một cách chính xác việc dữ liệu cá nhân của họ được thu thập như thế nào và được sử dụng ra sao. Các bang khác đã có dự thảo luật hoặc đang trong quá trình thông qua bao gồm Ohio, Pennsylvania, New York, New Jersey, North Carolina, Massachusetts¹⁰. Ngoài ra, quy định về bảo vệ thông tin cá nhân còn xuất hiện rải rác ở nhiều đạo luật khác như: Đạo luật về tự do thông tin (FOIA); Đạo luật về sự riêng tư; Đạo luật chính phủ điện tử; Đạo luật Báo cáo Tín dụng Công bằng; Đạo luật Bảo mật truyền thông điện tử...¹¹

2.2. Quy định của pháp luật Việt Nam

2.2.1. Dữ liệu cá nhân

Ở Việt Nam, thuật ngữ “thông tin cá nhân” (TTCN) được sử dụng phổ biến hơn là “dữ liệu cá nhân” mặc dù có nhiều nét tương đồng. Thuật ngữ này xuất hiện rải rác trong các văn bản quy phạm pháp luật như Luật Dược 2005 tại khoản 3 Điều 57: người tham gia thử lâm sàng “*được giữ bí mật về những thông tin cá nhân có liên quan*”; Luật Hàng không dân dụng 2006 tại điểm đ khoản 2 Điều 126: doanh nghiệp kinh doanh hệ thống đặt ghế chỗ bằng máy tính phải “*bảo mật thông tin cá nhân của khách hàng*”; Luật Công nghệ thông tin 2006 tại khoản 1 Điều 21: “*Tổ chức, cá nhân thu thập, xử lý và sử dụng thông tin cá nhân của người khác trên môi trường mạng phải được người đó đồng ý*”, tuy nhiên chưa có định nghĩa chính xác TTCN là gì. Đến khoản 5 Điều 3 Nghị định 64/2007/NĐ-CP về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước mới quy định TTCN là “*thông tin đủ để xác định chính xác danh tính một cá nhân, bao gồm ít nhất nội dung trong những thông tin sau đây: họ tên, ngày sinh, nghề nghiệp, chức danh, địa chỉ liên hệ, địa chỉ thư điện tử, số điện thoại, số chứng minh nhân dân, số hộ chiếu*”. Tiếp đó,

¹⁰ Iapp (2021), *US State Privacy Legislation Tracker*,

https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Map.pdf, truy cập ngày 5/7/2021.

¹¹ Lê Thị Thuỳ Trang (2017), *Nghiên cứu một số quy định về bảo vệ thông tin cá nhân trên thế giới và tại Việt Nam*, Trang Thông tin điện tử Cục Tin học hoá, Bộ Thông tin và Truyền thông.

TRƯỜNG ĐẠI HỌC LUẬT, ĐẠI HỌC HUẾ

khoản 13 Điều 3 Nghị định 52/2013/NĐ-CP về thương mại điện tử cũng định nghĩa TTCN là “các thông tin góp phần định danh một cá nhân cụ thể, bao gồm tên, tuổi, địa chỉ nhà riêng, số điện thoại, thông tin y tế, số tài khoản, thông tin về các giao dịch thanh toán cá nhân và những thông tin khác mà cá nhân mong muốn giữ bí mật”.

Lần đầu tiên thuật ngữ TTCN được quy định trong một văn bản luật cụ thể là “thông tin gắn với việc xác định danh tính của một người cụ thể” theo khoản 15 Điều 3 Luật An toàn thông tin mạng năm 2015 được Quốc hội thông qua ngày 19/11/2015 và có hiệu lực từ ngày 1/7/2016.

Gần đây nhất, Dự thảo Nghị định về bảo vệ dữ liệu cá nhân 2021 được lấy ý kiến rộng rãi cho thấy sự quan tâm của Nhà nước và người dân đến vấn đề này. Theo khoản 1 Điều 2, dữ liệu cá nhân là “dữ liệu về cá nhân hoặc liên quan đến việc xác định hoặc có thể xác định một cá nhân cụ thể”. Dự thảo phân biệt rõ hai loại dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm lần lượt tại khoản 2 và khoản 3. Trong đó, Dự thảo liệt kê các loại dữ liệu cá nhân nhạy cảm và định nghĩa một số thuật ngữ nội hàm mang tính thời sự cao như dữ liệu cá nhân về tình trạng giới tính, về tài chính.

Dữ liệu cá nhân cơ bản (khoản 2)	Dữ liệu cá nhân nhạy cảm (khoản 3)
<p>a) Họ, chữ đệm và tên khai sinh, bí danh (nếu có);</p> <p>b) Ngày, tháng, năm sinh; ngày, tháng, năm chết hoặc mất tích;</p> <p>c) Nhóm máu, giới tính;</p> <p>d) Nơi sinh, nơi đăng ký khai sinh, nơi thường trú, nơi ở hiện tại, quê quán, địa chỉ liên hệ, địa chỉ thư điện tử;</p> <p>đ) Trình độ học vấn;</p> <p>e) Dân tộc;</p> <p>g) Quốc tịch;</p>	<p>a) Dữ liệu cá nhân về quan điểm chính trị, tôn giáo;</p> <p>b) Dữ liệu cá nhân về tình trạng sức khỏe là thông tin liên quan đến trạng thái sức khỏe thể chất hoặc tinh thần của chủ thể dữ liệu được thu thập, xác định trong quá trình đăng ký hoặc cung cấp dịch vụ y tế;</p> <p>c) Dữ liệu cá nhân về di truyền là thông tin liên quan đến các đặc điểm di truyền được thừa hưởng hoặc có được của cá nhân;</p> <p>d) Dữ liệu cá nhân về sinh trắc học là thông tin về thuộc tính vật lý, đặc điểm sinh học riêng của mỗi cá nhân;</p> <p>đ) Dữ liệu cá nhân về tình trạng giới tính là thông tin về người được xác định có giới tính nam, nữ, người kết hợp giữa nữ và nam, không phải nữ hoàn toàn hoặc nam toàn, không phải nữ cũng không phải nam hoặc là tình trạng của chủ thể dữ liệu có ý thức về giới tính không phù hợp với</p>

<p>h) Số điện thoại;</p> <p>i) Số chứng minh nhân dân, số hộ chiếu, số căn cước công dân, số giấy phép lái xe, số biển số xe, số mã số thuế cá nhân, số bảo hiểm xã hội;</p> <p>k) Tình trạng hôn nhân;</p> <p>l) Dữ liệu phản ánh hoạt động hoặc lịch sử hoạt động trên không gian mạng.</p>	<p>giới tính được xác định khi sinh;</p> <p>e) Dữ liệu cá nhân về đời sống, xu hướng tình dục;</p> <p>g) Dữ liệu cá nhân về tội phạm, hành vi phạm tội được thu thập, lưu trữ bởi các cơ quan thực thi pháp luật;</p> <p>h) Dữ liệu cá nhân về tài chính là thông tin được sử dụng để xác định tài khoản, thẻ, công cụ thanh toán do tổ chức tài chính cung cấp cho chủ thẻ dữ liệu hoặc thông tin về mối quan hệ giữa tổ chức tài chính, dữ liệu tiền gốc với chủ thẻ dữ liệu, bao gồm cả hồ sơ, tình trạng tài chính, lịch sử tín dụng, mức thu nhập;</p> <p>i) Dữ liệu cá nhân về vị trí là thông tin về vị trí địa lý thực tế của cá nhân ở quá khứ và hiện tại;</p> <p>k) Dữ liệu cá nhân về các mối quan hệ xã hội;</p> <p>l) Dữ liệu cá nhân khác được pháp luật quy định là đặc thù và cần có biện pháp bảo mật cần thiết.</p>
---	--

2.2.2. Bảo hộ dữ liệu cá nhân

Cuộc cách mạng công nghiệp lần thứ tư với AI và các công nghệ số đã làm thay đổi nhận thức về các loại tài sản. Rất nhiều loại “tài sản ảo”, tài sản vô hình có thể quy đổi ra thành tiền, thành tài sản thật. Trong xu thế đó, các loại dữ liệu, đặc biệt là dữ liệu cá nhân, trở nên có giá trị và trở thành một loại tài sản phi truyền thống¹². Do vậy, dữ liệu cá nhân rất cần được bảo vệ không chỉ với tư cách là quyền nhân thân đơn thuần mà còn hơn thế nữa.

Bảo hộ dữ liệu cá nhân thường được hiểu là bảo vệ TTCN ở Việt Nam ngày càng trở nên cấp thiết trong bối cảnh phát triển AI và các công nghệ số khác. Nước ta đang trong quá trình chuyển đổi số trên quy mô quốc gia, điều đó đồng nghĩa với hệ thống cơ sở dữ liệu quản lý công dân vô cùng lớn đòi hỏi cập nhật, bổ sung đầu vào liên tục. Hầu hết các ngành, lĩnh vực đều sử dụng dữ liệu cá nhân để xử lý vận hành như: hành chính, y tế, hình sự, hộ tịch, quốc tịch, chứng thực, thương mại điện tử, giáo dục, tài chính, ngân hàng, thuế và hoạt động thuế, công nghệ thông tin, truyền thông... Nếu không được bảo vệ chặt chẽ, nghiêm ngặt trước những kẻ tấn công, tội phạm hay virus, cộng với sự lơ là thiếu thận trọng của bản thân chủ thể dữ liệu thì nguy cơ rò rỉ TTCN hoặc mua bán trái phép rất dễ xảy ra.

¹² Lê Sơn (2021), *Cần coi dữ liệu cá nhân là một loại tài sản phi truyền thống*, <http://baochinhphu.vn/Phap-luat/Can-coi-du-lieu-ca-nhan-la-mot-loai-tai-san-phi-truyen-thong/434039.vgp>, truy cập ngày 4/7/2021.

Bằng chứng là cuối năm 2019, TTCN của 2 triệu khách hàng được cho là của Ngân hàng MSB đã bị đăng tải miễn phí, công khai trên Raidforums (diễn đàn mua bán dữ liệu của các hacker)¹³. Ông lớn Facebook cũng không ngoại lệ, khi TTCN của hơn 533 triệu người dùng ở 106 quốc gia bị đánh cắp từ lỗ hổng bảo mật đã vá năm 2019, rò rỉ trên một diễn đàn tin tặc bao gồm số điện thoại, tên định danh (ID) Facebook, họ tên, nơi ở, ngày sinh, thậm chí tiểu sử và địa chỉ email¹⁴. Trong đó, khoảng 300.000 người Việt là nạn nhân bởi tốc độ phát triển internet cao nhất thế giới, số lượng người dùng mạng xã hội facebook là 58 triệu tài khoản và có 62 triệu tài khoản google. Đi kèm với đó là lượng dữ liệu phát sinh từ hàng chục triệu người dùng cũng tăng lên nhanh chóng. Việc mạo danh, giả danh người dùng để lừa đảo, chiếm đoạt tài sản là hành vi nguy hiểm diễn ra phổ biến trên không gian mạng. Thách thức trước những dịch vụ mới, việc sử dụng, cung cấp TTCN trong thanh toán trực tuyến, thương mại điện tử, trò chơi trực tuyến, kinh doanh tiền ảo, kinh doanh đa cấp qua mạng... đã đặt ra nhiều vấn đề liên quan tới an ninh quốc gia, trật tự an toàn xã hội gây nguy cơ mất an ninh mạng¹⁵. Do đó, phải đảm bảo cho thông tin cá nhân được sử dụng đúng mục đích, phục vụ đặc lực cho xã hội, hạn chế tối đa nguy cơ bị sử dụng, lạm dụng và có cơ chế, chế tài xử lý các hành vi vi phạm.

Dự thảo Nghị định về bảo vệ dữ liệu cá nhân 2021 cũng đưa ra khái niệm bảo vệ dữ liệu cá nhân là “phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm quy định của pháp luật về dữ liệu cá nhân” (khoản 4 Điều 2).

2.2.3. Thực trạng quy định pháp luật Việt Nam

* Những kết quả đạt được:

Những kinh nghiệm của Mỹ, châu Âu và nhiều tổ chức, doanh nghiệp nước ngoài... đã được Việt Nam nghiên cứu, tiếp thu và căn cứ vào tình hình thực tiễn. Pháp luật Việt Nam đã bước đầu quan tâm đến vấn đề bảo hộ dữ liệu cá nhân thể hiện ở một số luật, bộ luật. Bảo vệ TTCN xuất hiện trong Luật Công nghệ thông tin 2006 liên quan đến thu thập, xử lý, sử dụng và chuyển nhượng trên môi trường mạng chứ không quy định các biện pháp bảo vệ TTCN nói chung. Ngoài ra, Luật Bảo vệ người tiêu dùng 2010 cũng có quy định cụ thể đối với bảo vệ thông tin người tiêu dùng và trách nhiệm của các chủ thể liên quan. Một quy định khác về bảo hộ dữ liệu cá nhân là Điều 38 Bộ luật Dân sự 2015 về quyền về đời

¹³ Bích Thủy (2019), *Ngân hàng MSB bị lộ 2 triệu dữ liệu khách hàng*, <http://antoanthongtin.vn/an-toan-thong-tin/ngan-hang-msb-bi-lo-2-trieu-du-lieu-khach-hang-105655>, truy cập ngày 4/7/2021.

¹⁴ Hoàng Linh (2021), *Hơn 533 người dùng Facebook bị rò rỉ dữ liệu cá nhân*, <https://hanoimoi.com.vn/tin-tuc/Oto-xemay/995429/hon-533-trieu-nguoi-dung-facebook-bi-ro-ri-du-lieu-ca-nhan>, truy cập ngày 5/7/2021.

¹⁵ Ngọc Bích (2019), *Nguy hiểm từ việc lọt, lộ thông tin cá nhân trên mạng Internet*, <https://cand.com.vn/Cong-nghe/Nguy-hiem-tu-viec-lot-lo-thong-tin-ca-nhan-tren-mang-Internet-i530219/>, truy cập ngày 5/7/2021.

sống riêng tư, bí mật cá nhân, bí mật gia đình. Cùng với đó là Luật An toàn thông tin mạng 2015 với nguyên tắc bảo vệ TTCN trên mạng (Điều 16), việc thu thập và sử dụng TTCN (Điều 17), việc cập nhật, sửa đổi và hủy bỏ TTCN (Điều 18), yêu cầu bảo đảm an toàn TTCN trên mạng (Điều 19) và trách nhiệm của cơ quan quản lý nhà nước trong bảo vệ TTCN trên mạng (Điều 20)¹⁶.

Phạm vi điều chỉnh của Luật An toàn thông tin mạng chỉ quy định các vấn đề liên quan đến kỹ thuật nhằm đảm bảo thông tin truyền đưa trên mạng được nguyên vẹn, không bị gián đoạn, sửa đổi hoặc phá hoại, được bảo đảm bí mật, nên không điều chỉnh vấn đề liên quan đến nội dung thông tin và thông tin riêng¹⁷. Tuy nhiên, tại Điều 18 đã quy định rõ, chủ thể TTCN có quyền yêu cầu tổ chức, cá nhân xử lý TTCN cập nhật, sửa đổi, hủy TTCN của mình mà tổ chức, cá nhân đó đã thu thập, lưu trữ, hoặc ngừng cung cấp TTCN của mình cho bên thứ ba. Ngay khi nhận được yêu cầu, phía tổ chức, cá nhân xử lý TTCN có trách nhiệm thực hiện và thông báo lại cho chủ thể TTCN hoặc cung cấp quyền tiếp cận để họ tự cập nhật, sửa đổi, hủy bỏ. Luật cũng quy định tổ chức, cá nhân xử lý TTCN phải hủy bỏ TTCN đã được lưu trữ khi đã hoàn thành mục đích sử dụng hoặc hết thời hạn lưu trữ và thông báo cho chủ thể biết. Ngoài ra, cần thiết lập kênh thông tin trực tuyến, xử lý các phản ánh của người dân về các vấn đề bảo vệ TTCN. Một điểm mới của Luật là chỉ rõ trách nhiệm của chính người dùng trong việc bảo vệ TTCN của mình, trên nguyên tắc chung là mỗi người phải có trách nhiệm tự bảo vệ TTCN và tự chịu trách nhiệm khi cung cấp những thông tin đó trên mạng. Về chế tài xử phạt đối với các hành vi phát tán, chia sẻ TTCN, tùy theo mức độ, hành vi thì tổ chức, cá nhân vi phạm sẽ bị xử lý vi phạm hành chính hoặc xử lý trách nhiệm hình sự theo các quy định pháp luật hiện hành.

Đáng chú ý, ngày 09/02/2021, Bộ Công an đã công bố dự thảo Nghị định quy định về bảo vệ dữ liệu cá nhân để lấy ý kiến đóng góp của các cơ quan, tổ chức, cá nhân. Dự thảo Nghị định gồm 06 chương 30 điều, quy định về dữ liệu cá nhân, xử lý dữ liệu cá nhân, biện pháp bảo vệ dữ liệu cá nhân, Ủy ban bảo vệ dữ liệu cá nhân, xử lý vi phạm về dữ liệu cá nhân, trách nhiệm bảo vệ dữ liệu cá nhân của cơ quan, tổ chức, cá nhân có liên quan. Đối với việc xử lý dữ liệu cá nhân, Chương II của dự thảo quy định cụ thể quyền của chủ thể dữ liệu liên quan đến tiết lộ; hạn chế tiếp cận dữ liệu cá nhân; xử lý dữ liệu cá nhân sau khi chủ thể dữ liệu chết; xử lý dữ liệu cá nhân trong trường hợp không có sự đồng ý của

¹⁶ Nguyễn Văn Cương (2020), *Thực trạng pháp luật về bảo vệ thông tin cá nhân ở Việt Nam hiện nay và hướng hoàn thiện*, Tạp chí Nghiên cứu Lập pháp số 15 (415), tháng 8/2020.

¹⁷ Công an Trà Vinh (2016), *Quy định pháp luật về việc bảo vệ thông tin cá nhân*, <http://congan.travinh.gov.vn/ch10/93-Quy-dinh-phap-luat-ve-viec-bao-ve-thong-tin-ca-nhan.html>, truy cập ngày 15/7/2021.

chủ thể dữ liệu; thông báo cho chủ thể dữ liệu về việc xử lý dữ liệu cá nhân; xử lý dữ liệu cá nhân phục vụ công tác nghiên cứu khoa học hoặc thống kê; xử lý dữ liệu cá nhân tự động, dữ liệu cá nhân của trẻ em...

Việc xử lý vi phạm quy định bảo vệ dữ liệu cá nhân được áp dụng đối với toàn bộ các tổ chức, doanh nghiệp, cá nhân trong và ngoài nước có hoạt động kinh doanh tại Việt Nam. Điều 22 của dự thảo quy định cụ thể mức xử phạt hành chính đối với những hành vi vi phạm quy định về xử lý dữ liệu cá nhân từ 50.000.000 đồng đến 100.000.000 đồng. Ngoài mức phạt được quy định, trường hợp Bên xử lý dữ liệu cá nhân vi phạm nhiều lần, với hậu quả lớn có thể bị phạt tối đa 5% tổng doanh thu¹⁸.

* Một số hạn chế:

Thực tế, bảo vệ dữ liệu cá nhân ở Việt Nam được quy định tản mát ở nhiều văn bản thuộc các lĩnh vực khác nhau và với các cấp độ khác nhau (Luật, Nghị định, Thông tư liên tịch, Thông tư, thậm chí là Quyết định của Bộ trưởng). Vì vậy, đã dẫn đến tình trạng còn một số văn bản quy phạm pháp luật liên quan đến bảo vệ dữ liệu cá nhân có quy định mâu thuẫn, chồng chéo, bất cập hoặc chưa phù hợp với thực tiễn. Điều đó đòi hỏi phải có một đạo luật riêng thống nhất điều chỉnh trực tiếp, cụ thể vấn đề này.

Thứ nhất, chưa thống nhất sử dụng thuật ngữ “dữ liệu cá nhân” hay “thông tin cá nhân” giữa các văn bản quy phạm pháp luật có liên quan (thể hiện cả trong nội dung quy định và trong kỹ thuật lập pháp). Quy định của các luật, nghị định từ trước đến nay đều dùng thuật ngữ TTCN với các cách hiểu rộng, hẹp khác nhau, nhưng Dự thảo Nghị định về bảo vệ dữ liệu cá nhân mới nhất lại sử dụng thuật ngữ “dữ liệu cá nhân”.

Thứ hai, còn thiếu các quy định về trách nhiệm hình sự đối với hành vi xâm phạm quyền được bảo vệ đối với dữ liệu cá nhân. Hiện nay, Bộ luật Hình sự năm 2015 quy định 02 tội danh là: “Tội xâm phạm bí mật hoặc an toàn thư tín, điện thoại, điện tín hoặc hình thức trao đổi thông tin riêng tư khác của người khác” (Điều 159); và “Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông” (Điều 288). Tuy nhiên, cả 2 tội danh này chưa quy định cụ thể, trực tiếp về các hành vi vi phạm pháp luật liên quan tới dữ liệu cá nhân đang diễn ra hiện nay.

Thứ ba, mức xử phạt những hành vi vi phạm quyền với dữ liệu cá nhân còn nhẹ, chưa tương xứng với mức độ nguy hiểm và thiệt hại nặng nề gây ra. Mức phạt tiền nặng nhất đối với vi phạm quyền về sự riêng tư trong pháp luật hành chính của Việt Nam hiện là

¹⁸ Bộ Công an (2021), *Dự thảo Nghị định quy định về bảo vệ dữ liệu cá nhân*.
<http://bocongan.gov.vn/vanban/Pages/van-ban-moi.aspx?ItemID=519>, truy cập ngày 15/7/2021.

70 triệu đồng (Điều 66 Nghị định số 174/2013/NĐ-CP), trong pháp luật hình sự là 200 triệu đồng (Điều 288 Bộ luật Hình sự 2015, sửa đổi, bổ sung năm 2017)¹⁹. Chưa gắn hình phạt với trách nhiệm bồi thường thiệt hại do vi phạm, trong khi thiệt hại sau khi bị xâm phạm còn lớn hơn rất nhiều so với số tiền nêu trên.

3. Tác động của trí tuệ nhân tạo và các công nghệ số tới quy định của pháp luật về bảo hộ dữ liệu cá nhân

3.1. Tác động tích cực

Sự phát triển mạnh mẽ của công nghệ trong thời đại số luôn mang lại lợi ích trực tiếp cho cuộc sống con người, đặc biệt trong lĩnh vực kinh tế - xã hội. Điều này cũng ảnh hưởng đến lối sống, văn hoá, các thói quen hàng ngày của chúng ta như sử dụng thiết bị điện tử để giao tiếp và tham gia tích cực vào mạng xã hội.

AI là một trong số những công nghệ có vai trò quan trọng trong đời sống với việc cắt giảm tối đa thời gian, chi phí thực hiện tác vụ, cho phép hoàn thành đa nhiệm và giảm bớt quá tải cho các nguồn lực hiện có. Việc thu thập, phân tích và xử lý lượng dữ liệu lớn trong thời gian ngắn giúp tối ưu hoá trải nghiệm cá nhân, thiết kế những dịch vụ đáp ứng nhu cầu, sở thích của từng người. Đáng kể nhất trong địa hạt y tế, AI đưa ra chẩn đoán nhanh, chính xác, loại bỏ lỗi thường gặp ở con người trong theo dõi tình hình sức khoẻ, cảnh báo trường hợp nguy kịch và trợ giúp bệnh nhân mọi lúc mọi nơi. Trong kinh doanh, AI có thể đảm nhiệm việc phỏng vấn, tuyển dụng, tìm kiếm, chăm sóc khách hàng thay cho con người. Trong điều tra, AI giúp nhận diện, truy vết tội phạm. Ngoài ra, AI có thể soạn nhạc, giảm tiếng ồn, trở thành thú cưng xoa dịu con người...

Bên cạnh đó, các công nghệ số khác cùng với AI khiến kết nối xã hội trở nên dễ dàng hơn bao giờ hết, con người xích lại gần nhau, xoá bỏ mọi rào cản về ngôn ngữ, văn hoá, khoảng cách địa lý, mở rộng cơ hội học tập, làm việc, đa dạng các hình thức giải trí, thư giãn. Không chỉ các doanh nghiệp mà chính phủ các nước, các tổ chức trên thế giới cũng sử dụng chúng như công cụ hữu hiệu để quản lý và vận hành nội bộ. Việc áp dụng công nghệ số trong lĩnh vực luật pháp nói chung cũng như pháp luật về bảo hộ dữ liệu cá nhân nói riêng mang lại lợi ích không nhỏ khi cơ sở dữ liệu được pháp điển hoá công khai, được mở rộng tiếp cận bởi nhiều đối tượng trong xã hội, bảo đảm quyền được thông tin, quyền tham gia quản lý nhà nước của công dân... Tất cả những công nghệ trên đều ảnh hưởng và

¹⁹ Vũ Công Giao, Lê Trần Như Tuyên (2020), *Bảo vệ quyền đối với dữ liệu cá nhân trong pháp luật quốc tế, pháp luật ở một số quốc gia và giá trị tham khảo cho Việt Nam*, Tạp chí Nghiên cứu Lập pháp số 09 (409), tháng 5/2020.

định hình xã hội ngày nay với sự tiến bộ không ngừng và hứa hẹn nhiều đột phá trong tương lai.

3.2. Tác động tiêu cực và những hạn chế

Tầm ảnh hưởng của AI và các công nghệ số khác là không thể phủ nhận, nhưng đồng thời chúng cũng có những biến thể và hệ quả khôn lường nếu không được kiểm soát đúng mức. Vì vậy, con người nói chung, người sử dụng nói riêng, nhất là các chính phủ, các tổ chức quốc tế, tổ chức phi lợi nhuận cần nhận thức rõ để có sự chuẩn bị đối phó với tình huống phức tạp này trên tất cả khía cạnh trách nhiệm pháp lý, trách nhiệm xã hội và đạo đức.

Đầu tiên, khả năng của công nghệ hiện đại vượt trội hơn nhiều so với con người nên một số lao động sẽ bị mất việc làm. Nhiều nhà máy có thể hoạt động tự động hoàn toàn bằng robot mà không hề có bóng dáng của bất kỳ công nhân nào. Thậm chí, có ý kiến cho rằng tương lai robot thông minh sẽ thay thế và tiêu diệt con người để thống trị thế giới – nghe như một bộ phim viễn tưởng nhưng không phải không có cơ sở xảy ra. Nếu mọi hoạt động của con người, tổ chức ngày càng phụ thuộc vào AI và các công nghệ số tức là dựa vào hệ thống nền tảng máy tính, mạng nội bộ, internet thì một khi hệ thống đó bị hack, toàn bộ hoạt động sẽ đình trệ, mất nhiều thời gian, tiền bạc để khôi phục lại. Về cơ bản, bất kỳ cá nhân hoặc tổ chức nào sử dụng internet đều có thể trở thành mục tiêu của hacker²⁰, trong đó nhóm nguy cơ cao bao gồm người nổi tiếng, tổ chức tài chính, ngân hàng, doanh nghiệp, trang thương mại điện tử, cơ quan chính trị, an ninh...

Tiếp đó, việc lạm dụng các thiết bị điện tử, di động ảnh hưởng nghiêm trọng đến sức khỏe của con người, dễ gây ra bệnh lý cả về thể chất lẫn tinh thần như mất ngủ, đau đầu, mất tập trung, thị lực kém, nghiện game, trầm cảm, chống đối xã hội... Trong bối cảnh thông tin đa chiều, vấn đề an ninh mạng đang đặt ra nhiều thách thức về bảo vệ dữ liệu cá nhân và bí mật đời tư, bảo đảm an toàn cho giao dịch điện tử, quyền sở hữu trí tuệ, tội phạm công nghệ cao. Với những thành tựu khoa học công nghệ ngày càng hiện đại, thông minh, việc AI âm thầm thu thập dữ liệu cá nhân của người dùng qua các ứng dụng, trò chơi trên điện thoại, máy tính bảng, laptop nếu không được kiểm soát chặt chẽ sẽ dẫn đến hậu quả khôn lường. Nhiều trường hợp bị làm phiền liên tục bởi sim rác, số nước ngoài từ quảng cáo, môi giới bất động sản, bảo hiểm đến đòi nợ, vay tiền... Ngoài nguyên nhân do tội phạm cố tình lấy cắp hoặc mua bán thông tin bất hợp pháp, việc người dùng chưa cẩn trọng trong đăng tải công khai một số thông tin cá nhân trên mạng xã hội đã tạo điều kiện cho

²⁰ CyberPolicy (2021), *What type of organizations do hackers target the most*, <https://www.cyberpolicy.com/cybersecurity-education/what-type-of-organizations-do-hackers-target-the-most>, truy cập ngày 1/7/2021.

các ứng dụng này tự động thu thập thông tin, dẫn đến việc lộ lọt thông tin không mong muốn xảy ra.

Trong khi đó, quy định của pháp luật đã có từ trước khi công nghệ ra đời nên cần phải chỉnh sửa, bổ sung để theo kịp sự phát triển của AI và các công nghệ số khác.

4. Giải pháp hoàn thiện pháp luật về bảo hộ dữ liệu cá nhân

Thứ nhất, đẩy nhanh tiến độ tổng hợp ý kiến và thông qua Dự thảo Nghị định về bảo vệ dữ liệu cá nhân 2021, trước khi có thể xây dựng Luật Bảo vệ dữ liệu cá nhân. Đây là một bước đệm để từng bước đưa pháp luật vào cuộc sống, xem xét tính hợp lý của quy định đối với thực tiễn.

Thứ hai, thống nhất sử dụng thuật ngữ “TTCN” thành “dữ liệu cá nhân” ở tất cả các văn bản quy phạm pháp luật.

Thứ ba, bổ sung điều khoản về các tội hình sự liên quan đến hành vi thu thập, sử dụng, khai thác, chuyển nhượng trái phép TTCN gây hậu quả nghiêm trọng hoặc được thực hiện ở quy mô lớn trong Điều 159, Điều 288 Bộ luật Hình sự hiện hành (áp dụng cho cả cá nhân và pháp nhân thương mại có hành vi vi phạm).

Thứ tư, nâng mức phạt tiền đối với các hành vi vi phạm quyền bảo vệ dữ liệu cá nhân tại Điều 22 Dự thảo Nghị định về bảo vệ dữ liệu cá nhân từ 100 triệu lên 200 triệu, có hướng dẫn rõ hơn về bồi thường thiệt hại và trách nhiệm khắc phục hậu quả đối với chủ thể có hành vi vi phạm theo hướng tạo điều kiện thuận lợi cho chủ thể bị xâm hại có thể khởi kiện đòi bồi thường.

Thứ năm, trong trường hợp phát hiện dữ liệu cá nhân bị thu thập, mua bán trái phép, cần trình báo cơ quan chức năng để xác minh, ngăn chặn và xử lý theo quy định của pháp luật. Riêng đối với các tin nhắn, điện thoại, email rác chào mua bảo hiểm, bất động sản, vay tiền..., người dùng có thể chặn số, từ chối nhận quảng cáo thông qua hướng dẫn từ các nhà mạng hoặc sử dụng dịch vụ chủ động đưa ra danh sách đen (blacklist); về phía các đơn vị quảng cáo, bắt buộc phải đăng ký số hotline, tổng đài với Bộ Thông tin và Truyền thông²¹, ngoài ra không được dùng sim rác để tiếp cận khách hàng.

Cuối cùng, chủ thể dữ liệu cần tự giác bảo vệ TTCN của mình trước khi yêu cầu đối tác, bên thứ ba không làm lộ, lọt ra bên ngoài để tội phạm lợi dụng. Hạn chế công khai TTCN trên mạng xã hội, ứng dụng mua hàng online, trò chơi trực tuyến, truy cập vào wifi miễn phí, các đường dẫn không rõ nguồn gốc trong mail... Ngoài ra, người sử dụng cũng cần lưu ý, hiện có rất nhiều ứng dụng có thể lưu trữ lịch sử di chuyển, cũng như sử dụng trí

²¹ Thế Khiêm (2021), *Quản lý cuộc gọi rác và giải pháp quản lý “Make in Viet Nam” của Viettel*, Tạp chí Thông tin và Truyền thông số 2 tháng 2/2021.

tuệ nhân tạo để biết các hoạt động như tìm kiếm, check-in, mua sắm, thậm chí là nghe lén người dùng. Do đó, chỉ nên chọn vị trí truy cập trên các ứng dụng ở chế độ chỉ hiện thị vị trí khi dùng để tự bảo vệ mình. Bên cạnh đó, người dùng phải sử dụng phần mềm diệt virus, diệt mã độc chuyên dùng, cập nhật thường xuyên để tránh bị mất thông tin quan trọng trong các thiết bị máy tính, điện thoại di động hay các thiết bị cá nhân có kết nối Internet²².

DANH MỤC TÀI LIỆU THAM KHẢO

1. Ngọc Bích (2019), *Nguy hiểm từ việc lọt, lộ thông tin cá nhân trên mạng Internet*, <https://cand.com.vn/Cong-nghe/Nguy-hiem-tu-viec-lot-lo-thong-tin-ca-nhan-tren-mang-Internet-i530219/> truy cập ngày 5/7/2021.
2. Bộ Công an (2021), Dự thảo *Nghị định quy định về bảo vệ dữ liệu cá nhân*.
3. Công an Trà Vinh (2016), *Quy định pháp luật về việc bảo vệ thông tin cá nhân*, <http://congan.travinh.gov.vn/ch10/93-Quy-dinh-phap-luat-ve-viec-bao-ve-thong-tin-ca-nhan.html> truy cập ngày 15/7/2021.
4. CyberPolicy (2021), *What type of organizations do hackers target the most*, <https://www.cyberpolicy.com/cybersecurity-education/what-type-of-organizations-do-hackers-target-the-most> truy cập ngày 1/7/2021.
5. Nguyễn Văn Cường (2020), *Thực trạng pháp luật về bảo vệ thông tin cá nhân ở Việt Nam hiện nay và hướng hoàn thiện*, Tạp chí Nghiên cứu Lập pháp số 15 (415), tháng 8/2020.
6. Department of Industry, Science, Energy and Resources, Australia Government, *Understanding emerging technologies*, <https://www.industry.gov.au/data-and-publications/australias-tech-future/introduction/understanding-emerging-technologies>, truy cập ngày 30/6/2021.
7. EU (2016), *General Data Protection Regulation*, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>, truy cập ngày 1/7/2021.
8. Vũ Công Giao, Lê Trần Như Tuyên (2020), *Bảo vệ quyền đối với dữ liệu cá nhân trong pháp luật quốc tế, pháp luật ở một số quốc gia và giá trị tham khảo cho Việt Nam*, Tạp chí Nghiên cứu Lập pháp số 09 (409), tháng 5/2020.
9. Iapp (2021), *US State Privacy Legislation Tracker*, https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Map.pdf, truy cập ngày 5/7/2021.

²² <https://cand.com.vn/Cong-nghe/Nguy-hiem-tu-viec-lot-lo-thong-tin-ca-nhan-tren-mang-Internet-i530219/>, truy cập ngày 15/7/2021.

10. IBM (2019), *What is artificial intelligence*, <https://www.ibm.com/cloud/learn/what-is-artificial-intelligence>, truy cập ngày 30/6/2021.
11. Investopedia (2020), *Virtual reality*, <https://www.investopedia.com/terms/v/virtual-reality.asp>, truy cập ngày 30/6/2021.
12. Thế Khiêm (2021), *Quản lý cuộc gọi rác và giải pháp quản lý “Make in Viet Nam” của Viettel*, Tạp chí Thông tin và Truyền thông số 2 tháng 2/2021.
13. Hoàng Linh (2021), *Hơn 533 người dùng Facebook bị rò rỉ dữ liệu cá nhân*, <https://hanoimoi.com.vn/tin-tuc/Oto-xemay/995429/hon-533-trieu-nguoi-dung-facebook-bi-ro-ri-du-lieu-ca-nhan> truy cập ngày 5/7/2021.
14. McCarthy (2004), *What is Artificial intelligence?*, Stanford University, Stanford.
15. National Institute of Standards and Technology, U.S. Department of Commerce, <https://csrc.nist.gov/glossary/term/PII> truy cập ngày 8/11/2021.
16. Stuart Russell, Peter Norvig (1994), *Artificial Intelligence: A Modern Approach*, Englewood Cliffs, NJ: Prentice Hall.
17. Lê Sơn (2021), *Cần coi dữ liệu cá nhân là một loại tài sản phi truyền thống*, <http://baochinhphu.vn/Phap-luat/Can-coi-du-lieu-ca-nhan-la-mot-loai-tai-san-phi-truyen-thong/434039.vgp>, truy cập ngày 4/7/2021.
18. Bích Thủy (2019), *Ngân hàng MSB bị lộ 2 triệu dữ liệu khách hàng*, <http://antoanthongtin.vn/an-toan-thong-tin/ngan-hang-msb-bi-lo-2-trieu-du-lieu-khach-hang-105655>, truy cập ngày 4/7/2021.
19. Lê Thị Thùy Trang (2017), *Nghiên cứu một số quy định về bảo vệ thông tin cá nhân trên thế giới và tại Việt Nam*, Trang Thông tin điện tử Cục Tin học hoá, Bộ Thông tin và Truyền thông.
20. A. M. Turing (1950), *Computing Machinery and Intelligence*, *Mind* 49: 433-460.
21. UNESCO IITE and TheNextMinds (2020). *Artificial Intelligence: Media and Information Literacy, Human Rights and Freedom of Expression*.