MÃ HÓA ĐỂ BẢO VỆ QUYỀN RIÊNG TƯ VÀ RÀO CẢN TRONG VIỆC BẢO VỆ TRẺ EM TRÊN MÔI TRƯỜNG MẠNG

HOÀNG THU GIANG
Cục An toàn thông tin - Bộ Thông tin và Truyền thông

Quyền riêng tư cá nhân vốn là điều được quy định theo Hiến pháp và luật của mỗi quốc gia ở ngoài đời thực, thế nhưng trên thế giới ảo, quyền riêng tư tại các nền tảng nhắn tin trực tuyến, mạng xã hội lại có thể trở thành nơi che giấu một số tội ác nghiêm trọng, đặc biệt đối với trẻ em. Trong những năm gần đây, số lượng tài liệu "đen" về lạm dụng trẻ em được tạo ra và phát tán với một số lượng đáng ngạc nhiên trên các nền tảng trao đổi dữ liệu trực tuyến. Hiện tại, trên thế giới cũng như tại Việt Nam, vẫn chưa có hành lang pháp lý rõ ràng cho các doanh nghiệp nền tảng trong việc rà quét các tài liệu "đen" này, đặc biệt khi công nghệ mã hóa đầu cuối "end to end encryption" đang được các doanh nghiệp áp dụng dưới hình thức bảo vệ quyền riêng tư cá nhân lại đang tạo cơ sở cho kẻ xấu tận dụng để che giấu hành vi tội phạm của mình.

Mã hóa đầu cuối và quyền của người dùng

Với tốc độ phát triển của công nghệ hiện nay, chúng ta dường như không thể phủ nhận được mức độ phụ thuộc của con người vào công nghệ. Cuộc sống trở nên hoàn thiện hơn, con người giải quyết việc nhanh chóng hơn và trẻ em cũng được mở rộng kiến thức, cập nhật hơn so với những thông tin trẻ có được từ bạn bè của mình và giáo viên như trước kia. Với sự phát triển và óc sáng tạo của con người, những công nghệ mới cập nhật và phát triển đi trước thời đại bên cạnh đó là những rủi ro do chúng đem lại với con người. Các tập đoàn công nghệ lớn đa quốc gia cũng đang đối mặt với nhiều vấn đề khi họ đang cố gắng hòa hợp giữa các yếu tố về lợi ích kinh tế, sự sáng tạo và vấn đề về đạo đức con người, đặc biệt liên quan đến trẻ em.

30 năm trước, việc trao đổi thông tin dường như chỉ hạn chế trong tầm quốc gia, giữa các nhóm nhỏ thì giờ đây các mạng xã hội lớn trên thế giới đã mang lại lợi ích tiến bộ vượt bậc là kết nối đa quốc gia. Con người giờ đây tại mọi tầng lớp, lứa tuổi và ở bất kỳ vị trí nào trên thế giới đều có thể giao lưu, chia sẻ, cập nhật thông tin nhanh hơn, nhiều hơn. Góc nhìn của con người về sự vật cũng được thay đổi thành 360 độ và không thể phủ nhận con người cũng phát triển nhiều ý tưởng, sáng tạo hơn thông qua việc chia sẻ, tiếp nhận thông tin từ nhiều nguồn, đa chiều và sáng tạo hơn.

Quyền tự do cá nhân là quyền cơ bản mà mỗi quốc gia đều tuyên bố trong hiến chương và luật pháp của đất nước mình. Người lớn, được hiểu là với một độ tuổi trưởng thành nhất định (tại Việt Nam là 16 tuổi trở lên) người lớn phải chịu trách nhiệm trước hành vi và ý kiến cá nhân của mình. Người lớn hiểu quyền được chia sẻ và bảo vệ bí mật thông tin cá nhân của mình đối với người khác và trẻ em cũng vậy. Trẻ em có quyền được bảo vệ bí mật thông tin cá nhân, cha mẹ muốn chia sẻ thông tin, hay đọc những thông tin trẻ muốn giữ bí mật phải xin ý kiến, không được ép buộc trẻ khi truy cập những thông tin này nếu trẻ không đồng ý.

Khi công nghệ phát triển, giữ bí mật thông tin cá nhân là điều kiện được mỗi quốc gia đưa ra để bảo vệ quyền công dân của mình đối với các nhà phát triển công nghệ. Tuy nhiên, đây cũng là vấn đề phát sinh mâu thuẫn về việc bảo mật thông tin hay sâu hơn nữa là bảo vệ người yếu thế, trong đó có đối tượng trẻ em. Đó là khi mã hóa đầu cuối (end – to – end encryption) được đưa vào áp dụng để bảo vệ quyền lợi người dùng.

Nói một cách dễ hiểu, mã hóa là việc xáo trộn thông tin liên lạc để các thông tin này không thể bị đọc bởi bất kỳ ai trừ khi họ có khóa tương ứng để giải mã dữ liệu. Tất cả các hệ thống công nghệ thông tin đều sử dụng một mức mã hóa nhằm đảm bảo an toàn cho các tệp dữ liệu của mình, các tập đoàn và tiểu bang sử dụng mã hóa để bảo vệ mình các mối đe dọa đối với an ninh quốc gia như chiến tranh mạng, vi phạm dữ liệu và việc can thiệp vào các cuộc bầu cử. Các ngân hàng sử dụng mã hóa để đảm bảo an toàn cho các giao dịch tài chính. Các bệnh viện sử dụng mã hóa để bảo vệ thông tin sức khỏe cá nhân. Các công ty truyền thông xã hội có thể sử dụng mã hóa để bảo vệ thông tin cá nhân và các cuộc trò chuyện riêng tư của người dùng.

Mã hóa đầu cuối là một hình thức mã hóa đặc biệt mạnh, trong đó bên trung gian - bên thứ ba (như nhà cung cấp dịch vụ) không có khóa để giải mã thông tin liên lạc; các thông tin này chỉ có thể đọc được bởi hai bên trao đổi. Điều này khác với mã hóa yếu khi nhà cung cấp dịch vụ giữ lại một khóa để giải mã dữ liệu theo yêu cầu, bởi cơ quan thực thi pháp luật hoặc các cơ quan có thẩm quyền của chính phủ. Về mặt này, mã hóa đầu cuối là một công cụ quan trọng cho phép các nhóm dễ bị tổn thương giao tiếp và cuối cùng có thể thực hiện quyền tự do ngôn luận của mình.

Báo cáo viên của Liên Hợp Quốc về Tự do ngôn luận đã gọi mã hóa đầu cuối là "khối bí mật hoàn hảo" cho bảo mật kỹ thuật số trên các ứng dụng nhắn tin. Do vai trò quan trọng của nó, Báo cáo viên lưu ý thêm rằng: *"trách nhiệm bảo vệ quyền tự do ngôn luận và quyền riêng tư có thể yêu cầu các công ty thiết lập mã hóa đầu cuối làm cài đặt mặc định trong các sản phẩm nhắn tin khi phát triển nền tảng của mình"*. Phát ngôn viên cũng gợi ý rằng các công ty cung cấp ứng dụng nhắn tin *"nên tìm cách cung cấp cài đặt quyền riêng tư cao nhất cho người dùng theo cơ chế mặc định"*.

Mã hóa cũng rất quan trọng để đảm bảo an toàn cho trẻ em. Các thiết bị kỹ thuật số và thông tin liên lạc của trẻ chứa thông tin cá nhân có thể ảnh hưởng đến quyền riêng tư và sự an toàn của trẻ nếu rơi vào tay kẻ xấu. Thông tin này bao gồm dữ liệu về các vị trí hiện tại và trước đây cho biết trẻ đang ở đâu hoặc sẽ đi đâu; những tuyến đường trẻ đi đến trường hoặc địa điểm trẻ thường ghé qua vào thời gian rảnh của mình. Thông tin có thể gồm địa chỉ nhà, thông tin liên lạc của những người mà trẻ biết, tội phạm có thể sử dụng các thông tin này để mạo danh người nào đó gần gũi với trẻ để thực hiện các hành vi dụ dỗ, phạm tội. Thông tin liên lạc kỹ thuật số của trẻ cấu thành một bản ghi các cuộc gọi, tin nhắn, tìm kiếm trên web và hình ảnh, là thông tin riêng tư và nhạy cảm có thể được sử dụng để đe dọa hoặc tống tiền. Việc áp dụng mã hóa mạnh đồng nghĩa với việc thông tin này có thể an toàn hơn.

Vấn đề quan trọng liên quan đến dữ liệu là mã hóa đầu cuối (end-to-end) chủ yếu giải quyết các hành vi vi phạm quyền riêng tư của người dùng bởi các đối tượng bên ngoài. Công ty sở hữu nền tảng cũng có thể thu thập siêu dữ liệu liên quan đến việc sử dụng ngay cả khi mã hóa end-to-end được triển khai, và có giá trị đáng kể khi quy đổi ra tiền. Điều này đồng nghĩa với việc các công ty có thể xác định người sử dụng đang giao tiếp với ai, khi nào họ đang thực hiện việc giao tiếp, nơi giao tiếp và thông tin khác về các hoạt động trực tuyến của thiết bị ngoại. Quyền truy cập vào thông tin này cũng là một vấn đề về quyền trẻ em, vì điều này đồng nghĩa với việc dữ liệu của trẻ em có thể và sẽ được các công ty sử dụng và chia sẻ. Mặc dù mục đích của vấn đề này cũng có thể là để hỗ trợ các mục tiêu phát triển và nhân đạo của các tổ chức trong lĩnh vực này, nhưng điều này cũng cho thấy vấn đề về quyền trẻ em hiện chưa được quan tâm đầy đủ.

Công nghệ ảnh hưởng tới vấn đề xâm hại tình dục trẻ em

Vấn nạn xâm hại tình dục trẻ em trên môi trường mạng ngày càng trở nên bức thiết và nguy hiểm hơn khi tội phạm công nghệ sử dụng lợi thế về bảo vệ quyền riêng tư giống như một công cụ bảo vệ cho những hoạt động tội phạm của chúng. Nếu hàng triệu các file dữ liệu hình ảnh tình dục trẻ em được kẻ tội phạm truyền tải và lưu trữ thông qua các nền tảng công nghệ, và các file ảnh này được tự do trao đổi dưới dạng mã hóa đầu cuối thì các hành vi tội phạm sẽ trở nên nguy hiểm và tinh vi đến mức nào. Trẻ em là đối tượng yếu thế trong xã hội, cần được bảo vệ giờ đây là con mồi cho những tên tội phạm ấu dâm, chúng sử dụng các thủ đoạn dụ dỗ, dọa nạt, lừa gạt và gửi các hình ảnh đồi trụy cho trẻ để tuyên truyền cho trẻ rằng các hành động đó là bình thường.

Lạm dụng và bóc lột tình dục trẻ em là một mối quan tâm lớn trên toàn thế giới. Với việc tiếp cận và sử dụng Internet ngày càng tăng, việc lạm dụng và bóc lột tình dục trẻ em không còn chỉ giới hạn trong gia đình, trường học và cộng đồng. Việc thủ phạm sử dụng Internet mở rộng khả năng tiếp cận của họ với nhiều nạn nhân tiềm năng hơn, vì trẻ em và thanh thiếu niên dưới 18 tuổi chiếm khoảng một phần ba số người dùng Internet trên toàn thế giới.

Tài liệu lạm dụng tình dục trên mạng là một trong những hình thức nghiêm trọng nhất tác động tới trẻ em trong không gian trực tuyến. Internet cũng đã hình thành các hình thức lạm dụng tình dục mới. Ví dụ như các dịch vụ được thực hiện theo đơn đặt hàng cho phép thủ phạm yêu cầu sản xuất nội dung tình dục trong đó có xác định phạm vi tuổi, giới tính và chủng tộc của trẻ em được chỉ định theo sở thích tình dục của thủ phạm. Hình thức phát trực tiếp (livestream) việc lạm dụng tình dục trẻ em là một hình thức lạm dụng mới nổi trong thời gian gần đây, trong đó thủ phạm có thể mua quyền truy cập vào một số kênh để quan sát và chỉ đạo việc lạm dụng trẻ em trong lúc livestream.

Trong một bức thư gửi tới Facebook, đại diện Chính phủ của Hoa Kỳ, Vương quốc Anh (Anh) và Australia cảnh báo rằng việc triển khai mã hóa đầu cuối trên Facebook Messenger sẽ làm giảm đáng kể số lượng báo cáo các hình ảnh xâm hại tình dục được gửi tới Trung tâm Quốc gia về Trẻ em Mất tích Bị bóc lột (NCMEC). Nguyên nhân là khi triển khai mã hóa đầu cuối, thông tin liên lạc kỹ thuật số được chia sẻ trên Facebook không thể được giám sát trên quy mô lớn.

"Năm 2018, Facebook đã gửi 16,8 triệu báo cáo cho Trung tâm Quốc gia về Trẻ em Mất tích Bị bóc lột – con số này chiếm hơn 90% trong tổng số 18,4 triệu báo cáo trong năm. Liên quan đến hình ảnh lạm dụng trẻ em, 8.000 báo cáo có liên quan đến việc tội phạm cố gắng tìm cách gặp gỡ tiếp xúc, dụ dỗ hoặc lôi kéo trẻ chia sẻ hình ảnh chụp ảnh khiêu dâm cũng như thực hiện các cuộc gặp với mục đích xấu ngoài đời thực". Cơ quan Tội phạm Quốc gia Anh ước tính rằng, năm 2019, căn cứ theo báo cáo của NCMEC từ Facebook có đến hơn 2.500 vụ bắt giữ tội phạm xâm hại trẻ em đã được cơ quan thực thi pháp luật Anh hành động và gần 3.000 trẻ em được bảo vệ an toàn ở Anh.

Không thể khẳng định Internet và mã hóa đầu cuối tạo điều kiện thuận lợi cho việc lạm dụng tình dục trẻ em trên các nền tảng truyền thông kỹ thuật số. Nhưng điều này thể hiện những hạn chế đối với nỗ lực toàn cầu nhằm chấm dứt lạm dụng và bóc lột tình dục trẻ em. Công nghệ làm cho việc xác định, điều tra và truy tố những hành vi phạm tội đó trở nên khó khăn hơn. Trong khi trẻ em có quyền được bảo vệ khỏi lạm dụng và bóc lột tình dục ở bất cứ đâu, kể cả trên mạng hay ngoài đời thực. Các quốc gia có nghĩa vụ thực hiện các giải pháp để hành động và bảo vệ hiệu quả, bao gồm cả việc hỗ trợ phục hồi và thực thi công lý.

Điều quan trọng là chúng ta phải xem xét làm thế nào để cân bằng giữa việc bảo vệ và xâm phạm các quyền này khi đề xuất các giải pháp. Trong hành động cân bằng này, có thể xem xét đến các giải pháp khác nhau và tác động tỷ lệ thuận của chúng về quy mô và mức độ nghiêm trọng. Đến một lúc, chúng ta cần phải xem xét và hạn chế lại quyền riêng tư cũng như những hành động thực tế để đảm bảo quyền lợi của những người sử dụng mạng xã hội mà vẫn đảm bảo được sự an toàn của trẻ trên môi trường mạng. Các nhà phát triển công nghệ cần xem xét và đưa ra giải pháp.

Và công nghệ hỗ trợ bảo vệ trẻ em

Vào ngày 5 tháng 8 năm 2021, Apple đã công bố một giải pháp mới nhằm phát hiện các tài liệu xâm hại tình dục cho trẻ em nhưng vẫn đảm bảo cam kết bảo vệ quyền riêng tư của người dùng. Giải pháp đưa ra là sử dụng phương pháp đối sánh hình ảnh mà không cần phải nhìn rà soát hình ảnh cụ thể. Công cụ được sử dụng ở đây gọi là giao điểm tập hợp riêng được các chuyên gia mật mã nghiên cứu từ năm 1980. Công cụ này cho phép hai người có thể tìm kiếm các điểm chung trong tập tài liệu của họ mà không để lộ các thông tin khác.

Đây là cách hoạt động của đối sánh hình ảnh. Apple sẽ cập nhật cài cho iPhone, iPad và Mac của người sử dụng một cơ sở dữ liệu chứa các mã hóa không thể giải mã liên quan đến các hình ảnh lạm dụng trẻ em. Đối với mỗi ảnh người sử dụng tải lên iCloud, thiết bị của người đó sẽ áp dụng một dấu vân tay kỹ thuật số, được gọi là NeuralHash. Tính năng lấy dấu vân tay hoạt động ngay cả khi hình ảnh đó được thay đổi về kích cỡ, hoặc những thay đổi không quá khác biệt. Sau đó, thiết bị của người sử dụng sẽ tạo mã code cho ảnh mà thiết bị của người sử dụng không thể biết, nhưng mã code này sẽ cho máy chủ biết liệu ảnh đã tải lên có khớp với tài liệu lạm dụng trẻ em trong cơ sở dữ liệu hay không. Nếu đủ chứng cớ từ một thiết bị cho thấy hình ảnh tải lên khớp với các hình ảnh lạm dụng trẻ em đã biết, máy chủ sẽ học các khóa bí mật để giải mã tất cả các bức ảnh trong tệp dữ liệu có trùng khớp - nhưng không phải khóa cho các bức ảnh khác. Đối với các hình ảnh không trùng khớp, máy chủ không thể xem bất kỳ ảnh nào.

Việc để quy trình đối sánh này diễn ra trên thiết bị của người sử dụng có thể tốt hơn cho quyền riêng tư của người dùng so với các phương pháp trước đây, trong đó quá trình đối sánh diễn ra trên máy chủ - nếu nó được triển khai đúng cách.

Công nghệ quét điện thoại của Apple được thiết kế để bảo vệ quyền riêng tư. Các chuyên gia về chính sách công nghệ và bảo mật máy tính được đào tạo để nghiên cứu những cách mà công nghệ có thể bị sử dụng hoặc lạm dụng, bất kể mục đích của người tạo ra nó là gì. Tuy nhiên, giải pháp này đang trong quá trình nghiên cứu và triển khai, chúng ta sẽ cần thời gian để xem các công nghệ này khi đưa vào ứng dụng sẽ có kết quả cụ thể ra sao.

Kế tiếp đến động thái này, gần đây nhất Apple vừa phát hành bản cập nhật iOS 14.5 buộc các nhà phát triển ứng dụng phải xin phép người dùng trước khi thu thập dữ liệu. Quy định này áp dụng cho tất cả các ứng dụng, bao gồm những ứng dụng do Apple phát triển. Có thể nói đây chính là một cuộc chiến công nghệ giữa các doanh nghiệp công nghệ lớn trên thế giới bảo vệ quyền lợi, thông tin cá nhân của người dùng.

Việc có thể thấy trước hết là số lượng doanh thu quảng cáo từ Facebook giảm xuống nhanh chóng khi không có dữ liệu cá nhân người dùng, người bán sẽ không còn cơ sở để nhắm tới đối tượng tiềm năng cho sản phẩm của mình. Đứng từ phía người sử dụng thì mọi người cảm thấy an toàn và yên tâm về việc thông tin cá nhân của mình đã được Apple bảo vệ an toàn, nhưng từ góc độ doanh nghiệp thì việc phụ thuộc vào các quảng cáo trên Facebook đã làm cho họ sụt giảm một số lượng doanh thu lớn.

Tuy nhiên, chúng ta có thể thấy rằng sự phát triển của công nghệ càng yêu cầu những nghiên cứu sáng tạo phát triển, các doanh nghiệp cũng cần phải tự định hướng cho sự tồn tại và phát triển của mình hướng tới một môi trường kinh doanh an toàn, lành mạnh và bảo vệ quyền lợi người dùng của mình. Đây cũng là một cách để hướng đến một hệ sinh thái công nghệ an toàn bền vững.

Bàn luận và khuyến nghị

Không có gì đáng ngạc nhiên khi chúng ta biết rằng nhiều trẻ em đang sử dụng các nền tảng trực tuyến dù chúng chưa đủ tuổi sử dụng. Cũng không có gì là bí mật khi chúng ta cũng biết rằng ngày càng nhiều trẻ em trở thành đối tượng bị xâm hại tình dục trên các trang web phổ biến. Mặc dù vấn đề này đã được thảo luận trong vài năm trở lại đây, nhưng thế giới trực tuyến vẫn là một môi trường luôn tiềm ẩn yếu tố tích cực cũng như tiêu cực đối với trẻ em. Và dường như các công ty công nghệ vẫn đang còn có rất ít các hoạt động được triển khai để bảo vệ đối tượng người dùng dễ bị tổn thương trên môi trường mạng, đặc biệt là trẻ em.

Việc tiến tới sử dụng giải pháp mã hóa đầu cuối end-to-end để đảm bảo an toàn dữ liệu cá nhân người dùng mà không có các biện pháp bảo vệ thích hợp cho thấy: đối với nhiều công ty công nghệ, việc bảo vệ nhu cầu của trẻ em là điều được cân nhắc sau cùng chứ không phải là vấn đề chính phải quan tâm đầu tiên. Do đó, với sự phát triển nhanh chóng của công nghệ, Chính phủ cần triển khai các biện pháp tích cực hơn nữa trong việc đưa ra các yêu cầu và giải pháp với các công ty công nghệ về bảo vệ người dùng, đặc biệt là trên lãnh thổ Việt Nam.

Hiện nay, tại Việt Nam Thủ tướng Chính phủ đã giao cho Bộ Công an nghiên cứu triển khai Đề án "Phát triển ứng dụng dữ liệu về dân cư, định danh và xác thực điện tử phục vụ chuyển đổi số quốc gia năm 2022-2025, tầm nhìn đến năm 2030" (Đề án 06) vấn đề đảm bảo an toàn thông tin khi kết nối chia sẻ hệ thống cơ sở dữ liệu quốc gia về dân cư và các cơ sở dữ liệu chuyên ngành đã được nhấn mạnh. Tuy nhiên Việt Nam cần phải có thêm những yêu cầu chặt chẽ hơn nữa đối với doanh nghiệp phát triển nền tảng trong việc phối hợp các giải pháp sàng lọc và kiểm tra các các nội dung xâm hại tình dục trẻ em, có báo cáo lại với cơ quan chức năng để xây dựng cơ sở dữ liệu tội phạm xâm hại tình dục trẻ em. Các quy định đối với doanh nghiệp công nghệ về vấn đề này cần được làm rõ như sau:

(1) Đưa ra quy định mạnh đối với các doanh nghiệp phát triển nền tảng trong việc xác minh độ tuổi người dùng. Việc này cần phải được triển khai trên tất cả các nền tảng nói chung không chỉ riêng các nền tảng có đối tượng nhắm tới là trẻ em.

(2) Ban hành các chế tài mạnh đối với các công ty vi phạm các quy định trong việc xác minh và để các đối tượng tội phạm lợi dụng nền tảng của mình để xâm hại người dùng, đặc biệt là đối tượng dễ tổn thương là trẻ em. Biện pháp mạnh tay có thể chặn ISP. Các công ty cũng phải đưa ra cảnh báo với ngôn ngữ dễ hiểu để trẻ em và người sử dụng có thể tự biết cách phòng tránh và bảo vệ mình.

(3) Cần có quy định rõ ràng về vấn đề bảo vệ trẻ em đối với các nền tảng ứng dụng có dịch vụ cho trẻ em ngay từ khi xây dựng nền tảng để các nhà phát triển nội dung có căn cứ triển khai.

Với sự phát triển nhanh chóng của công nghệ, trong tương lai sẽ còn nhiều những ý kiến liên quan đến việc dung hòa các nội dung của yếu tố phát triển công nghệ và các quy định pháp luật với các vấn đề mới ra sao. Thế giới là sự phát triển của quá trình tiến hóa và các tranh luận để tìm ra giải pháp mới. Chúng ta vẫn đang cùng tìm kiếm các giải pháp để hướng đến một xã hội an toàn, lành mạnh cho người dùng trên Internet đặc biệt là đối với trẻ em. THÔNG TIN & TRUYỀN THÔNG

Tài liệu tham khảo:

1. *Encrytion, Privacy and Children's Right to Protection from Harm, Unicef Oct 2020.*
2. *An examination of Apple's plans to 'scan' your iPhone photos for abusive content (thenextweb.com)*
3. *How the Apple iOS 14 release may affect your ads and reporting, (https://www.facebook.com/business/help/331612538028890?id=428636648170202)*