Di chúc số và vấn đề công nhận giá trị pháp lý trong bối cảnh chuyển đổi số

14/07/2026

Tóm tắt: Sự phát triển của công nghệ thông tin đã đặt ra nhu cầu nhìn nhận lại các quy định về thừa kế. Bên cạnh di chúc văn bản và di chúc miệng được ghi nhận trong Bộ luật Dân sự năm 2015, di chúc số mở ra cơ hội về tiết kiệm chi phí, bảo mật và đặc biệt phù hợp với tài sản số như tài sản ảo hay tài sản mã hóa. Dựa trên nguyên tắc tương đương chức năng, kinh nghiệm quốc tế và các chuẩn an ninh, kết hợp mô hình hóa kiểm chứng, bài viết đề xuất mô hình di chúc số an toàn dựa trên hạ tầng khóa công khai và chia sẻ bí mật, đáp ứng yêu cầu bảo mật, toàn vẹn, xác thực và chống chối bỏ. Từ đó, kiến nghị hoàn thiện khung pháp lý để hướng tới khả năng công nhận di chúc số ở Việt Nam trong tương lai.

Từ khóa: Hình thức di chúc; di chúc số; chuyển đổi số.

Abstract: The development of information technology has raised the need to re-examine the provisions on inheritance. Alongside written and oral wills recognized in the 2015 Civil Code, digital wills open up opportunities for cost savings, security, and are particularly suitable for digital assets such as virtual or crypto assets. Based on the principle of functional equivalence, international experience, and security standards, combined with verification modeling, the article proposes a secure digital will model based on public key infrastructure and secret sharing, satisfying requirements for confidentiality, integrity, authentication, and non-repudiation. Then, it makes recommendations to improve the legal framework towards the recognition of digital wills in Vietnam in the future.

Keywords: Form of will; digital will; digital transformation.

Ảnh minh họa: Nguồn Internet.

Đặt vấn đề

Di chúc là một chế định pháp luật cổ điển, vốn gắn liền với các hình thức di chúc bằng văn bản và di chúc miệng, hiện đang bộc lộ nhiều hạn chế: thủ tục công chứng, chứng thực, ràng buộc về mặt địa lý, các loại tài sản, và nguy cơ tiết lộ thông tin nhạy cảm trước thời điểm mở thừa kế. Khác với di chúc điện tử là di chúc được lập, lưu trữ

hoặc chứng thực bằng phương tiện điện tử, thay thế văn bản giấy thì di chúc số được bảo mật toàn diện, xây dựng trên nền tảng mật mã học, bảo đảm an toàn từ khâu lập, lưu trữ đến công bố ý chí định đoạt tài sản của người để lại di sản hoàn toàn trên tảng số hóa, hứa hẹn khắc phục những bất cập này. Bài viết sử dụng phương pháp phân tích pháp luật, so sánh kinh nghiệm quốc tế, vận dụng lý thuyết bảo mật thông tin theo chuẩn quốc tế, đồng thời khai thác kết quả mô hình hóa và kiểm chứng bằng Bộ công cụ kiểm chứng tự động các giao thức bảo mật trên Internet (Automated Validation of Internet Security Protocols and Applications - AVISPA). Trên cơ sở đó, bài viết sẽ mô tả một mô hình di chúc số an toàn về mặt kỹ thuật, đồng thời đề xuất khung pháp lý phù hợp để triển khai tại Việt Nam nhằm đáp ứng yêu cầu của kỷ nguyên số cũng như đa dạng hình thức của di chúc cho người lập di chúc.

1. Cơ sở của vấn đề công nhận giá trị pháp lý của di chúc số

1.1. Cơ sở pháp luật

Hiệu lực của di chúc được quy định tại Bộ luật Dân sự năm 2015 (BLDS năm 2015), dựa trên ba nguyên tắc cơ bản: (i) Người lập di chúc minh mẫn, sáng suốt trong khi lập di chúc; không bị lừa dối, đe dọa, cưỡng ép; (ii) Nội dung di chúc không vi phạm điều cấm của luật, không trái đạo đức xã hội; (iii) Hình thức của di chúc không trái quy định của luật.

Trong bối cảnh giao dịch điện tử, lý thuyết "tương đương chức năng" (*functional equivalence*)[1] đóng vai trò nền tảng, cho phép các hình thức điện tử được công nhận có giá trị pháp lý tương đương với hình thức truyền thống nếu chúng đáp ứng đầy đủ các tiêu chí về xác thực, toàn vẹn và khả năng lưu trữ lâu dài. Theo quy định tại Điều 119 BLDS năm 2015 thì giao dịch dân sự thông qua phương tiện điện tử dưới hình thức thông điệp dữ liệu theo quy định của pháp luật về giao dịch điện tử được coi là giao dịch bằng văn bản. Nguyên tắc này đã được áp dụng trong Luật Giao dịch điện tử của nhiều quốc gia và là cơ sở lý luận quan trọng để xem xét công nhận di chúc số. Đồng thời, bất kỳ mô hình di chúc nào cũng phải bảo đảm nguyên tắc bảo vệ quyền thừa kế và tôn trọng tuyệt đối ý chí của người để lại di sản. Bởi vì di chúc là sự thể hiện ý chí cá nhân nhằm chuyển tài sản riêng của mình cho người khác sau khi chết. Do đó, việc đa dạng các hình thức di chúc sẽ đáp ứng nhu cầu riêng của cá nhân phù hợp với mong muốn, sở thích, hoàn cảnh của mình. Hiện nay, BLDS năm 2015 quy định các hình thức di chúc bằng văn bản và di chúc miệng được cân nhắc dựa trên các yếu tố như đơn giản, tiết kiệm chi phí; bảo đảm di chúc không thất lạc và giữ bí mật; hỗ trợ người không am hiểu pháp luật hoặc không thể tự viết; bảo đảm ý chí thật của người lập di chúc, tránh giả mạo và trong tình huống khẩn cấp.

Tuy nhiên, cùng với sự thay đổi nhanh chóng của đời sống xã hội, nhận thức pháp luật tăng, công nghệ số và Internet đã phủ sóng rộng khắp cả nước[2] thì nhu cầu ghi nhận di chúc theo hình thức mới như di chúc số với loại tài sản số theo quy định của Luật Công nghiệp công nghệ số năm 2025 cần được xem xét và ghi nhận, để pháp luật luôn đi trước và chủ động điều chỉnh các vấn đề phát sinh trong đời sống xã hội.

1.2. Khung lý thuyết bảo mật thông tin

Từ góc độ kỹ thuật, các yêu cầu bảo mật của một hệ thống di chúc số cần được đánh giá dựa trên các chuẩn quốc tế, đặc biệt là khung bảo mật ITU-T X.800[3] và tiêu chuẩn quản lý an toàn thông tin ISO/IEC 27001[4]. Khung bảo mật ITU-T X.800 cung cấp một cách tiếp cận toàn diện, xuyên suốt trong việc bảo đảm an ninh mạng, bao quát từ hạ tầng, dịch vụ đến ứng dụng. Nó cho phép phát hiện, dự đoán và khắc phục các lỗ hổng bảo mật thông qua việc phân tách thành các thành phần kiến trúc riêng biệt, từ đó hỗ trợ cả việc thiết kế giải pháp mới lẫn đánh giá hệ thống hiện có. Trong khi đó, ISO/IEC 27001 là hệ thống tiêu chuẩn quốc tế về quản lý an toàn thông tin, tập trung vào việc thiết lập, triển khai, vận hành, giám sát và cải tiến liên tục hệ thống quản lý an ninh thông tin (ISMS). Việc áp dụng ISO/IEC 27001 giúp tổ chức/doanh nghiệp xác định rõ ràng các loại thông tin, rủi ro và mối đe dọa, đồng thời đưa ra các cơ chế kiểm soát và quy trình để giảm thiểu rủi ro, phù hợp với mọi quy mô và lĩnh vực kinh tế. Sự kết hợp giữa ITU-T X.800 và ISO/IEC 27001 tạo nên một nền tảng chuẩn mực, vừa mang tính kỹ thuật, vừa mang tính quản trị, bảo đảm cho hệ thống di chúc số đạt được mức độ bảo mật toàn diện.

1.3. Các thành phần kỹ thuật chính của hệ thống di chúc số

Diffie và Hellman[5] đã giới thiệu một khái niệm mang tính cách mạng về mật mã khóa công khai (public key cryptography), đồng thời đề xuất một phương pháp trao đổi khoá mới cho phép hai người dùng có thể trao đổi khóa một cách an toàn, từ đó có thể sử dụng khóa này cho các quá trình mã hóa sau đó. Trên nền tảng của Diffie và Hellman thì Rivest, Shamir và Adleman[6] cũng đã giới thiệu một thuật toán RSA - là hệ mật mã bất đối xứng thực tiễn đầu tiên. Đặc điểm của hệ thống này là sử dụng một thuật toán mật mã có hai khóa: khóa riêng tư và khóa công khai[7]. Trong điều kiện bình thường, khóa riêng tư được người dùng bảo vệ nghiêm ngặt. Tuy nhiên, nếu khóa bị mất hoặc bị huỷ, thì dữ liệu mã hóa sẽ không thể khôi phục lại. Để giải quyết nhược điểm này, hệ thống ký gửi khóa (The key escrow system) đã được đề xuất. Đây là một hệ thống phục hồi khóa cho phép bên thứ ba có quyền truy cập vào khóa để giải mã trong những trường hợp nhất định[8]. Bên cạnh đó, hệ thống chia sẻ bí mật (secret sharing) là một giải pháp thay thế khác để phân phối một bí mật cho một nhóm người tham gia, trong đó mỗi người sẽ được phân một phần của bí mật (shadow). Bí mật này chỉ có thể được khôi phục khi đủ số lượng các phần (shares) được kết hợp lại[9].

Nội dung kỹ thuật của hệ thống di chúc số được xây dựng dựa trên các nền tảng mật mã học sau:

Chữ ký số

Bằng cách sử dụng các thuật toán mật mã, chữ ký số sẽ cung cấp khả năng xác thực thông điệp và không thể chối bỏ. Chữ kỹ sẽ bảo đảm rằng thông điệp là xác thực và không bị thay đổi trong quá trình truyền tải. Ngoài ra, người ký sẽ không thể phủ nhận việc đã ký vào thông điệp, từ đó mang lại lý do hợp lý để người nhận tin rằng chữ ký họ nhận được thực sự được tạo bởi đúng người đã khai báo. Mỗi người dùng sở hữu

một khóa riêng và một khóa công khai tương ứng. Người ký sử dụng khóa riêng của mình để ký vào một thông điệp. Khi nhận được chữ ký, người nhận sử dụng khóa công khai của người ký để xác minh tính hợp lệ của chữ ký đó. Hiện nay, đã có rất nhiều thuật toán chữ ký được đề xuất, chẳng hạn như RSA (Rivest, Shamir, và Adleman)[10] và ElGamal[11]. Tính bảo mật của các thuật toán này dựa trên giả định về độ của một số bài toán toán học: chữ ký RSA an toàn dựa trên bài toán phân tích số nguyên, còn chữ ký ELGamal dựa trên bài toán logarit rời rạc trong module lớn.

Thuật toán mã hóa/giải mã

Trong mật mã truyền thống, mã hóa là quá trình biến đổi thông tin (hay là plaintext) thành dạng đã được mã hóa (gọi là bản mã - ciphertext) sao cho những người không có kiến thức đặc biệt, thường là khóa, sẽ không thể đọc được. Các bên tham gia giao tiếp cần chia sẻ trước một khóa bí mật chung, sau đó sử dụng nó cho cả quá trình mã hóa văn bản gốc và giải mã văn bản mã[12]. Hiện nay là sự phổ biến của mật mã khóa công khai. Hệ thống này sử dụng hai khóa riêng biệt, một khóa bí mật và một khóa công khai. Cặp khóa này được liên kết với nhau bằng các thuật toán toán học. Người gửi sẽ mã hóa thông điệp bằng khóa công khai của người nhận, sau đó truyền bản mã đến người nhận. Khi nhận được thông tin đã mã hóa, người nhận có thể giải mã bản mã bằng khóa bí mật của mình[13]. Mật mã khóa công khai đã được nghiên cứu rộng rãi, và nhiều hệ mật khóa công khai đã được đề xuất, chẳng hạn như thuật toán RSA, hệ mã hóa ElGamal và các hệ mật mã dựa trên nhận dạng (IBE - Identity-Based Encryption)[14].

Mã hóa có xác thực

Để khắc phục những hạn chế của các mô hình trước đó, Araki và cộng sự đã đưa khái niệm “chuyển đổi chữ ký”[15] vào thực tiễn và đề xuất một sơ đồ chữ ký có khả năng chuyển đổi với phạm vi xác minh hạn chế. Tuy nhiên, quá trình chuyển đổi chữ ký đòi hỏi phải có sự hỗ trợ từ chính người ký, điều này có thể không khả thi nếu người ký không sẵn sàng hợp tác. Để cải thiện cơ chế chuyển đổi và đạt hiệu năng tốt hơn, Wu và Hsu[16] đã đề xuất một sơ đồ mã hóa xác thực có thể chuyển đổi (CAE - Convertible Authenticated Encryption), trong đó quá trình chuyển đổi chữ ký trở nên đơn giản và có thể được thực hiện hoàn toàn bởi người nhận mà không cần thêm nỗ lực tính toán nào.

Kể từ đó, nhiều biến thể của mô hình mã hóa có xác thực tự chứng nhận (self-certified CAE) đã được đề xuất, chẳng hạn như mã hóa có xác thực với khóa công khai tự chứng nhận (self-certified public key CAE[17]), mã hóa có xác thực ủy quyền tự chứng nhận (self-certified proxy CAE[18]), và sơ đồ mã hóa đa xác thực có thể chuyển đổi (convertible multi-authenticated encryption scheme[19]), cho phép áp dụng trong nhiều bối cảnh ứng dụng khác nhau.

Chứng thư số

Trong các hệ mật mã khóa công khai, mỗi người dùng đều có thể giả mạo thành một người dùng vô danh khác bằng cách sử dụng một khóa công khai hợp lệ nhưng không chính xác. Nghĩa là, một người có thể mạo danh người khác và gửi khóa giả đến

cho người khác. Để tăng cường mức độ an toàn, có thể duy trì một thư mục động công khai chứa các khóa công khai. Việc duy trì thư mục này phải do một tổ chức hoặc thực thể đáng tin cậy chịu trách nhiệm. Định kỳ, các thực thể đó sẽ công bố toàn bộ thư mục hoặc cập nhật thư mục. Cách tiếp cận này rõ ràng an toàn hơn việc công bố khóa công khai cá nhân, nhưng vẫn tồn tại lỗ hổng, chẳng hạn như việc kẻ tấn công có thể can thiệp vào hồ sơ do cơ quan quản lý lưu giữ. Do đó, cơ quan quản lý phải thực hiện việc kiểm soát chặt chẽ hơn đối với việc phân phối khóa công khai từ thư mục. Để lấy được khóa công khai của một người, người dùng phải yêu cầu cơ quan quản lý cung cấp khóa công khai của mọi người khác. Điều này có thể dẫn đến tắc nghẽn trong cơ chế trên. Vì vậy, khái niệm chứng chỉ đã được đề xuất để giải quyết vấn đề này. Một chứng chỉ là một tài liệu điện tử chứa khóa công khai của người dùng và được ký bởi khóa bí mật của một tổ chức chứng thực đáng tin cậy (Certificate Authority - CA). Nhờ chứng chỉ, mỗi người dùng có thể trao đổi khóa mà không cần liên hệ trực tiếp với cơ quan khóa công khai, giống như việc khóa đó được lấy trực tiếp từ chính người sở hữu.

Một người dùng có thể đăng ký nhiều chứng thư số từ CA khác nhau, nhưng danh tính của mỗi người dùng phải là duy nhất trong phạm vi từng miền CA. Trong hạ tầng khóa công khai (Public Key Infrastructure - PKI), chứng thư số được sử dụng để xác minh rằng một khóa công khai cụ thể thuộc về một cá nhân nhất định. Về mặt chức năng, nó tương đương với các giấy tờ định danh cá nhân (chẳng hạn như căn cước công dân, hộ chiếu) trong môi trường mạng. X.509[20] là một tiêu chuẩn được sử dụng rộng rãi để định nghĩa cấu trúc chứng thư số. Nó được ban hành lần đầu vào năm 1988 như một phần của tiêu chuẩn ITU X.500 về dịch vụ thư mục, sau đó được sửa đổi để giải quyết các vấn đề liên quan đến bảo mật và đã trở thành tiêu chuẩn phổ biến cho định dạng chứng thư khóa công khai. Hiện nay, chứng thư X.509 được sử dụng trong hầu hết các ứng dụng bảo mật mạng[21].

Các sơ đồ chia sẻ bí mật

Trong thực tế, một số thông tin riêng tư và quan trọng cần được bảo vệ tuyệt đối khỏi việc bị tiết lộ. Các phương pháp mã hóa truyền thống không phù hợp để đồng thời đạt được cả mức độ bảo mật cao và tính khả dụng. Việc tăng độ tin cậy bằng cách lưu nhiều bản sao sẽ làm giảm mức độ bảo mật, vì tạo ra nhiều cơ hội hơn cho kẻ tấn công, nghĩa là có nhiều khả năng hơn để một bản sao rơi vào tay kẻ xấu[22]. Tính khả dụng có thể được giải quyết bằng cách phân phối sự tin cậy cho nhiều cơ quan hoặc các bên khác nhau. Khi đó, việc chia sẻ các bí mật giữa các bên cũng trở nên cần thiết.

Hiện nay, các sơ đồ chia sẻ bí mật được sử dụng trong nhiều giao thức và ứng dụng mật mã, chẳng hạn như: Tính toán đa bên an toàn, kiểm soát truy cập, tiền điện tử, bầu cử điện tử.

Hệ thống giữ khóa

Thông thường, thông tin đã mã hóa chỉ có thể được đọc bởi người nhận dự kiến, vì khóa sẽ không được tiết lộ cho bất kỳ ai khác ngoài người gửi và người nhận. Tuy nhiên, hệ thống giữ khóa cũng có thể được xem là một rủi ro bảo mật, vì người dùng đã

trao quyền truy cập thông tin cho đại lý giữ khóa (escrow agent). Thêm vào đó, cơ chế này có thể bị lợi dụng để thực hiện các hoạt động trái pháp luật nhằm xâm phạm trật tự công cộng. Micali là người đầu tiên đề xuất hệ thống giữ khóa[23] để giải quyết vấn đề tiến thoái lưỡng nan khi người dùng muốn hoạt động trong vòng bí mật, trong khi người giám sát lại muốn tăng khả năng kiểm soát. Ông đã áp dụng hệ mật mã bất đối xứng để triển khai ý tưởng giữ khóa. Người dùng sẽ không thấy được sự khác biệt cơ bản nào trong quá trình sử dụng. Chỉ khi xảy ra các tình huống đặt biệt, cơ quan nhà nước có thẩm quyền mới được phép giám sát các nội dung của người dùng. Nhằm giới hạn các ngoại lệ này, Chính phủ Hoa Kỳ đã công bố cơ chế Clipper Chip vào năm 1993, còn được gọi là hệ thống giữ khóa. Sau đó, Chính phủ phê duyệt dự luật về ký gửi khóa và ban hành Tiêu chuẩn Mã hóa ký gửi (Escrowed Encryption Standard - EES), là một tiêu chuẩn không bắt buộc dành cho các thông tin nhạy cảm nhưng không bí mật[24].

AVISPA

Với sự phát triển rộng khắp của Internet và các dịch vụ dựa trên mạng, số lượng và quy mô của các giao thức bảo mật mới đang ngày càng vượt xa khả năng phân tích và kiểm tra thủ công của con người. Do đó, việc có những công cụ hỗ trợ phân tích chặt chẽ các giao thức bảo mật là rất quan trọng để nhằm phát hiện ra các lỗ hổng hoặc chứng minh tính đúng đắn của các giao thức đó. Những công cụ này cần phải tự động hóa hoàn toàn, không định kiến, mạnh mẽ, có khả năng biểu đạt cao và dễ sử dụng. Sự ra đời của công cụ AVISPA[25] được đề xuất nhằm cung cấp một bộ công cụ để xây dựng và phân tích các mô hình hình thức của giao thức bảo mật, phục vụ việc xác minh tự động cho các giao thức và ứng dụng nhạy cảm về bảo mật Internet. AVISPA là một công cụ dạng push-button, sử dụng một ngôn ngữ mô tả giao thức chính thức là ngôn ngữ mô tả giao thức ở mức cao (High Level Protocol Specification Language - HLPSL) để mô tả các giao thức bảo mật và các thuộc tính bảo mật mong muốn. Một đặc tả HLPSL được chuyển đổi thành một đặc tả ở mức thấp hơn. Quá trình này được thực hiện tự động bởi bộ chuyển đổi hlpsl2if, tạo ra một đặc tả dưới dạng định dạng trung gian (Intermediate Format- IF). Đặc tả IF sau đó được xử lý bởi các bộ kiểm tra mô hình (model-checkers) nhằm phân tích xem liệu các mục tiêu an ninh có bị vi phạm hay không, và nó có thể được các hệ thống xử lý phía sau (back-ends) của công cụ AVISPA đọc trực tiếp. Các back-end này được sử dụng để kiểm chứng sự phá vỡ giao thức, cũng như thực hiện kiểm tra có giới hạn và không giới hạn.

Có bốn công cụ kiểm tra (verification back-ends) khác nhau được sử dụng để phân tích đặc tả IF, bao gồm: OFMC - Trình kiểm tra mô hình *On-the-Fly* (On-the-Fly Model-Checker), CL-AtSe - Bộ tìm kiếm tấn công dựa trên logic ràng buộc (Constraint Logic–based Attack Searcher), SATMC - Trình kiểm tra mô hình dựa trên SAT (SAT-based Model Checker), TA4SP - Phân tích giao thức bảo mật dựa trên tự động hình cây với các phép xấp xỉ tự động (Tree Automata based on Automatic Approximations for the Analysis of Security Protocols).

2. Mô hình hệ thống di chúc số an toàn

2.1. Khái quát mô hình

Mô hình di chúc số được thiết kế nhằm đáp ứng đồng thời hai nhóm yêu cầu: (i) Yêu cầu pháp lý về tính xác thực, toàn vẹn, bảo vệ ý chí cuối cùng của người lập di chúc; và (ii) Yêu cầu kỹ thuật về bảo mật, khả năng kiểm chứng và chống lại các hình thức tấn công mạng. Cốt lõi của mô hình là việc ứng dụng PKI và cơ chế chia sẻ bí mật để bảo vệ nội dung di chúc ngay cả khi lưu trữ hoặc truyền tải qua môi trường mạng.

Điểm đáng chú ý là mô hình này không chỉ sao chép quy trình lập di chúc truyền thống sang hình thức điện tử, mà còn bổ sung cơ chế bảo vệ nhiều lớp, trong đó quyền truy cập và giải mã được phân tán cho nhiều bên, giảm thiểu rủi ro gian lận hoặc lạm dụng quyền hạn. Đây là cách tiếp cận phù hợp với nguyên tắc "niềm tin được thiết kế" (*trust by design*)[26], nơi niềm tin không chỉ dựa vào con người và pháp luật, mà còn được bảo đảm bởi cấu trúc công nghệ.

2.2. Các bên tham gia

Mô hình gồm sáu nhóm chủ thể tham gia với vai trò và trách nhiệm rõ ràng, gồm Cơ quan quản lý hệ thống (System authority-SA), người lập di chúc, người quản lý di sản, ngân hàng lưu trữ di chúc, Tòa án và người thừa kế.

- *Cơ quan quản lý hệ thống*

SA đóng vai trò trung tâm, chỉ chịu trách nhiệm tạo ra các tham số hệ thống, hàm mật mã và cặp khóa riêng/công khai cho từng thành viên tham gia. Khóa công khai của người tham gia được xác định bởi sự phối hợp giữa SA và người đó, trong khi khóa riêng được giữ bí mật và chỉ do người tham gia tự chọn - SA không được biết. Vai trò này tương tự "cơ quan công chứng số" trong lĩnh vực di chúc điện tử, nhưng có thêm năng lực kỹ thuật để bảo đảm an toàn thông tin. Sau giai đoạn khởi tạo, SA không tham gia vào quá trình thực thi hệ thống, từ đó giúp giảm chi phí triển khai.

- *Người lập di chúc*

Là người để lại di chúc, có hiệu lực khi họ qua đời. Người lập di chúc có quyền (i) Chỉ định người thừa kế; truất quyền hưởng di sản của người thừa kế; (ii) Phân định phần di sản cho từng người thừa kế; (iii) Dành một phần tài sản trong khối di sản để di tặng, thờ cúng; (iv) Giao nghĩa vụ cho người thừa kế; (v) Chỉ định người giữ di chúc, người quản lý di sản, người phân chia di sản. Người lập di chúc có thể sửa đổi, bổ sung, thay thế, hủy bỏ di chúc đã lập vào bất cứ lúc nào. Trường hợp người lập di chúc bổ sung di chúc thì di chúc đã lập và phần bổ sung có hiệu lực pháp luật như nhau; nếu một phần của di chúc đã lập và phần bổ sung mâu thuẫn nhau thì chỉ phần bổ sung có hiệu lực pháp luật[27].

- *Người quản lý di sản*

Về nguyên tắc, người lập di chúc có thể yêu cầu tổ chức hành nghề công chứng lưu giữ hoặc gửi người khác giữ bản di chúc. Người giữ bản di chúc có nghĩa vụ giữ bí mật nội dung di chúc; giữ gìn, bảo quản bản di chúc; nếu bản di chúc bị thất lạc, hư hại thì phải báo ngay cho người lập di chúc[28]. Tuy nhiên, trong mô hình được đề xuất, người đó phải thường xuyên kiểm tra khóa công khai của những người thụ hưởng từ SA

hoặc từ thư mục khóa công khai, và thông báo cho người lập di chúc nếu có ai thay đổi khóa. Khi người lập di chúc qua đời, người đó sẽ thông báo cho từng người trong danh sách thụ hưởng và cho ngân hàng lưu trữ di chúc. Ngoài ra, người đó còn được phép công bố di chúc và nộp hồ sơ tại cơ quan nhà nước có thẩm quyền để xin giấy chứng tử của người lập di chúc.

- Ngân hàng lưu trữ di chúc

Ngân hàng lưu trữ di chúc là một tổ chức - có thể là ngân hàng thương mại hoặc một tổ chức chuyên thực hiện nghĩa vụ ủy thác chuyên đảm nhận vai trò người được ủy thác cho nhiều loại quỹ tín thác và quản lý tài sản. Người này chịu trách nhiệm chính trong việc lưu giữ an toàn bản di chúc đã mã hóa, danh sách người thụ hưởng đã mã hóa và một số thông tin liên quan. Việc lựa chọn ngân hàng xuất phát từ yếu tố tin cậy về cơ sở hạ tầng lưu trữ và quy trình bảo mật, tương tự như "két sắt pháp lý" trong mô hình truyền thống.

- Tòa án

Trong cả hệ thống luật Common law và Civil law, Tòa án là cơ quan trung tâm để giải quyết tranh chấp, và nhìn chung mọi người đều có quyền đưa yêu cầu của mình ra trước tòa. Trong hệ thống được đề xuất, vai trò này chính là trọng tài. Khi nhận được yêu cầu từ ngân hàng, dựa trên thẩm quyền và trách nhiệm của Tòa án, người này sẽ giải mã khóa bí mật của di chúc đã mã hóa bằng khóa riêng của mình và công bố khóa đó. Như vậy, Toà án là cơ quan cuối cùng xác minh điều kiện công bố di chúc và thực hiện giải mã thay thế nếu cần, bảo đảm quy trình tuân thủ pháp luật và bảo vệ quyền lợi các bên.

- Người thừa kế

Người thừa kế là cá nhân phải là người còn sống vào thời điểm mở thừa kế hoặc sinh ra và còn sống sau thời điểm mở thừa kế nhưng đã thành thai trước khi người để lại di sản chết[29]. Như vậy, người thừa kế có thể là cá nhân hoặc pháp nhân được nhận tài sản hoặc các quyền lợi khác từ một di chúc. Khi nhận được thông báo từ người quản lý di sản, mỗi người thừa kế phải chứng minh danh tính của mình với ngân hàng để xác nhận rằng họ thực sự nằm trong danh sách hưởng di sản thừa kế. Lưu ý rằng, người thừa kế có thể không biết mình có tên trong danh sách cho đến khi nhận được thông báo từ người quản lý di sản. Trong mô hình này, quyền tiếp cận nội dung di chúc của họ chỉ được kích hoạt khi đáp ứng đầy đủ điều kiện pháp lý. Việc phân tách vai trò này thể hiện nguyên tắc phân quyền trong bảo mật thông tin, hạn chế tối đa rủi ro thao túng hoặc giả mạo di chúc.

2.3. Quy trình vận hành

Quy trình vận hành được thiết kế thành năm giai đoạn tuần tự, bảo đảm sự kiểm soát chặt chẽ ở mỗi bước:

- Giai đoạn khởi tạo

Ở giai đoạn này, SA phát hành và quản lý chứng thư số cho tất cả các bên, thiết lập cơ chế chia sẻ bí mật để phân tách khóa giải mã thành nhiều phần và lưu giữ tại các

bên khác nhau. Đây là bước nền tảng nhằm bảo đảm rằng không bên nào có thể tự ý truy cập nội dung di chúc.

- *Giai đoạn lập di chúc*

Người lập di chúc soạn thảo nội dung, ký số để xác nhận danh tính và ý chí, sau đó mã hóa bằng khóa đối xứng. Khóa này tiếp tục được mã hóa bằng khóa công khai của các bên liên quan và phân chia theo cơ chế *secret sharing*. Việc này bảo đảm tính toàn vẹn và bảo mật ngay từ khi di chúc được tạo ra, loại bỏ nguy cơ chỉnh sửa ngoài ý muốn.

- *Giai đoạn lưu giữ di chúc*

Bản di chúc mã hóa cùng thông tin về các phần khóa được lưu trữ tại Ngân hàng lưu giữ. Cơ chế kiểm tra định kỳ giúp phát hiện sớm mọi dấu hiệu xâm nhập hoặc thay đổi dữ liệu. Bình diện pháp lý ở đây là bảo đảm "niềm tin liên tục" (*continuous trust*) vào tính nguyên vẹn của di chúc.

- *Giai đoạn công bố di chúc*

Khi có giấy chứng tử hợp pháp, hệ thống kích hoạt quy trình thu thập các phần khóa từ các bên ủy quyền. Sau khi khôi phục khóa giải mã, nội dung di chúc được công bố dưới sự giám sát của Tòa án, bảo đảm vừa tuân thủ quy định pháp luật, vừa đáp ứng yêu cầu bảo mật.

- *Giai đoạn xác minh/giải trình*

Nếu một hoặc nhiều phần khóa bị mất hoặc bị từ chối cung cấp, Tòa án áp dụng cơ chế dự phòng để giải mã. Quy định này bảo vệ quyền lợi của người thụ hưởng, tránh trường hợp di chúc hợp lệ không thể thực hiện vì sự cố kỹ thuật hoặc hành vi cản trở.

2.4. Các tình huống đặc biệt

Mô hình cũng dự liệu các tình huống có thể phát sinh trong quá trình lưu giữ, như thay đổi khóa công khai, điều chỉnh danh sách người thừa kế, sửa đổi, bổ sung di chúc hoặc thay đổi, hủy khóa bí mật. Mỗi trường hợp đều đòi hỏi tái thiết lập hoặc phân phối lại khóa kèm theo quy trình xác minh pháp lý và kỹ thuật, nhằm bảo đảm thông tin trong hệ thống luôn phù hợp với ý chí của người lập di chúc. Về mặt pháp lý, mọi thay đổi phải được chứng thực và ghi nhận trong hồ sơ điện tử để bảo đảm giá trị chứng cứ khi xảy ra tranh chấp. Điều này thể hiện tính linh hoạt của mô hình: có thể thích ứng với thực tế nhưng vẫn duy trì được tính bảo mật và độ tin cậy.

3. Phân tích bảo mật và khả năng triển khai

3.1. Phân tích bảo mật theo chuẩn quốc tế

Việc đánh giá mô hình di chúc số cần dựa trên các chuẩn bảo mật quốc tế, trong đó khung tham chiếu ITU-T X.800 là cơ sở quan trọng để phân tích toàn diện bốn thuộc tính then chốt:

- Tính bảo mật: Mô hình bảo đảm rằng chỉ các chủ thể được ủy quyền và đáp ứng điều kiện pháp lý mới có quyền truy cập nội dung di chúc. Việc kết hợp mã hóa đối xứng, mã hóa bất đối xứng và chia sẻ bí mật giúp loại bỏ khả năng truy cập trái phép

ngay cả khi dữ liệu bị đánh cắp từ nơi lưu trữ. Đây là yếu tố đặc biệt quan trọng với di chúc, bởi nội dung của nó thường chứa thông tin tài sản nhạy cảm.

- Toàn vẹn dữ liệu: Cơ chế ký số bảo đảm mọi thay đổi trong nội dung di chúc đều có thể bị phát hiện. Ngay cả khi kẻ tấn công can thiệp vào bản mã hóa, hệ thống vẫn sẽ từ chối giải mã nếu chữ ký số không khớp. Điều này tương đương với việc niêm phong vật lý trong di chúc truyền thống, nhưng an toàn hơn vì có thể kiểm chứng bằng thuật toán.

- Tính xác thực: Sử dụng chứng thư số do cơ quan chứng thực tin cậy cấp, mô hình bảo đảm danh tính của người lập di chúc và các bên tham gia được xác minh chính xác. Đây là điều kiện tiên quyết để di chúc số có giá trị pháp lý tương đương với di chúc có công chứng, chứng thực truyền thống.

- Chống chối bỏ: Khi người lập di chúc ký số, hành vi này được lưu trữ cùng dấu thời gian và chứng thư số, tạo bằng chứng không thể phủ nhận về việc họ đã lập di chúc. Điều này đặc biệt hữu ích khi có tranh chấp, bởi chứng cứ điện tử được tạo ra có giá trị chứng minh mạnh mẽ trước tòa.

Ngoài ra, mô hình còn được thiết kế để chống lại các dạng tấn công phổ biến:

- Giả mạo: Chứng thư số và xác thực hai lớp ngăn chặn việc mạo danh.

- Phát lại: Các bản ghi giao dịch kèm dấu thời gian và mã định danh duy nhất loại bỏ khả năng sử dụng lại thông điệp cũ.

- Xen giữa: Mã hóa đầu - cuối và cơ chế trao đổi khóa an toàn giúp vô hiệu hóa nguy cơ bị can thiệp trong quá trình truyền dữ liệu.

3.2. Kết quả kiểm chứng AVISPA

Để kiểm chứng tính an toàn của mô hình, công cụ AVISPA được sử dụng. Đây là một nền tảng kiểm tra bảo mật dựa trên mô hình hình thức, cho phép mô phỏng và đánh giá khả năng chống chịu của giao thức trước các tấn công đã biết.

Quy trình mô phỏng bắt đầu bằng việc chuyển đổi các bước giao tiếp trong mô hình di chúc số sang ngôn ngữ đặc tả HLPSL. Sau đó, các kịch bản tấn công giả định như giả mạo, phát lại, xen giữa được thiết lập. AVISPA thực hiện kiểm tra bằng nhiều back-end, trong đó OFMC (On-the-Fly Model Checker) và CL-AtSe (Constraint-Logic-based Attack Searcher) cho kết quả "SAFE", nghĩa là không phát hiện lỗ hổng bảo mật đối với các dạng tấn công đã mô phỏng. Điểm đáng chú ý là kết quả kiểm chứng không chỉ xác nhận mô hình đạt chuẩn an toàn, mà còn minh chứng khả năng ứng dụng thực tiễn, vì AVISPA là công cụ được giới nghiên cứu và công nghiệp tin cậy trên toàn cầu.

3.3. Khả năng triển khai mô hình

Về mặt hạ tầng kỹ thuật, Việt Nam đã xây dựng hạ tầng khóa công khai quốc gia (National PKI) và hệ thống các tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng được cấp phép. Đây là nền tảng quan trọng để triển khai mô hình di chúc số mà không cần đầu tư lại từ đầu. Bên cạnh đó, nhiều ngân hàng thương mại lớn tại Việt Nam đã đạt chuẩn ISO/IEC 27001 về quản lý an toàn thông tin, đủ năng lực đóng vai trò ngân hàng lưu giữ trong mô hình. Về phía cơ quan tư pháp, hệ thống Tòa án nhân dân các cấp

đang từng bước áp dụng số hóa hồ sơ và ứng dụng công nghệ trong xét xử, cho thấy khả năng tiếp nhận quy trình giải mã và công bố di chúc số là hoàn toàn khả thi.

Tuy nhiên, để triển khai thành công, cần đồng bộ hóa ba yếu tố: (i) Bổ sung quy định pháp lý công nhận di chúc số; (ii) Xây dựng quy trình nghiệp vụ chuẩn cho các bên tham gia; (iii) Tổ chức đào tạo, nâng cao năng lực vận hành và bảo mật thông tin cho cán bộ, công chức và các đơn vị lưu giữ.

4. Khoảng trống pháp lý tại Việt Nam

BLDS năm 2015 và Luật Công chứng năm 2024 chưa có quy định công nhận hình thức di chúc số. Dù Luật Giao dịch điện tử năm 2005 và năm 2023 đã thừa nhận giá trị pháp lý của thông điệp dữ liệu trong giao dịch dân sự, nhưng điều này chưa được dẫn chiếu hay áp dụng cụ thể vào chế định thừa kế. Luật Công chứng năm 2024 cũng duy trì yêu cầu lập di chúc phải thực hiện bằng văn bản giấy với sự chứng nhận trực tiếp của công chứng viên hoặc người có thẩm quyền. Quy trình này mặc định rằng việc lập, ký và lưu giữ di chúc phải diễn ra trong môi trường vật lý, không tính đến khả năng xác lập và lưu trữ bằng phương tiện điện tử.

Có ba nhóm rào cản pháp lý chính khiến di chúc số chưa thể triển khai ở Việt Nam:

- Yêu cầu văn bản giấy: BLDS năm 2015 và Luật Công chứng năm 2024 đều gắn điều kiện hiệu lực của di chúc với hình thức văn bản giấy, khiến di chúc số không đáp ứng tiêu chí hình thức ngay từ đầu.

- Thiếu quy định về định danh điện tử trong lập di chúc: Luật Giao dịch điện tử và các văn bản liên quan chưa đưa ra cơ chế định danh điện tử chuyên biệt cho giao dịch lập di chúc, dẫn đến khó khăn khi xác thực danh tính và ý chí của người lập di chúc.

- Giá trị chứng cứ của tài liệu số: Bộ luật Tố tụng dân sự năm 2015 chưa quy định rõ về giá trị chứng minh của di chúc được lập và lưu trữ điện tử, đặc biệt là khi cần so sánh với bản gốc hoặc kiểm chứng tính toàn vẹn.

Những rào cản này cho thấy khoảng trống giữa công nghệ và pháp luật, đồng thời phản ánh sự cần thiết phải điều chỉnh các quy định hiện hành để đáp ứng thực tiễn số hóa.

5. Đề xuất khung pháp lý cho di chúc số

5.1. Nguyên tắc xây dựng

Thứ nhất, nguyên tắc bảo mật - toàn vẹn - xác thực - chống chối bỏ.

Đây là "bốn trụ cột" của bảo mật thông tin theo chuẩn quốc tế (ITU-T X.800, ISO/IEC 27001). Nếu không nội luật hóa rõ ràng, di chúc số sẽ thiếu nền tảng để chống lại rủi ro tấn công mạng hoặc tranh chấp về tính xác thực. Ví dụ, ở một số quốc gia đã công nhận di chúc điện tử, phần lớn tranh chấp xuất phát từ nghi ngờ về danh tính hoặc việc chỉnh sửa tài liệu. Do đó, khung pháp lý của Việt Nam phải quy định rõ ràng: di chúc số chỉ có hiệu lực khi được tạo lập, lưu trữ và công bố theo quy trình bảo đảm đủ bốn yếu tố này.

Thứ hai, nguyên tắc tôn trọng ý chí cá nhân và quyền thừa kế.

Pháp luật về thừa kế, dù ở dạng truyền thống hay số hóa, đều phải xuất phát từ việc bảo vệ ý chí tự do của người lập di chúc. Đặc biệt với di chúc số, các cơ chế kỹ thuật (như mã hóa, phân tán khóa) phải được thiết kế sao cho người lập di chúc có thể thay đổi hoặc hủy bỏ di chúc bất kỳ lúc nào, tương tự các quyền đã được BLDS năm 2015 ghi nhận. Điều này giúp bảo đảm nguyên tắc bình đẳng giữa hình thức số và hình thức truyền thống, tránh tình trạng "kỹ thuật lấn át pháp lý".

5.2. Một số đề xuất

- Một là, định nghĩa "di chúc số" trong BLDS năm 2015.

Việc bổ sung định nghĩa "di chúc số" là nền tảng để giải quyết khoảng trống pháp lý. Nếu chỉ dùng khái niệm "di chúc điện tử" thì sẽ bỏ sót yếu tố kiến trúc bảo mật, vốn là cốt lõi của digital will. Định nghĩa này cần thể hiện hai nội dung: (i) Phương thức lập, lưu trữ và công bố hoàn toàn bằng điện tử; (ii) Tuân thủ các chuẩn bảo mật quốc tế nhằm bảo vệ ý chí và thông tin tài sản. Điều này cũng giúp phân định rõ với di chúc điện tử chỉ dừng ở mức thay thế giấy tờ.

- Hai là, quy định về cơ quan chứng thực số và lưu giữ di chúc.

Một trong những điểm yếu của di chúc truyền thống là phụ thuộc vào công chứng viên hoặc người làm chứng, vốn có thể bị mua chuộc hoặc sai sót. Trong di chúc số, chức năng này nên được giao cho cơ quan chứng thực số - tương đương "công chứng viên điện tử" - có quyền cấp chứng thư số và xác thực danh tính qua các phương thức mạnh (biometrics, eID quốc gia). Về lưu giữ, nên giao cho ngân hàng, tổ chức tài chính hoặc trung tâm dữ liệu đạt chuẩn bảo mật quốc tế (ISO/IEC 27001). Điều này vừa tận dụng hạ tầng sẵn có, vừa bảo đảm năng lực bảo mật, tương tự mô hình của Canada và bang Nevada (Mỹ).

- Ba là, quy trình xác nhận, lưu giữ, công bố.

Quy trình này nên được luật hóa thành các bước rõ ràng:

Xác nhận: Người lập ký số bằng chứng thư số hợp lệ, gắn dấu thời gian (*timestamp*) để chống sửa đổi và tranh chấp về thời điểm lập di chúc.

Lưu giữ: Lưu bản mã hóa của di chúc cùng các phần khóa được phân chia cho các bên ủy quyền; định kỳ kiểm tra tính toàn vẹn dữ liệu.

Công bố: Khi có giấy chứng tử hợp pháp, thu thập các phần khóa để giải mã và công bố dưới sự giám sát của Tòa án, bảo đảm cả tính hợp pháp và hợp lệ về kỹ thuật.

- Bốn là, cơ chế giải quyết tranh chấp và giải mã thay thế.

Điểm mới của di chúc số là khả năng dự phòng giải mã nếu một hoặc nhiều bên giữ khóa không hợp tác hoặc bị mất dữ liệu. Tòa án nên có thẩm quyền kích hoạt cơ chế này, sử dụng bản sao khóa lưu trữ an toàn hoặc cơ chế khôi phục bằng mật mã ngưỡng *(threshold cryptography)*. Đồng thời, cần quy định rõ giá trị chứng cứ của log hệ thống, dấu thời gian, và chứng thư số để chúng có thể được chấp nhận như chứng cứ điện tử hợp pháp.

Điểm mạnh của đề xuất này là tận dụng hạ tầng PKI quốc gia và hệ thống ngân hàng mà vốn đã tồn tại và đạt chuẩn bảo mật để giảm chi phí triển khai. Tuy nhiên, thách

thức lớn nhất sẽ là thay đổi nhận thức pháp lý và đào tạo nhân sự có khả năng vận hành, giám sát mô hình di chúc số.

Kết luận

Sự bùng nổ của công nghệ thông tin, đặc biệt là PKI và các chuẩn bảo mật quốc tế, đang mở ra khả năng hiện thực hóa mô hình di chúc số tại Việt Nam. BLDS năm 2015 và Luật Công chứng năm 2024 chưa công nhận hình thức lập và lưu giữ di chúc hoàn toàn điện tử, đồng thời chưa có quy định về định danh điện tử, tiêu chuẩn bảo mật và giá trị chứng cứ của di chúc số. Khoảng trống này đồng nghĩa với việc, dù công nghệ đã sẵn sàng, di chúc số vẫn "đứng ngoài cuộc chơi" của chế định thừa kế./.

---

[1] Michaels, R, *The functional method of comparative law*, The Oxford handbook of comparative law, 2006, tr. 345-389.

[2] Theo Bộ Thông tin và Truyền thông, 88,7% thuê bao di động sử dụng smartphone, 82,3% hộ gia đình có kết nối Internet cáp quang băng rộng và mạng 4G phủ sóng 99,8% lãnh thổ, https://mst.gov.vn/internet-viet-nam-ba-muoi-nam-phat-trien-than-toc-197241227122858638.htm, truy cập ngày 01/11/2025.

[3] Tiêu chuẩn ITU-T X.800 có hai nhiệm vụ chính: (1) Mô tả tổng quan các dịch vụ và cơ chế bảo mật trong mô hình OSI, như xác thực, toàn vẹn, bí mật, mã hóa, chữ ký số và kiểm soát truy cập; (2) Xác định vị trí thích hợp trong từng tầng của mô hình OSI để triển khai các dịch vụ và cơ chế này, https://www.itu.int/rec/T-REC-X.800-199610-I!Amd1, truy cập ngày 01/11/2025.

[4] ISO/IEC 27001 là tiêu chuẩn quốc tế về Hệ thống Quản lý an toàn thông tin (ISMS), giúp tổ chức xây dựng và duy trì hệ thống bảo mật nhằm đảm bảo bí mật – toàn vẹn – sẵn sàng của thông tin, đồng thời giảm rủi ro và tuân thủ pháp luật, https://www.iso.org/standard/27001, truy cập ngày 01/11/2025.

[5] W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory, số 6, 1976, tr. 644 - 654.

[6] R.L. Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, số 2, 1978, tr. 120 - 126.

[7] Khóa riêng tư (private key) do người dùng giữ bí mật và khóa công khai (public key) được công bố rộng rãi.

[8] S. Jiang and Y. Zhang, *Partial key escrow monitoring scheme*, Cryptology ePrint Archive, Report 2002/039, available at http://eprint.iacr.org/2002/039, truy cập ngày 01/11/2025.

[9] M. Tompa and H. Woll, *How to share a secret with cheaters*, Journal of Cryptology, số 3, 1989, tr. 133 - 138.

[10] R.L. Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, số 2, 1978, tr. 120 - 126.

[11] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory, số 4, 1985, tr. 469 - 472.

[12] FIPS 197, *Advanced encryption standard (AES)*, National Institute of Standards and Technology, Federal Information Processing Standards Publication 197, Nov. 2001.

[13] ISO/IEC 9594-8, *Information technology - Open Systems Interconnection - The directory: authentication framework*, International Organization for Standardization, Geneva, Switzerland, 1998.

[14] B. Waters, *Efficient Identity-based encryption without random oracles*, Advances in Cryptology - EUROCRYPT'05, Lecture Notes in Computer Science, 2005, tr. 114 - 127.

[15] S. Araki, S. Uehara and K. Imamura, *The limited verifier signature and its application*,IEICE Transactions on Fundamentals, số 1, 1999, tr. 63 - 68.

[16] T.S. Wu and C.L. Hsu, *Convertible authenticated encryption scheme*, The Journal of Systems and Software, số 3, 2002, tr. 205 - 209.

[17] T.S. Wu, Y.S. Chen and H.Y. Lin, *Toward efficient convertible authenticated encryption schemes using self-certified public key system*, KSII Transactions on Internet and Information Systems, số 3, 2014, tr. 1157 - 1177.

[18] Q. Xie, G. Wang, F. Xia, and D. Chen, *Self-certified proxy convertible authenticated encryption: formal definitions and a provably secure scheme*, Concurrency and Computation: Practice and Experience, 2013.

[19] J.L. Tsai, N.W. Lo and T.C. Wu, *Efficient convertible multi-authenticated encryption scheme for group communications*, Biometrics and Security Technologies (ISBAST), 2012, tr. 54 - 58.

[20] ISO/IEC 9594-8, *Information technology – Open Systems Interconnection - The directory: authentication framework*, International Organization for Standardization, Geneva, Switzerland, 1998.

[21] H.Y. Lin, T.S. Wu, and S.K. Huang, *Certificate-Based secure three-party signcryption scheme with low costs*, Journal of Information Science and Engineering, số 4, 2012, tr. 739 - 753.

[22] M. Michels and P. Horster, *On the risk of disruption in several multiparty signature schemes*, Advances in Cryptology – ASIACRYPT'96, Lecture Notes in Computer Science, 1996, tr. 334 - 345.

[23] S. Micali, *Fair public-key cryptosystems*, Advances in Cryptology - CRYPTO'92, Lecture Notes in Computer Science, 1992, tr. 113 - 138.

[24] FIPS 185, *Escrowed encryption standard (EES)*, National Institute of Standards and Technology, Federal Information Processing Standards Publication 185, Feb. 1994.

[25] AVISPA, Automated validation of internet security protocols and applications, https://avispa-project.org/main, truy cập ngày 01/11/2025.

[26] Ferraris, D., Fernandez-Gago, C., & Lopez, J., *A trust-by-design framework for the internet of things*, In 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE, 2018, tr. 1 - 4.

[27] Điều 640 BLDS năm 2015.

[28] Điều 641 BLDS năm 2015.

[29] Điều 613 BLDS năm 2015.