# AN TOÀN, BẢO MẬT THÔNG TIN TRONG CHUYỂN ĐỔI SỐ

LÊ THỊ THU THỦY*

*Chuyển đổi số là quá trình sử dụng các công nghệ số để cải thiện hiệu quả, chất lượng và giá trị của các hoạt động và dịch vụ. Chuyển đổi số đã mở ra một kỷ nguyên mới cho sự kết nối và tiện ích trong các lĩnh vực của đời sống xã hội, tuy nhiên, cũng đặt ra nhiều thách thức và rủi ro về an toàn, bảo mật thông tin, như: bị mất mát, hư hỏng, xâm nhập, đánh cắp, lợi dụng, sai lệch thông tin, vi phạm quyền riêng tư, bảo mật, pháp luật. Bài viết nghiên cứu thực trạng an toàn, bảo mật thông tin, từ đó đề xuất một số giải pháp nhằm nâng cao công tác bảo đảm an toàn, bảo mật thông tin trong quá trình chuyển đổi số tại Việt Nam.*

***Từ khóa:*** *Chuyển đổi số; an toàn và bảo mật thông tin; công nghệ số.*

*Digital transformation is the process of using digital technologies to improve the efficiency, quality, and value of operations and services. While digital transformation has opened a new era of connectivity and utility across various aspects of social life, it also presents numerous challenges and risks concerning information safety and security, including loss, damage, intrusion, theft, exploitation, misinformation, privacy violations, and legal breaches. The article examines the current situation of information safety and security and proposes solutions to enhance information safety and security during the digital transformation process in Vietnam.*

***Keywords:*** *Digital transformation; information safety and security; digital technology.*

NGÀY NHẬN: 12/4/2024 NGÀY PHẢN BIỆN, ĐÁNH GIÁ: 19/6/2024 NGÀY DUYỆT: 16/7/2024

DOI: https:/doi.org/10.59394/qlnn.342.2024.913

## 1. Đặt vấn đề

Khi kỷ nguyên công nghệ số bắt đầu, thông tin trở thành tài sản sống còn của tất cả các tổ chức. Đặc biệt, mọi hoạt động của các cơ quan hành chính nhà nước đều diễn ra trên môi trường mạng, như: nhận, gửi văn bản điện tử, chữ ký số; cung cấp dịch vụ hành chính công tích hợp một cửa điện tử, sử dụng hệ thống hội nghị truyền hình trực tuyến... Điều đó cho thấy, việc bảo đảm an toàn, bảo mật thông tin, an ninh mạng cho các hệ thống thông tin, viễn thông tại các cơ quan, tổ chức rất quan trọng, cần được kiểm tra, rà soát thường xuyên, kịp thời để có những giải pháp đối phó, ngăn chặn các rủi ro có thể xảy ra.

## 2. Vai trò của an toàn, bảo mật thông tin trong chuyển đổi số

Ngày 15/7/2013, Chính phủ ban hành Nghị định số 72/2013/NĐ-CP về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng, theo đó, an toàn thông tin là sự bảo vệ thông tin và các hệ thống thông tin tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin. An ninh thông tin là

* *ThS, Học viện Hành chính Quốc gia*

việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của các tổ chức, cá nhân.

Bảo mật thông tin là bảo quản tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin. Ngoài ra, các tính chất khác, như: tính xác thực, trách nhiệm, không thoái thác và độ tin cậy cũng có thể được tham gia (định nghĩa theo tiêu chuẩn an ninh thông tin ISO/IEC 27000: 2009 - Viện Tiêu chuẩn Anh quốc). Các nguyên tắc cơ bản của bảo mật thông tin thường được tóm tắt bởi bộ ba CIA (Confidenttiality, Integrity, Availability) là tính bảo mật, tính toàn vẹn và tính sẵn sàng.

Chuyển đổi số là quá trình thay đổi tổng thể và toàn diện của cá nhân, tổ chức về cách sống, cách làm việc và phương thức sản xuất dựa trên các công nghệ số[1]. Do đó, vai trò của an toàn, bảo mật thông tin trong chuyển đổi số gồm:

(1) Bảo vệ dữ liệu quan trọng, trong quá trình chuyển đổi số, dữ liệu trở thành một tài nguyên quan trọng. An toàn và bảo mật thông tin giúp bảo vệ dữ liệu quan trọng của tổ chức khỏi mất mát, sửa đổi trái phép hoặc truy cập trái phép.

(2) Giảm thiểu rủi ro, an toàn và bảo mật thông tin giúp giảm thiểu các rủi ro liên quan đến mất mát dữ liệu, sự sụp đổ hệ thống hoặc thiệt hại về hình ảnh do các cuộc tấn công mạng hoặc lỗi hệ thống.

(3) Bảo vệ quyền riêng tư, bảo mật và pháp luật của các cá nhân, tổ chức liên quan đến các tài liệu, hồ sơ, thông tin. Điều này giúp tránh việc bị rò rỉ hoặc tiết lộ cho những người không liên quan. Việc bảo vệ quyền riêng tư, bảo mật và pháp luật cũng giúp nâng cao uy tín và niềm tin của khách hàng, đối tác và người dùng.

(4) Ngăn chặn các mối đe dọa mạng, trong môi trường kỹ thuật số, mối đe dọa mạng ngày càng phức tạp và nguy hiểm hơn. An toàn và bảo mật thông tin giúp ngăn chặn các cuộc tấn công mạng, virus, phần mềm độc hại và các hành vi tấn công khác.

(5) Tăng cường năng lực ứng phó và xử lý kịp thời các sự cố an toàn bảo mật thông tin giúp giảm thiểu thiệt hại và khôi phục hoạt động bình thường của các tổ chức.

(6) Phối hợp với các cơ quan chức năng để giám sát, kiểm tra và xử lý các hành vi vi phạm an toàn, bảo mật thông tin; tăng cường hợp tác quốc tế trong lĩnh vực an toàn bảo mật thông tin.

## 3. Thực trạng về an toàn, bảo mật thông tin trong chuyển đổi số ở Việt Nam

*Thứ nhất, về nhận thức và ý thức của tổ chức, cá nhân.*

Quá trình chuyển đổi số đã đặt ra nhiều thách thức, xuất hiện nhiều lỗ hổng trong công tác bảo mật, bảo đảm an ninh mạng ở nhiều tổ chức, cơ quan với các mối đe dọa từ không gian mạng, các cuộc tấn công, xâm nhập và đánh cắp dữ liệu liên tục xảy ra; các tin tặc đặc biệt chú ý đến việc đánh cắp dữ liệu trên hệ thống mạng của các cơ quan chính phủ, các cơ sở an ninh quốc phòng, tập đoàn kinh tế và cơ quan truyền thông quốc gia. Vì vậy, những năm qua, Cục An toàn thông tin, Bộ Thông tin và Truyền thông đã tích cực phát động các chương trình với mục đích tuyên truyền, giáo dục nâng cao nhận thức về các mối đe dọa trên môi trường mạng cho đội ngũ cán bộ, công chức, viên chức. Các chương trình đều đặc biệt chú trọng đến việc tuyên truyền và nâng cao ý thức nhận biết, phòng tránh và biện pháp kỹ thuật để khắc phục hậu quả trong trường hợp bị tấn công không gian mạng bằng mã độc[2]. Thông qua các khóa đào tạo, các hội nghị, hội thảo cũng như các chương trình tập huấn, diễn tập về an toàn, bảo mật thông tin cho cán bộ, nhân viên giúp họ nhận biết và phản ứng với các mối đe dọa an ninh mạng.

Tuy nhiên, trong thực tế vẫn còn một số thách thức cần vượt qua, như: nhiều tổ chức, cá nhân vẫn thiếu kiến thức chuyên môn về an toàn, bảo mật thông tin và cách áp dụng các biện pháp bảo mật; gặp khó khăn trong việc cung cấp đủ nhân lực và nguồn lực để triển khai và duy trì các biện pháp an toàn thông tin; còn chủ quan trong việc tự thực

hiện an toàn, bảo mật thông tin; chưa có chính sách bảo mật hoặc chính sách đang còn lơ lửng, không đủ cụ thể để bảo đảm an toàn thông tin; thiếu kỹ năng giải quyết sự cố, do vậy, khi gặp sự cố bảo mật, nhiều tổ chức thiếu kỹ năng và quy trình để giải quyết nhanh chóng và hiệu quả.

*Thứ hai, về quy định và tiêu chuẩn liên quan đến an toàn và bảo mật thông tin.*

Các cơ quan chức năng đã ban hành một số quy định, tiêu chuẩn quan trọng áp dụng trong việc bảo đảm an toàn và bảo mật thông tin, như: *Luật An ninh mạng* năm 2018; *Luật Bảo vệ bí mật nhà nước* năm 2018; Quy định về bảo mật thông tin cơ bản (TCVN ISO/IEC 27001) dựa trên ISO/IEC 27001 và áp dụng trong việc xây dựng, thực hiện, duy trì và cải tiến hệ thống quản lý an toàn thông tin; Quy định về bảo mật thông tin cụ thể (TCVN ISO/IEC 27002) cung cấp hướng dẫn về các biện pháp bảo mật cụ thể mà các tổ chức có thể thực hiện để bảo đảm an toàn thông tin; Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại; Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam; Chỉ thị số 01/CT-BTTTT ngày 20/01/2023 của Bộ trưởng Bộ Thông tin và Truyền thông về định hướng phát triển ngành Thông tin và Truyền thông năm 2023 và giai đoạn 2024 - 2025; Quyết định số 2692/QĐ-BTP ngày 09/11/2023 của Bộ trưởng Bộ Tư pháp về ban hành quy chế bảo đảm an toàn, an ninh thông tin mạng theo cấp độ cho trung tâm dữ liệu điện tử của Bộ Tư pháp; Quyết định số 1013/QĐ-BTC ngày 19/5/2023 của Bộ trưởng Bộ Tài chính về ban hành quy chế an toàn thông tin mạng và an ninh mạng Bộ Tài chính; Chỉ thị số 09/CT-TTg ngày 23/02/2024 của Thủ tướng Chính phủ về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ; gần đây nhất là Công điện số 33/CĐ-TTg ngày 07/4/2024 của Thủ tướng Chính phủ về tăng cường bảo đảm an toàn thông tin mạng.

Tuy nhiên, ở một số địa phương, những quy định, hướng dẫn cụ thể, chi tiết tại các cơ quan, tổ chức vẫn còn thiếu, hạn chế do các quy định và tiêu chuẩn thường rất phức tạp và đa dạng. Đặc biệt, đối với các cơ quan, tổ chức nhỏ và vừa càng trở nên khó khăn vì quy định và tiêu chuẩn đòi hỏi phải đầu tư lớn về tài nguyên, công nghệ và nhân lực. Mặt khác, công nghệ luôn thay đổi và phát triển nhanh chóng làm cho các quy định và tiêu chuẩn trở nên lạc hậu và không còn phù hợp với thực tiễn.

*Thứ ba, về công nghệ và thiết bị.*

Hiện nay, các tổ chức đã đầu tư công nghệ và thiết bị an toàn, bảo mật thông tin cung cấp nền tảng quan trọng để bảo vệ thông tin nhằm duy trì tính toàn vẹn của hệ thống, như: thiết bị tường lửa (Firewall) được sử dụng để kiểm soát và giám sát lưu lượng mạng, ngăn chặn các tấn công từ mạng bên ngoài và bảo đảm tính toàn vẹn của mạng nội bộ; hệ thống phát hiện xâm nhập (Intrusion Detection System - IDS) nhằm giám sát các hoạt động trong mạng để phát hiện các hành vi đáng ngờ và các tấn công; hệ thống phòng ngừa (Prevention System - IPS) là phiên bản nâng cấp của IDS, không chỉ phát hiện mà còn ngăn chặn các tấn công ngay từ khi bắt đầu xảy ra; giải pháp bảo mật điểm cuối (Endpoint Security Solutions) gồm phần mềm chống mã độc và phần mềm bảo mật cho các thiết bị cuối, như: máy tính và điện thoại di động; phần cứng mật mã (Cryptography Hardware) là thiết bị mã hóa phần cứng được sử dụng để thực hiện quá trình mã hóa và giải mã dữ liệu, bảo đảm tính bí mật và toàn vẹn của thông tin.

Theo báo cáo từ Công ty cổ phần Công nghệ an ninh mạng quốc gia Việt Nam (NCS), năm 2023 đã ghi nhận 13.900 vụ tấn công mạng vào các hệ thống tại Việt Nam (mỗi tháng có gần 1.200 vụ), tăng 9,5% so với năm 2022. Tỷ lệ máy tính tại Việt Nam bị mã độc tấn công trong năm 2023 là 43,6%, giảm 8,6% so với năm 2022 nhưng vẫn ở mức cao của thế giới; có tới 83.000 máy tính, máy chủ ghi nhận bị tấn công bởi mã độc mã hóa dữ liệu, tăng 8,4% so với năm 2022[3]. Thống kê mới nhất từ

Kaspersky Security Network (KSN), số vụ tấn công trực tuyến tại Việt Nam được Kaspersky phát hiện và ngăn chặn trong năm 2023 là 29.625.939 vụ, giảm 29% so với năm 2022, đưa Việt Nam đứng vị trí thứ 67 trên toàn thế giới về mức độ nguy hiểm liên quan đến việc lướt web. Ngoài ra, dữ liệu từ KSN cho thấy, các vụ tấn công mạng do các nguồn đe dọa gây ra vào năm 2023 có giảm nhẹ so với năm trước đó, với 1.674.418 sự cố (so với 1.726.804 sự cố năm 2021). Điều này đưa Việt Nam đứng thứ 3 Đông Nam Á, sau Singapore và Indonesia[4].

Những thách thức về tích hợp và tương tác do các hệ thống và thiết bị an toàn, bảo mật thông tin phải tích hợp với nhiều thành phần khác nhau nên sự tương tác giữa các thành phần này có thể tạo ra lỗ hổng bảo mật nếu không được quản lý chặt chẽ, như: khả năng rò rỉ thông tin do các thiết bị và công nghệ không an toàn; các thiết bị và công nghệ an toàn, bảo mật thông tin chứa các lỗ hổng bảo mật; thiết bị IoT thường được kết nối vào mạng nên nguy cơ bị tấn công rất lớn...

*Thứ tư, sự phối hợp và hợp tác giữa các cơ quan, tổ chức.*

Hệ thống thông tin văn thư và lưu trữ bao gồm nhiều bộ phận khác nhau, như: hệ thống ứng dụng, cơ sở dữ liệu, hạ tầng mạng; đồng thời, khả năng chia sẻ thông tin, dữ liệu giữa các cơ quan, tổ chức đang tồn tại nhiều rào cản cũng như quá trình quản lý dữ liệu và bảo mật thông tin. Việc sử dụng hệ thống dữ liệu và thông tin trên môi trường mạng khiến tiến trình chuyển đổi số đối mặt với nhiều nguy cơ, như: thư điện tử giả mạo, file đính kèm hay liên kết ẩn chứa mã độc, tội phạm công nghệ cao, tấn công mạng...

Thời gian qua, việc triển khai thực hiện các nhiệm vụ được Đảng, Nhà nước, Bộ Quốc phòng giao, Ban Cơ yếu Chính phủ đang phối hợp với các bộ, ngành, địa phương triển khai các nhiệm vụ về cơ yếu, bảo mật, an toàn thông tin theo *Luật Cơ yếu* năm 2011, *Luật Bảo vệ bí mật nhà nước* năm 2018, *Luật An toàn thông tin mạng* năm 2015, *Luật An ninh mạng* năm 2018, phục vụ nhiệm vụ xây dựng, phát triển chính phủ điện tử, chính phủ số, chỉ đạo, điều hành của lãnh đạo Đảng, Nhà nước, các bộ, ngành, địa phương. Đồng thời, Ban Cơ yếu Chính phủ đã thường xuyên phối hợp với các bộ, ngành, địa phương tổ chức, đào tạo nhằm tạo nguồn nhân lực xây dựng lực lượng cơ yếu; triển khai các hệ thống máy mã, sản phẩm mật mã; chỉ đạo về chuyên môn, nghiệp vụ bảo đảm hoạt động cho hệ thống tổ chức cơ yếu, triển khai các sản phẩm bảo mật[5].

## 4. Giải pháp tăng cường bảo mật, an toàn thông tin trong chuyển đổi số

Để triển khai các ứng dụng trong công tác quản lý nhà nước về bảo mật, an toàn thông tin trên môi trường chuyển đổi số, các cơ quan, đơn vị cần chú trọng các giải pháp sau đây:

*Một là,* từ các quy định, văn bản pháp lý cốt lõi, xác định tầm quan trọng của an toàn, bảo mật thông tin, các cơ quan, tổ chức cần xây dựng và triển khai thi hành chính sách an toàn, bảo mật thông tin hiệu quả. Các chính sách này nêu rõ mục tiêu, phạm vi và cam kết của cơ quan, tổ chức đối với việc bảo vệ thông tin; đồng thời, xác định rõ trách nhiệm của các bộ phận, cá nhân trong việc tuân thủ các biện pháp bảo mật. Các cơ quan, tổ chức cần xây dựng quy trình quản lý quyền truy cập để bảo đảm thông tin chỉ được truy cập bởi người có quyền. Xác định tiêu chuẩn mã hóa dữ liệu cho dữ liệu nhạy cảm để bảo đảm dữ liệu được bảo vệ khi chuyển đổi và lưu trữ. Quy định quy trình báo cáo và xử lý sự cố bảo mật giúp nhận biết và giải quyết các vấn đề bảo mật một cách kịp thời.

*Hai là,* thiết lập bộ phận chuyên trách về quản lý an toàn, bảo mật thông tin để xây dựng và phát triển các chính sách, quy trình và tiêu chuẩn về an toàn, bảo mật thông tin. Từ đó, thực hiện các biện pháp bảo mật cụ thể, quy định về quản lý quyền truy cập, quản lý thiết bị và quản lý dữ liệu nhạy cảm; các biện pháp bảo mật cần được xác định trong chính sách và quy trình, như: mã hóa dữ liệu, cấu hình bảo mật hệ thống, thiết lập các hệ thống kiểm tra thâm nhập và giám sát liên tục.

Đồng thời, tiến hành kiểm tra việc tuân thủ và đánh giá rủi ro định kỳ giúp xác định các vị trí yếu của hệ thống để tìm ra các lỗ hổng bảo mật, từ đó đề xuất các biện pháp cải thiện.

*Ba là*, tổ chức các khóa đào tạo, bồi dưỡng, hướng dẫn cho cán bộ, công chức, viên chức, nhân viên về an toàn, bảo mật thông tin giúp họ nhận thức về các nguy cơ bị tấn công và biện pháp bảo mật nhằm thực hiện các quy trình an toàn, bảo mật một cách chính xác. Việc cán bộ, công chức, viên chức, nhân viên nhận thức về nguy cơ an ninh mạng, như: các loại tấn công, lừa đảo, phần mềm độc hại giúp họ cảnh giác, có các biện pháp phòng ngừa, giảm thiểu nguy cơ xảy ra sự cố an ninh mạng; biết cách tránh những thao tác không an toàn và thực hiện đúng các quy trình, thủ tục bảo đảm an toàn, an ninh mạng có hiệu quả và biết cách phản hồi đúng trong trường hợp có sự cố an toàn, bảo mật thông tin xảy ra…

*Bốn là*, mã hóa dữ liệu là một cách quan trọng để bảo đảm tính bảo mật của thông tin. Tùy thuộc vào tình huống và môi trường cụ thể để lựa chọn các phương pháp mã hóa phù hợp, như: sử dụng các công cụ mã hóa email để bảo vệ nội dung email khỏi việc đọc trái phép; sử dụng các phần mềm mã hóa để mã hóa các tệp văn bản và tài liệu trước khi lưu trữ; sử dụng mã hóa cơ sở dữ liệu để bảo vệ dữ liệu trong cơ sở dữ liệu. Đối với các ứng dụng nhắn tin hoặc chia sẻ tệp cần sử dụng mã hóa đầu cuối để bảo đảm rằng dữ liệu chỉ có thể được đọc bởi người nhận cuối cùng.

*Năm là*, sao lưu dữ liệu định kỳ giúp bảo vệ dữ liệu khỏi mất mát do sự cố hệ thống, lỗi phần mềm, tấn công mạng hoặc lỗi người dùng. Việc sao lưu định kỳ có thể phục hồi dữ liệu nếu bị tấn công ransomware hoặc các hình thức tấn công khác; giúp nâng cao sự tin cậy của hệ thống do dữ liệu luôn có bản sao an toàn. Trong trường hợp nâng cấp hệ thống hoặc chuyển đổi sang phần mềm mới vẫn có bản sao lưu giúp việc chuyển đổi trở nên dễ dàng hơn. Khi thực hiện sao lưu định kỳ, cần chú ý xác định dữ liệu quan trọng cần sao lưu, xác định chu kỳ sao lưu, lựa chọn phương pháp sao lưu, sử dụng công cụ sao lưu, giám sát quá trình sao lưu, kiểm tra định kỳ các bản sao lưu để bảo đảm rằng chúng vẫn có thể được khôi phục một cách chính xác.

## 5. Kết luận

Chuyển đổi số mang lại nhiều cơ hội cho sự phát triển nhưng cũng đặt ra nhiều thách thức về an toàn, bảo mật thông tin. Qua việc thực hiện các biện pháp an toàn, bảo mật cụ thể, các cơ quan, tổ chức có thể bảo vệ thông tin quan trọng, tăng cường tính bảo mật và tin cậy của hệ thống. An toàn, bảo mật thông tin trong chuyển đổi số không chỉ là một nhiệm vụ kỹ thuật mà còn liên quan đến quản lý rủi ro, đào tạo, văn hóa tổ chức và sự phối hợp cùng nhau. Sự quan tâm và đầu tư đúng mức vào việc bảo vệ thông tin sẽ bảo đảm cho các tổ chức, cơ quan có thể vận hành an toàn và hiệu quả trong môi trường số ngày càng phức tạp❐

***Chú thích:***

1. Cục Tin học hóa - Bộ Thông tin và Truyền thông (2023). *Chuyển đổi số là gì?* https://dx.mic.gov.vn, ngày 22/4/2023.

2. Cục An toàn thông tin (2024). *Chiến dịch tuyên truyền, phổ biến và ban hành cẩm nang an toàn, an ninh mạng cho cán bộ, nhân viên các cơ quan, đơn vị nhà nước khu vực công.* https://ais.gov.vn, truy cập ngày 10/6/2024.

3. Vân Anh (2023). *3 điểm yếu của các hệ thống tại Việt Nam vị hacker tấn công nhiều nhất.* https://vietnamnet.vn, ngày 25/6/2024.

4. Hạnh Tâm (2024). *Sự tấn công trực tuyến tại Việt Nam giảm đáng kể.* https://ictvietnam.vn, ngày 25/6/2024.

5. Nguyễn Ngoan (2024). *Thanh tra Chính phủ tăng cường công tác cơ yếu, bảo mật và an toàn thông tin.* https://antoanthongtin.vn, ngày 14/5/2024.

***Tài liệu tham khảo:***

1. Trần Đức Sự (chủ biên), Nguyễn Văn Tảo, Trần Thị Lượng (2015). *Giáo trình an toàn bảo mật dữ liệu.* NXB Đại học Thái Nguyên.

2. Quốc hội (2018). *Luật An ninh mạng* năm 2018.

3. Quốc hội (2015). *Luật An toàn thông tin mạng* năm 2015.

4. Quốc hội (2018). *Luật Bảo vệ bí mật Nhà nước* năm 2018.