

## ẢNH HƯỞNG CỦA LUẬT AN NINH MẠNG ĐẾN VĂN HÓA TỔ CHỨC VÀ QUẢN LÝ CỦA CÁC TRƯỜNG ĐẠI HỌC Ở VIỆT NAM TRONG BỐI CẢNH CHUYỂN ĐỔI SỐ

Nguyễn Thu Hằng<sup>1</sup>, Đỗ Huyền Linh<sup>2</sup>

**Tóm tắt.** Trong kỷ nguyên số, các trường đại học đang trải qua một cuộc chuyển đổi số sâu rộng. Song hành với đó, các mối đe dọa an ninh mạng ngày càng gia tăng, đặt ra những yêu cầu mới về quản trị và bảo vệ thông tin. Luật An ninh mạng, với vai trò là một công cụ pháp lý quan trọng, không chỉ tác động đến các hoạt động kỹ thuật mà còn định hình lại văn hóa tổ chức và quản lý của các trường đại học. Bài viết này sẽ phân tích chi tiết những ảnh hưởng này, đồng thời đưa ra các gợi ý để các nhà quản lý giáo dục xây dựng một văn hóa an ninh mạng hiệu quả.

**Từ khóa:** Luật An ninh mạng, văn hóa tổ chức, bảo mật thông tin, trách nhiệm cá nhân và tổ chức, an toàn thông tin.

### 1. Đặt vấn đề

Chuyển đổi số đã mang đến cho các trường đại học nhiều cơ hội mới, từ việc nâng cao chất lượng giảng dạy đến việc mở rộng hợp tác quốc tế. Tuy nhiên, bên cạnh những lợi ích, quá trình này cũng đặt ra nhiều thách thức, đặc biệt là về an ninh mạng. Các cuộc tấn công mạng, rò rỉ dữ liệu, và các hình thức tấn công mạng khác đang ngày càng trở nên tinh vi và phức tạp, đe dọa đến hoạt động của các trường đại học và sự an toàn của cộng đồng học thuật. Điều này, đòi hỏi các trường đại học cần phải có cách quản lý hiệu quả phù hợp với các quy định về bảo vệ an ninh mạng.

Ngày 03 tháng 6 năm 2020, Chính phủ ban hành Quyết định số 749/QĐ-TTg phê duyệt “Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030”. Đây là văn bản pháp lý quan trọng đặt nền móng cho sự phát triển của chuyển đổi số, hướng Việt Nam trở thành quốc gia số. Ngày 25 tháng 01 năm 2022, Thủ tướng Chính phủ ban hành Quyết định số 131/QĐ-TTg phê duyệt Đề án “Tăng cường ứng dụng công nghệ thông tin và chuyển đổi số trong giáo dục và đào tạo giai đoạn 2022 - 2025, định hướng đến năm 2030”. Bộ Giáo dục và Đào tạo đã ban hành nhiều văn bản về chuyển đổi số trong lĩnh vực giáo dục, trong đó có nhiều quy định về chuyển đổi số trong giáo dục đại học. Ngày 30/12/2022, Bộ Giáo dục và Đào tạo ban hành Quyết định số 4740/QĐ-BGDĐT về Bộ chỉ số, tiêu chí đánh giá chuyển đổi số cơ sở giáo dục đại học. Cấu trúc Bộ chỉ số, tiêu chí đánh giá chuyển đổi số trường đại học gồm hai nhóm tiêu chí thành phần như sau:

Nhóm tiêu chí “Chuyển đổi số trong đào tạo”.

Nhóm tiêu chí “Chuyển đổi số trong quản trị cơ sở giáo dục đại học”.

Có nhiều định nghĩa khác nhau về chuyển đổi số nhưng có thể hiểu một cách khái quát “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].

Ngày nhận bài: 17/12/2024. Ngày chỉnh sửa: 12/01/2025. Ngày nhận đăng: 18/01/2025.

<sup>1</sup>Khoa Quản lý, Học viện Quản lý giáo dục; e-mail: [huthuhang@gmail.com](mailto:huthuhang@gmail.com)

<sup>2</sup>Học viện Ngân hàng; e-mail: [linhdh@hvn.edu.vn](mailto:linhdh@hvn.edu.vn)

Tác giả liên hệ: Nguyễn Thu Hằng. Địa chỉ e-mail: [huthuhang@gmail.com](mailto:huthuhang@gmail.com)

Chuyển đổi số trong giáo dục là việc ứng dụng công nghệ thông tin và truyền thông vào mọi hoạt động của ngành giáo dục, từ quản lý, giảng dạy đến học tập. Điều này nhằm mục tiêu nâng cao hiệu quả, chất lượng giáo dục, tạo ra những trải nghiệm học tập mới mẻ và đáp ứng yêu cầu của xã hội số. Trong đó có các ứng dụng cơ bản là: Ứng dụng công nghệ trong phương thức giảng dạy, ứng dụng công nghệ trong quản lý và ứng dụng công nghệ trong lớp học.

Có thể thấy những lợi ích to lớn mà chuyển đổi số mang lại như:

**Đáp ứng nhu cầu của thời đại kỹ thuật số:** Các công nghệ số như Internet, điện toán đám mây, trí tuệ nhân tạo đang ngày càng thay đổi cách thức hoạt động của các tổ chức, trong đó có các trường đại học. Việc chuyển đổi số giúp các trường đại học có thể nắm bắt và vận dụng các công nghệ mới này để cải thiện chất lượng đào tạo, quản lý và phục vụ người học.

**Nâng cao trải nghiệm người học:**

Tạo ra môi trường học tập hiện đại, tương tác.

**Cá nhân hóa quá trình học tập:** Việc sử dụng các công nghệ số như học trực tuyến, thực tế ảo/tăng cường, phân tích dữ liệu có thể giúp nâng cao trải nghiệm của người học, tạo ra những môi trường học tập năng động, cá nhân hóa và hiệu quả hơn.

**Tiếp cận nguồn kiến thức vô tận trên Internet:** Sinh viên ở mọi nơi có thể tiếp cận với giáo dục chất lượng cao; Xóa bỏ rào cản về không gian và thời gian.

Trang bị cho sinh viên những kỹ năng cần thiết để sống và làm việc trong xã hội số.

**Cải thiện hiệu quả quản lý và vận hành:** Chuyển đổi số giúp các trường đại học số hóa các quy trình, dữ liệu và hoạt động, từ đó nâng cao tính minh bạch, tự động hóa các công việc, cải thiện ra quyết định dựa trên dữ liệu. Nhờ có chuyển đổi số mà các trường quản lý dữ liệu sinh viên, giảng viên và kết quả học tập một cách hiệu quả và tự động hóa các công việc hành chính. Việc sử dụng các hình thức lớp học thông minh, học trực tuyến (qua các nền tảng như Google Classroom, Zoom, Moodle), sử dụng các ứng dụng di động, thư viện số (thay vì sách giấy, sinh viên có thể truy cập vào kho tàng kiến thức khổng lồ trên thư viện số) hay quản lý sinh viên bằng phần mềm (phần mềm quản lý điểm số, lịch học, thông tin của sinh viên, quản lý đánh giá và kiểm định chất lượng thông qua phần mềm lưu trữ các minh chứng,...) đã và đang chứng minh những tác dụng có ích của chuyển đổi số.

## **2. Ảnh hưởng của Luật An ninh mạng đến văn hóa tổ chức và quản lý của các trường đại học**

Ngày 12 tháng 6 năm 2018, Quốc hội đã thông qua Luật An ninh mạng. Luật có 7 chương, 43 điều, bắt đầu có hiệu lực từ ngày 01 tháng 01 năm 2019. Luật điều chỉnh vấn đề an ninh trên môi trường mạng, đảm bảo các hoạt động diễn ra trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. Luật quy định các biện pháp để đảm bảo an ninh mạng. Đồng thời, luật quy định các hành vi bị cấm liên quan đến an ninh mạng. Luật An ninh mạng được ban hành với mục tiêu bảo vệ an ninh quốc gia, trật tự, an toàn xã hội trong không gian mạng. Việc thực thi luật này đã ảnh hưởng đáng kể đến hoạt động của các trường đại học, đặc biệt là về văn hóa tổ chức và quản lý. Với sự ra đời của Luật An ninh mạng làm thay đổi nhận thức cộng đồng về tầm quan trọng của an ninh mạng, từ đó thúc đẩy các trường đại học xây dựng một văn hóa bảo mật.

### **2.1. Luật An ninh mạng góp phần nâng cao nhận thức và tăng cường trách nhiệm của chủ thể quản lý**

Luật An ninh mạng quy định rõ ràng trách nhiệm của từng cá nhân và tổ chức trong việc bảo vệ thông tin. Tại khoản 2 Điều 23 có quy định trách nhiệm của người đứng đầu cơ quan tổ chức “Người đứng đầu cơ quan, tổ chức có trách nhiệm triển khai hoạt động bảo vệ an ninh mạng thuộc quyền quản lý”. Với quy định này thì người đứng đầu các trường Đại học phải có trách nhiệm triển khai hoạt động an ninh mạng thuộc quyền quản lý. Vai trò này không chỉ mang tính pháp lý mà còn có ý nghĩa quan trọng trong việc đảm bảo

hoạt động hiệu quả và an toàn của nhà trường. Khi người đứng đầu nhà trường quan tâm và đầu tư vào an ninh mạng, điều này sẽ tạo ra một văn hóa tổ chức chú trọng đến bảo mật thông tin. Cụ thể: (i) Tăng cường niềm tin cho sinh viên: Sinh viên, giảng viên và các đối tác sẽ cảm thấy an tâm hơn khi biết rằng thông tin cá nhân và dữ liệu của họ được bảo vệ an toàn. (ii) Nâng cao hiệu quả làm việc: Một hệ thống thông tin an toàn và ổn định sẽ giúp cải thiện hiệu quả làm việc của cán bộ, giảng viên và sinh viên. (iii) Xây dựng hình ảnh: Một trường đại học có hệ thống an ninh mạng tốt sẽ tạo dựng được hình ảnh uy tín và chuyên nghiệp. Để thực hiện tốt vai trò này, người đứng đầu cần có tầm nhìn chiến lược, sự đầu tư đúng mức và sự phối hợp chặt chẽ với các đơn vị liên quan. Bảo vệ an ninh mạng không chỉ là một yêu cầu pháp lý mà còn là một yếu tố quyết định đến sự phát triển bền vững của nhà trường.

Luật An ninh mạng góp phần tư duy đổi tư duy về an ninh mạng. Trước tiên, đó là tư duy từ thụ động sang chủ động: Luật đã chuyển đổi tư duy về an ninh mạng từ việc ứng phó sự cố sang chủ động phòng ngừa, xây dựng một hệ thống bảo mật toàn diện. Trước khi Luật An ninh mạng được ban hành, nhiều tổ chức, trong đó có các trường đại học, thường có xu hướng chỉ chú trọng vào việc ứng phó khi sự cố an ninh mạng xảy ra. Điều này dẫn đến nhiều hệ lụy như:

**Thiệt hại lớn:** Các cuộc tấn công mạng thường gây ra những hậu quả nghiêm trọng về kinh tế, uy tín và thậm chí cả an ninh quốc gia.

**Mất thời gian và nguồn lực:** Việc khắc phục hậu quả thường tốn kém nhiều thời gian và nguồn lực hơn so với việc phòng ngừa.

Luật An ninh mạng đã tạo ra một bước ngoặt quan trọng, yêu cầu các tổ chức phải chuyển đổi tư duy từ bị động sang chủ động. Cụ thể:

**Đề cao phòng ngừa:** Luật nhấn mạnh tầm quan trọng của việc xây dựng và triển khai các biện pháp phòng ngừa, như đánh giá rủi ro, xây dựng hệ thống bảo mật,...

**Xây dựng hệ thống bảo mật toàn diện:** Luật yêu cầu các tổ chức phải xây dựng một hệ thống bảo mật bao gồm nhiều lớp bảo vệ, từ hạ tầng mạng đến ứng dụng và người dùng.

**Ứng phó kịp thời:** Mặc dù đề cao phòng ngừa, Luật vẫn quy định các biện pháp ứng phó khi sự cố xảy ra, nhưng với mục tiêu hạn chế thiệt hại đến mức thấp nhất.

Các quy định cụ thể trong Luật An ninh mạng thể hiện rõ sự chuyển đổi tư duy này. Tại Điều 16 của Luật An ninh mạng quy định quy định về ứng phó với sự cố an ninh mạng, nhưng đồng thời cũng yêu cầu các tổ chức phải có kế hoạch ứng phó trước.

**Điều 16. Phòng ngừa, xử lý thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế.**

Thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm: a) Tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân; b) Chiến tranh tâm lý, kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước; c) Xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc.

Thông tin trên không gian mạng có nội dung kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng bao gồm: a) Kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân; b) Kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự.

Thông tin trên không gian mạng có nội dung làm nhục, vu khống bao gồm: a) Xúc phạm nghiêm trọng danh dự, uy tín, nhân phẩm của người khác; b) Thông tin bịa đặt, sai sự thật xâm phạm danh dự, uy tín, nhân phẩm hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác.

Thông tin trên không gian mạng có nội dung xâm phạm trật tự quản lý kinh tế bao gồm: a) Thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá

khác; b) Thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp, chứng khoán.

Thông tin trên không gian mạng có nội dung bịa đặt, sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác.

Hiện nay, các trường đại học sở hữu trang web riêng là một lợi thế lớn trong việc truyền thông và kết nối. Ở nhiều trường đại học, cấp khoa, cấp phòng cũng có những trang web riêng và có các diễn đàn trao đổi, điều này cũng đồng thời mở ra khả năng bị lợi dụng để truyền bá thông tin sai lệch, kích động gây rối. Khi thực hiện chuyển đổi số thì việc các trường đại học phải ứng dụng công nghệ vào giáo dục đã trở nên phổ biến. Tuy nhiên, các nhà trường cần đặc biệt lưu ý đến vấn đề bảo mật thông tin cá nhân của sinh viên, giảng viên và nhân viên nhà trường. Những rủi ro có thể thường gặp là:

**Rò rỉ dữ liệu cá nhân:** Khi sử dụng các nền tảng học tập trực tuyến, thông tin cá nhân của học sinh như tên, ngày sinh, địa chỉ, số điện thoại có thể bị xâm nhập và sử dụng trái phép dẫn đến dữ liệu của sinh viên có thể bị rò rỉ do các lỗ hổng bảo mật của nền tảng hoặc do hành vi của người dùng.

**Mất dữ liệu học tập:** Dữ liệu học tập của sinh viên có thể bị mất hoặc bị hỏng do sự cố kỹ thuật hoặc tấn công mạng.

**Nguy cơ bị tấn công mạng:** Các hệ thống quản lý sinh viên, điểm số, lịch học... nếu không được bảo mật tốt có thể trở thành mục tiêu tấn công của hacker, Các nền tảng học tập trực tuyến có thể trở thành mục tiêu của các cuộc tấn công mạng như virus, phần mềm độc hại, tấn công từ chối dịch vụ (DDoS) dẫn đến việc làm gián đoạn quá trình học tập và gây ảnh hưởng đến uy tín của nhà trường.

**Vi phạm bản quyền:** Việc sử dụng trái phép các tài liệu, phần mềm học tập có bản quyền có thể dẫn đến các vấn đề pháp lý cho nhà trường và giảng viên. Việc sử dụng các nền tảng học tập trực tuyến mang lại nhiều lợi ích nhưng cũng tiềm ẩn nhiều rủi ro, đặc biệt là về bảo mật dữ liệu.

Nếu dữ liệu cá nhân của sinh viên bị rò rỉ, có thể gây ra nhiều hậu quả nghiêm trọng, bao gồm:

**Lừa đảo:** Thông tin cá nhân như số điện thoại, địa chỉ, số tài khoản có thể bị kẻ xấu lợi dụng để thực hiện các hoạt động lừa đảo, chiếm đoạt tài sản.

**Mạo danh:** Kẻ xấu có thể sử dụng thông tin cá nhân của sinh viên để mạo danh, gây ảnh hưởng đến uy tín và danh dự của người bị hại.

**Quấy rối:** Sinh viên có thể bị quấy rối, đe dọa qua điện thoại, email hoặc mạng xã hội.

**Mất việc làm:** Trong một số trường hợp, thông tin cá nhân bị rò rỉ có thể ảnh hưởng đến cơ hội việc làm của sinh viên trong tương lai.

**Mất niềm tin:** Sự cố rò rỉ dữ liệu có thể làm giảm niềm tin của sinh viên vào nhà trường, ảnh hưởng đến uy tín của tổ chức.

Để đối phó với tình trạng này, các trường cần sử dụng các công nghệ mới để tăng cường bảo mật cho trang web.

Tại Điều 17 Luật An ninh mạng đã quy định về việc phòng chống gián điệp mạng. Điều này, đòi hỏi lãnh đạo các trường đại học phải đặc biệt quan tâm nhằm đảm bảo thông tin, bí mật cá nhân của giảng viên, nhân viên và sinh viên trên môi trường mạng.

**Điều 17. Phòng, chống gián điệp mạng; bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân trong không gian mạng**

Các cơ quan, tổ chức, cá nhân có trách nhiệm bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân trong không gian mạng.

Cơ quan nhà nước có thẩm quyền bảo vệ thông tin thuộc bí mật nhà nước trong không gian mạng.

Các tổ chức, cá nhân có nghĩa vụ thực hiện các biện pháp bảo vệ thông tin thuộc bí mật công tác, bí mật kinh doanh, bí mật cá nhân của mình và của người khác trong không gian mạng.

## 2.2. Luật An ninh mạng góp phần thay đổi văn hóa quản lý trong các trường đại học

Luật An ninh mạng quy định trách nhiệm của người đứng đầu cơ quan tổ chức tại khoản 2 Điều 23 của luật “Người đứng đầu cơ quan, tổ chức có trách nhiệm triển khai hoạt động bảo vệ an ninh mạng thuộc quyền quản lý” [5].

Trước những tác động của Luật An ninh mạng, khi thực hiện chuyển đổi số các trường đại học cần phải cải cách quy trình quản lý:

Quản lý rủi ro: Các trường đại học phải xây dựng và thực hiện các quy trình quản lý rủi ro an ninh mạng, đánh giá thường xuyên và điều chỉnh cho phù hợp. Các trường đại học phải xây dựng một mô hình quản lý linh hoạt, thích ứng với sự thay đổi không ngừng của môi trường an ninh mạng. Cụ thể là:

Xây dựng, hoàn thiện quy định, quy chế sử dụng mạng máy tính nội bộ, mạng máy tính có kết nối mạng Internet; phương án bảo đảm an ninh mạng đối với hệ thống thông tin; phương án ứng phó, khắc phục sự cố an ninh mạng;

Ứng dụng, triển khai phương án, biện pháp, công nghệ bảo vệ an ninh mạng đối với hệ thống thông tin và thông tin, tài liệu được lưu trữ, soạn thảo, truyền đưa trên hệ thống thông tin thuộc phạm vi quản lý;

Tổ chức bồi dưỡng kiến thức về an ninh mạng cho cán bộ quản lý, giảng viên, viên chức, người lao động và sinh viên nâng cao năng lực bảo vệ an ninh mạng cho lực lượng bảo vệ an ninh mạng;

Bảo vệ an ninh mạng trong hoạt động cung cấp dịch vụ công trên không gian mạng, cung cấp, trao đổi, thu thập thông tin với cơ quan, tổ chức, cá nhân, chia sẻ thông tin trong nội bộ và với cơ quan khác hoặc trong hoạt động khác theo quy định của Chính phủ;

Đầu tư, xây dựng hạ tầng cơ sở vật chất phù hợp với điều kiện bảo đảm triển khai hoạt động bảo vệ an ninh mạng đối với hệ thống thông tin;

Kiểm tra an ninh mạng đối với hệ thống thông tin; phòng, chống hành vi vi phạm pháp luật về an ninh mạng; ứng phó, khắc phục sự cố an ninh mạng.

Thực hiện quản lý bảo mật thông tin: Việc thu thập, lưu trữ và xử lý dữ liệu cá nhân phải tuân thủ nghiêm ngặt các quy định của Luật, đòi hỏi các trường phải xây dựng hệ thống quản lý thông tin bảo mật.

Luật An ninh mạng đã và đang tạo ra những tác động sâu sắc đến văn hóa tổ chức của các trường đại học Việt Nam, đặc biệt là trong việc hình thành và phát triển các giá trị cốt lõi như: Văn hóa chia sẻ, văn hóa tuân thủ, văn hóa học hỏi và văn hóa trách nhiệm.

Văn hóa chia sẻ: Luật An ninh mạng khuyến khích các tổ chức chia sẻ thông tin về các mối đe dọa, các vụ việc an ninh mạng để cùng nhau nâng cao khả năng phòng ngừa và ứng phó. Cùng với đó, việc áp dụng luật góp phần xây dựng cộng đồng học hỏi, hỗ trợ lẫn nhau trong việc bảo vệ an ninh mạng. Các trường đại học có thể cùng hợp tác với các cơ quan chức năng, các đơn vị cung cấp dịch vụ an ninh mạng để cùng nhau giải quyết các vấn đề chung về an ninh mạng.

Luật An ninh mạng góp phần hình thành văn hóa tuân thủ pháp luật, điều này là rất cần thiết trong bối cảnh nhà nước ta đang trong tiến trình hoàn thiện nhà nước pháp quyền. Luật An ninh mạng đặt ra các quy định chặt chẽ về việc bảo vệ thông tin, các hành vi bị cấm trên không gian mạng. Các trường đại học phải đảm bảo tuân thủ nghiêm chỉnh các quy định này. Tuân thủ các quy định nội bộ, mỗi trường đại học cần xây dựng các quy định nội bộ về an ninh mạng và mọi thành viên đều phải tuân thủ.

Luật An ninh mạng góp phần tạo ra văn hóa học hỏi: Luật An ninh mạng khuyến khích các tổ chức không ngừng cập nhật kiến thức về an ninh mạng để thích ứng với tình hình mới; Các trường đại học phải tổ chức các khóa đào tạo về an ninh mạng cho cán bộ, giảng viên và sinh viên cũng như khuyến khích các hoạt động nghiên cứu khoa học về an ninh mạng để tìm ra các giải pháp mới, hiệu quả hơn trong vấn đề bảo vệ nguồn dữ liệu. Điều này góp phần hình thành văn hóa học hỏi của các nhà trường.

Luật An ninh mạng góp phần tạo văn hóa trách nhiệm. Trước tiên, đó là trách nhiệm cá nhân, mỗi cá nhân đều có trách nhiệm bảo vệ thông tin của mình và của tổ chức. Sau đó, là trách nhiệm tập thể, trách nhiệm của người đứng đầu cơ quan tổ chức và toàn bộ cộng đồng nhà trường cùng chia sẻ trách nhiệm trong

việc bảo vệ an ninh mạng. Lãnh đạo nhà trường phải chịu trách nhiệm pháp lý nếu xảy ra các vi phạm an ninh mạng. Điều này buộc các nhà lãnh đạo phải quan tâm hơn đến vấn đề an ninh mạng và đầu tư nguồn lực để bảo vệ hệ thống thông tin. Lãnh đạo cần thể hiện rõ ràng cam kết của mình đối với an ninh mạng bằng cách tham gia vào các hoạt động tuyên truyền, đào tạo và xây dựng chính sách. Và như vậy, các trường đại học có trách nhiệm góp phần vào việc bảo vệ an ninh mạng quốc gia.

### 3. Kết luận

Luật An ninh mạng không chỉ là một bộ quy tắc pháp lý mà còn là một động lực mạnh mẽ, góp phần định hình lại văn hóa tổ chức trong các trường đại học. Thông qua việc đưa ra các quy định rõ ràng về bảo mật thông tin, cũng như quy định trách nhiệm của các cá nhân và tổ chức, luật này đã tác động sâu sắc đến cách thức vận hành và tương tác của các trường đại học, từ đó tạo ra một sự thay đổi mạnh mẽ giúp các trường xây dựng một văn hóa tổ chức hướng tới bảo vệ an toàn thông tin. Tuy nhiên, việc xây dựng và phát triển một văn hóa như vậy không phải là điều đơn giản, mà là một quá trình lâu dài, đòi hỏi sự nỗ lực đồng bộ của toàn thể cộng đồng trong các trường đại học.

### TÀI LIỆU THAM KHẢO

- [1] Bộ Giáo dục và Đào tạo (2017), Cẩm nang chuyển đổi số, NXB Thông tin Truyền thông, Hà Nội.
- [2] Bộ Giáo dục và Đào tạo (2022), Quyết định số 4740/QĐ-BGDĐT ngày 06/12/2022 ban hành bộ tiêu chí đánh giá chuyển đổi số cơ sở giáo dục đại học, Hà Nội.
- [3] Thủ tướng Chính phủ (2020), Quyết định số 749/QĐ-TTg ngày 03/6/2020 của Thủ tướng Chính phủ phê duyệt “Chương trình Chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030”, Hà Nội.
- [4] Chính phủ (2022), Quyết định số 131/QĐ-TTg ngày 25/01/2022 của Thủ tướng Chính phủ phê duyệt Đề án “Tăng cường ứng dụng công nghệ thông tin và chuyển đổi số trong giáo dục và đào tạo giai đoạn 2022 - 2025, định hướng đến năm 2030”, Hà Nội.
- [5] Quốc hội (2018), Luật An ninh mạng, Hà Nội.

### ABSTRACT

#### **The impact of the Cybersecurity Law on the organizational and management culture of universities in Vietnam in the context of digital transformation**

In the digital age, universities are undergoing a profound digital transformation. Along with that, the increasing cyber security threats lead to new requirements for information management and security. The Cyber Security Law, as an important legal tool, not only affects technical operations but also reshapes the organizational and management culture of universities. This article will analyze these impacts in detail, and provide suggestions for educational administrators to build an effective cybersecurity culture.

**Keywords:** *Cybersecurity Law, Organizational Culture, Information Security, Individual and Organizational Responsibility, Information Safety.*